Framework Well-Architected da AWS

Pilar de segurança

Pilar de segurança: Framework Well-Architected da AWS

Table of Contents

Pilar Segurança: AWS Well-Architected Framework

Data de publicação: 6 de novembro de 2024 (Revisões do documento)

O foco deste documento é o pilar Segurança do AWS Well-Architected Framework. Ele contém orientações para ajudar você a aplicar práticas recomendadas e outras recomendações atuais ao design, à entrega e à manutenção de workloads da AWS seguras.

Introdução

O AWS Well-Architected Framework explica os prós e os contras das decisões tomadas no momento da criação de workloads na AWS. Ao usar o Framework, você aprenderá as práticas recomendadas atuais de arquitetura para projetar e operar workloads confiáveis, seguras, eficientes, econômicas e sustentáveis na nuvem. Ele oferece uma forma de avaliar consistentemente sua workload em relação às práticas recomendadas e identificar áreas de melhoria. Acreditamos que ter as workloads bem arquitetadas aumenta muito a probabilidade de sucesso nos negócios.

O framework é baseado em seis pilares:

- Excelência operacional
- Segurança
- Confiabilidade
- Eficiência de performance
- Otimização de custo
- Sustentabilidade

Este documento aborda o pilar Segurança. Ele ajudará você a cumprir requisitos empresariais e normativos seguindo as recomendações atuais da AWS. Ele se destina às pessoas com funções de tecnologia, como diretores de tecnologia (CTOs), diretores de segurança da informação (CSOs/CISOs), arquitetos, desenvolvedores e membros da equipe de operações.

Depois de ler este documento, você compreenderá as recomendações e as estratégias atuais da AWS para projetar arquiteturas de nuvem com foco em segurança. Este documento não fornece detalhes de implementação ou padrões de arquitetura; no entanto, inclui referências a recursos relevantes para essas informações. Ao adotar as práticas deste documento, você poderá criar

arquiteturas que protegem dados e sistemas, controlam o acesso e respondem automaticamente a eventos de segurança.

Fundamentos de segurança

O pilar de segurança descreve como aproveitar as tecnologias de nuvem para proteger dados, sistemas e ativos de uma forma que possa melhorar sua postura de segurança. Este documento fornece orientações detalhadas sobre práticas recomendadas para a arquitetura de sistemas confiáveis na AWS.

Princípios de design

Na nuvem, existem vários princípios que podem ajudá-lo a fortalecer a segurança da workload:

- Implementar uma base sólida de identidade: implemente o princípio do privilégio mínimo e separe as tarefas com autorização apropriada para cada interação com os recursos da AWS. Centralize o gerenciamento de identidades e procure eliminar a dependência de credenciais estáticas de longo prazo.
- Manter a rastreabilidade: monitore, alerte e examine ações e alterações em seu ambiente em tempo real. Integre a coleta de logs e métricas aos sistemas para investigar e executar ações automaticamente.
- Aplicar segurança em todas as camadas: aplique uma abordagem de defesa detalhada com vários controles de segurança. Aplique a todas as camadas (por exemplo, borda da rede, VPC, balanceamento de carga, cada instância e serviço de computação, sistema operacional, aplicação e código).
- Automatizar as práticas recomendadas de segurança: os mecanismos de segurança automatizados baseados em software aprimoram sua capacidade de dimensionar com segurança e de forma mais rápida e econômica. Crie arquiteturas seguras, incluindo a implementação de controles definidos e gerenciados como código em modelos controlados por versão.
- Proteger dados em trânsito e em repouso: classifique seus dados em níveis de confidencialidade e use mecanismos, como criptografia, tokenização e controle de acesso, quando apropriado.
- Manter as pessoas afastadas dos dados: crie mecanismos e ferramentas para reduzir ou eliminar a necessidade de acesso direto ou processamento manual de dados. Isso reduz o risco de erros de processamento ou modificação e erro humano ao manipular dados confidenciais.
- Preparar para eventos de segurança: prepare-se para um incidente com políticas e processos de gerenciamento e investigação de incidentes alinhados aos requisitos organizacionais. Execute simulações de resposta a incidentes e use ferramentas com automação para aumentar sua velocidade de identificação, investigação e recuperação.

Definição

A segurança na nuvem é composta por sete áreas:

- Fundamentos de segurança
- Gerenciamento de identidade e acesso
- Detecção
- Proteção da infraestrutura
- Proteção de dados
- Resposta a incidentes
- Segurança da aplicação

Responsabilidade compartilhada

Segurança e conformidade são uma responsabilidade compartilhada entre a AWS e o cliente. Esse modelo compartilhado pode ajudar a reduzir os encargos operacionais do cliente porque a AWS opera, gerencia e controla os componentes do sistema operacional do host e a camada de virtualização, incluindo a segurança física das instalações em que o serviço opera. O cliente assume o gerenciamento e a responsabilidade pelo sistema operacional convidado (inclusive por atualizações e correções de segurança) e por outro software de aplicação associado, bem como pela configuração do firewall dos grupos de segurança fornecido pela AWS. Os clientes devem examinar cuidadosamente os serviços que escolherem, pois suas respectivas responsabilidades variam de acordo com os serviços utilizados, a integração desses serviços ao seu ambiente de TI e as leis e regulamentações aplicáveis. A natureza dessa responsabilidade compartilhada também oferece a flexibilidade e o controle do cliente que permitem a implantação. Conforme mostrado no gráfico a seguir, normalmente essa diferenciação da responsabilidade é mencionada como segurança "da" nuvem versus segurança "na" nuvem.

"Segurança da nuvem" é responsabilidade da AWS: a AWS é responsável pela proteção da infraestrutura que executa todos os serviços oferecidos na Nuvem AWS. Essa infraestrutura é composta por hardware, software, redes e instalações que executam os serviços da Nuvem AWS.

"Segurança na nuvem" é responsabilidade do cliente: a responsabilidade do cliente será determinada pelos serviços da Nuvem AWS selecionados por um cliente. Isso define o volume do trabalho de configuração que o cliente deve executar como parte de suas responsabilidades com a segurança.

Por exemplo, um serviço como o Amazon Elastic Compute Cloud (Amazon EC2) é categorizado como infraestrutura como serviço (IaaS) e, como tal, exige que o cliente execute todas as tarefas necessárias de gerenciamento e configuração de segurança. Os clientes que implantam a instância do Amazon EC2 são responsáveis pelo gerenciamento do sistema operacional convidado (incluindo atualizações e patches de segurança), por todos os utilitários ou software de aplicação que instalarem nas instâncias e pela configuração do firewall fornecido pela AWS (chamado de grupo de segurança) em cada instância. Para serviços abstraídos, como o Amazon S3 e o Amazon DynamoDB, a AWS opera a camada de infraestrutura, o sistema operacional e as plataformas, e os clientes acessam os endpoints para armazenar e recuperar dados. Os clientes são responsáveis por gerenciar seus dados (incluindo opções de criptografia), classificar seus ativos e usar as ferramentas do IAM para aplicar as permissões apropriadas.

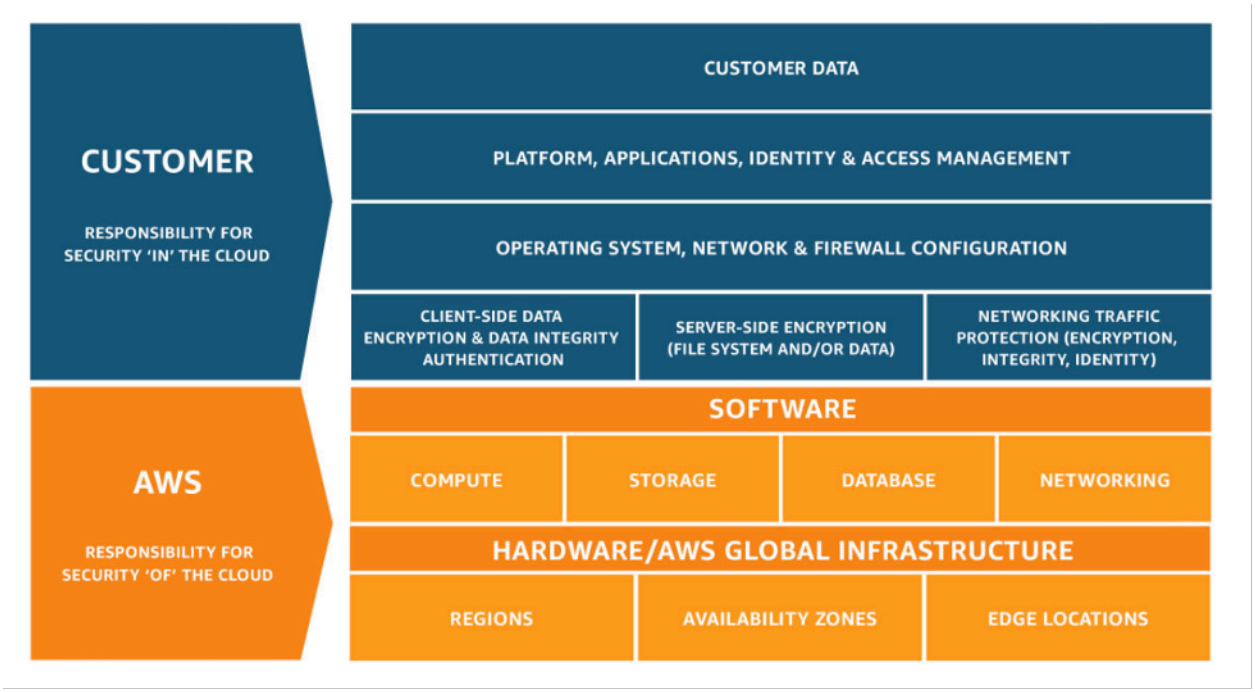


Figura 1: modelo de responsabilidade compartilhada da AWS.

Esse modelo de responsabilidade compartilhada entre o cliente e a AWS também se estende aos controles de TI. Assim como a responsabilidade de operar o ambiente de TI é compartilhada entre a AWS e seus clientes, o gerenciamento, a operação e a verificação dos controles de TI também são compartilhados. A AWS pode ajudar a aliviar a carga de controles operacionais do cliente gerenciando os controles associados à infraestrutura física implantada no ambiente da AWS que pode ter sido gerenciada anteriormente pelo cliente. Já que cada cliente é implantado de forma diferente na AWS, os clientes podem aproveitar a mudança do gerenciamento de determinados controles de TI para a AWS, o que resulta em um (novo) ambiente de controle distribuído. Os clientes podem utilizar a documentação de conformidade e controle da AWS disponível para realizar

procedimentos de avaliação e verificação de controle, conforme necessário. Veja a seguir exemplos de controles gerenciados pela AWS, por clientes da AWS ou por ambos.

Controles herdados: controles que um cliente herda totalmente da AWS.

- Controles físicos e ambientais

Controles compartilhados: controles que se aplicam tanto à camada de infraestrutura quanto às camadas do cliente, mas em contextos ou perspectivas separados. Em um controle compartilhado, a AWS fornece os requisitos para a infraestrutura e o cliente deve fornecer a própria implementação de controle dentro do uso de serviços da AWS. Os exemplos incluem:

- Gerenciamento de aplicação de patches: a AWS é responsável por aplicar patches e corrigir falhas na infraestrutura, mas os clientes são responsáveis por corrigir suas aplicações e sistemas operacionais convidados.
- Gerenciamento de configuração: a AWS mantém a configuração de seus dispositivos de infraestrutura, mas os clientes são responsáveis por configurar os próprios bancos de dados, aplicações e sistemas operacionais convidados.
- Conscientização e capacitação: a AWS capacita os funcionários da AWS, mas os clientes devem capacitar seus próprios funcionários.

Específicos do cliente: controles que são de responsabilidade exclusiva do cliente com base na aplicação que está sendo implantada nos serviços da AWS. Os exemplos incluem:

- Proteção de serviços e comunicações ou segurança de zona, que pode exigir que um cliente roteie ou localize dados em ambientes de segurança específicos.

Governança

A governança de segurança, como um subconjunto da abordagem geral, visa apoiar objetivos de negócios, definindo políticas e objetivos de controle para ajudar a gerenciar riscos. Gerencie os riscos seguindo uma abordagem em camadas para os objetivos de controle de segurança em que cada camada baseia-se na anterior. Compreender o Modelo de Responsabilidade Compartilhada da AWS é a camada mais importante. Esse conhecimento oferece clareza sobre a sua responsabilidade como cliente e o que é herdado da AWS. Um recurso benéfico é o AWS Artifact, que fornece acesso sob demanda aos relatórios de segurança e conformidade e contratos online selecionados da AWS.

Atenda à maioria dos objetivos de controle na próxima camada. É nela que reside a capacidade de toda a plataforma. Por exemplo, essa camada inclui o processo de provisionamento automático de contas da AWS, a integração com um provedor de identidades, como o AWS IAM Identity Center, e os controles de detecção comuns. Alguns dos resultados do processo de governança da plataforma também estão aqui. Quando você quiser começar a usar um novo serviço da AWS, atualize as políticas de controle de serviços (SCPs) no serviço AWS Organizations para fornecer as barreiras de proteção para o uso inicial do serviço. Você pode usar outros SCPs para implementar objetivos comuns de controle de segurança, geralmente chamados de invariantes de segurança. Esses são objetivos de controle ou configuração que você aplica a várias contas, unidades organizacionais ou a toda a organização da AWS. Os exemplos comuns são a limitação das Regiões em que a infraestrutura é executada ou o impedimento da desativação de controles de detecção. Essa camada intermediária também contém políticas codificadas, como regras de configuração ou verificações em pipelines.

A camada superior é onde as equipes de produto atendem aos objetivos de controle. Isso ocorre porque a implementação é feita nas aplicações controladas pelas equipes de produto. Isso pode ser implementar a validação de entrada em uma aplicação ou garantir que a identidade passe entre os microsserviços corretamente. Mesmo que a equipe de produto seja proprietária da configuração, ela ainda pode herdar alguns recursos da camada intermediária.

Independentemente de onde o controle seja implementado, o objetivo continua sendo o gerenciamento de riscos. Uma variedade de estruturas de gerenciamento de riscos se aplica a setores, regiões ou tecnologias específicos. O objetivo principal é destacar o risco com base na probabilidade e na consequência. Esse é o risco inerente. É possível então definir um objetivo de controle que reduza a probabilidade, a consequência ou ambos. Dessa forma, com um controle implementado, você poderá ver qual será o risco resultante. Esse é o risco residual. Os objetivos de controle podem ser aplicados a uma ou várias workloads. O diagrama a seguir mostra uma matriz de risco típica. A probabilidade é baseada na frequência de ocorrências anteriores e a consequência é baseada no custo financeiro, de reputação e de tempo do evento.

Likelihood	Risk Level				
Very Likely	Low	Medium	High	Critical	Critical
Likely	Low	Medium	Medium	High	Critical
Possible	Low	Low	Medium	Medium	High
Unlikely	Low	Low	Medium	Medium	High
Very unlikely	Low	Low		Medium	High
Consequence	Minimal	Low	Medium	High	Severe

Figura 2: Matriz de probabilidade de nível de risco

Gerenciamento e separação de contas da AWS

Recomendamos que organizar workloads em contas separadas e contas de grupo com base na função, nos requisitos de conformidade ou em um conjunto comum de controles, em vez de espelhar a estrutura hierárquica da sua organização. Na AWS, as contas são um limite rígido. Por exemplo, a separação no nível da conta é altamente recomendada para isolar as workloads de produção das de desenvolvimento e teste.

Gerencie contas de maneira centralizada: o AWS Organizations automatiza a criação e o gerenciamento de contas da AWS, além do controle dessas contas após sua criação. Quando você cria uma conta por meio do AWS Organizations, é importante considerar o endereço de e-mail usado, pois esse será o usuário-raiz que permite que a senha seja redefinida. O Organizations permite agrupar contas em unidades organizacionais (UOs), que podem representar ambientes diferentes com base nos requisitos e na finalidade da workload.

Defina controles centralmente: controle o que suas contas da AWS podem fazer, permitindo apenas serviços, Regiões e ações de serviço específicos no nível apropriado. O AWS Organizations permite usar políticas de controle de serviços (SCPs) para aplicar barreiras de proteção de permissão em

nível de organização, unidade organizacional ou conta, que se aplicam a todos os usuários e perfis do AWS Identity and Access Management (IAM). Por exemplo, você pode aplicar uma SCP que restrinja os usuários de iniciar recursos em regiões que você não tenha permitido explicitamente. O AWS Control Tower oferece uma maneira simplificada de configurar e controlar várias contas. Ele automatiza a configuração de contas no AWS Organizations, automatiza o provisionamento, aplica barreiras de proteção (que incluem prevenção e detecção) e fornece um painel para visibilidade.

Configure serviços e recursos de maneira centralizada: o AWS Organizations ajuda você a configurar serviços da AWS que se aplicam a todas as suas contas. Por exemplo, você pode configurar o registro em log centralizado de todas as ações executadas em toda a organização usando o AWS CloudTrail e impedir que as contas-membro desativem o registro em log. Também é possível agregar dados de maneira centralizada para regras definidas usando o AWS Config, o que permite auditar workloads quanto à conformidade e reagir rapidamente a alterações. AWS CloudFormation Os StackSets permitem que você gerencie centralmente pilhas do AWS CloudFormation entre contas e UOs na sua organização. Isso permite provisionar automaticamente uma nova conta para atender aos seus requisitos de segurança.

Use o recurso de administração delegada dos serviços de segurança para separar as contas usadas para gerenciamento da conta de faturamento organizacional (gerenciamento). Vários serviços da AWS, como GuardDuty, Security Hub e AWS Config, oferecem compatibilidade com integrações com o AWS Organizations, incluindo a designação de uma conta específica para funções administrativas.

Práticas recomendadas

- SEC01-BP01 Separar as workloads usando contas
- SEC01-BP02 Proteger as propriedades e o usuário-raiz das contas

SEC01-BP01 Separar as workloads usando contas

Estabeleça barreiras de proteção e isolamento entre workloads e ambientes (como de produção, desenvolvimento e teste) por meio de uma estratégia de várias contas. A separação em nível de conta é altamente recomendável, pois ela oferece um limite de isolamento robusto para segurança, faturamento e acesso.

Resultado desejado: uma estrutura de contas que isola operações em nuvem, workloads não relacionadas e ambientes em contas separadas, aumentando a segurança em toda a infraestrutura de nuvem.

Práticas comuns que devem ser evitadas:

- Colocação de várias workloads não relacionadas com diferentes níveis de confidencialidade na mesma conta.
- Estrutura de unidade organizacional (UO) definida de forma inadequada.

Benefícios de implementar esta prática recomendada:

- Redução do escopo de impacto se uma workload for acessada acidentalmente.
- Governança central de acesso a serviços, recursos e regiões da AWS.
- Manutenção da segurança da infraestrutura de nuvem com políticas e administração centralizada de serviços de segurança.
- Criação de contas automatizada e processo de manutenção.
- Auditoria centralizada da infraestrutura de conformidade e requisitos regulatórios.

Nível de risco exposto se esta prática recomendada não for estabelecida: Alto

Orientação para implementação

As Contas da AWS oferecem um limite de isolamento de segurança entre workloads ou recursos que operam em diferentes níveis de confidencialidade. Para utilizar esse limite de isolamento, a AWS oferece ferramentas para gerenciar em grande escala suas workloads de nuvem por meio de uma estratégia de várias contas. Para obter orientação sobre os conceitos, padrões e implementação de uma estratégia de várias contas na AWS, consulte Organizar seu ambiente da AWS usando várias contas.

Quando você tem várias Contas da AWS no gerenciamento central, elas devem ser organizadas em uma hierarquia definida por camadas de unidades organizacionais (UOs). Desse modo, os controles de segurança podem ser organizados e aplicados às UOs e às contas-membro, estabelecendo controles preventivos consistentes nas contas-membro da organização. Os controles de segurança são herdados, permitindo que você filtre as permissões disponíveis para as contas-membro localizadas em níveis inferiores de uma hierarquia de UOs. Um bom design aproveita essa herança para reduzir o número e a complexidade das políticas de segurança necessárias para obter os controles de segurança desejados para cada conta-membro.

AWS Organizations e AWS Control Tower são dois serviços que podem ser usados para implementar e gerenciar essa estrutura de várias contas em seu ambiente da AWS. O AWS Organizations permite que você organize contas em uma hierarquia definida por uma ou mais camadas de UOs, onde cada UO contém várias contas-membro. As políticas de controle de serviços

(SCPs) permitem que o administrador da organização estabeleça controles preventivos granulares nas contas-membro, e o AWS Config pode ser usado para estabelecer controles proativos e de detetive nas contas-membro. Muitos serviços da AWS se integram ao AWS Organizations para fornecer controles administrativos delegados e realizar tarefas específicas do serviço em todas as contas-membro da organização.

Em cima do AWS Organizations, o AWS Control Tower fornece uma configuração de práticas recomendadas com um clique para um ambiente da AWS de várias contas com uma zona de pouso. A zona de pouso é o ponto de entrada para o ambiente de várias contas estabelecido pelo Control Tower. O Control Tower oferece vários benefícios em relação ao AWS Organizations. Três benefícios que oferecem governança aprimorada de contas são:

- Controles de segurança obrigatórios e integrados que são aplicados automaticamente às contas admitidas na organização.
- Controles opcionais que podem ser ativados ou desativados em determinado conjunto de UOs.
- O AWS Control Tower Account Factory fornece implantação automatizada de contas contendo linhas de base e opções de configuração pré-aprovadas em sua organização.

Etapas de implementação

1. Projete uma estrutura de unidade organizacional: uma estrutura de unidade organizacional projetada adequadamente reduz a carga de gerenciamento necessária para criar e manter políticas de controle de serviços e outros controles de segurança. A estrutura da unidade organizacional deve estar alinhada às necessidades da empresa, à sensibilidade dos dados e à estrutura da workload.
2. Crie uma zona de pouso para seu ambiente de várias contas: uma zona de pouso fornece uma base consistente de segurança e infraestrutura a partir da qual sua organização pode desenvolver, lançar e implantar workloads rapidamente. Você pode usar uma zona de pouso personalizada ou o AWS Control Tower para orquestrar seu ambiente.
3. Estabeleça barreiras de proteção: implemente proteções de segurança consistentes para seu ambiente em sua zona de pouso. O AWS Control Tower fornece uma lista de controles obrigatórios e opcionais que podem ser implantados. Os controles obrigatórios são implantados automaticamente na implementação do Control Tower. Leia a lista de controles opcionais e altamente recomendados e implemente controles adequados às suas necessidades.
4. Restrinja o acesso a regiões recém-adicionadas: para novas Regiões da AWS, recursos do IAM como usuários e perfis são propagados somente para as regiões que você especificar. Essa ação

pode ser executada por meio do console ao usar o Control Tower ou ajustando as políticas de permissão do IAM no AWS Organizations.

5. Considere o AWS CloudFormation StackSets: o StackSets ajuda a implantar recursos, incluindo políticas, perfis e grupos do IAM, em diferentes contas e regiões da Contas da AWS por meio de um modelo aprovado.

Recursos

Práticas recomendadas relacionadas:

- SEC02-BP04 Confiar em um provedor de identidades centralizado

Documentos relacionados:

- AWS Control Tower
- Diretrizes de auditoria de segurança da AWS
- Práticas recomendadas do IAM
- Usar o CloudFormation StackSets para provisionar recursos em várias regiões e Contas da AWS
- Perguntas frequentes sobre o Organizations
- Terminologia e conceitos do AWS Organizations
- Práticas recomendadas para Políticas de controle de serviços do AWS Organizations em um ambiente com várias contas
- Guia de referência de gerenciamento de contas da AWS
- Organizar seu ambiente da AWS usando várias contas

Vídeos relacionados:

- Permitir a adoção da AWS em escala por meio de automação e governança
- Práticas recomendadas de segurança à maneira do Well-Architected
- Criar e gerenciar várias contas usando o AWS Control Tower
- Habilitar o Control Tower para organizações existentes

SEC01-BP02 Proteger as propriedades e o usuário-raiz das contas

O usuário-raiz é o mais privilegiado de uma Conta da AWS, com acesso administrativo integral a todos os recursos da conta, e em alguns casos não pode ser restringido por políticas de segurança. Desabilitar o acesso programático ao usuário-raiz, estabelecer controles apropriados para ele e evitar o uso rotineiro desse usuário ajuda a reduzir o risco de exposição acidental das credenciais raiz e o subsequente comprometimento do ambiente de nuvem.

Resultado desejado: proteger o usuário-raiz ajuda a reduzir a chance de que danos acidentais ou intencionais ocorram devido ao uso indevido das credenciais do usuário-raiz. Estabelecer controles de detecção também pode alertar o pessoal apropriado ações são postas em prática com o usuário-raiz.

Práticas comuns que devem ser evitadas:

- Utilizar o usuário-raiz para outras tarefas que não sejam aquelas que exigem credenciais do usuário-raiz.
- Negligenciar os testes dos planos de contingência regularmente a fim de verificar a funcionalidade da infraestrutura, dos processos e dos funcionários essenciais durante uma emergência.
- Considerar apenas o fluxo típico de login de contas e não considerar nem testar métodos de recuperação de contas alternativos.
- Não lidar com DNS, servidores de e-mail e operadoras de telefonia como parte do perímetro de segurança essencial, pois eles são usados no fluxo de recuperação de contas.

Benefícios de implementar esta prática recomendada: proteger o acesso ao usuário-raiz aumenta a confiança de que as ações em sua conta são controladas e auditadas.

Nível de risco exposto se esta prática recomendada não for estabelecida: Alto

Orientação para implementação

A AWS oferece muitas ferramentas para ajudar a proteger sua conta. No entanto, como algumas dessas medidas não estão habilitadas por padrão, é necessário implementá-las diretamente. Leve em consideração essas recomendações como etapas fundamentais para proteger sua Conta da AWS. Ao implementar essas etapas, é importante criar um processo para avaliar e monitorar os controles de segurança de forma contínua.

Ao criar uma Conta da AWS pela primeira vez, você começa com uma identidade que tem acesso completo a todos os recursos e serviços da AWS na conta. Essa identidade é chamada de usuário-

raiz da Conta da AWS. Você pode fazer login como usuário-raiz usando o endereço de e-mail e a senha que usou para criar a conta. Devido ao acesso elevado concedido ao usuário-raiz da AWS, limite o uso do usuário-raiz da AWS à realização de tarefas que o necessitem especificamente dele. As credenciais de login do usuário-raiz devem ser bem protegidas, e a autenticação multifator (MFA) sempre deve ser usada para o usuário-raiz da Conta da AWS.

Além do fluxo de autenticação normal para fazer login com seu usuário-raiz usando um nome de usuário, senha e o dispositivo de autenticação multifator (MFA), há fluxos de recuperação de contas para fazer login com seu usuário-raiz da Conta da AWS com o endereço de e-mail e o número de telefone associados à sua conta. Dessa forma, é igualmente importante proteger a conta de e-mail do usuário-raiz para a qual o e-mail de recuperação é enviado e o número de telefone associado à conta. Além disso, considere possíveis dependências circulares em que o endereço de e-mail associado ao usuário-raiz é hospedado em servidores de e-mail ou recursos de serviço de nome de domínio (DNS) da mesma Conta da AWS.

Quando o AWS Organizations é usado, há várias Contas da AWS, e cada uma tem um usuário-raiz. Uma conta é designada como a conta de gerenciamento e várias camadas de contas-membro podem ser adicionadas à conta de gerenciamento. Priorize a proteção do usuário-raiz de sua conta de gerenciamento e, depois, os usuários-raiz das contas-membro. A estratégia para proteger o usuário-raiz de sua conta de gerenciamento pode diferir da utilizada nos usuários raiz de suas contas-membro, e é possível implementar controles de segurança preventivos nos usuários-raiz dessas contas.

Etapas de implementação

As etapas de implementação a seguir são recomendadas para estabelecer controles para o usuário-raiz. Onde aplicável, as recomendações são cruzadas com o CIS AWS Foundations Benchmark versão 1.4.0. Além dessas etapas, consulte as diretrizes de práticas recomendadas do AWS para proteger sua Conta da AWS e seus recursos.

Controles preventivos

1. Configure informações de contato precisas para a conta.
    a. Essas informações são usadas para o fluxo de recuperação de senha perdida, o fluxo de recuperação de conta de dispositivo MFA perdida e para comunicações com sua equipe sobre segurança crítica.
    b. Utilize um endereço de e-mail hospedado por seu domínio corporativo, preferencialmente uma lista de distribuição, como o endereço de e-mail do usuário-raiz. O uso de uma lista de

distribuição em vez da conta de e-mail de um indivíduo oferece redundância e continuidade adicionais para o acesso à conta raiz por longos períodos.

c. O número de telefone listado nas informações de contato deve ser um telefone dedicado e seguro para esse fim. O número de telefone não deve ser listado nem compartilhado com ninguém.

2. Não crie chaves de acesso para o usuário-raiz. Se houver chaves de acesso, remova-as (CIS 1.4).
   a. Elimine todas as credenciais programáticas de longa duração (chaves de acesso e secretas) para o usuário-raiz.
   b. Se as chaves de acesso do usuário-raiz já existirem, você deverá fazer a transição dos processos usando essas chaves para usar chaves de acesso temporárias de um pefil do AWS Identity and Access Management (IAM) e, em seguida, excluir as chaves de acesso do usuário-raiz.
3. Determine se você precisa armazenar credenciais para o usuário-raiz.
   a. Ao usar o AWS Organizations para criar contas-membro, a senha inicial do usuário-raiz em novas contas-membro é definida como um valor aleatório que não é exposto a você. Considere usar o fluxo de redefinição de senha da sua conta de gerenciamento do AWS Organizations para obter acesso à conta-membro, se necessário.
   b. Para Contas da AWS autônomas ou a conta de gerenciamento do AWS Organizations, considere criar e armazenar de forma segura as credenciais do usuário-raiz. Use MFA para o usuário-raiz
4. Ative os controles preventivos para os usuários-raiz das contas-membro em ambientes de várias contas da AWS.
   a. Considere usar a barreira de proteção Não permitir a criação de chaves de acesso raiz para o usuário-raiz para contas-membro.
   b. Considere usar a barreira de proteção Não permitir ações como o usuário-raiz para contas-membro.
5. Se você precisar de credenciais para o usuário-raiz:
   a. Use uma senha complexa.
   b. Ative a autenticação multifator (MFA) para o usuário-raiz, especialmente para contas (pagantes) de gerenciamento do AWS Organizations (CIS 1.5).
   c. Considere o uso de dispositivos de MFA de hardware para ter resiliência e segurança, pois os dispositivos de uso único reduzem as chances de os dispositivos que contêm seus códigos

de MFA serem reutilizados para outros fins. Garanta que os dispositivos de MFA de hardware alimentados por bateria sejam substituídos regularmente. (CIS 1.6)

- Para configurar a MFA para o usuário-raiz, siga as instruções para criar uma MFA virtual ou um dispositivo com MFA de hardware.

d. Considere inscrever vários dispositivos de MFA para backup. Até 8 dispositivos de MFA são permitidos por conta.

- Observe que a inscrição de mais de um dispositivo de MFA para o usuário-raiz desativa automaticamente o fluxo para recuperar sua conta se o dispositivo de MFA for perdido.

e. Armazene a senha com segurança e considere as dependências circulares se for armazenar a senha eletronicamente. Não armazene a senha de uma forma que exija o acesso à mesma Conta da AWS para obtê-la.

6. Opcional: considere estabelecer um cronograma de rotação de senha periódica para o usuário-raiz.

- As práticas recomendadas de gerenciamento de credenciais dependem de seus requisitos regulatórios e de política. Os usuários-raiz protegidos por MFA não dependem da senha como um único fator de autenticação.
- Alterar a senha do usuário-raiz periodicamente reduz o risco de que uma senha exposta inadvertidamente possa ser usada indevidamente.

Controles de detecção

- Crie alarmes para detectar o uso das credenciais de usuário-raiz (CIS 1.7). O Amazon GuardDuty pode monitorar e alertar sobre o uso da credencial da API do usuário-raiz por meio da descoberta RootCredentialUsage.
- Avalie e implemente os controles de detetive incluídos no pacote de conformidade do pilar Segurança do AWS Well-Architected para AWS Config, ou se estiver usando o AWS Control Tower, os controles altamente recomendados disponíveis no Control Tower.

Orientação operacional

- Determine quem na organização deve ter acesso às credenciais do usuário-raiz.
  - Use uma regra de duas pessoas de forma que um indivíduo tenha acesso a todas as credenciais necessárias e MFA para obter acesso de usuário-raiz.

  - Verifique se é a organização, e não um único indivíduo, que mantém controle sobre o número de telefone e alias de e-mail associados à conta (que são utilizados para redefinição de senha e fluxo de redefinição de MFA).
- Utilize o usuário-raiz apenas como uma exceção (CIS 1.7).
  - O usuário-raiz da AWS não deve ser usado para tarefas diárias, mesmo que sejam tarefas administrativas. Faça login somente como usuário-raiz para realizar tarefas da AWS que exijam o usuário-raiz. Todas as outras ações devem ser realizadas por outros usuários com perfis apropriados.
- Confira periodicamente se o acesso ao usuário-raiz está funcionando de forma que os procedimentos sejam testados antes de uma situação de emergência que exija o uso das credenciais do usuário-raiz.
- Verifique periodicamente se o endereço de e-mail associado à conta e os listados em Contatos alternativos funcionam. Monitore as caixas de entrada de e-mail em busca de notificações de segurança que poderia receber de <abuse@amazon.com>. Além disso, garanta que todos os números de telefone associados à conta estejam funcionando.
- Prepare um procedimento de resposta a incidentes para responder ao mau uso da conta de usuário-raiz. Consulte o Guia de resposta a incidentes de segurança da AWS e as práticas recomendadas na seção Resposta a Incidentes do whitepaper Pilar Segurança para obter mais informações sobre como criar uma estratégia de resposta a incidentes para sua Conta da AWS.

Recursos

Práticas recomendadas relacionadas:

- SEC01-BP01 Separar as workloads usando contas
- SEC02-BP01 Usar mecanismos de início de sessão fortes
- SEC03-BP02 Conceder acesso de privilégio mínimo
- SEC03-BP03 Estabelecer processo de acesso de emergência
- SEC10-BP05 Provisionar acesso previamente

Documentos relacionados:

- AWS Control Tower
- Diretrizes de auditoria de segurança da AWS

- Práticas recomendadas do IAM
- Amazon GuardDuty — alerta de uso da credencial de usuário-raiz
- Orientação passo a passo sobre o monitoramento do uso da credencial de usuário-raiz via CloudTrail
- Tokens MFA aprovados para uso com o AWS
- Implementar o acesso de emergência na AWS
- Os 10 principais itens de segurança para melhorar em sua Conta da AWS
- O que devo fazer se perceber uma atividade não autorizada em minha Conta da AWS?

Vídeos relacionados:

- Permitir a adoção da AWS em escala por meio de automação e governança
- Práticas recomendadas de segurança à maneira do Well-Architected
- Limitar o uso de credenciais de usuário-raiz da AWS: AWS re:inforce 2022: Práticas recomendadas de segurança com o AWS IAM

Operar workloads com segurança

Operar workloads com segurança abrange todo o ciclo de vida de uma workload, desde o design até a criação, execução e melhoria contínua. Uma das formas de melhorar a capacidade de operar com segurança na nuvem é adotar uma abordagem organizacional de governança. Governança significa orientar as decisões de forma consistente, sem depender apenas do bom senso das pessoas envolvidas. O modelo e o processo de governança são a forma como você responde à pergunta "Como sei que os objetivos de controle para determinada workload foram atendidos e são apropriados para essa workload?". Ter uma abordagem consistente para tomar decisões acelera a implantação de workloads e ajuda a elevar o nível do recurso de segurança em sua organização.

Para operar seu workload com segurança, você deve aplicar as práticas recomendadas abrangentes em todas as áreas de segurança. Pegue os requisitos e processos que você definiu em excelência operacional em um nível organizacional e de workload e aplique-os a todas as áreas. Manter-se atualizado com as recomendações do setor e da AWS e a inteligência contra ameaças ajuda você a desenvolver seu modelo de ameaças e seus objetivos de controle. A automação de processos, testes e validação de segurança ajuda a escalar suas operações de segurança.

A automação possibilita consistência e repetibilidade dos processos. As pessoas podem ser boas em várias coisas, mas fazer a mesma coisa repetidamente e de forma consistente sem errar não é uma delas. Mesmo com runbooks bem escritos, você corre o risco de que as pessoas não realizem tarefas repetitivas de forma consistente. Isso acontece quando as pessoas têm diferentes responsabilidades e precisam responder a alertas desconhecidos. A automação, no entanto, responde sempre da mesma forma. A melhor maneira de implantar aplicações é por meio da automação. O código que executa a implantação pode ser testado e usado para realizar a implantação. Isso aumenta a confiança no processo de mudança e reduz o risco de uma mudança com falha.

Para verificar se a configuração atende aos seus objetivos de controle, primeiro teste a automação e a aplicação implantada em um ambiente de não produção. Dessa forma, você pode testar a automação para comprovar que ela executou todas as etapas corretamente. Você também receberá feedback antecipado no ciclo de desenvolvimento e implantação, reduzindo a possibilidade de refazer o trabalho. Para reduzir a probabilidade de erros de implantação, faça alterações de configuração por código, não por pessoa. Caso precise reimplantar uma aplicação, a automação facilitará muito. À medida que objetivos de controle adicionais são definidos, é possível adicioná-los facilmente à automação para todas as workloads.

Em vez de ter proprietários de workloads individuais investindo em segurança específica para elas, economize tempo usando recursos comuns e componentes compartilhados. Alguns exemplos de serviços que várias equipes podem consumir incluem o processo de criação de conta da AWS, identidade centralizada para pessoas, configuração de log comum e criação de imagem de base de contêineres e AMI. Essa abordagem pode ajudar os criadores a melhorar os tempos de ciclo da workload e atender consistentemente aos objetivos de controle de segurança. Quando as equipes são mais consistentes, você pode validar os objetivos de controle e relatar melhor a postura de controle e posição de risco para as partes interessadas.

Práticas recomendadas

- SEC01-BP03 Identificar e validar objetivos de controle
- SEC01-BP04 Manter-se em dia com ameaças e recomendações de segurança
- SEC01-BP05 Reduzir o escopo do gerenciamento de segurança
- SEC01-BP06 Automatizar a implantação de controles de segurança padrão
- SEC01-BP07 Identificar ameaças e priorizar mitigações usando um modelo de ameaça
- SEC01-BP08 Avaliar e implementar regularmente novos serviços e recursos de segurança

SEC01-BP03 Identificar e validar objetivos de controle

Com base em seus requisitos de conformidade e riscos identificados no modelo de ameaça, derive e valide os objetivos de controle e os controles que você precisa aplicar à workload. A validação contínua de objetivos de controle e controles ajuda a medir a eficácia da mitigação de riscos.

Resultado desejado: os objetivos de controle de segurança da sua empresa estão bem definidos e alinhados aos seus requisitos de conformidade. Os controles são implementados e aplicados por meio de automação e políticas, bem como continuamente avaliados quanto à respectiva eficácia para alcançar seus objetivos. As evidências de eficácia em determinado momento e durante um período de tempo podem ser facilmente relatadas aos auditores.

Práticas comuns que devem ser evitadas:

- Os requisitos regulatórios, as expectativas de mercado e os padrões do setor de garantia de segurança não são claros para sua empresa.
- Seus frameworks de segurança cibernética e seus objetivos de controle estão desalinhados em relação aos requisitos de sua empresa.
- A implementação de controles não se alinha de maneira consistente e mensurável aos seus objetivos de controle.
- Você não usa a automação para relatar a eficácia de seus controles.

Nível de risco exposto se esta prática recomendada não for estabelecida: Alto

Orientação para implementação

Há muitos frameworks comuns de segurança cibernética que podem servir de base para seus objetivos de controle de segurança. Considere os requisitos regulatórios, as expectativas de mercado e os padrões do setor aplicáveis à sua empresa a fim de determinar quais frameworks atendem melhor às suas necessidades. Os exemplos incluem AICPA SOC 2, HITRUST, PCI-DSS, ISO 27.001 e NIST SP 800-53.

Com relação aos objetivos de controle identificados, entenda como os serviços da AWS que você consome ajudam a atingi-los. Use o AWS Artifact para encontrar documentação e relatórios alinhados às suas estruturas de destino que descrevam o escopo de responsabilidade coberto pela AWS e orientações para o escopo restante que é de sua responsabilidade. Para obter mais orientações específicas do serviço, conforme elas se alinham a várias declarações de controle da estrutura, consulte os Guias de conformidade do cliente da AWS.

Ao definir os controles que viabilizam seus objetivos, codifique a imposição usando controles preventivos e automatize a mitigação usando controles de detecção. Ajude a evitar configurações e ações de recursos fora de conformidade em todo o seu AWS Organizations por meio do uso políticas de controle de serviços (SCP). Implemente regras no AWS Config para monitorar e relatar recursos fora de conformidade e, em seguida, mude as regras para um modelo de fiscalização quando estiver confiante em seu comportamento. Para implantar conjuntos de regras predefinidas e gerenciadas que se alinham às suas estruturas de segurança cibernética, avalie o uso de padrões do AWS Security Hub como sua primeira opção. O padrão de Práticas de Segurança Básica da AWS (FSBP) e o CIS AWS Foundations Benchmark são bons pontos de partida e têm controles que se alinham a muitos objetivos que são compartilhados em vários frameworks padrão. Onde o Security Hub não tem intrinsecamente as detecções de controle desejadas, ele pode ser complementado usando pacotes de conformidade do AWS Config.

Use pacotes de parceiros da APN recomendados pela equipe AWS Global Security and Compliance Acceleration (GSCA) para obter assistência de consultores de segurança, agências de consultoria, sistemas de coleta de evidências e relatórios, auditores e outros serviços complementares quando necessário.

Etapas de implementação

1. Avalie frameworks comuns de segurança cibernética e alinhe seus objetivos de controle aos escolhidos.
2. Obtenha documentação relevante sobre orientações e responsabilidades pelo uso de seu framework usando o AWS Artifact. Entenda quais partes da conformidade enquadram-se no modelo de responsabilidade compartilhada da AWS e quais partes são de sua responsabilidade.
3. Use SCPs, políticas de recursos, políticas de confiança de perfil e outras barreiras de proteção para evitar configurações e ações de recursos fora de conformidade.
4. Avalie a implantação de padrões do Security Hub e de pacotes de conformidade do AWS Config que se alinhem aos seus objetivos de controle.

Recursos

Práticas recomendadas relacionadas:

- SEC03-BP01 Definir requisitos de acesso
- SEC04-BP01 Configurar o registro em log de serviços e aplicações
- SEC07-BP01 Compreender seu esquema de classificação de dados

- OPS01-BP03 Avaliar os requisitos de governança
- OPS01-BP04 Avaliar os requisitos de conformidade
- PERF01-BP05 Usar políticas e arquiteturas de referência
- COST02-BP01 Desenvolver políticas com base nos requisitos da sua organização

Documentos relacionados:

- Guias de conformidade do cliente da AWS

Ferramentas relacionadas:

- AWS Artifact

SEC01-BP04 Manter-se em dia com ameaças e recomendações de segurança

Mantenha-se em dia com as ameaças e mitigações mais recentes monitorando as publicações de inteligência contra ameaças do setor e os feeds de dados para atualizações. Avalie as ofertas de serviços gerenciados que são atualizadas automaticamente com base nos dados de ameaças mais recentes.

Resultado desejado: você se mantém informado à medida que as publicações do setor são atualizadas com as ameaças e recomendações mais recentes. Você usa a automação para detectar possíveis vulnerabilidades e exposições à medida que identifica novas ameaças. Você toma medidas de mitigação contra essas ameaças. Você adota serviços da AWS que são atualizados automaticamente com a inteligência de ameaças mais recente.

Práticas comuns que devem ser evitadas:

- Não ter um mecanismo confiável e repetível para se manter em dia com as últimas informações sobre ameaças.
- Manter um inventário manual do portfólio de tecnologia, das workloads e das dependências que exigem análise humana de possíveis vulnerabilidades e exposições.
- Não ter mecanismos para atualizar workloads e dependências para as versões mais recentes disponíveis que ofereçam mitigações de ameaças conhecidas.

Benefícios de implementar esta prática recomendada: usar fontes de inteligência de ameaças para se manter atualizado reduz o risco de perder mudanças importantes no cenário de ameaças que podem afetar seus negócios. Ter a automação implementada para verificar, detectar e corrigir possíveis vulnerabilidades ou exposições em workloads e dependências pode ajudar você a reduzir os riscos de forma rápida e previsível em comparação com as alternativas manuais. Isso ajuda a controlar o tempo e os custos relacionados à mitigação de vulnerabilidades.

Nível de risco exposto se esta prática recomendada não for estabelecida: Alto

Orientação para implementação

Analise publicações confiáveis de inteligência contra ameaças para ficar por dentro do cenário de ameaças. Consulte a base de conhecimento MITRE ATT&CK para obter documentação sobre táticas, técnicas e procedimentos (TTPs) conhecidos de adversários. Analise a lista de Vulnerabilidades e exposições comuns (CVE) da MITRE para se manter informado sobre vulnerabilidades conhecidas em produtos nos quais você confia. Entenda os riscos críticos das aplicações Web com o popular projeto OWASP Top 10 do Open Worldwide Application Security Project (OWASP).

Mantenha-se em dia com os eventos de segurança da AWS e as etapas de correção recomendadas com os boletins de segurança da AWS para CVEs.

Para reduzir o esforço geral e as despesas indiretas para se manter em dia, considere usar serviços da AWS que incorporam automaticamente novas informações sobre ameaças ao longo do tempo. Por exemplo, o Amazon GuardDuty se mantém atualizado com a inteligência de ameaças do setor para detectar comportamentos anômalos e assinaturas de ameaças em suas contas. O Amazon Inspector mantém automaticamente um banco de dados dos CVEs que usa para seus recursos de verificação contínua atualizados. O AWS WAF e o AWS Shield Advanced fornecem grupos de regras gerenciados que são atualizados automaticamente à medida que novas ameaças surgem.

Revise o pilar de excelência operacional do Well-Architected para gerenciamento e correção automatizados de frotas.

Etapas de implementação

- Assine atualizações de publicações de inteligência contra ameaças que sejam relevantes para sua empresa e setor. Assine os Boletins de segurança da AWS.
- Considere a adoção de serviços que incorporem automaticamente novas informações sobre ameaças, como o Amazon GuardDuty e o Amazon Inspector.

- Implemente uma estratégia de gerenciamento e correção de frotas que se alinhe às práticas recomendadas do pilar Excelência operacional do Well-Architected.

Recursos

Práticas recomendadas relacionadas:

- SEC01-BP07 Identificar ameaças e priorizar mitigações usando um modelo de ameaça
- OPS01-BP05 Avaliar o cenário de ameaças
- OPS11-BP01 Adotar um processo para melhoria contínua

SEC01-BP05 Reduzir o escopo do gerenciamento de segurança

Determine se você pode reduzir seu escopo de segurança usando serviços da AWS que transferem o gerenciamento de determinados controles para a AWS (serviços gerenciados). Esses serviços podem ajudar a reduzir suas tarefas de manutenção de segurança, como provisionamento de infraestrutura, configuração de software, aplicação de patches ou backups.

Resultado desejado: você considera o escopo do seu gerenciamento de segurança ao selecionar AWS serviços para sua workload. O custo referente a despesas gerais de gerenciamento e a tarefas de manutenção (o custo total de propriedade ou TCO) é ponderado em relação ao custo dos serviços que você seleciona, além de outras considerações do Well-Architected. Você incorpora a documentação de controle e conformidade da AWS em seus procedimentos de avaliação e verificação de controle.

Práticas comuns que devem ser evitadas:

- Implantar workloads sem entender completamente o modelo de responsabilidade compartilhada referente aos serviços que você seleciona.
- Hospedar bancos de dados e outras tecnologias em máquinas virtuais sem ter avaliado um serviço gerenciado equivalente.
- Não incluir tarefas de gerenciamento de segurança no custo total de propriedade de tecnologias de hospedagem em máquinas virtuais em comparação com as opções de serviços gerenciados.

Benefícios de implementar esta prática recomendada: o uso de serviços gerenciados pode reduzir sua carga geral de gerenciar controles de segurança operacional, o que pode reduzir seus riscos de

segurança e o custo total de propriedade. O tempo que de outra forma seria gasto em determinadas tarefas de segurança pode ser reinvestido em tarefas que agregam maior valor aos negócios. Os serviços gerenciados também podem reduzir o escopo dos requisitos de conformidade ao transferir alguns requisitos de controle para a AWS.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

Há várias maneiras de integrar os componentes da workload na AWS. A instalação e a execução de tecnologias em instâncias do Amazon EC2 geralmente exigem que você assuma a maior parte da responsabilidade geral pela segurança. Para ajudar a diminuir a sobrecarga de operar determinados controles, identifique serviços gerenciados da AWS que reduzam o escopo da sua parte do modelo de responsabilidade compartilhada e entenda como é possível usá-los em sua arquitetura atual. Os exemplos incluem o uso do Amazon Relational Database Service (Amazon RDS) para implantação de bancos de dados, do Amazon Elastic Kubernetes Service (Amazon EKS) ou do Amazon Elastic Container Service (Amazon ECS) para orquestrar contêineres ou usar opções com tecnologia sem servidor. Ao criar novas aplicações, pense em quais serviços podem ajudar a reduzir o tempo e o custo referentes à implementação e ao gerenciamento de controles de segurança.

Os requisitos de conformidade também podem ser um fator na seleção de serviços. Os serviços gerenciados podem mudar a conformidade de alguns requisitos relacionados à AWS. Converse com sua equipe de conformidade sobre quanto ela se sente confortável para auditar os aspectos dos serviços que você opera e gerencia e aceitar declarações de controle em relatórios de auditoria relevantes da AWS. Você pode fornecer os artefatos de auditoria encontrados no AWS Artifact para seus auditores ou reguladores como evidência dos controles de segurança da AWS. Você também pode usar a orientação de responsabilidade fornecida por alguns dos artefatos de auditoria da AWS para projetar sua arquitetura, junto com os Guias de conformidade do cliente da AWS. Essas orientações ajudam a determinar os controles de segurança adicionais que você deve implementar para atender aos casos de uso específicos do seu sistema.

Ao usar serviços gerenciados, familiarize-se com o processo de atualização de recursos para versões mais recentes (por exemplo, atualizar a versão de um banco de dados gerenciado pelo Amazon RDS ou o runtime de uma linguagem de programação para um perfil do AWS Lambda). Embora o serviço gerenciado possa realizar essa operação para você, configurar o momento da atualização e entender o impacto em suas operações continua sendo sua responsabilidade. Ferramentas como essas AWS Health podem ajudar você a rastrear e gerenciar essas atualizações em todos os seus ambientes.

Etapas de implementação

1. Avalie os componentes da workload que podem ser substituídos por um serviço gerenciado.
   a. Se você estiver migrando uma workload para a AWS, considere a redução do gerenciamento (tempo e despesas) e a diminuição do risco ao avaliar se deve redefinir a hospedagem, refatorar, redefinir a plataforma, reformular, recompilar ou substituir a workload. Às vezes, investimentos adicionais no início de uma migração podem gerar economias significativas no longo prazo.
2. Pense em implementar serviços gerenciados (por exemplo, o Amazon RDS) em vez de instalar e gerenciar suas próprias implantações de tecnologia.
3. Use as orientações sobre responsabilidade no AWS Artifact para ajudar a determinar os controles de segurança que você deve implementar para a workload.
4. Mantenha um inventário dos recursos em uso e esteja sempre a par de novos serviços e abordagens a fim de identificar novas oportunidades para reduzir o escopo.

Recursos

Práticas recomendadas relacionadas:

- PERF02-BP01 Selecionar as melhores opções de computação para as workloads
- PERF03-BP01 Usar um datastore com propósitos específicos que melhor atenda aos requisitos de acesso e armazenamento de dados
- SUS05-BP03 Usar serviços gerenciados

Documentos relacionados:

- Eventos de ciclo de vida planejados para o AWS Health

Ferramentas relacionadas:

- AWS Health
- AWS Artifact
- Guias de conformidade do cliente da AWS

Vídeos relacionados:

- Como faço para migrar para uma instância de banco de dados Amazon RDS ou Aurora MySQL usando o AWS DMS?
- AWS re:Invent 2023: Gerenciar eventos do ciclo de vida dos recursos em grande escala com o AWS Health

SEC01-BP06 Automatizar a implantação de controles de segurança padrão

Aplique práticas modernas de DevOps ao desenvolver e implantar controles de segurança que são padrão em seus ambientes da AWS. Defina controles e configurações de segurança padrão usando modelos de infraestrutura como código (IaC), capture alterações em um sistema de controle de versão, teste as alterações como parte de um pipeline de CI/CD e automatize a implantação de mudanças em seus ambientes da AWS.

Resultado desejado: os modelos de IaC capturam controles de segurança padronizados e os comprometem com um sistema de controle de versão. Os pipelines de CI/CD estão em locais que detectam mudanças e automatizam os testes e a implantação de seus ambientes da AWS. Barreiras de proteção estão em vigor para detectar e emitir alertas sobre configurações incorretas nos modelos antes de prosseguir com a implantação. As workloads são implantadas em ambientes em que há controles padrão em vigor. As equipes têm acesso para implantar configurações de serviço aprovadas por meio de um mecanismo de autoatendimento. Existem estratégias seguras de backup e recuperação para controlar configurações, scripts e dados relacionados.

Práticas comuns que devem ser evitadas:

- Fazer alterações manuais nos controles de segurança padrão por meio de um console da web ou uma interface de linha de comandos.
- Contar com equipes de workload individuais para implementar manualmente os controles definidos por uma equipe central.
- Contar com uma equipe central de segurança para implantar controles em nível de workload a pedido de uma equipe de workload.
- Permitir que as mesmas pessoas ou equipes desenvolvam, testem e implantem scripts de automação de controle de segurança sem a separação adequada de deveres ou freios e contrapesos.

Benefícios de implementar esta prática recomendada: o uso de modelos para definir seus controles de segurança padrão permite rastrear e comparar as alterações ao longo do tempo usando

um sistema de controle de versão. Usar a automação para testar e implantar alterações gera padronização e previsibilidade, aumentando as chances de uma implantação bem-sucedida e reduzindo as tarefas manuais repetitivas. Fornecer um mecanismo de autoatendimento para as equipes de workload implantarem serviços e configurações aprovados reduz o risco de configuração incorreta e uso indevido. Isso também ajuda as equipes a incorporar controles logo no início no processo de desenvolvimento.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

Ao seguir as práticas descritas em SEC01-BP01 Separar workloads por meio de contas, você acabará com várias Contas da AWS para diferentes ambientes que você gerencia usando o AWS Organizations. Embora cada um desses ambientes e workloads possam precisar de controles de segurança distintos, você pode padronizar alguns deles em toda a sua organização. Isso inclui integração de provedores de identidades centralizados, definição de redes e firewalls e configuração de locais padrão para armazenar e analisar logs. Da mesma forma que você pode usar infraestrutura como código (IaC) para aplicar o mesmo rigor do desenvolvimento do código da aplicação ao provisionamento da infraestrutura, você também pode usar o IaC para definir e implantar seus controles de segurança padrão.

Sempre que possível, defina seus controles de segurança de forma declarativa, como em AWS CloudFormation, e armazene-os em um sistema de controle de origem. Use práticas de DevOps para automatizar a implantação de seus controles para obter lançamentos mais previsíveis, realizar testes automatizados usando ferramentas como o AWS CloudFormation Guard e detectar desvios entre os controles implantados e a configuração desejada. É possível usar serviços como AWS CodePipeline, AWS CodeBuild e AWS CodeDeploy para construir um pipeline de CI/CD. Considere a orientação em Organizar seu ambiente da AWS usando várias contas para configurar esses serviços em suas próprias contas, separadas de outros pipelines de implantação.

Você também pode definir modelos para padronizar a definição e a implantação de serviços, configurações e Contas da AWS. Essa técnica permite que uma equipe central de segurança gerencie essas definições e as forneça às equipes de workload por meio de uma abordagem de autoatendimento. Uma maneira de conseguir isso é usar o Service Catalog, onde você pode publicar modelos como produtos que as equipes de workload podem incorporar em suas próprias implantações de pipeline. Se você estiver usando o AWS Control Tower, alguns modelos e controles estarão disponíveis como ponto de partida. O Control Tower também fornece o recurso Account Factory, permitindo que as equipes de workload criem novas Contas da AWS usando os padrões definidos por você. Com esse recurso, não é preciso depender de uma equipe central para aprovar

e criar contas quando elas são identificadas como necessárias pelas equipes de workload. Talvez essas contas precisem isolar diferentes componentes da workload com base em motivos como a função que eles desempenham, a confidencialidade dos dados que estão sendo processados ou o comportamento desses componentes.

Etapas de implementação

1. Determine como você armazenará e manterá os modelos em um sistema de controle de versão.
2. Crie pipelines de CI/CD para testar e implantar modelos. Defina testes para verificar se há configurações incorretas e se os modelos estão de acordo com os padrões da sua empresa.
3. Crie um catálogo de modelos padronizados para as equipes de workload implantarem serviços e Contas da AWS de acordo com suas necessidades.
4. Implemente estratégias seguras de backup e recuperação para suas configurações de controle, scripts e dados relacionados.

Recursos

Práticas recomendadas relacionadas:

- OPS05-BP01 Usar controle de versão
- OPS05-BP04 Usar sistemas de gerenciamento de compilação e implantação
- REL08-BP05 Implantar alterações com automação
- SUS06-BP01 Adotar métodos que podem introduzir rapidamente melhorias na sustentabilidade

Documentos relacionados:

- Organizar seu ambiente da AWS usando várias contas

Exemplos relacionados:

- Automatize a criação de contas e o provisionamento de recursos usando Service Catalog, o AWS Organizations e o AWS Lambda
- Fortaleça o pipeline de DevOps e proteja os dados com o AWS Secrets Manager, o AWS KMS e o AWS Certificate Manager

Ferramentas relacionadas:

- AWS CloudFormation Guard
- Acelerador de zona de pouso na AWS

SEC01-BP07 Identificar ameaças e priorizar mitigações usando um modelo de ameaça

Realize a modelagem de ameaças para identificar e manter um registro atualizado de possíveis ameaças e mitigações associadas para sua workload. Priorize suas ameaças e adapte as mitigações de controles de segurança para prevenir, detectar e responder. Revise e mantenha isso no contexto de sua workload e no cenário de segurança em evolução.

Nível de risco exposto se esta prática recomendada não for estabelecida: Alto

Orientação para implementação

O que é modelagem de ameaças?

"A modelagem de ameaças funciona para identificar, comunicar e entender ameaças e mitigações no contexto da proteção de algo de valor." – Modelagem de ameaças a aplicações do Open Web Application Security Project (OWASP)

Por que você deveria usar um modelo de ameaça?

Os sistemas são complexos e se tornam cada vez mais intrincados e qualificados com o passar do tempo, oferecendo maior valor empresarial e maior satisfação e engajamento do cliente. Isso significa que as decisões de design de TI precisam considerar um número cada vez maior de casos de uso. Essa complexidade e o número de permutações de caso de uso geralmente tornam as abordagens não estruturadas ineficazes para encontrar e mitigar ameaças. Em vez disso, você precisa de uma abordagem sistemática para enumerar as possíveis ameaças ao sistema, elaborar mitigações e priorizá-las a fim de garantir que os recursos limitados de sua organização tenham impacto máximo na melhoria do procedimento geral de segurança do sistema.

A modelagem de ameaças foi projetada para oferecer essa abordagem sistemática com o objetivo de encontrar e resolver problemas na fase inicial do processo de design, quando as mitigações têm custo e esforço relativamente baixos em comparação com a fase posterior do ciclo de vida. Essa abordagem se alinha ao princípio de segurança shift-left do setor. Por fim, a modelagem de ameaças é integrada ao processo de gerenciamento de riscos de uma organização e ajuda a impulsionar as decisões sobre quais controles implementar usando uma abordagem orientada a ameaças.

Quando a modelagem de ameaças deve ser realizada?

Inicie a modelagem de ameaças o quanto antes no ciclo de vida de sua workload. Isso oferece a você maior flexibilidade sobre o que fazer com as ameaças identificadas. Muito semelhante aos bugs de software, quanto mais cedo você identificar as ameaças, mais econômico será resolvê-las. Um modelo de ameaças é um documento ativo e deve continuar a evoluir à medida que suas workloads mudam. Revise seus modelos de ameaça no decorrer do tempo, inclusive quando há uma alteração importante ou uma alteração no cenário de ameaças ou ao adotar um novo recurso ou serviço.

Etapas de implementação

Como podemos realizar a modelagem de ameaças?

Há muitas formas diferentes de realizar a modelagem de ameaças. Muito semelhante às linguagens de programação, há vantagens e desvantagens em cada uma, e é necessário escolher a forma mais adequada para você. Uma abordagem é começar com o Quadro de quatro perguntas para modelagem de ameaças do Shostack, que apresenta perguntas abertas para fornecer estrutura ao seu exercício de modelagem de ameaças:

1. Em que estamos trabalhando?

   A finalidade dessa pergunta é ajudar você a entender e chegar a um acordo sobre o sistema que você está construindo e os detalhes sobre ele que são relevantes para a segurança. Criar um modelo ou diagrama é a forma mais popular de responder a essa pergunta, pois ajuda a visualizar o que você está criando, por exemplo, usando um diagrama de fluxo de dados. Escrever as suposições e os detalhes importantes sobre seu sistema também ajuda a definir o que está no escopo. Isso permite que todos que estão contribuindo para o modelo de ameaças se concentrem na mesma coisa e evitem desvios demorados para tópicos fora do escopo (inclusive versões desatualizadas do sistema). Por exemplo, se você está criando uma aplicação Web, provavelmente não vale a pena criar uma modelagem de ameaças da sequência de inicialização confiável do sistema operacional para clientes de navegador, pois não há nenhuma possibilidade de seu design ter influência nisso.
2. O que pode acontecer de errado?

   É nessa fase que você identifica ameaças ao seu sistema. Ameaças são ações ou eventos acidentais ou intencionais que causam impactos indesejados que podem afetar a segurança de seu sistema. Sem um claro entendimento do que pode dar errado, não há o que fazer sobre isso.

Não há uma lista canônica do que pode dar errado. A criação dessa lista exige um brainstorming e a colaboração entre todos os indivíduos de sua equipe e pessoas relevantes envolvidas no exercício de modelagem de ameaças. Você pode ajudar seu brainstorming usando um modelo para identificar ameaças, como o STRIDE, que sugere diferentes categorias para avaliação: falsificação, adulteração, repúdio, divulgação de informações, negação de serviço e elevação de privilégios. Além disso, talvez você queira ajudar no brainstorming revisando as listas e pesquisas existentes em busca de inspiração, incluindo o OWASP Top 10, o HiTrust Threat Catalog e o catálogo de ameaças da sua própria organização.

3. O que vamos fazer sobre isso?

   Como no caso da primeira pergunta, não há uma lista canônica de todas as mitigações possíveis. A entradas nessa etapa são as ameaças identificadas, as pessoas e as áreas de melhoria da etapa anterior.

   Segurança e conformidade são uma responsabilidade compartilhada entre você e a AWS. É importante entender que ao perguntar "O que vamos fazer a respeito?" você também está perguntando "Quem é responsável por fazer algo a respeito?". Entender o equilíbrio entre suas responsabilidades e as da AWS ajuda a definir o escopo de seu exercício de modelagem de ameaças para as mitigações que estão sob seu controle, que, geralmente, são uma combinação de opções de configuração de serviços da AWS e suas mitigações específicas do sistema.

   Para a parte da AWS da responsabilidade compartilhada, você descobrirá que os serviços da AWS estão no escopo de muitos programas de conformidade. Esses programas ajudam você a entender os controles sólidos implementados na AWS para manter a segurança e a conformidade da nuvem. Os relatórios de auditoria desses programas estão disponíveis para download para clientes da AWS no AWS Artifact.

   Seja quais forem os serviços da AWS que você está utilizando, sempre há um elemento de responsabilidade do cliente, e as mitigações alinhadas a essas responsabilidades devem ser incluídas em seu modelo de ameaças. Para mitigações de controle de segurança dos próprios serviços da AWS, convém considerar a implementação de controles de segurança em todos os domínios; por exemplo, domínios como gerenciamento de identidade e acesso (autenticação e autorização), proteção de dados (em repouso e em trânsito), segurança de infraestrutura, registro em log e monitoramento. A documentação de cada serviço da AWS conta com um capítulo de segurança dedicado que fornece orientação sobre os controles de segurança a serem considerados como mitigações. É importante considerar o código que você está escrevendo e suas dependências e pensar nos controles que você poderia implementar para resolver essas

ameaças. Esses controles podem ser coisas como validação de entrada, tratamento de sessão e tratamento de limites. Com frequência, a maioria das vulnerabilidades é introduzida em código personalizado. Por isso, concentre-se nessa área.

4. Fizemos um bom trabalho?

   O objetivo é a sua equipe e a organização aprimorarem a qualidade dos modelos de ameaças e a velocidade na qual você está realizando a modelagem de ameaças no decorrer do tempo. Essas melhorias vêm de uma combinação entre prática, aprendizado, instrução e revisão. Para se aprofundar e colocar a mão na massa, é recomendável que você e sua equipe concluam o workshop ou curso de treinamento Modelagem de ameaças da maneira certa para construtores. Além disso, se você estiver procurando orientação sobre como integrar a modelagem de ameaças ao ciclo de vida de desenvolvimento de aplicações da sua organização, consulte Como abordar a modelagem de ameaças no blog de segurança da AWS.

Compositor de ameaças

Para obter ajuda e orientação na execução da modelagem de ameaças, considere usar a ferramenta Threat Composer, que visa reduzir o tempo de obtenção de valor na modelagem de ameaças. Essa ferramenta ajuda você a:

- Escrever declarações de ameaças úteis alinhadas à gramática de ameaças que funcionem em um fluxo de trabalho natural não linear
- Gerar um modelo de ameaça legível por humanos.
- Gerar um modelo de ameaça legível por máquina para permitir tratar os modelos de ameaças como código.
- Identificar rapidamente as áreas de melhoria de qualidade e de cobertura usando o painel do Insights.

Para obter mais referências, visite o Threat Composer e alterne para o Exemplo de espaço de trabalho definido pelo sistema.

Recursos

Práticas recomendadas relacionadas:

- SEC01-BP03 Identificar e validar objetivos de controle
- SEC01-BP04 Manter-se em dia com ameaças e recomendações de segurança

- SEC01-BP05 Reduzir o escopo do gerenciamento de segurança
- SEC01-BP08 Avaliar e implementar regularmente novos serviços e recursos de segurança

Documentos relacionados:

- Como abordar a modelagem de ameaças (Blog de segurança da AWS)
- NIST: Guia para modelagem de ameaças a sistemas centrada em dados

Vídeos relacionados:

- AWS Summit ANZ 2021: Como abordar a modelagem de ameaças
- AWS Summit ANZ 2022: Escalar a segurança: otimizar para entrega rápida e segura

Treinamento relacionado:

- Modelagem de ameaças da maneira certa para criadores: treinamento individualizado virtual do AWS Skill Builder
- Modelagem de ameaças da maneira certa para construtores: workshop da AWS

Ferramentas relacionadas:

- Compositor de ameaças

SEC01-BP08 Avaliar e implementar regularmente novos serviços e recursos de segurança

Avalie e implemente serviços e recursos de segurança da AWS e de parceiros da AWS que ajudem você a desenvolver o procedimento de segurança de suas workloads.

Resultado desejado: você tem uma prática padrão em vigor que informa sobre novos recursos e serviços lançados pela AWS e os parceiros da AWS. Você avalia como esses novos recursos influenciam o design dos controles novos e atuais de seus ambientes e workloads.

Práticas comuns que devem ser evitadas:

- Não assinar blogs e feeds RSS da AWS para tomar conhecimento rapidamente de novos recursos e serviços relevantes.
- Recorrer a notícias e atualizações sobre serviços e recursos de segurança de fontes secundárias.
- Não incentivar os usuários da AWS da sua organização a se manterem informados sobre as atualizações mais recentes

Benefícios de implementar esta prática recomendada: ao se manter atualizado sobre os novos serviços e recursos de segurança, você pode tomar decisões informadas sobre a implementação de controles em seus ambientes e workloads na nuvem. Essas fontes ajudam a aumentar a conscientização sobre o cenário de segurança em constante evolução e como os serviços da AWS podem ser usados para impedir ameaças novas e emergentes.

Nível de risco exposto se esta prática recomendada não for estabelecida: Baixo

Orientação para implementação

A AWS informa os clientes sobre novos serviços e recursos de segurança por meio de vários canais:

- Novidades da AWS
- Notícias do blog da AWS
- Blog de segurança da AWS
- Boletins de segurança da AWS
- Visão geral da documentação da AWS

Você pode assinar um tópico do AWS Daily Feature Updates usando o Amazon Simple Notification Service (Amazon SNS) para obter um resumo diário abrangente das atualizações. Alguns serviços de segurança, como o Amazon GuardDuty e o AWS Security Hub, fornecem seus próprios tópicos de SNS para manter você em dia com os novos padrões, descobertas e outras atualizações desses serviços específicos.

Novos serviços e recursos também são anunciados e descritos em detalhes durante conferências, eventos e webinars realizados em todo o mundo a cada ano. Em destaque está a conferência anual de segurança AWS re:Inforce e a conferência mais geral AWS re:Invent. Os canais de notícias da AWS mencionados anteriormente compartilham esses anúncios de conferências sobre segurança e outros serviços, e você pode assistir a sessões educacionais aprofundadas on-line no canal AWS Events no YouTube.

Você também pode perguntar à equipe da sua Conta da AWS sobre as atualizações e recomendações mais recentes do serviço de segurança. Para entrar em contato com sua equipe, use o formulário de Suporte de Vendas se não tiver as informações de contato direto. Da mesma forma, se você se inscreveu no AWS Enterprise Support, receberá atualizações semanais do seu gerente técnico de contas (TAM) e poderá agendar uma reunião regular de revisão com ele.

Etapas de implementação

1. Assine vários blogs e boletins com o leitor de RSS de sua preferência ou o tópico de atualizações diárias de recursos do SNS.
2. Avalie de quais eventos da AWS você deve participar para saber em primeira mão sobre novos recursos e serviços.
3. Agende reuniões com a equipe da sua Conta da AWS para esclarecer dúvidas sobre a atualização de serviços e recursos de segurança.
4. Considere a possibilidade de assinar o Enterprise Support para consultar regularmente um gerente técnico de contas (TAM).

Recursos

Práticas recomendadas relacionadas:

- PERF01-BP01 Conhecer e compreender os serviços e recursos de nuvem disponíveis
- COST01-BP07 Manter-se em dia com os novos lançamentos de serviços

Gerenciamento de identidade e acesso

Para usar os serviços da AWS, é necessário conceder aos usuários e aplicações acesso a recursos em suas contas da AWS. À medida que executa mais workloads na AWS, você precisa de gerenciamento de identidade robusto e de permissões implementadas para garantir que as pessoas certas tenham acesso aos recursos certos nas condições certas. A AWS oferece uma grande variedade de recursos para ajudar a gerenciar identidades humanas e de máquinas e suas permissões. As práticas recomendadas para esses recursos se encaixam em duas áreas principais.

Tópicos

Gerenciamento de identidades

Há dois tipos de identidades que você precisa gerenciar ao abordar a operação de workloads seguros da AWS.

- Identidades humanas: as identidades humanas que exigem acesso aos ambientes e aplicações da AWS podem ser categorizadas em três grupos: força de trabalho, terceiros e usuários.

  O grupo força de trabalho inclui administradores, desenvolvedores e operadores que são membros da sua organização. Eles precisam de acesso para gerenciar, criar e operar os recursos da AWS.

  Terceiros são colaboradores externos, como prestadores de serviços, fornecedores ou parceiros. Eles interagem com os recursos da AWS como parte do engajamento com a organização.

  Os usuários são os consumidores das aplicações. Eles acessam os recursos da AWS por meio de um navegador da web, aplicações-cliente, aplicativos móveis ou ferramentas interativas de linha de comandos.
- Identidades de máquina: suas aplicações de workload, ferramentas operacionais e componentes precisam de uma identidade para solicitar serviços da AWS, como ler dados. Essas identidades também incluem máquinas em execução no ambiente da AWS, como instâncias do Amazon EC2 ou funções do AWS Lambda. Você também pode gerenciar identidades de máquina para partes externas, ou máquinas fora da AWS, que exigem acesso ao seu ambiente da AWS.

Práticas recomendadas

- SEC02-BP01 Usar mecanismos de início de sessão fortes
- SEC02-BP02 Usar credenciais temporárias
- SEC02-BP03 Armazenar e usar segredos com segurança
- SEC02-BP04 Confiar em um provedor de identidades centralizado
- SEC02-BP05 Auditar e fazer a rotação das credenciais periodicamente
- SEC02-BP06 Utilizar grupos de usuários e atributos

SEC02-BP01 Usar mecanismos de início de sessão fortes

Os inícios de sessão (autenticação com credenciais de login) podem apresentar riscos quando não são usados mecanismos, como autenticação multifator (MFA), especialmente em situações em que as credenciais de login foram divulgadas acidentalmente ou podem ser deduzidas com facilidade. Utilize mecanismos de início de sessão fortes para reduzir essas riscos exigindo MFA e políticas de senhas fortes.

Resultado desejado: reduzir os riscos de acesso não intencional às credenciais na AWS usando mecanismos de login robustos para usuários do AWS Identity and Access Management (IAM), o usuário-raiz da Conta da AWS, o AWS IAM Identity Center e provedores de identidade terceirizados. Isso significa exigir MFA, impor políticas de senhas fortes e detectar comportamento de login anômalo.

Práticas comuns que devem ser evitadas:

- Não impor uma política de senhas fortes para suas identidades incluindo senhas complexas e MFA.
- Compartilhar as mesmas credenciais entre usuários diferentes.
- Não utilizar controles de detecção para logins suspeitos.

Nível de risco exposto se esta prática recomendada não for estabelecida: Alto

Orientação para implementação

Há muitas maneiras pelas quais identidades humanas podem iniciar sessão na AWS. É prática recomendada da AWS confiar em um provedor de identidades centralizado utilizando federação

(federação direta SAML 2.0 entre o AWS IAM e o IdP centralizado, ou usando o Centro de Identidade do AWS IAM) ao realizar a autenticação na AWS. Nesse caso, estabeleça um processo de início de sessão seguro com o provedor de identidades ou o Microsoft Active Directory.

Ao abrir pela primeira vez uma Conta da AWS, você começa com um usuário-raiz da Conta da AWS. Você só deve usar o usuário-raiz da conta para configurar o acesso para seus usuários (e para tarefas que exijam o usuário-raiz). É importante ativar a autenticação multifator (MFA) para o usuário-raiz da conta imediatamente após abrir sua Conta da AWS e proteger o usuário-raiz usando o guia de práticas recomendadas da AWS.

O Centro de Identidade do AWS IAM foi projetado para usuários da força de trabalho, e você pode criar e gerenciar identidades de usuários dentro do serviço e proteger o processo de login com MFA. O AWS Cognito, por outro lado, foi projetado para gerenciamento de identidade e acesso de clientes (CIAM), que fornece grupos de usuários e provedores de identidades para usuários externos nas aplicações.

Se você criar usuários no Centro de Identidade do AWS IAM, proteja o processo de início de sessão nesse serviço e ative a MFA. Para identidades de usuários externos, é possível usar grupos de usuários do Amazon Cognito e proteger o processo de início de sessão nesse serviço ou usar um dos provedores de identidades compatíveis com os grupos de usuários do Amazon Cognito.

Além disso, para usuários do Centro de Identidade do AWS IAM, você pode usar o Acesso Verificado pela AWS para fornecer uma camada adicional de segurança, verificando a identidade do usuário e a postura do dispositivo antes que tenha acesso aos recursos da AWS.

Se você estiver utilizando usuários do AWS Identity and Access Management (IAM), proteja o processo de início de sessão usando o IAM.

Você pode usar o Centro de Identidade do AWS IAM e a federação direta do IAM simultaneamente para gerenciar o acesso à AWS. Você pode usar a federação do IAM para gerenciar o acesso ao AWS Management Console e aos serviços e o Centro de Identidade do IAM para gerenciar o acesso a aplicações empresariais, como o QuickSight ou o Amazon Q Business.

Seja qual for o método de início de sessão, é essencial impor uma política de login forte.

Etapas de implementação

Veja a seguir as recomendações gerais de início de sessão forte. As configurações reais que você configurar deverão ser definidas pela política da sua empresa ou usar um padrão como o NIST 800-63.

- Solicite a MFA. É prática recomendada do IAM exigir MFA para identidades humanas e workloads. A ativação da MFA oferece uma camada adicional de segurança que exige que os usuários forneçam credenciais de início de sessão e uma senha de uso único (OTP) ou uma string gerada e verificada criptograficamente por um dispositivo de hardware.
- Imponha um comprimento mínimo de senha, que é um fator essencial da força da senha.
- Imponha complexidade para tornar as senhas mais difíceis de deduzir.
- Permitir que os usuários troquem suas próprias senhas.
- Crie identidades individuais em vez de credenciais compartilhadas. Com a criação de identidades individuais, é possível fornecer a cada usuário um conjunto exclusivo de credenciais de segurança. Os usuários individuais oferecem a capacidade de auditar a atividade de cada usuário.

Recomendações do Centro de Identidade do IAM:

- O Centro de Identidade do IAM fornece uma política de senha predefinida ao usar o diretório padrão que estabelece o tamanho, a complexidade e os requisitos de reutilização da senha.
- Ative o MFA e defina a configuração contextual ou sempre ativa do MFA quando a fonte de identidade for o diretório padrão, o AWS Managed Microsoft AD ou o AD Connector.
- Permita que os usuários registrem seus próprios dispositivos de MFA.

Recomendações do diretório de grupos de usuários do Amazon Cognito:

- Configure as opções de força da senha.
- Exija MFA para os usuários.
- Use as configurações de segurança avançadas dos grupos de usuários do Amazon Cognito para recursos como a autenticação adaptativa, a qual pode bloquear logins suspeitos.

Recomendações para usuários do IAM:

- Em teoria, você está utilizando Centro de Identidade do IAM ou federação direta. No entanto, talvez você precise de usuários do IAM. Nesse caso, defina uma política de senhas para usuários do IAM. A política de senhas pode ser usada para definir requisitos como extensão mínima ou a obrigatoriedade de uso de caracteres não alfabéticos.
- Crie uma política do IAM para impor o início de sessão com MFA para que os usuários possam gerenciar suas próprias senhas e dispositivos de MFA.

Recursos

Práticas recomendadas relacionadas:

- SEC02-BP03 Armazenar e usar segredos com segurança
- SEC02-BP04 Confiar em um provedor de identidades centralizado
- SEC03-BP08 Compartilhar recursos com segurança em sua organização

Documentos relacionados:

- Política de senhas do Centro de Identidade do AWS IAM
- Política de senhas de usuários do IAM
- Definir da senha do usuário-raiz da Conta da AWS
- Política de senhas do Amazon Cognito
- Credenciais da AWS
- Práticas recomendadas de segurança do IAM

Vídeos relacionados:

- Gerenciar permissões de usuário em grande escala com o Centro de Identidade do AWS IAM
- Como dominar a identidade em cada camada do bolo

SEC02-BP02 Usar credenciais temporárias

Ao realizar qualquer tipo de autenticação, é melhor utilizar credenciais temporárias em vez de credenciais de longo prazo a fim de reduzir ou eliminar riscos como credenciais que são divulgadas acidentalmente, compartilhadas ou roubadas.

Resultado desejado: para reduzir o risco de credenciais de longo prazo, use credenciais temporárias sempre que possível para identidades humanas e de máquinas. Credenciais de longo prazo criam muitos riscos, como exposição por meio de uploads para repositórios públicos. Ao utilizar credenciais temporárias, você reduz significativamente as chances de comprometimento das credenciais.

Práticas comuns que devem ser evitadas:

- Desenvolvedores que usam chaves de acesso de longo prazo de usuários do IAM em vez de obter credenciais temporárias da CLI usando federação.

- Desenvolvedores que incorporam chaves de acesso de longo prazo no código e fazem upload desse código para repositórios públicos do Git.
- Desenvolvedores que incorporam chaves de acesso de longo prazo em aplicações móveis que, depois, são disponibilizadas em lojas de aplicações.
- Usuários que compartilham chaves de acesso de longo prazo com outros usuários ou funcionários que deixam a empresa e não devolvem as chaves de acesso de longo prazo.
- Utilizar chaves de acesso de longo prazo para identidades de máquina quando é possível usar credenciais temporárias.

Nível de risco exposto se esta prática recomendada não for estabelecida: Alto

Orientação para implementação

Utilize credenciais de segurança temporárias em vez de credenciais de longo prazo para todas as solicitações à AWS API e CLI. As solicitações de API e CLI para serviços da AWS devem, em quase todos os casos, ser assinadas usando chaves de acesso da AWS. Essas solicitações podem ser assinadas com credenciais temporárias ou de longo prazo. A única vez em que você deve usar credenciais de longo prazo, também conhecidas como chaves de acesso de longo prazo, é se estiver usando um usuário do IAM ou o usuário-raiz da Conta da AWS. Quando você se federa à AWS ou assume um perfil do IAM por meio de outros métodos, credenciais temporárias são geradas. Mesmo quando você acessa o AWS Management Console utilizando credenciais de login, credenciais temporárias são geradas para você fazer chamadas para serviços da AWS. Há poucas situações nas quais você precisa de credenciais de longo prazo, e é possível realizar quase todas as tarefas usando credenciais temporárias.

Evitar o uso de credenciais de longo prazo em favor de credenciais temporárias deve andar lado a lado com uma estratégia de reduzir o uso de usuários do IAM em favor da federação e de perfis do IAM. Embora usuários do IAM tenham sido usados para identidades humanas e de máquina no passado, agora recomendamos não utilizá-los para evitar os riscos de utilizar chaves de acesso de longo prazo.

Etapas de implementação

Identidades humanas

Para identidades da força de trabalho, como funcionários, administradores, desenvolvedores e operadores:

- Recomenda-se confiar em um provedor de identidade centralizado e exigir que os usuários humanos usem federação com um provedor de identidades para acessar a AWS usando credenciais temporárias. A federação para os usuários pode ser feita com federação direta para cada Conta da AWS ou usando o Centro de Identidade do AWS IAM e um provedor de identidades escolhido por você. A federação oferece uma série de vantagens em comparação com a utilização de usuários do IAM que vão além de eliminar credenciais de longo prazo. Seus usuários também podem solicitar credenciais temporárias na linha de comando para federação direta ou usando o Centro de Identidade do IAM. Isso significa que há poucos casos de uso que exigem usuários do IAM ou credenciais de longo prazo para seus usuários.

Para identidades de terceiros:

- Ao conceder a terceiros, como provedores de software como serviço (SaaS), acesso aos recursos em sua Conta da AWS, você pode usar funções entre contas e políticas baseadas em recursos. Além disso, você pode usar o fluxo de credenciais de concessão do Amazon Cognito OAuth 2.0 para clientes ou parceiros de SaaS B2B.

Identidades de usuários que acessam os recursos da AWS por meio de um navegador da web, aplicações-cliente, aplicativos móveis ou ferramentas interativas de linha de comandos:

- Se precisar conceder às aplicações para consumidores ou clientes acesso aos seus recursos da AWS, você pode usar bancos de identidades do Amazon Cognito ou grupos de usuários do Amazon Cognito para fornecer credenciais temporárias. As permissões para as credenciais são configuradas por meio dos perfis do IAM. Você também pode definir uma função do IAM separada com permissões limitadas para usuários convidados que não são autenticados.

Identidades de máquina

Para identidades de máquina, talvez seja necessário utilizar credenciais de longo prazo. Nesses casos, exija que as workloads usem credenciais temporárias com perfis do IAM para acessar a AWS.

- Para o Amazon Elastic Compute Cloud (Amazon EC2), é possível usar perfis para o Amazon EC2.
- O AWS Lambda permite configurar um perfil de execução do Lambda para conceder ao serviço permissões para realizar ações AWS usando credenciais temporárias. Há muitos outros modelos semelhantes para os serviços da AWS concederem credenciais temporárias utilizando perfis do IAM.

- Para dispositivos de IoT, você pode usar o provedor de credenciais do AWS IoT Core para solicitar credenciais temporárias.
- Para sistemas on-premises ou sistemas que funcionam fora da AWS e que precisam de acesso a recursos da AWS, é possível usar o IAM Roles Anywhere.

Há cenários em que credenciais temporárias não são compatíveis, o que exige o uso de credenciais de longo prazo. Nessas situações, audite e alterne essas credenciais periodicamente e alterne as chaves de acesso regularmente. Para chaves de acesso de usuário do IAM altamente restritas, considere as seguintes medidas de segurança adicionais:

- Conceda permissões altamente restritas:
  - Siga o princípio do privilégio mínimo (seja específico sobre ações, recursos e condições).
  - Considere conceder ao usuário do IAM somente a operação AssumeRole para uma função específica. Dependendo da arquitetura on-premises, essa abordagem ajuda a isolar e proteger as credenciais de longo prazo do IAM.
- Limite as fontes de rede e os endereços IP permitidos na política de confiança do perfil do IAM.
- Monitore o uso e configure alertas para permissões não utilizadas ou uso indevido (usando filtros métricos e alarmes do AWS CloudWatch Logs).
- Imponha limites de permissão (políticas de controle de serviço (SCPs) e limites de permissão se complementam — os SCPs são granulares, enquanto os limites de permissão são refinados).
- Implemente um processo para provisionar e armazenar com segurança (em um cofre on-premises) as credenciais.

Algumas outras opções para cenários que exigem credenciais de longo prazo incluem:

- Crie sua própria API de venda de tokens (usando o Amazon API Gateway).
- Para cenários em que você precisa usar credenciais de longo prazo, ou para credenciais que não sejam chaves de acesso da AWS (como logins de bancos de dados), é possível usar um serviço projetado para lidar com o gerenciamento de segredos, como o AWS Secrets Manager. O Secrets Manager simplifica o gerenciamento, a rotação e o armazenamento seguro de segredos criptografados. Muitos serviços da AWS oferecem suporte à integração direta com o Secrets Manager.
- Para integrações multinuvem, você pode usar a federação de identidades com base nas credenciais do provedor de serviços de credenciais (CSP) de origem (consulte AWS STS AssumeRoleWithWebIdentity).

Para obter mais informações sobre a mudança de credenciais de longo prazo, consulte a mudança de chaves de acesso

Recursos

Práticas recomendadas relacionadas:

- SEC02-BP03 Armazenar e usar segredos com segurança
- SEC02-BP04 Confiar em um provedor de identidades centralizado
- SEC03-BP08 Compartilhar recursos com segurança em sua organização

Documentos relacionados:

- Credenciais de segurança temporárias
- Credenciais da AWS
- Práticas recomendadas de segurança do IAM
- Perfis do IAM
- Centro de Identidade do IAM
- Provedores de identidade e federação
- Fazer a rotação das chave de acesso
- Soluções para parceiros de segurança: acesso e controle
- O usuário-raiz da conta da AWS
- Acesse AWS usando uma identidade de workload nativa do Google Cloud Platform
- How to access AWS resources from Microsoft Entra ID tenants using AWS Security Token Service

Vídeos relacionados:

- Gerenciar permissões de usuário em grande escala com o Centro de Identidade do AWS IAM
- Como dominar a identidade em cada camada do bolo

SEC02-BP03 Armazenar e usar segredos com segurança

Uma workload exige um recurso automatizado para comprovar a identidade dela em bancos de dados, recursos e serviços de terceiros. Isso é feito com o uso de credenciais de acesso secretas, como chaves de acesso de API, senhas e tokens do OAuth. Utilizar um serviço com

propósito específico para armazenar, gerenciar e fazer a rotação de credenciais ajuda a reduzir a probabilidade de comprometimento dessas credenciais.

Resultado desejado: implementar um mecanismo para gerenciar com segurança credenciais da aplicação que atinja as seguintes metas:

- Identificar quais segredos são necessários para a workload.
- Reduzir o número de credenciais de longo prazo necessárias substituindo-as por credenciais de curto prazo quando possível.
- Estabelecer um armazenamento seguro e uma rotação automatizada das credenciais de longo prazo restantes.
- Auditar o acesso aos segredos existentes na workload.
- Monitorar continuamente para confirmar que nenhum segredo seja incorporado ao código-fonte durante o processo de desenvolvimento.
- Reduzir a probabilidade de divulgação acidental de credenciais.

Práticas comuns que devem ser evitadas:

- Ausência de rotação de credenciais.
- Armazenar credenciais de longo prazo em código-fonte ou arquivos de configuração.
- Armazenar credenciais em repouso não criptografadas.

Benefícios de implementar esta prática recomendada:

- Os segredos são armazenados com criptografia em repouso e em trânsito.
- O acesso às credenciais é controlado por meio de uma API (pense nisso como uma máquina de venda automática de credenciais).
- O acesso a uma credencial (de leitura e gravação) é auditado e registrado.
- Separação de preocupações: a rotação de credenciais é realizada por um componente separado que pode ser segregado do restante da arquitetura.
- Os segredos são automaticamente distribuídos sob demanda em componentes de software e a rotação ocorre em um local central.
- O acesso às credenciais pode ser controlado de forma detalhada.

Nível de risco exposto se esta prática recomendada não for estabelecida: Alto

Orientação para implementação

No passado, as credenciais usadas para realizar a autenticação em bancos de dados, APIs de terceiros, tokens e outros segredos podiam ser incorporadas em código-fonte ou em arquivos do ambiente. A AWS oferece vários mecanismos para armazenar essas credenciais com segurança, alterná-las automaticamente e auditar o uso delas.

A melhor forma de abordar o gerenciamento de segredos é seguir as orientações de remover, substituir e fazer a rotação. A credencial mais segura é a que você não precisa armazenar, gerenciar nem processar. Pode haver credenciais que não sejam mais necessárias ao funcionamento da workload que podem ser removidas com segurança.

Para credenciais que ainda são necessárias ao funcionamento adequado da workload, pode haver uma oportunidade de substituir uma credencial de longo prazo por uma credencial temporária ou de curto prazo. Por exemplo, em vez de codificar uma chave de acesso secreta da AWS, considere substituir essa credencial de longo prazo por uma temporária utilizando perfis do IAM.

Em algumas situações, talvez alguns segredos de longa duração não possam removidos ou substituídos. Esses segredos podem ser armazenados em um serviço, como o AWS Secrets Manager, onde podem ser armazenados, gerenciados e ter a rotação feita centralmente de tempos em tempos.

Uma auditoria do código-fonte da workload e os arquivos de configuração podem revelar muitos tipos de credencial. A seguinte tabela resume as estratégias para lidar com tipos comuns de credenciais:

Tipo de credencial	Descrição	Estratégia sugerida
Chaves de acesso ao IAM	Chaves secretas e de acesso do AWS IAM usadas para assumir perfis do IAM dentro de uma workload	Substitua: em vez disso, use perfis do IAM atribuídos às instâncias de computaçã o (como Amazon EC2 ou AWS Lambda). Para interoper abilidade com terceiros que precisam de acesso a recursos em sua Conta da AWS, pergunte se eles oferecem suporte ao acesso entre contas da AWS. Para

Tipo de credencial	Descrição	Estratégia sugerida
		aplicações móveis, considere usar credenciais temporárias nos bancos de identidades do Amazon Cognito (identidades federadas). Para workloads executadas fora da AWS, considere o usar o IAM Roles Anywhere ou o AWS Systems Manager Hybrid Activations. Para contêineres, consulte Perfil do IAM para tarefas do Amazon ECS ou Perfil do IAM em nós do Amazon EKS.
Chaves SSH	Chaves privadas do Secure Shell usadas para fazer login em instâncias do EC2 Linux, manualmente ou como parte de um processo automatizado	Substitua: use o AWS Systems Manager ou o EC2 Instance Connect para fornecer acesso programát ico e humano às instâncias do EC2 usando perfis do IAM.
Credenciais de aplicações e bancos de dados	Senhas: sequência de texto simples	Rotação: armazene as credenciais no AWS Secrets Manager e estabeleça a rotação automática, se possível.

Tipo de credencial	Descrição	Estratégia sugerida
Credenciais do Amazon RDS e do Aurora Admin Database	Senhas: sequência de texto simples	Substitua: use a integração do Secrets Manager com o Amazon RDS ou o Amazon Aurora. Além disso, alguns tipos de banco de dados do RDS podem usar perfis do IAM em vez de senhas para alguns casos de uso (para obter mais detalhes, consulte Autenticação de banco de dados do IAM).
Tokens OAuth	Tokens secretos: sequência de texto simples	Rotação: armazene tokens no AWS Secrets Manager e configure a rotação automátic a.
Chaves e tokens de API	Tokens secretos: sequência de texto simples	Rotação: armazene no AWS Secrets Manager e estabeleç a a rotação automática, se possível.

Um prática não recomendada comum é incorporar chaves de acesso do IAM a código-fonte, arquivos de configuração ou aplicações móveis. Quando uma chave de acesso do IAM for necessária para se comunicar com um serviço da AWS, use credenciais de segurança temporárias (de curto prazo). Essas credenciais de curto prazo podem ser fornecidas por meio de perfis do IAM para instâncias do EC2, funções de execução para funções Lambda, perfis do IAM do Cognito para acesso de usuários móveis e políticas do IoT Core para dispositivos de IoT. Ao interagir com terceiros, prefira delegar acesso a um perfil do IAM com o acesso necessário aos recursos da sua conta em vez de configurar um usuário do IAM e enviar para terceiros a chave de acesso secreta desse usuário.

Há muitos casos em que a workload exige o armazenamento dos segredos necessários para interoperar com outros serviços e recursos. O AWS Secrets Manager foi criado especificamente para gerenciar com segurança essas credenciais, bem como o armazenamento, o uso e a rotação de tokens de API, senhas e outras credenciais.

O AWS Secrets Manager oferece cinco recursos principais para garantir o armazenamento e o manuseio seguros de credenciais confidenciais: criptografia em repouso, criptografia em trânsito, auditoria abrangente, controle de acesso refinado e rotação extensível de credenciais. Outros serviços de gerenciamento de segredos de parceiros da AWS ou soluções desenvolvidas localmente que oferecem recursos e garantias semelhantes também são aceitáveis.

Ao recuperar um segredo, é possível usar os componentes de cache do lado do cliente do Secrets Manager a fim de armazená-lo em cache para uso futuro. Recuperar um segredo armazenado em cache é mais rápido do que recuperá-lo do Secrets Manager. Além disso, como há um custo para chamar APIs do Secrets Manager, usar um cache pode reduzir os custos. Para ver todas as formas pelas quais você pode recuperar segredos, consulte Obter segredos.

> **Note**
>
> Algumas linguagens podem exigir que você implemente sua própria criptografia na memória para o armazenamento em cache do lado do cliente.

Etapas de implementação

1. Identifique caminhos de código contendo credenciais codificadas usando ferramentas automatizadas, como o Amazon CodeGuru.
   a. Utilize o Amazon CodeGuru para verificar seus repositórios de código. Quando a revisão estiver concluída, filtre Type=Secrets no CodeGuru para encontrar linhas de código problemáticas.
2. Identifique credenciais que possam ser removidas ou substituídas.
   a. Identifique credenciais não mais necessárias e marque-as para remoção.
   b. Para chaves secretas da AWS incorporadas ao código-fonte, substitua-as por perfis do IAM associados aos recursos necessários. Se parte da sua workload for externa à AWS, mas exigir credenciais do IAM para acessar os recursos da AWS, considere usar o IAM Roles Anywhere ou o AWS Systems Manager Hybrid Activations.
3. Para outros segredos duradouros de terceiros que exijam o uso da estratégia de rotação, integre o Secrets Manager ao seu código para recuperar segredos de terceiros em tempo de execução.
   a. O console do CodeGuru pode criar automaticamente um segredo no Secrets Manager usando as credenciais descobertas.
   b. Integre a recuperação de segredos do Secrets Manager ao código da sua aplicação.

   i. As funções do Lambda sem servidor podem usar uma extensão do Lambda independente de linguagem.
   ii. Para instâncias ou contêineres do EC2, a AWS fornece exemplos de código do lado do cliente para recuperar segredos do Secrets Manager em várias linguagens de programação populares.
4. Revise periodicamente sua base de código e verifique novamente para confirmar se não há novos segredos adicionados ao código.
   a. Considere usar uma ferramenta como git-secrets para evitar a confirmação de novos segredos em seu repositório de código-fonte.
5. Monitore a atividade do Secrets Manager em busca de indicações de uso inesperado, acesso inadequado a segredos ou tentativas de exclusão de segredos.
6. Reduza a exposição humana às credenciais. Restrinja o acesso a credenciais de leitura, gravação e modificação a um perfil do IAM dedicado a esse fim, e apenas forneça acesso para assumir o perfil a um pequeno subconjunto de usuários operacionais.

Recursos

Práticas recomendadas relacionadas:

- SEC02-BP02 Usar credenciais temporárias
- SEC02-BP05 Auditar e fazer a rotação das credenciais periodicamente

Documentos relacionados:

- Conceitos básicos do AWS Secrets Manager
- Provedores de identidade e federação
- Amazon CodeGuru apresenta o detector de segredos
- Como o AWS Secrets Manager usa o AWS Key Management Service.
- Criptografia e descriptografia de segredos no Secrets Manager
- Entradas de blog do Secrets Manager
- Amazon RDS anuncia integração com AWS Secrets Manager

Vídeos relacionados:

- Práticas recomendadas para gerenciar, recuperar e fazer a rotação de segredos em escala
- Encontrar segredos codificados com o detector de segredos do Amazon CodeGuru
- Proteger segredos para workloads híbridas usando o AWS Secrets Manager

Workshops relacionados:

- Armazenar, recuperar e gerenciar credenciais confidenciais no AWS Secrets Manager
- AWSAtivações híbridas do Systems Manager

SEC02-BP04 Confiar em um provedor de identidades centralizado

Para identidades da força de trabalho (funcionários e prestadores de serviços), confie em um provedor de identidade que permita gerenciar identidades em um local centralizado. Isso facilita o gerenciamento do acesso em várias aplicações e sistemas, pois você está criando, atribuindo, gerenciando, revogando e auditando o acesso de um único local.

Resultado desejado: você tem um provedor de identidade centralizado no qual gerencia centralmente os usuários da força de trabalho, as políticas de autenticação (como a exigência de autenticação multifator (MFA)) e a autorização para sistemas e aplicações (como atribuir acesso com base na associação ou nos atributos do grupo de um usuário). Os usuários da sua força de trabalho fazem login no provedor de identidade central e se federam (autenticação única) a aplicações internas e externas, eliminando a necessidade de os usuários se lembrarem de várias credenciais. Seu provedor de identidade é integrado aos seus sistemas de recursos humanos (RH) para que as mudanças de pessoal sejam automaticamente sincronizadas com seu provedor de identidade. Por exemplo, se alguém deixar sua organização, você poderá revogar automaticamente o acesso a aplicações e sistemas federados (inclusive a AWS). Você habilitou o registro em log detalhado de auditoria em seu provedor de identidade e está monitorando esses logs em busca de comportamentos incomuns do usuário.

Práticas comuns que devem ser evitadas:

- Você não usa federação e autenticação única. Os usuários da sua força de trabalho criam contas de usuário e credenciais separadas em várias aplicações e sistemas.
- Você não automatizou o ciclo de vida das identidades dos usuários da força de trabalho, por exemplo, integrando seu provedor de identidade aos seus sistemas de RH. Quando um usuário deixa sua organização ou muda de função, você segue um processo manual para excluir ou atualizar seus registros em várias aplicações e sistemas.

Benefícios de implementar esta prática recomendada: ao usar um provedor de identidades centralizado, você tem um único local para gerenciar as identidades e políticas dos usuários da força de trabalho, a capacidade de atribuir acesso às aplicações a usuários e grupos e a capacidade de monitorar a atividade de login do usuário. Ao se integrar aos seus sistemas de recursos humanos (RH), quando um usuário muda de função, essas alterações são sincronizadas com o provedor de identidade e atualizam automaticamente as aplicações e permissões atribuídas. Quando um usuário sai da sua organização, sua identidade é automaticamente desativada no provedor de identidade, revogando seu acesso a aplicações e sistemas federados.

Nível de risco exposto se esta prática recomendada não for estabelecida: Alto

Orientação para implementação

Orientação para usuários da força de trabalho que acessam a AWS: os usuários da força de trabalho na organização, como funcionários e prestadores de serviços, podem precisar acessar a AWS usando o AWS Management Console ou a AWS Command Line Interface (AWS CLI) para desempenhar suas funções de trabalho. Você pode conceder acesso à AWS aos usuários da sua força de trabalho federando a partir de seu provedor de identidade centralizado para a AWS em dois níveis: federação direta para cada Conta da AWS ou federação para várias contas em sua organização da AWS.

Para federar os usuários da sua força de trabalho diretamente com cada Conta da AWS, é possível usar um provedor de identidade centralizado para federar o AWS Identity and Access Management na conta em questão. A flexibilidade do IAM permite que você habilite um SAML 2.0 ou um provedor de identidade Open ID Connect (OIDC) separado para cada Conta da AWS e atributos de usuário federados para controle de acesso. Os usuários da sua força de trabalho usarão o navegador da Web para fazer login no provedor de identidade fornecendo suas respectivas credenciais (como senhas e códigos de token MFA). O provedor de identidade emite uma declaração SAML para o navegador, que é enviada ao URL de login do AWS Management Console para permitir que o usuário faça autenticação única no AWS Management Console assumindo um perfil do IAM. Seus usuários também podem obter credenciais da API da AWS temporárias para uso no AWS CLI ou AWS SDKs do AWS STS assumindo o perfil do IAM usando uma declaração SAML do provedor de identidade.

Para federar os usuários da sua força de trabalho com várias contas em sua organização da AWS, é possível usar o Centro de Identidade do AWS IAM para gerenciar centralmente o acesso dos usuários a Contas da AWS e aplicações. Você ativa o Identity Center para sua organização e configura sua fonte de identidade. O IAM Identity Center fornece um diretório de origem de identidade padrão que você pode usar para gerenciar seus usuários e grupos. Como alternativa,

você pode escolher uma fonte de identidade externa conectando-se ao seu provedor de identidade externo usando SAML 2.0 e provisionando automaticamente usuários e grupos usando o SCIM ou conectando-se ao seu Microsoft AD Directory usando o AWS Directory Service. Depois que uma fonte de identidade é configurada, você pode atribuir acesso a usuários e grupos a Contas da AWS definindo políticas de privilégios mínimos em seus conjuntos de permissões. Os usuários da sua força de trabalho podem se autenticar por meio de seu provedor de identidade central para entrar no portal de acesso da AWS e fazer login único nas aplicações em nuvem atribuídas a Contas da AWS eles. Este tópico descreve como configurar a AWS CLI v2 para autenticar o usuário com o Centro de Identidade e obter credenciais para executar comandos da AWS CLI. O Centro de Identidade também permite acesso com login único a aplicações da AWS, como o Amazon SageMaker AI Studio e os portais do AWS IoT Sitewise Monitor.

Depois de seguir as orientações anteriores, os usuários da sua força de trabalho não precisarão mais utilizar usuários e grupos do IAM para operações normais ao gerenciar workloads na AWS. Em vez disso, seus usuários e grupos serão gerenciados fora da AWS e os usuários poderão acessar recursos da AWS como identidade federada. As identidades federadas usam os grupos definidos pelo seu provedor de identidade centralizado. Você deve identificar e remover grupos do IAM, usuários do IAM e credenciais de usuário de longa duração (senhas e chaves de acesso) que não são mais necessárias nas suas Contas da AWS. Você pode encontrar credenciais não utilizadas usando relatórios de credenciais do IAM, excluir os usuários do IAM correspondentes e excluir grupos do IAM. Você pode aplicar uma Política de controle de serviços (SCP) à sua organização que ajuda a impedir a criação de novos usuários e grupos do IAM, impondo esse acesso à AWS por meio de identidades federadas.

> **Note**
>
> Você é responsável por lidar com a rotação dos tokens de acesso do SCIM, conforme descrito na documentação de provisionamento automático. Além disso, você é responsável pela rotação dos certificados que oferecem suporte à federação de identidades.

Orientação para os usuários das aplicações: você pode gerenciar as identidades dos usuários das aplicações, como um aplicativo móvel, usando o Amazon Cognito como provedor de identidades centralizado. O Amazon Cognito habilita a autenticação, autorização e gerenciamento de usuários para suas aplicações Web e móveis. O Amazon Cognito fornece um armazenamento de identidades que pode ser escalado para milhões de usuários, oferece suporte à federação de identidades sociais e corporativas e oferece recursos avançados de segurança para ajudar a proteger seus usuários e negócios. É possível integrar sua aplicação Web ou móvel personalizada ao Amazon Cognito para

adicionar autenticação de usuário e controle de acesso a suas aplicações em minutos. Desenvolvido com base em padrões de identidade abertos, como SAML e Open ID Connect (OIDC), o Amazon Cognito oferece suporte a vários regulamentos de conformidade e se integra aos recursos de desenvolvimento de frontend e backend.

Etapas de implementação

Etapas para usuários da força de trabalho acessarem a AWS

- Federe os usuários da sua força de trabalho à AWS usando um provedor de identidade centralizado de acordo com uma das seguintes abordagens:
  - Use o Centro de Identidade do IAM para habilitar a autenticação única para várias Contas da AWS em sua organização da AWS via federação com seu provedor de identidade.
  - Use o IAM para conectar seu provedor de identidade diretamente a cada Conta da AWS, permitindo acesso federado refinado.
- Identifique e remova usuários e grupos do IAM que são substituídos por identidades federadas.

Etapas para usuários das suas aplicações

- Use o Amazon Cognito como um provedor de identidades centralizado para suas aplicações.
- Integre suas aplicações personalizadas com o Amazon Cognito usando o OpenID Connect e o OAuth. Você pode desenvolver suas aplicações personalizadas usando as bibliotecas do Amplify que fornecem interfaces simples para integração com uma variedade de serviços da AWS, como o Amazon Cognito para autenticação.

Recursos

Práticas recomendadas relacionadas:

- SEC02-BP06 Utilizar grupos de usuários e atributos
- SEC03-BP02 Conceder acesso de privilégio mínimo
- SEC03-BP06 Gerenciar o acesso com base no ciclo de vida

Documentos relacionados:

- Federação de identidades na AWS
- Práticas recomendadas de segurança no IAM

- Práticas recomendadas do AWS Identity and Access Management
- Conceitos básicos da administração delegada no Centro de Identidade do IAM
- Como usar políticas gerenciadas pelo cliente no Centro de Identidade do IAM para casos de uso avançados
- AWS CLI v2: fornecedor de credenciais do Centro de Identidade do IAM

Vídeos relacionados:

- AWS re:Inforce 2022: Mergulho profundo no AWS Identity and Access Management (IAM)
- AWS re:Invent 2022: Simplificar o acesso da sua força de trabalho com o Centro de Identidade do IAM
- AWS re:Invent 2018: Dominar a identidade em todos os aspectos

Exemplos relacionados:

- Workshop: Using AWS IAM Identity Center to achieve strong identity management

Ferramentas relacionadas:

- Parceiros de competência Segurança da AWS: gerenciamento de identidade e acesso
- saml2aws

SEC02-BP05 Auditar e fazer a rotação das credenciais periodicamente

Audite e faça a rotação das credenciais periodicamente para limitar o período durante o qual as credenciais podem ser usadas para acessar seus recursos. Credenciais de longo prazo criam muitos riscos, e estes podem ser reduzidos por meio da rotação periódica das credenciais de longo prazo.

Resultado desejado: implemente a rotação de credenciais para ajudar a reduzir os riscos associados ao uso de credenciais a longo prazo. Audite e corrija regularmente a não conformidade com políticas de rotação de credenciais.

Práticas comuns que devem ser evitadas:

- Não auditar o uso de credenciais.
- Utilizar credenciais de longo prazo desnecessariamente.

- Utilizar credenciais de longo prazo e não fazer sua rotação regularmente.

Nível de risco exposto se esta prática recomendada não for estabelecida: Alto

Orientação para implementação

Quando você não puder contar com credenciais temporárias e exigir credenciais de longo prazo, faça uma auditoria das credenciais para garantir que os controles definidos, por exemplo, autenticação multifator (MFA), sejam aplicados, sofram rotação periódica e tenham o nível de acesso apropriado.

A validação periódica, preferencialmente por meio de uma ferramenta automatizada, é necessária para verificar se os controles corretos são aplicados. Para identidades humanas, exija que os usuários alterem suas senhas periodicamente e substituam chaves de acesso por credenciais temporárias. Ao migrar de usuários do AWS Identity and Access Management (IAM) para identidades centralizadas, você pode gerar um relatório de credenciais para auditar seus usuários.

Também recomendamos implementar e monitorar a MFA no provedor de identidades. É possível configurar o Regras do AWS Config ou usar padrões de segurança do AWS Security Hub para monitorar se os usuários configuraram a MFA. Considere utilizar o IAM Roles Anywhere para fornecer credenciais temporárias para identidades de máquina. Em situações em que o uso de perfis do IAM e credenciais temporárias não é possível, é necessário realizar auditoria frequente e fazer a rotação das chaves de acesso.

Etapas de implementação

- Audite as credenciais periodicamente: a auditoria das identidades configuradas em seu provedor de identidades e no IAM ajuda a garantir que somente identidades autorizadas tenham acesso à sua workload. Essas identidades podem incluir, entre outros, usuários do IAM, usuários do Centro de Identidade do AWS IAM, usuários do Active Directory ou usuários em um provedor de identidades upstream diferente. Por exemplo, remova as pessoas que saem da organização os perfis entre contas que não são mais necessários. Estabeleça um processo para auditar periodicamente as permissões para os serviços acessados por uma entidade do IAM. Isso ajuda a identificar as políticas que você precisa modificar a fim de remover todas as permissões não utilizadas. Use relatórios de credenciais e o AWS Identity and Access Management Access Analyzer para auditar credenciais e permissões do IAM. Você pode usar o Amazon CloudWatch para configurar alarmes para chamadas de API específicas chamadas dentro do seu ambiente. AWS O Amazon GuardDuty também pode alertar você sobre atividades inesperadas, o que pode indicar acesso excessivamente permissivo ou acesso não intencional às credenciais do IAM.

- Faça a rotação das credenciais regularmente: quando não conseguir usar credenciais temporárias, faça a rotação das chaves de acesso do IAM de longo prazo regularmente (máximo a cada 90 dias). Se uma chave de acesso for divulgada acidentalmente sem seu conhecimento, isso limitará o período de uso das credenciais para acessar seus recursos. Para obter mais informações sobre a rotação de chaves de acesso para usuários do IAM, consulte Fazer a rotação das chave de acesso.
- Revise suas permissões do IAM: para melhorar a segurança da sua conta da Conta da AWS, você deve revisar e monitorar regularmente cada uma de suas políticas do IAM. Verifique se as políticas seguem o princípio de privilégio mínimo.
- Considere automatizar a criação e as atualizações de recursos do IAM: o Centro de Identidade do IAM automatiza muitas tarefas do IAM, como gerenciamento de perfis e políticas. Como alternativa, o AWS CloudFormation pode ser usado para automatizar a implantação de recursos do IAM, como perfis e políticas, para reduzir a chance de erros humanos, pois os modelos podem ser verificados e ter controle de versão.
- Use o IAM Roles Anywhere para substituir usuários do IAM por identidades de máquina: o IAM Roles Anywhere permite que você use perfis em áreas que tradicionalmente não poderia, como servidores on-premises. O IAM Roles Anywhere utiliza um certificado X.509 confiável para realizar a autenticação na AWS e receber credenciais temporárias. O uso do IAM Roles Anywhere evita a necessidade de fazer a rotação dessas credenciais, pois credenciais de longo prazo não são mais armazenadas em seu ambiente on-premises. Você precisará monitorar e fazer a rotação do certificado X.509 à medida que ele se aproxima da validade.

Recursos

Práticas recomendadas relacionadas:

- SEC02-BP02 Usar credenciais temporárias
- SEC02-BP03 Armazenar e usar segredos com segurança

Documentos relacionados:

- Conceitos básicos do AWS Secrets Manager
- Práticas recomendadas do IAM
- Provedores de identidade e federação
- Soluções para parceiros de segurança: acesso e controle

- Credenciais de segurança temporárias
- Obter relatórios de credenciais da sua Conta da AWS

Vídeos relacionados:

- Práticas recomendadas para gerenciar, recuperar e fazer a rotação de segredos em escala
- Gerenciar permissões de usuário em grande escala com o Centro de Identidade do AWS IAM
- Como dominar a identidade em cada camada do bolo

SEC02-BP06 Utilizar grupos de usuários e atributos

A definição de permissões de acordo com grupos de usuários e atributos ajuda a reduzir o número e a complexidade das políticas, simplificando o cumprimento do princípio do privilégio mínimo. Você pode usar grupos de usuários para gerenciar permissões para várias pessoas em um só lugar com base na função que elas desempenham em sua organização. Os atributos, como departamento, projeto ou localização, podem ampliar o escopo de permissão quando as pessoas realizam uma função que, embora semelhante, envolve diferentes subconjuntos de recursos.

Resultado desejado: é possível aplicar alterações nas permissões com base na função a todos os usuários que executam essa função. A associação a grupos e os atributos governam as permissões de usuário, reduzindo a necessidade de gerenciar permissões para cada usuário. Os grupos e atributos que você define em seu provedor de identidades (IdP) são propagados automaticamente para seus ambientes da AWS.

Práticas comuns que devem ser evitadas:

- Gerenciar permissões para usuários individuais e duplicá-las entre vários usuários.
- Definir grupos em um nível muito alto, concedendo permissões excessivamente amplas.
- Definir grupos em um nível muito detalhado, criando duplicação e confusão em termos de associação.
- Usar grupos com permissões duplicadas em subconjuntos de recursos quando, em vez disso, é possível usar atributos.
- Não gerenciar grupos, atributos e associações por meio de um provedor de identidades padronizado integrado aos seus ambientes da AWS.
- Usar o encadeamento de perfis ao utilizar sessões do Centro de Identidade do AWS IAM

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

As permissões da AWS são definidas em documentos chamados de políticas, os quais são associados a uma entidade principal, como usuário, grupo, perfil ou recurso. Você pode escalar o gerenciamento de permissões organizando as atribuições de permissões (grupo, permissões, conta) com base na função do trabalho, na workload e no ambiente SDLC. Para sua força de trabalho, isso permite definir grupos com base na função desempenhada pelos usuários dentro da organização, e não nos recursos que estão sendo acessados. Por exemplo, um grupo WebAppDeveloper pode ter uma política anexada para configurar serviços como o Amazon CloudFront em uma conta de desenvolvimento. Um grupo `AutomationDeveloper` pode apresentar sobreposição de algumas permissões com o grupo `WebAppDeveloper`. Essas permissões comuns podem ser capturadas em uma política separada e associadas aos dois grupos, em vez de fazer com que os usuários de ambas as funções pertençam a um grupo `CloudFrontAccess`.

Além dos grupos, você pode usar atributos para controlar melhor o escopo do acesso. Por exemplo, você pode ter um atributo Projeto para os usuários do seu grupo `WebAppDeveloper` para definir o escopo do acesso a recursos específicos do projeto. O uso dessa técnica elimina a necessidade de ter grupos diferentes para desenvolvedores de aplicações que estão trabalhando em diferentes projetos se, em outras circunstâncias, as permissões deles forem as mesmas. A forma como você se refere aos atributos nas políticas de permissão baseia-se na respectiva origem, sejam eles definidos como parte do seu protocolo de federação (por ex., SAML, OIDC ou SCIM) ou como declarações SAML personalizadas, ou definidos dentro do Centro de Identidade do IAM.

Etapas de implementação

1. Estabeleça onde você definirá grupos e atributos:
   a. Seguindo as orientações em SEC02-BP04 Confiar em um provedor de identidades centralizado, é possível determinar se há necessidade de definir grupos e atributos no seu provedor de identidades, no Centro de Identidade do IAM ou com grupos de usuários do IAM em uma conta específica.
2. Defina grupos:
   a. Determine seus grupos com base na função e no escopo de acesso necessário. Considere usar uma estrutura hierárquica ou convenções de nomenclatura para organizar grupos de forma eficaz.
   b. Se estiver definindo no Centro de Identidade do IAM, crie grupos e associe o nível de acesso desejado usando conjuntos de permissões.

c. Se estiver definindo em um provedor de identidades externo, determine se o provedor atende ao protocolo SCIM e considere habilitar o provisionamento automático no Centro de Identidade do IAM. Esse recurso sincroniza a criação, associação e exclusão de grupos entre seu provedor e o Centro de Identidade do IAM.

3. Defina atributos:

a. Se usar um provedor de identidades externo, os protocolos SCIM e SAML 2.0 fornecem determinados atributos por padrão. Atributos adicionais podem ser definidos e transmitidos por meio de declarações SAML usando o nome do atributo `https://aws.amazon.com/SAML/Attributes/PrincipalTag`. Consulte a documentação do provedor de identidades para obter orientação sobre a definição e configuração de atributos personalizados.

b. Se você definir perfis no Centro de Identidade do IAM, habilite o recurso de controle de acesso por atributo (ABAC) e defina os atributos conforme desejado. Considere os atributos que se alinham à estrutura da sua organização ou à estratégia de marcação de recursos.

Se você precisar do encadeamento de perfis do IAM assumidos por meio do Centro de Identidade do IAM, valores como `source-identity` e `principal-tags` não serão propagados. Para mais detalhes, consulte Habilite e configure atributos para controle de acesso.

1. Defina o escopo das permissões com base em grupos e atributos:

a. Considere incluir condições em suas políticas de permissão que comparem os atributos da entidade principal aos atributos dos recursos que estão sendo acessados. Por exemplo, é possível definir uma condição para permitir o acesso a um recurso somente se o valor de uma chave de condição `PrincipalTag` corresponder ao valor de uma chave `ResourceTag` com o mesmo nome.

b. Ao definir as políticas de ABAC, siga as orientações nas práticas recomendadas e exemplos de autorização por ABAC.

c. Revise e atualize regularmente sua estrutura de grupos e atributos à medida que as necessidades de sua organização evoluem para garantir o gerenciamento ideal de permissões.

Recursos

Práticas recomendadas relacionadas:

- SEC02-BP04 Confiar em um provedor de identidades centralizado
- SEC03-BP02 Conceder acesso de privilégio mínimo

- COST02-BP04 Implementar grupos e perfis

Documentos relacionados:

- Práticas recomendadas do IAM
- Gerenciar identidades no Centro de Identidade do IAM
- O que é ABAC para AWS?
- ABAC no Centro de Identidade do IAM
- Exemplos de política de ABAC

Vídeos relacionados:

- Gerenciar permissões de usuário em grande escala com o Centro de Identidade do AWS IAM
- Como dominar a identidade em cada camada do bolo

Gerenciamento de permissões

Gerencie permissões para controlar o acesso a identidades de humanos e máquinas que precisam de acesso à AWS e à suas workloads. Com as permissões, você controla quem pode acessar o quê e em quais condições. Ao definir permissões para identidades humanas e de máquina específicas, você concede a elas acesso a ações de serviço específicas em recursos específicos. Além disso, você pode especificar condições que precisem ser verdadeiras para que o acesso seja concedido.

Há várias maneiras de conceder acesso a diferentes tipos de recursos. Uma maneira é usar diferentes tipos de política.

As políticas baseadas em identidade no IAM são gerenciadas ou em linha e anexadas às identidades do IAM, incluindo usuários, grupos ou perfis. Essas políticas permitem que você especifique o que cada identidade pode fazer (suas respectivas permissões). As políticas baseadas em identidade podem ser subdivididas em outras categorias.

Políticas gerenciadas: políticas autônomas baseadas em identidade que você pode anexar a vários usuários, grupos e funções em sua conta da AWS. Existem dois tipos de políticas gerenciadas:

- Políticas gerenciadas pela AWS: políticas gerenciadas que são criadas e gerenciadas pela AWS.

- Políticas gerenciadas pelo cliente: políticas gerenciadas que você cria e gerencia em sua conta da AWS. As políticas gerenciadas pelo cliente fornecem controle mais preciso sobre suas políticas do que as políticas gerenciadas pela AWS.

As políticas gerenciadas são o método preferencial para aplicar permissões. No entanto, também é possível usar políticas em linha adicionadas diretamente a um único usuário, grupo ou perfil. As políticas em linha mantêm um relacionamento estrito de um para um entre uma política e uma identidade. As políticas em linha são excluídas quando a identidade é excluída.

Na maioria dos casos, é necessário criar suas próprias políticas gerenciadas pelo cliente seguindo o princípio do privilégio mínimo.

Políticas baseadas em recurso são anexadas a um recurso. Por exemplo, uma política de bucket do S3 é uma política baseada em recursos. Essas políticas concedem permissão a uma entidade principal que pode estar na mesma conta que o recurso ou em outra conta. Para obter uma lista de serviços que oferecem suporte a permissões baseadas em recursos, consulte Serviços da AWS que funcionam com o IAM.

Os limites de permissões usam uma política gerenciada para determinar as permissões máximas que um administrador pode definir. Isso permite que você delegue a capacidade de criar e gerenciar permissões para desenvolvedores, como a criação de um perfil do IAM, mas limita as permissões que eles podem conceder para que não possam escalar as próprias permissões usando o que eles criaram.

O Controle de acesso por atributo (ABAC) na AWS permite que você conceda permissões com base em atributos chamados de tags. As tags podem ser anexadas a entidades principais (usuários ou perfis) do IAM e a recursos da AWS. Os administradores podem criar políticas do IAM reutilizáveis que aplicam permissões com base nos atributos da entidade principal do IAM. Por exemplo, como administrador, você pode usar uma única política do IAM que concede aos desenvolvedores em sua organização acesso a recursos da AWS que correspondem às tags de projeto dos desenvolvedores. À medida que a equipe de desenvolvedores adiciona recursos aos projetos, as permissões são aplicadas automaticamente com base em atributos, eliminando a necessidade de atualizações de políticas para cada novo recurso.

As políticas de controle de serviços (SCP) de organizações definem o máximo de permissões para os membros da conta de uma organização ou unidade organizacional (UO). As SCPs limitam as permissões que as políticas baseadas em identidade ou políticas baseadas em recurso concedem a entidades (usuários ou funções) dentro da conta, mas não concedem permissões.

As políticas de sessão assumem uma função ou um usuário federado. Passe as políticas de sessão ao usar as políticas de sessão da AWS CLI ou AWS API para limitar as permissões que as políticas baseadas em identidade do usuário ou da função concedem à sessão. As políticas de sessão limitam as permissões para uma sessão criada, mas não concedem permissões. Para obter mais informações, consulte Políticas de sessão.

Práticas recomendadas

- SEC03-BP01 Definir requisitos de acesso
- SEC03-BP02 Conceder acesso de privilégio mínimo
- SEC03-BP03 Estabelecer processo de acesso de emergência
- SEC03-BP04 Reduzir as permissões continuamente
- SEC03-BP05 Definir barreiras de proteção de permissões para sua organização
- SEC03-BP06 Gerenciar o acesso com base no ciclo de vida
- SEC03-BP07 Analisar o acesso público e entre contas
- SEC03-BP08 Compartilhar recursos com segurança em sua organização
- SEC03-BP09 Compartilhar recursos com terceiros de forma segura

SEC03-BP01 Definir requisitos de acesso

Cada componente ou recurso de seu workload precisa ser acessado por administradores, usuários finais ou outros componentes. Tenha uma definição clara de quem ou o que deve ter acesso a cada componente, escolha o tipo de identidade e o método de autenticação e autorização apropriados.

Práticas comuns que devem ser evitadas:

- Codificação rígida ou armazenamento de segredos em sua aplicação.
- Concessão de permissões personalizadas a cada usuário.
- Uso de credenciais de longa duração.

Nível de risco exposto se esta prática recomendada não for estabelecida: Alto

Orientação para implementação

Cada componente ou recurso de seu workload precisa ser acessado por administradores, usuários finais ou outros componentes. Tenha uma definição clara de quem ou o que deve ter acesso a cada componente, escolha o tipo de identidade e o método de autenticação e autorização apropriados.

O acesso regular a Contas da AWS dentro da organização deve ser fornecido usando acesso federado ou um provedor de identidade centralizado. Você também deve centralizar o gerenciamento de identidade e garantir que haja uma prática estabelecida para integrar o acesso à AWS ao ciclo de vida de acesso dos funcionários. Por exemplo, quando um funcionário muda para um cargo com um nível de acesso diferente, sua associação ao grupo também deve mudar para refletir os novos requisitos de acesso.

Ao definir os requisitos de acesso para identidades não humanas, determine quais aplicações e componentes precisam de acesso e como as permissões são concedidas. O uso de perfis do IAM criados com o modelo de acesso de privilégio mínimo é uma abordagem recomendada. AWS As políticas gerenciadas fornecem políticas do IAM predefinidas que abordam a maioria dos casos de uso comuns.

Serviços da AWS, como AWS Secrets Manager e o AWS Systems Manager Parameter Store, podem ajudar a desacoplar os segredos da aplicação ou workload com segurança em casos em que não é viável usar perfis do IAM. No Secrets Manager, é possível estabelecer uma rotação automática das suas credenciais. É possível usar o Systems Manager para referenciar parâmetros em seus scripts, comandos, documentos do SSM, configurações e fluxos de trabalho de automação usando o nome exclusivo que você especificou ao criar o parâmetro.

É possível usar o AWS IAM Roles Anywhere para obter credenciais de segurança temporárias no IAM para workloads executadas fora da AWS. Suas workloads podem usar as mesmas políticas IAM e os mesmos perfis do IAM que você usa com aplicações da AWS para acessar recursos da AWS.

Quando possível, prefira credenciais temporárias de curta duração em vez de credenciais estáticas de longa duração. Para cenários em que você precisa de usuários do com acesso programático e credenciais de longo prazo, use as informações de última utilização da chave de acesso para fazer a rotação e remover chaves de acesso.

Os usuários precisam de acesso programático se quiserem interagir com a AWS de fora do AWS Management Console. A forma de conceder acesso programático depende do tipo de usuário que está acessando a AWS.

Para conceder acesso programático aos usuários, selecione uma das seguintes opções:

Qual usuário precisa de acesso programático?	Para	Por
Identificação da força de trabalho (Usuários gerenciados no Centro de Identidade do IAM)	Use credenciais temporárias para assinar solicitações programáticas para a AWS CLI, os SDKs da AWS ou as APIs da AWS.	Siga as instruções da interface que deseja utilizar. • Para a AWS CLI, consulte Configuração da AWS CLI para usar o AWS IAM Identity Center no Guia do usuário da AWS Command Line Interface. • Para os SDKs da AWS, ferramentas e APIs da AWS, consulte Autenticação do Centro de Identidade do IAM no Guia de referência de ferramentas e SDKs da AWS.
IAM	Use credenciais temporárias para assinar solicitações programáticas para a AWS CLI, os SDKs da AWS ou as APIs da AWS.	Siga as instruções em Como usar credenciais temporárias com recursos da AWS no Guia do usuário do IAM.
IAM	(Não recomendado) Use credenciais de longo prazo para assinar solicitações programáticas para a AWS CLI, os SDKs da AWS ou as APIs da AWS.	Siga as instruções da interface que deseja utilizar. • Para a AWS CLI, consulte Autenticação usando as credenciais de usuário do IAM no Guia do usuário da AWS Command Line Interface. • Para as ferramentas e SDKs da AWS, consulte

Qual usuário precisa de acesso programático?	Para	Por
		Autenticação usando as credenciais de longo prazo no Guia de referência de ferramentas e SDKs da AWS. • Para as APIs da AWS, consulte Gerenciamento de chaves de acesso de usuários do IAM no Guia do usuário do IAM.

Recursos

Documentos relacionados:

- Controle de acesso por atributo (ABAC)
- AWS IAM Identity Center
- IAM Roles Anywhere
- Políticas gerenciadas pela AWS para o IAM Identity Center
- Condições de política do AWS IAM
- Casos de uso do IAM
- Remover credenciais desnecessárias
- Trabalhar com políticas do
- Como controlar o acesso a recursos da AWS com base em Conta da AWS, UO ou organização
- Identificar, organizar e gerenciar segredos facilmente usando a pesquisa avançada no AWS Secrets Manager

Vídeos relacionados:

- Torne-se um mestre e políticas do IAM em no máximo 60 minutos
- Separação de deveres, privilégio mínimo, delegação e CI/CD

- Simplificação do gerenciamento de identidade e acesso para inovação

SEC03-BP02 Conceder acesso de privilégio mínimo

Conceda somente o acesso de que os usuários precisam para realizar ações em recursos específicos e sob condições específicas. Use grupos e atributos de identidade para definir permissões dinamicamente em escala, em vez de definir permissões para usuários individuais. Por exemplo, é possível permitir o acesso de um grupo de desenvolvedores para gerenciar apenas recursos de seu próprio projeto. Dessa forma, se um desenvolvedor sair do projeto, seu acesso será automaticamente revogado sem que seja necessário alterar as políticas de acesso adjacentes.

Resultado desejado: os usuários têm apenas as permissões mínimas necessárias para suas funções de trabalho específicas. Use Contas da AWS separadas para isolar os desenvolvedores dos ambientes de produção. Quando os desenvolvedores precisam acessar ambientes de produção para tarefas específicas, eles recebem acesso limitado e controlado somente durante a duração dessas tarefas. O acesso à produção é imediatamente revogado após a conclusão do trabalho necessário. Você realiza revisões regulares das permissões e as revoga imediatamente quando não são mais necessárias, como quando um usuário muda de função ou sai da organização. Você restringe os privilégios de administrador a um grupo pequeno e confiável para reduzir a exposição ao risco. Você concede às contas de máquinas ou de agente apenas as permissões mínimas necessárias para executar as tarefas pretendidas.

Práticas comuns que devem ser evitadas:

- Por padrão, você concede permissões de administrador aos usuários.
- Você usa a conta de usuário-raiz para atividades diárias.
- Você cria políticas excessivamente permissivas sem um escopo adequado.
- Suas revisões de permissões não são frequentes, o que leva ao aumento de permissões.
- Você depende exclusivamente do controle de acesso baseado em atributos para isolamento do ambiente ou gerenciamento de permissões.

Nível de risco exposto se esta prática recomendada não for estabelecida: Alto

Orientação para implementação

O princípio do privilégio mínimo afirma que as identidades só devem ter permissão para realizar o menor conjunto de ações necessárias para cumprir uma tarefa específica. Isso equilibra a

usabilidade, eficiência e segurança. Operar sobre esse princípio ajuda a limitar acesso não intencional e a rastrear quem tem acesso a quais recursos. Usuários e perfis do IAM não têm permissões por padrão. O usuário-raiz tem acesso total por padrão e deve ser rigorosamente controlado, monitorado e usado somente para tarefas que exijam acesso de usuário-raiz.

Políticas do IAM são usadas para conceder explicitamente permissões aos perfis do IAM ou recursos específicos. Por exemplo, políticas com base em identidade podem ser anexadas a grupos do IAM, enquanto buckets do S3 podem ser controlados por políticas baseadas em recursos.

Ao criar uma política do IAM, você pode especificar as ações de serviço, os recursos e as condições que devem ser verdadeiras para que a AWS permita ou negue o acesso. A AWS oferece suporte a uma variedade de condições para ajudar você a reduzir o acesso. Por exemplo, usando a chave de condição PrincipalOrgID, você poderá negar ações se o solicitante não fizer parte da sua organização da AWS.

Você também pode controlar as solicitações feitas pelos serviços da AWS em seu nome, como o AWS CloudFormation criando uma função do AWS Lambda usando a chave de condição CalledVia. Você pode aplicar camadas de tipos diferentes de políticas para estabelecer a defesa em profundidade e limitar as permissões gerais dos usuários. É possível restringir as permissões que podem ser concedidas e sob quais condições. Por exemplo, você pode permitir que as equipes de workloads criem as próprias políticas do IAM para os sistemas que elas desenvolvem, mas somente se aplicarem um limite de permissão para limitar o máximo de permissões que o sistema pode receber.

Etapas de implementação

- Implementar políticas de privilégio mínimo: atribua políticas de acesso com privilégio mínimo a grupos e perfis do IAM para refletir a função do usuário ou a função que você definiu.
- Isolar ambientes de desenvolvimento e produção por meio de Contas da AWS separadas: use Contas da AWS separadas para ambientes de desenvolvimento e produção e controle o acesso entre eles usando políticas de controle de serviços, políticas de recursos e políticas de identidade.
- Baseie as políticas no uso da API: uma forma de determinar as permissões necessárias é revisar os logs da AWS CloudTrail. Você pode usar essa revisão para criar permissões personalizadas para as ações que o usuário realiza na AWS. O IAM Access Analyzer pode gerar automaticamente uma política do IAM com base na atividade de acesso. É possível usar o IAM Access Advisor em nível de organização ou conta para rastrear as últimas informações acessadas para uma política específica.

- Considere usar políticas gerenciadas pela AWS para cargos comuns: ao começar a criar políticas de permissões refinadas, pode ser útil usar políticas gerenciadas pela AWS para cargos comuns, como faturamento, administradores de banco de dados e cientistas de dados. Essas políticas podem ajudar a diminuir o acesso dos usuários enquanto você determina como implementar as políticas de privilégio mínimo.
- Remova permissões desnecessárias: detecte e remova entidades, credenciais e permissões do IAM não utilizadas para alcançar o princípio do privilégio mínimo. Você pode usar o IAM Access Analyzer para identificar o acesso externo e não utilizado, e a geração de políticas do IAM Access Analyzer pode ajudar a ajustar as políticas de permissões.
- Garanta que os usuários tenham acesso limitado aos ambientes de produção: os usuários só devem ter acesso aos ambientes de produção com um caso de uso válido. Depois de o usuário realizar as tarefas específicas para as quais o acesso à produção foi necessário, o acesso deve ser revogado. Limitar o acesso a ambientes de produção ajuda a prevenir eventos não intencionais e que causam impacto à produção, além de diminuir o escopo do impacto do acesso não intencional.
- Considere usar limites de permissões: um limite de permissões é um recurso avançado para usar uma política gerenciada que define o número máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM. O limite de permissões de uma entidade permite que a entidade execute somente as ações permitidas por ambas as políticas baseadas em identidade e seus limites de permissões.
- Refine o acesso usando controle de acesso por atributo e etiquetas de recursos: é possível usar o controle de acesso por atributo (ABAC) com etiquetas de recursos para refinar as permissões quando há suporte. Você pode usar um modelo ABAC que compara as tags da entidade principal às tags de recursos para refinar o acesso com base nas dimensões personalizadas que você define. Essa abordagem pode simplificar e reduzir o número de políticas de permissão em sua organização.
  - É recomendável que o ABAC seja usado apenas para controle de acesso quando as entidades principais e os recursos forem de propriedade da sua organização da AWS. Partes externas podem usar os mesmos nomes e valores de tag de sua organização para suas próprias entidades principais e recursos. Se você depende exclusivamente desses pares de nome/valor para conceder acesso a entidades principais ou recursos externos, você pode fornecer permissões não intencionais.
- Use políticas de controle de serviço para o AWS Organizations: as políticas de controle de serviço controlam centralmente o máximo de permissões disponíveis para contas-membro na organização. É importante notar que você pode usar as políticas de controle de serviço para restringir as

permissões do usuário-raiz nas contas-membro. Considere também usar o AWS Control Tower, que fornece controles gerenciados prescritivos que enriquecem o AWS Organizations. Também é possível definir os seus próprios controles no Control Tower.

- Estabeleça uma política de ciclo de vida do usuário para sua organização: as políticas de ciclo de vida do usuário definem tarefas a serem executadas quando os usuários são integrados à AWS, mudam de função ou escopo de trabalho ou não precisam mais de acesso à AWS. Realize revisões das permissões durante todas as etapas do ciclo de vida do usuário para verificar se as permissões estão adequadamente restritivas e para evitar desvios nas permissões.
- Estabeleça um cronograma regular para revisar as permissões e remover todas as permissões desnecessárias: revise regularmente o acesso dos usuários para verificar se os usuários não têm acesso excessivamente permissivo. O AWS Config e o IAM Access Analyzer podem ajudar durante as auditorias de permissões dos usuários.
- Estabeleça uma matriz de funções de trabalho: uma matriz de funções de trabalho visualiza as várias funções e níveis de acesso necessários em sua presença da AWS. Com uma matriz de cargos, você pode definir e separar as permissões com base nas responsabilidades do usuário dentro da sua organização. Use grupos em vez de aplicar permissões diretamente a usuários ou funções individuais.

Recursos

Documentos relacionados:

- Conceder privilégio mínimo
- Limites de permissões para entidades do IAM
- Técnicas para criar políticas do IAM de privilégio mínimo
- O IAM Access Analyzer facilita a implementação de permissões de privilégio mínimo ao gerar políticas do IAM com base na atividade de acesso
- Delegar o gerenciamento de permissões aos desenvolvedores usando os limites de permissões do IAM
- Refinar permissões usando as informações de último acesso
- Tipos de política do IAM e quando usá-las
- Testar as políticas do IAM com o simulador de políticas do IAM
- Barreiras de proteção no AWS Control Tower
- Arquiteturas de confiança zero: uma perspectiva da AWS

- Como implementar o princípio de privilégio mínimo com o CloudFormation StackSets
- Controle de acesso por atributo (ABAC)
- Reduzir o escopo da política pela visualização das atividades do usuário
- Visualizar acesso do perfil
- Usar a marcação com tags para organizar seu ambiente e impulsionar a responsabilidade
- Estratégias de marcação com tags da AWS
- Marcando recursos do AWS

Vídeos relacionados:

- Gerenciamento de permissões de última geração
- Confiança zero: uma perspectiva da AWS

SEC03-BP03 Estabelecer processo de acesso de emergência

Crie um processo que permita acesso emergencial às suas workloads no caso improvável de um problema com seu provedor de identidades centralizado.

Crie processos para diferentes modos de falha que poderiam resultar em um evento de emergência. Por exemplo, em circunstâncias normais, os usuários da sua força de trabalho são federados na nuvem usando um provedor de identidades centralizado (SEC02-BP04) para gerenciar suas workloads. No entanto, se o provedor de identidades centralizado falhar ou a configuração da federação na nuvem for modificada, talvez os usuários de sua força de trabalho não consigam se federar na nuvem. Um processo de acesso de emergência permite que administradores autorizados acessem seus recursos de nuvem por meios alternativos (como uma forma alternativa de federação ou acesso direto do usuário) para corrigir problemas com sua configuração de federação ou workloads. O processo de acesso de emergência é usado até o mecanismo normal de federação ser restaurado.

Resultado desejado:

- Você definiu e documentou os modos de falha que são considerados uma emergência: considere suas circunstâncias normais e os sistemas dos quais seus usuários dependem para gerenciar suas workloads. Pense em como cada uma dessas dependências pode falhar e causar uma situação de emergência. Talvez você considere as perguntas e as práticas recomendadas do pilar

Confiabilidade úteis para identificar modos de falha e arquitetar sistemas mais resilientes para minimizar a probabilidade de falhas.

- Você documentou as etapas que devem ser seguidas para confirmar uma falha como emergência. Por exemplo, é possível exigir que os administradores de identidade confiram o status de seus provedores de identidade primário e de reserva e, se nenhum dos dois estiver disponível, declarar um evento de emergência por falha do provedor de identidades.
- Você definiu um processo de acesso de emergência específico de cada tipo de modo de emergência ou falha. Ser específico pode reduzir a tentação de seus usuários de abusar de um processo geral para todos os tipos de emergência. Seus processos de acesso de emergência descrevem as circunstâncias em que cada processo deve ser usado e, inversamente, as situações em que o processo não deve ser usado e apontam para processos alternativos que podem ser aplicados.
- Seus processos são bem documentados com instruções detalhadas e playbooks que podem ser seguidos com rapidez e eficiência. Lembre-se de que um evento de emergência pode ser um momento estressante para os usuários e eles podem estar sob extrema pressão de tempo. Portanto, desenvolva o processo para ser o mais simples possível.

Práticas comuns que devem ser evitadas:

- Você não tem processos de acesso de emergência bem documentados e bem testados. Os usuários não estão preparados para uma emergência e seguem processos improvisados quando um evento de emergência ocorre.
- Seus processos de acesso de emergência dependem dos mesmos sistemas (como um provedor de identidades centralizado) que seus mecanismos de acesso normais. Isso significa que uma falha desse sistema pode afetar os mecanismos de acesso normal e de emergência e prejudicar sua capacidade de se recuperar da falha.
- Seus processos de acesso de emergência são usados em situações não emergenciais. Por exemplo, os usuários muitas vezes utilizam de forma indevida os processos de acesso de emergência, pois acham mais fácil fazer alterações diretamente do que enviá-las por meio de um pipeline.
- Seus processos de acesso de emergência não geram logs suficientes para auditar os processos, ou os logs não são monitorados para alertar sobre o possível uso indevido dos processos.

Benefícios de implementar esta prática recomendada:

- Com processos de acesso de emergência bem documentados e testados, é possível reduzir o tempo gasto pelos usuários para responder e resolver um evento de emergência. Isso pode resultar em menos tempo de inatividade e maior disponibilidade dos serviços fornecidos aos seus clientes.
- É possível rastrear cada solicitação de acesso de emergência e detectar e alertar sobre tentativas não autorizadas de uso indevido do processo para eventos não emergenciais.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

Esta seção fornece orientação para criar processos de acesso de emergência para vários modos de falha relacionados às workloads implantadas na AWS, começando com uma orientação comum que se aplica a todos os modos de falha e seguida por uma orientação específica com base no tipo de modo de falha.

Orientação comum para todos os modos de falha

Pense no seguinte ao projetar um processo de acesso de emergência para um modo de falha:

- Documente as pré-condições e as suposições do processo: quando o processo deve ou não ser usado. Isso ajuda a detalhar o modo de falha e documentar suposições, como o estado de outros sistemas relacionados. Por exemplo, o processo do Modo de falha 2 pressupõe que o provedor de identidades está disponível, mas a configuração na AWS foi modificada ou expirou.
- Pré-crie os recursos necessários para o processo de acesso de emergência (SEC10-BP05). Por exemplo, crie previamente a Conta da AWS de acesso de emergência com usuários e perfis do IAM e os perfis do IAM entre contas em todas as contas da workload. Isso verifica se esses recursos estão prontos e disponíveis quando um evento de emergência ocorre. Ao pré-criar recursos, você não depende das APIs do ambiente de gerenciamento da AWS (usadas para criar e modificar recursos da AWS) que podem estar indisponíveis em caso de emergência. Além disso, ao pré-criar recursos do IAM, não é necessário considerar possíveis atrasos devido a consistência eventual.
- Inclua processos de acesso de emergência como parte dos planos de gerenciamento de incidentes (SEC1-BP02). Documente como os eventos de emergência são acompanhados e comunicados a outras pessoas na organização, como equipes de colegas, sua liderança e, quando aplicável, externamente a seus clientes e parceiros de negócios.

- Defina o processo de solicitação de acesso de emergência no sistema de fluxo de trabalho de solicitação de serviço existente, caso haja um. Normalmente, esses sistemas de fluxo de trabalho permitem criar formulários de admissão para coletar informações sobre a solicitação, rastrear a solicitação em cada estágio do fluxo de trabalho e adicionar etapas de aprovação automatizadas e manuais. Relacione cada solicitação a um evento de emergência correspondente acompanhado no sistema de gerenciamento de incidentes. Ter um sistema uniforme para acessos de emergência permite que você acompanhe essas solicitações em um único sistema, analise as tendências de uso e melhore os processos.
- Verifique se os processos de acesso de emergência só podem ser iniciados por usuários autorizados e exigem aprovações dos colegas ou da gerência do usuário, conforme apropriado. O processo de aprovação deve operar de forma eficaz dentro e fora do horário comercial. Defina como as solicitações de aprovação permitirão aprovadores secundários se os aprovadores primários não estiverem disponíveis e forem encaminhadas para a cadeia de gerenciamento até serem aprovadas.
- Implemente mecanismos robustos de registro em log, monitoramento e alerta para o processo e os mecanismos de acesso de emergência. Gere logs de auditoria detalhados para todas as tentativas bem-sucedidas e fracassadas de obter acesso de emergência. Correlacione a atividade com eventos de emergência contínuos do sistema de gerenciamento de incidentes e inicie alertas quando as ações ocorrerem fora dos períodos esperados ou quando a conta de acesso de emergência for usada durante as operações normais. A conta de acesso de emergência só deve ser acessada durante emergências, pois os procedimentos de quebra de vidro podem ser considerados uma backdoor. Integre-se à sua ferramenta de gerenciamento de eventos e informações de segurança (SIEM) ou AWS Security Hubpara relatar e auditar todas as atividades durante o período de acesso de emergência. Ao retornar às operações normais, alterne automaticamente as credenciais de acesso de emergência e notifique as equipes relevantes.
- Teste os processos de acesso de emergência periodicamente para verificar se as etapas estão claras e garantir o nível correto de acesso com rapidez e eficiência. Seus processos de acesso de emergência devem ser testados como parte das simulações de resposta a incidentes (SEC10-BP07) e dos testes de recuperação de desastres (REL13-BP03).

Modo de falha 1: o provedor de identidades usado para federação na AWS não está disponível

Conforme descrito em SEC02-BP-04 Confiar em um provedor de identidade federado, recomendamos confiar em um provedor de identidades centralizado para federar os usuários de sua força de trabalho e conceder acesso a Contas da AWS. Você pode federar em várias Contas da AWS na organização da AWS usando o Centro de Identidade do IAM ou federar em Contas da AWS

individuais usando o IAM. Nos dois casos, os usuários da força de trabalho se autenticam com seu provedor de identidades centralizado antes de serem redirecionados a um endpoint de login da AWS para SSO.

No caso improvável do provedor de identidades centralizado não estar disponível, os usuários da sua força de trabalho não poderão se federar nas Contas da AWS nem gerenciar as workloads. Nesse evento de emergência, é possível fornecer um processo de acesso de emergência para um pequeno grupo de administradores acessar as Contas da AWS a fim de realizar tarefas essenciais que não podem esperar até que seus provedores de identidades centralizados estejam online novamente. Por exemplo, seu provedor de identidades fica indisponível por quatro horas e, durante esse período, você precisa modificar os limites superiores de um grupo do Amazon EC2 Auto Scaling em uma conta de produção para lidar com um aumento inesperado no tráfego de clientes. Seus administradores de emergência devem seguir o processo de acesso de emergência a fim de obter acesso à Conta da AWS de produção específica e fazer as alterações necessárias.

O processo de acesso de emergência depende de uma Conta da AWS de acesso de emergência pré-criada usada exclusivamente para acesso de emergência e tem recursos da AWS (como perfis e usuários do IAM) para apoiar o processo de acesso de emergência. Durante as operações normais, ninguém deve acessar a conta de acesso de emergência, e você deve monitorar e alertar sobre o uso indevido dessa conta (para receber mais detalhes, consulte a seção Orientação comum anterior).

A conta de acesso de emergência tem perfis do IAM de acesso de emergência com permissões para assumir perfis entre contas nas Contas da AWS que exigem acesso de emergência. Esses perfis do IAM são pré-criados e configurados com políticas de confiança que confiam nos perfis do IAM da conta de emergência.

O processo de acesso de emergência pode usar uma das seguintes abordagens:

- É possível pré-criar um conjunto de usuários do IAM para seus administradores de emergência na conta de acesso de emergência com senhas fortes e tokens de MFA associados. Esses usuários do IAM têm permissões para assumir os perfis do IAM que permitem o acesso entre contas à Conta da AWS onde o acesso de emergência é necessário. Recomendamos criar o menor número possível de usuários e atribuir cada um a um único administrador de emergência. Durante uma emergência, um usuário administrador de emergência entra na conta de acesso de emergência usando sua senha e código de token MFA, muda para o perfil do IAM de acesso de emergência na conta de emergência e, por fim, para o perfil do IAM de acesso de emergência na conta da workload para realizar a ação de alteração de emergência. A vantagem dessa abordagem é que cada usuário do IAM é atribuído a um administrador de emergência, e é possível saber qual

usuário fez login analisando os eventos do CloudTrail. A desvantagem é que você precisa manter vários usuários do IAM com as respectivas senhas de longa duração e tokens de MFA associados.

- É possível usar o usuário-raiz da Conta da AWS de emergência para entrar na conta de acesso de emergência, assumir o perfil do IAM para acesso de emergência e assumir o perfil entre contas na conta da workload. Recomendamos definir uma senha forte e vários tokens de MFA para o usuário-raiz. Também recomendamos armazenar a senha e os tokens de MFA em um cofre de credenciais corporativo seguro que imponha autenticação e autorização fortes. Você deve proteger a senha e os fatores de redefinição de tokens de MFA: defina o endereço de e-mail da conta como uma lista de distribuição de e-mail monitorada pelos administradores de segurança na nuvem e o número de telefone da conta como um número de telefone compartilhado que também seja monitorado pelos administradores de segurança. A vantagem dessa abordagem é que há um conjunto de credenciais de usuário-raiz para gerenciar. A desvantagem é que, como se trata de um usuário compartilhado, vários administradores podem fazer login como usuário-raiz. Você deve fazer auditoria dos eventos de log do cofre corporativo para identificar qual administrador fez check-out da senha do usuário-raiz.

Modo de falha 2: a configuração do provedor de identidades na AWS foi modificada ou expirou

Para permitir que os usuários de sua força de trabalho sejam federados nas Contas da AWS, é possível configurar o Centro de Identidade do IAM com um provedor de identidades externo ou criar um provedor de identidades do IAM (SEC02-BP04). Normalmente, você os configura importando um documento XML de metadados SAML fornecido pelo provedor de identidades. O documento XML de metadados inclui um certificado X.509 correspondente a uma chave privada que o provedor de identidades usa para assinar as declarações SAML.

Essas configurações no lado da AWS podem ser modificadas ou excluídas por engano por um administrador. Em outro cenário, o certificado X.509 importado para a AWS pode expirar, e um novo XML de metadados com um novo certificado ainda não foi importado para a AWS. Os dois cenários podem interromper a federação na AWS para os usuários de sua força de trabalho, ocasionando uma emergência.

Nesse evento de emergência, você pode fornecer aos seus administradores de identidade acesso à AWS para resolver os problemas de federação. Por exemplo, seu administrador de identidade usa o processo de acesso de emergência para fazer login na Conta da AWS de acesso de emergência, muda para um perfil na conta de administrador do Centro de Identidade e atualiza a configuração do provedor de identidades externo importando o documento XML de metadados SAML mais recente do provedor de identidades para reativar a federação. Após a federação ser corrigida, os usuários

da sua força de trabalho continuarão usando o processo operacional normal para federar em suas contas da workload.

Você pode seguir as abordagens detalhadas no Modo de falha 1 anterior para criar um processo de acesso de emergência. É possível conceder permissões de privilégio mínimo aos seus administradores de identidade a fim de acessar somente a conta de administrador do Centro de Identidade e realizar ações no Centro de Identidade nessa conta.

Modo de falha 3: interrupção do Centro de Identidade

No caso improvável de uma interrupção do Centro de Identidade do IAM ou da Região da AWS, recomendamos definir uma configuração que possa ser usada para conceder acesso temporário ao AWS Management Console.

O processo de acesso de emergência usa a federação direta do provedor de identidades no IAM em uma conta de emergência. Para obter detalhes sobre o processo e as considerações de design, consulte Configurar o acesso de emergência ao AWS Management Console.

Etapas de implementação

Etapas comuns para todos os modos de falha

- Crie uma Conta da AWS dedicada aos processos de acesso de emergência. Crie previamente os recursos do IAM necessários na conta, como perfis ou usuários do IAM e, opcionalmente, provedores de identidades do IAM. Além disso, crie previamente perfis do IAM entre contas nas Contas da AWS da workload com relacionamentos de confiança com os perfis do IAM correspondentes na conta de acesso de emergência. É possível usar o AWS CloudFormation StackSets com AWS Organizations para criar esses recursos nas contas-membro da sua organização.

- Crie políticas de controle de serviços (SCP) do AWS Organizations para negar a exclusão e a modificação dos perfis do IAM entre contas nas Contas da AWS-membro.
- Ative o CloudTrail para a Conta da AWS de acesso de emergência e envie os eventos da trilha a um bucket central do S3 em sua Conta da AWS de coleção de logs. Se você estiver usando o AWS Control Tower para configurar e controlar seu ambiente de várias contas da AWS, todas as contas que você criar usando o AWS Control Tower ou inscrever no AWS Control Tower terão o CloudTrail ativado por padrão e serão enviadas a um bucket do S3 em uma Conta da AWS de arquivo de log dedicado.

- Monitore a atividade da conta de acesso de emergência criando regras do EventBridge que correspondam ao login do console e à atividade da API pelos perfis do IAM de emergência. Envie notificações ao seu centro de operações de segurança quando ocorrerem atividades fora de um evento de emergência contínuo acompanhado no sistema de gerenciamento de incidentes.

Etapas adicionais para o Modo de falha 1: o provedor de identidades usado para federar na AWS não está disponível; Modo de falha 2: a configuração do provedor de identidades na AWS foi modificada ou expirou

- Crie previamente recursos de acordo com o mecanismo escolhido para acesso de emergência:
  - Utilizar usuários do IAM: crie previamente os usuários do IAM com senhas fortes e dispositivos MFA associados.
  - Utilizar o usuário-raiz da conta de emergência: configure o usuário-raiz com uma senha forte e armazene a senha no seu cofre de credenciais corporativo. Associe vários dispositivos físicos de MFA ao usuário-raiz e armazene os dispositivos em locais que possam ser acessados rapidamente pelos membros de sua equipe de administradores de emergência.

Etapas adicionais para o Modo de falha 3: interrupção do Centro de Identidade

- Conforme detalhado em Configurar o acesso de emergência ao AWS Management Console, na Conta da AWS de acesso de emergência, crie um provedor de identidades do IAM para ativar a federação direta de SAML a partir do provedor de identidades.
- Crie grupos de operações de emergência no IdP sem membros.
- Crie perfis do IAM correspondentes aos grupos de operações de emergência na conta de acesso de emergência.

Recursos

Práticas recomendadas do Well-Architected relacionadas:

- SEC02-BP04 Confiar em um provedor de identidades centralizado
- SEC03-BP02 Conceder acesso de privilégio mínimo
- SEC10-BP02 Desenvolver planos de gerenciamento de incidentes
- SEC10-BP07 Promover game days

Documentos relacionados:

- Configurar o acesso de emergência ao AWS Management Console
- Habilitar o acesso de usuários federados SAML 2.0 ao AWS Management Console
- Acesso de emergência

Vídeos relacionados:

- AWS re:Invent 2022: Simplificar o acesso da sua força de trabalho com o Centro de Identidade do IAM
- AWS re:Inforce 2022: Mergulho profundo no AWS Identity and Access Management (IAM)

Exemplos relacionados:

- Perfil de acesso de emergência da AWS
- Framework do playbook do cliente da AWS
- Exemplos de playbook de resposta a incidentes da AWS

SEC03-BP04 Reduzir as permissões continuamente

À medida que suas equipes determinarem o acesso de que precisam, remova as permissões desnecessárias e estabeleça processos de análise para obter permissões de privilégio mínimo. Monitore e remova continuamente identidades e permissões não utilizadas para acesso humano e de máquina.

Resultado desejado: as políticas de permissão devem seguir o princípio de privilégio mínimo. À medida que os cargos e os perfis se tornem mais bem definidos, suas políticas de permissões precisam ser analisadas para remover permissões desnecessárias. Essa abordagem reduz o escopo do impacto caso as credenciais sejam expostas de forma acidental ou sejam acessadas sem autorização.

Práticas comuns que devem ser evitadas:

- Usar como padrão a concessão de permissões de administrador aos usuários.
- Criar políticas permissivas demais, mas sem privilégios completos de administrador.
- Manter as políticas de permissão quando não são mais necessárias.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

Enquanto as equipes e os projetos estiverem apenas começando, políticas de permissão permissivas podem ser usadas para inspirar inovação e agilidade. Por exemplo, em um ambiente de desenvolvimento ou teste, os desenvolvedores podem receber acesso a uma ampla gama de serviços da AWS. Recomendamos avaliar o acesso de forma contínua e restringir o acesso somente àqueles serviços e ações de serviço necessários para concluir o trabalho atual. Recomendamos essa avaliação para identidades humanas e de máquina. Identidades de máquina, às vezes, denominadas contas de sistema ou serviço, são identidades que fornecem acesso da AWS a aplicações ou servidores. Esse acesso é especialmente importante em um ambiente de produção, em que as permissões excessivamente permissivas podem causar um grande impacto e expor dados dos clientes.

A AWS oferece vários métodos para ajudar a identificar usuários, perfis, permissões e credenciais não utilizados. A AWS também pode ajudar a analisar a atividade de acesso dos usuários e dos perfis do IAM, como chaves de acesso associadas, e o acesso aos recursos da AWS, como objetos em buckets do Amazon S3. A geração de políticas do AWS Identity and Access Management Access Analyzer pode auxiliar você a criar políticas de permissão restritivas com base nos serviços e nas ações reais com os quais uma entidade principal interage. O controle de acesso por atributo (ABAC) pode ajudar a simplificar o gerenciamento de permissões, pois você pode fornecer permissões aos usuários usando seus atributos em vez de anexar políticas de permissões diretamente a cada usuário.

Etapas de implementação

- Use o AWS Identity and Access Management Access Analyzer: o IAM Access Analyzer ajuda a identificar os recursos em sua organização e suas contas, como buckets do Amazon Simple Storage Service (Amazon S3) ou perfis do IAM que são compartilhados com uma entidade externa.
- Use a geração de políticas do IAM Access Analyzer: a geração de políticas do IAM Access Analyzer ajuda você a criar políticas de permissão refinadas com base na atividade de acesso de um usuário ou perfil do IAM.
- Teste as permissões em ambientes inferiores antes da produção: comece usando os ambientes menos críticos de sandbox e desenvolvimento para testar as permissões necessárias para várias funções de trabalho usando o IAM Access Analyzer. Em seguida, restrinja e valide progressivamente essas permissões nos ambientes de teste, garantia de qualidade e preparação

antes de aplicá-las à produção. Inicialmente, os ambientes inferiores podem ter permissões mais relaxadas, pois as políticas de controle de serviços (SCPs) impõem barreiras de proteção ao limitar o máximo de permissões concedidas.

- Determine um prazo e uma política de uso aceitáveis para usuários e funções do IAM: use o carimbo de data/hora do último acesso para identificar usuários e perfis não utilizados e removê-los. Revise as informações de serviço e ação acessadas mais recentemente para identificar e definir o escopo das permissões para usuários e perfis específicos. Por exemplo, você pode usar as informações acessadas mais recentemente para identificar as ações específicas do Amazon S3 exigidas pelo perfil da aplicação e restringir o acesso do perfil apenas a essas ações. Recursos de informações acessadas mais recentemente estão disponíveis no AWS Management Console e de maneira programática para permitir que você As incorpore aos fluxos de trabalho de infraestrutura e ferramentas automatizadas.
- Considere registrar em log eventos de dados no AWS CloudTrail: por padrão, o CloudTrail não registra eventos de dados em log, como atividades em nível de objeto do Amazon S3 (por exemplo, `GetObject` e `DeleteObject`) ou atividades de tabela do Amazon DynamoDB (por exemplo, `PutItem` e `DeleteItem`). Considere ativar o registro em log desses eventos para determinar quais usuários e perfis precisam acessar objetos do Amazon S3 ou itens de tabelas do DynamoDB específicos.

Recursos

Documentos relacionados:

- Conceder privilégio mínimo
- Remover credenciais desnecessárias
- O que é o AWS CloudTrail?
- Trabalhar com políticas do
- Registrar em log e monitorar no DynamoDB
- Usar o registro em log de eventos do CloudTrail para buckets e objetos do Amazon S3
- Obter relatórios de credenciais da sua Conta da AWS

Vídeos relacionados:

- Torne-se um mestre e políticas do IAM em no máximo 60 minutos
- Separação de deveres, privilégio mínimo, delegação e CI/CD

- AWS re:Inforce 2022: Mergulho profundo no AWS Identity and Access Management (IAM)

SEC03-BP05 Definir barreiras de proteção de permissões para sua organização

Use barreiras de proteção de permissões para reduzir o escopo das permissões disponíveis que podem ser concedidas a entidades principais. A cadeia de avaliação da política de permissões inclui suas grades de proteção para determinar as permissões efetivas de uma entidade principal ao tomar decisões de autorização. Você pode definir barreiras de proteção usando uma abordagem baseada em camadas. Aplique algumas barreiras de proteção de maneira abrangente em toda a organização e outras de forma detalhada às sessões de acesso temporário.

Resultado desejado: você obtém um isolamento claro dos ambientes usando Contas da AWS sparapdpas. As políticas de controle de serviços (SCPs) são usadas para definir barreiras de proteção de permissões em toda a organização. As barreiras de proteção mais amplas são definidas nos níveis hierárquicos mais próximos da raiz da sua organização e as barreiras de proteção mais rígidas são definidas mais perto do nível das contas individuais.

Quando aceitas, as políticas de recursos definem as condições que uma entidade principal deve satisfazer para obter acesso a um recurso. As políticas de recursos também abrangem o conjunto de ações permitidas, quando apropriado. Os limites de permissão são impostos às entidades principais que gerenciam as permissões da workload, delegando o gerenciamento de permissões aos proprietários de workload individuais.

Práticas comuns que devem ser evitadas:

- Criar Contas da AWS-membro dentro de uma organização da AWS, mas não usar SCPs para restringir o uso e as permissões disponíveis para suas credenciais de raiz.
- Atribuir permissões com base em privilégio mínimo, mas não colocar barreiras de proteção no conjunto máximo de permissões que podem ser concedidas.
- Confiar na base de negação implícita do AWS IAM para restringir as permissões, confiando que as políticas não concederão uma permissão explícita indesejada.
- Executar vários ambientes de workload na mesma Conta da AWS e confiar em mecanismos como VPCs, tags ou políticas de recursos para impor limites de permissão.

Benefícios de implementar esta prática recomendada: as barreiras de proteção de permissões ajudam a criar confiança de que permissões indesejadas não podem ser concedidas, mesmo quando

uma política de permissão tenta fazer isso. Isso pode simplificar a definição e o gerenciamento de permissões, reduzindo o escopo máximo das permissões que precisam ser consideradas.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

Recomendamos usar uma abordagem baseada em camadas para definir barreiras de proteção de permissões para sua organização. Essa abordagem reduz sistematicamente o conjunto máximo de permissões possíveis à medida que camadas adicionais são aplicadas. Isso ajuda você a conceder acesso com base no princípio de privilégio mínimo, reduzindo o risco de acesso indesejado devido à configuração incorreta de alguma política.

A primeira etapa para estabelecer barreiras de proteção de permissões é isolar workloads e ambientes em Contas da AWS separadas. As entidades principais de uma conta não podem acessar recursos em outra conta sem permissão explícita para fazer isso, mesmo quando as duas contas estão na mesma organização da AWS ou na mesma unidade organizacional (UO). Você pode usar UOs para agrupar contas que deseja administrar como uma única unidade.

A próxima etapa é reduzir o conjunto máximo de permissões que você pode conceder às entidades principais nas contas-membro da sua organização. Você pode usar políticas de controle de serviço (SCPs) para essa finalidade, as quais podem ser aplicadas a uma UO ou a uma conta. As SCPs podem impor controles de acesso comuns, como restringir o acesso a determinadas Regiões da AWS, ajudar a impedir a exclusão de recursos ou desabilitar ações de serviço possivelmente arriscadas. As SCPs que você aplica à raiz da sua organização afetam apenas as contas-membro, mas não a conta de gerenciamento. As SCPs regem apenas as entidades principais da sua organização. As SCPs não regem entidades principais externas à sua organização que estão acessando seus recursos.

Se você estiver usando o AWS Control Tower, poderá aproveitar os controles e as zonas de pouso como base para as barreiras de proteção de permissões e ambiente de várias contas. As zonas de pouso fornecem um ambiente básico seguro e pré-configurado com contas separadas para diferentes workloads e aplicações. As barreiras de proteção impõem controles obrigatórios sobre segurança, operações e conformidade por meio de uma combinação de políticas de controle de serviços (SCPs), regras do AWS Config e outras configurações. No entanto, ao usar barreiras de proteção e zonas de pouso do Control Tower com as SCPs personalizadas da organização, é crucial seguir as práticas recomendadas descritas na documentação da AWS para evitar conflitos e garantir a governança adequada. Consulte a orientação do AWS Control Tower para o AWS Organizations

a fim de obter recomendações detalhadas sobre o gerenciamento de SCPs, contas e unidades organizacionais (OUs) em um ambiente do Control Tower.

Ao aderir a essas diretrizes, você pode aproveitar com eficácia as barreiras de proteção e zonas de pouso do Control Tower e as SCPs personalizadas, ao mesmo tempo em que mitiga possíveis conflitos e garante a governança e o controle adequados sobre seu ambiente de várias contas da AWS.

Outra etapa é usar políticas de recursos do IAM para definir o escopo das ações disponíveis que você pode realizar nos recursos por elas governados, juntamente com quaisquer condições que o diretor interino deva atender. Isso pode ser tão amplo quanto permitir todas as ações, desde que a entidade principal faça parte da sua organização (usando a chave de condição PrincipalOrgID), ou tão granular quanto permitir apenas ações específicas de um perfil do IAM específico. É possível adotar uma abordagem semelhante com as condições das políticas de confiança de perfis do IAM. Se uma política de confiança de recursos ou perfis nomear explicitamente uma entidade principal na mesma conta que o perfil ou o recurso por ela governado, essa entidade principal não precisará de uma política do IAM anexada que conceda as mesmas permissões. Se a entidade principal estiver em uma conta diferente da conta do recurso, ela precisará de uma política do IAM anexada que conceda essas permissões.

Muitas vezes, uma equipe de workload quer gerenciar as permissões exigidas pela workload em questão. Isso, por sua vez, pode exigir que a equipe crie políticas de permissão e perfis do IAM. É possível capturar o escopo máximo de permissões que a equipe pode conceder em um limite de permissão do IAM e associar esse documento a um perfil do IAM que a equipe pode usar para gerenciar seus perfis do IAM e permissões. Essa abordagem pode proporcionar à equipe a flexibilidade para concluir o trabalho e, ao mesmo tempo, reduzir os riscos de acesso administrativo ao IAM.

Uma etapa mais granular é implementar técnicas de gerenciamento de acesso privilegiado (PAM) e gerenciamento de acesso elevado temporário (TEAM). Um exemplo de PAM é exigir que as entidades principais realizem a autenticação multifator antes de executar ações privilegiadas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA. O TEAM exige uma solução que gerencie a aprovação e o período durante o qual uma entidade principal pode ter acesso elevado. Uma abordagem é adicionar temporariamente a entidade principal à política de confiança de perfis referente a um perfil do IAM que tenha acesso elevado. Outra abordagem é, em operação normal, reduzir o escopo das permissões concedidas a uma entidade principal por um perfil do IAM usando uma política de sessão e, em seguida, suspender temporariamente essa

restrição durante o período aprovado. Para saber mais sobre as soluções validadas pela AWS e por parceiros selecionados, consulte Acesso elevado temporário.

Etapas de implementação

1. Isole workloads e ambientes em Contas da AWS separadas.
2. Use SCPs para reduzir o conjunto máximo de permissões que podem ser concedidas às entidades principais nas contas dos membros da sua organização.
   a. Ao definir SCPs para reduzir o conjunto máximo de permissões que podem ser concedidas às entidades principais nas contas dos membros da sua organização, você pode escolher entre uma abordagem de lista de permissões ou listas de negação. A estratégia da lista de permissões especifica explicitamente o acesso permitido e bloqueia implicitamente todos os outros acessos. A estratégia da lista de negação especifica explicitamente o acesso não permitido e permite todos os outros acessos por padrão. Ambas as estratégias têm suas vantagens e desvantagens, e a escolha apropriada depende dos requisitos específicos e do modelo de risco de sua organização. Para obter mais detalhes, consulte Estratégia para usar SCPs.
   b. Além disso, analise os exemplos de políticas de controle de serviços para entender como construir SCPs de forma eficaz.
3. Use políticas de recursos do IAM para reduzir o escopo e especificar as condições das ações permitidas nos recursos. Use condições nas políticas de confiança de perfis do IAM para criar restrições aos perfis assumidos.
4. Atribua limites de permissão do IAM a perfis do IAM que as equipes de workload podem usar para gerenciar perfis e permissões do IAM de suas próprias workloads.
5. Avalie as soluções de PAM e TEAM com base em suas necessidades.

Recursos

Documentos relacionados:

- Perímetro de dados na AWS
- Estabelecer barreiras de proteção para permissões usando perímetros de dados
- Lógica da avaliação de política

Exemplos relacionados:

- Exemplos de políticas de controle de serviço

Ferramentas relacionadas:

- Solução da AWS: gerenciamento de acesso elevado temporário
- Soluções validadas de parceiros de segurança para TEAM

SEC03-BP06 Gerenciar o acesso com base no ciclo de vida

Monitore e ajuste as permissões concedidas às entidades principais (usuários, funções e grupos) durante todo o ciclo de vida em sua organização. Ajuste as associações de grupo à medida que os usuários mudarem de função e remova o acesso quando um usuário sair da organização.

Resultado desejado: você monitora e ajusta as permissões em todo o ciclo de vida dos diretores da organização, reduzindo o risco de privilégios desnecessários. Você concede acesso apropriado ao criar um usuário. Você modifica o acesso à medida que as responsabilidades do usuário mudam e remove o acesso quando o usuário não está mais ativo ou sai da organização. Você gerencia centralmente as alterações em seus usuários, perfis e grupos. Você usa a automação para propagar alterações em seus ambientes da AWS.

Práticas comuns que devem ser evitadas:

- Conceder privilégios de acesso excessivos ou amplos às identidades com antecedência, para além daqueles exigidos inicialmente.
- Não revisar nem ajustar os privilégios de acesso à medida que as funções e responsabilidades das identidades mudam ao longo do tempo.
- Manter identidades inativas ou encerradas com privilégios de acesso ativos. Isso aumenta o risco de acesso não autorizado.
- Não aproveitar a automação para gerenciar o ciclo de vida das identidades.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

Gerencie e ajuste cuidadosamente os privilégios de acesso concedidos às identidades (como usuários, funções, grupos) durante todo o ciclo de vida. Esse ciclo de vida inclui a fase inicial de

integração, mudanças contínuas em perfis e responsabilidades e eventual desligamento ou rescisão. Gerencie proativamente o acesso com base no estágio do ciclo de vida para manter o nível de acesso adequado. Siga o princípio de privilégio mínimo para reduzir o risco de privilégios de acesso excessivos ou desnecessários.

Você pode gerenciar o ciclo de vida dos usuários do IAM diretamente na Conta da AWS ou por meio de federação no provedor de identidades de seu quadro de funcionários para o Centro de Identidade do IAM da AWS. Para usuários do IAM, é possível criar, modificar e excluir usuários e as respectivas permissões associadas na Conta da AWS. No caso de usuários federados, você pode usar o Centro de Identidade do IAM para gerenciar o respectivo ciclo de vida sincronizando as informações de usuários e grupos do provedor de identidades da sua organização por meio do protocolo System for Cross-Domain Identity Management (SCIM).

O SCIM é um protocolo de padrão aberto para provisionamento e desprovisionamento automatizados de identidades de usuários em diferentes sistemas. Ao integrar seu provedor de identidades ao Centro de Identidade do IAM usando o SCIM, você pode sincronizar automaticamente as informações do usuário e do grupo para ajudar a validar que os privilégios de acesso sejam concedidos, modificados ou revogados com base nas alterações na fonte de identidade autorizada da sua organização.

À medida que as funções e responsabilidades dos funcionários mudam em sua organização, ajuste os respectivos privilégios de acesso de maneira correspondente. Você pode usar os conjuntos de permissões do Centro de Identidade do IAM para definir diferentes funções ou responsabilidades de trabalho e associá-las a políticas e permissões apropriadas do IAM. Quando a função de um funcionário muda, você pode atualizar o conjunto de permissões atribuído para refletir as novas responsabilidades. Verifique se ele tem o acesso necessário e segue o princípio de privilégio mínimo.

Etapas de implementação

1. Defina e documente um processo de ciclo de vida do gerenciamento de acesso, incluindo procedimentos para concessão de acesso inicial, revisões periódicas e desligamento.
2. Implemente perfis, grupos e limites de permissões do IAM para gerenciar o acesso coletivamente e impor os níveis máximos de acesso permitidos.
3. Integre-se a um provedor de identidades federado (como Microsoft Active Directory, Okta, Ping Identity) como fonte confiável para uso de informações de usuários e grupos usando o Centro de Identidade do IAM.
4. Use o protocolo SCIM para sincronizar informações de usuários e grupos do provedor de identidades com o repositório de identidades do Centro de Identidade do IAM.

5. Crie conjuntos de permissões no Centro de Identidade do IAM que representem diferentes cargos ou responsabilidades em sua organização. Defina as políticas e permissões apropriadas do IAM para cada conjunto de permissões.
6. Implemente análises regulares de acesso, revogação imediata do acesso e melhoria contínua do processo do ciclo de vida do gerenciamento de acesso.
7. Ofereça treinamento e conhecimento aos funcionários sobre as práticas recomendadas de gerenciamento de acesso.

Recursos

Práticas recomendadas relacionadas:

- SEC02-BP04 Confiar em um provedor de identidades centralizado

Documentos relacionados:

- Gerenciar sua fonte de identidade
- Gerenciar identidades no Centro de Identidade do IAM
- Como usar o AWS Identity and Access Management Access Analyzer
- Geração de políticas do IAM Access Analyzer

Vídeos relacionados:

- AWS re:Inforce 2023: Gerenciar o acesso elevado temporário com o AWS IAM Identity Center
- AWS re:Invent 2022: Simplificar o acesso da sua força de trabalho com o Centro de Identidade do IAM
- AWS re:Invent 2022: Aproveitar o poder das políticas do IAM e controlar permissões com o Access Analyzer

SEC03-BP07 Analisar o acesso público e entre contas

Monitore continuamente as descobertas que destacam o acesso público e entre contas. Limite o acesso público e o acesso entre contas somente aos recursos específicos que exigem esse tipo de acesso.

Resultado desejado: saiba quais de seus recursos da AWS são compartilhados e com quem. Monitore e audite continuamente seus recursos compartilhados para verificar se eles são compartilhados apenas com entidades principais autorizadas.

Práticas comuns que devem ser evitadas:

- Não manter um inventário dos recursos compartilhados.
- Não seguir um processo de aprovação do acesso público ou entre contas aos recursos.

Nível de risco exposto se esta prática recomendada não for estabelecida: Baixo

Orientação para implementação

Se a sua conta estiver no AWS Organizations, você poderá conceder acesso aos recursos à toda a organização, a unidades organizacionais específicas ou a contas individuais. Se sua conta não for membro de uma organização, você poderá compartilhar recursos com contas individuais. Você pode conceder acesso direto entre contas usando políticas baseadas em recursos — por exemplo, políticas de bucket do Amazon Simple Storage Service (Amazon S3) — ou permitindo que um principal em outra conta assuma uma função do IAM em sua conta. Ao utilizar políticas de recursos, verifique se o acesso é concedido apenas a entidades principais autorizadas. Defina um processo para aprovar todos os recursos que devem ser acessíveis publicamente.

O AWS Identity and Access Management Access Analyzer segurança comprovada para identificar todos os caminhos de acesso a um recurso de fora de sua conta. Ele revisa as políticas de recursos continuamente e relata descobertas de acesso público e entre contas para facilitar a análise de acesso potencialmente amplo. Considere a configuração do IAM Access Analyzer com o AWS Organizations para verificar se você tem visibilidade em todas as suas contas. O IAM Access Analyzer também permite que você visualize as descobertas antes de implantar permissões de recursos. Isso permite validar que as alterações de política concedam apenas o acesso público e entre contas pretendido aos seus recursos. Ao designar para acesso a várias contas, você pode usar políticas de confiança para controlar em quais casos um perfil pode ser assumido. Por exemplo, você pode usar a chave de condição `PrincipalOrgId` para negar uma tentativa de assumir uma função fora da sua AWS Organizations.

O AWS Config pode relatar recursos que estão configurados incorretamente e, por meio de verificações de políticas do AWS Config, pode detectar recursos com acesso público configurado. Serviços como AWS Control Tower e AWS Security Hub simplificam as barreiras de proteção e as verificações de implantação em um AWS Organizations para identificar e corrigir recursos

publicamente expostos. Por exemplo, AWS Control Tower tem uma barreira de proteção gerenciada que pode detectar se algum snapshot do Amazon EBS pode ser restaurado por Contas da AWS.

Etapas de implementação

- Considere usar o AWS Config para AWS Organizations: o AWS Config permite agregar descobertas de várias contas em um AWS Organizations na conta de um administrador delegado. Isso fornece uma visão abrangente e permite que você implante Regras do AWS Config em várias contas para detectar recursos acessíveis ao público.
- Configure o AWS Identity and Access Management Access Analyzer: O IAM Access Analyzer ajuda você a identificar os recursos em sua organização e suas contas, como buckets do Amazon S3 ou perfis do IAM, que são compartilhados com uma entidade externa.
- Use a remediação automática no AWS Config para responder a mudanças na configuração de acesso público dos buckets do Amazon S3: você pode ativar automaticamente as configurações de bloqueio de acesso público para buckets do Amazon S3.
- Implemente monitoramento e alertas para identificar se os buckets do Amazon S3 se tornaram públicos: você deve ter monitoramento e alertas em vigor para identificar quando o Bloqueio de Acesso Público do Amazon S3 está desativado e se os buckets do Amazon S3 se tornam públicos. Além disso, se você estiver usando o AWS Organizations, poderá criar uma política de controle de serviços que impeça alterações nas políticas de acesso público do Amazon S3. O AWS Trusted Advisor procura buckets do Amazon S3 que têm permissões de acesso livre. As permissões de bucket que concedem acesso de upload ou exclusão a todos criam possíveis problemas de segurança, pois permitem que qualquer pessoa adicione, modifique ou remova itens em um bucket. A verificação do Trusted Advisor examina as permissões de bucket explícitas e as políticas de bucket associadas que podem substituir as permissões de bucket. Você também pode utilizar o AWS Config para monitorar seus buckets do Amazon S3 para acesso público. Para obter mais informações, consulte Como usar o AWS Config para monitorar e responder a buckets do Amazon S3 que permitem acesso público.

Ao analisar os controles de acesso dos buckets do Amazon S3, é importante considerar a natureza dos dados armazenados neles. O Amazon Macie é um serviço desenvolvido para ajudar você a descobrir e proteger dados confidenciais, como informações de identificação pessoal (PII), informações de saúde protegidas (PHI) e credenciais, como chaves privadas ou chaves de acesso da AWS.

Recursos

Documentos relacionados:

- Como usar o AWS Identity and Access Management Access Analyzer
- Biblioteca de controles do AWS Control Tower
- Padrão de práticas recomendas de segurança básica da AWS
- Regras gerenciadas do AWS Config
- Referência de verificação do AWS Trusted Advisor
- Monitorar resultados da verificação do AWS Trusted Advisor com o Amazon EventBridge
- Habilitar regras do AWS Config em todas as contas na sua organização
- AWS Config e AWS Organizations
- Disponibilizar publicamente sua AMI para uso no Amazon EC2

Vídeos relacionados:

- Práticas recomendadas para proteger seu ambiente de várias contas
- Mergulho profundo no IAM Access Analyzer

SEC03-BP08 Compartilhar recursos com segurança em sua organização

À medida que o número de workloads aumenta, talvez você precise compartilhar o acesso aos recursos nessas workloads ou fornecer os recursos várias vezes nas contas. É possível usar constructos para compartimentalizar seu ambiente, por exemplo, para ter ambientes de desenvolvimento, teste e produção. No entanto, ter constructos de separação não impede que você compartilhe com segurança. Ao compartilhar componentes que se sobrepõem, você pode reduzir a sobrecarga operacional e possibilitar uma experiência consistente sem precisar adivinhar o que ignorou ao criar o mesmo recurso várias vezes.

Resultado desejado: minimize o acesso não intencional usando métodos seguros para compartilhar recursos em sua organização e ajudar na sua iniciativa de prevenção de perda de dados. Reduza sua sobrecarga operacional em comparação com o gerenciamento de componentes individuais, reduza os erros gerados pela criação manual do mesmo componente várias vezes e aumente a escalabilidade das suas workloads. É possível se beneficiar da redução de tempo para a resolução em cenários de falhas em vários pontos e aumentar sua confiança na determinação de quando

um componente não é mais necessário. Para obter recomendações sobre a análise de recursos compartilhados externamente, consulte SEC03-BP07 Analisar o acesso público e entre contas.

Práticas comuns que devem ser evitadas:

- Ausência de um processo para monitorar de forma contínua e alertar automaticamente sobre o compartilhamento externo inesperado.
- Ausência de referência sobre o que deve ou não ser compartilhado.
- Adotar como padrão uma política amplamente aberta em vez de compartilhar explicitamente quando necessário.
- Criar manualmente recursos básicos que se sobrepõem quando necessário.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

Projete seus controles e padrões de acesso para reger o consumo de recursos compartilhados com segurança e somente com entidades confiáveis. Monitore recursos compartilhados e revise o acesso a eles de forma contínua e seja alertado sobre o compartilhamento inadequado ou inesperado. Revise Analisar o acesso público e entre contas para saber como estabelecer uma governança para limitar o acesso externo somente aos recursos que o exijam e estabelecer um processo para monitorar continuamente e enviar alertas de forma automática.

O compartilhamento entre contas no AWS Organizations é aceito por vários serviços da AWS, como AWS Security Hub, Amazon GuardDuty e AWS Backup. Esses serviços possibilitam compartilhar os dados em uma conta central, acessá-los ou gerenciar recursos e dados dessa conta. Por exemplo, o AWS Security Hub pode transferir as descobertas de contas individuais para uma conta central onde é possível visualizar todas elas. O AWS Backup pode fazer um backup de um recurso e compartilhá-lo entre contas. É possível usar o AWS Resource Access Manager (AWS RAM) para compartilhar outros recursos comuns, como sub-redes de VPC e anexos do gateway de trânsito, AWS Network Firewall ou pipelines do Amazon SageMaker AI.

Para restringir sua conta para compartilhar apenas recursos dentro de sua organização, use políticas de controle de serviços (SCPs) para impedir o acesso a entidades externas. Ao compartilhar recursos, combine controles baseados em identidade e controles de rede para criar um perímetro de dados para sua organização e ajudar a se proteger contra acesso não intencional. Um perímetro de dados é um conjunto de barreiras de proteção preventivas que ajudam a garantir que apenas suas

identidades confiáveis acessem recursos confiáveis das redes esperadas. Esses controles impõem limites apropriados sobre quais recursos podem ser compartilhados e impedir o compartilhamento ou a exposição de recursos que não devem ser permitidos. Por exemplo, como parte do seu perímetro de dados, você pode usar as políticas de endpoint da VPC e a condição `AWS:PrincipalOrgId` para garantir que as identidades que acessam seus buckets do Amazon S3 pertençam à sua organização. É importante observar que as SCPs não se aplicam a perfis vinculados a serviços ou entidades principais de serviços da AWS.

Ao usar o Amazon S3, desative as ACLs do seu bucket do Amazon S3 e use as políticas do IAM para definir o controle de acesso. Para restringir o acesso a uma origem do Amazon S3 do Amazon CloudFront, migre da identidade do acesso de origem (OAI) para um controle de acesso de origem (OAC) compatível com recursos adicionais, incluindo criptografia do lado do servidor com o AWS Key Management Service.

Em alguns casos, convém permitir o compartilhamento de recursos fora de sua organização ou conceder a terceiros acesso aos seus recursos. Para obter recomendações sobre o gerenciamento de permissões para compartilhar recursos externamente, consulte Gerenciamento de permissões.

Etapas de implementação

1. Use o AWS Organizations: O AWS Organizations é um serviço de gerenciamento de contas que permite consolidar várias Contas da AWS em uma organização criada e gerencia centralmente por você. É possível agrupar suas contas em unidades organizacionais (UOs) e anexar políticas diferentes a cada UO a fim de ajudar a atender às suas necessidades orçamentárias, de segurança e conformidade. Também é possível controlar como serviços de inteligência artificial (IA) e machine learning (ML) da AWS podem coletar e armazenar dados e usar o gerenciamento de várias contas dos serviços da AWS integrados ao Organizations.
2. Integre o AWS Organizations com serviços da AWS: quando você usa um serviço da AWS para executar tarefas em seu nome nas contas-membro da organização, o AWS Organizations cria um perfil vinculado ao serviço (SLR) do IAM para esse serviço em cada conta-membro. Você deve gerenciar o acesso confiável usando o AWS Management Console, as APIs da AWS ou a AWS CLI. Para obter recomendações sobre como ativar o acesso confiável, consulte Usar o AWS Organizations com outros serviços da AWS e Serviços da AWS que você pode usar com o Organizations.
3. Estabeleça um perímetro de dados: um perímetro de dados fornece um limite claro de confiança e propriedade. Na AWS, costuma ser representado como sua organização na AWS gerenciada pelo AWS Organizations, com quaisquer redes ou sistemas on-premises que acessam os recursos da AWS. O objetivo do perímetro de dados é garantir que o acesso seja permitido se a identidade e

o recurso forem confiáveis e a rede for esperada. No entanto, estabelecer um perímetro de dados não é uma abordagem única. Avalie e adote os objetivos de controle descritos no whitepaper sobre como criar um perímetro na AWS com base em modelos e requisitos de risco de segurança específicos. Você deve considerar cuidadosamente sua postura de risco exclusiva e implementar os controles de perímetro que se alinhem às suas necessidades de segurança.

4. Use o compartilhamento de recursos nos serviços da AWS e restrinja adequadamente: muitos serviços da AWS permitem compartilhar recursos com outra conta ou apontar para um recurso em outra conta, como imagens de máquina da Amazon (AMIs) e AWS Resource Access Manager (AWS RAM). Restrinja a API `ModifyImageAttribute` para especificar as contas confiáveis com as quais a AMI será compartilhada. Especifique a condição `ram:RequestedAllowsExternalPrincipals` ao usar o AWS RAM para restringir o compartilhamento somente à sua organização, ajudando assim a impedir o acesso de identidades não confiáveis. Para orientações e recomendações, consulte Compartilhamento de recursos e destinos externos.
5. Use AWS RAM para compartilhar com segurança em uma conta ou com outras Contas da AWS: O AWS RAM ajuda você a compartilhar com segurança os recursos criados com perfis e usuários em sua conta e em outras Contas da AWS. Em um ambiente de várias contas, o AWS RAM permite criar um recurso uma vez e compartilhá-lo com outras contas. Essa abordagem ajuda a reduzir sua sobrecarga operacional enquanto oferece consistência, visibilidade e capacidade de auditoria por meio de integrações com o Amazon CloudWatch e o AWS CloudTrail, o que você não recebe ao utilizar o acesso entre contas.

   Se você tiver recursos que compartilhou anteriormente usando uma política baseada em recursos, poderá usar a API `PromoteResourceShareCreatedFromPolicy` ou equivalente para promover o compartilhamento de recursos em um compartilhamento de recursos do AWS RAM completo.

   Em alguns casos, convém realizar etapas adicionais para compartilhar recursos. Por exemplo, para compartilhar um snapshot criptografado, é necessário compartilhar uma chave do AWS KMS.

Recursos

Práticas recomendadas relacionadas:

- SEC03-BP07 Analisar o acesso público e entre contas
- SEC03-BP09 Compartilhar recursos com terceiros de forma segura
- SEC05-BP01 Criar camadas de rede

Documentos relacionados:

- O proprietário do bucket concede permissão entre contas para objetos que não possui
- Como usar políticas de confiança com o IAM
- Como criar um perímetro de dados na AWS
- Como usar um ID externo ao conceder acesso aos seus recursos da AWS para terceiros
- Serviços da AWS que você pode usar com o AWS Organizations
- Estabelecer um perímetro de dados na AWS: permitir que somente identidades confiáveis acessem os dados da empresa

Vídeos relacionados:

- Acesso granular com o AWS Resource Access Manager
- Como proteger seu perímetro de dados com endpoints da VPC
- Estabelecer um perímetro de dados na AWS

Ferramentas relacionadas:

- Exemplos de políticas de perímetro de dados

SEC03-BP09 Compartilhar recursos com terceiros de forma segura

A segurança de seu ambiente de nuvem não para na sua organização. Sua organização pode contar com terceiros para gerenciar uma parte de seus dados. O gerenciamento de permissões para o sistema gerenciado por terceiros deve seguir a prática de acesso just-in-time utilizando o princípio de privilégio mínimo com credenciais temporárias. Ao trabalhar em parceria com terceiros, é possível reduzir o escopo do impacto e o risco de acesso acidental.

Resultado desejado: você evita usar credenciais de longo prazo do AWS Identity and Access Management (IAM), como chaves de acesso e chaves secretas, pois elas representam um risco de segurança se usadas indevidamente. Em vez disso, você usa perfis do IAM e credenciais temporárias para melhorar sua postura de segurança e minimizar a sobrecarga operacional do gerenciamento de credenciais de longo prazo. Ao conceder acesso a terceiros, use um identificador universalmente exclusivo (UUID) como ID externo na política de confiança do IAM e mantenha as políticas do IAM anexadas ao perfil sob seu controle para garantir privilégio mínimo de acesso. Para

conferir recomendações sobre a análise de recursos compartilhados externamente, consulte SEC03-BP07 Analisar o acesso público e entre contas.

Práticas comuns que devem ser evitadas:

- Utilizar a política de confiança padrão do IAM sem nenhuma condição.
- Utilizar credenciais e chaves de acesso de longo prazo do IAM.
- Reutilizar IDs externos.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

Talvez você deseje permitir o compartilhamento de recursos fora do AWS Organizations ou conceder a terceiros acesso à sua conta. Por exemplo, um parceiro (terceiro) pode oferecer uma solução de monitoramento que precise acessar recursos em sua conta. Nesses casos, crie um perfil entre contas do IAM somente com os privilégios necessários para o parceiro. Além disso, defina uma política de confiança usando a condição de ID externo. Ao utilizar um ID externo, você ou o parceiro pode gerar um ID exclusivo para cada cliente, terceiro ou locação. O ID exclusivo não deve ser controlado por ninguém, exceto por você, depois de criado. O parceiro deve implementar um processo para relacionar o ID externo ao cliente de forma segura, auditável e reproduzível.

Também é possível usar o IAM Roles Anywhere para gerenciar perfis do IAM para aplicações fora da AWS que usam APIs da AWS.

Se o parceiro não precisar mais de acesso ao seu ambiente, remova o perfil. Evite fornecer credenciais de longo prazo para terceiros. Conheça outros serviços da AWS que oferecem suporte ao compartilhamento, como a permissão do AWS Well-Architected Tool ao compartilhamento de uma workload com outras Contas da AWS e o AWS Resource Access Manager, que ajuda a compartilhar com segurança um recurso da AWS que você possui com outras contas.

Etapas de implementação

1. Use perfis entre contas para fornecer acesso a contas externas. Os perfis entre contas reduzem a quantidade de informações confidenciais armazenadas por contas externas e por terceiros para atender os clientes. Os perfis entre contas possibilitam que você conceda acesso aos recursos da AWS em sua conta de maneira segura a terceiros, como parceiros da AWS ou outras contas em sua organização, ao mesmo tempo que mantém a capacidade de gerenciar e auditar esse

acesso. O parceiro pode oferecer serviço a você a partir de uma infraestrutura híbrida ou, como alternativa, extrair dados de um local externo. O IAM Roles Anywhere ajuda você a permitir que workloads de terceiros interajam com segurança com suas workloads da AWS e a reduzir ainda mais a necessidade de credenciais de longo prazo.

Você não deve usar credenciais ou chaves de acesso de longo prazo associadas a usuários para conceder acesso a contas externas. Em vez disso, utilize perfis entre contas para conceder acesso entre contas.

2. Realize a devida diligência e garanta o acesso seguro para provedores de SaaS de terceiros. Ao compartilhar recursos com provedores de SaaS de terceiros, realize a devida diligência para garantir que eles tenham uma abordagem segura e responsável para acessar os recursos da AWS. Avalie seu modelo de responsabilidade compartilhada para entender quais medidas de segurança eles fornecem e o que está sob sua responsabilidade. Garanta que o provedor de SaaS tenha um processo seguro e auditável para acessar seus recursos, incluindo o uso de IDs externos e princípios de acesso com privilégios mínimos. O uso de IDs externos ajuda a resolver o problema de representante confuso.

   Implemente controles de segurança para garantir acesso seguro e aderir ao princípio de privilégio mínimo ao conceder acesso a provedores de SaaS de terceiros. Isso pode incluir o uso de IDs externos, identificadores universalmente exclusivos (UUIDs) e políticas de confiança do IAM que limitam o acesso somente ao estritamente necessário. Trabalhe em estreita colaboração com o provedor de SaaS para estabelecer mecanismos de acesso seguro, revisar regularmente o acesso deles aos recursos da AWS e realizar auditorias para garantir a conformidade com os requisitos de segurança.

3. Deprecie as credenciais de longo prazo fornecidas pelo cliente. Deprecie o uso de credenciais de longo prazo e use perfis entre clientes ou o IAM Roles Anywhere. Se você precisar utilizar credenciais de longo prazo, estabeleça um plano para migrar para um acesso baseado em perfil. Para obter detalhes sobre o gerenciamento de chaves, consulte Gerenciamento de identidades. Trabalhe também com a equipe da sua Conta da AWS e o parceiro para estabelecer um runbook de mitigação de riscos. Para conferir recomendações sobre como responder e mitigar o impacto potencial de um incidente de segurança, consulte Resposta a incidentes.

4. Verifique se a configuração possui recomendações ou é automatizada. O ID externo não é tratado como segredo, mas ele não pode ser um valor facilmente dedutível, como um número de telefone, um nome ou o ID da conta. Torne o ID externo um campo somente leitura de forma que o ID externo não possa ser alterado com o fim de representar a configuração.

Você ou o parceiro podem gerar o ID externo. Defina um processo para determinar quem é responsável pela geração do ID. Seja qual for a entidade que crie o ID externo, o parceiro impõe a exclusividade e os formatos de forma consistente entre os clientes.

A política criada para acesso entre contas em suas contas deve seguir o princípio de privilégio mínimo. O terceiro deve fornecer um documento de política de perfil ou um mecanismo de configuração automatizada que utilize um modelo do AWS CloudFormation ou um equivalente para você. Isso reduz a chance de erros associados à criação manual de políticas e oferece uma trilha auditável. Para obter mais informações sobre como usar um modelo do AWS CloudFormation para criar funções entre contas, consulte Funções entre contas.

O terceiro deve fornecer um mecanismo de configuração automatizado e auditável. No entanto, ao utilizar o documento de política de perfis que descreve o acesso necessário, você deve automatizar a configuração do perfil. Com um modelo do AWS CloudFormation ou equivalente, monitore alterações com detecção de desvios como parte da prática de auditoria.

5. Considere as alterações. Sua estrutura de contas, sua necessidade de terceiros ou a oferta de serviço pode sofrer alterações. Você deve antecipar alterações e falhas e planejar adequadamente com as pessoas, o processo e a tecnologia corretos. Audite o nível de acesso que você concede periodicamente e implemente métodos de detecção para ser alertado sobre alterações inesperadas. Monitore e audite o uso do perfil e o datastore dos IDs externos. Você deve estar preparado para revogar o acesso de terceiros, seja de forma temporária ou permanente, como resultado de alterações ou padrões de acesso inesperados. Além disso, meça o impacto de sua operação de revogação, inclusive o tempo para realizá-la, as pessoas envolvidas, o custo e o impacto de outros recursos.

   Para obter recomendações sobre métodos de detecção, consulte as práticas recomendadas de detecção.

Recursos

Práticas recomendadas relacionadas:

- SEC02-BP02 Usar credenciais temporárias
- SEC03-BP05 Definir barreiras de proteção de permissões para sua organização
- SEC03-BP06 Gerenciar o acesso com base no ciclo de vida
- SEC03-BP07 Analisar o acesso público e entre contas

- SEC04 Detecção

Documentos relacionados:

- O proprietário do bucket concede permissão entre contas para objetos que não possui
- Como usar políticas de confiança com perfis do IAM
- Delegar acesso entre Contas da AWS usando perfis do IAM
- Como faço para acessar recursos em outra Conta da AWS usando o IAM?
- Práticas recomendadas de segurança no IAM
- Lógica de avaliação de política entre contas
- Como usar um ID externo ao conceder acesso aos seus recursos da AWS para terceiros
- Coletar informações de recursos da AWS CloudFormation criados em contas externas com recursos personalizados
- Usar IDs externos com segurança para acessar contas da AWS pertencentes a terceiros
- Estender os perfis do IAM para workloads fora do IAM com o IAM Roles Anywhere

Vídeos relacionados:

- Como faço para permitir que usuários ou perfis em uma Conta da AWS separada tenham acesso à minha Conta da AWS?
- AWS re:Invent 2018: Become an IAM Policy Master in 60 Minutes or Less
- Centro de Conhecimentos da AWS Live: Práticas recomendadas e decisões de design do IAM

Exemplos relacionados:

- Configurar o acesso entre contas ao Amazon DynamoDB
- Ferramenta de consulta de rede do AWS STS

Detecção

A detecção consiste em duas partes: detecção de alterações de configuração inesperadas ou indesejadas e detecção de comportamento inesperado. O primeiro pode ocorrer em vários locais do ciclo de vida de entrega de uma aplicação. Usando a infraestrutura como código (por exemplo, um modelo do CloudFormation), é possível verificar configurações indesejadas antes que uma workload seja implantada por meio da implementação de verificações nos pipelines de CI/CD ou no controle de origem. Então, ao implantar uma workload em ambientes de não produção e de produção, você pode verificar a configuração usando ferramentas nativas da AWS, de código aberto ou de parceiros da AWS. Essas verificações podem ser para configurações que não atendem a princípios de segurança ou a práticas recomendas, ou para alterações feitas entre uma configuração testada e uma implantada. Para uma aplicação em execução, você pode verificar se a configuração foi alterada de forma inesperada, inclusive fora de uma implantação conhecida ou de um evento de ajuste de escala automatizado.

Para a segunda parte da detecção, comportamento inesperado, é possível usar ferramentas ou alertar sobre um aumento em um tipo específico de chamada de API. Usando o Amazon GuardDuty, você pode ser alertado quando atividades inesperadas e, possivelmente, não autorizadas ou maliciosas ocorrerem nas suas contas da AWS. Você também deve monitorar explicitamente as chamadas de API mutantes que você não esperaria que fossem usadas em sua workload e as chamadas de API que alteram a postura de segurança.

A detecção permite identificar uma possível configuração incorreta de segurança, uma ameaça ou um comportamento inesperado. Essa é uma parte essencial do ciclo de vida de segurança e pode ser usada para apoiar um processo de qualidade, uma obrigação legal ou de conformidade e os esforços de identificação e resposta a ameaças. Existem diferentes tipos de mecanismos de detecção. Por exemplo, os logs da workload podem ser analisados em busca de explorações que estão sendo usadas. Revise regularmente os mecanismos de detecção relacionados à sua workload para garantir que você esteja atendendo às políticas e aos requisitos internos e externos. Os alertas e notificações automatizados devem se basear em condições definidas para permitir que as equipes ou ferramentas investiguem. Esses mecanismos são fatores reativos importantes que podem ajudar a organização a identificar e entender o escopo de atividades anômalas.

Na AWS, há várias abordagens para lidar com mecanismos de detecção. As seções a seguir descrevem como usar essas abordagens:

Práticas recomendadas

- SEC04-BP01 Configurar o registro em log de serviços e aplicações
- SEC04-BP02 Capturar logs, descobertas e métricas em locais padronizados
- SEC04-BP03 Correlacionar e enriquecer alertas de segurança
- SEC04-BP04 Iniciar a correção de recursos fora de conformidade

SEC04-BP01 Configurar o registro em log de serviços e aplicações

Retenha logs de eventos de segurança de serviços e aplicações. Esse é um princípio fundamental de segurança para auditoria, investigações e casos de uso operacionais e um requisito de segurança comum orientado por padrões, políticas e procedimentos de governança, risco e conformidade (GRC).

Resultado desejado: uma organização deve ser capaz de recuperar de forma confiável e consistente logs de eventos de segurança de serviços e aplicações da AWS em tempo hábil quando necessário para cumprir um processo ou obrigação interna, como uma resposta a incidente de segurança. Considere centralizar os logs para obter os melhores resultados operacionais.

Práticas comuns que devem ser evitadas:

- Os logs são armazenados de forma perpétua ou excluídos muito precocemente.
- Todos podem acessar os logs.
- Contar inteiramente com processos manuais para uso e governança de logs.
- Armazenar todo e qualquer tipo de log para uma eventual necessidade.
- Conferir a integridade dos logs apenas quando necessário.

Benefícios de implementar esta prática recomendada: implemente um mecanismo de análise de causa-raiz (RCA) para incidentes de segurança e uma fonte de evidência para suas obrigações de governança, risco e conformidade.

Nível de risco exposto se esta prática recomendada não for estabelecida: Alto

Orientação para implementação

Durante uma investigação de segurança ou outros casos de uso com base em seus requisitos, você precisa ser capaz de analisar os logs relevantes a fim de registrar e entender o escopo total e a linha do tempo do incidente. Os logs também são necessários para geração de alertas indicando que

ocorreram determinadas ações de interesse. É essencial selecionar, ativar, armazenar e configurar mecanismos de consulta, recuperação e alertas.

Etapas de implementação

- Selecione e use fontes de log. Antes de uma investigação de segurança, você precisa capturar logs relevantes para reconstruir de forma retroativa a atividade em uma Conta da AWS. Selecione fontes de logs relevantes para suas workloads.

  Os critérios de seleção de fonte de logs devem se basear nos casos de uso necessários à sua empresa. Estabeleça uma trilha para cada Conta da AWS utilizando o AWS CloudTrail ou uma trilha do AWS Organizations e configure um bucket do Amazon S3 para ela.

  O AWS CloudTrail é um serviço de registro em log que rastreia chamadas de API feitas em uma Conta da AWS capturando a atividade do serviço da AWS. Ele é ativado por padrão com uma retenção de 90 dias de eventos de gerenciamento que podem ser recuperados por meio do histórico de eventos do CloudTrail via AWS Management Console, AWS CLI ou AWS SDK. Para maior retenção e visibilidade dos eventos de dados, crie uma trilha do CloudTrail e associe-a a um bucket do Amazon S3 e, opcionalmente, a um grupo de log do Amazon CloudWatch. Como alternativa, você pode criar um CloudTrail Lake, o qual retém os logs do CloudTrail por até sete anos e fornece um recurso de consulta baseado em SQL

  A AWS recomenda que os clientes que usam VPC ativem os logs de tráfego de rede e DNS usando Logs de fluxo da VPC e Logs de consulta do Amazon Route 53 Resolver, respectivamente, e os transmitam para um bucket do Amazon S3 ou um grupo de logs do CloudWatch. É possível criar um log de fluxo de VPC, uma sub-rede ou uma interface de rede. Para logs de fluxo de VPC, é possível ser seletivo em relação a como e onde usar os logs de fluxo para reduzir o custo.

  Logs do AWS CloudTrail, logs de fluxo de VPC e logs de consulta do Route 53 Resolver são as fontes básicas de registro em log para oferecer compatibilidade com investigações de segurança na AWS. Também é possível usar o Amazon Security Lake para coletar, normalizar e armazenar esses dados de log no formato Apache Parquet e no Open Cybersecurity Schema Framework (OCSF), que está pronto para consulta. O Security Lake também é compatível com outros logs da AWS e logs de fontes de terceiros.

  Os serviços da AWS podem gerar logs não capturados pelas fontes de log básicas, como logs do Elastic Load Balancing, logs do AWS WAF, logs de gravador do AWS Config, descobertas do Amazon GuardDuty, logs de auditoria do Amazon Elastic Kubernetes Service (Amazon EKS) e logs de sistema operacional e aplicações e de instâncias do Amazon EC2. Para obter uma

lista completa das opções de registro e monitoramento, consulte o Apêndice A: Definições de capacidade de nuvem – Log e eventos do Guia de Resposta a Incidentes de Segurança da AWS.

- Pesquise recursos de log para cada serviço e aplicação da AWS: cada serviço e aplicação da AWS oferece opções de armazenamento de log, cada uma com seus próprios recursos de retenção e ciclo de vida. Os dois serviços de armazenamento de logs mais comuns são o Amazon Simple Storage Service (Amazon S3) e o Amazon CloudWatch. Para períodos de retenção longos, é recomendável utilizar o Amazon S3 para seus recursos de economia e ciclo de vida flexíveis. Se a opção de registro em log principal for o Amazon CloudWatch Logs, como opção, você deve considerar o arquivamento de logs menos acessados no Amazon S3.
- Selecione o armazenamento de logs: a escolha do armazenamento de logs geralmente está relacionada à ferramenta de consulta que você usa, aos recursos de retenção, à familiaridade e ao custo. As principais opções para armazenamento de logs são um bucket do Amazon S3 ou um grupo de logs do CloudWatch.

  Um bucket do Amazon S3 oferece armazenamento econômico e durável com uma política de ciclo de vida opcional. Os logs armazenados em buckets do Amazon S3 podem ser consultados com serviços como o Amazon Athena.

  Um grupo de logs do CloudWatch oferece armazenamento durável e um recurso de consultas incorporado por meio do CloudWatch Logs Insights.
- Identifique a retenção apropriada de logs: ao usar um bucket do Amazon S3 ou um grupo de logs do CloudWatch para armazenar logs, você deve estabelecer ciclos de vida adequados para cada fonte de log para otimizar os custos de armazenamento e recuperação. Os clientes geralmente têm entre três meses a um ano de logs prontamente disponíveis para consultas, com retenção de até sete anos. A escolha de disponibilidade e retenção deve se alinhar aos seus requisitos de segurança e um composto de atribuições regulatórias, estatutárias e de negócios.
- Use o registro em log para cada serviço e aplicação da AWS com políticas adequadas de retenção e ciclo de vida: para cada serviço ou aplicação da AWS em sua organização, procure a orientação específica de configuração do log:
  - Configurar trilha do AWS CloudTrail
  - Configurar Logs de fluxo da VPC
  - Configurar a exportação de descobertas do Amazon GuardDuty
  - Configurar a gravação do AWS Config
  - Configurar o tráfego de ACL da Web do AWS WAF
  - Configurar logs de tráfego de rede do AWS Network Firewall

  - Configurar logs de acesso do Elastic Load Balancing
  - Configurar logs de consulta do Amazon Route 53 Resolver
  - Configurar logs do Amazon RDS
  - Configurar logs do ambiente de gerenciamento do Amazon EKS
  - Configurar o agente do Amazon CloudWatch para instâncias do Amazon EC2 e servidores on-premises
- Selecione e implemente mecanismos de consulta para logs: para consultas em logs, é possível usar o CloudWatch Logs Insights para dados armazenados em grupos de log do CloudWatch, e o Amazon Athena e o Amazon OpenSearch Service para dados armazenados no Amazon S3. Também é possível usar ferramentas de consulta de terceiros, como um serviço de gerenciamento de eventos e informações de segurança (SIEM).

  O processo para selecionar uma ferramenta de consulta de log deve considerar as pessoas, o processo e os aspectos de tecnologia de suas operações de segurança. Selecione uma ferramenta que atenda aos requisitos operacionais, de negócios e segurança, esteja acessível e possa receber manutenção no longo prazo. Lembre-se de que as ferramentas de consulta de logs funcionam da forma ideal quando o número de logs a serem verificados é mantido dentro dos limites da ferramenta. Não é incomum ter várias ferramentas de consulta devido a restrições financeiras ou técnicas.

  Por exemplo, você pode usar uma ferramenta de gerenciamento de eventos e informações de segurança (SIEM) de terceiros para realizar consultas para os últimos 90 dias de dados, mas usar o Athena para realizar consultas além de 90 dias devido ao custo de ingestão de logs de um SIEM. Seja qual for a implementação, garanta que sua abordagem minimize o número de ferramentas necessárias para maximizar a eficiência operacional, especialmente durante a investigação de um evento de segurança.
- Use logs para alertas: a AWS fornece alertas por meio de vários serviços de segurança.
  - O AWS Config monitora e registra as configurações de recursos da AWS e permite automatizar as tarefas de avaliação e correção em relação às configurações desejadas.
  - O Amazon GuardDuty é um serviço de detecção de ameaças que monitora continuamente atividades mal-intencionadas e comportamentos não autorizados para proteger suas Contas da AWS e workloads. O GuardDuty ingere, agrega e analisa informações de fontes, como eventos de gerenciamento e dados do AWS CloudTrail, logs de DNS, logs de fluxo de VPC e logs de auditoria do Amazon EKS. O GuardDuty extrai fluxos de dados independentes diretamente do CloudTrail, dos logs de fluxo de VPC, dos logs de consulta ao DNS e do Amazon EKS. Não

é necessário gerenciar políticas de bucket do Amazon S3 nem modificar a forma de coletar e armazenar logs. Ainda é recomendável reter esses logs para sua própria investigação e fins de conformidade.

- O AWS Security Hub fornece um único local que agrega, organiza e prioriza alertas de segurança ou descobertas de vários serviços da AWS e produtos opcionais de terceiros para oferecer uma visão abrangente dos alertas de segurança e do status de conformidade.

Você também pode utilizar mecanismos de geração de alertas personalizados para alertas de segurança não cobertos por esses serviços ou para alertas específicos relevantes para o seu ambiente. Para obter informações sobre como criar esses alertas e detecções, consulte Detecção no Guia de resposta a incidentes de segurança da AWS.

Recursos

Práticas recomendadas relacionadas:

- SEC04-BP02 Capturar logs, descobertas e métricas em locais padronizados
- SEC07-BP04 Definir o gerenciamento escalável do ciclo de vida dos dados
- SEC10-BP06 Implantar ferramentas previamente

Documentos relacionados:

- Guia de resposta a incidentes de segurança da AWS
- Conceitos básicos do Amazon Security Lake
- Conceitos básicos do Amazon CloudWatch Logs

Vídeos relacionados:

- AWS re:Invent 2022: Lançamento do Amazon Security Lake

Exemplos relacionados:

- Ativador de log assistido para AWS
- Exportação do histórico de descobertas do AWS Security Hub

SEC04-BP02 Capturar logs, descobertas e métricas em locais padronizados

As equipes de segurança confiam em logs e descobertas para analisar eventos que podem indicar atividades não autorizadas ou alterações não intencionais. Para agilizar essa análise, capture logs e descobertas de segurança em locais padronizados. Fazer isso disponibiliza pontos de dados de interesse para correlação e pode simplificar a integração de ferramentas.

Resultado desejado: você tem uma abordagem padronizada para coletar, analisar e visualizar dados de log, descobertas e métricas. As equipes de segurança podem correlacionar, analisar e visualizar com eficiência os dados de segurança em sistemas diferentes para descobrir possíveis eventos de segurança e identificar anomalias. Os sistemas de gerenciamento de eventos e informações de segurança (SIEM) ou outros mecanismos são integrados para consultar e analisar dados de log e oferecer respostas oportunas, rastreamento e encaminhamento de eventos de segurança.

Práticas comuns que devem ser evitadas:

- As equipes são proprietárias e gerenciam de forma independente o registro em log e a coleta de métricas que são inconsistentes com a estratégia de registro em log da organização.
- As equipes não têm controles de acesso adequados para restringir a visibilidade e a alteração dos dados coletados.
- As equipes não controlam logs, descobertas e métricas de segurança como parte da política de classificação de dados.
- As equipes negligenciam os requisitos de soberania e localização dos dados ao configurar as coletas de dados.

Benefícios de implementar esta prática recomendada: uma solução de registro em log padronizada para coletar e consultar dados e eventos de registro melhora os insights derivados das informações neles contidas. Configurar um ciclo de vida automatizado para os dados de log coletados pode reduzir os custos incorridos pelo armazenamento de logs. É possível criar um controle de acesso refinado para as informações de log coletadas de acordo com a confidencialidade dos dados e os padrões de acesso necessários para as equipes. Você pode integrar ferramentas para correlacionar, visualizar e obter insights dos dados.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

O aumento do uso da AWS em uma organização resulta em um número crescente de workloads e ambientes distribuídos. Como cada um desses ambientes e workloads gera dados sobre as atividades dentro deles, capturar e armazenar esses dados localmente representa um desafio para as operações de segurança. As equipes de segurança usam ferramentas, como sistemas de gerenciamento de eventos e informações de segurança (SIEM), para coletar dados de fontes distribuídas e submetê-los a fluxos de trabalho de correlação, análise e resposta. Isso requer o gerenciamento de um conjunto complexo de permissões para acessar as várias fontes de dados e despesas operacionais indiretas adicionais na operação dos processos de extração, transformação e carregamento (ETL).

Para superar esses desafios, considere agregar todas as fontes relevantes de dados de log de segurança em uma conta de arquivamento de logs, conforme descrito em Como organizar seu ambiente da AWS usando várias contas. Isso inclui todos os dados relacionados à segurança da sua workload e dos logs gerados pelos serviços da AWS, como AWS CloudTrail, AWS WAF, Elastic Load Balancing e Amazon Route 53. Há vários benefícios resultantes da captura desses dados em locais padronizados em uma Conta da AWS separada com as devidas permissões entre contas. Essa prática ajuda a evitar a violação de logs em workloads e ambientes comprometidos, fornece um único ponto de integração para ferramentas adicionais e oferece um modelo mais simplificado para configurar a retenção de dados e o ciclo de vida. Avalie os impactos da soberania de dados, dos escopos de conformidade e de outras regulamentações para determinar se vários locais de armazenamento de dados de segurança e períodos de retenção são necessários.

Para facilitar a captura e padronização de logs e descobertas, avalie o Amazon Security Lake em sua conta de arquivamento de logs. É possível configurar o Security Lake para ingerir automaticamente dados de fontes comuns, como CloudTrail, Route 53, Amazon EKS e logs de fluxo de VPC. Também é possível configurar AWS Security Hub como fonte de dados no Security Lake, permitindo que você correlacione descobertas de outros serviços da AWS, como Amazon GuardDuty e Amazon Inspector, com seus dados de log. Você também pode usar integrações de fontes de dados de terceiros ou configurar fontes de dados personalizadas. Todas as integrações padronizam seus dados no formato Open Cybersecurity Schema Framework (OCSF) e são armazenadas em buckets do Amazon S3 como arquivos Parquet, eliminando a necessidade de processamento de ETL.

O armazenamento de dados de segurança em locais padronizados fornece recursos avançados de análise. A AWS recomenda implantar ferramentas para análise de segurança que operem em um ambiente da AWS em uma conta do Security Tooling separada da sua conta de arquivamento de logs. Essa abordagem permite implantar controles detalhados para proteger a integridade e a

disponibilidade dos logs e do processo de gerenciamento de logs, diferentemente das ferramentas que os acessam. Considere usar serviços, como o Amazon Athena, para executar consultas sob demanda que correlacionam várias fontes de dados. Também é possível integrar ferramentas de visualização, como o QuickSight. As soluções baseadas em IA estão se tornando cada vez mais disponíveis e podem desempenhar funções como traduzir descobertas em resumos legíveis por humanos e interação em linguagem natural. Essas soluções geralmente são mais fáceis de integrar por terem um local de armazenamento de dados padronizado para consulta.

Etapas de implementação

1. Crie as contas do Log Archive e do Security Tooling
    a. Usando o AWS Organizations, crie as contas Log Archive e Security Tooling em uma unidade organizacional de segurança. Se estiver usando o AWS Control Tower para gerenciar sua organização, as contas de arquivo de logs e de ferramentas de segurança serão criadas automaticamente para você. Configure perfis e permissões para acessar e administrar essas contas conforme necessário.
2. Configure seus locais de dados de segurança padronizados
    a. Determine sua estratégia para criar locais de dados de segurança padronizados. É possível conseguir isso por meio de opções como abordagens comuns de arquitetura de data lake, produtos de dados de terceiros ou Amazon Security Lake. A AWS recomenda capturar dados de segurança de Regiões da AWS opted-in para suas contas, mesmo quando não estiverem em uso ativo.
3. Configurar a publicação da fonte de dados em seus locais padronizados
    a. Identifique as fontes de seus dados de segurança e configure-as para publicação em seus locais padronizados. Avalie as opções para exportar dados automaticamente no formato desejado, em vez daquelas em que é necessário desenvolver processos de ETL. Com o Amazon Security Lake, é possível coletar dados de fontes da AWS compatíveis e sistemas integrados de terceiros.
4. Configurar ferramentas para acessar seus locais padronizados
    a. Configure ferramentas (como o Amazon Athena e o QuickSight) ou soluções de terceiros para ter o acesso necessário aos locais padronizados. Configure essas ferramentas para operar fora da conta de ferramentas de segurança com acesso de leitura entre contas à conta de arquivo de logs quando aplicável. Crie assinantes no Amazon Security Lake para fornecer a essas ferramentas acesso aos seus dados.

Recursos

Práticas recomendadas relacionadas:

- SEC01-BP01 Separar workloads usando contas
- SEC07-BP04 Definir o gerenciamento do ciclo de vida dos dados
- SEC08-BP04 Aplicar controle de acesso
- OPS08-BP02 Analisar logs de workloads

Documentos relacionados:

- Whitepapers da AWS: Organizar seu ambiente da AWS usando várias contas
- Recomendações da AWS: Arquitetura de referência de segurança da AWS (AWS SRA)
- Recomendações da AWS: Guia de log e monitoramento para proprietários de aplicações

Exemplos relacionados:

- Agregar, pesquisar e visualizar dados de log de fontes distribuídas com o Amazon Athena e o QuickSight
- Como visualizar descobertas do Amazon Security Lake com o QuickSight
- Gerar insights baseados em IA para o Amazon Security Lake usando o Amazon SageMaker AI Studio e o Amazon Bedrock
- Identificar anomalias de segurança cibernética em dados do Amazon Security Lake usando o Amazon SageMaker AI
- Ingerir, transformar e entregar eventos publicados pelo Amazon Security Lake para o Amazon OpenSearch Service
- Simplify AWS CloudTrail log analysis with natural language query generation in CloudTrail Lake

Ferramentas relacionadas:

- Amazon Security Lake
- Integrações de parceiros do Amazon Security Lake
- Open Cybersecurity Schema Framework (OCSF)
- Amazon Athena

- QuickSight
- Amazon Bedrock

SEC04-BP03 Correlacionar e enriquecer alertas de segurança

Atividades inesperadas podem gerar vários alertas de segurança de diferentes fontes, exigindo mais correlação e enriquecimento para entender o contexto completo. Implemente a correlação automatizada e o enriquecimento de alertas de segurança para ajudar a obter identificações e respostas mais precisas a incidentes.

Resultado desejado: à medida que a atividade gera alertas diferentes em seus ambientes e workloads, mecanismos automatizados correlacionam dados e enriquecem esses dados com informações adicionais. Esse pré-processamento apresenta uma compreensão mais detalhada do evento, o que ajuda os investigadores a determinar a importância do evento e se ele constitui um incidente que requer uma resposta formal. Esse processo reduz a carga sobre suas equipes de monitoramento e investigação.

Práticas comuns que devem ser evitadas:

- Diferentes grupos de pessoas investigam descobertas e alertas gerados por sistemas diferentes, a menos que seja exigido de outra forma pelos requisitos de separação de deveres.
- Sua organização canaliza todos os dados de detecção e alerta de segurança para locais padrão, mas exige que os investigadores realizem a correlação e o enriquecimento manualmente.
- Você depende exclusivamente da inteligência dos sistemas de detecção de ameaças para relatar descobertas e determinar a gravidade.

Benefícios de implementar esta prática recomendada: a correlação e o enriquecimento automatizados de alertas ajudam a reduzir a carga cognitiva geral e a preparação manual de dados exigidas de seus investigadores. Essa prática pode reduzir o tempo necessário para determinar se o evento representa um incidente e iniciar uma resposta formal. O contexto adicional também ajuda a avaliar com precisão a verdadeira gravidade de um evento, pois ela pode ser maior ou menor do que o sugerido por qualquer alerta.

Nível de risco exposto se esta prática recomendada não for estabelecida: Baixo

Orientação para implementação

Os alertas de segurança podem vir de várias fontes diferentes na AWS, incluindo:

- Serviços como Amazon GuardDuty, AWS Security Hub, Amazon Macie, Amazon Inspector, AWS Config, AWS Identity and Access Management Access Analyzer e Analisador de Acesso à Rede
- Alertas de análises automatizadas de logs de serviços, infraestrutura e aplicações da AWS, como do Security Analytics for Amazon OpenSearch Service.
- Alarmes em resposta a alterações em sua atividade de faturamento de fontes como Amazon CloudWatch, Amazon EventBridge ou AWS Budgets.
- Fontes de terceiros, como feeds de inteligência de ameaças e soluções de parceiros de segurança da AWS Partner Network
- Contato via AWS Trust & Safety ou por outras fontes, como clientes ou funcionários internos.

Em sua forma mais fundamental, os alertas contêm informações sobre quem (a entidade principal ou identidade) está fazendo o quê (a ação tomada) a quê (os recursos afetados). Em cada uma dessas fontes, identifique se há maneiras de criar associações nos identificadores referentes a essas identidades, ações e recursos como base para realizar a correlação. Isso poderia ser integrar fontes de alerta a uma ferramenta de gerenciamento de eventos e informações de segurança (SIEM) para realizar a correlação automatizada para você, criar seus próprios pipelines e processamento de dados ou uma combinação de ambos.

Um exemplo de serviço que pode realizar a correlação para você é o Amazon Detective. O Detective realiza a ingestão contínua de alertas de várias fontes da AWS e de terceiros e usa diferentes formas de inteligência com o objetivo de montar um grafo visual das respectivas relações para auxiliar nas investigações.

Embora a gravidade inicial de um alerta ajude na priorização, o contexto em que o alerta aconteceu determina sua verdadeira gravidade. Como exemplo, o Amazon GuardDuty pode alertar que uma instância do Amazon EC2 em sua workload está consultando um nome de domínio inesperado. O GuardDuty pode atribuir por conta própria uma baixa criticidade a esse alerta. Entretanto, a correlação automatizada com outras atividades em torno do momento do alerta pode revelar que várias centenas de instâncias do EC2 foram implantadas pela mesma identidade, o que aumenta os custos operacionais gerais. Nesse caso, esse contexto de evento correlacionado garantiria um novo alerta de segurança e a gravidade pode ser definida como alta, o que agilizaria ações futuras.

Etapas de implementação

1. Identifique fontes de informações sobre alertas de segurança. Entenda como os alertas desses sistemas representam identidade, ação e recursos para determinar onde a correlação é possível.

2. Estabeleça um mecanismo para capturar alertas de diferentes fontes. Considere serviços como Security Hub, EventBridge e CloudWatch para essa finalidade.
3. Identifique fontes para correlação e enriquecimento de dados. Exemplos de fontes incluem AWS CloudTrail, logs de fluxo de VPC, logs do Route 53 Resolver e logs de infraestrutura e aplicações. Qualquer um ou todos esses logs podem ser consumidos por meio de uma única integração com o Amazon Security Lake.
4. Integre os alertas às fontes de correlação e enriquecimento de dados para criar contextos de eventos de segurança mais detalhados e determinar a gravidade.
   a. O Amazon Detective, ferramentas de SIEM ou outras soluções de terceiros podem realizar determinado nível de ingestão, correlação e enriquecimento automaticamente.
   b. Você também pode usar serviços da AWS para criar seus próprios alertas. Por exemplo, você pode invocar uma função do AWS Lambda para executar uma consulta do Amazon Athena no AWS CloudTrail ou no Amazon Security Lake e publicar os resultados no EventBridge.

Recursos

Práticas recomendadas relacionadas:

- SEC10-BP03 Preparar recursos forenses
- OPS08-BP04 Criar alertas acionáveis
- REL06-BP03 Enviar notificações (processamento e emissão de alarmes em tempo real)

Documentos relacionados:

- Guia de resposta a incidentes de segurança da AWS

Exemplos relacionados:

- Como enriquecer as descobertas do AWS Security Hub com metadados da conta

Ferramentas relacionadas:

- Amazon Detective
- Amazon EventBridge
- AWS Lambda

- Amazon Athena

SEC04-BP04 Iniciar a correção de recursos fora de conformidade

Seus controles de detecção podem emitir alertas sobre recursos que não estão em conformidade com seus requisitos de configuração. É possível iniciar correções definidas de maneira programática, tanto manual quanto automaticamente, para corrigir esses recursos e ajudar a minimizar possíveis impactos. Definir correções programaticamente permite tomar medidas rápidas e consistentes.

Embora a automação possa aprimorar as operações de segurança, você deve implementá-la e gerenciá-la com cuidado. Estabeleça mecanismos apropriados de supervisão e controle para verificar se as respostas automatizadas são eficazes e precisas e estão alinhadas com as políticas organizacionais e a propensão ao risco.

Resultado desejado: você define os padrões de configuração de recursos junto com as etapas de correção quando os recursos são detectados como fora de conformidade. Sempre que possível, você definiu as correções programaticamente para que elas possam ser iniciadas de modo manual ou por meio de automação. Existem sistemas de detecção para identificar recursos fora de conformidade e publicar alertas em ferramentas centralizadas que são monitoradas por suas equipes de segurança. Essas ferramentas comportam a execução das correções programáticas, tanto manual quanto automaticamente. As correções automáticas têm mecanismos apropriados de supervisão e controle para governar o respectivo uso.

Práticas comuns que devem ser evitadas:

- Você implementa a automação, mas não consegue testar e validar minuciosamente as ações de correção. Isso pode resultar em consequências indesejadas, como interrupção de operações comerciais legítimas ou instabilidade no sistema.
- Você melhora os tempos de resposta e os procedimentos por meio da automação, mas sem monitoramento e mecanismos adequados que permitam a intervenção e avaliação humanas quando necessário.
- Você depende exclusivamente de correções, em vez de tê-las como parte de um programa mais amplo de resposta e recuperação de incidentes.

Benefícios de implementar esta prática recomendada: as correções automáticas podem responder a configurações incorretas mais rapidamente do que os processos manuais, o que ajuda a minimizar possíveis impactos nos negócios e reduzir a janela de oportunidade para usos não

intencionais. Quando você define as remediações de forma programática, elas são aplicadas de forma consistente, o que reduz o risco de erro humano. A automação também pode lidar com um volume maior de alertas de forma simultânea, o que é particularmente importante em ambientes que operam em grande escala.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

Conforme descrito em SEC01-BP03 Identificar e validar objetivos de controle, serviços como AWS Config e AWS Security Hub podem ajudar a monitorar a configuração de recursos nas contas para atender às suas necessidades. Quando recursos não compatíveis são detectados, serviços como o AWS Security Hub podem ajudar no roteamento adequado de alertas e na remediação. Essas soluções fornecem um local central para os investigadores de segurança monitorarem os problemas e adotarem medidas corretivas.

Embora algumas situações em que há recursos fora de conformidade sejam únicas e exijam avaliação humana para ser corrigidas, outras têm uma resposta padrão que você pode definir programaticamente. Por exemplo, uma resposta padrão a um grupo de segurança da VPC configurado incorretamente pode ser remover as regras não permitidas e notificar o responsável. As respostas podem ser definidas em funções do AWS Lambda, documentos do AWS Systems Manager Automation ou por meio de outros ambientes de código de sua preferência. O ambiente deve estar apto a se autenticar na AWS usando um perfil do IAM com as permissões mínimas necessárias para tomar medidas corretivas.

Depois de definir a remediação desejada, você poderá determinar seus meios preferidos para iniciá-la. O AWS Config pode iniciar remediações para você. Se você estiver usando o Security Hub, poderá fazer isso por meio de ações personalizadas que publicam as informações de descoberta no Amazon EventBridge. Uma regra do EventBridge pode então iniciar a correção. Você pode configurar a execução automática ou manual das remediações pelo Security Hub.

Para remediação programática, recomendamos que manter logs e auditorias abrangentes das ações tomadas, bem como de seus resultados. Revise e analise esses logs para avaliar a eficácia dos processos automatizados e identificar áreas de melhoria. Capture registros no Amazon CloudWatch Logs e resultados de correções como notas de descoberta no Security Hub.

Como ponto de partida, considere a Resposta de Segurança Automatizada na AWS, que oferece correções criadas previamente para resolver configurações incorretas de segurança comuns.

Etapas de implementação

1. Analise e priorize os alertas.
    a. Consolide alertas de segurança de vários serviços da AWS no Security Hub para ter visibilidade, priorização e correção centralizadas.
2. Desenvolva correções.
    a. Use serviços como o Systems Manager e o AWS Lambda para executar correções programáticas.
3. Configure como as correções são iniciadas.
    a. Usando o Systems Manager, defina ações personalizadas para publicar descobertas no EventBridge. Configure essas ações para serem iniciadas manual ou automaticamente.
    b. Também é possível usar o Amazon Simple Notification Service (SNS) para enviar notificações e alertas às partes interessadas relevantes (como equipes de segurança ou equipes de resposta a incidentes) para intervenção manual ou escalação, se necessário.
4. Revise e analise os logs de correção em prol da eficácia e melhoria.
    a. Envie a saída do log ao CloudWatch Logs. Capture resultados como notas de descoberta no Security Hub.

Recursos

Práticas recomendadas relacionadas:

- SEC06-BP03 Reduzir o gerenciamento manual e o acesso interativo

Documentos relacionados:

- Guia de resposta a incidentes de segurança da AWS: Detecção

Exemplos relacionados:

- Resposta de segurança automatizada na AWS
- Monitorar pares de chaves de instância do EC2 com o AWS Config
- Crie regras personalizadas do AWS Config usando políticas do AWS CloudFormation Guard
- Corrija automaticamente instâncias e clusters de banco de dados não criptografados do Amazon RDS

Ferramentas relacionadas:

- AWS Systems Manager Automation
- Resposta de segurança automatizada na AWS

Proteção da infraestrutura

A proteção da infraestrutura abrange metodologias de controle, como defesa em profundidade, que são necessárias para atender às práticas recomendadas e às obrigações organizacionais ou regulatórias. O uso dessas metodologias é fundamental para o êxito de operações contínuas na nuvem.

A proteção da infraestrutura é elemento essencial de um programa de segurança da informação. Ela garante que os sistemas e os serviços de sua workload sejam protegidos contra acesso não intencional e não autorizado e possíveis vulnerabilidades. Por exemplo, você definirá limites de confiança (por exemplo, limites de rede e conta), configuração e manutenção da segurança do sistema (por exemplo, fortalecimento, minimização e aplicação de patches), autenticação e autorizações do sistema operacional (por exemplo, usuários, chaves e níveis de acesso) e outros pontos de aplicação de políticas apropriados (por exemplo, firewalls de aplicações Web e/ou API gateways).

Regiões, zonas de disponibilidade, zonas locais da AWS e AWS Outposts

Certifique-se de estar familiarizado com os conceitos de regiões, zonas de disponibilidade, zonas locais da AWS e AWS Outposts, todos eles componentes da infraestrutura global segura da AWS.

A AWS tem o conceito de região, que é um local físico em alguma parte do mundo onde agrupamos data centers. Cada grupo de data centers lógicos é chamado de zona de disponibilidade (AZ). Cada região da AWS consiste em várias AZs isoladas e fisicamente separadas em uma área geográfica. Se você tiver requisitos de residência de dados, poderá escolher a região da AWS próxima ao local desejado. Você mantém controle total e proprietário sobre a região em que seus dados estão localizados fisicamente, facilitando a conformidade com requisitos regionais de conformidade e a residência de dados. Cada AZ conta com fornecimento de energia, refrigeração e segurança física independentes. Se uma aplicação for particionada entre AZs, você terá níveis melhores de isolamento e proteção contra problemas como falta de energia elétrica, raios, tornados, terremotos e muito mais. As AZs estão separadas fisicamente por uma distância significativa, a muitos quilômetros de qualquer outra AZ, embora todas estejam a no máximo 100 km (60 milhas) de distância umas das outras. Todas as AZs em uma região AWS são interconectadas com rede de alta largura de banda e baixa latência, por fibra metropolitana dedicada totalmente redundante, fornecendo uma rede de alto throughput e baixa latência entre as zonas. Todo o tráfego entre AZs é criptografado. Os clientes da AWS focados na alta disponibilidade podem projetar suas aplicações para serem executadas em várias AZs a fim de obter uma tolerância ainda maior a falhas. AWS Com as regiões, é possível atingir os mais altos níveis de segurança, conformidade e proteção de dados.

As zonas locais da AWS coloca os recursos de computação, armazenamento, banco de dados e outros serviços da AWS selecionados mais perto dos usuários finais. Com as zonas locais da AWS, é possível executar facilmente aplicações altamente exigentes que exigem latências de um dígito em milissegundos para seus usuários finais, como criação de conteúdo de mídia e entretenimento, jogos em tempo real, simulações de reservatórios, automação de design eletrônico e machine learning. Cada localização de zona local da AWS é uma extensão de uma região da AWS na qual você pode executar suas aplicações sensíveis à latência usando serviços da AWS como Amazon EC2, Amazon VPC, Amazon EBS, Amazon File Storage e Elastic Load Balancing em um local fisicamente próximo dos usuários finais. AWS As zonas locais fornecem uma conexão segura e de alta largura de banda entre workloads locais e aquelas em execução na região da AWS, permitindo que você se conecte perfeitamente a toda a gama de serviços na região por meio das mesmas APIs e conjuntos de ferramentas.

Os AWS Outposts trazem serviços, infraestrutura e modelos operacionais nativos da AWS para praticamente qualquer data center, espaço de compartilhamento ou instalação on-premises. Você pode usar as mesmas APIs, ferramentas e infraestrutura da AWS nas instalações on-premises e na Nuvem AWS para oferecer uma experiência híbrida verdadeiramente consistente. AWS O Outposts foi projetado para ambientes conectados e pode ser usado para suportar workloads que devem permanecer no local devido à baixa latência ou às necessidades locais de processamento de dados.

A AWS tem várias abordagens para a proteção da infraestrutura. As seções a seguir descrevem como usar essas abordagens.

Tópicos

Proteção de redes

Os usuários, tanto em sua força de trabalho quanto em seus clientes, podem estar localizados em qualquer lugar. Você precisa se afastar dos modelos tradicionais de confiar em qualquer pessoa e em qualquer coisa que tenha acesso à sua rede. Ao seguir o princípio de aplicar segurança em todas as camadas, você emprega uma abordagem Zero Trust. A segurança Zero Trust é um modelo em que os componentes ou microsserviços da aplicação são considerados distintos uns dos outros e nenhum componente ou microsserviço confia em nenhum outro.

O planejamento e o gerenciamento minuciosos do design da rede são a base do isolamento e dos limites para os recursos em sua workload. Como muitos recursos da workload operam em uma VPC e herdam as propriedades de segurança, é essencial que o projeto tenha o suporte de mecanismos de inspeção e proteção respaldados por automação. Da mesma forma, para workloads que operam fora de uma VPC, usando serviços puramente de borda e/ou sem servidor, as práticas recomendadas se aplicam em uma abordagem mais simplificada. Consulte a Lente de aplicações sem servidor do AWS Well-Architected para obter orientações específicas sobre segurança sem servidor.

Práticas recomendadas

- SEC05-BP01 Criar camadas de rede
- SEC05-BP02 Controlar o fluxo de tráfego dentro das camadas de rede
- SEC05-BP03 Implementar proteção baseada em inspeção
- SEC05-BP04 Automatizar a proteção da rede

SEC05-BP01 Criar camadas de rede

Segmente a topologia de rede em diferentes camadas com base nos agrupamentos lógicos dos componentes da workload e de acordo com a confidencialidade dos dados e os requisitos de acesso. Diferencie os componentes que exigem acesso de entrada pela internet, como endpoints públicos da web e aqueles que precisam apenas de acesso interno, como bancos de dados.

Resultado desejado: as camadas de sua rede fazem parte de uma abordagem integral de defesa aprofundada à segurança que complementa a estratégia de autenticação e autorização de identidade de suas workloads. As camadas estão posicionadas de acordo com a confidencialidade dos dados e os requisitos de acesso, com mecanismos apropriados de fluxo e controle de tráfego.

Práticas comuns que devem ser evitadas:

- Você cria todos os recursos em uma única VPC ou sub-rede.
- Você constrói as camadas de rede sem considerar os requisitos de confidencialidade dos dados, o comportamento dos componentes ou a funcionalidade.
- Você usa VPCs e sub-redes como padrão para todas as considerações de camada de rede e não considera como os serviços gerenciados da AWS influenciam sua topologia.

Benefícios de implementar esta prática recomendada: estabelecer camadas de rede é a primeira etapa para restringir caminhos desnecessários na rede, especialmente aqueles que levam a sistemas e dados críticos. Desse modo, o acesso de agentes não autorizados à sua rede e a outros recursos dentro dela torna-se mais difícil. Camadas de rede discretas reduzem de forma favorável o escopo da análise para sistemas de inspeção, por exemplo, para detecção de intrusões ou prevenção de malware. Isso reduz a possibilidade de falsos positivos e a sobrecarga de processamento desnecessária.

Nível de risco exposto se esta prática recomendada não for estabelecida: Alto

Orientação para implementação

Quando se projeta uma arquitetura de workload, é comum separar os componentes em diferentes camadas com base nas respectivas responsabilidades. Por exemplo, uma aplicação web pode ter uma camada de apresentação, uma camada de aplicação e uma camada de dados. É possível adotar uma abordagem semelhante ao projetar sua topologia de rede. Os controles de rede subjacentes podem ajudar a aplicar os requisitos de acesso aos dados da workload. Por exemplo, em uma arquitetura de aplicação web de três camadas, você pode armazenar seus arquivos de camada de apresentação estática no Amazon S3 e servi-los desde uma rede de entrega de conteúdo (CDN), como o Amazon CloudFront. A camada de aplicação pode ter endpoints públicos que um Application Load Balancer (ALB) serve em uma sub-rede pública da Amazon VPC (semelhante a uma zona desmilitarizada, ou DMZ), com serviços de backend implantados em sub-redes privadas. A camada de dados, que hospeda recursos como bancos de dados e sistemas de arquivos compartilhados, pode residir em diferentes sub-redes privadas dos recursos da camada de aplicação. Em cada um desses limites de camada (CDN, sub-rede pública, sub-rede privada), é possível implantar controles que permitam somente a entrada do tráfego autorizado.

De modo semelhante à modelagem de camadas de rede com base na finalidade funcional dos componentes da workload, considere também a confidencialidade dos dados que estão sendo processados. Usando o exemplo de aplicação web, embora todos os serviços de workload possam residir na camada de aplicação, serviços diferentes podem processar dados com diferentes níveis de confidencialidade. Nesse caso, dividir a camada de aplicação usando várias sub-redes privadas, diferentes VPCs na mesma Conta da AWS ou até mesmo diferentes VPCs em diferentes Contas da AWS para cada nível de confidencialidade de dados pode ser apropriado de acordo com seus requisitos de controle.

Uma consideração adicional sobre as camadas de rede é a consistência do comportamento dos componentes da workload. Continuando com o exemplo, na camada de aplicação, você pode ter serviços que aceitem entradas de usuários finais ou integrações de sistemas externos que são

inerentemente mais arriscadas do que as entradas de outros serviços. Os exemplos incluem uploads de arquivos, scripts de código para execução, verificação de e-mails e assim por diante. Colocar esses serviços em uma camada de rede própria ajuda a criar um limite de isolamento mais forte em torno deles e pode impedir que o comportamento exclusivo de cada um deles crie alertas falsos positivos nos sistemas de inspeção.

Como parte do seu design, considere como o uso de serviços gerenciados da AWS influencia sua topologia de rede. Explore como serviços como o Amazon VPC Lattice podem ajudar a facilitar a interoperabilidade dos componentes da workload nas camadas da rede. Ao usar o AWS Lambda, implante nas sub-redes da VPC, a menos que haja motivos específicos para não fazê-lo. Determine onde a VPC termina e o AWS PrivateLink pode simplificar a adesão às políticas de segurança que limitam o acesso aos gateways da Internet.

Etapas de implementação

1. Revise a arquitetura da sua workload. Agrupe logicamente os componentes e serviços com base nas funções às quais eles atendem, na confidencialidade dos dados que estão sendo processados e no respectivo comportamento.
2. Com relação a componentes que respondem a solicitações da internet, considere usar balanceadores de carga ou outros proxies para fornecer endpoints públicos. Explore mudanças nos controles de segurança usando serviços gerenciados, como CloudFront, Amazon API Gateway, Elastic Load Balancing e AWS Amplify para hospedar endpoints públicos.
3. Para componentes executados em ambientes computacionais, como instâncias do Amazon EC2, contêineres do AWS Fargate ou funções do Lambda, implante-os em sub-redes privadas com base em seus grupos desde a primeira etapa.
4. Para serviços da AWS totalmente gerenciados, como Amazon DynamoDB, Amazon Kinesis ou Amazon SQS, considere usar endpoints da VPC como padrão para acesso por endereços IP privados.

Recursos

Práticas recomendadas relacionadas:

- REL02 Planejar a topologia da rede
- PERF04-BP01 Compreender como a rede afeta a performance

Vídeos relacionados:

- AWS re:Invent 2023: Fundamentos de rede na AWS

Exemplos relacionados:

- Exemplos de VPC
- Acessar aplicações de contêiner de forma privada no Amazon ECS usando o AWS Fargate, o AWS PrivateLink e um Network Load Balancer
- Servir conteúdo estático em um bucket do Amazon S3 por meio de uma VPC usando o Amazon CloudFront

SEC05-BP02 Controlar o fluxo de tráfego dentro das camadas de rede

Dentro das camadas da sua rede, use uma segmentação adicional para restringir o tráfego somente aos fluxos necessários para cada workload. Primeiro, concentre-se em controlar o tráfego entre a Internet ou outros sistemas externos para uma workload e seu ambiente (tráfego norte-sul). Depois, observe os fluxos entre diferentes componentes e sistemas (tráfego leste-oeste).

Resultado desejado: você permite somente os fluxos de rede necessários para que os componentes de suas workloads se comuniquem uns com os outros e com seus clientes e com quaisquer outros serviços dos quais eles dependam. Seu design considera questões como comparação entre entradas e saídas públicas e privadas, classificação de dados, regulamentações regionais e requisitos de protocolo. Sempre que possível, você favorece fluxos ponto a ponto em vez de emparelhamento de rede como parte de um princípio de design de privilégio mínimo.

Práticas comuns que devem ser evitadas:

- Você adota uma abordagem de segurança de rede baseada em perímetro e controla apenas o fluxo de tráfego no limite das camadas de sua rede.
- Você presume que todo o tráfego dentro de uma camada de rede está autenticado e autorizado.
- Você aplica controles para o tráfego de entrada ou de saída, mas não para ambos.
- Você depende exclusivamente dos componentes da workload e dos controles de rede para autenticar e autorizar o tráfego.

Benefícios de implementar esta prática recomendada: essa prática ajuda a reduzir o risco de movimentação não autorizada em sua rede e adiciona uma camada extra de autorização às suas

workloads. Ao realizar o controle do fluxo de tráfego, você pode restringir o escopo do impacto de um incidente de segurança e acelerar a detecção e a resposta.

Nível de risco exposto se esta prática recomendada não for estabelecida: Alto

Orientação para implementação

Embora as camadas de rede ajudem a estabelecer os limites em torno de componentes da workload que atendem a funções, níveis de confidencialidade de dados e comportamentos semelhantes, você pode criar um nível de controle de tráfego bem mais refinado usando técnicas para segmentar ainda mais os componentes dentro dessas camadas, seguindo o princípio de privilégio mínimo. Na AWS, as camadas de rede são definidas principalmente via sub-redes de acordo com faixas de endereços IP em uma Amazon VPC. As camadas também podem ser definidas usando diferentes VPCs, como para agrupar ambientes de microsserviços por domínio de negócios. Ao usar várias VPCs, medie o roteamento usando um AWS Transit Gateway. Embora isso forneça controle de tráfego em um nível de camada 4 (endereços IP e intervalos de portas) usando grupos de segurança e tabelas de rotas, você pode obter mais controle usando serviços adicionais como AWS PrivateLink, Firewall de DNS do Amazon Route 53 Resolver, AWS Network Firewall e AWS WAF.

Entenda e faça um inventário do fluxo de dados e dos requisitos de comunicação de workloads em termos de partes que iniciam a conexão, portas, protocolos e camadas de rede. Avalie os protocolos disponíveis para estabelecer conexões e transmitir dados para selecionar aqueles que atendam aos seus requisitos de proteção (por exemplo, HTTPS em vez de HTTP). Capture esses requisitos nos limites de suas redes e dentro de cada camada. Depois que esses requisitos forem identificados, explore as opções para permitir que apenas o tráfego necessário flua em cada ponto de conexão. Um bom ponto de partida é usar grupos de segurança em sua VPC, pois eles podem ser anexados a recursos que usam uma interface de rede elástica (ENI), como instâncias do Amazon EC2, tarefas do Amazon ECS, pods do Amazon EKS ou bancos de dados do Amazon RDS. Ao contrário de um firewall de camada 4, um grupo de segurança pode ter uma regra que permite o tráfego de outro grupo de segurança por meio do respectivo identificador, minimizando as atualizações à medida que os recursos dentro do grupo mudam ao longo do tempo. Você também pode filtrar o tráfego por meio de regras de entrada e saída usando grupos de segurança.

Quando o tráfego se move entre as VPCs, é comum usar o emparelhamento de VPCs para roteamento simples ou o AWS Transit Gateway para roteamento complexo. Com essas abordagens, você facilita os fluxos de tráfego entre o intervalo de endereços IP das redes de origem e de destino. No entanto, se sua workload exigir apenas fluxos de tráfego entre componentes específicos em VPCs diferentes, considere usar uma conexão ponto a ponto usando o AWS PrivateLink. Para isso, identifique qual serviço deve atuar como produtor e qual deve atuar como consumidor. Implante um

balanceador de carga compatível para o produtor, ative o PrivateLink adequadamente e, em seguida, aceite uma solicitação de conexão do consumidor. Em seguida, o serviço do produtor recebe um endereço IP privado da VPC do consumidor que o consumidor pode usar para fazer solicitações subsequentes. Essa abordagem reduz a necessidade de emparelhar as redes. Inclua os custos de processamento de dados e balanceamento de carga como parte da avaliação do PrivateLink.

Embora os grupos de segurança e o PrivateLink ajudem a controlar o fluxo entre os componentes de suas workloads, outra consideração importante é como controlar quais domínios DNS seus recursos podem acessar (se houver). Dependendo da configuração DHCP das suas VPCs, é possível considerar dois serviços da AWS diferentes para essa finalidade. A maioria dos clientes usa o serviço DNS padrão do Route 53 Resolver (também chamado de servidor Amazon DNS ou AmazonProvideDDNS) disponível para VPCs no endereço +2 de seu intervalo CIDR. Com essa abordagem, é possível criar regras de firewall de DNS e associá-las à VPC para determinar quais ações devem ser realizadas para as listas de domínios que você fornece.

Se você não estiver usando o Route 53 Resolver, ou se quiser complementar o Resolver com recursos mais detalhados de inspeção e controle de fluxo, além da filtragem de domínio, considere implantar um AWS Network Firewall. Esse serviço inspeciona pacotes individuais usando regras sem estado ou com estado para determinar se deve negar ou permitir o tráfego. Você pode adotar uma abordagem semelhante para filtrar o tráfego de entrada da web para seus endpoints públicos usando o AWS WAF. Para obter mais orientações sobre esses serviços, consulte SEC05-BP03 Implementar proteção baseada em inspeção.

Etapas de implementação

1. Identifique os fluxos de dados necessários entre os componentes das workloads.
2. Aplique vários controles com uma abordagem de defesa profunda para tráfego de entrada e saída, incluindo o uso de grupos de segurança e tabelas de rotas.
3. Use firewalls para definir um controle refinado sobre o tráfego de rede que entra, sai e atravessa suas VPCs, como o Firewall de DNS do Route 53 Resolver, o AWS Network Firewall e o AWS WAF. Considere usar o AWS Firewall Manager para configurar e gerenciar centralmente suas regras de firewall em toda a organização.

Recursos

Práticas recomendadas relacionadas:

- REL03-BP01 Escolher como segmentar a workload

- SEC09-BP02 Impor a criptografia em trânsito

Documentos relacionados:

- Práticas recomendadas de segurança para a VPC
- Dicas de otimização de rede da AWS
- Orientação para segurança de rede na AWS
- Proteger o tráfego de rede de saída da sua VPC na Nuvem AWS

Ferramentas relacionadas:

- AWS Firewall Manager

Vídeos relacionados:

- Arquiteturas de referência do AWS Transit Gateway para muitas VPCs
- Aceleração e proteção de aplicações com Amazon CloudFront, AWS WAF e AWS Shield
- AWS re:Inforce 2023: Firewalls e onde colocá-los

SEC05-BP03 Implementar proteção baseada em inspeção

Configure pontos de inspeção de tráfego entre as camadas de rede para garantir que os dados em trânsito correspondam aos padrões e categorias esperados. Analise padrões, metadados e fluxos de tráfego para ajudar a identificar, detectar e responder a eventos com maior eficiência.

Resultado desejado: o tráfego que passa entre suas camadas de rede é inspecionado e autorizado. As decisões de permissão e negação baseiam-se em regras explícitas, inteligência contra ameaças e desvios dos comportamentos de referência. As proteções tornam-se mais rígidas à medida que o tráfego aproxima-se dos dados confidenciais.

Práticas comuns que devem ser evitadas:

- Confiar somente em regras de firewall baseadas em portas e protocolos. Não aproveitar os sistemas inteligentes.
- Criar regras de firewall com base em padrões específicos de ameaças atuais que estão sujeitos a alterações.

- Inspecionar somente o tráfego que transita de sub-redes privadas para públicas ou de sub-redes públicas para a internet.
- Não ter uma visão de referência do tráfego da rede para comparar com anomalias de comportamento.

Benefícios de implementar esta prática recomendada: os sistemas de inspeção permitem que você crie regras inteligentes, como permitir ou negar tráfego somente quando houver determinadas condições nos dados de tráfego. Beneficie-se de conjuntos de regras gerenciados pela AWS e por parceiros, com base na inteligência contra ameaças mais recente, à medida que o cenário de ameaças muda ao longo do tempo. Isso reduz as despesas indiretas de manter regras e pesquisar indicadores de comprometimento, reduzindo o potencial de falsos positivos.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

Mantenha um controle refinado sobre seu tráfego de rede com e sem estado usando o AWS Network Firewall ou outros firewalls e sistemas de prevenção de intrusões (IPS) no AWS Marketplace você pode implantar por trás de um Gateway Load Balancer (GWLB). O AWS Network Firewall oferece suporte a especificações IPS de código aberto compatíveis com Suricata para ajudar a proteger sua workload.

Tanto o AWS Network Firewall quanto as soluções de fornecedor que usam um GWLB comportam diferentes modelos de implantação de inspeção em linha. Por exemplo, você pode realizar a inspeção por VPC, centralizar em uma VPC de inspeção ou implantar em um modelo híbrido em que o tráfego leste-oeste flui por meio de uma VPC de inspeção e a entrada da internet é inspecionada por VPC. Outra consideração é se a solução comporta o desempacotamento do Transport Layer Security (TLS), permitindo a inspeção detalhada de pacotes para fluxos de tráfego iniciados em qualquer direção. Para obter mais informações e detalhes sobre essas configurações, consulte o Guia de práticas recomendadas do AWS Network Firewall.

Se você usa soluções que realizam inspeções fora de banda, como análise pcap de dados de pacotes de interfaces de rede operando em modo promíscuo, é possível configurar o espelhamento de tráfego de VPC. O tráfego espelhado é computado na largura de banda disponível de suas interfaces e está sujeito às mesmas cobranças de transferência de dados que o tráfego não espelhado. É possível ver se as versões virtuais desses appliances estão disponíveis no AWS Marketplace, o que pode oferecer suporte à implantação em linha por trás de um GWLB.

Para componentes que operam por meio de protocolos baseados em HTTP, proteja sua aplicação contra ameaças comuns com um firewall de aplicações Web (WAF). O AWS WAF é um firewall de aplicações Web que permite monitorar e bloquear solicitações HTTP(S) que correspondem a suas regras configuráveis antes de enviar para o Amazon API Gateway, o Amazon CloudFront, o AWS AppSync ou um Application Load Balancer. Considere a inspeção detalhada de pacotes ao avaliar a implantação do firewall de aplicações Web, pois alguns exigem que você encerre o TLS antes da inspeção de tráfego. Para começar a usar o AWS WAF, é possível usar AWS Managed Rules em combinação com as suas próprias regras ou usar as integrações de parceiros existentes.

Você pode gerenciar centralmente o AWS WAF, o AWS Shield Advanced, o AWS Network Firewall e os grupos de segurança da Amazon VPC em toda a sua organização da AWS com o AWS Firewall Manager.

Etapas de implementação

1. Determine se você pode definir um escopo amplo das regras de inspeção, como por meio de uma VPC de inspeção, ou se precisa de uma abordagem mais detalhada por VPC.
2. Para soluções de inspeção em linha:
    a. Se estiver usando o AWS Network Firewall, crie regras, políticas de firewall e o próprio firewall. Após a configuração, você poderá rotear o tráfego para o endpoint do firewall para permitir a inspeção.
    b. Se estiver usando um appliance de terceiros com um Gateway Load Balancer (GWLB), implante e configure seu appliance em uma ou mais zonas de disponibilidade. Em seguida, crie o GWLB, o serviço de endpoint e o endpoint e configure o roteamento para o tráfego.
3. Para soluções de inspeção fora de banda:
    1. Ative o espelhamento de tráfego da VPC em interfaces nas quais o tráfego de entrada e saída deve ser espelhado. É possível usar regras do Amazon EventBridge para invocar uma função do AWS Lambda que ative o espelhamento de tráfego em interfaces quando são criados recursos. Aponte as sessões de espelhamento de tráfego para o Network Load Balancer na frente do appliance que processa o tráfego.
4. Para soluções de tráfego da Web de entrada:
    a. Para configurar o AWS WAF, primeiro configure uma lista de controle de acesso à web (ACL da web). A ACL da web é um conjunto de regras com uma ação padrão processada em série (permitir ou negar) que define como o WAF lida com o tráfego. Você pode criar seus próprios grupos e regras ou usar grupos de regras gerenciadas da AWS em sua ACL da Web.

b. Assim que a ACL da Web for configurada, ela poderá ser associada a um recurso da AWS (como um Application Load Balancer, uma API REST do API Gateway ou uma distribuição do CloudFront) para começar a proteger o tráfego da Web.

Recursos

Documentos relacionados:

- O que é espelhamento de tráfego?
- Implementar a inspeção de tráfego em linha usando appliances de segurança de terceiros
- Exemplos de arquiteturas do AWS Network Firewall com roteamento
- Arquitetura de inspeção centralizada com o AWS Gateway Balancer e o AWS Transit Gateway

Exemplos relacionados:

- Práticas recomendadas para implantar o balanceador de carga do gateway
- Configuração de inspeção TLS para tráfego de saída criptografado e AWS Network Firewall

Ferramentas relacionadas:

- AWS Marketplace IDS/IPS

SEC05-BP04 Automatizar a proteção da rede

Automatize a implantação de suas proteções de rede usando práticas de DevOps, como infraestrutura como código (IaC) e pipelines de CI/CD. Essas práticas podem ajudar você a monitorar alterações nas proteções da rede por meio de um sistema de controle de versão, reduzir o tempo necessário para implantar alterações e detectar se as proteções de rede se desviam da configuração desejada.

Resultado desejado: você define as proteções de rede com modelos e as compromete em um sistema de controle de versão. Quando novas alterações são feitas, os pipelines automatizados são iniciados para orquestrar os respectivos testes e a implantação. Verificações de políticas e outros testes estáticos estão em vigor para validar as alterações antes da implantação. Você implanta as alterações em um ambiente de preparação para validar se os controles estão operando conforme

o esperado. A implantação nos ambientes de produção também é executada automaticamente quando os controles são aprovados.

Práticas comuns que devem ser evitadas:

- Contar com equipes de workload individuais para que definam sua pilha de rede completa, proteções e automações. Não publicar os aspectos padrão da pilha de rede e das proteções de maneira centralizada para as equipes de workload consumirem.
- Contar com uma equipe de rede central para definir todos os aspectos da rede, proteções e automações. Não delegar aspectos específicos da workload da pilha de rede e das proteções à equipe da workload em questão.
- Conseguir o equilíbrio certo de centralização e delegação entre a equipe de rede e as equipes de workload, mas não aplicar padrões consistentes de teste e implantação aos modelos de IaC e pipelines de CI/CD. Não capturar as configurações necessárias em ferramentas que verificam a aderência aos modelos.

Benefícios de implementar esta prática recomendada: o uso de modelos para definir suas proteções de rede permite rastrear e comparar as alterações ao longo do tempo com um sistema de controle de versão. Usar automação para testar e implantar alterações gera padronização e previsibilidade, aumentando as chances de uma implantação bem-sucedida e reduzindo configurações manuais repetitivas.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

Vários controles de proteção de rede descritos em SEC05-BP02 Controlar fluxos de tráfego em suas camadas de rede e SEC05-BP03 Implementar a proteção baseada em inspeção são fornecidos com sistemas de regras gerenciados que podem ser atualizados automaticamente com base nas informações mais recentes sobre ameaças. Exemplos de proteção de seus endpoints da Web incluem regras gerenciadas pelo AWS WAF e mitigação de DDoS na camada de aplicações automática do AWS Shield Advanced. Use grupos de regras gerenciados pelo AWS Network Firewall para se manter atualizado com listas de domínios de baixa reputação e assinaturas de ameaças.

Além das regras gerenciadas, recomendamos usar práticas de DevOps para automatizar a implantação dos recursos de rede, das proteções e das regras que você especificar. Você pode capturar essas definições no AWS CloudFormation ou em outra ferramenta de infraestrutura como código (IaC) de sua escolha, confirmá-las em um sistema de controle de versão e implantá-las

usando pipelines de CI/CD. Use essa abordagem para obter os benefícios tradicionais de DevOps para gerenciar seus controles de rede, como lançamentos mais previsíveis, testes automatizados usando ferramentas como o AWS CloudFormation Guarde detecção de desvios entre o ambiente implantado e a configuração desejada.

Com base nas decisões tomadas como parte de SEC05-BP01 Criar camadas de rede, você pode adotar uma abordagem de gerenciamento central para criar VPCs dedicadas aos fluxos de entrada, saída e inspeção. Conforme descrito na Arquitetura de referência de segurança da AWS (AWS SRA), é possível definir essas VPCs em uma conta de infraestrutura de rede dedicada. Você pode usar técnicas semelhantes para definir centralmente as VPCs usadas pelas workloads em outras contas, os respectivos grupos de segurança, as implantações do AWS Network Firewall, as regras do Route 53 Resolver, as configurações do firewall de DNS e outros recursos de rede. Você pode compartilhar esses recursos com suas outras contas com o AWS Resource Access Manager. Com essa abordagem, é possível simplificar os testes automatizados e a implantação dos controles de rede na conta de rede, o que resulta em apenas um destino para gerenciar. É possível fazer isso em um modelo híbrido no qual você implanta e compartilha determinados controles centralmente e delega outros controles às equipes individuais de workload e respectivas contas.

Etapas de implementação

1. Estabeleça a propriedade para definir quais aspectos da rede e das proteções são definidos centralmente e quais as equipes de workload podem manter.
2. Crie ambientes para testar e implantar alterações na rede e nas respectivas proteções. Por exemplo, use uma conta de teste de rede e uma conta de produção de rede.
3. Determine como você armazenará e manterá os modelos em um sistema de controle de versão. Os modelos centrais podem ser armazenados em um repositório diferente dos repositórios de workload, enquanto os modelos de workload podem ser armazenados em repositórios específicos para essa workload.
4. Crie pipelines de CI/CD para testar e implantar modelos. Defina testes para verificar se há configurações incorretas e se os modelos estão de acordo com os padrões da sua empresa.

Recursos

Práticas recomendadas relacionadas:

- SEC01-BP06 Automatizar a implantação de controles de segurança padrão

Documentos relacionados:

- Arquitetura de referência de segurança da AWS: Conta de rede

Exemplos relacionados:

- Arquitetura de referência do pipeline de implantação da AWS
- NetDevSecOps para modernizar as implantações de rede da AWS
- Integrar testes de segurança do AWS CloudFormation com relatórios do AWS Security Hub e do AWS CodeBuild

Ferramentas relacionadas:

- AWS CloudFormation
- AWS CloudFormation Guard
- cfn_nag

Proteção da computação

Os recursos de computação incluem instâncias do EC2, contêineres, funções do AWS Lambda, serviços de banco de dados, dispositivos de IoT e muito mais. Cada um desses tipos de recursos computacionais exige abordagens diferentes para protegê-los. No entanto, eles compartilham estratégias comuns que devem ser levadas em conta: defesa em profundidade, gerenciamento de vulnerabilidades, redução na superfície de ataque, automação da configuração e operação e execução de ações à distância. Nesta seção, você encontrará orientações gerais para proteger seus recursos computacionais para os principais serviços. Para cada serviço da AWS usado, é importante verificar as recomendações de segurança específicas na documentação do serviço.

Práticas recomendadas

- SEC06-BP01 Realizar o gerenciamento de vulnerabilidades
- SEC06-BP02 Provisionar computação com base em imagens reforçadas
- SEC06-BP03 Reduzir o gerenciamento manual e o acesso interativo
- SEC06-BP04 Validar a integridade do software
- SEC06-BP05 Automatizar a proteção da computação

SEC06-BP01 Realizar o gerenciamento de vulnerabilidades

Verifique e corrija com frequência vulnerabilidades no código, nas dependências e na infraestrutura para se proteger contra novas ameaças.

Resultado desejado: você tem uma solução que verifica continuamente sua workload em busca de vulnerabilidades de software, possíveis defeitos e exposição não intencional da rede. Você estabeleceu processos e procedimentos para identificar, priorizar e corrigir essas vulnerabilidades com base nos critérios de avaliação de risco. Além disso, você implementou o gerenciamento automatizado de patches para suas instâncias computacionais. Seu programa de gerenciamento de vulnerabilidades é integrado ao seu ciclo de vida de desenvolvimento de software, com soluções para escanear seu código-fonte durante o pipeline de CI/CD.

Práticas comuns que devem ser evitadas:

- Não ter um programa de gerenciamento de vulnerabilidades.
- Realizar a aplicação de patches do sistema sem considerar a gravidade ou formas de evitar riscos.
- Utilizar software que ultrapassou a data de fim de vida útil (EOL) indicada pelo fornecedor.
- Implantar código em produção antes de analisar a existência de problemas de segurança.

Nível de risco exposto se esta prática recomendada não for estabelecida: Alto

Orientação para implementação

O gerenciamento de vulnerabilidades é um aspecto fundamental para manter um ambiente de nuvem seguro e robusto. Ele envolve um processo abrangente que inclui verificações de segurança, identificação e priorização de problemas e operações de correção para resolver as vulnerabilidades identificadas. A automação desempenha um papel fundamental nesse processo porque facilita a verificação contínua das workloads em busca de possíveis problemas e exposição não intencional da rede, bem como esforços de remediação.

O Modelo de Responsabilidade Compartilhada da AWS é um conceito fundamental que sustenta o gerenciamento de vulnerabilidades. De acordo com esse modelo, a AWS é responsável por proteger a infraestrutura subjacente, incluindo hardware, software, redes e instalações que executam os serviços da AWS. Por outro lado, você é responsável por proteger seus dados, configurações de segurança e tarefas de gerenciamento associadas a serviços como instâncias do Amazon EC2 e objetos do Amazon S3.

AWSA oferece diversos serviços para apoiar os programas de gerenciamento de vulnerabilidades. O Amazon Inspector verifica continuamente as workloads da AWS em busca de vulnerabilidades de software e acesso não intencional à rede, enquanto o Gerenciador de Patches do AWS Systems Manager ajuda a gerenciar a aplicação de patches nas instâncias do Amazon EC2. Esses serviços podem ser integrados ao AWS Security Hub, um serviço de gerenciamento da postura de segurança na nuvem que automatiza as verificações de segurança da AWS, centraliza os alertas de segurança e fornece uma visão abrangente da postura de segurança de uma organização. Além disso, o Amazon CodeGuru Security usa análise estática de código para identificar possíveis problemas em aplicações Java e Python durante a fase de desenvolvimento.

Ao incorporar práticas de gerenciamento de vulnerabilidades ao ciclo de vida de desenvolvimento de software, você pode abordar as vulnerabilidades de forma proativa antes que elas sejam introduzidas nos ambientes de produção, o que reduz o risco de eventos de segurança e minimiza o impacto potencial das vulnerabilidades.

Etapas de implementação

1. Entenda o modelo de responsabilidade compartilhada: revise o modelo de responsabilidade compartilhada da AWS para entender suas responsabilidades de proteger as workloads e os dados na nuvem. A AWS é responsável por proteger a infraestrutura de nuvem subjacente, enquanto você é responsável por proteger as aplicações, os dados e os serviços utilizados.
2. Implemente a verificação de vulnerabilidades: configure um serviço de verificação de vulnerabilidades, como o Amazon Inspector, para verificar automaticamente as instâncias de computação (por exemplo, máquinas virtuais, contêineres ou funções de tecnologia sem servidor) em busca de vulnerabilidades de software, possíveis defeitos e exposição não intencional da rede.
3. Estabeleça processos de gerenciamento de vulnerabilidades: defina processos e procedimentos para identificar, priorizar e corrigir vulnerabilidades. Isso pode incluir a configuração de cronogramas regulares de verificação de vulnerabilidades, o estabelecimento de critérios de avaliação de risco e a definição de cronogramas de remediação com base na gravidade da vulnerabilidade.
4. Configure o gerenciamento de patches: use um serviço de gerenciamento de patches para automatizar o processo de correção de suas instâncias de computação, tanto para sistemas operacionais quanto para aplicações. Você pode configurar o serviço para verificar as instâncias em busca de patches ausentes e instalá-las automaticamente de acordo com um cronograma. Considere o Gerenciador de Patches do AWS Systems Manager para fornecer essa funcionalidade.

5. Configure a proteção contra malware: implemente mecanismos para detectar software malicioso em seu ambiente. Por exemplo, você pode usar ferramentas como o Amazon GuardDuty para analisar, detectar e alertar sobre malware em volumes EC2 e EBS. O GuardDuty também pode escanear objetos recém-enviados ao Amazon S3 em busca de possíveis malwares ou vírus e tomar medidas para isolá-los antes que sejam ingeridos em processos posteriores.
6. Integre a verificação de vulnerabilidades em pipelines de CI/CD: se você estiver usando um pipeline de CI/CD para a implantação da aplicação, integre ferramentas de verificação de vulnerabilidades em seu pipeline. Ferramentas como o Amazon CodeGuru Security e opções de código aberto podem escanear seu código-fonte, dependências e artefatos em busca de possíveis problemas de segurança.
7. Configure um serviço de monitoramento de segurança: configure um serviço de monitoramento de segurança, como o AWS Security Hub, para ter uma visão abrangente da postura de segurança em vários serviços de nuvem. O serviço deve coletar descobertas de segurança de várias fontes e apresentá-las em um formato padronizado para facilitar a priorização e a remediação.
8. Implemente teste de penetração de aplicativos web: se sua aplicação for um aplicativo web e sua organização tiver as habilidades necessárias ou puder contratar assistência externa, considere a implementação de teste de penetração do aplicativo web para identificar possíveis vulnerabilidades nele.
9. Automatize com infraestrutura como código: use ferramentas de infraestrutura como código (IaC), como AWS CloudFormation, para automatizar a implantação e a configuração de seus recursos, incluindo os serviços de segurança mencionados anteriormente. Essa prática ajuda você a criar uma arquitetura de recursos mais consistente e padronizada em várias contas e ambientes.
10. Monitore e melhore continuamente: monitore continuamente a eficácia do seu programa de gerenciamento de vulnerabilidades e faça melhorias conforme necessário. Analise as descobertas de segurança, avalie a eficácia de seus esforços de remediação e ajuste seus processos e ferramentas adequadamente.

Recursos

Documentos relacionados:

- AWS Systems Manager
- Visão geral da segurança do AWS Lambda
- Amazon CodeGuru

- Gerenciamento de vulnerabilidades aprimorado e automatizado para workloads na nuvem com um novo Amazon Inspector
- Automatize o gerenciamento e a correção de vulnerabilidades na AWS usando o Amazon Inspector e o AWS Systems Manager: parte 1

Vídeos relacionados:

- Proteger serviços com tecnologia sem servidor e em contêineres
- Práticas recomendadas de segurança para o serviço de metadados da instância do Amazon EC2

SEC06-BP02 Provisionar computação com base em imagens reforçadas

Ofereça menos oportunidades de acesso indesejado aos ambientes de runtime implantando-os com base em imagens reforçadas. Adquira somente dependências de runtime, como imagens de contêiner e bibliotecas de aplicações, de registros confiáveis e verifique as respectivas assinaturas. Crie seus próprios registros privados para armazenar imagens e bibliotecas confiáveis para uso nos processos de criação e implantação.

Resultado desejado: seus recursos computacionais são provisionados a partir de imagens de referência reforçadas. Você recupera dependências externas, como imagens de contêiner e bibliotecas de aplicações, somente de registros confiáveis e verifica as respectivas assinaturas. Elas são armazenadas em registros privados para que seus processos de compilação e implantação as consultem. Você verifica e atualiza imagens e dependências regularmente para ajudar a oferecer proteção contra qualquer vulnerabilidade recém-descoberta.

Práticas comuns que devem ser evitadas:

- Adquirir imagens e bibliotecas de registros confiáveis, mas não verificar a respectiva assinatura nem realizar verificações de vulnerabilidades antes de colocá-las em uso.
- Reforçar as imagens, mas não testá-las regularmente em busca de novas vulnerabilidades ou atualizá-las para a versão mais recente.
- Instalar ou não remover pacotes de software que não são necessários durante o ciclo de vida previsto da imagem.
- Confiar apenas na aplicação de patches para manter os recursos de computação de produção atualizados. Ao utilizar apenas a aplicação de patches, os recursos de computação podem se desviar do padrão reforçado com o passar do tempo. A aplicação de patches também pode

não conseguir remover malware instalado por um agente de ameaças durante um evento de segurança.

Benefícios de implementar esta prática recomendada: o reforço de imagens ajuda a reduzir o número de caminhos disponíveis em seu ambiente de runtime que podem permitir acesso não intencional a usuários ou serviços não autorizados. Ele também pode reduzir o escopo do impacto caso ocorra algum acesso indesejado.

Nível de risco exposto se esta prática recomendada não for estabelecida: Alto

Orientação para implementação

Para reforçar seus sistemas, comece com as versões mais recentes de sistemas operacionais, imagens de contêiner e bibliotecas de aplicações. Aplique patches aos problemas conhecidos. Minimize o sistema removendo quaisquer aplicações, serviços, drivers de dispositivo, usuários padrão e outras credenciais desnecessários. Execute qualquer outra ação necessária, como desabilitar portas para criar um ambiente que tenha somente os recursos e capacidades essenciais para as workloads. Com base nesse parâmetro, você pode instalar software, agentes ou outros processos necessários para finalidades como monitoramento da workload ou gerenciamento de vulnerabilidades.

É possível reduzir a carga de reforçar os sistemas usando orientações fornecidas por fontes confiáveis, como o Center for Internet Security (CIS) e os Guias de implementação técnica de segurança (STIGs) da Defense Information Systems Agency (DISA). Recomendamos começar com uma imagem de máquina da Amazon (AMI) publicada pela AWS ou um parceiro da APN e use o AWS EC2 Image Builder para automatizar a configuração de acordo com uma combinação apropriada de controles CIS e STIG.

Embora existam imagens reforçadas e fórmulas do EC2 Image Builder disponíveis que aplicam as recomendações do CIS ou do STIG da DISA, talvez você veja que sua configuração impede que seu software seja executado com êxito. Nessa situação, você pode começar com uma imagem base não reforçada, instalar o software e, em seguida, aplicar incrementalmente os controles do CIS para testar o respectivo impacto. Com relação a qualquer controle do CIS que impeça a execução do software, teste se é possível implementar as recomendações de fortalecimento mais refinadas em um STIG da DISA. Acompanhe os diferentes controles do CIS e as configurações do STIG da DISA que você pode aplicar com sucesso. Use-os para definir adequadamente suas fórmulas de reforço de imagem no EC2 Image Builder.

Para workloads em contêineres, imagens reforçadas do Docker estão disponíveis no repositório público do Amazon Elastic Container Registry (ECR). Você pode usar o EC2 Image Builder para reforçar imagens de contêiner, bem como AMIs.

Semelhante aos sistemas operacionais e às imagens de contêiner, você pode obter pacotes de código (ou bibliotecas) de repositórios públicos por meio de ferramentas como pip, npm, Maven e NuGet. Recomendamos gerenciar pacotes de código integrando repositórios privados, como os do AWS CodeArtifact, a repositórios públicos confiáveis. Com essa integração, você não precisa se preocupar em lidar com a recuperação, o armazenamento e a manutenção de pacotes atualizados. Seus processos de criação de aplicações podem então obter e testar a versão mais recente desses pacotes, bem como a aplicação, usando técnicas como análise de composição de software (SCA), testes estáticos de segurança de aplicações (SAST) e testes dinâmicos de segurança de aplicações (DAST).

Para workloads sem servidor que usam o AWS Lambda, simplifique o gerenciamento de dependências de pacotes usando camadas do Lambda. Use camadas do Lambda para configurar um conjunto de dependências padrão que são compartilhadas em diferentes funções em um arquivo independente. Você pode criar e manter camadas por meio de seu próprio processo de criação, fornecendo um meio centralizado para manter as funções atualizadas.

Etapas de implementação

- Reforce os sistemas operacionais. Use imagens básicas de fontes confiáveis como base para criar AMIs reforçadas. Use o EC2 Image Builder para ajudar a personalizar o software instalado em suas imagens.
- Reforce os recursos em contêineres. Configure recursos em contêineres para atender a práticas recomendadas de segurança. Ao usar contêineres, implemente a varredura de imagens do ECR no pipeline de compilação e regularmente no repositório de imagens para procurar CVEs nos contêineres.
- Ao usar a implementação sem servidor com o AWS Lambda, use camadas do Lambda para separar o código da função da aplicação e as bibliotecas dependentes compartilhadas. Configure a assinatura de código para Lambda para garantir que apenas código confiável seja executado em suas funções do Lambda.

Recursos

Práticas recomendadas relacionadas:

- OPS05-BP05 Realizar o gerenciamento de patches

Vídeos relacionados:

- Mergulho profundo na segurança do AWS Lambda

Exemplos relacionados:

- Criar rapidamente uma AMI compatível com STIG usando o EC2 Image Builder
- Criar imagens de contêiner melhores
- Usar camadas do Lambda para simplificar seu processo de desenvolvimento
- Desenvolver e implantar camadas do AWS Lambda usando um framework sem servidor
- Criar um pipeline de CI/CD completo do AWS DevSecOps com ferramentas de código aberto SCA, SAST e DAST

SEC06-BP03 Reduzir o gerenciamento manual e o acesso interativo

Use a automação para realizar tarefas de implantação, configuração, manutenção e investigação sempre que possível. Considere usar o acesso manual aos recursos de computação em casos de procedimentos de emergência ou em ambientes seguros (sandbox) quando a automação não estiver disponível.

Resultado desejado: scripts programáticos e documentos de automação (runbooks) capturam ações autorizadas em seus recursos computacionais. Os runbooks são iniciados automaticamente por meio de sistemas de detecção de alterações ou manualmente quando a avaliação humana é necessária. O acesso direto aos recursos de computação só é disponibilizado em situações de emergência quando a automação não está disponível. Todas as atividades manuais são registradas em log e incorporadas a um processo de análise para aprimorar continuamente os recursos de automação.

Práticas comuns que devem ser evitadas:

- Usar o acesso interativo a instâncias do Amazon EC2 com protocolos como SSH ou RDP.
- Manter logins de usuários individuais, como `/etc/passwd` ou usuários locais do Windows.
- Compartilhar uma senha ou chave privada para acessar uma instância entre vários usuários.
- Instalar software e criar ou atualizar manualmente arquivos de configuração.

- Atualizar ou aplicar patches manualmente no software.
- Fazer login em uma instância para solucionar problemas.

Benefícios de implementar esta prática recomendada: a execução de ações com automação ajuda a reduzir o risco operacional de alterações não intencionais e configurações incorretas. Eliminar o uso do Secure Shell (SSH) e do Remote Desktop Protocol (RDP) para acesso interativo reduz o escopo do acesso aos seus recursos de computação. Fazer isso elimina um caminho comum para ações não autorizadas. Capturar suas tarefas de gerenciamento de recursos de computação em documentos de automação e scripts programáticos oferece um mecanismo para definir e auditar todo o escopo das atividades autorizadas em um nível de detalhes refinado.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

Fazer login em uma instância é uma abordagem clássica à administração de sistemas. Após a instalação do sistema operacional do servidor, os usuários normalmente fazem login manualmente para configurar o sistema e instalar o software desejado. Durante o ciclo de vida do servidor, os usuários podem fazer login para realizar atualizações de software, aplicar patches, alterar configurações e solucionar problemas.

No entanto, o acesso manual apresenta vários riscos. Ele exige um servidor que escuta solicitações, como um serviço SSH ou RDP, o que pode fornecer um possível caminho para acessos não autorizados. Ele também aumenta o risco de erro humano associado à execução de etapas manuais. Isso pode resultar em incidentes de workload, corrompimento ou destruição de dados ou outros problemas de segurança. O acesso humano também exige proteções contra o compartilhamento de credenciais, o que cria uma sobrecarga adicional de gerenciamento.

Para mitigar esses riscos, você pode implementar uma solução de acesso remoto baseada em agente, como o AWS Systems Manager. AWS Systems Manager O agente (SSM Agent) inicia um canal criptografado e, portanto, não depende da escuta de solicitações iniciadas externamente. Considere configurar o SSM Agent para estabelecer esse canal em um endpoint da VPC.

O Systems Manager oferece controle refinado sobre como você pode interagir com suas instâncias gerenciadas. Você define as automações a serem executadas, quem pode executá-las e quando elas podem ser executadas. O Systems Manager pode aplicar patches, instalar software e fazer alterações na configuração sem ter acesso interativo à instância. O Systems Manager também pode fornecer acesso a um shell remoto e registrar cada comando invocado e sua saída durante a sessão

nos logs e no Amazon S3. O AWS CloudTrail registra as invocações das APIs do Systems Manager para inspeção.

Etapas de implementação

1. Instale o AWS Systems Manager Agent (SSM Agent) nas suas instâncias do Amazon EC2. Verifique se o SSM Agent está incluído e foi iniciado automaticamente como parte da configuração básica da AMI.
2. Verifique se as funções do IAM associadas aos seus perfis de instância do EC2 incluem a política `AmazonSSMManagedInstanceCore` gerenciada pelo IAM.
3. Desabilite o SSH, o RDP e outros serviços de acesso remoto em execução nas instâncias. Você pode fazer isso executando scripts configurados na seção de dados do usuário dos seus modelos de lançamento ou criando AMIs personalizadas com ferramentas como o EC2 Image Builder.
4. Verifique se as regras de entrada do grupo de segurança aplicáveis às instâncias do EC2 não permitem acesso na porta 22/tcp (SSH) ou na porta 3389/tcp (RDP). Implemente a detecção e o alerta de grupos de segurança configurados incorretamente usando serviços como o AWS Config.
5. Defina automações, runbooks e comandos de execução apropriados no Systems Manager. Use políticas do IAM para definir quem pode realizar essas ações e as condições sob as quais elas são permitidas. Teste essas automações minuciosamente em um ambiente de não produção. Invoque essas automações quando necessário, em vez de acessar a instância de forma interativa.
6. Use o AWS Systems Manager Session Manager para fornecer acesso interativo às instâncias quando necessário. Ative o log de atividades da sessão para manter uma trilha de auditoria no Amazon CloudWatch Logs ou no Amazon S3.

Recursos

Práticas recomendadas relacionadas:

- REL08-BP04 Implantar usando infraestrutura imutável

Exemplos relacionados:

- Substituir o acesso SSH para reduzir a sobrecarga de gerenciamento e segurança com o AWS Systems Manager

Ferramentas relacionadas:

- AWS Systems Manager

Vídeos relacionados:

- Controlar o acesso da sessão do usuário à instâncias no Gerenciador de Sessões do AWS Systems Manager

SEC06-BP04 Validar a integridade do software

Use a verificação criptográfica para validar a integridade dos artefatos de software (incluindo imagens) que a workload usa. Assine criptograficamente seu software como uma proteção contra alterações não autorizadas executadas em seus ambientes de computação.

Resultado desejado: todos os artefatos são obtidos de fontes confiáveis. Os certificados do site do fornecedor são validados. Os artefatos baixados são verificados criptograficamente com base na respectiva assinatura. Seu próprio software é assinado e verificado criptograficamente por seus ambientes de computação.

Práticas comuns que devem ser evitadas:

- Confiar em sites de fornecedores de boa reputação para obter artefatos de software, mas ignorar os avisos de expiração de certificado. Prosseguir com os downloads sem confirmar se os certificados são válidos.
- Validar certificados de sites de fornecedores, mas não verificar criptograficamente os artefatos baixados desses sites.
- Confiar apenas em resumos ou hashes para validar a integridade do software. Os hashes estabelecem que os artefatos não foram modificados da versão original, mas não validam a respectiva fonte.
- Não assinar seu próprio software, código ou biblioteca, mesmo quando usados apenas em suas próprias implantações.

Benefícios de implementar esta prática recomendada: validar a integridade dos artefatos dos quais sua workload depende ajuda a impedir a entrada de malware em seus ambientes computacionais. Assinar seu software ajuda a impedir a execução não autorizada em seus ambientes de computação. Proteja sua cadeia de suprimentos de software assinando e verificando o código.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

As imagens do sistema operacional, as imagens de contêiner e os artefatos de código geralmente são distribuídos com verificações de integridade disponíveis, como por meio de um resumo ou hash. Isso permite que os clientes verifiquem a integridade calculando o hash da carga útil e validando se ele é o mesmo que o publicado. Embora essas verificações ajudem a verificar se a carga não foi adulterada, elas não validam que a carga veio da fonte original (sua procedência). A verificação de procedência exige um certificado emitido por uma autoridade confiável para assinar o artefato digitalmente.

Se você estiver usando um software ou artefatos baixados na workload, verifique se o provedor fornece uma chave pública para verificação de assinatura digital. Veja alguns exemplos de como a AWS fornece uma chave pública e instruções de verificação para o software que publicamos:

- EC2 Image Builder: verificar a assinatura do download da instalação do AWS TOE
- AWS Systems Manager: verificar a assinatura do SSM Agent
- Amazon CloudWatch: verificar a assinatura do pacote do agente do CloudWatch

Incorpore a verificação de assinatura digital aos processos que você usa para obter e reforçar imagens, conforme discutido em SEC06-BP02 Provisionar a computação com base em imagens reforçadas.

Você pode usar o AWS Signer para ajudar a gerenciar a verificação de assinaturas, bem como seu próprio ciclo de vida de assinatura de código para seu próprio software e artefatos. Tanto o AWS Lambda quanto o Amazon Elastic Container Registry fornecem integrações com o Signer para verificar as assinaturas do seu código e imagens. Usando os exemplos na seção “Recursos”, você pode incorporar o Signer aos pipelines de integração e entrega contínuas (CI/CD) para automatizar a verificação de assinaturas e a assinatura de código e imagens.

Recursos

Documentos relacionados:

- Assinatura criptográfica para contêineres
- Práticas recomendadas para ajudar a proteger sua imagem de contêiner: crie um pipeline usando AWS Signer
- Assinatura de imagens de contêineres com o AWS Signer e o Amazon EKS
- Configurar a assinatura de código para o AWS Lambda

- Práticas recomendadas e padrões avançados para assinatura de código do Lambda
- Assinatura de código usando CA privada do AWS Certificate Manager e chaves assimétricas do AWS Key Management Service

Exemplos relacionados:

- Automatizar a assinatura de código do Lambda com o Amazon CodeCatalyst e o AWS Signer
- Assinar e validar artefatos OCI com o AWS Signer

Ferramentas relacionadas:

- AWS Lambda
- AWS Signer
- AWS Certificate Manager
- AWS Key Management Service
- AWS CodeArtifact

SEC06-BP05 Automatizar a proteção da computação

Automatize as operações de proteção da computação para reduzir a necessidade de intervenção humana. Use a verificação automatizada para detectar possíveis problemas em seus recursos de computação e corrigir com respostas programáticas automatizadas ou operações de gerenciamento de frota. Incorpore a automação em seus processos de CI/CD para implantar workloads confiáveis com dependências atualizadas.

Resultado desejado: sistemas automatizados realizam todas as verificações e correções dos recursos computacionais. Você usa a verificação automatizada para determinar se as imagens e dependências do software são provenientes de fontes confiáveis e não foram adulteradas. As workloads são verificadas automaticamente em busca de dependências atualizadas e assinadas para estabelecer a confiabilidade em ambientes computacionais da AWS. As correções automatizadas são iniciadas quando recursos fora de conformidade são detectados.

Práticas comuns que devem ser evitadas:

- Seguir a prática de infraestrutura imutável, mas sem ter uma solução para correção emergencial ou substituição de sistemas de produção.

- Usar a automação para corrigir recursos configurados incorretamente, mas sem ter um mecanismo de substituição manual instalado. Podem surgir situações em que você precise ajustar os requisitos e suspender as automações até fazer essas alterações.

Benefícios de implementar esta prática recomendada: a automação pode reduzir o risco de acesso e uso não autorizados de seus recursos computacionais. Isso ajuda a evitar que configurações incorretas entrem nos ambientes de produção e a detectar e corrigir configurações incorretas caso elas ocorram. A automação também ajuda a detectar acesso e uso não autorizados de recursos de computação para reduzir o tempo de resposta. Isso, por sua vez, pode reduzir o escopo geral do impacto do problema.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

É possível aplicar as automações descritas nas práticas do pilar de segurança para proteger seus recursos de computação. SEC06-BP01 Realizar o gerenciamento de vulnerabilidades descreve como você pode usar o Amazon Inspector em seus pipelines de CI/CD e para verificar continuamente seus ambientes de runtime em busca de vulnerabilidades e exposições comuns (CVEs) conhecidas. Você pode usar o AWS Systems Manager para aplicar patches ou reimplantar com base em novas imagens por meio de runbooks automatizados para manter sua frota computacional atualizada com o software e as bibliotecas mais recentes. Use essas técnicas para reduzir a necessidade de processos manuais e acesso interativo aos seus recursos de computação. Consulte SEC06-BP03 Reduzir o gerenciamento manual e o acesso interativo para saber mais.

A automação também desempenha um papel na implantação de workloads confiáveis, descritas em SEC06-BP02 Provisionar computação com base em imagens reforçadas e SEC06-BP04 Validar a integridade do software. É possível usar serviços como EC2 Image Builder, AWS Signer, AWS CodeArtifact e Amazon Elastic Container Registry (ECR) para baixar, verificar, construir e armazenar imagens reforçadas e aprovadas e dependências de código. Com o Inspector, cada um desses serviços pode desempenhar um papel no processo de CI/CD, de forma que a workload chegue à produção somente quando for confirmado que suas dependências estão atualizadas e provêm de fontes confiáveis. Sua workload também é assinada para que ambientes computacionais da AWS, como AWS Lambda e Amazon Elastic Kubernetes Service (EKS), possam verificar se ela não foi adulterada antes de permitir sua execução.

Além desses controles preventivos, você também pode usar a automação nos controles de detecção para seus recursos de computação. Como exemplo, o AWS Security Huboferece o padrão NIST

800-53 Rev. 5, que inclui verificações como [EC2.8] As instâncias do EC2 devem usar o Instance Metadata Service Version 2 (IMDSv2). O IMDSv2 usa as técnicas de autenticação de sessão, bloqueando solicitações que contêm um cabeçalho HTTP X-Forwarded-For e um TTL de rede de 1 para interromper o tráfego proveniente de fontes externas e recuperar informações sobre a instância do EC2. Essa verificação no Security Hub pode detectar quando as instâncias do EC2 usam o IMDSv1 e iniciar a autocorreção. Saiba mais sobre detecção e remediações automatizadas em SEC04-BP04 Iniciar a correção para recursos fora de conformidade.

Etapas de implementação

1. Automatize a criação de AMIs seguras, em conformidade e reforçadas com o EC2 Image Builder. Você pode produzir imagens que incorporem controles dos padrões de referência do Center for Internet Security (CIS) ou do Security Technical Implementation Guide (STIG) com base em imagens básicas da AWS e de parceiros da APN.
2. Automatize o gerenciamento de configuração. Aplique e valide configurações seguras automaticamente em seus recursos de computação usando um serviço ou uma ferramenta de gerenciamento de configuração.
    a. Gerenciamento automatizado de configurações usando o AWS Config
    b. Gerenciamento automatizado da postura de segurança e conformidade usando o AWS Security Hub
3. Automatize a aplicação de patches ou a substituição de instâncias do Amazon Elastic Compute Cloud (Amazon EC2). AWS O Gerenciador de Patches do Systems Manager automatiza o processo de aplicação de patches em instâncias gerenciadas com atualizações relacionadas à segurança e com outros tipos de atualizações. Você pode usar o Patch Manager para aplicar patches de sistemas operacionais e aplicações.
    a. Gerenciador de patches do AWS Systems Manager
4. Automatize a verificação de recursos de computação em busca de vulnerabilidades e exposições comuns (CVEs) e incorpore soluções de verificação de segurança em seu pipeline de criação.
    a. Amazon Inspector
    b. Verificação de imagens do ECR
5. Considere o Amazon GuardDuty para detecção automática de malware e ameaças para proteger os recursos computacionais. O GuardDuty também pode identificar possíveis problemas quando uma função do AWS Lambda é invocada em seu ambiente da AWS.
    a. Amazon GuardDuty

6. Considere as soluções dos parceiros da AWS. AWS Os parceiros oferecem produtos líderes do setor que são equivalentes, idênticos ou se integram aos controles existentes nos seus ambientes on-premises. Esses produtos complementam os serviços existentes da AWS para que você possa implantar uma arquitetura de segurança abrangente e obter uma experiência mais uniforme em seus ambientes na nuvem e on-premises.
   a. Segurança da infraestrutura

Recursos

Práticas recomendadas relacionadas:

- SEC01-BP06 Automatizar a implantação de controles de segurança padrão

Documentos relacionados:

- Obtenha todos os benefícios do IMDSv2 e desative o IMDSv1 em sua infraestrutura da AWS

Vídeos relacionados:

- Práticas recomendadas de segurança para o serviço de metadados da instância do Amazon EC2

Proteção de dados

Antes de criar a arquitetura de qualquer workload, práticas fundamentais que influenciam a segurança devem ser adotadas. Por exemplo, a classificação de dados fornece uma maneira de categorizar os dados organizacionais com base nos níveis de sensibilidade, e a criptografia protege os dados tornando-os ininteligíveis ao acesso não autorizado. Esses métodos são importantes porque apoiam objetivos como evitar o manuseio indevido ou o cumprimento de obrigações regulatórias.

Na AWS, há várias abordagens a serem consideradas para lidar com a proteção de dados. A seção a seguir descreve como usar essas abordagens.

Tópicos

Classificação de dados

A classificação de dados fornece uma maneira de categorizar dados organizacionais com base em criticidade e confidencialidade para ajudá-lo a determinar os controles de proteção e retenção apropriados.

Práticas recomendadas

SEC07-BP01 Compreender seu esquema de classificação de dados

Compreenda a classificação dos dados que a workload está processando, os requisitos de tratamento, os processos de negócios associados, onde os dados são armazenados e quem é o proprietário dos dados. Seu esquema de classificação e tratamento de dados deve considerar

os requisitos legais e de conformidade aplicáveis à workload e quais controles de dados são necessários. Compreender os dados é a primeira etapa da jornada de classificação de dados.

Resultado desejado: os tipos de dados presentes em sua workload são bem compreendidos e documentados. Controles apropriados estão em vigor para proteger os dados confidenciais com base na respectiva classificação. Esses controles regem fatores como: quem tem permissão para acessar os dados e com que finalidade, onde eles são armazenados, a respectiva política de criptografia e como as chaves de criptografia são gerenciadas, o ciclo de vida dos dados e os requisitos de retenção, os processos de destruição apropriados, quais processos de backup e recuperação estão em vigor e a auditoria do acesso.

Práticas comuns que devem ser evitadas:

- Não ter uma política formal de classificação de dados em vigor para definir os níveis de confidencialidade dos dados e os requisitos de tratamento
- Não ter uma boa compreensão dos níveis de confidencialidade dos dados na workload e não capturar essas informações na documentação de arquitetura e operações
- Não aplicar os controles apropriados sobre os dados com base na confidencialidade e nos respectivos requisitos, conforme descrito em sua política de classificação e tratamento de dados
- Não fornecer feedback sobre os requisitos de classificação e tratamento de dados aos proprietários das políticas.

Benefícios de implementar esta prática recomendada: essa prática elimina a ambiguidade em relação ao tratamento adequado dos dados em sua workload. A aplicação de uma política formal que defina os níveis de confidencialidade dos dados em sua organização e as proteções necessárias pode ajudar você a cumprir as regulamentações legais e outros atestados e certificações de segurança cibernética. Os proprietários das workloads podem ter certeza sobre onde os dados confidenciais estão armazenados e quais controles de proteção estão em vigor. Capturá-los na documentação ajuda os novos membros da equipe a compreendê-los melhor e a manter os controles no início de sua gestão. Essas práticas também podem ajudar a reduzir os custos ao dimensionar corretamente os controles para cada tipo de dados.

Nível de risco exposto se esta prática recomendada não for estabelecida: Alto

Orientação para implementação

Ao projetar uma workload, você pode considerar opções para proteger os dados confidenciais de forma intuitiva. Por exemplo, em uma aplicação multilocatário, é intuitivo considerar os dados de

cada locatário como confidenciais e implementar proteções para impedir que um locatário acesse os dados de outro locatário. Da mesma forma, você pode projetar controles de acesso intuitivamente para que apenas os administradores modifiquem os dados e os outros usuários tenham acesso somente leitura ou não tenham nenhum acesso.

Com esses níveis de confidencialidade de dados definidos e capturados na política, bem como os respectivos requisitos de proteção de dados, você pode identificar formalmente quais dados residem na workload. Em seguida, é possível determinar se os controles corretos estão em vigor, se os controles podem ser auditados e quais respostas são apropriadas se os dados forem tratados incorretamente.

Para ajudar a identificar onde os dados confidenciais residem em sua workload, considere usar um catálogo de dados. Um catálogo de dados é um banco de dados que mapeia dados em sua organização, sua localização, nível de sensibilidade e os controles em vigor para proteger esses dados. Além disso, considere usar tags de recursos quando disponíveis. Por exemplo, você pode aplicar uma tag que tenha uma chave de tag de `Classification` e um valor de tag de `PHI` para informações de saúde protegidas (PHI) e outra tag que tenha uma chave de tag de `Sensitivity` e um valor de tag de `High`. Serviços como o AWS Config podem então ser usados para monitorar esses recursos em busca de alterações e alertar se eles forem modificados de uma forma que os tire da conformidade com seus requisitos de proteção (como alterar as configurações de criptografia). Você pode capturar a definição padrão de suas chaves de tag e valores aceitáveis usando políticas de tag, um recurso do AWS Organizations. Não é recomendável que a chave ou o valor da tag contenha dados privados ou confidenciais.

Etapas de implementação

1. Entenda o esquema de classificação de dados e os requisitos de proteção da sua organização.
2. Identifique os tipos de dados confidenciais processados pelas workloads.
3. Capture os dados em um catálogo de dados que fornece uma visão única da residência de dados na organização e do nível de confidencialidade desses dados.
4. Considere usar a marcação em nível de recursos e dados, quando disponível, para marcar o nível de confidencialidade dos dados e outros metadados operacionais que possam ajudar no monitoramento e resposta a incidentes.
    a. As políticas de tag do AWS Organizations podem ser usadas para impor padrões de marcação.

Recursos

Práticas recomendadas relacionadas:

- SUS04-BP01 Implementar uma política de classificação de dados

Documentos relacionados:

- Whitepaper Classificação de dados
- Práticas recomendadas para marcação de recursos da AWS com tags

Exemplos relacionados:

- Sintaxe e exemplos de políticas de tags AWS Organizations

Ferramentas relacionadas

- AWS Tag Editor

SEC07-BP02 Aplicar controles de proteção de dados com base na confidencialidade dos dados

Aplique controles de proteção de dados que ofereçam um nível apropriado de controle para cada classe de dados definida em sua política de classificação. Essa prática pode permitir que você proteja dados confidenciais contra acesso e uso não autorizados, preservando a disponibilidade e o uso dos dados.

Resultado desejado: você tem uma política de classificação que define os diferentes níveis de sensibilidade dos dados em sua organização. Para cada um desses níveis de confidencialidade, você tem diretrizes claras publicadas para serviços e locais de armazenamento e manuseio aprovados e as respectivas configurações necessárias. Você implementa os controles para cada nível conforme o nível de proteção necessário e os custos correspondentes. Você dispõe de monitoramento e alertas para detectar se há dados em locais não autorizados, se eles são processados em ambientes não autorizados, se eles são acessados por agentes não autorizados ou se a configuração dos serviços relacionados está fora de conformidade.

Práticas comuns que devem ser evitadas:

- Aplicar o mesmo nível de controles de proteção em todos os dados. Isso pode levar ao superprovisionamento de controles de segurança para dados com baixo nível de confidencialidade ou à proteção insuficiente dos dados altamente confidenciais.
- Não envolver as partes interessadas relevantes das equipes de segurança, conformidade e negócios ao definir os controles de proteção de dados.
- Ignorar as despesas operacionais indiretas e os custos associados à implementação e manutenção dos controles de proteção de dados.
- Não realizar revisões periódicas de controle de proteção de dados para manter o alinhamento com as políticas de classificação.
- Não ter um inventário completo da residência de dados em repouso e em trânsito.

Benefícios de implementar esta prática recomendada: ao alinhar seus controles ao nível de classificação de seus dados, sua organização pode investir em níveis mais altos de controle quando necessário. Isso pode incluir a ampliação dos recursos de proteção, monitoramento, medição, correção e geração de relatórios. Nas circunstâncias em que é apropriado usar menos controles, você pode melhorar a acessibilidade e a completude dos dados para seu quadro de funcionários, clientes ou membros. Essa abordagem possibilita que sua organização use os dados da forma mais flexível possível e, ao mesmo tempo, cumpra os requisitos de proteção de dados.

Nível de risco exposto se esta prática recomendada não for estabelecida: Alto

Orientação para implementação

A implementação de controles de proteção de dados com base nos níveis de confidencialidade dos dados envolve várias etapas importantes. Primeiro, identifique os diferentes níveis de confidencialidade de dados em sua arquitetura de workload (como público, interno, confidencial e restrito) e avalie onde você armazena e processa esses dados. Em seguida, defina limites de isolamento em torno dos dados com base no respectivo nível de confidencialidade. Recomendamos separar os dados em diferentes Contas da AWS usando políticas de controle de serviços (SCPs) para restringir serviços e ações permitidos para cada nível de confidencialidade de dados. Dessa forma, é possível criar limites de isolamento robustos e aplicar o princípio de privilégio mínimo.

Após a definição dos limites de isolamento, implemente controles de proteção apropriados com base nos níveis de confidencialidade dos dados. Consulte as práticas recomendadas para Proteger dados em repouso e Proteger dados em trânsito para implementar controles relevantes, como criptografia, controles de acesso e auditoria. Considere técnicas como tokenização ou anonimização para reduzir

o nível de confidencialidade dos dados. Simplifique a aplicação de políticas de dados consistentes em sua empresa com um sistema centralizado para tokenização e destokenização.

Monitore e teste continuamente a eficácia dos controles implementados. Analise e atualize regularmente o esquema de classificação de dados, as avaliações de risco e os controles de proteção à medida que as ameaças e o cenário de dados de sua organização evoluírem. Alinhe os controles de proteção de dados implementados com as regulamentações, os padrões e os requisitos legais relevantes do setor. Além disso, ofereça conscientização e treinamento sobre segurança para ajudar os funcionários a entender o esquema de classificação de dados e suas responsabilidades no tratamento e proteção de dados confidenciais.

Etapas de implementação

1. Identifique os níveis de classificação e confidencialidade dos dados em sua workload.
2. Defina limites de isolamento para cada nível e determine uma estratégia de imposição.
3. Avalie os controles definidos por você que regem acesso, criptografia, auditoria, retenção e outras questões exigidas por sua política de classificação de dados.
4. Avalie as opções para reduzir o nível de confidencialidade dos dados quando apropriado, como usar tokenização ou anonimização.
5. Verifique os controles usando testes e monitoramento automatizados dos recursos configurados.

Recursos

Práticas recomendadas relacionadas:

- PERF03-BP01 Usar um datastore com propósitos específicos que melhor atenda aos requisitos de acesso e armazenamento de dados
- COST04-BP05 Impor políticas de retenção de dados

Documentos relacionados:

- Whitepaper Classificação de dados
- Práticas recomendadas de segurança, identidade e conformidade
- Práticas recomendadas do AWS KMS.
- Práticas recomendadas e recursos de criptografia para serviços da AWS

Exemplos relacionados:

- Criar uma solução de tokenização sem servidor para mascarar dados confidenciais
- Como usar a tokenização para melhorar a segurança dos dados e reduzir o escopo da auditoria

Ferramentas relacionadas:

- AWS Key Management Service (AWS KMS)
- AWS CloudHSM
- AWS Organizations

SEC07-BP03 Automatizar a identificação e a classificação

Automatizar a identificação e a classificação de dados pode ajudar a implementar os controles corretos. O uso da automação para ampliar a determinação manual reduz o risco de erro humano e a exposição.

Resultado desejado: você pode verificar se os controles adequados estão em vigor com base em sua política de classificação e manuseio. Ferramentas e serviços automatizados ajudam a identificar e classificar o nível de confidencialidade dos dados. A automação também ajuda a monitorar continuamente os ambientes para detectar e alertar se os dados estão sendo armazenados ou manipulados de forma não autorizada para que medidas corretivas possam ser tomadas rapidamente.

Práticas comuns que devem ser evitadas:

- Confiar apenas em processos manuais para identificação e classificação de dados, os quais podem ser propensos a erros e demorados. Isso pode resultar em uma classificação de dados ineficiente e inconsistente, especialmente à medida que os volumes de dados aumentam.
- Não ter mecanismos para monitorar e gerenciar ativos de dados em toda a organização.
- Ignorar a necessidade de monitoramento e classificação contínuos dos dados conforme eles se movimentam e evoluem dentro da organização.

Benefícios de implementar esta prática recomendada: automatizar a identificação e a classificação de dados pode levar a uma aplicação mais consistente e precisa dos controles de proteção de dados, reduzindo o risco de erro humano. A automação também pode fornecer visibilidade sobre o

acesso e a movimentação de dados confidenciais, ajudando a detectar o tratamento não autorizado e a adotar medidas corretivas.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

Embora a avaliação humana seja frequentemente usada para classificar dados durante as fases iniciais de projeto de uma workload, considere a possibilidade de ter sistemas que automatizem a identificação e a classificação dos dados de teste como um controle preventivo. Por exemplo, os desenvolvedores podem receber uma ferramenta ou serviço para verificar dados representativos e determinar o nível de confidencialidade. Na AWS, é possível carregar conjuntos de dados no Amazon S3 e examiná-los usando o Amazon Macie, o Amazon Comprehend ou o Amazon Comprehend Medical. Da mesma forma, considere a possibilidade de verificar os dados como parte dos testes de unidade e integração para detectar onde não deve haver dados confidenciais. Utilizar alertas sobre dados confidenciais nesse estágio pode destacar brechas nas proteções antes da implantação na produção. Outros recursos do AWS Glue, como detecção de dados confidenciais no Amazon SNS e no Amazon CloudWatch, também podem ser usados para detectar PII e aplicar as medidas mitigadoras necessárias. Com relação a quaisquer ferramentas ou serviços automatizados, entenda como eles definem dados confidenciais e complemente-os com outras soluções humanas ou automatizadas para resolver qualquer brecha conforme necessário.

Como controle de detecção, use o monitoramento contínuo dos ambientes para detectar se os dados confidenciais estão sendo armazenados fora de conformidade. Isso pode ajudar a detectar determinadas situações, como publicação ou cópia de dados confidenciais em arquivos de log ou para um ambiente de análise de dados sem a devida desidentificação ou edição. Com relação aos dados armazenados no Amazon S3, os dados confidenciais podem ser monitorados continuamente usando o Amazon Macie.

Etapas de implementação

1. Revise o esquema de classificação de dados em sua organização descrito em SEC07-BP01.
   a. Com uma compreensão do esquema de classificação de dados da sua organização, você pode estabelecer processos precisos para identificação e classificação automatizadas que estejam alinhados às políticas da sua empresa.
2. Execute uma verificação inicial dos ambientes para identificação e classificação automatizadas.
   a. Uma verificação inicial completa dos dados pode ajudar a gerar uma compreensão abrangente do local em que os dados confidenciais residem nos ambientes. Quando uma verificação

completa não for necessária inicialmente ou não puder ser concluída antecipadamente devido ao custo, avalie se as técnicas de amostragem de dados são adequadas para alcançar seus resultados. Por exemplo, o Amazon Macie pode ser configurado para realizar uma ampla operação automatizada de descoberta de dados confidenciais nos buckets do S3. Esse recurso usa técnicas de amostragem para realizar de forma econômica uma análise preliminar do local em que os dados confidenciais residem. Uma análise mais detalhada dos buckets do S3 pode então ser realizada usando um trabalho de descoberta de dados confidenciais. Outros datastores também podem ser exportados para o S3 para serem verificados pelo Macie.

   b. Estabeleça o controle de acesso definido em SEC07-BP02 para seus recursos de armazenamento de dados identificados em seu escaneamento.

3. Configure verificações contínuas dos ambientes.
   a. O recurso automatizado de descoberta de dados confidenciais do Macie pode ser usado para realizar verificações contínuas dos ambientes. Os buckets do S3 conhecidos e autorizados a armazenar dados confidenciais podem ser excluídos usando uma lista de permissões em no Macie.
4. Incorpore identificação e classificação nos processos de compilação e teste.
   a. Identifique as ferramentas que os desenvolvedores podem usar para verificar a confidencialidade dos dados enquanto as workloads estão sendo desenvolvidas. Use essas ferramentas como parte dos testes de integração para emitir alertas quando houver dados confidenciais inesperados e evitar implantações adicionais.
5. Implemente um sistema ou um runbook para tomar medidas quando dados confidenciais forem encontrados em locais não autorizados.
   a. Restrinja o acesso aos dados usando a correção automática. Por exemplo, você pode mover esses dados para um bucket do S3 com acesso restrito ou marcar o objeto se usar o controle de acesso por atributo (ABAC). Além disso, considere mascarar os dados quando eles forem detectados.
   b. Alerte suas equipes de proteção de dados e resposta a incidentes para investigar a causa raiz do incidente. Qualquer aprendizado que elas identifiquem pode ajudar a evitar futuros incidentes.

Recursos

Documentos relacionados:

- AWS Glue: Detectar e processar dados confidenciais

- Usar identificadores de dados gerenciados no Amazon SNS
- Amazon CloudWatch Logs: ajude a proteger dados de log confidenciais com mascaramento

Exemplos relacionados:

- Habilitar a classificação de dados para o banco de dados do Amazon RDS com o Macie
- Detectar dados confidenciais no DynamoDB com o Macie

Ferramentas relacionadas:

- Amazon Macie
- Amazon Comprehend
- Amazon Comprehend Medical
- AWS Glue

SEC07-BP04 Definir o gerenciamento escalável do ciclo de vida dos dados

Entenda os requisitos do ciclo de vida dos dados relacionados aos seus diferentes níveis de classificação e tratamento de dados. Isso pode incluir como os dados são tratados quando entram pela primeira vez em seu ambiente, como os dados são transformados e as regras para sua destruição. Considere fatores como períodos de retenção, acesso, auditoria e rastreamento da procedência.

Resultado desejado: você classifica os dados o mais próximo possível do ponto e da hora da ingestão. Quando a classificação de dados exige mascaramento, tokenização ou outros processos que reduzam o nível de confidencialidade, você executa essas ações o mais próximo possível do ponto e hora de ingestão.

Você exclui os dados de acordo com sua política quando não é mais apropriado mantê-los e com base na respectiva classificação.

Práticas comuns que devem ser evitadas:

- Implementar uma abordagem única de gerenciamento do ciclo de vida dos dados sem considerar os diferentes níveis de confidencialidade e requisitos de acesso.
- Considerar o gerenciamento do ciclo de vida somente do ponto de vista dos dados utilizáveis ou dos dados submetidos a backup, mas não de ambos.

- Supor que os dados que entraram na workload são válidos, sem estabelecer o respectivo valor ou procedência.
- Confiar na durabilidade dos dados como substituto dos backups e da proteção de dados.
- Reter os dados depois que eles já perderam a utilidade e após o período de retenção exigido.

Benefícios de implementar esta prática recomendada: uma estratégia de gerenciamento do ciclo de vida de dados bem definida e escalável ajuda a manter a conformidade regulatória, melhora a segurança dos dados, otimiza os custos de armazenamento e permite o acesso e o compartilhamento eficientes dos dados ao mesmo tempo que os controles adequados são mantidos.

Nível de risco exposto se esta prática recomendada não for estabelecida: Alto

Orientação para implementação

Os dados em uma workload geralmente são dinâmicos. A forma que eles assumem ao entrar no ambiente da workload pode ser diferente de quando são armazenados ou usados em lógica de negócios, relatórios, análises ou machine learning. Além disso, a importância dos dados pode mudar com o tempo. Alguns dados são de natureza temporal e perdem o valor à medida que se tornam obsoletos. Considere como essas mudanças nos dados afetam a avaliação em seu esquema de classificação de dados e controles associados. Sempre que possível, use um mecanismo de ciclo de vida automatizado, como as políticas de ciclo de vida do Amazon S3 e o Amazon Data Lifecycle Manager, para configurar seus processos de retenção, arquivamento e expiração de dados. Para dados armazenados no DynamoDB, você pode usar o recurso Vida útil (TTL) para definir um carimbo de data/hora de expiração por item.

Diferencie os dados que estão disponíveis para uso e os dados armazenados como backup. Considere usar o AWS Backup para automatizar o backup de dados em todos os serviços da AWS. Os snapshots do Amazon EBS oferecem uma forma de copiar um volume do EBS e armazená-lo usando recursos do S3, incluindo ciclo de vida, proteção de dados e acesso a mecanismos de proteção. Dois desses mecanismos são o Bloqueio de Objetos do S3 e o AWS Backup Vault Lock, que podem fornecer segurança e controle adicionais sobre seus backups. Gerencie a separação clara de deveres e acesso para backups. Isole os backups no nível da conta para manter a separação do ambiente afetado durante um evento.

Outro aspecto do gerenciamento do ciclo de vida é registrar o histórico dos dados à medida que eles progridem em sua workload, o que é chamado de rastreamento da procedência dos dados. Desse modo, você pode ter certeza de que sabe de onde os dados vieram, quais transformações foram

realizadas, qual proprietário ou processo fez essas alterações e quando. Ter esse histórico ajuda a solucionar problemas e investigações durante possíveis eventos de segurança. Por exemplo, você pode registrar metadados sobre transformações em uma tabela do Amazon DynamoDB. Em um data lake, você pode manter cópias dos dados transformados em diferentes buckets do S3 para cada estágio do pipeline de dados. Armazene as informações do esquema e do carimbo de data/hora em um AWS Glue Data Catalog. Independentemente da sua solução, considere os requisitos dos usuários finais para determinar as ferramentas apropriadas e necessárias para oferecer um relatório sobre a procedência dos dados. Isso ajudará você a determinar a melhor forma de rastrear a procedência.

Etapas de implementação

1. Analise os tipos de dados, os níveis de confidencialidade e os requisitos de acesso da workload para classificar os dados e definir estratégias apropriadas de gerenciamento do ciclo de vida.
2. Projete e implemente políticas de retenção de dados e processos automatizados de destruição que se alinhem aos requisitos legais, regulatórios e organizacionais.
3. Estabeleça processos e automação para monitoramento, auditoria e ajuste contínuos de estratégias, controles e políticas de gerenciamento do ciclo de vida dos dados à medida que os requisitos e as regulamentações da workload evoluem.
   a. Detecte recursos que não têm o gerenciamento automatizado do ciclo de vida ativado com o AWS Config.

Recursos

Práticas recomendadas relacionadas:

- COST04-BP05 Impor políticas de retenção de dados
- SUS04-BP03 Usar políticas para gerenciar o ciclo de vida de conjuntos de dados

Documentos relacionados:

- Whitepaper Classificação de dados
- Esquema da AWS para defesa contra ransomware
- Orientação de DevOps: melhorar a rastreabilidade com o rastreamento da procedência de dados

Exemplos relacionados:

- Como proteger dados confidenciais durante todo o seu ciclo de vida na AWS
- Como construir linhagem de dados para data lakes usando o AWS Glue, o Amazon Neptune e o Spline

Ferramentas relacionadas:

- AWS Backup
- Amazon Data Lifecycle Manager
- AWS Identity and Access Management Access Analyzer

Proteção de dados em repouso

Os dados em repouso representam todos os dados mantidos no armazenamento não volátil por qualquer período na workload. Isso inclui armazenamento em bloco, armazenamento de objetos, bancos de dados, arquivos, dispositivos IoT e qualquer outro meio de armazenamento no qual os dados persistam. Proteger seus dados em repouso reduz o risco de acesso não autorizado quando a criptografia e os controles de acesso adequados são implementados.

Criptografia e tokenização são dois esquemas importantes, mas distintos, de proteção de dados.

Tokenização é um processo que permite definir um token para representar uma informação confidencial (por exemplo, o número do cartão de crédito de um cliente). Um token não deve ter um significado por si só nem deve ser derivado dos dados que ele tokeniza. Portanto, um resumo criptográfico não pode ser utilizado como um token. Ao definir cuidadosamente a abordagem de tokenização, você pode fornecer proteção adicional ao seu conteúdo e garantir o cumprimento dos requisitos de conformidade. Por exemplo, você pode reduzir o escopo de conformidade de um sistema de processamento de cartão de crédito se utilizar um token em vez de um número de cartão de crédito.

Criptografia é uma maneira de transformar o conteúdo de forma a torná-lo ilegível sem uma chave secreta para descriptografar o conteúdo novamente em texto sem formatação. Tanto a tokenização quanto a criptografia podem ser usadas para guardar e proteger as informações conforme apropriado. Além disso, o mascaramento é uma técnica que permite que parte dos dados seja editada até um ponto em que os dados restantes não são considerados confidenciais. Por exemplo, o PCI-DSS permite que os últimos quatro dígitos de um número de cartão sejam retidos fora do limite de escopo de conformidade para indexação.

Auditoria do uso de chaves de criptografia: entenda e faça a auditoria do uso de chaves de criptografia para confirmar se os mecanismos de controle de acesso nas chaves foram implementados adequadamente. Por exemplo, qualquer serviço da AWS que use uma chave do AWS KMS registra cada uso no AWS CloudTrail. Em seguida, você pode consultar o AWS CloudTrail usando uma ferramenta como o Amazon CloudWatch Logs Insights para garantir que todos os usos de suas chaves sejam válidos.

Práticas recomendadas

- SEC08-BP01 Implementar o gerenciamento seguro de chaves
- SEC08-BP02 Aplicar criptografia em repouso
- SEC08-BP03 Automatizar a proteção de dados em repouso
- SEC08-BP04 Aplicar controle de acesso

SEC08-BP01 Implementar o gerenciamento seguro de chaves

O gerenciamento seguro de chaves inclui o armazenamento, a rotação, o controle de acesso e o monitoramento do material essencial necessário para proteger os dados em repouso para sua workload.

Resultado desejado: um mecanismo de gerenciamento de chaves escalável, repetível e automatizado. O mecanismo impõe o acesso de privilégio mínimo ao material de chave e fornece o equilíbrio correto entre disponibilidade, confidencialidade e integridade das chaves. Você monitora o acesso às chaves e, se a rotação do material de chave for necessária, você as alterna usando um processo automatizado. Você não permite que o material de chave seja acessado por operadores humanos.

Práticas comuns que devem ser evitadas:

- Acesso humano a material de chave não criptografado.
- Criação de algoritmos criptográficos personalizados.
- Permissões excessivamente amplas para acessar materiais importantes.

Benefícios de implementar esta prática recomendada: ao estabelecer um mecanismo seguro de gerenciamento de chaves para sua workload, você pode ajudar a proteger seu conteúdo contra acesso não autorizado. Além disso, você pode estar sujeito a requisitos regulatórios para criptografar

seus dados. Uma solução eficaz de gerenciamento de chaves pode fornecer mecanismos técnicos alinhados a essas regulamentações para proteger o material das chaves.

Nível de risco exposto se esta prática recomendada não for estabelecida: Alto

Orientação para implementação

A criptografia de dados em repouso é um controle de segurança fundamental. Para implementar esse controle, a workload precisa de um mecanismo para armazenar e gerenciar com segurança o material de chave usado para criptografar os dados em repouso.

A AWS oferece o AWS Key Management Service (AWS KMS) para fornecer armazenamento durável, seguro e redundante para chaves do AWS KMS. Muitos serviços da AWS se integram ao AWS KMS para oferecer suporte à criptografia de seus dados. O AWS KMS usa módulos de segurança de hardware validados pelo FIPS 140-2 Nível 3 para proteger suas chaves. Não há mecanismo para exportar chaves do AWS KMS em texto simples.

Ao implantar workloads usando uma estratégia de várias contas, mantenha as chaves do AWS KMS na mesma conta da workload que as utiliza. Esse modelo distribuído deixa a responsabilidade pelo gerenciamento das chaves do AWS KMS com sua equipe. Em outros casos de uso, a organização pode optar por armazenar as chaves do AWS KMS em uma conta centralizada. Essa estrutura centralizada requer políticas adicionais para permitir o acesso entre contas necessário para que a conta da workload acesse as chaves armazenadas na conta centralizada, mas pode ser mais aplicável em casos de uso em que uma única chave é compartilhada entre várias Contas da AWS.

Independentemente de onde o material de chave esteja armazenado, você deve controlar rigorosamente o acesso à chave por meio de políticas de chave e políticas do IAM. Políticas de chave são a principal forma de controlar o acesso a uma chave do AWS KMS. Além disso, concessões à chave do AWS KMS podem fornecer acesso a serviços da AWS para criptografar e descriptografar dados em seu nome. Revise as orientações para controle de acesso às chaves do AWS KMS.

Monitore o uso de chaves de criptografia para detectar padrões de acesso incomuns. As operações realizadas usando chaves gerenciadas pela AWS e chaves gerenciadas pelo cliente armazenadas no AWS KMS podem ser registradas no AWS CloudTrail e devem ser revisadas periodicamente. Atenção especial ao monitoramento dos eventos de destruição de chaves. Para mitigar a destruição acidental ou maliciosa de material de chave, os eventos de destruição da chave não excluem o material da chave imediatamente. Tentativas de excluir chaves no AWS KMS estão sujeitas a um período de espera cujo padrão é 30 dias, com um mínimo de 7 dias, o que dá aos administradores tempo para revisar essas ações e reverter a solicitação, se necessário.

A maioria dos serviços da AWS usam o AWS KMS de forma transparente para você. Seu único requisito é decidir se quer usar uma chave gerenciada pela AWS ou gerenciada pelo cliente. Se a workload exigir o uso direto do AWS KMS para criptografar ou descriptografar dados, use a criptografia envelopada para proteger os dados. O SDK de criptografia da AWS pode fornecer primitivas de criptografia do lado do cliente às suas aplicações para implementar a criptografia envelopada e integrar com o AWS KMS.

Etapas de implementação

1. Determine as opções apropriadas de gerenciamento de chaves (gerenciadas pela AWS ou gerenciadas pelo cliente) para a chave.
   a. Para facilitar o uso, a AWS oferece, para a maioria dos serviços, chaves pertencentes à AWS e gerenciadas pela AWS que fornecem capacidade de criptografia em repouso sem a necessidade de gerenciar materiais ou políticas de chaves.
   b. Ao usar chaves gerenciadas pelo cliente, considere o armazenamento de chaves padrão para fornecer o melhor equilíbrio entre agilidade, segurança, soberania de dados e disponibilidade. Outros casos de uso podem exigir o uso de armazenamentos de chaves personalizadas com o AWS CloudHSM ou o repositório de chaves externo.
2. Analise a lista de serviços que você está usando para sua workload para entender como o AWS KMS se integra ao serviço. Por exemplo, as instâncias do EC2 podem usar volumes criptografados do EBS, verificando se os snapshots do Amazon EBS criados com base nesses volumes também são criptografados usando uma chave gerenciada pelo cliente e mitigando a divulgação acidental de dados de snapshots não criptografados.
   a. Como os serviços da AWS usam o AWS KMS
   b. Para obter informações detalhadas sobre as opções de criptografia oferecidas por um serviço da AWS, consulte o tópico Criptografia em repouso no manual do usuário ou no Guia do desenvolvedor do serviço.
3. Implemente o AWS KMS: o AWS KMS simplifica a criação e o gerenciamento de chaves e o controle do uso da criptografia em uma ampla variedade de serviços da AWS e em suas aplicações.
   a. Conceitos básicos: AWS Key Management Service (AWS KMS)
   b. Reserve tempo para analisar as práticas recomendadas para controle de acesso às suas chaves do AWS KMS.
4. Considere o SDK de criptografia da AWS: use a integração do SDK de criptografia da AWS com o AWS KMS quando sua aplicação precisar criptografar dados do lado do cliente.

   a. SDK de criptografia da AWS
5. Habilite o IAM Access Analyzer para revisar e notificar automaticamente se houver políticas de chaves do AWS KMS excessivamente amplas.
   a. Considere usar verificações de políticas personalizadas para verificar se uma atualização da política de recursos não concede acesso público às chaves KMS.
6. Habilite o Security Hub para receber notificações se houver políticas de chaves configuradas incorretamente, chaves agendadas para exclusão ou chaves sem a rotação automática ativada.
7. Determine o nível de registro em log apropriado para suas chaves do AWS KMS. Como as chamadas para o AWS KMS, incluindo eventos somente para leitura, são registradas em log, os logs do CloudTrail associados ao AWS KMS podem se tornar volumosos.
   a. Algumas organizações preferem registrar a atividade de log do AWS KMS em uma trilha separada. Para obter mais detalhes, consulte a seção Registrar em log as chamadas de API do AWS KMS com o CloudTrail do Guia do desenvolvedor do AWS KMS.

Recursos

Documentos relacionados:

- AWS Key Management Service
- Ferramentas e serviços criptográficos da AWS
- Proteção de dados do Amazon S3 usando criptografia
- Criptografia de envelope
- Promessa de soberania digital
- Desmistificação das operações de chave do AWS KMS, traga sua própria chave, armazenamento de chaves personalizado e portabilidade de texto cifrado
- Detalhes criptográficos do AWS Key Management Service

Vídeos relacionados:

- Como funciona a criptografia na AWS
- Como proteger seu armazenamento em bloco na AWS
- Proteção de dados na AWS: usar bloqueios, chaves, assinaturas e certificados

Exemplos relacionados:

- Implemente mecanismos avançados de controle de acesso usando o AWS KMS

SEC08-BP02 Aplicar criptografia em repouso

Criptografe os dados privados em repouso para manter a confidencialidade e oferecer uma camada adicional de proteção contra a divulgação e exfiltração acidentais dos dados. A criptografia protege os dados para que não possam ser lidos nem acessados sem ser descriptografados primeiro. Faça o inventário e controle dados não criptografados para mitigar os riscos associados à exposição de dados.

Resultado desejado: é possível ter mecanismos que criptografam os dados privados por padrão quando em repouso. Esses mecanismos ajudam a manter a confidencialidade dos dados e oferecem uma camada adicional de proteção contra a divulgação ou exfiltração não intencional dos dados. Você mantém um inventário de dados não criptografados e compreende os controles que existem para protegê-los.

Práticas comuns que devem ser evitadas:

- Não utilizar configurações de criptografia por padrão.
- Conceder acesso excessivamente permissivo para chaves de descriptografia.
- Não monitorar o uso de chaves de criptografia e descriptografia.
- Armazenar dados não criptografados.
- Utilizar a mesma chave de criptografia para todos os dados, seja qual for o uso, os tipos e a classificação de dados.

Nível de risco exposto se esta prática recomendada não for estabelecida: Alto

Orientação para implementação

Mapeie as chaves de criptografia às classificações de dados em suas workloads. Essa abordagem ajuda a proteger contra o acesso excessivamente permissivo ao usar uma única chave de criptografia ou um número muito pequeno de chaves de criptografia para seus dados (consulte SEC07-BP01 Compreender seu esquema de classificação de dados).

O AWS Key Management Service (AWS KMS) integra-se a muitos serviços da AWS para facilitar a criptografia de seus dados em repouso. Por exemplo, no Amazon Elastic Compute Cloud (Amazon

EC2), é possível definir a criptografia padrão nas contas para que os novos volumes do EBS sejam criptografados automaticamente. Ao utilizar o AWS KMS, considere o nível de restrição necessário para os dados. Chaves do AWS KMS controladas por serviço e padrão são gerenciadas e utilizadas em seu nome pelo AWS. Para dados sigilosos que exijam acesso refinado à chave de criptografia subjacente, considere chaves gerenciadas pelo cliente (CMKs). Você tem total controle sobre as CMKs, como gerenciamento de rotação e acesso pelo uso de políticas de chave.

Além disso, serviços como o Amazon Simple Storage Service (Amazon S3) agora criptografam todos os novos objetos por padrão. Essa implementação fornece segurança aprimorada sem impacto no desempenho.

Outros serviços, como o Amazon Elastic Compute Cloud (Amazon EC2) ou o Amazon Elastic File System (Amazon EFS), oferecem suporte às configurações de criptografia padrão. Você também pode usar o Regras do AWS Config para verificar automaticamente se está usando criptografia para volumes do Amazon Elastic Block Store (Amazon EBS), instâncias do Amazon Relational Database Service (Amazon RDS), buckets do Amazon S3 e outros serviços na organização.

A AWS também oferece operações de criptografia do lado do cliente, possibilitando que você criptografe os dados antes de fazer seu upload para a nuvem. O AWS Encryption SDK fornece uma maneira de criptografar seus dados usando criptografia envelopada. Você fornece a chave de encerramento e o AWS Encryption SDK gera uma chave de dados exclusiva para cada objeto de dados que ele criptografa. Considere utilizar o AWS CloudHSM se precisar de um módulo de segurança de hardware de um locatário (HSM) gerenciado. O AWS CloudHSM possibilita gerar, importar e gerenciar chaves criptográficas em um HSM validado de nível 3 FIPS 140-2. Alguns casos de uso do AWS CloudHSM incluem proteger chaves privadas para emitir uma autoridade de certificado (CA) e ativar a criptografia de dados transparente (TDE) para bancos de dados Oracle. O AWS CloudHSM Client SDK oferece software que possibilita criptografar dados do lado do cliente com chaves armazenadas no AWS CloudHSM antes de fazer upload de seus dados para AWS. O Amazon DynamoDB Encryption Client também possibilita criptografar e assinar itens antes de fazer upload para uma tabela do DynamoDB.

Etapas de implementação

- Configure a criptografia padrão para novos volumes do Amazon EBS: especifique que você deseja que todos os volumes do Amazon EBS recém-criados sejam criados em formato criptografado, com a opção de usar a chave padrão fornecida pela AWS ou uma chave que você criar.
- Configure imagens de máquina da Amazon (AMIs) criptografadas: copiar uma AMI existente com a criptografia configurada criptografará automaticamente os volumes raiz e snapshots.

- Configure a criptografia do Amazon RDS: configure a criptografia para seus clusters de banco de dados do Amazon RDS e snapshots em repouso usando a opção de criptografia.
- Crie e configure chaves do AWS KMS com políticas que limitam o acesso das entidades principais apropriadas para cada classificação de dados: por exemplo, crie uma chave do AWS KMS para criptografar dados de produção e uma chave diferente para criptografar dados de desenvolvimento ou teste. Você também pode conceder acesso de chave a outras Contas da AWS. Considere ter contas diferentes para seus ambientes de desenvolvimento e produção. Se seu ambiente de produção precisar descriptografar artefatos na conta de desenvolvimento, você poderá editar a política de CMK utilizada para criptografar os artefatos de desenvolvimento a fim de conferir à conta de produção a capacidade de descriptografar esses artefatos. O ambiente de produção pode, então, ingerir os dados descriptografados para uso na produção.
- Configure a criptografia em serviços da AWS adicionais: para outros serviços da AWS que você usa, revise a documentação de segurança desse serviço para determinar as opções de criptografia do serviço.

Recursos

Documentos relacionados:

- AWS Crypto Tools
- AWS Encryption SDK
- Whitepaper Detalhes criptográficos do AWS KMS
- AWS Key Management Service
- Ferramentas e serviços criptográficos da AWS
- Criptografia do Amazon EBS
- Criptografia padrão para volumes do Amazon EBS
- Como criptografar recursos do Amazon RDS
- Como faço para habilitar a criptografia padrão em um bucket do Amazon S3?
- Proteção de dados do Amazon S3 usando criptografia

Vídeos relacionados:

- Como funciona a criptografia na AWS
- Como proteger seu armazenamento em bloco na AWS

SEC08-BP03 Automatizar a proteção de dados em repouso

Use a automação para validar e aplicar controles de dados em repouso. Use a verificação automatizada para detectar configurações incorretas de soluções de armazenamento de dados e realize correções por meio de resposta programática automatizada sempre que possível. Incorpore a automação nos processos de CI/CD para detectar configurações incorretas de armazenamento de dados antes que elas sejam implantadas na produção.

Resultado desejado: sistemas automatizados examinam e monitoram os locais de armazenamento de dados em busca de configurações incorretas de controles, acesso não autorizado e uso inesperado. A detecção de locais de armazenamento configurados incorretamente inicia correções automatizadas. Processos automatizados criam backups de dados e armazenam cópias imutáveis fora do ambiente original.

Práticas comuns que devem ser evitadas:

- Não considerar as opções para habilitar as configurações de criptografia por padrão, onde compatíveis.
- Não considerar eventos de segurança, além dos eventos operacionais, ao formular uma estratégia automatizada de backup e recuperação.
- Não impor configurações de acesso público para serviços de armazenamento.
- Não monitorar e auditar os controles para proteger os dados em repouso.

Benefícios de implementar esta prática recomendada: a automação ajuda a evitar o risco de configuração incorreta dos locais de armazenamento de dados. Isso ajuda a evitar que configurações incorretas entrem nos ambientes de produção. Essa prática recomendada também ajuda a detectar e corrigir configurações incorretas, caso elas ocorram.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

A automação é um tema em todas as práticas para proteger os dados em repouso. SEC01-BP06 Automatizar a implantação de controles de segurança padrão descreve como é possível capturar a configuração de seus recursos usando modelos de infraestrutura como código (IaC), como o AWS CloudFormation. Esses modelos estão comprometidos com um sistema de controle de versão e são usados para implantar recursos da AWS por meio de um pipeline de CI/CD. Essas técnicas

também se aplicam à automação da configuração de soluções de armazenamento de dados, como configurações de criptografia em buckets do Amazon S3.

Você pode verificar as configurações definidas nos modelos de IaC para verificar se há erros de configuração nos pipelines de CI/CD usando regras no AWS CloudFormation Guard. Você pode monitorar configurações que ainda não estão disponíveis no CloudFormation ou em outras ferramentas de IaC em busca de configurações incorretas com AWS Config. Os alertas que o Config gera para configurações incorretas podem ser corrigidos automaticamente, conforme descrito em SEC04-BP04 Iniciar a correção de recursos fora de conformidade.

Usar a automação como parte da estratégia de gerenciamento de permissões também é um componente essencial das proteções de dados automatizadas. SEC03-BP02 Conceder acesso de privilégio mínimo e SEC03-BP04 Reduzir permissões continuamente descrevem a configuração de políticas de acesso de privilégio mínimo que são continuamente monitoradas pelo AWS Identity and Access Management Access Analyzer para gerar descobertas quando a permissão pode ser reduzida. Além da automação para monitoramento de permissões, é possível configurar o Amazon GuardDuty para observar comportamentos anômalos de acesso aos dados em seus volumes do EBS (por meio de uma instância do EC2), buckets do S3 e bancos de dados do Amazon Relational Database Service compatíveis.

A automação também desempenha um papel para detectar o armazenamento de dados confidenciais em locais não autorizados. SEC07-BP03 Automatizar a identificação e a classificação descreve como o Amazon Macie pode monitorar seus buckets do S3 em busca de dados confidenciais inesperados e gerar alertas que podem iniciar uma resposta automática.

Siga as práticas de REL09 Backup de dados para desenvolver uma estratégia automatizada de backup e recuperação de dados. O backup e a recuperação de dados são importantes para a recuperação tanto de eventos de segurança quanto de eventos operacionais.

Etapas de implementação

1. Capture a configuração de armazenamento de dados em modelos de IaC. Use verificações automatizadas nos pipelines de CI/CD para detectar configurações incorretas.
   a. É possível usar para AWS CloudFormation seus modelos de IaC e o AWS CloudFormation Guard para verificar se há erros de configuração nos modelos.
   b. Use o AWS Config para executar regras em um modo de avaliação proativa. Use essa configuração como uma etapa em seu pipeline de CI/CD para verificar a conformidade de um recurso antes de criá-lo.
2. Monitore os recursos em busca de configurações incorretas de armazenamento de dados.

   a. Configure o AWS Config para monitorar os recursos de armazenamento de dados em busca de alterações nas configurações de controle e gerar alertas para invocar ações de remediação ao detectar uma configuração incorreta.
   b. Consulte SEC04-BP04 Iniciar a correção para recursos fora de conformidade para obter mais orientações sobre correções automatizadas.
3. Monitore e reduza continuamente as permissões de acesso aos dados por meio da automação.
   a. O IAM Access Analyzer pode ser executado continuamente para gerar alertas quando as permissões podem ser potencialmente reduzidas.
4. Monitore e emita alertas sobre comportamentos anômalos de acesso aos dados.
   a. O GuardDuty observa tanto as assinaturas de ameaças conhecidas quanto os desvios dos comportamentos de acesso básicos para recursos de armazenamento de dados, como volumes do EBS, buckets do S3 e bancos de dados do RDS.
5. Monitore e emita alertas sobre dados confidenciais armazenados em locais inesperados.
   a. Use o Amazon Macie para examinar continuamente seus buckets do S3 em busca de dados confidenciais.
6. Automatize backups seguros e criptografados dos dados.
   a. O AWS Backupé um serviço gerenciado que cria backups criptografados e seguros de várias fontes de dados na AWS. O Elastic Disaster Recovery permite copiar workloads completas do servidor e manter a proteção contínua dos dados com um objetivo de ponto de recuperação (RPO) medido em segundos. Você pode configurar os dois serviços para que funcionem juntos e automatizem a criação de backups de dados e os copiem para locais de failover. Isso pode ajudar a manter os dados disponíveis quando eles forem afetados por eventos operacionais ou de segurança.

Recursos

Práticas recomendadas relacionadas:

- SEC01-BP06 Automatizar a implantação de controles de segurança padrão
- SEC03-BP02 Conceder acesso de privilégio mínimo
- SEC03-BP04 Reduzir as permissões continuamente
- SEC04-BP04 Iniciar a correção de recursos fora de conformidade
- SEC07-BP03 Automatizar a identificação e a classificação
- REL09-BP02 Proteger e criptografar backups

- REL09-BP03 Fazer backup de dados automaticamente

Documentos relacionados:

- Recomendação da AWS: Criptografar automaticamente volumes novos e existentes do Amazon EBS
- Gerenciamento de riscos de ransomware na AWS usando o CSF (Cyber Security Framework) do NIST

Exemplos relacionados:

- Como usar regras proativas do AWS Config e hooks do AWS CloudFormation proativos para evitar a criação de recursos de nuvem fora de conformidade
- Automatizar e gerenciar centralmente a proteção de dados para o Amazon S3 com o AWS Backup
- AWS re:Invent 2023: Implementar proteção proativa de dados usando snapshots do Amazon EBS
- AWS re:Invent 2022: Criar e automatizar para alcançar resiliência com proteção de dados moderna

Ferramentas relacionadas:

- AWS CloudFormation Guard
- Registro de regras do AWS CloudFormation Guard
- IAM Access Analyzer
- Amazon Macie
- AWS Backup
- Elastic Disaster Recovery

SEC08-BP04 Aplicar controle de acesso

Para ajudar a proteger os dados em repouso, implemente o controle de acesso utilizando mecanismos como isolamento e versionamento. Aplique o privilégio mínimo e os controles de acesso condicional. Evite conceder acesso público aos seus dados.

Resultado desejado: você verifica se somente usuários autorizados podem acessar os dados com base na necessidade real de acesso. Você protege os dados com backups regulares e versionamento a fim de impedir a modificação ou exclusão de dados de maneira intencional ou

acidental. Você isola os dados críticos dos outros dados a fim de proteger a confidencialidade e a integridade desses dados.

Práticas comuns que devem ser evitadas:

- Armazenar dados com requisitos de confidencialidade ou classificações diferentes juntos.
- Utilizar permissões excessivamente tolerantes em chaves de descriptografia.
- Classificar dados de modo inadequado.
- Não reter backups detalhados de dados importantes.
- Conceder acesso persistente a dados de produção.
- Não auditar o acesso aos dados nem rever as permissões regularmente.

Nível de risco exposto se esta prática recomendada não for estabelecida: Alto

Orientação para implementação

Proteger dados em repouso é importante para manter a integridade, a confidencialidade e a conformidade dos dados com os requisitos normativos. Você pode implementar vários controles para ajudar a conseguir isso, incluindo controle de acesso, isolamento, acesso condicional e versionamento.

Você pode aplicar o controle de acesso com o princípio do privilégio mínimo, que fornece somente as permissões necessárias aos usuários e serviços para realizar suas tarefas. Isso inclui acesso às chaves de criptografia. Revise suas políticas do AWS Key Management Service (AWS KMS) para verificar se o nível de acesso concedido é apropriado e se as condições relevantes se aplicam.

Você pode separar dados com base em diferentes níveis de classificação usando Contas da AWS distintas para cada nível e gerenciar essas contas usando o AWS Organizations. Esse isolamento pode ajudar a impedir o acesso não autorizado e minimizar o risco de exposição de dados.

Revise regularmente o nível de acesso concedido em políticas de bucket do S3. Evite buckets que possam ser lidos ou gravados publicamente, a menos que seja absolutamente necessário. Considere usar o AWS Config para detectar buckets disponíveis publicamente e o Amazon CloudFront para fornecer conteúdo do Amazon S3. Garanta que os buckets que não devem permitir acesso público sejam configurados adequadamente para evitá-lo.

Implemente mecanismos de versionamento e bloqueio de objetos para dados críticos armazenados no Amazon S3. O versionamento do Amazon S3 preserva as versões anteriores dos objetos para

recuperar dados de exclusões ou substituições acidentais. A funcionalidade Bloqueio de Objetos do Amazon S3 fornece controle de acesso obrigatório para objetos, o que impede que eles sejam excluídos ou substituídos, mesmo pelo usuário-raiz, até que o bloqueio expire. Além disso, o Amazon S3 Glacier Vault Lock oferece um recurso semelhante para arquivos armazenados no Amazon S3 Glacier.

Etapas de implementação

1. Imponha o controle de acesso com o princípio de privilégio mínimo:
    - Analise as permissões de acesso concedidas aos usuários e serviços e verifique se eles têm somente as permissões necessárias para realizar suas tarefas.
    - Revise o acesso às chaves de criptografia verificando as políticas do AWS Key Management Service (AWS KMS).
2. Separe dados com base em diferentes níveis de classificação:
    - Use Contas da AWS distintas para cada nível de classificação de dados.
    - Gerencie essas contas usando o AWS Organizations.
3. Revise as permissões de buckets e objetos do Amazon S3:
    - Revise regularmente o nível de acesso concedido em políticas de bucket do S3.
    - Evite buckets que possam ser lidos ou gravados publicamente, a menos que seja absolutamente necessário.
    - Considere usar o AWS Config para detectar buckets disponíveis publicamente.
    - Use o Amazon CloudFront para fornecer conteúdo do Amazon S3.
    - Garanta que os buckets que não devem permitir acesso público sejam configurados adequadamente para evitá-lo.
    - Você pode aplicar o mesmo processo de revisão para bancos de dados e qualquer outra fonte de dados que use a autenticação do IAM, como SQS ou armazenamentos de dados de terceiros.
4. Use o AWS IAM Access Analyzer:
    - É possível usar o AWS IAM Access Analyzer para analisar buckets do Amazon S3 e gerar descobertas quando uma política do S3 concede acesso a uma entidade externa.
5. Implemente mecanismos de versionamento e bloqueio de objetos:
    - Use o versionamento do Amazon S3 para preservar as versões anteriores dos objetos, o que permite a recuperação de exclusões ou substituições acidentais.

- Use a funcionalidade Bloqueio de Objetos do Amazon S3 para fornecer controle de acesso obrigatório para objetos, o que impede que eles sejam excluídos ou substituídos, mesmo pelo usuário-raiz, até que o bloqueio expire.
- Use o Amazon S3 Glacier Vault Lock para arquivos armazenados no Amazon S3 Glacier.

6. Use o Inventário Amazon S3:
   - Você pode usar o Inventário Amazon S3 para auditar e gerar relatórios sobre o status de replicação e criptografia dos objetos do S3.
7. Revise as permissões de compartilhamento do Amazon EBS e da AMI:
   - Revise as permissões de compartilhamento para o Amazon EBS e para compartilhamento de AMIs a fim de verificar que as imagens e os volumes não são compartilhados com Contas da AWS externas à sua workload.
8. Revise os compartilhamentos do AWS Resource Access Manager periodicamente:
   - Você pode usar o AWS Resource Access Manager para compartilhar recursos, como políticas do AWS Network Firewall, regras do Amazon Route 53 Resolver e sub-redes em suas Amazon VPCs.
   - Faça auditoria em recursos compartilhados regularmente e interrompa o compartilhamento dos que não precisam mais ser compartilhados.

Recursos

Práticas recomendadas relacionadas:

- SEC03-BP01 Definir requisitos de acesso
- SEC03-BP02 Conceder acesso de privilégio mínimo

Documentos relacionados:

- Whitepaper Detalhes criptográficos do AWS KMS
- Introdução ao gerenciamento de permissões de acesso aos recursos do Amazon S3
- Visão geral do gerenciamento de acesso a recursos do AWS KMS
- Regras do AWS Config
- Amazon S3 + Amazon CloudFront: uma combinação feita na nuvem
- Usar versionamento

- Bloquear objetos usando o bloqueio de objetos do Amazon S3
- Compartilhar um snapshot do Amazon EBS
- AMIs compartilhadas
- Hospedar uma aplicação de página única no Amazon S3
- Chaves de condições globais da AWS
- Como criar um perímetro de dados na AWS

Vídeos relacionados:

- Como proteger seu armazenamento em bloco na AWS

Proteção de dados em trânsito

Os dados em trânsito são quaisquer dados enviados de um sistema para outro. Isso inclui a comunicação entre recursos em sua workload, bem como a comunicação entre outros serviços e seus usuários finais. Ao fornecer o nível apropriado de proteção para os dados em trânsito, você protege a confidencialidade e a integridade dos dados da sua workload.

Proteja dados entre a VPC ou locais on-premises: o AWS PrivateLink pode ser usado para criar uma conexão de rede segura e privada entre a Amazon Virtual Private Cloud (Amazon VPC) ou conectividade on-premises com serviços hospedados na AWS. Você pode acessar serviços da AWS, serviços de terceiros e serviços em outros Contas da AWS como se estivessem em sua rede privada. Com o AWS PrivateLink, você pode acessar serviços em contas com CIDRs IP sobrepostos sem precisar de um gateway da Internet ou NAT. Também não é necessário configurar regras de firewall, definições de caminhos ou tabelas de rotas. O tráfego permanece no backbone da Amazon e não atravessa a Internet. Portanto, seus dados estão protegidos. Você pode manter a conformidade com as regulamentações de conformidade específicas do setor, como HIPAA e EU/US Privacy Shield. O AWS PrivateLink funciona perfeitamente com soluções de terceiros para criar uma rede global simplificada, permitindo que você acelere sua migração para a nuvem e usufrua dos serviços da AWS disponíveis.

Práticas recomendadas

- SEC09-BP01 Implementar o gerenciamento seguro de chaves e certificados
- SEC09-BP02 Impor a criptografia em trânsito
- SEC09-BP03 Autenticar as comunicações de rede

SEC09-BP01 Implementar o gerenciamento seguro de chaves e certificados

Os certificados Transport Layer Security (TLS) são usados para proteger as comunicações de rede e estabelecer a identidade de sites, recursos e workloads na Internet, bem como em redes privadas.

Resultado desejado: um sistema seguro de gerenciamento de certificados que pode provisionar, implantar, armazenar e renovar certificados em uma infraestrutura de chave pública (PKI). Um mecanismo seguro de gerenciamento de chaves e certificados evita que o material da chave privada do certificado seja divulgado e renova automaticamente o certificado periodicamente. Ele também se integra a outros serviços para fornecer comunicações de rede seguras e identidade para os recursos da máquina na workload. O material da chave nunca deve estar acessível para identidades humanas.

Práticas comuns que devem ser evitadas:

- Executar etapas manuais durante os processos de implantação ou renovação de certificados.
- Não prestar a devida atenção à hierarquia da autoridade de certificação (CA) ao criar uma CA privada.
- Usar certificados autoassinados para recursos públicos.

Benefícios de implementar esta prática recomendada:

- Simplificar o gerenciamento de certificados por meio de implantação e renovação automatizadas.
- Incentivar a criptografia de dados em trânsito usando certificados TLS.
- Aumentar a segurança e a auditabilidade das ações de certificação realizadas pela autoridade de certificação.
- Organizar as tarefas de gerenciamento em diferentes camadas da hierarquia da CA.

Nível de risco exposto se esta prática recomendada não for estabelecida: Alto

Orientação para implementação

As workloads modernas fazem uso extensivo de comunicações de rede criptografadas usando protocolos de PKI, como TLS. O gerenciamento de certificados PKI pode ser complexo, mas o provisionamento, a implantação e a renovação automatizados de certificados podem reduzir o atrito associado ao gerenciamento deles.

A AWS oferece dois serviços para gerenciar certificados de PKI de uso geral: AWS Certificate Manager e AWS Private Certificate Authority (AWS Private CA). O ACM é o principal serviço usado pelos clientes para provisionar, gerenciar e implantar certificados para uso em workloads públicas e privadas da AWS. O ACM emite certificados privados usando o AWS Private CA e se integra a muitos outros serviços gerenciados pela AWS para fornecer certificados TLS seguros para workloads. O ACM também pode emitir certificados publicamente confiáveis do Amazon Trust Services. Os certificados públicos do ACM podem ser usados em workloads públicas, pois navegadores e sistemas operacionais modernos confiam nesses certificados por padrão.

A AWS Private CA permite estabelecer a própria autoridade de certificação raiz ou subordinada e emitir certificados TLS por meio de uma API. É possível usar esses tipos de certificado em cenários em que você controla e gerencia a cadeia de confiança do lado do cliente da conexão TLS. Além dos casos de uso do TLS, a AWS Private CA pode ser usada para emitir certificados para pods do Kubernetes, atestados de produtos de dispositivos Matter, assinatura de código e outros casos de uso com um modelo personalizado. Também é possível usar o IAM Roles Anywhere para fornecer credenciais do IAM temporárias para workloads on-premises que receberam certificados X.509 assinados pela CA privada.

Além do ACM e AWS Private CA, o AWS IoT Core fornece suporte especializado para provisionamento, gerenciamento e implantação de certificados PKI em dispositivos de IoT. O AWS IoT Core fornece mecanismos especializados para integrar dispositivos de IoT em sua infraestrutura de chave pública em escala.

Alguns serviços da AWS, como o Amazon API Gateway e o Elastic Load Balancing, oferecem recursos próprios para usar certificados para proteger conexões de aplicações. Por exemplo, tanto o API Gateway quanto o Application Load Balancer (ALB) oferecem suporte a TLS mútuo (mTLS) usando certificados de cliente que você cria e exporta usando o AWS Management Console, a CLI ou as APIs.

Considerações para estabelecer uma hierarquia de CA privada

Quando é necessário estabelecer uma CA privada, é importante tomar cuidado especial para projetar adequadamente a hierarquia da CA com antecedência. É prática recomendada implantar cada nível de sua hierarquia de CA em Contas da AWS separadas ao criar uma hierarquia de CA privada. Essa etapa intencional reduz a área de superfície de cada nível na hierarquia da CA, simplificando a descoberta de anomalias nos dados de log do CloudTrail e reduzindo o escopo de acesso ou impacto se houver acesso não autorizado a uma das contas. A CA raiz deve residir em uma própria conta separada e deve ser usada somente para emitir um ou mais certificados de CA intermediários.

Depois, crie uma ou mais CAs intermediárias em contas separadas da conta da CA raiz para emitir certificados para usuários finais, dispositivos ou outras workloads. Por fim, emita certificados da CA raiz para as CAs intermediárias, que, por sua vez, emitirão certificados para os usuários finais ou dispositivos. Para obter mais informações sobre como planejar a implantação de CA e projetar a hierarquia de CA, incluindo planejamento de resiliência, replicação entre regiões, compartilhamento de CAs na organização e muito mais, consulte Planejar sua implantação da AWS Private CA.

Etapas de implementação

1. Determine os serviços da AWS relevantes e necessários para seu caso de uso:
   - Muitos casos de uso podem aproveitar a infraestrutura de chave pública da AWS existente usando o AWS Certificate Manager. O ACM pode ser usado para implantar certificados TLS para servidores Web, balanceadores de carga ou outros usos para certificados publicamente confiáveis.
   - Considere o AWS Private CA quando precisar estabelecer a própria hierarquia de autoridade de certificação privada ou precisar acessar certificados exportáveis. O ACM pode então ser usado para emitir vários tipos de certificados de entidade final utilizando a AWS Private CA.
   - Para casos de uso em que os certificados devem ser provisionados em grande escala para dispositivos incorporados de Internet das Coisas (IoT), considere usar o AWS IoT Core.
   - Considere usar a funcionalidade nativa do mTLS em serviços como Amazon API Gateway ou Application Load Balancer.
2. Implemente a renovação automática do certificado sempre que possível:
   - Use a renovação gerenciada pelo ACM para certificados emitidos pelo ACM junto com serviços gerenciados da AWS integrados.
3. Estabeleça trilhas de auditoria e registro em log:
   - Habilite os Logs do CloudTrail para monitorar o acesso às contas que detêm autoridades de certificação. Considere configurar a validação da integridade do arquivo de log no CloudTrail para verificar a autenticidade dos dados de log.
   - Gere e revise periodicamente relatórios de auditoria que listam os certificados que sua CA privada emitiu e revogou. Esses relatórios podem ser exportados para um bucket do S3.
   - Ao implantar uma CA privada, você também precisará estabelecer um bucket do S3 para armazenar a lista de revogação de certificados (CRL). Para obter orientação sobre como configurar esse bucket do S3 com base nos requisitos da workload, consulte Planejar uma lista de revogação de certificados (CRL).

Recursos

Práticas recomendadas relacionadas:

- SEC02-BP02 Usar credenciais temporárias
- SEC08-BP01 Implementar o gerenciamento seguro de chaves
- SEC09-BP03 Autenticar as comunicações de rede

Documentos relacionados:

- Como hospedar e gerenciar toda uma infraestrutura de certificados privados na AWS
- Como proteger uma hierarquia de CA privada do ACM em escala empresarial para o setor automotivo e de manufatura
- Práticas recomendadas de CA privada
- Como usar o AWS RAM para compartilhar sua CA privada do ACM entre contas

Vídeos relacionados:

- Como ativar a CA privada do AWS Certificate Manager (workshop)

Exemplos relacionados:

- Workshop de CA privada
- Workshop de gerenciamento de dispositivos IoT (incluindo provisionamento de dispositivos)

Ferramentas relacionadas:

- Plug-in para o gerenciador de certificados do Kubernetes para uso da AWS Private CA

SEC09-BP02 Impor a criptografia em trânsito

Aplique os requisitos de criptografia definidos com base em políticas, obrigações regulatórias e padrões da organização para cumprir os requisitos organizacionais, legais e de conformidade. Utilize somente protocolos com criptografia ao transmitir dados sigilosos para fora da sua nuvem privada virtual (VPC). A criptografia ajuda a manter a confidencialidade dos dados mesmo quando os dados passam por redes não confiáveis.

Resultado desejado: criptografe o tráfego de rede entre os recursos e a internet para reduzir o acesso não autorizado aos dados. Você criptografa o tráfego de rede no ambiente interno da AWS de acordo com seus requisitos de segurança. Você criptografa dados em trânsito usando protocolos TLS seguros e pacotes de cifras.

Práticas comuns que devem ser evitadas:

- Utilizar versões obsoletas de SSL, TLS e componentes do pacote de criptografia (por exemplo, SSL v3.0, chaves RSA de 1024 bits e criptografia RC4).
- Permitir tráfego não criptografado (HTTP) para ou de recursos voltados para o público.
- Não monitorar e substituir certificados X.509 antes da validade.
- Utilizar certificados X.509 autoassinados para TLS.

Nível de risco exposto se esta prática recomendada não for estabelecida: Alto

Orientação para implementação

Os serviços da AWS fornecem endpoints HTTPS usando TLS para comunicação, fornecendo criptografia em trânsito quando se comunicam com as APIs da AWS. Protocolos HTTP não seguros podem ser auditados e bloqueados em uma nuvem privada virtual (VPC) por meio do uso de grupos de segurança. As solicitações HTTP também podem ser redirecionadas automaticamente para HTTPS no Amazon CloudFront ou em um Application Load Balancer. Você pode usar uma política de bucket do Amazon Simple Storage Service (Amazon S3) para restringir a capacidade de fazer upload de objetos via HTTP, impondo efetivamente o uso de HTTPS para uploads de objetos nos buckets. Você tem controle total sobre seus recursos de computação para implementar a criptografia em trânsito em seus serviços. Além disso, você pode usar a conectividade de VPN em sua VPC a partir de uma rede externa ou do AWS Direct Connect para facilitar a criptografia do tráfego. Verifique se os clientes fazem chamadas para APIs da AWS usando pelo menos o TLS 1.2, já que a AWS descontinuou o uso de versões anteriores do TLS em fevereiro de 2024. Recomendamos usar o TLS 1.3. Se você tiver requisitos especiais para criptografia em trânsito, poderá encontrar soluções de terceiros disponíveis noAWS Marketplace.

Etapas de implementação

- Aplique a criptografia em trânsito: os requisitos de criptografia definidos devem se basear nos mais recentes padrões e práticas recomendadas e permitir apenas protocolos seguros. Por exemplo, configure um grupo de segurança para permitir o protocolo HTTPS apenas para a um Application Load Balancer ou instância do Amazon EC2.

- Configure protocolos seguros em serviços de borda: configure o HTTPS com o Amazon CloudFront e use um perfil de segurança apropriado para sua postura de segurança e caso de uso.
- Use uma VPN para conectividade externa: considere usar uma VPN IPsec para proteger conexões ponto a ponto ou rede a rede para ajudar a garantir a privacidade e a integridade dos dados.
- Configure protocolos seguros em balanceadores de carga: selecione uma política de segurança que forneça os pacotes de criptografia mais fortes compatíveis pelos clientes que se conectarão ao receptor. Crie um receptor HTTPS para seu Application Load Balancer.
- Configure protocolos seguros no Amazon Redshift: configure seu cluster para exigir uma conexão Secure Socket Layer (SSL) ou Transport Layer Security (TLS).
- Configure protocolos seguros: revise a documentação do serviço da AWS para determinar os recursos de criptografia em trânsito.
- Configure o acesso seguro ao fazer o upload para buckets do Amazon S3: use os controles de política do bucket do Amazon S3 para impor o acesso seguro aos dados.
- Considere usar o AWS Certificate Manager: o ACM permite que você provisione, gerencie e implante certificados TLS públicos para uso com serviços da AWS.
- Considere usar o AWS Private Certificate Authoritypara necessidades de PKI privado: a AWS Private CA permite criar hierarquias de autoridade de certificação (CA) privada para emitir certificados X.509 de entidade final que podem ser usados para criar canais TLS criptografados.

Recursos

Documentos relacionados:

- Usar HTTPS com o CloudFront
- Conectar sua VPC a redes remotas usando a AWS Virtual Private Network
- Criar um receptor HTTPS para seu Application Load Balancer
- Tutorial: configurar o SSL/TLS no Amazon Linux 2
- Usar SSL/TLS para criptografar uma conexão com uma instância de um banco de dados
- Configurar as opções de segurança para conexões

SEC09-BP03 Autenticar as comunicações de rede

Verifique a identidade das comunicações usando protocolos que oferecem suporte à autenticação, como Transport Layer Security (TLS) ou IPsec.

Projete a workload para usar protocolos de rede seguros e autenticados sempre que uma comunicação entre serviços, aplicações ou usuários for feita. O uso de protocolos de rede compatíveis com a autenticação e a autorização fornece maior controle sobre os fluxos de rede e reduz o impacto causado por acessos não autorizados.

Resultado desejado: uma workload com fluxos de tráfego de plano de dados e ambiente de gerenciamento bem definidos entre os serviços. Os fluxos de tráfego usam protocolos de rede autenticados e criptografados quando tecnicamente viável.

Práticas comuns que devem ser evitadas:

- Fluxos de tráfego não criptografados ou não autenticados na workload.
- Reutilizar credenciais de autenticação em vários usuários ou entidades.
- Confiar apenas nos controles de rede como um mecanismo de controle de acesso.
- Criar um mecanismo de autenticação personalizado em vez de depender de mecanismos de autenticação padrão do setor.
- Fluxos de tráfego excessivamente permissivos entre componentes de serviço ou outros recursos na VPC.

Benefícios de implementar esta prática recomendada:

- Limita o escopo do impacto do acesso não autorizado a uma parte da workload.
- Fornece um nível mais alto de garantia de que as ações são executadas somente por entidades autenticadas.
- Melhora o desacoplamento de serviços definindo e aplicando claramente as interfaces de transferência de dados pretendidas.
- Melhora o monitoramento, o log e a resposta a incidentes por meio da atribuição de solicitações e interfaces de comunicação bem definidas.
- Oferece defesa profunda para as workloads combinando controles de rede com controles de autenticação e de autorização.

Nível de risco exposto se esta prática recomendada não for estabelecida: Baixo

Orientação para implementação

Os padrões de tráfego de rede da workload podem ser caracterizados em duas categorias:

- O tráfego leste-oeste representa fluxos de tráfego entre serviços que compõem uma workload.
- O tráfego norte-sul representa fluxos de tráfego entre a workload e os consumidores.

Embora seja uma prática comum criptografar o tráfego norte-sul, é menos comum proteger o tráfego leste-oeste usando protocolos autenticados. As práticas modernas de segurança recomendam que o design da rede por si só não conceda um relacionamento confiável entre duas entidades. Quando dois serviços podem residir dentro de um limite de rede comum, criptografar, autenticar e autorizar as comunicações ainda são práticas recomendadas entre esses serviços.

Como exemplo, as APIs de serviço da AWS usam o protocolo de assinatura AWS Signature Version 4 (SigV4) para autenticar o chamador, independentemente da rede de origem da solicitação. Essa autenticação garante que as APIs da AWS possam verificar a identidade que solicitou a ação e que essa identidade possa ser combinada com políticas para tomar uma decisão de autorização a fim de determinar se a ação deve ser permitida ou não.

Serviços como o Amazon VPC Lattice e o Amazon API Gateway permitem que você use o mesmo protocolo de assinatura SigV4 para adicionar autenticação e autorização ao tráfego leste-oeste em suas próprias workloads. Se recursos fora do seu ambiente da AWS precisarem se comunicar com serviços que exigem autenticação e autorização baseadas em SIGV4, é possível usar o AWS Identity and Access Management (IAM) Roles Anywhere no recurso externo à AWS para adquirir credenciais temporárias da AWS. Essas credenciais podem ser usadas para assinar solicitações para serviços que usam o SigV4 para autorizar o acesso.

Outro mecanismo comum para autenticar o tráfego leste-oeste é a autenticação mútua TLS (mTLS). Muitas aplicações da Internet das Coisas (IoT), aplicações business to business e microsserviços usam o mTLS para validar a identidade de ambos os lados de uma comunicação TLS por meio do uso de certificados X.509 do lado do cliente e do servidor. Esses certificados podem ser emitidos pela AWS Private Certificate Authority (AWS Private CA). Você pode usar serviços como o Amazon API Gateway para fornecer autenticação mTLS para comunicação entre workloads ou dentro de uma mesma workload. O Application Load Balancer também oferece suporte a mTLS para workloads internas ou externas. Embora o mTLS forneça informações de autenticação aos dois lados de uma comunicação TLS, ele não fornece um mecanismo de autorização.

Por fim, o OAuth 2.0 e o OpenID Connect (OIDC) são dois protocolos normalmente usados para controlar o acesso dos usuários aos serviços, mas agora também estão se tornando populares para o tráfego entre serviços. O API Gateway fornece um autorizador JSON Web Token (JWT), permitindo que as workloads restrinjam o acesso às rotas de API usando JWTs emitidos por provedores de identidade OIDC ou OAuth 2.0. Os escopos do OAuth2 podem ser usados como uma fonte para decisões básicas de autorização, mas as verificações de autorização ainda precisam ser implementadas na camada da aplicação, e os escopos do OAuth2 em si não atendem a necessidades de autorização mais complexas.

Etapas de implementação

- Defina e documente seus fluxos de rede de workload: a primeira etapa na implementação de uma estratégia de defesa aprofundada é definir os fluxos de tráfego da sua workload.
  - Crie um diagrama de fluxo de dados que defina claramente como os dados são transmitidos entre os diferentes serviços que compõem a workload. Esse diagrama é a primeira etapa para aplicar esses fluxos por meio de canais de rede autenticados.
  - Instrumente a workload nas fases de desenvolvimento e testes para validar se o diagrama de fluxo de dados reflete com precisão o comportamento da workload em tempo de execução.
  - Um diagrama de fluxo de dados também pode ser útil ao realizar uma simulação de modelagem de ameaças, conforme descrito em SEC01-BP07 Identificar ameaças e priorizar mitigações usando um modelo de ameaça.
- Estabeleça controles de rede: considere os recursos da AWS para estabelecer controles de rede alinhados aos seus fluxos de dados. Embora os limites da rede não devam ser o único controle de segurança, eles fornecem uma camada na estratégia de defesa profunda para proteger a workload.
  - Use grupos de segurança para estabelecer, definir e restringir fluxos de dados entre recursos.
  - Considere usar o AWS PrivateLink para se comunicar com a AWS e com serviços de terceiros compatíveis com o AWS PrivateLink. Os dados enviados por meio de um endpoint da interface do AWS PrivateLink permanecem na estrutura da rede da AWS e não atravessam a Internet pública.
- Implemente autenticação e autorização em todos os serviços em sua workload: escolha o conjunto de serviços da AWS mais adequado para fornecer fluxos de tráfego autenticados e criptografados em sua workload.
  - Considere o Amazon VPC Lattice para proteger a comunicação entre serviços. O VPC Lattice pode usar a autenticação SigV4 combinada com políticas de autenticação para controlar o acesso entre serviços.

  - Para comunicação entre serviços usando mTLS, considere o API Gateway ou o Application Load Balancer. A AWS Private CA pode ser usada para estabelecer uma hierarquia de CA privada capaz de emitir certificados para uso com mTLS.
  - Ao fazer a integração com serviços usando OAuth 2.0 ou OIDC, considere o API Gateway usando o autorizador JWT.
  - Para comunicação entre sua workload e dispositivos de IoT, considere usar o AWS IoT Core, que fornece várias opções para criptografia e autenticação de tráfego de rede.
- Monitore o acesso não autorizado: monitore continuamente canais de comunicação não intencionais, entidades principais não autorizadas tentando acessar recursos protegidos e outros padrões de acesso impróprios.
  - Se estiver usando o VPC Lattice para gerenciar o acesso aos seus serviços, considere habilitar e monitorar os logs de acesso do VPC Lattice. Esses logs de acesso incluem informações sobre a entidade solicitante, informações de rede que incluem a VPC de origem e de destino e os metadados da solicitação.
  - Considere habilitar os Logs de fluxo da VPC para capturar metadados em fluxos de rede e analisar periodicamente se há anomalias.
  - Consulte o Guia de resposta a incidentes de segurança da AWS e a seção Resposta a Incidentes do pilar Segurança do AWS Well-Architected Framework para obter mais orientações sobre planejamento, simulação e resposta a incidentes de segurança.

Recursos

Práticas recomendadas relacionadas:

- SEC03-BP07 Analisar o acesso público e entre contas
- SEC02-BP02 Usar credenciais temporárias
- SEC01-BP07 Identificar ameaças e priorizar mitigações usando um modelo de ameaça

Documentos relacionados:

- Avaliar métodos de controle de acesso para proteger as APIs do Amazon API Gateway
- Configurar a autenticação TLS mútua para uma API REST
- Como proteger endpoints HTTP do API Gateway com o autorizador JWT

- Autorizar chamadas diretas para serviços da AWS usando o provedor de credenciais do AWS IoT Core
- Guia de resposta a incidentes de segurança da AWS

Vídeos relacionados:

- AWS re:invent 2022: Introdução ao VPC Lattice
- AWS re:Invent 2020: Autenticação da API sem servidor para APIs HTTP na AWS

Exemplos relacionados:

- Workshop sobre Amazon VPC Lattice
- Zero-Trust Episódio 1: workshop sobre o Phantom Service Perimeter

Resposta a incidentes

Mesmo com controles preventivos e de detecção consolidados, sua organização deve implementar mecanismos para responder e atenuar o impacto potencial de incidentes de segurança. Sua preparação afeta muito a capacidade das equipes operarem efetivamente durante um incidente, isolarem, conterem e analisarem problemas e restaurarem as operações para um estado adequado conhecido. Implementar as ferramentas e o acesso antes de um incidente de segurança e praticar rotineiramente game days para validar a resposta a incidentes ajudam a garantir que você possa se recuperar enquanto minimiza interrupções empresariais.

Tópicos

Aspectos da resposta a incidentes da AWS

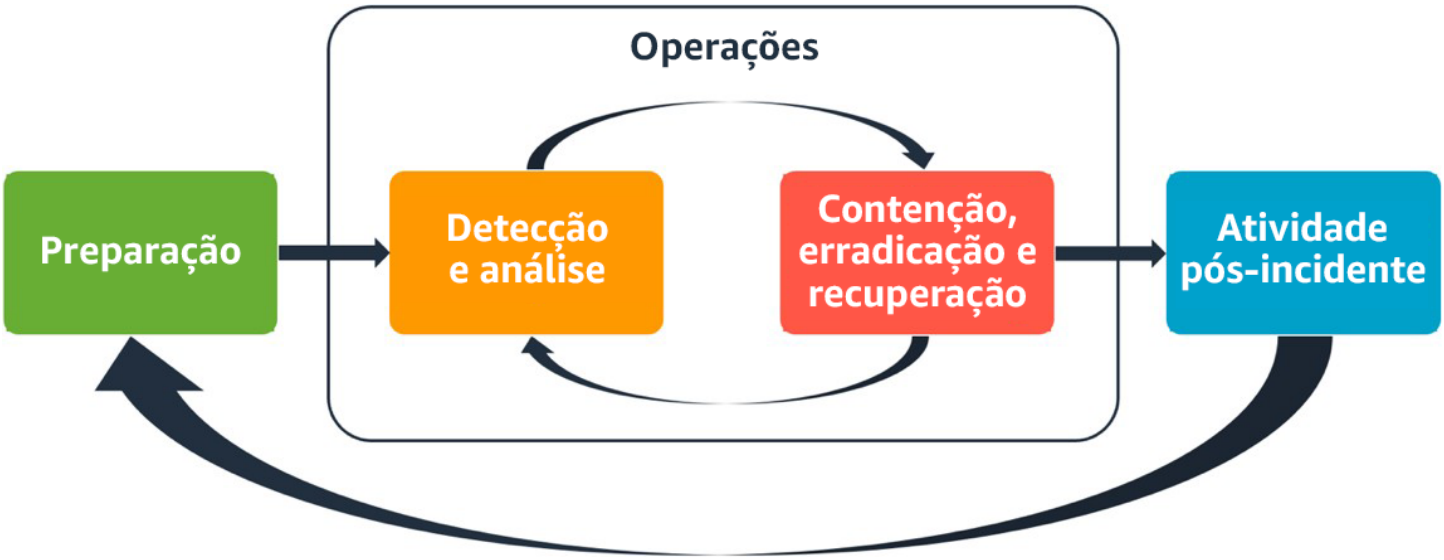
Todos os usuários da AWS de uma organização devem ter uma compreensão básica dos processos de resposta a incidentes de segurança, e a equipe de segurança deve entender como responder aos problemas de segurança. Educação, treinamento e experiência são essenciais para um programa bem-sucedido de resposta a incidentes na nuvem e são preferencialmente implementados bem antes de precisar lidar com um possível incidente de segurança. A base de um programa bem-sucedido de resposta a incidentes na nuvem consiste em Preparação, Operações e Atividade pós-incidente.

Para entender cada um desses aspectos, considere as seguintes descrições:

- Preparação: prepare sua equipe de resposta a incidentes para detectar e responder aos incidentes na AWS ativando controles de detecção e verificando o acesso adequado às ferramentas e aos serviços de nuvem necessários. Além disso, prepare os playbooks necessários, tanto os automatizados quanto os manuais, para garantir respostas confiáveis e consistentes.
- Operações: opere em eventos de segurança e possíveis incidentes seguindo as fases de resposta a incidentes do NIST: detectar, analisar, conter, erradicar e recuperar.

- Atividade pós-incidente: itere o resultado de seus eventos e simulações de segurança para melhorar a eficácia da resposta, aumentar o valor derivado da resposta e da investigação e reduzir ainda mais os riscos. Você precisa aprender com os incidentes e ter uma propriedade consistente das atividades de melhoria.

O diagrama a seguir mostra o fluxo desses aspectos, alinhando-se ao ciclo de vida de resposta a incidentes do NIST mencionado anteriormente, mas com operações que abrangem detecção e análise com contenção, erradicação e recuperação.



Aspectos da resposta a incidentes da AWS

Elaborar metas da resposta da nuvem

Embora os processos e os mecanismos gerais de resposta a incidentes, como os definidos no NIST SP 800-61 Guia de tratamento de incidentes de computadores, permaneçam válidos, recomendamos que você avalie os objetivos específicos desse projeto que são relevantes para responder a incidentes de segurança em um ambiente de nuvem:

- Estabeleça objetivos de resposta: trabalhe com as partes interessadas, a assessoria jurídica e a liderança organizacional para determinar a meta da resposta a um incidente. Algumas metas comuns são: conter e atenuar o problema, recuperar os recursos afetados, preservar dados para análise forense, retornar às operações seguras conhecidas e, finalmente, aprender com os incidentes.
- Responda usando a nuvem: implemente padrões de resposta na nuvem, onde o evento e os dados ocorrem.

- Saiba o que você tem e o que precisa: preserve logs, recursos, instantâneos e outras evidências copiando e armazenando-os em uma conta centralizada na nuvem dedicada à resposta. Use tags, metadados e mecanismos que impõem políticas de retenção. Você precisará entender quais serviços são usados e identificar os requisitos para investigar esses serviços. Para ajudar você a entender seu ambiente, você também pode usar marcação com tags.
- Use mecanismos de reimplantação: se um problema de segurança puder ser atribuído a uma configuração incorreta, a correção poderá ser tão simples quanto a remoção da variação com a reimplantação dos recursos com a configuração apropriada. Se um possível comprometimento for identificado, verifique se sua redistribuição inclui a atenuação bem-sucedida e verificada das causas principais.
- Automatize sempre que possível: à medida que problemas surgem ou incidentes se repetem, crie mecanismos para fazer a triagem programática e responder a eventos comuns. Use respostas humanas para incidentes exclusivos, complexos ou confidenciais em que as automações são insuficientes.
- Escolha soluções escaláveis: esforce-se para combinar a escalabilidade da abordagem de sua organização com a computação em nuvem. Implemente mecanismos de detecção e resposta que se expandam em seus ambientes para reduzir efetivamente o tempo entre a detecção e a resposta.
- Aprenda e aprimore seu processo: seja proativo na identificação de lacunas em seus processos, ferramentas ou pessoas e implemente um plano para corrigi-las. Simulações são métodos seguros para encontrar lacunas e melhorar processos.

Essas metas de design são um lembrete para analisar a implementação de sua arquitetura quanto à capacidade de conduzir tanto a resposta a incidentes quanto a detecção de ameaças. Ao planejar suas implementações de nuvem, pense em responder a um incidente, de preferência, com uma metodologia de resposta sólida em termos forenses. Em alguns casos, isso significa que você pode ter várias organizações, contas e ferramentas configuradas especificamente para essas tarefas de resposta. Essas ferramentas e funções devem ser disponibilizadas para a equipe de atendimento a incidentes por meio do pipeline de implantação. Elas não devem ser estáticas, pois podem causar um risco maior.

Preparação

A preparação para um incidente é fundamental para uma resposta oportuna e eficaz a incidentes. A preparação é feita em três domínios:

- Pessoas: preparar seu pessoal para um incidente de segurança envolve identificar as partes interessadas relevantes para a resposta a incidentes e treiná-las em resposta a incidentes e tecnologias de nuvem.
- Processos: preparar seus processos para um incidente de segurança envolve documentar arquiteturas, desenvolver planos completos de resposta a incidentes e criar playbooks para uma resposta consistente a eventos de segurança.
- Tecnologia: preparar sua tecnologia para um incidente de segurança envolve configurar o acesso, agregar e monitorar os logs necessários, implementar mecanismos de alerta eficazes e desenvolver recursos de resposta e investigação.

Cada um desses domínios é igualmente importante para uma resposta eficaz a incidentes. Nenhum programa de resposta a incidentes é completo ou eficaz sem os três. Você precisará preparar pessoas, processos e tecnologias com uma forte integração para se preparar para um incidente.

Práticas recomendadas

- SEC10-BP01 Identificar equipes e recursos externos fundamentais
- SEC10-BP02 Desenvolver planos de gerenciamento de incidentes
- SEC10-BP03 Preparar recursos forenses
- SEC10-BP04 Desenvolver e testar playbooks de resposta a incidentes de segurança
- SEC10-BP05 Provisionar acesso previamente
- SEC10-BP06 Implantar ferramentas previamente
- SEC10-BP07 Executar simulações

SEC10-BP01 Identificar equipes e recursos externos fundamentais

Identifique as equipes, as obrigações legais e os recursos internos e externos que ajudam sua organização a responder a um incidente.

Resultado desejado: você tem uma lista dos principais funcionários, suas informações de contato e as funções que eles desempenham ao responder a um evento de segurança. Você revisa essas informações regularmente e as atualiza para refletir mudanças de equipes do ponto de vista das ferramentas internas e externas. Você considera todos os provedores de serviços e fornecedores terceirizados ao documentar essas informações, incluindo parceiros de segurança, provedores de nuvem e aplicações de software como serviço (SaaS). Durante um evento de segurança, as equipes

estão preparadas com o nível apropriado de responsabilidade, contexto e acesso para resposta e recuperação.

Práticas comuns que devem ser evitadas:

- Não manter uma lista atualizada das principais equipes com informações de contato, funções e responsabilidades para responder a eventos de segurança.
- Supor que todos saibam quais são as pessoas, as dependências, a infraestrutura e as soluções necessárias para resposta a um evento e recuperação.
- Não ter um documento ou repositório de conhecimentos que represente a infraestrutura principal ou o design da aplicação.
- Não ter processos de integração adequados para que novos funcionários contribuam eficazmente para uma resposta a eventos de segurança, como a realização de simulações de eventos.
- Não ter um caminho de encaminhamento estabelecido quando as equipes principais estão temporariamente indisponíveis ou não respondem durante eventos de segurança.

Benefícios de implementar esta prática recomendada: essa prática reduz a triagem e o tempo de resposta gastos na identificação do pessoal certo e de seus perfis durante um evento. Minimize o tempo perdido durante um evento mantendo uma lista atualizada das principais equipes e de suas funções para que você possa convocar as pessoas certas para a triagem e se recuperar de um evento.

Nível de risco exposto se esta prática recomendada não for estabelecida: Alto

Orientação para implementação

Identifique o pessoal-chave em sua organização: mantenha uma lista de contatos do pessoal de sua organização que você precisa envolver. Revise e atualize regularmente essas informações em caso de movimentação de equipes, como mudanças organizacionais, promoções e mudanças de equipe. Isso é especialmente importante para funções importantes, como gerentes de incidentes, respondedores a incidentes e líderes de comunicação.

- Gerente de incidentes: os gerentes de incidentes têm autoridade geral durante a resposta ao evento.
- Respondedores a incidentes: os respondedores a incidentes são responsáveis pelas atividades de investigação e correção. Essas pessoas podem diferir com base no tipo de evento, mas normalmente são desenvolvedores e equipes operacionais responsáveis pela aplicação afetada.

- Líder de comunicação: o líder de comunicação é responsável pelas comunicações internas e externas, especialmente com órgãos públicos e reguladores e clientes.
- Processo de integração: treine e integre regularmente novos funcionários para equipá-los com as habilidades e conhecimentos necessários para contribuir de forma eficaz com os esforços de resposta a incidentes. Incorpore simulações e exercícios práticos como parte do processo de integração para facilitar sua preparação
- Especialistas no assunto (SME): no caso de equipes distribuídas e autônomas, recomendamos que você identifique um SME para workloads de missão crítica. Eles oferecem insights sobre a operação e a classificação de dados das workloads críticas envolvidas no evento.

Formato de tabela de exemplo:

```
  | Role | Name | Contact Information | Responsibilities |
1 | ——- | ——- | ——- | ——- |
2 | Incident Manager | Jane Doe| jane.doe@example.com | Overall authority during
 response |
3 | Incident Responder | John Smith | john.smith@example.com | Investigation and
 remediation |
4 | Communications Lead | Emily Johnson | emily.johnson@example.com | Internal and
 external communications |
5 | Communications Lead | Michael Brown | michael.brown@example.com | Insights on
 critical workloads |
```

Considere usar o recurso AWS Systems Manager Incident Manager para capturar os principais contatos, definir um plano de resposta, automatizar cronogramas de plantão e criar planos de escalação. Automatize e faça a rotação de toda a equipe por meio de um cronograma de plantão para que a responsabilidade pela workload seja compartilhada entre os respectivos responsáveis. Isso favorece boas práticas, como emitir métricas e logs relevantes e definir limites de alarme importantes para a workload.

Identifique parceiros externos: as empresas usam ferramentas criadas por provedores de software independentes (ISVs), parceiros e subcontratados para criar soluções diferenciadas para seus clientes. Envolva as principais equipes dessas partes que possam ajudar na resposta e recuperação de um incidente. Recomendamos se inscrever no nível apropriado do Suporte para obter acesso imediato a especialistas da AWS por meio de um caso de suporte. Considere acordos semelhantes com todos os provedores de soluções essenciais para as workloads. Alguns eventos de segurança exigem que as empresas de capital aberto notifiquem os órgãos públicos e reguladores relevantes

sobre o evento e os impactos. Mantenha e atualize as informações de contato dos departamentos relevantes e das pessoas responsáveis.

Etapas de implementação

1. Configure uma solução de gerenciamento de incidentes.
   a. Considere implantar o Incident Manager em sua conta de ferramentas de segurança.
2. Defina contatos em sua solução de gerenciamento de incidentes.
   a. Defina pelo menos dois tipos de canal de contato para cada contato (como SMS, telefone ou e-mail) para garantir a acessibilidade durante um incidente.
3. Defina um plano de resposta.
   a. Identifique os contatos mais adequados a serem mobilizados durante um incidente. Defina planos de encaminhamento alinhados às funções das equipes a serem mobilizadas, em vez de contatos individuais. Considere incluir contatos que possam ter a responsabilidade de informar entidades externas, mesmo que eles não sejam diretamente mobilizados para resolver o incidente.

Recursos

Práticas recomendadas relacionadas:

- OPS02-BP03 Atividades de operações com proprietários identificados responsáveis pela performance

Documentos relacionados:

- Guia de resposta a incidentes de segurança da AWS

Exemplos relacionados:

- Framework do playbook do cliente da AWS
- Como se preparar e responder a incidentes de segurança no ambiente da AWS

Ferramentas relacionadas:

- AWS Systems Manager Incident Manager

Vídeos relacionados:

- A abordagem da Amazon à segurança durante o desenvolvimento

SEC10-BP02 Desenvolver planos de gerenciamento de incidentes

O primeiro documento a ser desenvolvido para resposta a incidentes é o plano de resposta a incidentes. O plano de resposta a incidentes foi projetado para ser a base de seu programa e estratégia de resposta a incidentes.

Benefícios de implementar esta prática recomendada: o desenvolvimento de processos de resposta a incidentes completos e claramente definidos é fundamental para um programa de resposta a incidentes bem-sucedido e escalável. Quando um evento de segurança ocorre, etapas e fluxos de trabalho claros poderão ajudar você a responder em tempo hábil. Talvez você já tenha processos de resposta a incidentes existentes. Independentemente do seu estado atual, é importante atualizar, repetir e testar seus processos de resposta a incidentes regularmente.

Nível de risco exposto se esta prática recomendada não for estabelecida: Alto

Orientação para implementação

Um plano de gerenciamento de incidentes é fundamental para responder, mitigar e se recuperar de possíveis impactos de incidentes de segurança. Um plano de gerenciamento de incidentes é um processo estruturado de identificação, correção e resposta em tempo hábil a incidentes de segurança.

A nuvem tem muitos dos mesmos requisitos e perfis operacionais encontrados em um ambiente on-premises. Ao criar um plano de gerenciamento de incidentes, é importante definir estratégias de resposta e recuperação que se alinhem melhor aos seus resultados empresariais e requisitos de conformidade. Por exemplo, se você opera workloads na AWS em conformidade com o FedRAMP dos Estados Unidos, siga as recomendações em NIST SP 800-61 Computer Security Handling Guide. Da mesma forma, ao operar workloads que armazenam informações de identificação pessoal (PII), considere como se proteger e responder a incidentes relacionados ao uso e à residência de dados.

Ao criar um plano de gerenciamento de incidentes para suas workloads na AWS, comece com o Modelo de responsabilidade compartilhada da AWS para criar uma abordagem de defesa aprofundada para a resposta a incidentes. Nesse modelo, a AWS gerencia a segurança da nuvem, e você é responsável pela segurança na nuvem. Isso significa que você mantém o controle e

é responsável pelos controles de segurança que escolhe implementar. O Guia de resposta a incidentes de segurança da AWS detalha os conceitos e as orientações básicas para criar um plano de gerenciamento de incidentes centrado na nuvem.

Um plano de gerenciamento de incidentes eficaz deve ser continuamente trabalhado e permanecer atualizado com relação às suas metas de operações na nuvem. Considere o uso dos planos de implementação detalhados abaixo à medida que cria e evolui seu plano de gerenciamento de incidentes.

Etapas de implementação

1. Defina funções e responsabilidades em sua organização para lidar com eventos de segurança. Isso deve envolver representantes de vários departamentos, incluindo:
   - Recursos humanos (RH)
   - Equipe executiva
   - Departamento jurídico
   - Proprietários e desenvolvedores de aplicações (especialistas no assunto, ou SMEs)
2. Descreva claramente quem é responsável, consultado e informado (RACI) durante um incidente. Crie um gráfico RACI para facilitar a comunicação rápida e direta e descreva claramente a liderança em diferentes estágios de um evento.
3. Envolva proprietários e desenvolvedores de aplicações (SMEs) durante um incidente, pois eles podem fornecer informações e contexto valiosos para ajudar a medir o impacto. Desenvolva relacionamentos com esses SMEs e pratique cenários de resposta a incidentes com eles antes que um incidente real ocorra.
4. Envolva parceiros confiáveis ou especialistas externos no processo de investigação ou resposta, pois eles podem oferecer experiência e perspectiva adicionais.
5. Alinhe seus planos e funções de gerenciamento de incidentes com quaisquer regulamentações locais ou requisitos de conformidade que regem sua organização.
6. Pratique e teste seus planos de resposta a incidentes regularmente e envolva todas as funções e responsabilidades definidas. Isso ajuda a agilizar o processo e a verificar se você tem uma resposta coordenada e eficiente aos incidentes de segurança.
7. Revise e atualize as funções, responsabilidades e o gráfico RACI periodicamente ou à medida que sua estrutura organizacional ou requisitos mudarem.

Entender as equipes de resposta e o suporte da AWS

- AWS Support
  - O Suporte oferece uma variedade de planos que permitem conceder acesso a ferramentas e conhecimentos que oferecem suporte ao sucesso e à integridade operacional das soluções da AWS. Se precisar de suporte técnico e mais recursos para ajudar a planejar, implantar e otimizar seu ambiente da AWS, selecione um plano de suporte mais adequado ao seu caso de uso da AWS.
  - Considere o Support Center no AWS Management Console (é necessário iniciar sessão) como ponto central de contato para obter suporte para problemas que afetam seus recursos da AWS. O acesso ao Suporte é controlado pelo AWS Identity and Access Management. Para mais informações sobre como obter acesso aos recursos da Suporte, consulte Conceitos básicos do Suporte.
- Equipe de Resposta a Incidentes de Clientes (CIRT) da AWS
  - A Equipe de Resposta a Incidentes de Clientes (CIRT) da AWS é uma equipe global da AWS especializada que está disponível 24 horas por dia, 7 dias por semana, para prestar assistência aos clientes durante eventos de segurança ativos no lado do cliente do Modelo de responsabilidade compartilhada da AWS.
  - Ao apoiar você, a CIRT da AWS presta assistência na triagem e na recuperação de um evento de segurança ativo na AWS. A equipe pode ajudar na análise da causa-raiz por meio do uso de logs de serviço da AWS e fornecer recomendações para recuperação. Ela também podem fornecer recomendações de segurança e práticas recomendadas para ajudar você a evitar eventos de segurança no futuro.
  - Os clientes da AWS podem solicita a ajuda da CIRT da AWS por meio de um caso do Suporte
- Suporte de resposta a DDoS
  - A AWS oferece o AWS Shield, que fornece um serviço gerenciado de proteção contra negação de serviço distribuída (DDoS) para proteger aplicações Web executadas na AWS. O Shield fornece detecção permanente e mitigações automáticas em linha que podem minimizar o tempo de inatividade e a latência das aplicações para que não seja necessário envolver o Suporte para usufruir da proteção contra DDoS. O Shield possui dois níveis: AWS Shield Standard e AWS Shield Advanced. Para saber mais sobre as diferenças entre esses dois níveis, consulte a Documentação de recursos do Shield.
- AWS Managed Services (AMS)
  - O AWS Managed Services (AMS) oferece gerenciamento contínuo de sua infraestrutura da AWS para que você possa se concentrar em suas aplicações. Ao implementar práticas recomendadas para manter sua infraestrutura, o AMS ajuda a reduzir a sobrecarga e os riscos operacionais.

O AMS automatiza atividades comuns, como solicitações de alteração, monitoramento, gerenciamento de patches, segurança e serviços de backup, além de disponibilizar serviços de ciclo de vida total para provisionar, executar e apoiar a sua infraestrutura.

- O AMS assume a responsabilidade de implantar um pacote de controles de detecção de segurança e fornece uma primeira linha de resposta aos alertas 24 horas por dia, 7 dias por semana. Quando um alerta é iniciado, o AMS segue um conjunto padrão de guias e playbooks automatizados para verificar uma resposta consistente. Esses playbooks são compartilhados com os clientes do AMS durante a integração para que eles possam desenvolver e coordenar uma resposta com o AMS.

Desenvolva o plano de resposta a incidentes

O plano de resposta a incidentes foi projetado para ser a base de seu programa e estratégia de resposta a incidentes. O plano de resposta a incidentes deve estar em um documento formal. Um plano de resposta a incidentes geralmente inclui as seguintes seções:

- Visão geral da equipe de resposta a incidentes: descreve as metas e funções da equipe de resposta a incidentes.
- Papéis e responsabilidades: lista as partes interessadas na resposta a incidentes e detalha seus papéis quando um incidente ocorre.
- Plano de comunicação: detalha as informações de contato e como você se comunica durante um incidente.
- Métodos de comunicação de backup: é prática recomendada ter comunicação fora de banda como backup para a comunicação de incidentes. Um exemplo de aplicação que fornece um canal seguro de comunicação fora de banda é AWS Wickr.
- Fases da resposta a incidentes e ações necessárias: enumera as fases da resposta a incidentes (por exemplo, detectar, analisar, erradicar, conter e recuperar), incluindo ações de alto nível a serem realizadas nessas fases.
- Definições de severidade e priorização de incidentes: detalha como classificar a severidade de um incidente, como priorizar o incidente e, depois, como as definições de severidade afetam os procedimentos de escalação.

Embora essas seções sejam comuns em empresas de diferentes tamanhos e setores, o plano de resposta a incidentes de cada organização é único. Você precisa criar um plano de resposta a incidentes que funcione melhor para a organização.

Recursos

Práticas recomendadas relacionadas:

- SEC04 Detecção

Documentos relacionados:

- Guia de resposta a incidentes de segurança da AWS
- NIST: Guia de tratamento de incidentes de segurança de computadores

SEC10-BP03 Preparar recursos forenses

Antes de um incidente de segurança, considere o desenvolvimento de recursos forenses para contribuir com as investigações de eventos de segurança.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Os conceitos da análise forense on-premises tradicional se aplicam à AWS. Para obter informações importantes para começar a desenvolver recursos forenses na Nuvem AWS, consulte Estratégias do ambiente de investigação forense na Nuvem AWS.

Depois de configurar o ambiente e a estrutura da Conta da AWS para análise forense, defina as tecnologias necessárias para executar com eficácia metodologias forenses sólidas nas quatro fases:

- Coleta: colete logs relevantes da AWS, como do AWS CloudTrail, do AWS Config, logs de fluxo de VPC e logs em nível de host. Colete snapshots, backups e despejos de memória dos recursos afetados da AWS, quando disponíveis.
- Exame: examine os dados coletados extraindo e avaliando as informações relevantes.
- Análise: analise os dados coletados para entender o incidente e tirar conclusões do ocorrido.
- Relatório: apresente as informações resultantes da fase de análise.

Etapas de implementação

Prepare o ambiente forense

O AWS Organizations ajuda a gerenciar e reger centralmente um ambiente da AWS à medida que você expande e escala os recursos da AWS. Uma organização da AWS consolida suas Contas

da AWS para que você possa administrá-las como uma única unidade. Você pode usar unidades organizacionais (UOs) para agrupar contas e administrá-las como uma unidade única.

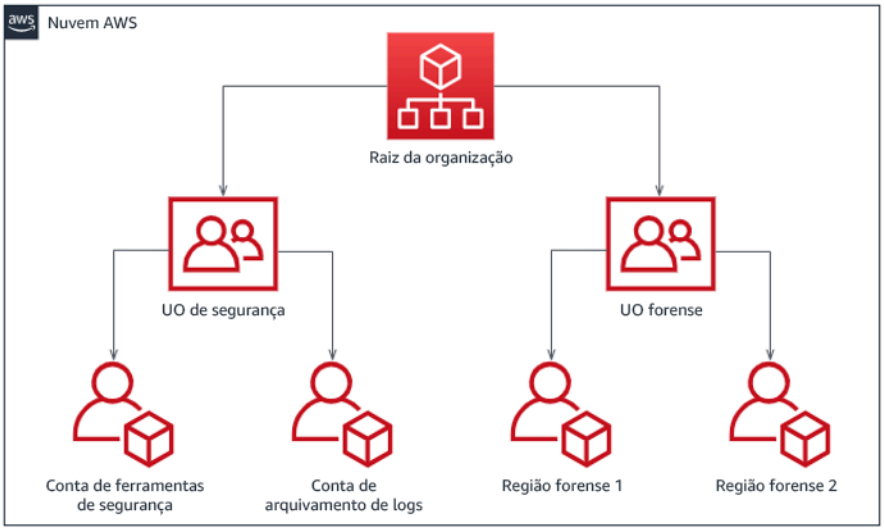
Para resposta a incidentes, é útil ter uma estrutura da Conta da AWS compatível com as funções de resposta a incidentes, que inclui uma UO de segurança e uma UO forense. Dentro da OU de segurança, é necessário ter contas para:

- Arquivamento de logs: agregue logs em uma Conta da AWS de arquivamento de logs com permissões limitadas.
- Ferramentas de segurança: centralize os serviços de segurança em uma Conta da AWS de ferramentas de segurança. Essa conta opera como administrador delegado dos serviços de segurança.

Dentro da UO forense, você tem a opção de implementar uma única conta ou contas forenses para cada região em que opera, dependendo da que funciona melhor para sua empresa e modelo operacional. Se você criar uma conta forense por região, poderá bloquear a criação de recursos da AWS fora dessa região e reduzir o risco de os recursos serem copiados para uma região não pretendida. Por exemplo, se você operasse apenas na região Leste dos EUA (Norte da Virgínia) (`us-east-1`) e Oeste dos EUA (Oregon) (`us-west-2`), você teria duas contas na UO forense: uma para `us-east-1` e outra para `us-west-2`.

É possível criar uma Conta da AWS de análise forense para várias regiões. Você deve ter cuidado ao copiar recursos da AWS para essa conta para verificar se está de acordo com seus requisitos de soberania de dados. Como é preciso tempo para provisionar novas contas, é imperativo criar e instrumentar as contas forenses bem antes de um incidente, para que os respondentes possam estar preparados para usá-las de forma eficaz em suas respostas.

O diagrama a seguir exibe um exemplo de estrutura de contas, incluindo uma UO forense com contas forenses por região:



Estrutura de contas por região para resposta a incidentes

Capture backups e snapshots

Configurar backups dos principais sistemas e bancos de dados é essencial para a recuperação de um incidente de segurança e para fins forenses. Com os backups em vigor, você pode restaurar seus sistemas ao estado seguro anterior. Na AWS, é possível criar snapshots de vários recursos. Os snapshots fornecem backups pontuais desses recursos. Há muitos serviços da AWS que podem ajudar em backup e recuperação. Para obter detalhes sobre esses serviços e abordagens para backup e recuperação, consulte Orientação prescritiva de backup e recuperação e Usar backups para se recuperar de incidentes de segurança.

Especialmente quando se trata de situações como ransomware, é fundamental que os backups estejam bem protegidos. Para obter orientações sobre como proteger backups, consulte As dez principais práticas recomendas de segurança para proteger backups na AWS. Além de proteger os backups, você deve testar regularmente seus processos de backup e restauração para verificar se a tecnologia e os processos implementados funcionam conforme o esperado.

Automatize a análise forense

Durante um evento de segurança, sua equipe de resposta a incidentes deve ser capaz de coletar e analisar evidências rapidamente, mantendo a precisão durante o período em torno do evento (como capturar registros relacionados a um evento ou recurso específico ou coletar o despejo de memória de uma instância do Amazon EC2). É desafiador e demorado para a equipe de resposta a incidentes coletar manualmente as evidências relevantes, especialmente em um grande número de instâncias

e contas. Além disso, a coleta manual pode estar sujeita a erros humanos. Por esses motivos, você deve desenvolver e implementar a automação para perícia forense o máximo possível.

A AWS oferece vários recursos de automação para análise forense, os quais são listados na seção de recursos a seguir. Esses recursos são exemplos de padrões forenses que desenvolvemos e que os clientes implementaram. Embora possam ser uma arquitetura de referência útil para começar, considere modificá-las ou criar padrões de automação forense com base em seu ambiente, requisitos, ferramentas e processos forenses.

Recursos

Documentos relacionados:

- Guia de resposta a incidentes de segurança da AWS: Desenvolver recursos forenses
- Guia de resposta a incidentes de segurança da AWS: Recursos forenses
- Estratégias do ambiente de investigação forense na Nuvem AWS
- Como automatizar a coleta forense de discos na AWS
- Recomendações da AWS: Automatizar a resposta a incidentes e a análise forense

Vídeos relacionados:

- Automatizar a resposta a incidentes e a análise forense

Exemplos relacionados:

- Framework de resposta a incidentes e análise forense automatizadas
- Orquestrador forense automatizado para Amazon EC2

SEC10-BP04 Desenvolver e testar playbooks de resposta a incidentes de segurança

Uma parte fundamental da preparação de seus processos de resposta a incidentes é desenvolver playbooks. Os playbooks de resposta a incidentes fornecem recomendações e etapas a serem seguidas quando um evento de segurança ocorre. Ter uma estrutura e etapas claras simplifica a resposta e reduz a probabilidade de erro humano.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

Os playbooks devem ser criados para cenários de incidentes, como:

- Incidentes esperados: os playbooks devem ser criados para os incidentes previstos. Isso inclui ameaças como negação de serviço (DoS), ransomware e comprometimento de credenciais.
- Descobertas ou alertas de segurança conhecidos: devem ser criados playbooks para abordar descobertas e alertas de segurança conhecidos, como os do Amazon GuardDuty. Quando você recebe uma descoberta do GuardDuty, o manual deve fornecer etapas claras para evitar o manuseio incorreto ou a ignorância do alerta. Para obter mais detalhes e orientações sobre remediação, consulte Correção de problemas de segurança descobertos pelo GuardDuty.

Os playbooks devem conter etapas técnicas a serem concluídas por um analista de segurança para investigar e responder adequadamente a um possível incidente de segurança.

Etapas de implementação

Os itens a serem incluídos em um playbook incluem:

- Visão geral do playbook: qual cenário de risco ou incidente esse playbook aborda? Qual é o objetivo do playbook?
- Pré-requisitos: quais logs, mecanismos de detecção e ferramentas automatizadas são necessários para esse cenário de incidente? Qual é a notificação esperada?
- Informações de comunicação e escalação: quem está envolvido e quais são suas informações de contato? Quais são as responsabilidades de cada parte interessada?
- Etapas da resposta: em todas as fases da resposta a incidentes, quais etapas táticas devem ser seguidas? Que consultas um analista deve executar? Que código deve ser executado para alcançar o resultado desejado?
  - Detectar: como o incidente será detectado?
  - Analisar: como o escopo do impacto será determinado?
  - Conter: como o incidente será isolado para limitar o escopo?
  - Erradicar: como a ameaça será removida do ambiente?
  - Recuperar: como o sistema ou o recurso afetado voltará à produção?
- Resultados esperados: depois que as consultas e o código forem executados, qual é o resultado esperado do playbook?

Recursos

Práticas recomendadas do Well-Architected relacionadas:

- SEC10-BP02 Desenvolver planos de gerenciamento de incidentes

Documentos relacionados:

- Framework para playbooks de resposta a incidentes
- Como desenvolver seus próprios playbooks de resposta a incidentes
- Exemplos de playbook de resposta a incidentes
- Criar um runbook de resposta a incidentes da AWS using playbooks do Jupyter e o CloudTrail Lake

SEC10-BP05 Provisionar acesso previamente

Verifique se os respondedores a incidentes têm o acesso correto pré-provisionado na AWS para reduzir o tempo de investigação necessário até a recuperação.

Práticas comuns que devem ser evitadas:

- Uso da conta raiz para a resposta a incidentes.
- Alterar contas de usuário existentes.
- Manipular permissões do IAM diretamente ao fornecer elevação de privilégios just-in-time.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

A AWS recomenda reduzir ou eliminar a dependência de credenciais de longa duração sempre que possível, dando preferência a credenciais temporárias e a mecanismos de escalação de privilégios just-in-time. As credenciais de longa duração são propensas a riscos de segurança e aumentam a sobrecarga operacional. Para a maioria das tarefas de gerenciamento, bem como para as tarefas de resposta a incidentes, recomendamos implementar a federação de identidades junto com a escalação temporária para acesso administrativo. Nesse modelo, um usuário solicita elevação para um nível de privilégio superior (como um perfil de resposta a incidentes) e, considerando que ele seja elegível para a elevação, a solicitação é enviada a um aprovador. Se a solicitação for aprovada,

o usuário receberá um conjunto de credenciais da AWS temporárias que podem ser usadas para concluir suas tarefas. Quando essas credenciais expirarem, o usuário deverá enviar uma nova solicitação de elevação.

Recomendamos usar a escalação de privilégio temporária para a maioria dos cenários de resposta a incidentes. A maneira correta de fazer isso é usar o AWS Security Token Service e políticas de sessão para definir o escopo do acesso.

Há cenários em que as identidades federadas não estão disponíveis, como:

- Interrupção relacionada a um provedor de identidades (IdP) comprometido.
- Erro de configuração ou erro humano causando uma falha no sistema de gerenciamento de acesso federado.
- Atividade mal-intencionada, como um evento de negação de serviço distribuído (DDoS) ou que causa a indisponibilidade do sistema.

Nos casos anteriores, deve haver um acesso emergencial de "vidro quebrado" configurado para permitir a investigação e a correção rápida de incidentes. Recomendamos usar um usuário, grupo ou perfil com as permissões apropriadas para realizar tarefas e acessar recursos da AWS. Use as credenciais de usuário-raiz somente para realizar tarefas que exijam as credenciais de usuário-raiz. Para verificar se os respondedores de um incidente têm o nível de acesso correto à AWS e a outros sistemas relevantes, recomendamos provisionar previamente contas dedicadas. As contas exigem acesso privilegiado e devem ser estritamente controladas e monitoradas. As contas devem ser criadas com os privilégios mínimos exigidos para realizar as tarefas necessárias e o nível de acesso deve ser baseado nos playbooks criados como parte do plano de gerenciamento de incidentes.

Como prática recomendada, utilize perfis e usuários dedicados e com propósito específico. Escalar temporariamente o acesso de usuários ou perfis por meio da adição de políticas do IAM não deixa claro qual é o acesso que os usuários tinham durante o incidente, e há um risco de que os privilégios escalados não sejam revogados.

É importante remover o máximo de dependências possível para verificar se o acesso pode ser obtido com o maior número possível de cenários de falha. Como forma de auxiliar esse processo, crie um playbook para verificar se os usuários de resposta a incidentes são criados como usuários em uma conta de segurança dedicada e não são gerenciados por nenhuma solução de autenticação única (SSO) ou federação existente. Cada respondedor individual deve ter sua própria conta nomeada. A configuração da conta deve aplicar uma política de senha forte e autenticação multifator (MFA). Se os playbooks de resposta a incidentes só exigem acesso ao AWS Management Console, o usuário

não deve ter chaves de acesso configuradas e deve ser proibido explicitamente de criar chaves de acesso. Isso pode ser configurado com políticas do IAM ou políticas de controle de serviços (SCPs), conforme mencionado nas Práticas recomendadas de segurança da AWS para SCPs do AWS Organizations Os usuários não devem ter privilégios além da capacidade de assumir perfis de resposta a incidentes em outras contas.

Durante um incidente, talvez seja necessário conceder acesso a outros indivíduos internos ou externos para apoiar a investigação, a correção ou as atividades de recuperação. Nesse caso, use o mecanismo do playbook mencionado anteriormente, e deve haver um processo para verificar se qualquer acesso adicional foi revogado imediatamente após a conclusão do incidente.

Para verificar se o uso de perfis de resposta a incidentes pode ser monitorado e auditado corretamente, é essencial que as contas de usuário do IAM criadas para esse fim não sejam compartilhadas entre indivíduos e que o Usuário raiz da conta da AWS não seja utilizado, a menos que isso seja necessário para uma tarefa específica. Se o usuário-raiz for necessário (por exemplo, quando o acesso do IAM a uma conta específica estiver indisponível), use um processo separado com um playbook disponível para verificar a disponibilidade das credenciais de início de sessão e do token de MFA do usuário-raiz.

Para configurar as políticas do IAM para os perfis de resposta a incidentes, considere usar o IAM Access Analyzer para gerar políticas com base em logs do AWS CloudTrail. Para fazer isso, conceda acesso de administrador ao perfil de resposta a incidentes em uma conta de não produção e execute as etapas descritas nos playbooks. Concluído o processo, uma política que permita somente as ações realizadas pode ser criada. Essa política pode ser então aplicada a todos os perfis de resposta a incidentes em todas as contas. Você pode criar uma política do IAM separada para cada playbook a fim de facilitar o gerenciamento e a auditoria. Exemplos de playbook podem incluir planos de resposta para ransomware, violações de dados, perda de acesso à produção, entre outros cenários.

Use as contas de resposta a incidentes para assumir perfis do IAM de resposta a incidentes dedicados em outras Contas da AWS Esses perfis também devem ser configurados para poder ser assumidos somente por usuários na conta de segurança, e o relacionamento de confiança deve exigir que a entidade principal que está fazendo a chamada seja autenticada com MFA. Os perfis devem usar políticas do IAM com escopo estritamente definido para controlar o acesso. Certifique-se de que todas as solicitações de `AssumeRole` para esses perfis sejam registradas em log no CloudTrail e acionem alertas, e que quaisquer ações realizadas usando esses perfis sejam registradas em log.

É altamente recomendável que as contas do IAM e os perfis do IAM sejam claramente nomeados para permitir que sejam encontrados com facilidade nos logs do CloudTrail. Um exemplo disso

seria nomear as contas do IAM como *<USER_ID>*-BREAK-GLASS e os perfis do IAM como BREAK-GLASS-ROLE.

O CloudTrail é usado para registrar a atividade da API em suas contas da AWS e deve ser usado para configurar alertas sobre o uso dos perfis de resposta a incidentes. Consulte a publicação do blog sobre como configurar alertas quando as chaves-raiz são usadas. As instruções podem ser modificadas para configurar o filtro métrico do Amazon CloudWatch para filtrar eventos AssumeRole relacionados ao perfil do IAM de resposta a incidentes:

```
{ $.eventName = "AssumeRole" && $.requestParameters.roleArn =
 "<INCIDENT_RESPONSE_ROLE_ARN>" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !
= "AwsServiceEvent" }
```

Como é provável que os perfis de resposta a incidentes tenham um alto nível de acesso, é importante que esses alertas sejam transmitidos a um grupo amplo e que as atitudes necessárias sejam tomadas rapidamente.

Durante um incidente, é possível que um respondedor possa exigir acesso a sistemas que não são protegidos diretamente pelo IAM. Isso pode incluir instâncias do Amazon Elastic Compute Cloud, bancos de dados do Amazon Relational Database Service ou plataformas de software como serviço (SaaS). É altamente recomendável que, em vez de usar protocolos nativos, como SSH ou RDP, o AWS Systems Manager Session Manager seja usado para todo o acesso administrativo às instâncias do Amazon EC2. Esse acesso pode ser controlado usando o IAM, que é seguro e auditado. Talvez também seja possível automatizar partes de seus playbook usando documentos de execução de comandos do AWS Systems Manager, o que pode reduzir os erros do usuário e melhorar o tempo de recuperação. Para acesso aos bancos de dados e a ferramentas de terceiros, recomendamos armazenar as credenciais de acesso no AWS Secrets Manager e conceder acesso aos perfis de respondedores a incidentes.

Por fim, o gerenciamento das contas do IAM de resposta a incidentes deve ser adicionado aos seus processos de Joiners, Movers e Leavers e revisado e testado periodicamente para verificar se somente o acesso pretendido é permitido.

Recursos

Documentos relacionados:

- Gerenciar o acesso elevado temporário ao seu ambiente da AWS
- Guia de resposta a incidentes de segurança da AWS

- AWS Elastic Disaster Recovery
- AWS Systems Manager Incident Manager
- Definir uma política de senhas de contas para usuários do IAM
- Usar a autenticação multifator (MFA) na AWS
- Configurar o acesso entre contas com MFA
- Usar o IAM Access Analyzer para gerar políticas do IAM
- Práticas recomendadas para Políticas de controle de serviços do AWS Organizations em um ambiente com várias contas
- Como receber notificações quando as chaves de acesso raiz da sua conta da AWS são usadas
- Criar permissões de sessão refinadas usando políticas gerenciadas pelo IAM
- Acesso de emergência

Vídeos relacionados:

- Automatizar a resposta a incidentes e a análise forense na AWS
- Guia de faça você mesmo para runbooks, relatórios de incidentes e resposta a incidentes
- Como se preparar e responder a incidentes de segurança no ambiente da AWS

SEC10-BP06 Implantar ferramentas previamente

Verifique se o pessoal de segurança tem as ferramentas certas pré-implantadas para reduzir o tempo de investigação até a recuperação.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

Para automatizar as funções de resposta e operações de segurança, é possível usar um conjunto abrangente de APIs e ferramentas da AWS. Você pode automatizar totalmente os recursos de gerenciamento de identidade, segurança de rede, proteção de dados e monitoramento e disponibilizá-los com métodos populares de desenvolvimento de software já em vigor. Quando você cria a automação da segurança, seu sistema pode monitorar, analisar e iniciar uma resposta, em vez de fazer com que as pessoas monitorem a sua posição de segurança e reajam manualmente a eventos.

Se as equipes de resposta a incidentes continuarem a responder aos alertas da mesma forma, haverá o risco de se acostumarem aos alertas. Com o passar do tempo, a equipe pode se tornar dessensibilizada para alertas e cometer erros ao lidar com situações comuns ou perder alertas incomuns. A automação ajuda a evitar a exaustão de alertas usando funções que processam alertas repetitivos e comuns, permitindo que as pessoas lidem com incidentes confidenciais e exclusivos. A integração de sistemas de detecção de anomalias, como Amazon GuardDuty, AWS CloudTrail Insights e Amazon CloudWatch Anomaly Detection, pode reduzir a carga de alertas baseados em limites comuns.

Você pode melhorar os processos manuais com a automatização programática das etapas do processo. Depois de definir o padrão de correção para um evento, você poderá decompor esse padrão em lógica acionável e desenvolver o código para executar essa lógica. Os respondedores podem executar esse código para corrigir o problema. Com o passar do tempo, você pode automatizar mais e mais etapas e, por fim, lidar automaticamente com classes inteiras de incidentes comuns.

Durante uma investigação de segurança, você precisa ser capaz de revisar os logs relevantes para registrar e compreender o escopo completo e o cronograma do incidente. Os logs também são necessários para geração de alertas indicando que determinadas ações de interesse ocorreram. É essencial selecionar, ativar, armazenar e configurar mecanismos de consulta e recuperação, bem como definir alertas. Além disso, uma forma eficaz de fornecer ferramentas para pesquisar dados de log é o Amazon Detective.

A AWS oferece mais de 200 serviços em nuvem e milhares de recursos. Recomendamos que você analise os serviços que podem apoiar e simplificar sua estratégia de resposta a incidentes.

Além do registro, você deve desenvolver e implementar uma estratégia de marcação. A marcação pode ajudar a fornecer contexto sobre a finalidade de um recurso da AWS. A marcação também pode ser usada para automação.

Etapas de implementação

Selecione e configure logs para análise e alertas

Consulte a documentação a seguir sobre como configurar logs para resposta a incidentes:

- Estratégias de log para resposta a incidentes de segurança
- SEC04-BP01 Configurar o registro em log de serviços e aplicações

Habilite serviços de segurança para oferecer suporte a detecção e resposta

A AWS fornece recursos nativos de detecção, prevenção e resposta, e outros serviços podem ser usados para arquitetar soluções de segurança personalizadas. Para obter uma lista dos serviços mais relevantes para resposta a incidentes de segurança, consulte Definições de capacidade de nuvem.

Desenvolva e implemente uma estratégia de marcação

Obter informações contextuais sobre o caso de uso empresarial e as partes interessadas internas relevantes em torno de um recurso da AWS pode ser difícil. Uma forma de fazer isso é na forma de tags, que atribuem metadados aos recursos da AWS e consistem em uma chave e um valor definidos pelo usuário. Você pode criar tags para categorizar os recursos por finalidade, proprietário, ambiente, tipo de dados processados e outros critérios de sua escolha.

Ter uma estratégia de marcação consistente pode acelerar os tempos de resposta e minimizar o tempo gasto no contexto organizacional, permitindo identificar e discernir rapidamente as informações contextuais sobre um recurso da AWS. As tags também podem servir como um mecanismo para iniciar automações de resposta. Para obter mais detalhes sobre o que marcar, consulte Como marcar seus recursos da AWS. Primeiro, você deve definir as tags que deseja implementar em toda a sua organização. Depois disso, você implementará e aplicará essa estratégia de marcação. Para obter mais detalhes sobre implementação e fiscalização, consulte Implementar a estratégia de marcação de recursos da AWS usando políticas de tags e políticas de controle de serviços (SCPs) da AWS.

Recursos

Práticas recomendadas do Well-Architected relacionadas:

- SEC04-BP01 Configurar o registro em log de serviços e aplicações
- SEC04-BP02 Capturar logs, descobertas e métricas em locais padronizados

Documentos relacionados:

- Estratégias de log para resposta a incidentes de segurança
- Definições de recursos de nuvem para resposta a incidentes

Exemplos relacionados:

- Detecção e resposta a ameaças com o Amazon GuardDuty e o Amazon Detective

- Workshop do Security Hub
- Gerenciamento de vulnerabilidades com o Amazon Inspector

SEC10-BP07 Executar simulações

À medida que as organizações crescem e evoluem com o tempo, o mesmo acontece com o cenário de ameaças, o que torna importante analisar continuamente seus recursos de resposta a incidentes. Executar simulações (também conhecidas como "game days") é um método que pode ser usado para realizar essa avaliação. As simulações usam cenários de eventos de segurança do mundo real projetados para imitar as táticas, as técnicas e os procedimentos (TTPs) de um agente de ameaças e permitir que uma organização exercite e avalie seus recursos de resposta a incidentes respondendo a esses eventos cibernéticos simulados da mesma forma que em uma situação real.

Benefícios de implantar esta prática recomendada: as simulações trazem vários benefícios:

- Validar a prontidão cibernética e desenvolver a confiança de seus socorristas.
- Testar a precisão e a eficiência de ferramentas e fluxos de trabalho.
- Refinar os métodos de comunicação e escalação alinhados ao seu plano de resposta a incidentes.
- Proporcionar uma oportunidade de responder a vetores menos comuns.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

Existem três tipos principais de simulações:

- Simulações teóricas: a abordagem de simulações teóricas é uma sessão baseada em discussões que envolvem as várias partes interessadas na resposta a incidentes para exercer funções e responsabilidades e usar ferramentas de comunicação e playbooks estabelecidos. A facilitação das simulações normalmente pode ser realizada em um dia inteiro em um local virtual, local físico ou uma combinação de ambos. Por ser baseada em discussões, a simulação teórica se concentra em processos, pessoas e colaboração. A tecnologia é parte integrante da discussão, mas o uso real de ferramentas ou scripts de resposta a incidentes geralmente não faz parte da simulação teórica.
- Simulações da equipe roxa: As simulações da equipe roxa aumentam o nível de colaboração entre os respondedores ao incidente (equipe azul) e os agentes de ameaças simuladas (equipe

vermelha). A equipe azul é composta por membros do centro de operações de segurança (SOC), mas também pode incluir outras partes interessadas que estariam envolvidas durante um evento cibernético real. A equipe vermelha é composta por uma equipe de testes de penetração ou pelas principais partes interessadas treinadas em segurança ofensiva. A equipe vermelha trabalha em colaboração com os facilitadores da simulação ao projetar um cenário que seja preciso e viável. Durante as simulações da equipe roxa, o foco principal está nos mecanismos de detecção, nas ferramentas e nos procedimentos operacionais padrão (SOPs) que apoiam os esforços de resposta a incidentes.

- Simulações da equipe vermelha: durante uma simulação da equipe vermelha, o infrator (equipe vermelha) realiza uma simulação para atingir um determinado objetivo ou conjunto de objetivos a partir de um escopo predeterminado. Os defensores (equipe azul) não necessariamente terão conhecimento do escopo e da duração da simulação, o que oferece uma avaliação mais realista de como eles responderiam a um incidente real. Como as simulações da equipe vermelha podem ser testes invasivos, tenha cuidado e implemente controles para verificar se a simulação não causa danos reais ao ambiente.

Considere facilitar as simulações cibernéticas em intervalos regulares. Cada tipo de simulação pode oferecer benefícios exclusivos aos participantes e à organização como um todo. Portanto, você pode optar por começar com tipos de simulação menos complexos (como simulações teóricas) e avançar para tipos de simulação mais complexos (simulações da equipe vermelha). Você deve selecionar um tipo de simulação com base em sua maturidade de segurança, recursos e resultados desejados. Alguns clientes podem não optar por realizar simulações da equipe vermelha devido à complexidade e ao custo.

Etapas de implementação

Independentemente do tipo de simulação que você escolher, as simulações geralmente seguem estas etapas de implementação:

1. Defina os elementos fundamentais da simulação: defina o cenário e os objetivos da simulação. Ambos devem ter aceitação da equipe de liderança.
2. Identifique as principais partes interessadas: no mínimo, a simulação precisa de facilitadores e participantes. Dependendo do cenário, outras partes interessadas, como departamento jurídico, de comunicação ou liderança executiva, podem estar envolvidos.
3. Crie e teste o cenário: talvez o cenário precise ser redefinido durante a criação se elementos específicos não forem viáveis. Espera-se um cenário finalizado como resultado dessa etapa.

4. Facilite a simulação: o tipo de simulação determina a facilitação usada (um cenário impresso em comparação a um cenário simulado altamente técnico). Os facilitadores devem alinhar suas táticas de facilitação aos objetos da simulação e envolver todos os participantes sempre que possível para proporcionar o máximo benefício.
5. Desenvolva o relatório pós-ação (AAR): identifique as áreas de sucesso, aquelas que podem ser melhoradas e possíveis lacunas. O AAR deve medir a eficácia da simulação, bem como a resposta da equipe ao evento simulado, para que o progresso possa ser monitorado ao longo do tempo com simulações futuras.

Recursos

Documentos relacionados:

- Guia de resposta a incidentes da AWS

Vídeos relacionados:

- AWS GameDay: edição de segurança
- Running effective security incident response simulations

Operações

As operações são a base da resposta a incidentes. É aqui que ocorrem as ações de resposta e atenuação de incidentes de segurança. As operações incluem as seguintes cinco fases: detecção, análise, contenção, erradicação e recuperação. As descrições dessas fases e dos objetivos podem ser encontradas na tabela a seguir.

Phase (Fase)	Objetivo
Detecção	Identifique um possível evento de segurança.
Análise	Determine se o evento de segurança é um incidente e avalie o escopo do incidente.
Contenção	Minimize e limite o escopo do evento de segurança.

Phase (Fase)	Objetivo
Erradicação	Remova recursos ou artefatos não autorizados relacionados ao evento de segurança. Implemente atenuações para as causas do incidente de segurança.
Recuperação	Restaure os sistemas ao estado seguro conhecido e monitore esses sistemas para verificar se não há retorno da ameaça.

As fases devem servir como orientação quando você responde e atua em incidentes de segurança, a fim de responder de forma eficaz e robusta. As ações reais realizadas variam de acordo com o incidente. Um incidente envolvendo ransomware, por exemplo, terá um conjunto de etapas de resposta a serem seguidas diferente do que o de um incidente que envolva um bucket público do Amazon S3. Além disso, essas fases não acontecem necessariamente de modo sequencial. Após a contenção e a erradicação, talvez seja necessário retornar à análise para entender se suas ações foram eficazes.

A preparação completa de seu pessoal, processos e tecnologia é fundamental para ser eficaz nas operações. Portanto, siga as práticas recomendadas da seção Preparação para poder responder com eficácia a um evento de segurança ativo.

Para saber mais, consulte a seção Operações do Guia de resposta a incidentes de segurança da AWS.

Atividade pós-incidente

O cenário de ameaças está mudando constantemente, e é importante ser igualmente dinâmico na capacidade de sua organização de proteger seus ambientes com eficácia. A chave para a melhoria contínua é iterar os resultados de seus incidentes e simulações a fim de melhorar seus recursos para detectar, responder e investigar com eficácia possíveis incidentes de segurança, reduzindo suas possíveis vulnerabilidades, o tempo de resposta e o retorno às operações seguras. Os mecanismos a seguir podem ajudar você a verificar se sua organização continua preparada com os recursos e os conhecimentos mais recentes para responder com eficácia, independentemente da situação.

Práticas recomendadas

SEC10-BP08 Estabelecer um framework para aprender com os incidentes

Implementar um framework de lições aprendidas e o recurso de análise da causa-raiz não só ajudará a melhorar os recursos de resposta a incidentes, mas também a evitar que o incidente se repita. Ao aprender com cada incidente, você pode ajudar a evitar a repetição dos mesmos erros, exposições ou configurações incorretas, não apenas melhorando seu procedimento de segurança, mas também minimizando o tempo perdido em situações evitáveis.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

É importante implementar um framework de lições aprendidas que estabeleça e atinja, em alto nível, os seguintes pontos:

- Quando um processo de lições aprendidas é realizado?
- O que está envolvido no processo de lições aprendidas?
- Como um processo de lições aprendidas é realizado?
- Quem está envolvido no processo e como?
- Como as áreas de melhoria serão identificadas?
- Como você garantirá que as melhorias sejam monitoradas e implementadas de forma eficaz?

O framework não deve se concentrar em culpar os indivíduos, mas sim na melhoria de ferramentas e processos.

Etapas de implementação

Além dos resultados de alto nível listados acima, é importante garantir que você faça as perguntas certas para obter o máximo valor (informações que levem a melhorias práticas) do processo. Considere estas perguntas para ajudar você a começar a promover discussões sobre lições aprendidas:

- Como foi o incidente?
- Quando o incidente foi identificado pela primeira vez?

- Como ele foi identificado?
- Que sistemas alertaram sobre a atividade?
- Que sistemas, serviços e dados estiveram envolvidos?
- O que ocorreu especificamente?
- O que funcionou bem?
- O que não funcionou bem?
- Que processos ou procedimentos falharam ou não tiveram a escala ajustada para responder ao incidente?
- O que pode ser melhorado nas seguintes áreas:
  - Pessoas
    - As pessoas que precisavam ser contatadas estavam realmente disponíveis e a lista de contatos estava atualizada?
    - As pessoas estavam perdendo treinamentos ou não tinham os recursos necessários para responder e investigar o incidente de forma eficaz?
    - Os recursos apropriados estavam prontos e disponíveis?
  - Processo
    - Os processos e procedimentos foram seguidos?
    - Os processos e procedimentos foram documentados e estavam disponíveis para esse (tipo de) incidente?
    - Havia processos e procedimentos necessários faltando?
    - Os respondedores conseguiram obter acesso oportuno às informações necessárias para responder ao problema?
  - Tecnologia
    - Os sistemas de alerta existentes identificaram e alertaram efetivamente sobre a atividade?
    - Como poderíamos ter reduzido o tempo de detecção em 50%?
    - Os alertas existentes precisam ser aprimorados ou novos alertas precisam ser criados para esse (tipo de) incidente?
    - As ferramentas existentes permitiram uma investigação (pesquisa/análise) eficaz do incidente?
    - O que pode ser feito para ajudar a identificar esse (tipo de) incidente mais cedo?
    - O que pode ser feito para ajudar a evitar que esse (tipo de) incidente ocorra novamente?
    - Quem é o proprietário do plano de melhoria e como você testará se ele foi implementado?

- Qual é o cronograma para que os controles e processos adicionais de monitoramento ou prevenção sejam implementados e testados?

Essa lista não inclui tudo, mas serve como ponto de partida para identificar quais são as necessidades da organização e da empresa e como você pode analisá-las para aprender com os incidentes de forma mais eficaz e melhorar constantemente seu procedimento de segurança. O mais importante é começar incorporando as lições aprendidas como parte padrão do processo de resposta a incidentes, da documentação e das expectativas das partes interessadas.

Recursos

Documentos relacionados:

- Guia de resposta a incidentes da AWS: estabelecer um framework para aprender com os incidentes
- Orientações do NCSC CAF: lições aprendidas

Segurança de aplicações

A segurança de aplicações (AppSec) retrata o processo geral de como projetar, criar e testar as propriedades de segurança das workloads desenvolvidas por você. Você precisa treinar a equipe adequadamente em sua organização, entender as propriedades de segurança de sua infraestrutura de compilação e lançamento e utilizar a automação para identificar problemas de segurança.

Adotar testes de segurança de aplicações como parte regular do ciclo de vida de desenvolvimento de software (SDLC) e processos de pós-lançamento ajuda a garantir que você tenha um mecanismo estruturado para identificar, corrigir e impedir que problemas de segurança de aplicações entrem no ambiente de produção.

Sua metodologia de desenvolvimento de aplicações deve incluir controles de segurança à medida que você projeta, cria, implanta e opera suas workloads. Ao fazer isso, alinhe o processo para redução contínua de defeitos e redução da dívida técnica. Por exemplo, o uso de modelagem de ameaças na fase de design ajuda a detectar falhas de design precocemente, o que torna mais fácil e menos caro corrigi-las em contraposição a aguardar e mitigá-las posteriormente.

O custo e a complexidade para resolver defeitos geralmente serão menores quanto mais no princípio do SDLC você estiver. A forma mais fácil de resolver problemas é não os ter. Por isso, começar com um modelo de ameaças ajuda você a se concentrar nos resultados corretos da fase de design. À medida que seu programa de AppSec amadurece, é possível aumentar a quantidade de testes realizados usando automação, aumentar a fidelidade do feedback para os criadores e reduzir o tempo necessário para as avaliações de segurança. Todas essas ações melhoram a qualidade do software desenvolvido e aumentam a velocidade de entrega de recursos à produção.

Essas diretrizes de implementação focam quatro áreas: organização e cultura, segurança do pipeline, segurança no pipeline e gerenciamento de dependências. Cada área oferece um conjunto de princípios que você pode implementar, bem como uma visão completa de como projetar, desenvolver, criar, implantar e operar workloads.

Na AWS, há várias abordagens para lidar com seu programa de segurança de aplicações. Algumas dessas abordagens dependem de tecnologia, enquanto outras focam a equipe e aspectos organizacionais do programa de segurança de aplicações.

Práticas recomendadas

- SEC11-BP01 Treinar para segurança de aplicações
- SEC11-BP02 Automatizar o teste durante o ciclo de vida de desenvolvimento e lançamento

- SEC11-BP03 Realizar teste de penetração regular
- SEC11-BP04 Realizar revisões de código
- SEC11-BP05 Centralizar serviços para pacotes e dependências
- SEC11-BP06 Implantar software programaticamente
- SEC11-BP07 Avaliar regularmente as propriedades de segurança dos pipelines
- SEC11-BP08 Criar um programa que incorpore a propriedade de segurança nas equipes de workload

SEC11-BP01 Treinar para segurança de aplicações

Forneça treinamento à sua equipe sobre práticas seguras de desenvolvimento e operação, o que os ajuda a criar software seguro e de alta qualidade. Essa prática ajuda sua equipe a prevenir, detectar e corrigir problemas de segurança no início do ciclo de vida do desenvolvimento. Considere um treinamento que abranja modelagem de ameaças, práticas seguras de codificação e uso de serviços para configurações e operações seguras. Forneça à sua equipe acesso ao treinamento por meio de recursos de autoatendimento e colete regularmente seus comentários para melhoria contínua.

Resultado desejado: você equipa sua equipe com o conhecimento e as habilidades necessárias para projetar e criar software com a segurança em mente desde o início. Por meio de treinamento em modelagem de ameaças e práticas seguras de desenvolvimento, sua equipe tem uma compreensão profunda dos possíveis riscos de segurança e de como mitigá-los durante o ciclo de vida de desenvolvimento de software (SDLC). Essa abordagem proativa de segurança faz parte da cultura da sua equipe, e você pode identificar e corrigir possíveis problemas de segurança desde o início. Como resultado, sua equipe fornece software e recursos seguros e de alta qualidade com mais eficiência, o que acelera o cronograma geral de entrega. Você tem uma cultura de segurança colaborativa e inclusiva em sua organização, na qual a propriedade da segurança é compartilhada por todos os criadores.

Práticas comuns que devem ser evitadas:

- Aguardar uma avaliação de segurança e só depois considerar as propriedades de segurança de um sistema.
- Deixar todas as decisões de segurança para uma equipe de segurança central.
- Não comunicar como as decisões tomadas no SDLC se relacionam às expectativas ou políticas de segurança gerais da organização.

- Iniciar o processo de avaliação da segurança muito tarde.

Benefícios de implementar esta prática recomendada:

- Melhor conhecimento dos requisitos organizacionais para a segurança na fase inicial do ciclo de desenvolvimento.
- Ser capaz de identificar e solucionar possíveis problemas de segurança com maior rapidez, promovendo uma entrega de recursos mais rápida.
- Maior qualidade do software e dos sistemas.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

Para criar software seguro e de alta qualidade, forneça treinamento à sua equipe sobre práticas comuns para desenvolvimento e operação de aplicações com segurança. Essa prática pode ajudar sua equipe a prevenir, detectar e corrigir problemas de segurança no início do ciclo de vida do desenvolvimento, o que pode acelerar o cronograma de entrega.

Para alcançar essa prática, considere treinar a equipe em modelagem de ameaças usando recursos da AWS, como o workshop de modelagem de ameaças. A modelagem de ameaças pode ajudar sua equipe a entender possíveis riscos de segurança e projetar sistemas com a segurança em mente desde o início. Além disso, você pode fornecer acesso ao Treinamento da AWS and Certification, indústria ou treinamento de parceiros da AWS sobre práticas seguras de desenvolvimento. Para conferir mais detalhes sobre uma abordagem abrangente para projetar, desenvolver, proteger e operar com eficiência em grande escala, consulte AWS DevOps Guidance.

Defina e comunique claramente o processo de avaliação da segurança da organização e descreva as responsabilidades da sua equipe, da equipe de segurança e de outras partes interessadas. Publique orientações de autoatendimento, exemplos de código e modelos que demonstrem como atender aos requisitos de segurança. Você pode usar serviços da AWS, como AWS CloudFormation, AWS Cloud Development Kit (AWS CDK) (AWS CDK) Constructs e Service Catalog, para fornecer configurações pré-aprovadas e seguras e reduzir a necessidade de configurações personalizadas.

Colete feedback regularmente da equipe sobre a experiência com o processo e o treinamento de avaliação da segurança e use esse feedback para promover melhorias contínuas. Conduza dias de jogos ou campanhas de combate de bugs para identificar e resolver problemas de segurança e, ao mesmo tempo, aprimorar as habilidades de sua equipe.

Etapas de implementação

1. Identifique as necessidades de treinamento: avalie o nível atual de habilidades e as lacunas de conhecimento da sua equipe em relação às práticas de desenvolvimento seguro por meio de pesquisas, revisões de código ou discussões com os membros da equipe.
2. Planeje o treinamento: com base nas necessidades identificadas, crie um plano de treinamento que aborde tópicos relevantes, como modelagem de ameaças, práticas seguras de codificação, testes de segurança e práticas de implantação segura. Empregue recursos, como o workshop de modelagem de ameaças, o Treinamento da AWS and Certification e programas de treinamento do setor ou de parceiros da AWS.
3. Agende e ofereça treinamento: agende sessões de treinamento ou workshops regulares para sua equipe. Eles podem ser conduzidos por um instrutor ou individualizados, dependendo das preferências e da disponibilidade da sua equipe. Incentive exercícios práticos e exemplos práticos para reforçar o aprendizado.
4. Defina um processo de análise de segurança: colabore com a equipe de segurança e outras partes interessadas para definir claramente o processo de revisão de segurança das aplicações. Documente as responsabilidades de cada equipe ou indivíduo envolvido no processo, incluindo sua equipe de desenvolvimento, equipe de segurança e outras partes interessadas relevantes.
5. Crie recursos de autoatendimento: desenvolva diretrizes de autoatendimento, exemplos de código e modelos que demonstrem como atender aos requisitos de segurança da sua organização. Considere serviços da AWS, como CloudFormation, AWS CDK Constructs e Service Catalog, para fornecer configurações pré-aprovadas e seguras e reduzir a necessidade de configurações personalizadas.
6. Comunique-se e socialize: comunique com eficácia o processo de revisão de segurança e os recursos de autoatendimento disponíveis para sua equipe. Conduza sessões de treinamento ou workshops para familiarizá-los com esses recursos e verificar se eles entendem como usá-los.
7. Obtenha feedback e melhore: colete feedback regularmente da equipe sobre a experiência com o processo e o treinamento de avaliação da segurança. Use esse feedback para identificar áreas de melhoria e refinar continuamente os materiais de treinamento, os recursos de autoatendimento e o processo de revisão de segurança.
8. Realize exercícios de segurança: organize dias de jogo ou campanhas de combate a bugs para identificar e resolver problemas de segurança nas aplicações. Esses exercícios não apenas ajudam a descobrir possíveis vulnerabilidades, mas também servem como oportunidades de aprendizado prático para sua equipe, aprimorando suas habilidades em desenvolvimento e operação seguros.

9. Continue aprendendo e melhorando: incentive sua equipe a se manter atualizada com as mais recentes práticas, ferramentas e técnicas de desenvolvimento seguro. Revise e atualize regularmente os materiais e recursos de treinamento para refletir o cenário de segurança em evolução e as práticas recomendadas.

Recursos

Práticas recomendadas relacionadas:

- SEC11-BP08 Criar um programa que incorpore a propriedade de segurança nas equipes de workload

Documentos relacionados:

- Treinamento da AWS e certificação
- Como pensar sobre a governança da segurança na nuvem
- Como abordar a modelagem de ameaças
- Acelerar o treinamento — AWS Skills Guild
- AWS DevOps Sagas

Vídeos relacionados:

- Segurança proativa: considerações e abordagens

Exemplos relacionados:

- Workshop sobre modelagem de ameaças
- Conscientização do setor para desenvolvedores

Serviços relacionados:

- AWS CloudFormation
- Constructos do AWS Cloud Development Kit (AWS CDK) (AWS CDK)
- Service Catalog

SEC11-BP02 Automatizar o teste durante o ciclo de vida de desenvolvimento e lançamento

Automatize o teste das propriedades de segurança durante o ciclo de vida de desenvolvimento e lançamento. Com a automação, é mais fácil identificar de forma consistente e repetível possíveis problemas no software antes do lançamento, o que reduz o risco de problemas de segurança no software que está sendo fornecido.

Resultado desejado: o objetivo dos testes automatizados é fornecer uma forma programática de detectar possíveis problemas com antecedência e frequência durante todo o ciclo de vida do desenvolvimento. Ao automatizar o teste de regressão, você pode executar novamente testes funcionais e não funcionais para verificar se o software testado anteriormente ainda funciona da forma esperada após uma alteração. Ao definir testes de unidade de segurança para conferir configurações incorretas comuns, como uma autenticação ausente ou danificada, é possível identificar e resolver esses problemas logo no início do processo de desenvolvimento.

A automação de testes utiliza casos de teste para um propósito específico para validação de aplicações, com base nos requisitos e na funcionalidade desejada da aplicação. O resultado dos testes automatizados baseia-se na comparação da saída do teste gerado com a respectiva saída esperada, o que acelera o ciclo de vida dos testes em geral. As metodologias de teste, como teste de regressão e pacotes de teste de unidade, são mais adequadas para automação. A automação dos testes de propriedades de segurança possibilita aos criadores receber feedback automatizado sem precisar esperar por uma avaliação da segurança. Os testes automatizados em forma de análise de código estático ou dinâmico podem melhorar a qualidade do código e ajudar a detectar possíveis problemas de software no ciclo de vida de desenvolvimento.

Práticas comuns que devem ser evitadas:

- Não comunicar os casos de teste e os resultados dos testes automatizados.
- Realizar os testes automatizados somente antes de um lançamento.
- Automatizar casos de teste com requisitos que mudam com frequência.
- Não fornecer orientações sobre como abordar os resultados dos testes de segurança.

Benefícios de implementar esta prática recomendada:

- Redução da dependência de pessoas que avaliam as propriedades de segurança dos sistemas.

- Descobertas consistentes em vários fluxos de trabalho que melhoram a consistência.
- Redução da probabilidade de introduzir problemas de segurança no software de produção.
- Redução do período de tempo entre a detecção e a correção devido à detecção precoce dos problemas de software.
- Maior visibilidade do problema sistêmico ou repetido entre os vários fluxos de trabalho, o que pode ser utilizado para promover melhorias em toda a organização.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

Ao criar um software, adote vários mecanismos de teste para garantir que você esteja testando os requisitos funcionais da aplicação com base na respectiva lógica de negócios e em requisitos não funcionais, os quais se focam a confiabilidade, a performance e a segurança da aplicação.

O teste de segurança de aplicação estática (SAST) analisa padrões de segurança anômalos no código-fonte e fornece indicações de código propenso a defeitos. O SAST depende de entradas estáticas, como documentação (especificação de requisitos, documentação e especificações de design) e código-fonte da aplicação, para testar uma série de problemas de segurança conhecidos. Os analisadores de código estático podem ajudar a acelerar a análise de grandes volumes de código. O NIST Quality Group fornece uma comparação de analisadores de segurança de código-fonte, que inclui ferramentas de código aberto para scanners de código em bytes e scanners de código binário.

Complemente seu teste estático com metodologias de teste de segurança de análise dinâmica (DAST), as quais realizam testes na aplicação em execução a fim de identificar comportamento possivelmente inesperado. O teste dinâmico pode ser utilizado para detectar possíveis problemas que não são detectáveis por meio de análise estática. Por meio dos testes nos estágios de repositório de código, compilação e pipeline, é possível impedir que diferentes tipos de problema em potencial ocorram no código. O Amazon Q Developer fornece recomendações de código, incluindo verificação de segurança, no IDE do construtor. O Amazon CodeGuru Security pode identificar problemas críticos, problemas de segurança e bugs difíceis de encontrar durante o desenvolvimento da aplicação e fornece recomendações para melhorar a qualidade do código. A extração da lista de materiais de software (SBOM) também permite extrair um registro formal contendo os detalhes e os relacionamentos dos vários componentes usados na construção do seu software. Isso permite que você informe o gerenciamento de vulnerabilidades e identifique rapidamente as dependências de software ou componentes e os riscos da cadeia de suprimentos.

O workshop Segurança para desenvolvedores usa ferramentas para desenvolvedores da AWS, como, AWS CodeBuild, AWS CodeCommit e AWS CodePipeline para automação do pipeline de lançamento que inclui metodologias de teste SAST e DAST.

À medida que você avançar no SDLC, estabeleça um processo iterativo que inclua avaliações de aplicação periódicas com sua equipe de segurança. O feedback coletado dessas avaliações de segurança deve ser abordado e validado como parte de sua revisão de prontidão do lançamento. Essas avaliações estabelecem um procedimento de segurança robusto de aplicações e fornecem aos criadores feedback útil para resolver possíveis problemas.

Etapas de implementação

- Implemente um IDE consistente, análise de código e ferramentas de CI/CD que incluam teste de segurança.
- Considere quando no SDLC é adequado bloquear pipelines em vez de apenas notificar os criadores de que problemas precisam ser corrigidos.
- O Automated Security Helper (ASH) é um exemplo de ferramenta de digitalização de segurança de código aberto.
- Realizar testes ou revisões de código usando ferramentas automatizadas, como o Amazon Q Developer integrado aos IDEs de desenvolvedores e o Amazon CodeGuru Security para verificar o código na confirmação, ajuda os criadores a obter feedback no momento certo.
- Ao compilar usando o AWS Lambda, é possível usar o Amazon Inspector para verificar o código da aplicação em suas funções.
- Quando testes automatizados são incluídos em pipelines de CI/CD, é necessário usar um sistema de emissão de tíquetes para rastrear a notificação e a correção de problemas de software.
- Para testes de segurança que podem gerar descobertas, a vinculação com orientações para correção ajuda os criadores a melhorar a qualidade do código.
- Analise regularmente as descobertas das ferramentas automatizadas para priorizar a próxima automação, o treinamento de criadores ou a campanha de conscientização.
- Para extrair o SBOM como parte de seus pipelines de CI/CD, use o Amazon Inspector SBOM Generator para produzir SBOMs para arquivos, imagens de contêineres, diretórios, sistemas locais e binários Go e Rust compilados no formato CycloneDX SBOM.

Recursos

Práticas recomendadas relacionadas:

- DevOps Guidance: DL.CR.3 Establish clear completion criteria for code tasks

Documentos relacionados:

- Entrega e implantação contínuas

- Parceiros de competência DevOps da AWS
- Parceiros de competência Segurança da AWS para segurança de aplicações
- Escolher uma abordagem de CI/CD do Well-Architected
- Detecção de segredos no Amazon CodeGuru Security
- Biblioteca de detecção de segurança do Amazon CodeGuru Security
- Acelerar as implantações na AWS com uma governança efetiva
- Como a AWS aborda a automatização de implantações seguras e sem intervenção manual
- Como o Amazon CodeGuru Security ajuda você a equilibrar de forma eficaz a segurança e a velocidade

Vídeos relacionados:

- Sem intervenção manual: como automatizar os pipelines de entrega contínua na Amazon
- Automatizar pipelines de CI/CD entre contas
- O processo de desenvolvimento de software na Amazon
- Testar software e sistemas na Amazon

Exemplos relacionados:

- Conscientização do setor para desenvolvedores
- Auxiliar de segurança automatizado (ASH)
- AWS CodePipeline Governance - Github

SEC11-BP03 Realizar teste de penetração regular

Realize um teste de penetração regular do software. Esse mecanismo ajuda a identificar possíveis problemas de software que não podem ser detectados pelo teste automatizado ou por uma revisão

manual do código. Ele também ajuda você a entender a eficácia dos controles de detecção. O teste de penetração deve tentar determinar se o software pode ser executado de formas inesperadas, por exemplo, expondo dados que devem ser protegidos ou concedendo permissões mais amplas que o esperado.

Resultado desejado: o teste de penetração é usado para detectar, corrigir e validar as propriedades de segurança da sua aplicação. O teste de penetração regular e agendado deve ser realizado como parte do ciclo de vida de desenvolvimento de software (SDLC). As descobertas do teste de penetração devem ser abordadas antes do lançamento do software. As descobertas do teste de penetração devem ser analisaras para identificar se há problemas que podem ser encontrados usando a automação. Ter um processo de teste de penetração regular e repetível que inclua um mecanismo de feedback ativo ajuda a transmitir as orientações aos criadores e melhora a qualidade do software.

Práticas comuns que devem ser evitadas:

- Realizar um teste de penetração somente para problemas de segurança conhecidos ou prevalentes.
- Realizar um teste de penetração em aplicações sem ferramentas e bibliotecas de terceiros dependentes.
- Realizar um teste de penetração em aplicações em busca de problemas de segurança de pacote e não avaliar a lógica de negócios implementada.

Benefícios de implementar esta prática recomendada:

- Maior confiança nas propriedades de segurança do software antes do lançamento.
- Oportunidade de identificar padrões de aplicação preferenciais, o que aumenta a qualidade do software.
- Um ciclo de feedback que identifica mais cedo no ciclo de desenvolvimento quando a automação ou treinamento adicional pode melhorar as propriedades de segurança do software.

Nível de risco exposto se esta prática recomendada não for estabelecida: Alto

Orientação para implementação

O teste de penetração é um exercício de teste de segurança estruturado em que você executa cenários de violação de segurança planejados a fim de detectar, corrigir e validar controles de

segurança. Os testes de penetração começam com o reconhecimento, fase durante a qual os dados são coletados com base no design atual da aplicação e nas respectivas dependências. Uma lista selecionada de cenários de teste específicos de segurança é criada e executada. A principal finalidade desses testes é revelar problemas de segurança em sua aplicação, os quais podem ser explorados para obter acesso não intencional ao seu ambiente ou acesso não autorizado aos dados. É necessáraio realizar o teste de penetração ao lançar novos recursos ou sempre que sua aplicação passar por alterações importantes na implementação técnica ou de funções.

É necessário identificar o estágio mais apropriado do ciclo de vida de desenvolvimento para realizar o teste de penetração. Esse teste deve ocorrer em uma fase tardia o suficiente para que a funcionalidade do sistema esteja próxima ao estado de lançamento pretendido, mas com tempo suficiente para corrigir todos os problemas.

Etapas de implementação

- Tenha um processo estruturado de como o teste de penetração é definido. Basear esse processo no modelo de ameaças é uma boa maneira de manter o contexto.
- Identifique o estágio apropriado do ciclo de vida de desenvolvimento para realizar o teste de penetração, o qual deverá ocorrer quando houver o mínimo de alterações esperadas na aplicação e tempo suficiente para realizar a correção.
- Treine os criadores sobre o que esperar das descobertas do teste de penetração e como ter informações sobre correção.
- Utilize ferramentas para acelerar o processo de testes de penetração automatizando testes comuns ou repetíveis.
- Analise as descobertas do teste de penetração para identificar problemas de segurança sistêmicos e utilize esses dados para embasar testes automatizados adicionais e a instrução contínua dos criadores.

Recursos

Práticas recomendadas relacionadas:

- SEC11-BP01 Treinar para segurança de aplicações
- SEC11-BP02 Automatizar o teste durante o ciclo de vida de desenvolvimento e lançamento

Documentos relacionados:

- O Teste de penetração da AWS fornece orientação detalhada para testes de penetração na AWS
- Acelerar as implantações na AWS com uma governança efetiva
- Parceiros de competência Segurança da AWS
- Modernizar sua arquitetura de testes de penetração no AWS Fargate
- AWS Fault Injection Simulator

Exemplos relacionados:

- Automatizar os testes de API com o AWS CodePipeline (GitHub)
- Auxiliar de segurança automatizado (GitHub)

SEC11-BP04 Realizar revisões de código

Implemente revisões de código para ajudar a verificar a qualidade e a segurança do software que está sendo desenvolvido. As revisões de código envolvem a participação de outros membros da equipe, além do autor do código original, na revisão do código em busca de possíveis problemas, vulnerabilidades e aderência aos padrões de codificação e às práticas recomendadas. Esse processo ajuda a detectar erros, inconsistências e falhas de segurança que podem ter sido ignoradas pelo desenvolvedor original. Use ferramentas automatizadas para ajudar nas revisões de código.

Resultado desejado: você inclui revisões de código durante o desenvolvimento para aumentar a qualidade do software que está sendo escrito. Você aprimora as habilidades dos membros menos experientes da equipe por meio de aprendizados identificados durante a revisão do código. Identifique oportunidades de automação e ofereça suporte ao processo de revisão de código usando ferramentas e testes automatizados.

Práticas comuns que devem ser evitadas:

- Não revisar o código antes da implantação.
- A mesma pessoa escreve e revisa o código.
- Não utilizar a automação para auxiliar ou orquestrar as revisões de código.
- Não treinar os criadores em segurança de aplicações antes de revisarem o código.

Benefícios de implementar esta prática recomendada:

- Código de melhor qualidade.
- Maior consistência do desenvolvimento do código por meio da reutilização de abordagens comuns.
- Redução no número de problemas descobertos durante o teste de penetração e em estágios posteriores.
- Maior transferência de conhecimentos na equipe.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

As revisões de código ajudam a verificar a qualidade e a segurança do software durante o desenvolvimento. As revisões manuais envolvem a participação de um membro da equipe, além do autor do código original, na revisão do código em busca de possíveis problemas, vulnerabilidades e aderência aos padrões de codificação e às práticas recomendadas. Esse processo ajuda a detectar erros, inconsistências e falhas de segurança que podem ter sido ignoradas pelo desenvolvedor original.

Considere o Amazon CodeGuru Security para ajudar a conduzir análises automatizadas de código. O CodeGuru Security usa machine learning e raciocínio automatizado para revisar o código e identificar possíveis vulnerabilidades de segurança e problemas de codificação. Integre revisões automatizadas de código com seus repositórios de código e pipelines de integração contínua/implantação contínua (CI/CD).

Etapas de implementação

1. Estabeleça um processo de revisão de código:
   - Defina quando as revisões de código devem ocorrer, como antes de mesclar o código na ramificação principal ou antes da implantação na produção.
   - Determine quem deve estar envolvido no processo de revisão de código, como membros da equipe, desenvolvedores seniores e especialistas em segurança.
   - Decida sobre a metodologia de revisão de código, incluindo o processo e as ferramentas a serem usadas.
2. Configure ferramentas de revisão de código:
   - Avalie e selecione ferramentas de revisão de código que atendam às necessidades da sua equipe, como Pull Requests do GitHub ou CodeGuru Security

- Integre as ferramentas escolhidas com seus repositórios de código e pipelines de CI/CD existentes.
- Configure as ferramentas para impor os requisitos de revisão de código, como o número mínimo de revisores e as regras de aprovação.

3. Defina uma lista de verificação e diretrizes de revisão de código:
   - Crie uma lista de verificação ou diretrizes de revisão de código que descrevam o que deve ser revisado. Considere fatores como qualidade do código, vulnerabilidades de segurança, aderência aos padrões de codificação e desempenho.
   - Compartilhe a lista de verificação ou as diretrizes com a equipe de desenvolvimento e verifique se todos entendem as expectativas.
4. Treine desenvolvedores sobre as práticas recomendadas de revisão de código:
   - Forneça treinamento à equipe sobre como conduzir revisões de código eficazes.
   - Eduque a equipe sobre os princípios de segurança de aplicações e as vulnerabilidades comuns a serem observadas durante as revisões.
   - Incentive o compartilhamento de conhecimento e sessões de programação em pares para aprimorar as habilidades dos membros menos experientes da equipe.
5. Implemente o processo de revisão de código:
   - Integre a etapa de revisão de código ao seu fluxo de trabalho de desenvolvimento, como criar uma pull request e designar revisores.
   - Exija que as alterações de código passem por uma revisão antes da fusão ou implantação.
   - Incentive a comunicação aberta e o feedback construtivo durante o processo de revisão.
6. Monitore e melhore:
   - Analise regularmente a eficácia do seu processo de revisão de código e obtenha feedback da equipe.
   - Identifique oportunidades de automação ou melhorias nas ferramentas para agilizar o processo de revisão de código.
   - Atualize e refine continuamente a lista de verificação ou as diretrizes de revisão de código com base nos aprendizados e nas práticas recomendadas do setor.
7. Promova uma cultura de revisão de código:
   - Enfatize a importância das revisões de código para manter a qualidade e a segurança do código.
   - Comemore os sucessos e os aprendizados do processo de revisão de código.

- Incentive um ambiente colaborativo e solidário em que os desenvolvedores se sintam à vontade para dar e receber feedback.

Recursos

Práticas recomendadas relacionadas:

- SEC11-BP02 Automatizar o teste durante o ciclo de vida de desenvolvimento e lançamento

Documentos relacionados:

- DevOps Guidance: DL.CR.2 Perform peer review for code changes
- Sobre solicitações pull no GitHub

Exemplos relacionados:

- Automatizar as revisões de código com o Amazon CodeGuru Security
- Automatizar a detecção de vulnerabilidades e bugs de segurança em pipelines de CI/CD usando a CLI do Amazon CodeGuru Security

Vídeos relacionados:

- Melhoria contínua da qualidade do código com o Amazon CodeGuru Security

SEC11-BP05 Centralizar serviços para pacotes e dependências

Forneça serviços centralizados para que as equipes obtenham pacotes de software e outras dependências. Isso permite validar pacotes antes que eles sejam incluídos no software que você escreve e fornece uma fonte de dados para a análise do software que está sendo usado na sua organização.

Resultado desejado: você cria sua workload a partir de pacotes de software externos, além do código que você escreve. Isso simplifica a implementação de funcionalidades que são utilizadas repetidamente, como um analisador JSON ou uma biblioteca de criptografia. Você centraliza as fontes desses pacotes e dependências para que a equipe de segurança possa validá-los antes que

eles sejam utilizados. Você utiliza essa abordagem com os fluxos de testes manuais e automatizados para aumentar a confiança na qualidade do software que desenvolve.

Práticas comuns que devem ser evitadas:

- Extrair pacotes de repositórios arbitrários na internet.
- Não testar novos pacotes antes de disponibilizá-los aos criadores.

Benefícios de implementar esta prática recomendada:

- Melhor entendimento de quais pacotes estão sendo utilizados no software que está sendo criado.
- Capacidade de notificar as equipes de workload quando um pacote precisa ser atualizado com base no entendimento de quem está usando o quê.
- Redução do risco de um pacote com problemas ser incluído em seu software.

Nível de risco exposto se esta prática recomendada não for estabelecida: Médio

Orientação para implementação

Forneça serviços centralizados para pacotes e dependências de uma forma simples para os criadores consumirem. Serviços centralizados podem ser centralizados logicamente em vez de implementados como um sistema monolítico. Essa abordagem possibilita fornecer serviços de uma forma que atenda às necessidades dos criadores. Você deve implementar uma forma eficiente de adicionar pacotes ao repositório quando ocorrerem atualizações ou surgirem novos requisitos. Serviços da AWS como o AWS CodeArtifact ou soluções similares de parceiros da AWS oferecem uma maneira de fornecer esse recurso.

Etapas de implementação

- Implemente um serviço de repositório centralizado logicamente disponível em todos os ambientes onde o software é desenvolvido.
- Inclua acesso ao repositório como parte do processo de provisionamento da Conta da AWS.
- Crie automação para testar pacotes antes de serem publicados em um repositório.
- Mantenha métricas dos pacotes mais utilizados, das linguagens e das equipes com a maior quantidade de alterações.
- Forneça um mecanismo automatizado para as equipes de criadores solicitarem novos pacotes e enviarem feedback.

- Verifique regularmente os pacotes em seu repositório para identificar o possível impacto de problemas recém-descobertos.

Recursos

Práticas recomendadas relacionadas:

- SEC11-BP02 Automatizar o teste durante o ciclo de vida de desenvolvimento e lançamento

Documentos relacionados:

- DevOps Guidance: DL.CS.2 Sign code artifacts after each build
- Níveis da cadeia de suprimentos para artefatos de software (SLSA)

Exemplos relacionados:

- Acelerar as implantações na AWS com uma governança efetiva
- Aumentar a segurança do seu pacote com o kit de ferramentas CodeArtifact Package Origin Control
- Pipeline de publicação de pacotes multirregionais (GitHub)
- Publicar módulos Node.js no AWS CodeArtifact usando o AWS CodePipeline (GitHub)
- Exemplo do Java CodeArtifact Pipeline no AWS CDK (GitHub)
- Distribuir pacotes .NET NuGet privados com o AWS CodeArtifact (GitHub)

Vídeos relacionados:

- Segurança proativa: considerações e abordagens
- A filosofia de segurança da AWS (re:Invent 2017)
- Quando a segurança, a proteção e a urgência são importantes: como lidar com o Log4Shell

SEC11-BP06 Implantar software programaticamente

Faça implantações de software de forma programática quando possível. Essa abordagem diminui a probabilidade de falha em uma implantação ou da introdução de um problema inesperado devido a erro humano.

Resultado desejado: a versão da workload que você testa é a versão que você implanta, e a implantação é sempre executada de forma consistente. Você externaliza a configuração da sua workload, o que ajuda você a implantar em diferentes ambientes sem alterações. Assinar de maneira criptográfica os pacotes de software é uma boa maneira de garantir que nada seja alterado entre os ambientes.

Práticas comuns que devem ser evitadas:

- Implantar software manualmente em produção.
- Realizar alterações manualmente no software para suprir diferentes ambientes.

Benefícios de implementar esta prática recomendada:

- Maior confiança no processo de lançamento de software.
- Redução do risco de uma alteração com falha afetar a funcionalidade dos negócios.
- Maior cadência de lançamentos devido ao menor risco de alterações.
- Recurso de reversão automática para eventos inesperados durante a implantação.
- Capacidade de comprovar de forma criptográfica que o software testado é o software implantado.

Nível de risco exposto se esta prática recomendada não for estabelecida: Alto

Orientação para implementação

Para manter uma infraestrutura de aplicações robusta e confiável, implemente práticas de implantação seguras e automatizadas. Essa prática envolve remover o acesso humano persistente dos ambientes de produção, usar ferramentas de CI/CD para implantações e externalizar dados de configuração específicos do ambiente. Ao seguir essa abordagem, você pode aprimorar a segurança, reduzir o risco de erros humanos e simplificar o processo de implantação.

Você pode criar uma estrutura de Conta da AWS para remover o acesso humano persistente dos ambientes de produção. Essa prática minimiza o risco de alterações não autorizadas ou modificações acidentais, o que melhora a integridade de seus sistemas de produção. Em vez do acesso humano direto, você pode usar ferramentas de CI/CD como AWS CodeBuilde AWS CodePipelinepara realizar implantações. Você pode usar esses serviços para automatizar os processos de criação, teste e implantação, o que reduz a intervenção manual e aumenta a consistência.

Para aprimorar ainda mais a segurança e a rastreabilidade, é possível assinar pacotes de aplicações depois de testados e validar essas assinaturas durante a implantação. Para fazer isso, use ferramentas criptográficas como AWS Signerou AWS Key Management Service(AWS KMS). Ao assinar e verificar pacotes, você pode garantir a implantação somente de código autorizado e validado em seus ambientes.

Além disso, sua equipe pode arquitetar a workload para obter dados de configuração específicos do ambiente de uma fonte externa, como o AWS Systems Manager Parameter Store. Essa prática separa o código da aplicação dos dados de configuração, o que ajuda você a gerenciar e atualizar as configurações de maneira independente, sem modificar o código da aplicação em si.

Para simplificar o provisionamento e o gerenciamento da infraestrutura, considere usar ferramentas de infraestrutura como código (IaC), como AWS CloudFormation ou AWS CDK. Você pode usar essas ferramentas para definir sua infraestrutura como código, o que melhora a consistência e a repetibilidade das implantações em diferentes ambientes.

Considere as implantações canário para validar a implantação bem-sucedida do software. As implantações canário envolvem a implementação de alterações em um subconjunto de instâncias ou usuários antes da implantação em todo o ambiente de produção. Em seguida, você pode monitorar o impacto das mudanças e revertê-las, se necessário, o que minimiza o risco de problemas generalizados.

Siga as recomendações descritas no whitepaper Organizando seu AWS ambiente usando várias contas. Este whitepaper fornece orientação sobre como separar ambientes (como desenvolvimento, preparação e produção) em Contas da AWS distintas, o que aumenta ainda mais a segurança e o isolamento.

Etapas de implementação

1. Configure a estrutura de Conta da AWS:
    - Siga as orientações no whitepaper Organizing Your AWS Environment Using Multiple Accounts para criar Contas da AWS separadas para diferentes ambientes (por exemplo, desenvolvimento, preparação e produção).
    - Configure os controles e permissões de acesso apropriados para cada conta para restringir o acesso humano direto aos ambientes de produção.
2. Implemente um pipeline de CI/CD:
    - Configure um pipeline de CI/CD usando serviços, como AWS CodeBuild e AWS CodePipeline.

- Configure o pipeline para criar, testar e implantar automaticamente o código da aplicação nos respectivos ambientes.
- Integre repositórios de código com o pipeline de CI/CD para controle de versão e gerenciamento de código.

3. Assine e verifique pacotes de aplicações:
   - Use o AWS Signer ou o AWS Key Management Service (AWS KMS) para assinar os pacotes de aplicações depois de testados e validados.
   - Configure o processo de implantação para verificar as assinaturas dos pacotes de aplicações antes de implantá-los nos ambientes de destino.
4. Externalize os dados de configuração:
   - Armazene dados de configuração específicos do ambiente no AWSSystems Manager Parameter Store.
   - Modifique o código da aplicação para recuperar dados de configuração do Parameter Store durante a implantação ou o runtime.
5. Implemente a infraestrutura como código (IaC):
   - Use ferramentas de IaC como AWS CloudFormationou AWS CDKpara definir e gerenciar sua infraestrutura como código.
   - Crie modelos do CloudFormation ou scripts de CDK para provisionar e configurar os recursos da AWS necessários para a aplicação.
   - Integre a IaC ao seu pipeline de CI/CD para implantar automaticamente as alterações na infraestrutura com as alterações no código da aplicação.
6. Implemente implantações canário:
   - Configure o processo de implantação para oferecer suporte a implantações canário, em que as alterações são implementadas em um subconjunto de instâncias ou usuários antes de serem implantadas em todo o ambiente de produção.
   - Use serviços, como o AWS CodeDeploy ou o AWS ECS, para gerenciar implantações canário e monitorar o impacto das mudanças.
   - Implemente mecanismos de reversão para reverter para a versão estável anterior se forem detectados problemas durante a implantação canário.
7. Monitore e audite:
   - Configure mecanismos de monitoramento e registro em log para rastrear implantações, desempenho de aplicações e mudanças na infraestrutura.

- Use serviços, como o Amazon CloudWatch e o AWS CloudTrail, para coletar e analisar logs e métricas.
- Implemente verificações de auditoria e conformidade para verificar a adesão às práticas recomendadas de segurança e aos requisitos regulatórios.

8. Melhore continuamente:
   - Analise e atualize regularmente suas práticas de implantação e incorpore feedback e lições aprendidas em implantações anteriores.
   - Automatize o máximo possível do processo de implantação para reduzir a intervenção manual e possíveis erros humanos.
   - Colabore com equipes multifuncionais (por exemplo, operações ou segurança) para alinhar e melhorar continuamente as práticas de implantação.

Seguindo essas etapas, você pode implementar práticas de implantação seguras e automatizadas em seu AWS ambiente, o que aumenta a segurança, reduz o risco de erros humanos e simplifica o processo de implantação.

Recursos

Práticas recomendadas relacionadas:

- SEC11-BP02 Automatizar o teste durante o ciclo de vida de desenvolvimento e lançamento
- O DL.CI.2 Trigger é criado automaticamente com base nas modificações do código-fonte

Documentos relacionados:

- Acelerar as implantações na AWS com uma governança efetiva
- Automatizar implantações seguras e sem intervenção manual
- Assinatura de código usando CA privada do AWS Certificate Manager e chaves assimétricas do AWS Key Management Service
- Assinatura de código, um controle de confiança e integridade para AWS Lambda

Vídeos relacionados:

- Sem intervenção manual: como automatizar os pipelines de entrega contínua na Amazon

Exemplos relacionados:

- Implantações azuis/verdes com o AWS Fargate

SEC11-BP07 Avaliar regularmente as propriedades de segurança dos pipelines

Aplique os princípios do pilar Segurança do Well-Architected aos seus pipelines, com atenção especial à separação das permissões. Avalie as propriedades de segurança de sua infraestrutura de pipelines. O gerenciamento eficaz da segurança dos pipelines permite fornecer segurança ao software que passa pelos pipelines.

Resultado desejado: os pipelines usados para criar e implantar o software seguem as mesmas práticas recomendadas de qualquer outra workload no ambiente. Os testes que você implementa em seus pipelines não são editáveis pelas equipes que os usam. Você concede aos pipelines somente as permissões necessárias para as implantações que eles estão realizando usando credenciais temporárias. Você implementa proteções para evitar que os pipelines sejam implantados nos ambientes errados. Você configura os pipelines para emitir o estado de modo que a integridade dos ambientes de compilação possa ser validada.

Práticas comuns que devem ser evitadas:

- Testes de segurança que podem ser ignorados pelos criadores.
- Permissões excessivamente amplas para pipelines de implantação.
- Pipelines não configurados para validar entradas.
- Ausência de análise regular das permissões associadas à infraestrutura de CI/CD.
- Uso de credenciais de longo prazo ou codificadas.

Benefícios de implementar esta prática recomendada:

- Maior confiança na integridade do software que está sendo criado e implantado pelos pipelines.
- Capacidade de interromper uma implantação quando há atividade suspeita.

Nível de risco exposto se esta prática recomendada não for estabelecida: Alto

Orientação para implementação

Seus pipelines de implantação são um componente essencial do ciclo de vida de desenvolvimento de software e devem seguir os mesmos princípios e práticas de segurança de qualquer outra workload em seu ambiente. Isso inclui a implementação de controles de acesso adequados, validação de entradas e revisão e auditoria regulares das permissões associadas à infraestrutura de CI/CD.

Verifique se as equipes responsáveis pela criação e implantação de aplicações não têm a capacidade de editar ou ignorar os testes e as verificações de segurança implementados nos pipelines. Essa separação de preocupações ajuda a manter a integridade de seus processos de criação e implantação.

Como ponto de partida, considere empregar a arquitetura de referência dos pipelines de implantação da AWS. Essa arquitetura de referência fornece uma base segura e escalável para a criação dos pipelines de CI/CD na AWS.

Além disso, você pode usar serviços como o AWS Identity and Access Management Access Analyzer para gerar políticas do IAM com privilégio mínimo para as permissões do pipeline e como uma etapa do pipeline para verificar as permissões da workload. Isso ajuda a verificar se seus pipelines e workloads têm somente as permissões necessárias para suas funções específicas, o que reduz o risco de acesso ou ações não autorizadas.

Etapas de implementação

- Comece com a arquitetura de referência dos pipelines de implantação da AWS.
- Considere usar o AWS IAM Access Analyzer para gerar programaticamente políticas do IAM com privilégios mínimos para os pipelines.
- Integre seus pipelines com monitoramento e alertas para receber notificações sobre atividades inesperadas ou anormais. Para serviços gerenciados da AWS, o Amazon EventBridge permite direcionar dados para destinos como o AWS Lambda ou o Amazon Simple Notification Service (Amazon SNS).

Recursos

Documentos relacionados:

- Arquitetura de referência dos pipelines de implantação da AWS

- Monitorar o AWS CodePipeline
- Práticas recomendadas de segurança para o AWS CodePipeline

Exemplos relacionados:

- Painel de monitoramento do DevOps (GitHub)

SEC11-BP08 Criar um programa que incorpore a propriedade de segurança nas equipes de workload

Crie um programa ou mecanismo que capacite as equipes de criadores a tomar decisões de segurança sobre o software que elas estão criando. Ainda é necessário que sua equipe de segurança valide essas decisões durante uma revisão, mas a incorporação da propriedade de segurança nas equipes de criadores aumenta a velocidade e segurança do processo de criação de workloads. Esse mecanismo também promove uma cultura de propriedade que afeta de forma positiva a operação dos sistemas que você cria.

Resultado desejado: você incorporou a propriedade de segurança e a tomada de decisões em suas equipes. Você treinou suas equipes sobre como pensar em segurança ou aumentou a equipe com pessoas de segurança incorporadas ou associadas. Como resultado, suas equipes tomam decisões de segurança de melhor qualidade logo no início do ciclo de desenvolvimento.

Práticas comuns que devem ser evitadas:

- Deixar todas as decisões de design de segurança para a equipe de segurança.
- Não abordar os requisitos de segurança cedo o suficiente no processo de desenvolvimento.
- Não obter feedback dos criadores e do pessoal de segurança sobre a operação do programa.

Benefícios de implementar esta prática recomendada:

- Redução do tempo para concluir as avaliações de segurança.
- Redução dos problemas de segurança que são detectados apenas no estágio de avaliação da segurança.
- Melhoria da qualidade geral do software que está sendo escrito.
- Oportunidade de identificar e entender problemas sistêmicos ou áreas de melhoria de alto valor.

- Redução da quantidade de revisão necessária devido às descobertas da avaliação da segurança.
- Melhoria da percepção da função de segurança.

Nível de risco exposto se esta prática recomendada não for estabelecida: Baixo

Orientação para implementação

Comece com a orientação em SEC11-BP01 Treinar para segurança de aplicações. Depois, identifique o modelo operacional para o programa que você acredita ser o melhor para a sua organização. Os dois padrões principais são treinar os criadores ou incorporar o pessoal de segurança às equipes de criadores. Depois de decidir sobre a abordagem inicial, é necessário criar um piloto com uma equipe de workload ou um grupo pequeno de equipes de workload para comprovar que o modelo funciona para sua organização. O apoio de liderança dos criadores e da segurança da organização contribui para a entrega e o sucesso do programa. À medida que você criar esse programa, é importante selecionar as métricas que podem ser utilizadas para mostrar seu valor. Saber como a AWS resolveu esse problema é uma boa experiência de aprendizado. A prática recomendada é muito concentrada na mudança e cultura organizacionais. As ferramentas que você utiliza devem ser compatíveis com a colaboração entre as comunidades de criadores e de segurança.

Etapas de implementação

- Comece com o treinamento dos criadores para segurança de aplicações.
- Crie uma comunidade e um programa de integração para instruir os criadores.
- Selecione um nome para o programa. Guardiões, patrocinadores ou defensores são utilizados com frequência.
- Identifique o modelo a ser utilizado: treinar criadores, incorporar engenheiros de segurança e ter perfis de segurança de afinidade.
- Identifique patrocinadores do projeto em grupos de segurança e de criadores e possivelmente em outros grupos relevantes.
- Rastreie as métricas do número de pessoas envolvidas no programa, o tempo gasto em avaliações e o feedback dos criadores e do pessoal de segurança. Utilize essas métricas para realizar melhorias.

Recursos

Práticas recomendadas relacionadas:

- SEC11-BP01 Treinar para segurança de aplicações
- SEC11-BP02 Automatizar o teste durante o ciclo de vida de desenvolvimento e lançamento

Documentos relacionados:

- Como abordar a modelagem de ameaças
- Como pensar sobre a governança da segurança na nuvem
- How AWS built the Security Guardians program, a mechanism to distribute security ownership
- Como criar um programa Security Guardians para distribuir a propriedade da segurança

Vídeos relacionados:

- Segurança proativa: considerações e abordagens
- AppSec tooling and culture tips from AWS and Toyota Motor North America

Conclusão

A segurança é um esforço contínuo. Quando ocorrem incidentes, eles devem ser tratados como oportunidades de melhorar a segurança da arquitetura. Ter controles fortes de identidade, automatizar respostas a eventos de segurança, proteger a infraestrutura em vários níveis e usar criptografia para gerenciar dados bem classificados proporcionam a defesa profunda que todas as empresas devem implementar. Esse trabalho é facilitado graças às funções programáticas e aos recursos e serviços da AWS discutidos neste documento.

A AWS se esforça para ajudar você a criar e operar arquiteturas que protegem informações, sistemas e ativos, enquanto agregam valor de negócios.

Colaboradores

Os seguintes indivíduos e organizações contribuíram para este documento:

- Jay Michael, arquiteto líder de soluções de segurança, Amazon Web Services
- Kiaan Sumeet, consultor líder de segurança, Amazon Web Services
- Michael Fischer, arquiteto líder de soluções, Amazon Web Services
- Conor Colgan, arquiteto líder de soluções, Amazon Web Services
- Dave Walker, arquiteto líder de soluções, segurança e conformidade, Amazon Web Services
- Patrick Palmer, arquiteto líder de soluções, segurança e conformidade, Amazon Web Services
- Monka Vu Minh, consultora de segurança, Amazon Web Services
- Kurt Kumar, consultor de segurança, Amazon Web Services
- Fahima Khan, arquiteta de soluções de segurança, Amazon Web Services
- Mutaz Hajeer, arquiteto sênior de soluções de segurança, Amazon Web Services
- Luis Pastor, arquiteto sênior de soluções de segurança, Amazon Web Services
- Colin Igbokwe, arquiteto sênior de soluções de segurança, Amazon Web Services
- Geoff Sweet, arquiteto sênior de soluções de segurança, Amazon Web Services
- Anthony Harvey, arquiteto sênior de soluções de segurança, Amazon Web Services
- Sowjanya Rajavaram, arquiteta sênior de soluções de segurança, Amazon Web Services
- Krishna Prasad, arquiteto sênior de soluções, Amazon Web Services
- Faisal Farooq, arquiteto sênior de soluções, Amazon Web Services
- Arun Krishnaswamy, arquiteto sênior de soluções, Amazon Web Services
- Dan Girard, arquiteto sênior de soluções, Amazon Web Services
- Marc Luescher, arquiteto sênior de soluções, Amazon Web Services
- Kyle Nicodemus, gerente técnico sênior de conta, Amazon Web Services
- Irina Szabo, gerente técnica sênior de conta, Amazon Web Services
- Arun Sivaraman, arquiteto de soluções, Amazon Web Services
- Stephen Novak, gerente técnico de conta, Amazon Web Services
- Jonathan Risbrook, gerente técnico de conta, Amazon Web Services
- Freddy Kasprzykowski, gerente de prática, Serviços financeiros globais, Amazon Web Services
- Pat Gaw, consultor líder de segurança, Amazon Web Services

- Jason Garman, arquiteto líder de soluções de segurança, Amazon Web Services
- Mark Keating, arquiteto líder de soluções de segurança, Amazon Web Services
- Zach Miller, arquiteto líder de soluções de segurança, Amazon Web Services
- Maitreya Ranganath, arquiteto líder de soluções de segurança, Amazon Web Services
- Reef Dsouza, arquiteto de soluções de segurança, Amazon Web Services
- Brad Burnett, arquiteto de soluções de segurança, Amazon Web Services
- Matt Saner, gerente sênior, Arquitetura de soluções de segurança, Amazon Web Services
- Priyank Ghedia, arquiteto sênior de soluções de segurança, Amazon Web Services
- Arthur Mnev, arquiteto sênior de soluções de segurança, Amazon Web Services
- Kyle Dickinson, arquiteto sênior de soluções de segurança, Amazon Web Services
- Kevin Boland, arquiteto sênior de soluções de segurança, Amazon Web Services
- Anna McAbee, arquiteta sênior de soluções de segurança, Amazon Web Services
- Recep Meric Degirmenci, arquiteto sênior de soluções de segurança, Amazon Web Services
- Daniel Salzedo, gerente técnico sênior de produtos de segurança, Amazon Web Services
- Jake Izumi, arquiteto sênior de soluções, Amazon Web Services
- Bert Bullough, arquiteto sênior de soluções, Amazon Web Services
- Robert McCall, arquiteto sênior de soluções, Amazon Web Services
- Angela Chao, ESL TAM, AWS Enterprise Support, Amazon Web Services
- Pratima Singh, especialista sênior em segurança ANZ arquiteta de soluções sênior, Amazon Web Services
- Darran Boyd, chefe de departamento do CISO, segurança da AWS, Amazon Web Services
- Kevin Boland, arquiteto sênior de soluções de segurança, Amazon Web Services

Outras fontes de leitura

Para obter ajuda adicional, consulte as seguintes fontes:

- Whitepaper AWS Well-Architected Framework
- Centro de Arquitetura do AWS

Revisões do documento

Para ser notificado sobre atualizações desse whitepaper, inscreva-se no feed RSS.

Alteração	Descrição	Data
Orientação atualizada sobre práticas recomendadas	As práticas recomendadas foram atualizadas com novas diretrizes nas seguintes áreas: SEC 2, SEC 3, SEC 4, SEC 6, SEC 7, SEC 8, SEC 9, SEC 10 e SEC 11. A orientação foi atualizada e refinada em todo o pilar.	6 de novembro de 2024
Orientação atualizada sobre práticas recomendadas	Atualizações em grande escala nas práticas recomendadas foram feitas em todo o pilar. Várias práticas recomendadas foram reordenadas e consolidadas. Mudanças significativas nos SEC 1, 4, 5, 6, 7, 8 e 9.	27 de junho de 2024
Orientação atualizada sobre práticas recomendadas	As práticas recomendadas foram atualizadas com novas diretrizes nas seguintes áreas: Operar workloads com segurança e Proteger dados em trânsito.	6 de dezembro de 2023
Orientação atualizada sobre práticas recomendadas	Atualizações importantes na orientação e nas práticas recomendadas em Resposta a incidentes.	3 de outubro de 2023

	Várias práticas recomendadas atualizadas em Preparação. Duas novas áreas adicionadas a Resposta a incidentes: Operações e Atividades pós-incidentes. Nova prática recomendada SEC10-BP08 Estabelecer uma estrutura para aprender com os incidentes adicionada.	
Orientação atualizada sobre práticas recomendadas	As práticas recomendadas foram atualizadas com novas orientações nas seguintes áreas: Preparar e Simular.	13 de julho de 2023
Atualizações para o novo Framework.	Atualizações nas práticas recomendadas com recomendações e adição de novas práticas recomendadas. Nova área de práticas recomendadas de segurança de aplicações (AppSec) adicionada.	10 de abril de 2023
Whitepaper atualizado	Práticas recomendadas atualizadas com novas orientações para implementação.	15 de dezembro de 2022
Whitepaper atualizado	Práticas recomendadas ampliadas e planos de melhoria adicionados.	20 de outubro de 2022
Atualização secundária	Informações do IAM atualizadas para refletir as práticas recomendadas atuais.	28 de junho de 2022

Atualização secundária	Informações adicionais do AWS PrivateLink incluídas e links quebrados corrigidos.	19 de maio de 2022
Atualização secundária	Adição do AWS PrivateLink.	6 de maio de 2022
Atualização secundária	Remoção de linguagem não inclusiva.	22 de abril de 2022
Atualização secundária	Adicionadas informações sobre o Analisador de Acesso à Rede da VPC.	2 de fevereiro de 2022
Atualização secundária	Link quebrado corrigido.	27 de maio de 2021
Atualização secundária	Alterações editoriais de modo geral.	17 de maio de 2021
Atualização principal	Seção adicionada sobre governança, detalhes adicionados a várias seções, novos recursos e serviços adicionados.	7 de maio de 2021
Atualização secundária	Links atualizados.	10 de março de 2021
Atualização secundária	Link quebrado corrigido.	15 de julho de 2020
Atualizações para o novo Framework	Atualização de orientaçõ es sobre gerenciamento de contas, identidades e permissões.	8 de julho de 2020
Atualizações para o novo Framework	Atualizado para estender orientações a todas as áreas, novas práticas recomendadas, serviços e recursos.	30 de abril de 2020

Whitepaper atualizado	Atualizações para refletir novos serviços e recursos da AWS e referências atualizadas.	1º de julho de 2018
Whitepaper atualizado	Seção Configuração e manutenção da segurança do sistema atualizada para refletir os novos serviços e recursos da AWS.	1 de maio de 2017
Publicação inicial	Publicação de Pilar Segurança : AWS Well-Architected Framework.	1º de novembro de 2016

Avisos

Os clientes são responsáveis por fazer a própria avaliação independente das informações contidas neste documento. Este documento: (a) é apenas para fins informativos, (b) representa as ofertas e práticas de produtos atuais da AWS, que estão sujeitas a alterações sem aviso prévio e (c) não criam nenhum compromisso ou garantia da AWS e de suas afiliadas, fornecedores ou licenciadores. Os produtos ou serviços da AWS são fornecidos “no estado em que se encontram”, sem garantias, representações ou condições de qualquer tipo, expressas ou implícitas. As responsabilidades e as obrigações da AWS com os seus clientes são controladas por contratos da AWS, e este documento não é parte de, nem modifica, qualquer contrato entre a AWS e seus clientes.

Glossário da AWS

Para obter a terminologia mais recente da AWS, consulte o glossário da AWS na Referência do Glossário da AWS.