Guia técnico da AWS

Guia de resposta a incidentes de segurança da AWS

Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Guia de resposta a incidentes de segurança da AWS: Guia técnico da AWS

Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e o visual comercial da Amazon não podem ser usados em conexão com nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa causar confusão entre os clientes ou que deprecie ou desacredite a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, conectados ou patrocinados pela Amazon.

Table of Contents

Resumo ... 1
Introdução ... 2
Antes de começar ... 2
Perspectiva de segurança do AWS CAF ... 3
Fundamento da resposta a incidentes ... 3
Educar ... 5
Responsabilidade compartilhada ... 5
Resposta a incidentes na nuvem ... 8
Elaborar objetivos da resposta da nuvem ... 8
Incidentes de segurança na nuvem ... 9
Domínios de incidentes ... 9
Indicadores de eventos de segurança na nuvem ... 10
Noções básicas dos recursos de nuvem ... 12
Privacidade dos dados ... 12
Resposta da AWS ao uso abusivo e comprometimento de recursos ... 13
Preparar: pessoas ... 15
Definir funções e responsabilidades ... 15
Fornecer treinamento ... 16
Definir mecanismos de resposta ... 17
Criar uma cultura de segurança receptiva e adaptável ... 17
Prever a resposta ... 18
Parceiros e a janela de resposta ... 18
Risco desconhecido ... 20
Preparar: tecnologia ... 23
Preparar o acesso às contas da AWS ... 23
Acesso indireto ... 24
Acesso direto ... 24
Acesso alternativo ... 25
Acesso à automação ... 25
Acesso a Managed Services ... 26
Preparar processos ... 26
Árvores de decisão ... 27
Usar contas alternativas ... 27
Exibir ou copiar dados ... 28

Compartilhar snapshots do Amazon EBS ... 28
Compartilhar o Amazon CloudWatch Logs ... 29
Usar armazenamento imutável ... 29
Iniciar recursos próximos ao evento ... 30
Isolar recursos ... 31
Iniciar estações de trabalho forenses ... 31
Suporte do provedor de nuvem ... 32
AWS Managed Services ... 33
AWS Support ... 33
Suporte de resposta DDoS ... 34
Simular ... 35
Simulações de resposta a incidentes de segurança ... 35
Etapas de simulação ... 36
Exemplos de simulação ... 36
Iteração ... 38
Runbooks ... 38
Criar runbooks ... 39
Conceitos básicos ... 39
Automação ... 40
Automatizar a resposta a incidentes ... 40
Resposta orientada por eventos ... 46
Exemplos de resposta a incidentes ... 48
Incidentes de domínio de serviço ... 48
Identidades ... 48
Recursos ... 49
Incidentes do domínio de infraestrutura ... 49
Decisões de investigação ... 51
Capturar dados voláteis ... 52
Usar o AWS Systems Manager ... 52
Automatizar a captura ... 53
Conclusão ... 54
Recursos adicionais ... 55
Mídia ... 55
Ferramentas de terceiros ... 56
Referências do setor ... 56
Revisões do documento ... 57

Apêndice A: Definições de capacidade da nuvem ... 58
Registro em log e eventos ... 58
Visibilidade e alertas ... 60
Automação ... 62
Armazenamento seguro ... 63
Personalizar ... 64
Apêndice B: Código de exemplo ... 65
Evento de exemplo AWS CloudTrail ... 65
Exemplo do AWS CloudWatch Events ... 66
Exemplo de atividades de CLI de domínio ... 66
Apêndice C: Exemplo de runbook ... 68
Runbook de resposta a incidentes: uso básico ... 68
Objetivo ... 68
Pressuposições ... 68
Indicadores de comprometimento ... 69
Etapas de correção: estabelecer o controle ... 69
Outras ações: determinar o impacto ... 69
Avisos ... 71

Guia de resposta a incidentes de segurança da AWS

Data de publicação: 23 de novembro de 2020 (Revisões do documento)

Este guia apresenta os princípios básicos da resposta a incidentes de segurança no ambiente da Nuvem AWS de um cliente. Ele se concentra em uma visão geral dos conceitos de segurança na nuvem e resposta a incidentes e identifica recursos, serviços e mecanismos de nuvem que estão disponíveis para clientes que estão respondendo a problemas de segurança.

Este documento se destina a pessoas em funções técnicas e pressupõe que você esteja familiarizado com os princípios gerais de segurança da informação, tenha uma compreensão básica da resposta a incidentes em seus ambientes on-premises atuais e tenha alguma familiaridade com os serviços de nuvem.

Introdução

A segurança é a maior prioridade na AWS. Como cliente da AWS, você aproveita um datacenter e uma arquitetura de rede criados para atender aos requisitos das empresas com as maiores exigências de segurança. A Nuvem AWS tem um modelo de responsabilidade compartilhada. A AWS gerencia a segurança da nuvem. Você é responsável pela sua segurança na nuvem. Isso significa que você retém o controle da segurança escolhido para implementação. Você tem acesso a centenas de ferramentas e serviços para ajudar a atingir seus objetivos de segurança. Esses recursos ajudam a estabelecer uma referência de segurança que atenda aos seus objetivos para suas aplicações em execução na nuvem.

Quando ocorre um desvio com relação a sua referência (por exemplo, por uma configuração incorreta), talvez seja necessário responder e investigar. Para fazer isso com êxito, é necessário entender os conceitos básicos de resposta a incidentes de segurança em seu ambiente da AWS, bem como os problemas que você precisa considerar para preparar, instruir e treinar suas equipes de nuvem antes que ocorram problemas de segurança. É importante saber quais controles e recursos você pode usar, analisar exemplos atuais para resolver possíveis problemas e identificar métodos de correção para aproveitar a automação e melhorar sua velocidade de resposta.

Como a resposta a incidentes de segurança pode ser um tópico complexo, recomendamos começar pequeno, desenvolver runbooks, aproveitar os recursos básicos e criar uma biblioteca inicial de mecanismos de resposta a incidentes para iterar e melhorar. Esse trabalho inicial deve incluir seu departamento jurídico, além das equipes que não estão envolvidas com segurança, para que você possa entender melhor o impacto que a resposta a incidentes (RI) e as escolhas feitas têm em seus objetivos corporativos.

Tópicos

- Antes de começar
- Perspectiva de segurança do AWS CAF
- Fundamento da resposta a incidentes

Antes de começar

Além deste documento, recomendamos analisar os whitepapers Práticas recomendadas de segurança, identidade e conformidade e Perspectiva de segurança do AWS Cloud Adoption Framework (CAF). O AWS CAF fornece orientações de apoio à coordenação entre as diferentes

partes das organizações que estão migrando para a nuvem. As orientações sobre o CAF são divididas em várias áreas de foco pertinentes à implementação de sistemas de TI baseados em nuvem, que chamamos de perspectivas. A perspectiva de segurança descreve como implementar um programa de segurança em vários fluxos de trabalho, um dos quais se concentra na resposta a incidentes. Este documento detalha algumas de nossas experiências em ajudar os clientes a avaliar e implementar mecanismos bem-sucedidos nesse fluxo de trabalho.

Perspectiva de segurança do AWS CAF

A perspectiva de segurança inclui quatro componentes:

- Os controles de diretiva determinam os modelos de governança, risco e conformidade em que o ambiente opera.
- Os controles de prevenção protegem suas workloads e reduzem ameaças e vulnerabilidades.
- Os controles de detecção fornecem total visibilidade e transparência sobre a operação das suas implantações na AWS.
- Os controles de resposta conduzem a correção de possíveis desvios com relação às suas referências de segurança.

Embora a resposta a incidentes seja geralmente vista de acordo com o componente de controles responsivos, eles são dependentes e influenciados pelos outros componentes. Por exemplo, controles de segurança de prevenção e diretiva ajudam a estabelecer uma linha de referência, para que você possa monitorar e investigar quaisquer desvios com relação a ela. Essa abordagem não apenas elimina o ruído, mas também contribui para um design de segurança defensivo.

Fundamento da resposta a incidentes

Todos os usuários da AWS em uma organização devem ter uma compreensão básica dos processos de resposta a incidentes de segurança, e a equipe de segurança deve entender profundamente como reagir a problemas de segurança. Experiência e instrução são essenciais para um programa de resposta a incidentes na nuvem antes de lidar com um evento de segurança. A base de um programa bem-sucedido de resposta a incidentes na nuvem é instruir, preparar, simular e iterar.

Para entender cada um desses aspectos, considere as seguintes descrições:

- Instrua sua equipe de operações de segurança e resposta a incidentes sobre as tecnologias de nuvem e como sua organização pretende usá-las.

- Prepare sua equipe de resposta a incidentes para detectar e responder a incidentes na nuvem, habilite recursos de detecção e garanta o acesso apropriado às ferramentas e aos serviços de nuvem necessários. Além disso, prepare os runbooks necessários, tanto os manuais quanto os automatizados, para garantir respostas confiáveis e consistentes. Trabalhe com outras equipes para estabelecer a linha base de operações esperada e use esse conhecimento para identificar desvios dessas operações normais.
- Simule eventos de segurança esperados e inesperados em seu ambiente de nuvem para compreender a eficácia de sua preparação.
- Itere o resultado da simulação para melhorar a escala da postura de sua resposta, diminuir o tempo de concretização de valor e reduzir ainda mais o risco.

Educar

Tópicos

- Responsabilidade compartilhada
- Resposta a incidentes na nuvem
- Incidentes de segurança na nuvem
- Noções básicas dos recursos de nuvem

Responsabilidade compartilhada

A responsabilidade pela segurança e a conformidade é compartilhada entre você e a AWS. Esse modelo compartilhado reduz um pouco dos seus encargos operacionais porque a AWS opera, gerencia e controla os componentes do sistema operacional host e a camada de virtualização, incluindo a segurança física das instalações em que o serviço opera.

Você é responsável por gerenciar os sistemas operacionais convidados (incluindo atualizações e patches de segurança) e as aplicações, além de configurar os controles de segurança fornecidos pela AWS, como grupos de segurança, listas de controle de acesso à rede e Gerenciamento de Identidade e Acesso. É importante considerar cuidadosamente os serviços escolhidos, pois suas responsabilidades variam de acordo com os serviços escolhidos, a integração desses serviços ao seu ambiente de TI e as leis e os regulamentos pertinentes. A Figura 2 mostra uma representação típica do modelo de responsabilidade compartilhada conforme ele se aplica a serviços de infraestrutura, como o Amazon Elastic Compute Cloud (Amazon EC2). Ele separa a maioria das responsabilidades em duas categorias: segurança da nuvem (gerenciada pela AWS) e segurança na nuvem (gerenciada pelo cliente). As responsabilidades podem mudar, dependendo de quais serviços você usa. Para serviços abstratos, 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 os dados deles (o que inclui opções de criptografia), classificar os ativos e usar as ferramentas de IAM para aplicar as permissões apropriadas.

No entanto, o modelo de responsabilidade compartilhada muda com a adição de contêineres e outros serviços que transferem o modelo operacional para o provedor de serviços. À medida que avançamos para a esquerda do modelo operacional, longe da IaaS e dos datacenters e em direção à PaaS, a responsabilidade do provedor de serviços aumenta. Um cliente tem menos

responsabilidades na nuvem e uma operação mais fácil ao usar a migração à esquerda do grafo. Observe as figuras a seguir e as diferenças na capacidade de operar ou funcionar na nuvem. À medida que sua responsabilidade compartilhada na nuvem muda, suas opções de resposta a incidentes ou análise forense também mudam. Como cliente, enquanto você planeja sua resposta a incidentes, você também precisará planejar as habilidades que possui em seu modelo operacional e as possíveis interações antes que elas ocorram no modelo escolhido. Planejar e compreender essas compensações e combiná-las com suas necessidades de governança é uma etapa crucial na resposta a incidentes.

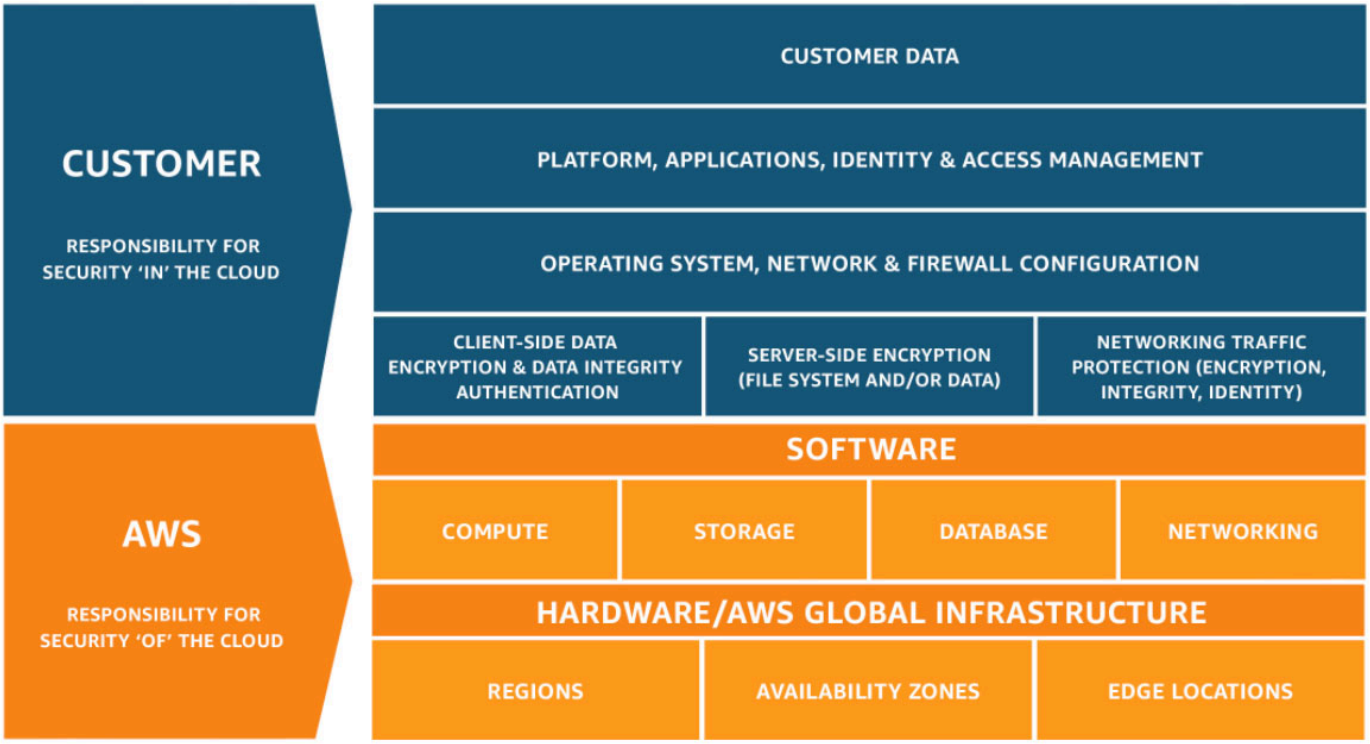

Figura 1: Modelo de responsabilidade compartilhada

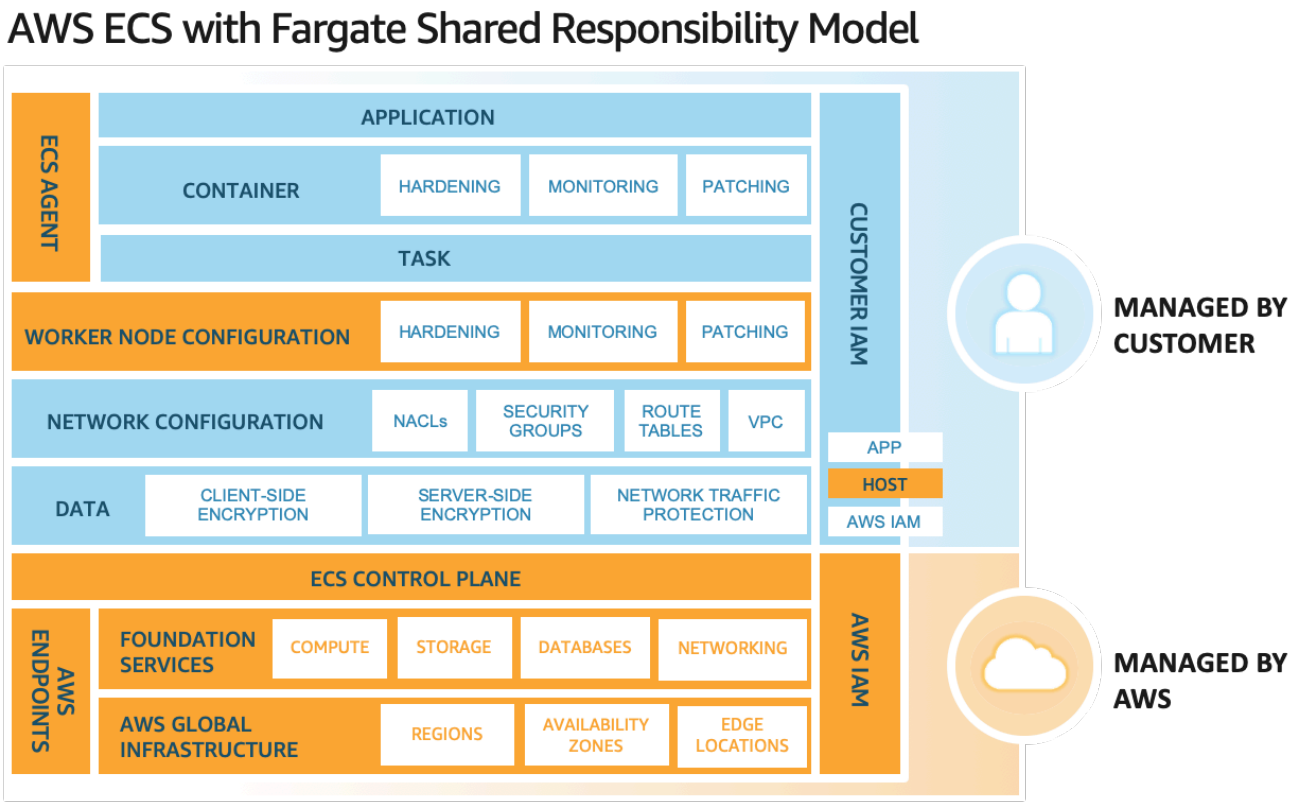

Figura 2: Amazon Elastic Container Service (Amazon ECS) com o modelo de responsabilidade compartilhada do tipo AWS Fargate

Além do relacionamento direto que você tem com a AWS, pode haver outras entidades que tenham incumbências em seu modelo de responsabilidade específico. Por exemplo, você pode ter unidades organizacionais internas que assumem a responsabilidade por alguns aspectos de suas operações. Também pode haver parceiros ou outros terceiros que desenvolvam, gerenciem ou operem parte de sua tecnologia de nuvem.

Criar um runbook adequado de resposta a incidentes e análise forense que corresponda ao seu modelo operacional é extremamente importante. Seu sucesso depende de quão bem você compreende os tipos de ferramentas que precisa criar ou as ferramentas que precisa comprar, para o modelo operacional selecionado. Quanto melhor sua organização entender as ferramentas disponíveis, mais preparado você estará para atender às necessidades do modelo de conformidade e risco de governança (GRC) da sua empresa.

Resposta a incidentes na nuvem

Elaborar objetivos da resposta da nuvem

Embora os processos e os mecanismos gerais de resposta a incidentes, como os definidos no NIST SP 800-61 Computer Security Incident Handling Guide (Guia de tratamento de incidentes de segurança de computadores NIST SP 800-61), permaneçam válidos, recomendamos que você considere 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 o objetivo da resposta a um incidente. São alguns objetivos comuns: conter e mitigar o problema, recuperar os recursos afetados, preservar dados para análise forense e atribuição.
- Responda usando a nuvem: implemente seus padrões de resposta onde o evento e os dados ocorrem.
- Saiba o que você tem e do que precisa: preserve logs, snapshots e outras evidências copiando-os para uma conta de nuvem de segurança centralizada. Use etiquetas, metadados e mecanismos que apliquem políticas de retenção. Por exemplo, você pode optar por usar o comando `dd` do Linux ou um equivalente do Windows para fazer uma cópia completa dos dados para fins investigativos.
- 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. Quando possível, torne seus mecanismos de resposta seguros para serem executados mais de uma vez e em ambientes em um estado desconhecido.
- Automatize sempre que possível: à medida que os problemas ou os incidentes se repetirem, crie mecanismos que façam triagem de modo programático e respondam a situações comuns. Use respostas humanas para incidentes exclusivos, novos e confidenciais.
- Escolha soluções escaláveis: procure corresponder à escalabilidade da abordagem de sua organização quanto à computação em nuvem e reduza o tempo entre a detecção e a resposta.
- Aprenda e melhore seu processo: quando você identificar lacunas em seu processo, ferramentas ou pessoas, implemente planos para corrigi-las. Simulações são métodos seguros para encontrar lacunas e melhorar processos.

As metas de design do NIST recomendam a análise da arquitetura quanto à capacidade de conduzir a resposta a incidentes e a detecção de ameaças. Ao planejar a implementação na nuvem, pense em responder a um incidente ou a um evento forense. 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 resposta a incidentes pelo pipeline de implantação e não devem ser estáticas, pois isso causaria um risco maior.

Incidentes de segurança na nuvem

Tópicos

- Domínios de incidentes
- Indicadores de eventos de segurança na nuvem

Domínios de incidentes

Há três domínios de responsabilidade do cliente em que podem ocorrer incidentes de segurança: serviço, infraestrutura e aplicação. A diferença entre os domínios está relacionada às ferramentas que você usa ao responder. Considere estes domínios:

- Domínio do serviço: incidentes no domínio do serviço afetam a conta da AWS de um cliente, as permissões do IAM, os metadados dos recursos, o faturamento e outras áreas. Um evento de domínio do serviço é aquele ao qual você responde exclusivamente com mecanismos de API da AWS ou no qual as causas básicas estão associadas à sua configuração ou a permissões de recursos, podendo ter registros orientados a serviço relacionados.
- Domínio de infraestrutura: incidentes no domínio da infraestrutura incluem dados ou atividades relacionadas à rede, como o tráfego para suas instâncias do Amazon EC2 na VPC, processos e dados em suas instâncias do Amazon EC2 e outras áreas, como contêineres e outros serviços futuros. Sua resposta a eventos de domínio de infraestrutura geralmente envolve recuperação, restauração ou aquisição de dados relacionados a incidentes para análise forense. Ela provavelmente inclui interação com o sistema operacional de uma instância e, em alguns casos, também pode envolver mecanismos de API da AWS.
- Domínio da aplicação: incidentes no domínio da aplicação ocorrem no código da aplicação ou no software implantado nos serviços ou infraestrutura. Esse domínio deve ser incluído em seus runbooks de detecção e resposta a ameaças na nuvem e pode incorporar respostas semelhantes às do domínio de infraestrutura. Com uma arquitetura de aplicação adequada e bem

pensada, você pode gerenciar esse domínio com ferramentas em nuvem, usando análise forense, recuperação e implantação automatizadas.

Nesses domínios, você deve considerar os atores que podem agir contra sua conta, recursos ou dados. Use uma framework de riscos, sejam eles internos ou externos, para determinar quais são os riscos específicos para sua organização e prepare-se adequadamente.

No domínio do serviço, você trabalha para atingir seus objetivos exclusivamente com as APIs da AWS. Por exemplo, lidar com um incidente de divulgação de dados de um bucket do Amazon S3 envolve chamadas de API para recuperar a política do bucket, analisando os logs de acesso do S3 e possivelmente examinando os logs do AWS CloudTrail. Neste exemplo, é improvável que sua investigação envolva ferramentas forenses de dados ou ferramentas de análise de tráfego de rede.

No domínio da infraestrutura, você pode usar uma combinação de APIs da AWS e software comum de análise forense digital/resposta a incidentes (DFIR) no sistema operacional de uma estação de trabalho, como uma instância do Amazon EC2 que você preparou para o trabalho de resposta a incidentes. Os incidentes de domínio de infraestrutura podem envolver a análise de capturas de pacotes de rede, blocos de disco em um volume do Amazon Elastic Block Store (Amazon EBS) ou memória volátil adquirida de uma instância.

Indicadores de eventos de segurança na nuvem

Há muitos eventos de segurança que você pode não classificar como incidentes, mas que ainda pode ser prudente investigá-los. Para detectar eventos relacionados à segurança em seu ambiente da Nuvem AWS, você pode usar esses mecanismos. Embora não seja uma lista exaustiva, considere os seguintes exemplos de alguns indicadores em potencial:

- Logs e monitores: analise logs da AWS (como Amazon CloudTrail, logs de acesso do Amazon S3 e VPC Flow Logs) e serviços de monitoramento de segurança (como Amazon GuardDuty, Amazon Detective, AWS Security Hub e Amazon Macie). Além disso, use monitores como verificações de integridade do Amazon Route 53 e alarmes do Amazon CloudWatch. Da mesma forma, use eventos do Windows, logs syslog do Linux e outros logs específicos de aplicações que você pode gerar em suas aplicações e faça login no Amazon CloudWatch usando agentes do CloudWatch.
- Atividade de cobrança: uma alteração repentina na atividade de cobrança pode indicar um evento de segurança.
- Inteligência contra ameaças: se você assinar um feed de inteligência contra ameaças de terceiros, poderá correlacionar essas informações com outras ferramentas de registro em log e monitoramento para identificar possíveis indicadores de eventos.

- Ferramentas de parceiros: os parceiros da Rede de Parceiros da AWS (APN) oferecem centenas de produtos líderes do setor que podem ajudar você a atingir seus objetivos de segurança. Para obter mais informações, consulte Soluções de parceiros de segurança e Soluções de segurança no AWS Marketplace.
- AWS Outreach: o AWS Support pode entrar em contato com você se identificarmos atividades de uso abusivo ou mal-intencionadas. Para obter mais informações, consulte a seção Resposta da AWS ao uso abusivo e comprometimento de recursos.
- Contato único: como podem ser seus clientes, desenvolvedores ou outros funcionários da sua organização a perceberem algo incomum, é importante ter um método bem conhecido e bem divulgado de entrar em contato com sua equipe de segurança. As opções populares incluem sistemas de emissão de tíquetes, endereços de e-mail de contato e formulários da Web. Se sua organização trabalha com o público em geral, você também pode precisar de um mecanismo de contato de segurança voltado para o público.

Uma das ferramentas que a AWS oferece para automação e detecção é o AWS Security Hub. O Security Hub oferece uma visão abrangente dos alertas de segurança de alta prioridade e do status de conformidade em todas as contas da AWS em um só lugar, permitindo uma melhor visibilidade desses indicadores. O AWS Security Hub não é um software de gerenciamento de eventos e informações de segurança (SIEM) e não armazena dados de log, mas agrega, organiza e prioriza seus alertas de segurança ou descobertas de vários serviços da AWS. O Security Hub também oferece a capacidade de criar insights personalizados que podem surgir de várias fontes. Isso dá à equipe de operações de segurança opções e insights sobre mais informações quando ocorre um evento. O Security Hub monitora continuamente seu ambiente usando verificações de conformidade automatizadas com base nas práticas recomendadas da AWS e nos padrões do setor que sua organização segue.

Você pode tomar medidas em relação a essas descobertas de segurança e conformidade investigando-as no Amazon Detective ou no Amazon Athena. Além disso, você pode usar as regras do Amazon CloudWatch Events ou do Event Bus para enviar as descobertas para emissão de tíquetes, chat, SIEM, Security Orchestration Automation and Response (SOAR), bem como para as ferramentas de gerenciamento de incidentes ou para personalizar os manuais de remediação. A automação baseada em eventos permite que você responda automaticamente aos incidentes ou eventos ocorridos. Essa abordagem muda a segurança e a maneira como você lida com eventos na nuvem quando comparada a ambientes on-premises.

Noções básicas dos recursos de nuvem

A AWS oferece uma ampla variedade de recursos de segurança que você pode usar para investigar eventos de segurança nos domínios. Por exemplo, a AWS fornece vários mecanismos de registro, como logs do AWS CloudTrail, Amazon CloudWatch Logs, logs de acesso do Amazon S3 e muito mais. Você deve considerar os serviços que está usando e ativar os logs que pertencem a esses serviços. A AWS também oferece uma Solução de registro centralizado, que pode ajudar você a entender como centralizar e armazenar os tipos comuns de logs na nuvem. Depois de habilitar essas origens de registro, você deve decidir como deseja analisá-las, por exemplo, usando o Amazon Athena para consultar logs mantidos em seus buckets do Amazon S3.

Além disso, há vários produtos de parceiros da APN que podem simplificar seu processo ao analisar esses logs, como os descritos no Programa de competência em segurança da APN. Há também vários serviços da AWS que podem ajudar você a obter insights valiosos sobre esses dados, como o Amazon GuardDuty (um serviço de detecção de ameaças) e o AWS Security Hub, que podem fornecer uma visão abrangente de seus alertas de segurança de alta prioridade e status de conformidade em todas as contas da AWS. O Amazon Detective também coleta dados de log de seus recursos da AWS e usa machine learning, análise estatística e teoria dos grafos para ajudar a identificar a causa raiz de possíveis problemas de segurança ou atividades suspeitas. Para obter mais informações sobre recursos adicionais de nuvem que você pode aproveitar durante suas investigações, consulte o Apêndice A: Definições de capacidade da nuvem.

Tópicos

- Privacidade dos dados
- Resposta da AWS ao uso abusivo e comprometimento de recursos

Privacidade dos dados

Sabemos que os clientes se preocupam muito com a privacidade e a segurança dos dados e, por isso, implementamos controles técnicos e físicos responsáveis e sofisticados projetados para impedir o acesso não autorizado ou a divulgação do conteúdo do cliente. A manutenção da confiança dos clientes é um compromisso contínuo. Você pode saber mais sobre os compromissos de privacidade de dados da AWS em nossa página Perguntas frequentes sobre privacidade de dados.

Esses controles intencionais e autoimpostos limitam a capacidade da AWS de ajudar a responder no ambiente de um cliente. Por isso, o foco na compreensão e na criação de recursos dentro do Modelo de responsabilidade compartilhada é fundamental para o sucesso na Nuvem AWS. Embora habilitar

os recursos de registro em log e monitoramento em suas contas da AWS antes que um incidente ocorra seja importante, há aspectos adicionais para a resposta a incidentes que são essenciais para um programa bem-sucedido.

Privacidade de dados do consumidor da Califórnia

A Lei de Privacidade do Consumidor da Califórnia de 2018 (CCPA) concede ao consumidor vários direitos em relação às informações pessoais relativas a ele mantidas pelas empresas que estão sujeitas à CCPA. Para obter informações sobre as políticas de privacidade e segurança de dados da AWS em relação a clientes sujeitos à CCPA, consulte o whitepaper Preparing for the California Consumer Privacy Act para obter orientações.

Regulamento geral de proteção de dados

O Regulamento Geral sobre a Proteção de Dados (RGPD) é uma lei europeia de privacidade (Regulamento 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016) que entrou em vigor em 25 de maio de 2018. O RGPD substitui a Diretiva de proteção de dados da UE, (Diretiva 95/46/EC) e destina-se a unificar as leis de proteção de dados em toda a União Europeia ao aplicar uma única lei de proteção de dados vinculativa em cada um dos estados-membros. Para obter informações sobre a conformidade da AWS em relação ao RGPD, consulte o whitepaper Navegar pelas orientações sobre o GDPR na AWS.

Resposta da AWS ao uso abusivo e comprometimento de recursos

Atividades de uso abusivo são comportamentos observados das instâncias dos clientes da AWS ou de outros recursos que são mal-intencionados, ofensivos, ilegais ou que possam prejudicar outros sites da Internet. A AWS trabalha com você para detectar e tratar atividades suspeitas e mal-intencionadas dos seus recursos da AWS. Comportamentos inesperados ou suspeitos de seus recursos podem indicar que seus recursos da AWS foram comprometidos, o que sinaliza possíveis riscos para sua empresa. Lembre-se de que você tem métodos alternativos de contato em sua conta da AWS. Use as práticas recomendadas ao adicionar contatos, tanto para segurança quanto para cobrança. Embora o e-mail da sua conta raiz seja o principal alvo da comunicação da AWS, a AWS também comunica problemas de segurança e problemas de faturamento para os endereços de e-mail secundários. Adicionar um endereço de e-mail destinado apenas a uma pessoa significa que você adicionou um ponto único de falha (SPOF) à sua conta da AWS. Adicione pelo menos uma lista de distribuição aos seus contatos.

A AWS detecta atividades de uso abusivo em seus recursos usando mecanismos, como:

- Monitoramento de eventos internos da AWS.
- Inteligência de segurança externa contra o espaço de endereço de rede da AWS.
- Reclamações de uso abusivo na Internet contra recursos da AWS.

Embora a equipe de resposta a uso abusivo da AWS monitore energicamente e encerre atividades não autorizadas em execução na AWS, a maioria das reclamações de uso abusivo se refere a clientes que têm negócios legítimos na AWS. Alguns exemplos de causas comuns de atividades de uso abusivo não intencional incluem:

- Recurso comprometido: uma instância do Amazon EC2 sem patch pode ser infectada e se tornar um agente de botnet.
- Uso abusivo não intencional: um rastreador da Web excessivamente agressivo pode ser classificado como um ataque de negação de serviço por alguns sites da Internet.
- Uso abusivo secundário: um usuário final do serviço fornecido por um cliente da AWS pode publicar arquivos de malware em um bucket público do Amazon S3.
- Reclamações falsas: às vezes, os internautas denunciam erroneamente atividades legítimas como uso abusivo.

A AWS tem o compromisso de trabalhar com os clientes da AWS para prevenir, detectar e mitigar uso abusivo e para se defender contra recorrências futuras. Recomendamos que você analise a Política de uso aceitável da AWS, que descreve os usos proibidos dos serviços da Web oferecidos pela Amazon Web Services e suas afiliadas. Para ter uma resposta oportuna às notificações de uso abusivo da AWS, verifique se as informações de contato da sua conta da AWS estão corretas. Quando você receber um aviso de uso abusivo da AWS, sua equipe operacional e de segurança deve investigar imediatamente o assunto. O atraso pode prolongar o impacto na reputação e as implicações legais para você e outras pessoas. Mais importante ainda, o recurso com implicação de uso abusivo pode ser comprometido por usuários mal-intencionados, e ignorar o comprometimento pode aumentar os danos aos seus negócios.

Preparar: pessoas

Processos automatizados permitem que as organizações dediquem mais tempo às medidas para aumentar a segurança de seu ambiente de nuvem e aplicações. A resposta automatizada a incidentes também disponibiliza pessoas para correlacionar eventos, praticar simulações, elaborar novos procedimentos de resposta, realizar pesquisas, desenvolver novas habilidades e testar ou criar ferramentas. Apesar do aumento da automação, analistas e a equipe de resposta de uma organização de segurança ainda têm muito a fazer. Equipes homogêneas podem criar pontos cegos, por isso é essencial criar uma equipe diversificada que ofereça diferentes sistemas de pensamento, pontos de vista culturais e experiência de trabalho e vida em situações complexas e fluidas. Uma das coisas mais impactantes que podemos fazer enquanto planejamos eventos é garantir que tenhamos diversidade incorporada em nossas equipes e planos de resposta. Uma equipe composta por pontos de vista diversificados consegue identificar pontos cegos que podem não ter sido detectados e identificar soluções que não teriam sido imaginadas de outra forma.

Tópicos

- Definir funções e responsabilidades
- Definir mecanismos de resposta
- Criar uma cultura de segurança receptiva e adaptável
- Prever a resposta

Definir funções e responsabilidades

As habilidades e os mecanismos de resposta a incidentes são os mais importantes ao lidar com eventos novos ou de grande escala. Esses eventos dependem dos padrões escritos que sua equipe desenvolveu e da prática que sua equipe teve. Como não podemos prever nem codificar todas as direções possíveis de um evento, contamos com a automação para tarefas simples e repetitivas, como coletar memória de instância ou logs de diagnóstico, e permitimos que as pessoas tomem decisões difíceis. Lidar com eventos de segurança pouco claros requer disciplina interorganizacional, iniciativa para executar ações decisivas e capacidade de entregar resultados. Em sua estrutura organizacional, deve haver muitas pessoas responsáveis, que sejam consultadas ou mantidas informadas durante um incidente, como representantes de Recursos Humanos (RH), sua equipe executiva e departamento jurídico. Considere essas funções e responsabilidades e se terceiros devem estar envolvidos. Observe que em muitas regiões geográficas, existem leis locais que regem o que pode e o que não pode ser feito. Embora possa parecer burocrático construir um grafo de

pessoas responsáveis, consultadas e informadas (RACI) para um incidente, isso permite uma comunicação rápida e direta e descreve claramente a liderança em diferentes estágios do evento.

Parceiros confiáveis podem ser envolvidos na investigação ou na resposta e fornecem experiência adicional e um exame valioso. Quando você não tem essas habilidades em sua própria equipe, convém contratar uma parte externa para obter assistência. Se você contratar uma parte externa, ela deverá treinar os membros da sua equipe. Quando essas partes externas trabalham com seus desenvolvedores e operadores internos, elas podem estender as habilidades dos membros da sua equipe e essa nova experiência pode ser valiosa para o seu programa de resposta a incidentes (RI) no futuro.

Durante um incidente, incluir os proprietários e os desenvolvedores das aplicações e dos recursos afetados é fundamental porque eles são especialistas no assunto (PMEs) que podem fornecer informações e contexto. Pratique e estabeleça relacionamentos com os desenvolvedores e os proprietários das aplicações antes de confiar em seus conhecimentos para resposta a incidentes. Os proprietários das aplicações ou PMEs podem ser obrigados a agir em situações em que o ambiente não é familiar, apresenta uma complexidade imprevista ou ao qual a equipe de resposta não tem acesso. Os PMEs das aplicações devem praticar e se sentir confortáveis trabalhando com a equipe de RI.

Fornecer treinamento

Para reduzir as dependências e diminuir o tempo de resposta, suas equipes de segurança e resposta devem ser informadas sobre os serviços de nuvem e ter oportunidades de prática com as plataformas de nuvem específicas que sua organização usa. Parte desse treinamento vem da criação da equipe e runbooks que ocorre no início do processo. Ao incluir o maior número possível de pessoas na etapa inicial de criação de runbooks, você proporciona uma melhor compreensão para suas equipes internas. Esse treinamento se torna mais real à medida que essas equipes começam a seguir esses runbooks em simulações teóricas.

A AWS e outros terceiros também oferecem workshops de segurança online (Workshops de segurança da AWS) que você pode baixar e usar. Sua organização pode oferecer treinamento adicional à equipe sobre habilidades de programação, processos de desenvolvimento (incluindo sistemas de versionamento e práticas de implantação) e automação da infraestrutura.

A AWS oferece várias opções de treinamento e planos de aprendizado por meio de treinamento digital, treinamento em sala de aula, parceiros da APN e certificações. Para saber mais, consulte Treinamento e certificação da AWS.

Definir mecanismos de resposta

Seu mecanismo de resposta depende do seu modelo de governança, risco e conformidade (GRC). O ideal é que seu modelo de GRC seja criado antes de você planejar a resposta a incidentes. Se você ainda não começou a criar um GRC, é uma primeira etapa necessária para criar um bom mecanismo de resposta a incidentes. Ao considerar sua abordagem para a resposta a incidentes na nuvem, em conjunto com outras equipes (como a assessoria jurídica, a liderança, partes interessadas de negócios e outros), você deve entender o que tem e do que precisa. Identifique as partes interessadas e os contatos pertinentes e tenha acesso adequado para responder da forma necessária.

Embora a nuvem possa fornecer maior visibilidade e recursos por meio de APIs de serviço, seu modelo de GRC mostra como usá-los em sua resposta. Identifique os números de contas da AWS da sua equipe, os intervalos de IP de Virtual Private Clouds (VPCs), diagramas de rede correspondentes, logs, locais de dados e classificações de dados. Muitos desses processos tecnológicos estão incluídos na seção Preparar: tecnologia. Depois, comece a documentar seus procedimentos de resposta a incidentes, geralmente chamados de procedimentos ou runbooks, que definem as etapas para investigar e remediar um incidente.

Criar uma cultura de segurança receptiva e adaptável

Na AWS, aprendemos que nossos clientes e nossas próprias equipes internas são mais bem-sucedidos quando as equipes de segurança são facilitadoras cooperativas para seus negócios e seus desenvolvedores, que promovem uma cultura que garante que todas as partes interessadas cooperem e escalem para manter um procedimento de segurança ágil e altamente responsivo. Embora melhorar a cultura de segurança da sua organização não seja o assunto deste documento, você pode obter informações relevantes de sua equipe que não seja de segurança se perceberem que a equipe de segurança está receptiva. Quando sua equipe de segurança está aberta e acessível, com o apoio da liderança, é mais provável que ela receba notificações, cooperação e respostas adicionais e oportunas a eventos de segurança.

Em algumas organizações, a equipe pode temer a retribuição se relatar um problema de segurança. Às vezes, simplesmente não sabem como relatar um problema. Em outros casos, podem não querer perder tempo ou se sentir constrangidos de relatar algo como um incidente de segurança que mais tarde descubram não se tratar de um problema. Da equipe de liderança para baixo, é importante promover uma cultura de aceitação e convidar todos a fazer parte da segurança da organização. Forneça um canal claro para que qualquer pessoa abra um tíquete de alta gravidade sempre que

acreditar que pode haver um risco ou ameaça em potencial. Receba essas notificações com a mente aberta e disposta, mas o mais importante, deixe claro para a equipe que não é de segurança que você aceita essas notificações. Enfatize que você prefere ser notificado demais sobre possíveis problemas do que não receber nenhuma notificação. É muito melhor para um desenvolvedor destacar seu próprio erro do que um pesquisador apontar o problema em um artigo público.

Essas notificações oferecem oportunidades valiosas para praticar investigações responsivas sob estresse. Elas podem servir como um encaminhamento de feedback importante enquanto você desenvolve seus procedimentos de resposta.

Prever a resposta

Como é impossível prever todos os eventos em potencial, você deve continuar confiando na análise humana. Dedicar um tempo para treinar cuidadosamente sua equipe e preparar sua organização ajuda você a prever o inesperado; no entanto, sua organização não precisa se preparar isoladamente. Colaborar com parceiros de segurança confiáveis para identificar eventos de segurança inesperados oferece às organizações o benefício de visibilidade e insight adicionais.

Parceiros e a janela de resposta

A jornada para a nuvem é diferente para cada organização. No entanto, existem padrões e práticas que outras organizações já encontraram e para os quais um parceiro de segurança confiável pode chamar sua atenção. É recomendável identificar parceiros externos de segurança da AWS (APN) que possam oferecer experiência externa e um ponto de vista diferente para aumentar seus recursos de resposta. Os parceiros de segurança confiáveis podem ajudar você a identificar possíveis riscos ou ameaças com os quais você talvez não esteja familiarizado.

Em 1955, Joseph Luft e Harrington Ingham criaram a janela Johari, um exercício para mapear características a categorias. A janela é representada como uma grade que consiste em quatro quadrantes, semelhante ao diagrama a seguir.

	Known to You	Not Known to You
Known to Others	**Obvious**	**Blind Spot**
Not Known to Others	**Internally Known**	**Unknown**

Figura 3: Janela Johari modificada para resposta a incidentes

Embora a janela Johari não tenha sido destinada à segurança da informação, podemos ajustar o conceito para usá-lo como um modelo mental simples a fim de considerar a dificuldade em avaliar as ameaças de uma organização. Em nosso conceito modificado, os quatro quadrantes são:

- Óbvio: risco do qual sua equipe e seu parceiro da APN estão cientes.
- Conhecido internamente: risco com o qual sua equipe está familiarizada, mas que seu parceiro da APN não está. Isso pode significar que você tem experiência interna ou conhecimento tribal.
- Ponto cego: risco com o qual seu parceiro da APN está familiarizado, mas que sua equipe não está.
- Desconhecido: risco com o qual nem você nem seu parceiro da APN estão familiarizados.

Embora esse diagrama seja simples, ele representa o valor que os parceiros da APN confiáveis podem alcançar. Mais importante ainda, pode haver pontos cegos que você não conheça, mas um parceiro da APN com a experiência certa possa evidenciar. Embora vocês dois estejam familiarizados com esses riscos no quadrante óbvio, seu parceiro da APN pode recomendar controles e soluções com os quais você não esteja familiarizado. Além disso, embora você possa chamar a atenção do seu parceiro da APN para esses riscos no quadrante conhecido internamente, ele também poderá identificar controles otimizados para reduzir esse risco. Ao avaliar suas melhorias, entre em contato com seu parceiro da APN para fornecer conselhos de especialistas.

Risco desconhecido

Se você se concentrou em personalizar alertas, melhorar seus procedimentos de resposta a incidentes com automação e melhorar suas defesas de segurança, talvez esteja se perguntando o que melhorar a seguir. Você pode estar curioso sobre seu risco desconhecido, conforme representado na categoria de desconhecido na Figura 3. É possível reduzir o risco desconhecido com os seguintes métodos:

- Definir afirmações de segurança: cite algumas verdades que você pode afirmar. Quais são as primitivas de segurança que devem ser verdadeiras em seu ambiente? Defini-las claramente permite que você procure o inverso. Isso é algo que é mais fácil de fazer no início de sua jornada para a nuvem em vez de tentar fazer engenharia reversa de suas afirmações de segurança posteriormente.
- Educação, comunicação e pesquisa: forme especialistas em segurança na nuvem em sua equipe ou inclua parceiros especializados para ajudar a examinar seu ambiente. Conteste suas suposições e tenha cuidado com o raciocínio sutil. Crie encaminhamentos de feedback em seus processos e ofereça mecanismos para que suas equipes de engenharia se comuniquem com as equipes de segurança. Você também pode expandir sua abordagem para monitorar listas de discussão de segurança relevantes e divulgações de segurança da informação.
- Reduzir a superfície de ataque: melhore sua defesa para evitar riscos e tenha mais tempo contra ataques desconhecidos. Bloqueie e desacelere invasores e force-os a serem ruidosos.
- Inteligência contra ameaças: assine um feed contínuo de ameaças, riscos e indicadores atuais e relevantes de todo o mundo.
- Alertas: gere notificações que alertam você sobre atividades incomuns, mal-intencionadas ou caras. Por exemplo, você pode criar uma notificação para atividades ocorridas em regiões ou serviços que você não usa.
- Machine learning: use o machine learning para identificar anomalias complexas para uma organização específica ou personas individuais. Para ajudar a identificar comportamentos incomuns, você também pode criar o perfil das características normais de suas redes, usuários e sistemas.

A inteligência contra ameaças se torna o tópico principal quando você considera pontos cegos e incógnitas desconhecidas. A janela de Johari mostra como categorizar o que você sabe e o que não sabe, mas a inteligência contra ameaças mostra como explicar o que você ainda não sabe. Trata-se de uma disciplina que ajuda as empresas a enxergar os meandros do modelo de ameaças e encontrar ameaças que sua empresa talvez ainda não saiba que existem.

Geralmente, a inteligência contra ameaças compreende:

1. Encontrar novas ameaças.
2. Definir novos padrões.
3. Definir novas técnicas de aquisições automatizadas.
4. Repetir esses processos.

Embora esse tipo de prática possa ser útil, o cuidado e a manutenção de uma equipe de inteligência contra ameaças podem sobrecarregar muitas empresas, até mesmo grandes empresas. No final, a questão passa a ser combinar seu modelo de ameaça, tamanho e adversidade ao risco. Considere estas perguntas:

- Seu modelo de ameaças é significativamente diferente o suficiente do mercado vertical padrão em que se encontra a empresa?
- Seu apetite pelo risco é baixo o suficiente para que essa equipe seja necessária?
- É fiscalmente correto administrar uma equipe para sua empresa?
- Seu perfil de risco é interessante o suficiente para atrair talentos razoáveis para sua causa?

Se você responder não a qualquer uma dessas perguntas, provavelmente encontrará um parceiro de inteligência contra ameaças. Este serviço é oferecido de forma competitiva por muitas empresas grandes e conhecidas.

A AWS fornece as ferramentas e os serviços para gerenciar esses problemas por conta própria. Usar o machine learning para identificar padrões maliciosos é um campo de estudo bem pesquisado, com padrões que são implementados por clientes, pelo AWS Professional Services, por parceiros da APN e serviços da AWS, como o Amazon GuardDuty e o Amazon Macie. Alguns desses padrões foram abordados nas sessões de conferência do AWS re:Invent. Para obter mais informações, consulte a seção Mídia deste whitepaper.

Os clientes também estão expandindo seus data lakes tradicionalmente centrados nos negócios para aproveitar padrões de arquitetura semelhantes ao desenvolver data lakes de segurança. As equipes de operações de segurança também estão expandindo o uso de ferramentas tradicionais de registro e monitoramento, como o Amazon OpenSearch Service e o OpenSearch Dashboards, para arquiteturas de big data.

Esses clientes estão coletando dados internos de logs de eventos do AWS CloudTrail, logs de fluxo de VPC, logs de acesso do Amazon CloudFront, logs de banco de dados e logs de aplicações e,

depois, combinando esses dados com dados públicos e inteligência contra ameaças. Com esses dados valiosos, os clientes incluíram habilidades de ciência e engenharia de dados em suas equipes de operações de segurança para aproveitar ferramentas como Amazon EMR, Amazon Kinesis Data Analytics, Amazon Redshift, Amazon QuickSight, AWS Glue, Amazon SageMaker e Apache MXNet on AWS para criar soluções que identificam e preveem anomalias exclusivas de seus negócios.

Por fim, consulte Soluções de parceiros de segurança para se informar sobre centenas de produtos líderes do setor dos parceiros da APN que são equivalentes, idênticos ou integrados aos controles existentes em seus ambientes on-premises. Esses produtos complementam os serviços da Nuvem AWS já existentes para que os clientes possam implantar uma arquitetura de segurança abrangente e obter uma experiência mais uniforme na nuvem e no ambiente on-premises.

Preparar: tecnologia

Tópicos

- Preparar o acesso às contas da AWS
- Preparar processos
- Suporte do provedor de nuvem

Preparar o acesso às contas da AWS

Durante um incidente, suas equipes de resposta a incidentes devem ter acesso aos ambientes e aos recursos envolvidos no incidente. As equipes devem ter acesso apropriado para executar suas funções antes que ocorra um evento. Para isso, você deve saber de qual nível de acesso os membros da equipe precisam (por exemplo, que tipos de ações eles provavelmente executarão) e provisionar o acesso com antecedência. Esse acesso é derivado das políticas de governança, gerenciamento de riscos e conformidade (GRC) da sua empresa. A autenticação e a autorização dos membros da sua equipe devem ser documentadas e testadas bem antes que um evento ocorra para garantir que eles possam executar uma resposta oportuna sem atrasos. Para responder a um incidente corretamente, parte de sua preparação deve ser uma revisão de como as contas da AWS são definidas e como as funções entre contas são permitidas e organizadas.

Nesse estágio, você deve trabalhar em estreita colaboração com seus desenvolvedores, arquitetos, parceiros, equipes de governança e equipes de conformidade para entender qual nível de acesso é necessário para a equipe de resposta. Identifique e discuta a estratégia de conta da AWS e a estratégia de identidade de nuvem com os arquitetos de nuvem da sua organização para entender quais métodos de autenticação e autorização estão configurados, por exemplo:

- Federação: um usuário assume uma função do IAM em uma conta da AWS de um provedor de identidade.
- Acesso entre contas: um usuário assume uma função do IAM entre várias contas da AWS.
- Autenticação: um usuário se autentica como um usuário do AWS IAM criado em uma única conta da AWS.

Essas opções definem as opções técnicas para autenticação na AWS e como obter acesso durante uma resposta, mas algumas organizações podem contar com outra equipe ou um parceiro para ajudar na resposta. As contas de usuários criadas especificamente para responder a um incidente

de segurança geralmente são privilegiadas para conceder acesso suficiente. Portanto, o uso dessas contas de usuário deve ser restrito, e elas não devem ser usadas para atividades diárias.

Antes de criar mecanismos de acesso, trabalhe com suas equipes de nuvem para entender como suas contas da AWS são organizadas e administradas. Muitos clientes usam o AWS Organizations para ajudar a gerenciar centralmente o faturamento, compartilhar recursos em suas contas da AWS e controlar o acesso, a conformidade e a segurança. Um recurso central do Organizations é que ele pode ser aproveitado para aplicar Políticas de controle de serviço a grupos de contas, o que permite que você obtenha gerenciamento de políticas em escala. Para obter informações adicionais sobre a implementação de mecanismos de governança em escala, consulte Governança da AWS em escala. Depois de entender como sua organização organizou e administrou suas contas da AWS, considere os seguintes padrões de resposta generalizada para ajudar a identificar quais abordagens são adequadas para sua organização.

Tópicos

- Acesso indireto
- Acesso direto
- Acesso alternativo
- Acesso à automação
- Acesso a Managed Services

Acesso indireto

Se você usar acesso indireto, os proprietários das suas contas ou as equipes de aplicações serão obrigados a realizar correções autorizadas em suas contas da AWS com orientação tática da equipe de resposta a incidentes, que são seus especialistas em segurança. Esse método é uma maneira mais lenta e complexa de executar tarefas, mas pode ser bem-sucedido quando a equipe de resposta não está familiarizada com a conta ou o ambiente de nuvem.

Acesso direto

Para conceder acesso direto à equipe de resposta a incidentes, implante uma função do AWS IAM nas contas da AWS que seus engenheiros de segurança ou a equipe de resposta a incidentes possam assumir durante um evento de segurança. A equipe de resposta a incidentes fará a autenticação por meio de um processo federado normal ou por meio de um processo especial de emergência, se o incidente afetar seu processo de autenticação normal. As permissões concedidas

à função do IAM de resposta a incidentes dependem das ações que você espera que a equipe de resposta realize.

Acesso alternativo

Se você acredita que um evento de segurança está afetando seus sistemas de segurança, identidade ou comunicação, talvez seja necessário buscar mecanismos e acesso alternativos para investigar e remediar o impacto. Ao usar uma nova conta da AWS criada para fins específicos, a equipe de resposta pode colaborar e trabalhar a partir de uma infraestrutura alternativa e segura.

Por exemplo, a equipe de resposta pode aproveitar a nova infraestrutura lançada na nuvem, como estações de trabalho remotas usando o Amazon WorkSpaces e serviços de e-mail fornecidos pelo Amazon WorkMail. Você deve preparar os controles de acesso apropriados (usando políticas do IAM) para delegar o acesso para que sua conta segura e alternativa da AWS possa assumir permissões para a conta da AWS afetada.

Depois de delegar o acesso apropriado, você pode usar as APIs da AWS na conta afetada para compartilhar dados pertinentes, como logs e snapshots de volume, para realizar trabalhos investigativos no ambiente isolado. Para obter mais informações sobre esse acesso entre contas, consulte Tutorial: Delegar acesso entre contas da AWS usando funções do IAM.

Acesso à automação

Ao migrar para o uso da automação a fim de reagir a eventos de segurança, você deve criar funções do IAM especificamente para serem usados por seus recursos de automação (como instâncias do Amazon EC2 ou funções do AWS Lambda). Esses recursos podem então assumir as funções do IAM e herdar as permissões atribuídas a elas. Em vez de criar e distribuir credenciais da AWS, delegue permissão para sua função do AWS Lambda ou instância do Amazon EC2. O recurso da AWS recebe automaticamente um conjunto de credenciais temporárias e as usa para assinar solicitações de API.

Você também pode considerar um método seguro para sua automação ou ferramentas autenticarem e executarem no sistema operacional de sua instância do Amazon EC2. Embora existam muitas ferramentas que podem executar essa automação, considere usar o AWS Systems Manager Run Command, que permite administrar instâncias de forma remota e segura usando um agente que você instala no sistema operacional da instância do Amazon EC2.

O AWS Systems Manager Agent (SSM Agent) é instalado por padrão em algumas imagens de máquina da Amazon (AMIs) do Amazon EC2, por exemplo, para o Microsoft Windows Server e o

Amazon Linux. No entanto, talvez seja necessário instalar manualmente o agente em outras versões do Linux e instâncias híbridas. Se você usar o Run Command ou outra ferramenta, conclua todas as configurações e configurações de pré-requisito antes de receber seu primeiro alerta relacionado à segurança a ser investigado.

Acesso a Managed Services

Sua organização pode já ter parceria com um provedor de tecnologia da informação que gerencie serviços e soluções em seu nome. Esses parceiros têm a responsabilidade compartilhada de apoiar a segurança de sua organização, e é importante entender claramente esse relacionamento antes que ocorra uma anomalia. Se você já trabalha com um parceiro fornecedor de serviços gerenciados (MSP) da AWS, um AWS Managed Services ou um parceiro de serviços de segurança gerenciados, você deve identificar as responsabilidades de cada parceiro no que se refere aos seus ambientes de nuvem, qual acessa os provedores já têm aos seus serviços de nuvem, de que acesso eles precisam e pontos de contato ou caminhos de escalonamento para quando você precisar da assistência deles. Por fim, você deve praticar isso com seu parceiro para garantir que seus planos de resposta sejam previsíveis e bem-sucedidos.

Preparar processos

Depois que o acesso apropriado tiver sido provisionado e testado, sua equipe de resposta a incidentes deverá definir e preparar os processos relacionados necessários para investigação e correção. Esse estágio exige muito esforço, pois você deve planejar suficientemente a resposta adequada aos eventos de segurança em seus ambientes de nuvem.

Trabalhe em estreita colaboração com suas equipes internas de serviços de nuvem e parceiros para identificar as tarefas necessárias a fim de garantir que esses processos sejam possíveis. Colabore ou atribua tarefas de atividade de resposta entre si e garanta que as configurações de conta necessárias estejam implementadas. Recomendamos preparar os processos e as configurações de pré-requisitos com antecedência para fornecer à sua organização os recursos de resposta a seguir.

Tópicos

- Árvores de decisão
- Usar contas alternativas
- Exibir ou copiar dados
- Compartilhar snapshots do Amazon EBS

- Compartilhar o Amazon CloudWatch Logs
- Usar armazenamento imutável
- Iniciar recursos próximos ao evento
- Isolar recursos
- Iniciar estações de trabalho forenses

Árvores de decisão

Às vezes, condições diferentes podem exigir ações ou etapas diferentes. Por exemplo, você pode realizar ações diferentes com base no tipo de conta da AWS (desenvolvimento versus produção), nas etiquetas dos recursos, no status de conformidade das regras AWS Config desses recursos ou em outras informações.

Para apoiar você na criação e na documentação dessas decisões, recomendamos elaborar uma árvore de decisão com suas outras equipes e partes interessadas. Semelhante a um fluxograma, uma árvore de decisão é uma ferramenta que pode ser aproveitada para apoiar a tomada de decisões, ajudando a orientar você a determinar as ações e resultados ideais com base em condições e entradas em potencial, incluindo probabilidades.

Usar contas alternativas

Embora possa ser necessário responder a um evento na conta afetada, é ideal investigar dados fora da conta afetada. Alguns clientes têm um processo para criar ambientes de conta da AWS separados e isolados, usando modelos que pré-configuram os recursos que devem provisionar. Esses modelos são implantados por meio de um serviço, como o AWS CloudFormation ou o Terraform, que fornece um método fácil para criar uma coleção de recursos relacionados da AWS e provisioná-los de maneira ordenada e previsível.

A pré-configuração dessas contas usando mecanismos de modelo ajuda a remover interações humanas durante os estágios iniciais de um incidente e garante que o ambiente e os recursos sejam preparados de maneira repetível e previsível, o que pode ser verificado por uma auditoria. Além disso, esse mecanismo também aumenta a capacidade de manter a segurança e a contenção de dados no ambiente forense.

Essa abordagem exige que você trabalhe com seus serviços de nuvem e equipes de arquitetura para determinar um processo de conta da AWS apropriado que possa ser usado para investigações. Por

exemplo, suas equipes de serviços de nuvem podem usar o AWS Organizations para gerar novas contas e ajudar você a pré-configurar essas contas usando um método com modelo ou script.

Esse método de segmentação é melhor quando você precisa proteger uma organização maior contra uma possível ameaça. Essa segmentação, usando uma conta da AWS nova e, em grande parte, desconectada, significa que um usuário da organização, identificado na documentação de várias contas como Unidade Organizacional (OU) de segurança, é capaz de se mover para a conta, realizar as atividades forenses necessárias e possivelmente entregar a conta como um todo para uma entidade legal, se necessário. Esse método de análise forense e atribuição requer revisão e planejamento significativos e deve estar alinhado com as políticas de GRC da empresa. Embora esse trabalho não seja fácil, é muito mais fácil fazê-lo antes de criar uma grande base de contas.

Exibir ou copiar dados

A equipe de resposta precisa acessar registros ou outras evidências a serem analisadas e deve garantir que tenha a capacidade de visualizar ou copiar dados. No mínimo, a política de permissão do IAM para a equipe de resposta deve fornecer acesso somente leitura para que possam investigar. Para habilitar o acesso apropriado, você pode considerar algumas políticas gerenciadas da AWS pré-criadas, como SecurityAudit ou ViewOnlyAccess.

Por exemplo, a equipe de resposta pode querer fazer uma cópia point-in-time dos dados, como os logs AWS CloudTrail, de um bucket do Amazon S3 em uma conta para um bucket do Amazon S3 em outra conta. As permissões fornecidas pela política gerenciada ReadOnlyAccess, por exemplo, permitem que a equipe de resposta execute essas ações. Para entender como usar a AWS Command Line Interface (CLI) para fazer isso, consulte Como posso copiar todos os objetos de um bucket do Amazon S3 para outro bucket?.

Compartilhar snapshots do Amazon EBS

Muitos clientes usam snapshots do Amazon Elastic Block Store (Amazon EBS) como parte de sua investigação de eventos de segurança que envolvem suas instâncias do Amazon EC2. Os snapshots dos volumes do Amazon EBS são backups incrementais. Para obter mais informações sobre snapshots incrementais do Amazon EBS, consulte Snapshots do Amazon EBS.

Para realizar uma investigação de um volume do Amazon EBS em uma conta separada e isolada, você deve modificar as permissões do snapshot para compartilhá-lo com as outras contas da AWS especificadas. Os usuários autorizados por você poderão usar os snapshots compartilhados como base para criar seus próprios volumes do EBS, ao passo que seu snapshot original não será afetado. Para obter mais informações, consulte Compartilhar um snapshot do Amazon EBS.

Se o snapshot estiver criptografado, você também deverá compartilhar a chave gerenciada pelo cliente (CMK) do AWS Key Management Service (AWS KMS) personalizada usada para criptografar o snapshot. Você pode aplicar permissões entre contas a uma CMK personalizada quando ela é criada ou posteriormente. Os snapshots são restritos à região em que foram criados, mas você pode compartilhar um snapshot com outra região copiando-o para essa região. Para obter mais informações, consulte Copiar um snapshot do Amazon EBS.

Compartilhar o Amazon CloudWatch Logs

Os logs registrados no Amazon CloudWatch Logs, como logs de fluxo da Amazon VPC, podem ser compartilhados com outra conta (como sua conta de segurança centralizada) por meio de uma assinatura do CloudWatch Logs. Por exemplo, os dados de eventos de log podem ser lidos em um Amazon Kinesis Stream centralizado para realizar processamento personalizado e análise. O processamento personalizado é especialmente útil quando você coleta dados de registro em log de várias contas. O ideal é criar essa configuração no início de sua jornada para a nuvem, antes que ocorra um evento relacionado à segurança. Para obter mais informações, consulte Compartilhar dados de log entre contas com assinaturas.

Usar armazenamento imutável

Ao copiar registros e outras evidências para uma conta alternativa, verifique se os dados replicados estão protegidos. Além de proteger a evidência secundária, você também deve proteger a integridade dos dados na fonte. Conhecidos como armazenamento imutável, esses mecanismos protegem a integridade de seus dados, impedindo que eles sejam adulterados ou excluídos.

Usando os recursos nativos do Amazon S3, você pode configurar um bucket do Amazon S3 para proteger a integridade dos seus dados. Por exemplo, ao usar o bloqueio de objetos do S3, você pode evitar que um objeto seja excluído ou substituído por um período fixo ou indefinidamente. Gerenciar permissões de acesso com políticas de bucket do S3, configurar o versionamento do S3 e habilitar a exclusão de MFA são outras maneiras de restringir como os dados podem ser gravados ou lidos. Esse tipo de configuração é útil para armazenar logs de investigação e evidências, e geralmente é chamado de write once, read many (WORM). Você também pode proteger os dados usando criptografia no lado do servidor com AWS Key Management Service (AWS KMS) e verificando se apenas as entidades principais apropriadas do IAM estão autorizadas a descriptografar os dados.

Além disso, se você quiser manter os dados com segurança em um armazenamento de longo prazo após a conclusão da investigação, pense em mover os dados do Amazon S3 para o Amazon S3 Glacier usando políticas de ciclo de vida de objetos. O Amazon S3 Glacier é um serviço de

armazenamento em nuvem seguro, duradouro e de custo extremamente baixo para arquivamento de dados e backups de longa duração. Ele foi projetado para oferecer durabilidade de 99,999999999% e oferece recursos abrangentes de segurança e conformidade.

Além disso, você pode proteger os dados no Amazon S3 Glacier usando o Amazon S3 Glacier Vault Lock, que permite implantar e aplicar facilmente controles de conformidade a cofres individuais do Amazon S3 Glacier com uma política de Vault Lock. Você pode especificar controles de segurança, como WORM, em uma política de Vault Lock e bloquear a política de edições futuras. Depois de bloqueada, a política não pode ser alterada. O Amazon S3 Glacier aplica os controles definidos na política de Vault Lock para ajudar a alcançar objetivos de conformidade, como retenção de dados. Você pode implantar uma variedade de controles de conformidade em uma política de Vault Lock usando a linguagem de política do AWS Identity and Access Management (IAM).

Iniciar recursos próximos ao evento

Para a equipe de resposta que é nova na nuvem, pode ser tentador tentar conduzir investigações de nuvem no local onde suas ferramentas existentes estão localizadas. Em nossa experiência, os clientes da AWS que respondem a incidentes usando tecnologias de nuvem obtêm melhores resultados. Os isolamentos podem ser automatizados, as cópias podem ser feitas com mais facilidade, as evidências ficam prontas para análise mais cedo e a análise pode ser realizada mais rapidamente.

A prática recomendada é realizar investigações e análises forenses na nuvem, onde os dados estão, em vez de tentar transferir os dados para um datacenter antes de investigar. Você pode usar os recursos seguros de computação e armazenamento da nuvem praticamente em qualquer lugar do mundo para realizar as operações de resposta segura. Muitos clientes optam por pré-criar uma conta separada da AWS que está pronta para realizar uma investigação, embora possa haver casos em que você opte por realizar sua análise na mesma conta da AWS. Se for esperado que sua organização retenha registros por motivos legais e de conformidade, pode ser prudente manter contas separadas para armazenamento de longo prazo e atividades legais.

Também é uma prática recomendada realizar a investigação na mesma região da AWS em que ocorreu o evento, em vez de replicar os dados para outra região. Recomendamos essa prática principalmente devido ao tempo adicional necessário para transferir os dados entre regiões. Para cada região da AWS em que você opera, garanta que o processo de resposta a incidentes e a equipe de resposta cumpram as leis de privacidade de dados pertinentes. Se você precisar mover dados entre regiões, pense nas implicações legais da movimentação de dados entre jurisdições. Geralmente, é uma prática recomendada manter os dados na mesma jurisdição nacional.

Se você acredita que um evento de segurança está afetando seus sistemas de segurança, identidade ou comunicação, talvez seja necessário buscar mecanismos e acesso alternativos para investigar e remediar o impacto. A AWS oferece a capacidade de iniciar rapidamente uma nova infraestrutura que pode ser usada para ambientes de trabalho alternativos e seguros. Por exemplo, enquanto você investiga a possível gravidade da situação, convém criar uma conta da AWS com as ferramentas seguras necessárias para que seus consultores jurídicos, relações públicas e equipes de segurança se comuniquem e continuem trabalhando. Serviços como AWS WorkSpaces (para desktops virtuais), AWS WorkMail (para e-mail) e Amazon Chime (para comunicação) podem fornecer às suas equipes de resposta, liderança e outros participantes os recursos e a conectividade de que eles precisam para se comunicar, investigar e corrigir um problema.

Isolar recursos

No decorrer da investigação, talvez seja necessário isolar recursos como parte de sua resposta a uma anomalia de segurança. A intenção por trás do isolamento de recursos é limitar o impacto em potencial, impedir a propagação adicional dos recursos afetados, limitar a exposição não intencional de dados e impedir o acesso não autorizado adicional.

Como em qualquer resposta, considerações comerciais, regulamentares, legais ou outras podem ser aplicadas. Pondere suas ações pretendidas e suas consequências esperadas e inesperadas. Se suas equipes de nuvem usam etiquetas de recursos, essas etiquetas podem ajudar você a identificar a criticidade do recurso ou do proprietário a ser contatado.

Iniciar estações de trabalho forenses

Algumas de suas atividades de resposta a incidentes podem incluir a análise de imagens de disco, sistemas de arquivos, despejos de RAM ou outros artefatos envolvidos em um incidente. Muitos clientes criam uma estação de trabalho forense personalizada que podem usar para montar cópias de quaisquer volumes de dados afetados (conhecidos como snapshots do EBS). Para isso, siga estas etapas básicas:

1. Escolha uma imagem de máquina da Amazon (AMI) básica (como Linux ou Microsoft Windows) que possa ser usada como uma estação de trabalho forense.
2. Execute uma instância do Amazon EC2 a partir dessa AMI básica.
3. Fortaleça o sistema operacional, remova pacotes de software desnecessários e configure mecanismos pertinentes de auditoria e registro em log.
4. Instale seu conjunto preferido de toolkits privados ou de código aberto, bem como qualquer software e pacotes de fornecedores necessários.

5. Pare a instância do Amazon EC2 e crie uma AMI a partir da instância interrompida.
6. Crie um processo semanal ou mensal para atualizar e reconstruir a AMI com os patches de software mais recentes.

Depois que o sistema forense for provisionado usando uma AMI, sua equipe de resposta a incidentes poderá usar esse modelo para criar uma AMI a fim de iniciar uma nova estação de trabalho forense para cada investigação. O processo para iniciar a AMI como uma instância do Amazon EC2 pode ser pré-configurado para simplificar o processo de implantação. Por exemplo, você pode criar um modelo dos recursos de infraestrutura forense necessários em um arquivo de texto e implantá-lo em sua conta da AWS usando o AWS CloudFormation.

Quando seus recursos estiverem disponíveis para serem implantados rapidamente a partir de um modelo, seus especialistas forenses bem treinados poderão usar novas estações de trabalho forenses para cada investigação, em vez de reutilizar a infraestrutura. Com esse processo, você pode garantir que não haja contaminação cruzada de outros exames forenses.

Tipos e locais de instância

O Amazon EC2 oferece uma ampla seleção de tipos de instâncias otimizadas para diferentes casos de uso. Os tipos de instâncias consistem em várias combinações de CPU, memória, armazenamento e capacidade de rede e oferecem flexibilidade de escolha da composição adequada de recursos para as suas aplicações. Muitos tipos de instância incluem vários tamanhos de instância, o que permite dimensionar seus recursos de acordo com os requisitos da workload de destino. Para instâncias de resposta a incidentes, siga as políticas de GRC da sua empresa para localização e segmentação da rede que executa instâncias de produção.

A rede aprimorada da AWS usa virtualização de E/S raiz (SR-IOV) para fornecer recursos de rede de alta performance em tipos de instâncias compatíveis. A SR-IOV é um método de virtualização de dispositivos que fornece desempenho de E/S mais elevado e menor utilização de CPU em comparação com interfaces de redes virtualizadas tradicionais. A rede avançada fornece uma largura de banda maior, um desempenho melhor de pacotes por segundo (PPS) e latências entre instâncias consistentemente mais baixas. Não há nenhuma cobrança adicional pelo uso da rede avançada. Para obter informações sobre quais tipos de instância são compatíveis com velocidades de rede de 10 ou 25 Gbps e outros recursos avançados, consulte Tipos de instância do Amazon EC2.

Suporte do provedor de nuvem

Tópicos

- AWS Managed Services
- AWS Support
- Suporte de resposta DDoS

AWS Managed Services

O AWS Managed Services (AMS) disponibiliza gerenciamento contínuo da infraestrutura da AWS para que você possa se concentrar nas suas aplicações. Ao implementar as 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.

Como operador de infraestrutura, o AMS assume a responsabilidade pela implantação de um conjunto de controles de detecção de segurança e fornece uma primeira linha de resposta 24 horas por dia, 7 dias por semana, aos alertas, usando um modelo “follow-the-sun”. Quando um alerta é acionado, o AMS segue um conjunto padrão de runbooks automatizados e manuais para garantir uma resposta consistente. Esses runbooks são compartilhados com os clientes do AMS durante a integração para que eles possam desenvolver e coordenar a resposta com o AMS. O AMS incentiva a execução conjunta de simulações de resposta de segurança com os clientes para desenvolver uma força operacional antes que ocorra um incidente real.

AWS Support

O AWS Support oferece uma variedade de planos que permitem acessar ferramentas e conhecimentos que apoiem o sucesso e a integridade operacional das suas soluções da AWS. Todos os planos de suporte oferecem acesso 24 horas por dia, 7 dias por semana ao atendimento ao cliente, à documentação da AWS, aos whitepapers e aos fóruns de suporte. Se precisar de suporte técnico e mais recursos para ajudar a planejar, implantar e otimizar o ambiente da AWS, você poderá selecionar um plano de suporte que se alinhe ao seu caso de uso da AWS.

Você deve considerar a Central de Suporte no AWS Management Console como o ponto central de contato para obter suporte para problemas que afetam seus recursos da AWS. O acesso ao AWS Support é controlado pelo IAM. Para obter mais informações sobre como obter acesso aos recursos de suporte da AWS, consulte Acessar o suporte.

Além disso, se você precisar denunciar uso abusivo do Amazon EC2, entre em contato com a Equipe de uso abusivo da AWS.

Suporte de resposta DDoS

Um ataque de negação de serviço (DoS) torna seu site ou aplicação indisponível para os usuários finais. Os invasores usam uma variedade de técnicas que consomem largura de banda da rede ou outros recursos, interrompendo o acesso de usuários finais legítimos. Em sua forma mais simples, um ataque DoS contra um alvo é executado por um único invasor de uma única fonte.

Em um ataque de negação de serviço distribuída (DDoS), um invasor usa várias fontes, que podem ser comprometidas ou controladas por um grupo de colaboradores, para orquestrar um ataque contra um alvo. Em um ataque DDoS, cada um dos colaboradores ou hosts comprometidos participa do ataque, gerando uma enxurrada de pacotes ou solicitações para sobrecarregar o alvo pretendido.

A AWS oferece o AWS Shield aos clientes, que é um serviço gerenciado de proteção contra DDoS que protege aplicações Web executadas na AWS. O AWS Shield fornece detecção sempre ativa e mitigações automáticas em linha que minimizam o tempo de inatividade e a latência das aplicações. Portanto, não há necessidade de contratar o AWS Support para se beneficiar da proteção contra DDoS. Existem dois níveis de AWS Shield: Standard e Advanced.

Todos os clientes da AWS se beneficiam das proteções automáticas do AWS Shield Standard sem custos. O AWS Shield Standard protege contra os ataques DDoS mais comuns e frequentes, que ocorrem na rede e na camada de transporte, e afetam seus sites ou aplicações. Quando você usa o AWS Shield Standard com o Amazon CloudFront e o Amazon Route 53, recebe proteção de disponibilidade abrangente contra todos os ataques à infraestrutura conhecidos (camadas 3 e 4).

Para obter níveis mais altos de proteção contra ataques direcionados a aplicações Web executadas em recursos dos serviços Amazon Elastic Compute Cloud (Amazon EC2) (EC2), Elastic Load Balancing (ELB), Amazon CloudFront e Amazon Route 53, você pode assinar o AWS Shield Advanced. Além disso, o AWS Shield Advanced oferece acesso 24 horas por dia, 7 dias por semana à Equipe de resposta a DDoS (DRT) da AWS. Para obter mais informações sobre AWS Shield Standard e AWS Shield Advanced, consulte AWS Shield.

Simular

Tópicos

- Simulações de resposta a incidentes de segurança
- Etapas de simulação
- Exemplos de simulação

Simulações de resposta a incidentes de segurança

Simulações de resposta a incidentes de segurança (SIRS) são eventos internos que oferecem uma oportunidade estruturada para praticar seu plano e procedimentos de resposta a incidentes durante um cenário realista. Os eventos de SIRS abrangem fundamentalmente a preparação e a melhoria iterativa dos recursos de resposta. Algumas das razões pelas quais os clientes encontram valor na realização de atividades de SIRS são:

- Validar a prontidão.
- Desenvolver confiança aprendendo com simulações e equipes de treinamento.
- Seguir a conformidade ou obrigações contratuais.
- Gerar artefatos para credenciamento.
- Ser ágil e obter melhorias incrementais com foco.
- Melhorar a velocidade e as ferramentas.
- Refinar a comunicação e a escalação.
- Ter tranquilidade diante de eventos raros e inesperados.

Por esses motivos, o valor derivado da participação em uma atividade do SIRS aumenta a eficácia da organização durante eventos estressantes. Desenvolver uma atividade de SIRS realista e benéfica pode ser um exercício difícil. Embora testar seus procedimentos ou automação para eventos bem compreendidos tenha certas vantagens, é igualmente valioso participar de atividades criativas de SIRS para testar a preparação diante do inesperado.

Etapas de simulação

Independentemente de você projetar sua própria SIRS ou ter um parceiro confiável para fornecer as bases, as simulações geralmente seguem estas etapas:

1. Encontrar um problema importante: defina o gatilho que deve causar uma resposta.
2. Identificar engenheiros de segurança qualificados: uma simulação exige um construtor e um testador.
3. Criar um sistema de modelo realista: a simulação deve ser realista e apropriada. Se não for realista, talvez os participantes não valorizem o exercício. Se for breve demais, o exercício poderá ser considerado trivial. Comece com exercícios simples e trabalhe visando um evento completo.
4. Criar e testar os elementos do cenário: pode ser necessário criar material de simulação relevante, como artefatos de registro em log, notificações e alertas por e-mail e possíveis runbooks.
5. Convidar outras pessoas de segurança e participantes interorganizacionais: convide todos que precisam treinar e participar. Se seu consultor jurídico geral, executivos e relações públicas participarem da simulação, você também deverá convidá-los.
6. Executar a simulação: determine se sua equipe deve esperar o evento de SIRS ou se a simulação deve permanecer sem aviso prévio.
7. Comemorar, medir, melhorar e repetir: a simulação tem fatores de estresse, por isso é importante incentivar e comemorar os esforços de seus participantes. Depois do incentivo, vem a oportunidade de medir, melhorar e iterar para a próxima simulação. A AWS incentiva você a criar o hábito de realizar essas atividades.

> **Important**
>
> Se você estiver planejando uma Simulação de resposta a incidentes de segurança (SIRS), consulte Teste de penetração e leia a seção Outros eventos simulados para obter as informações mais recentes sobre como proceder.

Exemplos de simulação

As simulações de segurança devem ser realistas para fornecer o valor esperado. Quando você ou seus parceiros trabalham para criar suas próprias simulações, sempre considere eventos

passados do mundo real como uma fonte valiosa para possíveis exercícios de simulação. Veja alguns exemplos que os clientes da AWS acharam úteis para usar em suas simulações iniciais:

- Alterações não autorizadas na configuração ou nos recursos da rede.
- Credenciais que foram expostas publicamente por engano devido à configuração incorreta do desenvolvedor.
- Conteúdo confidencial que foi disponibilizado publicamente por engano devido à configuração incorreta do desenvolvedor.
- Isolamento de um servidor Web que está se comunicando com endereços IP com suspeita de serem mal-intencionados.

Além do valioso aprendizado baseado em experiências, realizar atividades de SIRS gera resultados, como lições aprendidas, que você pode usar como contribuições para o próximo processo do seu programa: iteração.

Iteração

A seção anterior definiu alguns dos benefícios das atividades do SIRS. Entre essas vantagens estava ganhar agilidade por meio de melhorias incrementais. As simulações devem gerar resultados valiosos que você pode aproveitar para melhorar sua resposta de segurança. Elas fornecem um encaminhamento de feedback para a organização, sobre o que está ou não está funcionando. Com esse conhecimento, você pode criar procedimentos de forma incremental ou atualizar os existentes para melhorar sua resposta.

Tópicos

- Runbooks
- Automação

Runbooks

Quando uma anomalia de segurança é detectada, conter o evento e retornar a um bom estado conhecido são elementos importantes de um plano de resposta. Por exemplo, se a anomalia ocorreu devido a uma configuração incorreta de segurança, a correção pode ser tão simples quanto remover a variação por meio de uma reimplantação dos recursos com a configuração adequada. Para fazer isso, você precisará planejar com antecedência e definir seus próprios procedimentos de resposta de segurança, que geralmente são chamados de runbooks.

Um runbook é a forma documentada dos procedimentos de uma organização para conduzir uma tarefa ou série de tarefas. Essa documentação geralmente é armazenada em um sistema digital interno ou em papel impresso. No momento, você pode ter runbooks de resposta a incidentes ou precisar criá-los para estar em conformidade com uma framework de garantia de segurança. No entanto, quando você segue manualmente os runbooks escritos, aumenta o potencial de cometer erros. Em vez disso, recomendamos que você automatize todas as suas tarefas repetíveis. A automação libera sua equipe de resposta de tarefas comuns e as disponibiliza para tarefas mais importantes, como correlacionar eventos, praticar em simulações, elaborar procedimentos de resposta, realizar pesquisas, desenvolver novas habilidades e testar ou criar ferramentas. No entanto, antes de poder decompor as tarefas em lógica programável e iterar em direção à automação adequada, você deve começar redigindo um runbook.

Criar runbooks

Para criar runbooks para a nuvem, recomendamos que você primeiro se concentre nos alertas gerados atualmente. Se você gerar um alerta, é importante investigá-lo. Comece definindo as descrições dos processos manuais que você executa. Depois disso, teste os processos e itere o padrão de runbook para melhorar a lógica básica de sua resposta. Determine quais são as exceções e quais são as resoluções alternativas para esses cenários. Por exemplo, em um ambiente de desenvolvimento, talvez convenha encerrar uma instância do Amazon EC2 configurada incorretamente. No entanto, se o mesmo evento tiver ocorrido em um ambiente de produção, em vez de encerrar a instância, você poderá interrompê-la e verificar com as partes interessadas se os dados críticos não serão perdidos e se o encerramento é ou não aceitável.

Depois de determinar a melhor solução, você pode desconstruir a lógica em uma solução baseada em código, que pode ser usada como uma ferramenta pela equipe de resposta a fim de automatizar a resposta e remover a variação ou o trabalho de adivinhação da equipe. Isso acelera o ciclo de vida de uma resposta. O próximo objetivo é permitir a total automatização desse código por meio da invocação por alertas ou pelos eventos, e não por um respondente humano, para criar uma resposta orientada por eventos.

Conceitos básicos

Se você não tiver certeza de por onde começar, recomendamos iniciar com os alertas que podem ser gerados pelas AWS Trusted Advisor, Práticas recomendadas de segurança básicas do AWS Security Hub e Regras do AWS Config (incluindo o Repositório do Regras do AWS Config do Github). Depois, concentre-se nos eventos gerados por serviços que descreverão os sistemas com os quais você está preocupado.

O Amazon GuardDuty e o Access Analyzer descrevem muitos dos domínios que uma aplicação usará na AWS, e é por isso que eles geralmente são sugeridos. No entanto, o Amazon Inspector e o Amazon Macie têm usos específicos para os que têm preocupações com dados e endpoints. As informações sobre as descobertas do Amazon GuardDuty estão disponíveis no Guia do usuário do Amazon GuardDuty. As descobertas do Access Analyzer estão disponíveis no Guia do usuário do Amazon Access Analyzer. As descobertas do Macie estão disponíveis no Guia do usuário do Amazon Macie. As descobertas do Amazon Inspector estão disponíveis no Guia do usuário do Amazon Inspector. O Security Hub oferece a capacidade de unificar essas descobertas em um só lugar e reagir a elas em conjunto com baixa latência, e é por isso que é sugerido como um local central para correção.

Todos os serviços acima enviam notificações por meio do Amazon CloudWatch Events quando ocorre qualquer alteração nas descobertas ou alertas, incluindo alertas recém-gerados e atualizações de alertas existentes. Você pode configurar as regras do Amazon CloudWatch Events a fim de acionar funções do AWS Lambda para executar uma resposta orientada a eventos. No entanto, a capacidade de criar insights personalizados e adicionar suas próprias descobertas do domínio da aplicação aumenta os principais motivos para usar o Security Hub. Para obter mais informações, consulte a seção Resposta orientada por eventos.

Automação

A automação é um multiplicador de força, o que significa que ela dimensiona os esforços de sua equipe de resposta para corresponder à velocidade da organização. Migrar de processos manuais para processos automatizados permite que você gaste mais tempo aumentando a segurança do seu ambiente da Nuvem AWS.

Tópicos

- Automatizar a resposta a incidentes
- Resposta orientada por eventos

Automatizar a resposta a incidentes

Para automatizar as funções de engenharia e operações de segurança, você pode usar um conjunto abrangente de APIs e ferramentas da AWS. Você pode automatizar totalmente o gerenciamento de identidades, a segurança da rede, a proteção de dados e os recursos de monitoramento. 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 o seu procedimento de segurança e reajam manualmente a eventos.

Se as equipes de resposta a incidentes continuarem a responder aos alertas da mesma forma, há 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.

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 pode decompor esse padrão em lógica acionável e elaborar o código para executar essa lógica. Os respondentes 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.

No entanto, seu objetivo deve ser reduzir ainda mais o intervalo de tempo entre os mecanismos de detecção e os mecanismos responsivos. Historicamente, esse intervalo de tempo pode levar horas, dias ou até meses. Uma Pesquisa de resposta a incidentes realizada pela SANS em 2016 descobriu que 21% dos entrevistados afirmaram que seu tempo de detecção foi de dois a sete dias, e apenas 29% dos entrevistados conseguiram corrigir eventos no mesmo período. Na nuvem, você pode reduzir esse intervalo de tempo de resposta para segundos criando recursos de resposta orientados por eventos.

Tópicos

- Opções para automatizar a resposta
- Comparações de custos em métodos de verificação

Opções para automatizar a resposta

É importante equilibrar a implementação empresarial e a estrutura da organização. A Figura 4 ilustra as diferenças nos atributos técnicos de cada opção de resposta automatizada em sua implementação da AWS com um grafo de radar. No grafo, quanto mais o atributo técnico se move do centro, maior a força desse atributo técnico para a resposta de automação correspondente. Por exemplo, AWS Lambda oferece mais velocidade e requer menos habilidades técnicas. AWS Fargate oferece mais flexibilidade e requer menos manutenção e conjunto de habilidades técnicas. A Tabela 1 fornece uma visão geral dessas opções de automação e um resumo dos atributos técnicos de cada uma.

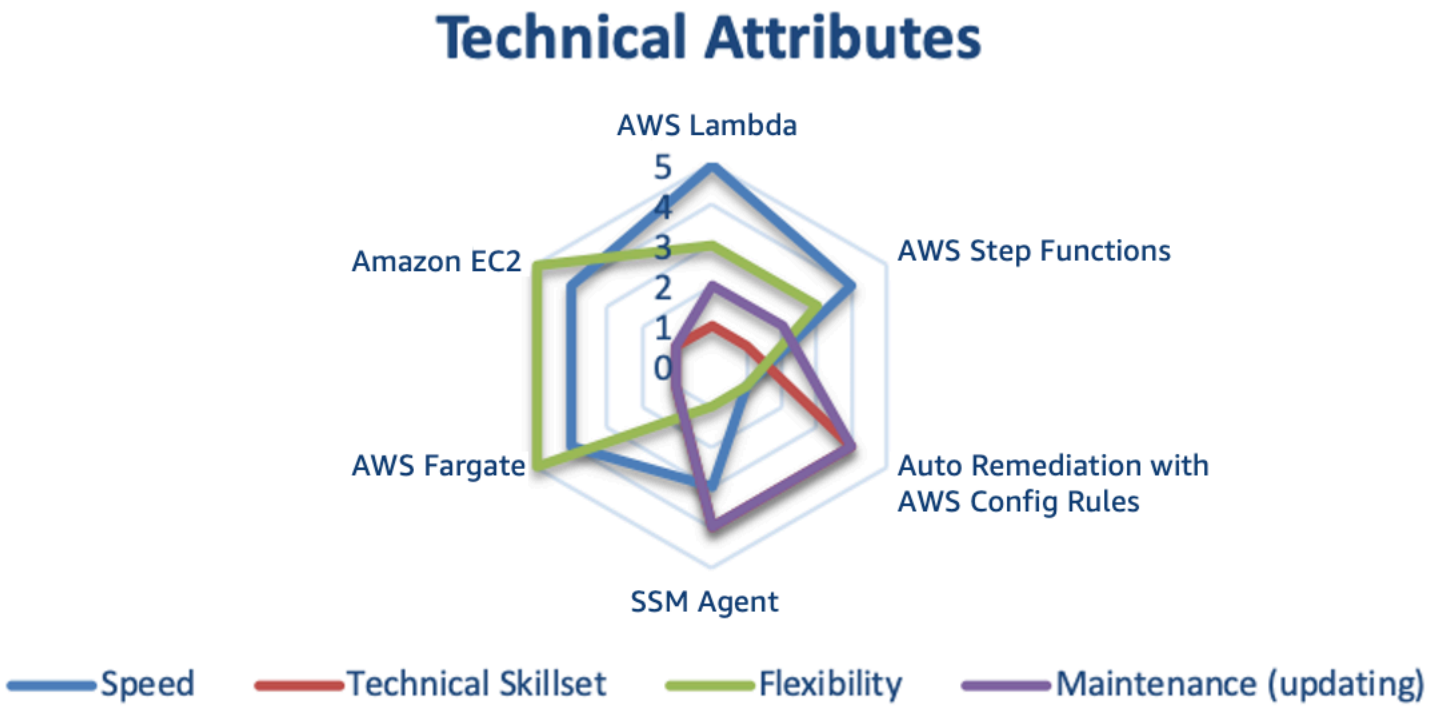

Figura 4: Diferenças nos atributos técnicos nas abordagens de resposta automatizada

Tabela 1: Opções de resposta automatizada

Serviço ou recurso da AWS	Descrição	Resumo dos atributos*
AWS Lambda	Sistema usando apenas o AWS Lambda, com a linguagem empresarial da sua organização.	Velocidade Flexibilidade Manutenção Conjunto de habilidades
AWS Step Functions	Sistema usando o AWS Step Functions, o Lambda e o SSM Agent.	Velocidade Flexibilidade Manutenção Conjunto de habilidades
Correção automática com Regras do AWS Config	Conjunto de Regras do AWS Config e correções automátic	Manutenção e conjunto de habilidades

Serviço ou recurso da AWS	Descrição	Resumo dos atributos*
	as que avaliam o ambiente e o colocam de volta na especific ação aprovada.	Velocidade e flexibilidade
SSM Agent	Conjunto de regras e documentos de automação que revisam várias partes dos ambientes e sistemas internos e fazem correções.	Manutenção e conjunto de habilidades Velocidade Flexibilidade
AWS Fargate	O sistema AWS Fargate que usa código de função de etapa de código aberto e os eventos do Amazon CloudWatch e outros sistemas para impulsionar a detecção e a correção.	Flexibilidade Velocidade Manutenção e conjunto de habilidades
Amazon EC2	Um sistema em execução em uma instância completa, semelhante à opção AWS Fargate.	Flexibilidade Velocidade Manutenção Conjunto de habilidades

* Os atributos são listados em ordem decrescente para cada serviço ou recurso. Por exemplo, o AWS Lambda oferece mais velocidade e requer menos habilidades técnicas. O AWS Fargate oferece mais flexibilidade e requer menos manutenção e conjunto de habilidades técnicas.

Ao considerar essas opções de automação em seu ambiente da AWS, você também precisa considerar a centralização e o período de verificação (eventos por segundo [EPS]).

A centralização se refere a uma conta central que impulsiona toda a detecção e correção de uma organização. Essa abordagem pode parecer a melhor escolha pronta para uso e é a prática recomendada atual. No entanto, algumas circunstâncias exigem que você se desvie dessa abordagem, e entender quando dependerá da forma como você lida com suas contas subordinadas.

Incentivamos você a começar utilizando a abordagem da conta do Security Tooling em Multi-Account Framework em AWS Organizations (Framework de várias contas em AWS Organizations) ou em AWS Control Tower.

Tabela 2: Prós e contras da centralização

	Centralização	Descentralização
Vantagens	Gerenciamento de configuração simples Não é possível cancelar nem modificar a resposta	Arquitetura simples Configuração inicial mais rápida
Desvantagens	Maior complexidade na arquitetura Integrar/desintegrar contas e recursos	Mais recursos para gerenciar Dificuldade em manter uma linha de referência de software

Uma comparação de custos dessas implementações também pode conduzir a decisão da sua empresa ao determinar a melhor opção. Eventos por segundo (EPS) é a métrica que você usa para estimar melhor o custo. No final das contas, pode ser muito mais fácil e barato usar abordagens centralizadas ou descentralizadas, mas é impossível analisar como você avaliará esse custo especificamente em sua conta. Considere o EPS ao enviar esses eventos para uma conta central para serem respondidos. Quanto mais EPS, maior o custo de enviar esses eventos para uma conta centralizada.

Comparações de custos em métodos de verificação

Os custos são determinados ainda pelo método de verificação pelo qual uma anomalia é detectada e pelo período entre as validações. Para métodos de verificação, você pode escolher entre análise baseada em evento ou de verificação periódica. A Tabela 3 mostra as vantagens e as desvantagens das duas abordagens.

Tabela 3: Vantagens e desvantagens dos diferentes métodos de verificação

	Baseada em eventos	Verificação periódica
Vantagens	Menos tempo desde o evento até a resposta Necessidade limitada de consultar chamadas de API adicionais	Imagem completa em um determinado momento
Desvantagens	Contexto de estado limitado em torno do recurso Os eventos acionados podem ser para um recurso que não está prontamente disponível	Limites do serviço para contas grandes Pode ser executado com limitação devido ao alto volume de chamadas de API

Em muitos casos, uma combinação das duas abordagens de verificação é provavelmente a melhor escolha em uma organização totalmente madura. O AWS Security Hub e o padrão e as práticas recomendadas de segurança básica da AWS oferecem uma combinação dos dois métodos de verificação.

A Figura 5 fornece um grafo de radar ilustrando a comparação de custos de eventos por segundo (EPS) para cada uma das abordagens de automação. Por exemplo, o Amazon EC2 e o AWS Fargate têm os custos mais altos para executar de 0 a 10 EPS, AWS Lambda e AWS Step Functions têm os custos mais altos para executar mais de 76 EPS.

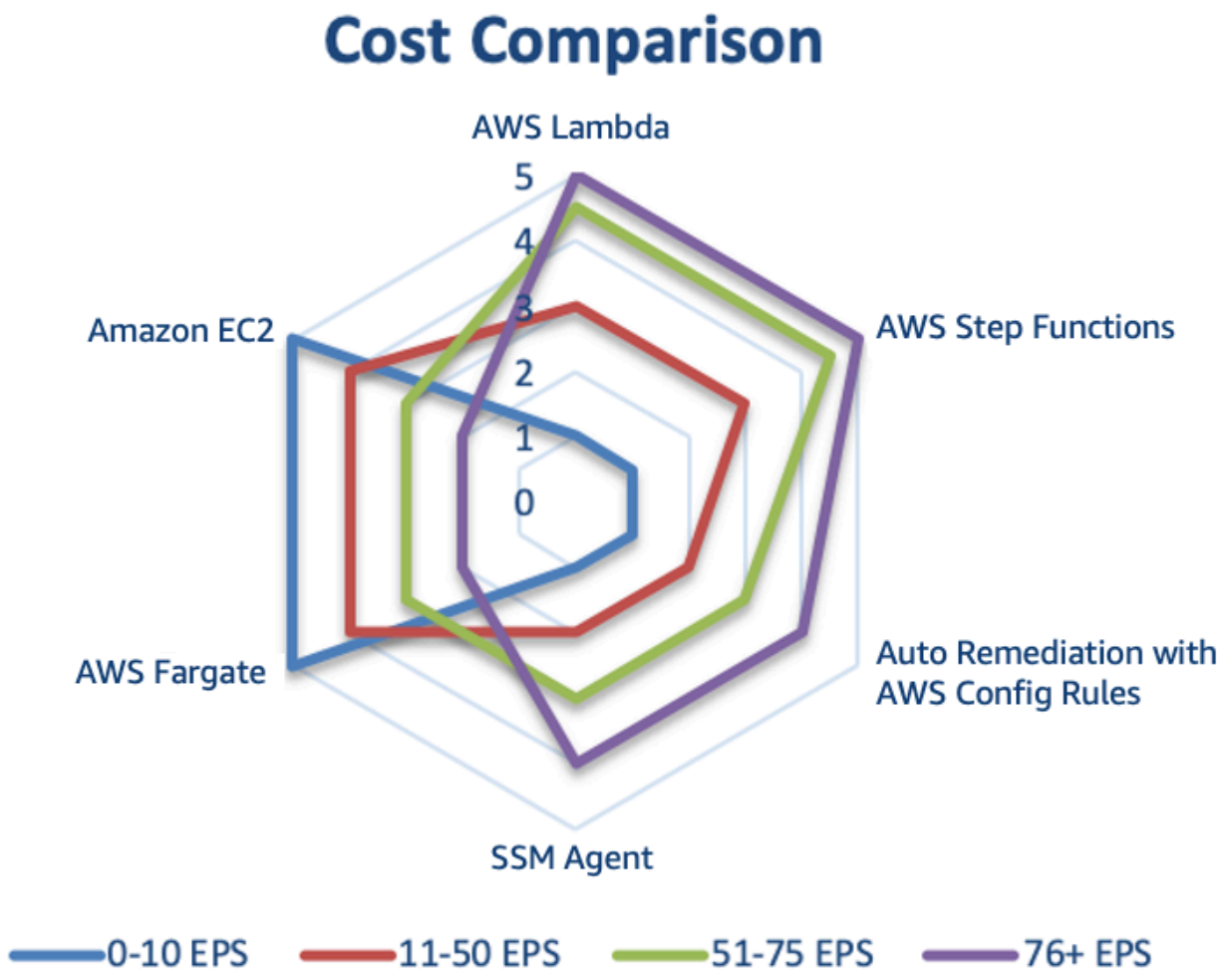

Figura 5: Comparação de custos dos métodos de verificação de opções de automação (eventos por segundo [EPS])

Resposta orientada por eventos

Com um sistema de resposta orientado por eventos, um mecanismo de detecção aciona um mecanismo responsivo para corrigir automaticamente o evento. Você pode usar recursos de resposta orientados por eventos para reduzir o tempo de retorno entre os mecanismos de detecção e os mecanismos responsivos. Para criar essa arquitetura orientada por eventos, é possível usar o AWS Lambda, que é um serviço computacional sem servidor que executa o código em resposta a eventos e gerencia automaticamente os recursos computacionais subjacentes.

Por exemplo, suponha que você tenha uma conta da AWS com o serviço AWS CloudTrail habilitado. Se o AWS CloudTrail for desabilitado (por meio da API `cloudtrail:StopLogging`), o procedimento de resposta é habilitar o serviço novamente e investigar o usuário que desativou

o registro em log AWS CloudTrail. Em vez de executar essas etapas manualmente no AWS Management Console, você pode habilitar o registro em log de forma programática novamente (por meio da API `cloudtrail:StartLogging`). Se você implementar isso com código, seu objetivo de resposta é executar essa tarefa o mais rápido possível e notificar a equipe de reposta que a resposta foi executada.

Você pode decompor a lógica em código simples para ser executado em uma função do AWS Lambda para realizar essas tarefas. Depois, você pode usar o Amazon CloudWatch Events para monitorar o evento do `cloudtrail:StopLogging` específico e invocar a função se ele ocorrer. Quando essa função de resposta do AWS Lambda é invocada pelo Amazon CloudWatch Events, você pode passar a ela os detalhes do evento específico com as informações da entidade principal que desativou o AWS CloudTrail, quando foi desabilitado, o recurso específico que foi afetado e outras informações pertinentes. Você pode usar essas informações para enriquecer a descoberta dos logs e, depois, gerar uma notificação ou alerta com apenas os valores específicos que um analista de resposta exigiria.

O ideal é que o objetivo da resposta orientada por eventos seja que a função de resposta do Lambda execute as tarefas de resposta e, depois, notifique a equipe de resposta que a anomalia foi resolvida com êxito com todas as informações contextuais pertinentes. Cabe então à equipe de resposta decidir como determinar por que isso ocorreu e como futuras recorrências podem ser evitadas. Esse encaminhamento de feedback impulsiona ainda mais a melhoria da segurança em seus ambientes de nuvem. Para atingir esse objetivo, você deve ter uma cultura que permita que sua equipe de segurança trabalhe mais de perto com suas equipes de desenvolvimento e operações.

Exemplos de resposta a incidentes

Tópicos

- Incidentes de domínio de serviço
- Incidentes do domínio de infraestrutura

Incidentes de domínio de serviço

Os incidentes de domínio de serviço geralmente são tratados exclusivamente por meio de APIs da AWS.

Identidades

A AWS fornece APIs para nossos serviços de nuvem que são usadas por milhões de clientes para criar aplicações e impulsionar resultados de negócios. Essas APIs podem ser invocadas por meio de vários métodos, como por Kits de Desenvolvimento de Software (SDKs), a AWS CLI e o AWS Management Console. Para interagir com a AWS por meio desses métodos, o serviço do IAM ajuda você a controlar com segurança o acesso aos recursos da AWS. Você usa o IAM para controlar quem é autenticado (fez login) e autorizado (tem permissões) a usar os recursos no nível da conta. Para obter uma lista dos serviços da AWS que você pode usar com o IAM, consulte Serviços da AWS que funcionam com o IAM.

Ao criar uma conta da AWS, você começa com uma identidade de autenticação única (SSO) que tem acesso completo a todos os serviços e recursos da AWS na conta. Essa identidade é chamada de usuário raiz da conta da AWS e é acessada pelo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável que você não use o usuário raiz para suas tarefas diárias e, particularmente, não para tarefas administrativas. Em vez disso, recomendamos seguir a prática recomendada de usar o usuário raiz apenas para criar o primeiro usuário do IAM, armazenar de forma segura as credenciais do usuário raiz e executar apenas algumas tarefas de gerenciamento de contas e serviços. Para obter mais informações, consulte Criar usuários individuais do IAM.

Embora essas APIs forneçam valor a milhões de clientes, algumas delas poderão ser utilizadas indevidamente se as pessoas erradas obtiverem acesso à sua conta do IAM ou às credenciais raiz. Por exemplo, você pode usar as APIs para habilitar o registro em log em sua conta, como AWS CloudTrail. No entanto, se invasores obtiverem suas credenciais, eles também poderão usar a API

para desabilitar esses logs. Você pode evitar esse tipo de uso abusivo configurando as permissões apropriadas do IAM que seguem um modelo de privilégio mínimo e protegendo adequadamente suas credenciais do IAM. Para obter mais informações, consulte as Práticas recomendadas do IAM no Guia do usuário do AWS Identity and Access Management. Se esse tipo de evento ocorrer, há vários controles de detecção para identificar que o registro em log do AWS CloudTrail foi desativado, incluindo o AWS CloudTrail, AWS Config, o AWS Trusted Advisor, o Amazon GuardDuty e o AWS CloudWatch Events.

Recursos

Outros recursos que podem ser utilizados ou configurados incorretamente variam de organização para organização, com base em como cada cliente opera na nuvem. Por exemplo, algumas organizações planejam tornar determinados dados ou aplicações acessíveis publicamente, enquanto outras mantêm suas aplicações e dados internos e confidenciais. Nem todos os eventos de segurança são mal-intencionados por natureza; alguns podem resultar de configurações não intencionais ou inadequadas. Considere quais APIs ou recursos têm um alto impacto em sua organização e se você os usa com mais frequência ou pouca frequência.

É possível identificar muitas configurações de segurança incorretas usando ferramentas e serviços. Por exemplo, o AWS Trusted Advisor fornece várias verificações para as práticas recomendadas. Os parceiros da APN também oferecem centenas de produtos líderes do setor que são equivalentes, idênticos ou se integram aos controles existentes nos seus ambientes on-premises. Vários desses produtos e soluções foram pré-qualificados pelo Programa de competência para parceiros da AWS. Recomendamos que você visite a seção Análise de configuração e vulnerabilidade do Programa de competência em segurança da APN para procurar essas soluções e determinar se elas podem atender aos seus requisitos.

Incidentes do domínio de infraestrutura

O domínio de infraestrutura normalmente inclui dados da aplicação ou atividades relacionadas à rede, como o tráfego para suas instâncias do Amazon EC2 na VPC e os processos em execução nos sistemas operacionais da instância do Amazon EC2.

Por exemplo, suponha que sua solução de monitoramento tenha notificado você sobre uma possível anomalia de segurança em sua instância do Amazon EC2. As ações a seguir são etapas comuns para resolver esse problema:

1. Capture os metadados da instância do Amazon EC2 antes de fazer qualquer alteração em seu ambiente.

2. Proteja a instância do Amazon EC2 contra encerramento acidental, habilitando a proteção contra o encerramento da instância.
3. Isole a instância do Amazon EC2 alternando o grupo de segurança da VPC. No entanto, lembre-se do rastreamento de conexão da VPC e outras técnicas de contenção.
4. Desvincule a instância do Amazon EC2 de todos os grupos AWS Auto Scaling.
5. Cancele o registro da instância do Amazon EC2 de todos os serviços Elastic Load Balancing relacionados.
6. Faça um snapshot dos volumes de dados do Amazon EBS anexados à instância do EC2 para preservação e investigações de acompanhamento.
7. Etiquete a instância do Amazon EC2 como colocada em quarentena para investigação e adicione todos os metadados pertinentes, como o tíquete de problema associado à investigação.

É possível executar todas as etapas anteriores usando as APIs da AWS e os AWS SDKs, além da AWS CLI e AWS Management Console. Para interagir com a AWS usando esses métodos, o serviço do IAM ajuda você a controlar com segurança o acesso aos recursos da AWS. Use o IAM para controlar quem está autenticado e autorizado a usar recursos no nível da conta. O serviço do IAM fornece a autenticação e a autorização para você executar essas ações e interagir com o domínio do serviço.

Um snapshot de um volume do Amazon EBS é uma cópia, no nível do bloco, de um volume de dados do EBS em um ponto anterior no tempo, que ocorre de forma assíncrona e pode levar algum tempo para ser concluído, mas é um delta desses dados desse ponto em diante. Você pode criar volumes do EBS a partir dessas cópias e montá-los na instância forense do EC2 para análise profunda offline por investigadores forenses. O diagrama a seguir mostra uma versão simplificada do resultado e não descreve todos os componentes de rede (como sub-redes, tabelas de roteamento e listas de controle de acesso à rede).

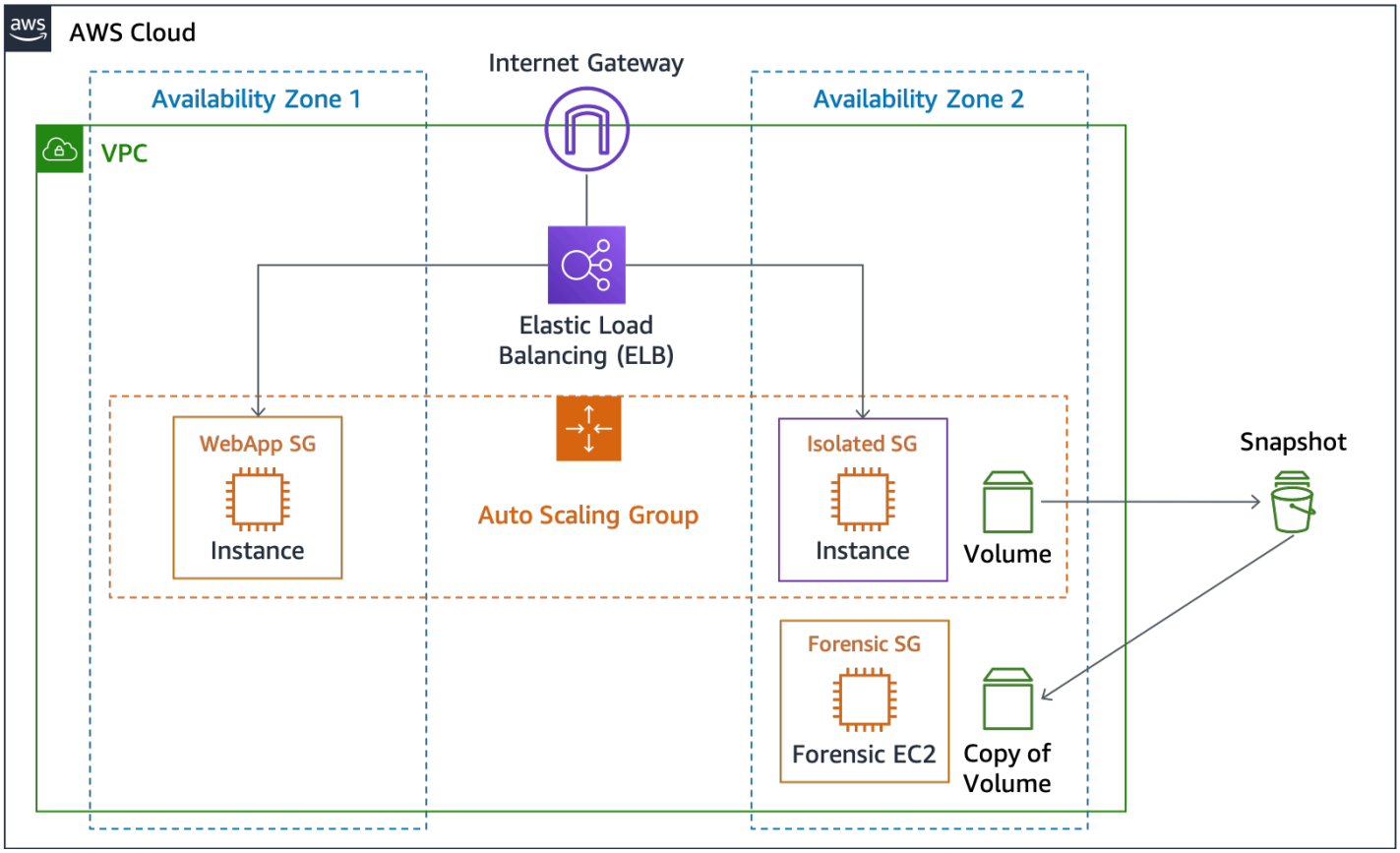

Figura 6: Isolamento e snapshots da instância do EC2

Tópicos

- Decisões de investigação
- Capturar dados voláteis
- Usar o AWS Systems Manager
- Automatizar a captura

Decisões de investigação

Nesse ponto, você pode escolher entre uma investigação offline (encerrar imediatamente a instância) ou uma investigação online (manter a instância em execução). Uma vantagem da investigação offline é que, depois que a instância é desligada, ela não pode mais afetar o ambiente existente. Além disso, você pode criar uma cópia da instância afetada a partir dos snapshots do EBS e analisá-la em uma conta isolada da AWS com um ambiente isolado projetado especificamente para sua investigação. No entanto, é possível optar por não desligar a instância imediatamente, se uma

investigação online permitir que você capture evidências voláteis do sistema operacional host, como memória ou tráfego de rede.

Capturar dados voláteis

Embora você possa optar por não realizar a investigação online, é importante entender os mecanismos necessários para capturar dados voláteis de uma instância. Uma investigação online exige interação com o sistema operacional que está sendo executado na instância do Amazon EC2. Nesse caso, você precisa de mais do que o serviço AWS IAM para executar tarefas em uma instância do Amazon EC2. Embora você possa realizar a autenticação diretamente na máquina usando um método padrão (como o shell seguro do Linux (SSH) ou a área de trabalho remota do Microsoft Windows (RDP)), a interação manual com o sistema operacional não é uma prática recomendada. Recomendamos usar programaticamente uma ferramenta de automação para executar tarefas em um host.

Usar o AWS Systems Manager

O AWS Systems Manager Run Command ajuda a executar alterações sob demanda de forma remota e segura executando scripts de shell do Linux e comandos do Windows PowerShell em uma instância de destino. Embora seja possível invocar o Run Command por meio de permissões no serviço AWS IAM, é necessário primeiro ativar suas instâncias do Amazon EC2 como instâncias gerenciadas, instalar o SSM Agent em suas máquinas (se ele não estiver instalado por padrão) e configurar as permissões do AWS IAM. Se você estiver interessado em usar o Run Command para atividades de automação ou resposta, execute as atividades de pré-requisito antes de realizar uma investigação.

O AWS Systems Manager, que inclui o Run Command, é integrado ao AWS CloudTrail, um serviço que captura chamadas de API feitas por ou em nome de um Systems Manager e entrega os arquivos de log a um bucket do Amazon S3 especificado por você. Usando as informações coletadas pelo AWS CloudTrail, você pode determinar qual solicitação foi feita, o endereço IP de origem a partir do qual a solicitação foi feita, quem a fez, quando ela foi feita etc. O CloudTrail cria logs de todas as ações da API do Systems Manager, incluindo solicitações de API para executar comandos usando o Run Command ou para criar documentos do Systems Manager.

Você pode usar o serviço AWS Systems Manager Run Command para chamar o SSM Agent que executa scripts de shell do Linux e comandos do Windows PowerShell. Esses scripts podem carregar e executar ferramentas específicas para capturar dados adicionais do host, como o módulo de kernel Linux Memory Extractor (LiME). Depois, você pode transferir a captura de memória

para sua instância forense do Amazon EC2 na rede VPC ou para um bucket do Amazon S3 para armazenamento durável.

Automatizar a captura

Um método para invocar o SSM Agent é direcionar o Run Command por meio do Amazon CloudWatch Events quando a instância é marcada com uma etiqueta específica. Por exemplo, se você aplicar a etiqueta `Response=Isolate+MemoryCapture` a uma instância afetada, poderá configurar o Amazon CloudWatch Events para acionar duas ações:

- Uma função do Lambda que executa as atividades de isolamento
- Um Run Command que executa um comando shell para exportar a memória Linux por meio do SSM Agent

Essa resposta orientada por etiqueta é outro método de resposta orientada a eventos.

Conclusão

Ao continuar sua jornada para a nuvem, é importante considerar os conceitos fundamentais de resposta a incidentes de segurança mencionados anteriormente para o seu ambiente da AWS. Você pode combinar os controles disponíveis, os recursos de nuvem e as opções de correção para ajudar a melhorar a segurança do seu ambiente de nuvem. Você também pode começar pequeno e iterar à medida que adota recursos de automação que melhoram sua velocidade de resposta, para que você esteja mais bem preparado quando ocorrerem eventos de segurança.

Recursos adicionais

Para obter informações adicionais, consulte:

- AWS Well-Architected
- Página AWS Cloud Adoption Framework
- Solução centralizada de registro em log da AWS
- Visualize AWS CloudTrail Logs usando o AWS Glue Amazon QuickSight
- Como monitorar alertas do sistema de detecção de intrusões baseado em host em instâncias do Amazon EC2
- Armazenar e monitorar arquivos de log de aplicações e sistema operacional com o Amazon CloudWatch
- Gerenciamento de Identidade e Acesso no Amazon S3
- Usar o versionamento (Amazon S3)
- Usar exclusão de MFA
- Proteger dados usando criptografia do servidor com chaves gerenciadas AWS KMS (SSE-KMS)
- Resposta a incidentes com o Console AWS e a CLI
- Preparar-se para a Lei de proteção da privacidade do consumidor da Califórnia

Mídia

- AWS re:Invent 2014 (SEC402): Detecção de intrusão na nuvem
- AWS re:Invent 2014 (SEC404): Resposta a incidentes na nuvem
- AWS re:Invent 2015 (SEC308): Enfrentar eventos de segurança na nuvem
- AWS re:Invent 2015 (SEC316): Fortalecer sua arquitetura com simulações de resposta a incidentes de segurança
- AWS re:Invent 2016 (SEC313): Automatizar a resposta a eventos de segurança, da ideia, ao código e à execução
- AWS re:Invent 2017 (SID302): Forçar a multiplicação da sua equipe de segurança com automação e Alexa
- AWS re:Invent 2016 (SAC316): Automação de segurança: gaste menos tempo protegendo suas aplicações

- AWS re:Invent 2016 (SAC304): Segurança preditiva: usar big data para fortalecer suas defesas
- AWS re:Invent 2017 (SID325): Amazon Macie: visibilidade de dados viabilizada pelo machine learning para workloads de segurança e conformidade
- AWS London Summit 2018: Automatizar a resposta a incidentes e a análise forense na AWS

Ferramentas de terceiros

Os links a seguir para ferramentas de terceiros são externos e não são endossados pela AWS. A AWS não oferece garantias nem presta declarações de nenhum tipo sobre essas ferramentas ou páginas.

- AWS_IR: utilitário de linha de comando instalável em Python para redução do comprometimento do host e de chaves.
- MargaritaShotgun: ferramenta de aquisição de memória remota.
- ThreatPrep: módulo Python para avaliação das práticas recomendadas da conta da AWS em relação à preparação para tratamento de incidentes.
- ThreatResponse Web: plataforma de análise baseada na Web para uso com a ferramenta da linha de comando AWS_IR.
- GRR Rapid Response: análise forense remota ao vivo para resposta a incidentes.
- Linux Write Blocker: o patch do kernel e as ferramentas de espaço do usuário para habilitar o bloqueio de gravação de software Linux.

Referências do setor

- NIST SP 800-61R2: Guia de tratamento de incidentes de segurança do computador

Revisões do documento

Para ser notificado sobre atualizações deste whitepaper, inscreva-se no RSS feed.

update-history-change	update-history-description	update-history-date
Atualizações secundárias	Correções de bugs e várias pequenas alterações.	2 de junho de 2021
Atualização secundária	Links quebrados corrigidos.	5 de março de 2021
Whitepaper atualizado	Correção de links quebrados e várias alterações do texto para melhorar a legibilidade.	23 de novembro de 2020
Atualização secundária	Correção do link para “Resposta a incidentes com a CLI e o Console AWS”.	30 de junho de 2020
Whitepaper atualizado	Atualizado com novos serviços de segurança, inteligência contra ameaças, responsab ilidade compartilhada por contêineres, automação e CCPA. Inclusão de apêndices com exemplo de árvore de decisão e runbook.	11 de junho de 2020
Publicação inicial	Primeira publicação do whitepaper	1 de junho de 2019

Apêndice A: Definições de capacidade da nuvem

A AWS oferece mais de 150 serviços de nuvem e milhares de recursos. Muitos deles fornecem recursos nativos de detecção, preventivos e responsivos, e outros podem ser usados para arquitetar soluções de segurança personalizadas. Esta seção inclui um subconjunto desses serviços que são mais relevantes para a resposta a incidentes na nuvem.

Tópicos

- Registro em log e eventos
- Visibilidade e alertas
- Automação
- Armazenamento seguro
- Personalizar

Registro em log e eventos

AWS CloudTrail: AWS CloudTrail é um serviço que permite governança, conformidade, auditoria operacional e auditoria de riscos da conta da AWS. Com o CloudTrail, é possível registrar em log, monitorar continuamente e reter a atividade da conta relacionada a ações em toda a infraestrutura da AWS. O CloudTrail fornece o histórico de eventos da atividade da conta da AWS, incluindo ações realizadas por meio do AWS Management Console, SDKs da AWS, ferramentas da linha de comando e outros serviços da AWS. Esse histórico de eventos simplifica a análise de segurança, o rastreamento de alterações de recursos e a solução de problemas.

Os arquivos de log validados são valiosíssimos para segurança e investigações forenses. Para determinar se um arquivo de log foi modificado, excluído ou permaneceu inalterado depois de fornecido pelo CloudTrail, use a validação de integridade do arquivo de log do CloudTrail. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Desse modo, é computacionalmente impraticável modificar, excluir ou forjar arquivos de log do CloudTrail sem detecção.

Por padrão, os arquivos de log entregues pelo CloudTrail ao seu bucket são criptografados pela criptografia do lado do servidor da Amazon. Você também pode usar as chaves gerenciadas AWS Key Management Service (AWS KMS) (SSE-KMS) para seus arquivos de log do CloudTrail.

Eventos do Amazon CloudWatch: o Amazon CloudWatch Events oferece uma transmissão quase em tempo real de eventos do sistema que descrevem alterações nos recursos da AWS ou quando as chamadas de API são publicadas pelo AWS CloudTrail. Com regras simples que você pode configurar rapidamente, é possível estabelecer correspondência com eventos e roteá-los para uma ou mais transmissões ou funções de destino. O CloudWatch Events fica ciente das alterações operacionais à medida que elas ocorrem. O CloudWatch Events pode responder a essas alterações operacionais e executar a ação corretiva conforme necessário, enviando mensagens para responder ao ambiente, ativando funções, fazendo alterações e capturando informações de estado. Alguns serviços de segurança, como o Amazon GuardDuty, produzem sua saída na forma do CloudWatch Events.

AWS Config: AWS Config é um serviço que possibilita avaliar e auditar as configurações de seus recursos da AWS. O Config monitora e grava continuamente registros das configurações de recursos da AWS e permite automatizar a avaliação das configurações registradas com base nas configurações desejadas. Com o Config, você pode revisar as alterações nas configurações e nos relacionamentos entre os recursos da AWS, manual ou automaticamente. Você pode revisar históricos detalhados da configuração dos recursos e determinar sua conformidade geral com as configurações especificadas nas diretrizes internas. Isso permite simplificar a auditoria de conformidade, a análise de segurança, o gerenciamento de alterações e a solução de problemas operacionais.

Logs de acesso do Amazon S3: se você armazenar informações confidenciais em um bucket do Amazon S3, poderá habilitar os logs de acesso do S3 para registrar cada upload, download e modificação desses dados. Esse log é separado e adicionado aos logs do CloudTrail que registram alterações no próprio bucket (como alteração de políticas de acesso e políticas de ciclo de vida).

Amazon CloudWatch Logs: você pode usar o Amazon CloudWatch Logs para monitorar, armazenar e acessar seus arquivos de log (como seu sistema operacional, aplicação e arquivos de log personalizados) de suas instâncias do Amazon Elastic Compute Cloud (Amazon EC2) usando o agente do CloudWatch Logs. Além disso, o Amazon CloudWatch Logs pode capturar logs do AWS CloudTrail, de consultas de DNS do Amazon Route 53, de logs de fluxo da VPC, de funções do Lambda e de outras fontes. Depois, é possível recuperar os dados de log associados do CloudWatch Logs.

Amazon VPC Flow Logs: logs de fluxo da VPC permitem capturar informações sobre o tráfego IP que entra e sai de interfaces de rede em sua VPC. Depois que você tiver criado um log de fluxo, poderá visualizar e recuperar esses dados no Amazon CloudWatch Logs. Os logs de fluxo da VPC podem ajudar em diversas tarefas. Por exemplo, você pode usar logs de fluxo para solucionar o problema

pelo qual o tráfego específico não está atingindo uma instância, o que pode ajudar a diagnosticar regras de grupo de segurança excessivamente restritivas. Além disso, é possível usar os logs de fluxo como ferramenta de segurança para monitorar o tráfego para a sua instância.

Logs do AWS WAF: o AWS WAF agora é compatível com o registro em log completo de todas as solicitações da web que são inspecionadas pelo serviço. Você pode armazenar esses logs no Amazon S3 para fins de conformidade e auditoria, bem como usá-los para depuração e análises forenses adicionais. Os logs ajudam você a compreender por que algumas regras são acionadas e algumas solicitações web são bloqueadas. Você também pode integrar os logs com seu SIEM e ferramentas de análise de log.

Outros registros da AWS: com o ritmo de inovação, continuamos a implantar novos recursos para os clientes praticamente todos os dias, o que significa que existem dezenas de serviços da AWS que fornecem recursos de registro em log e monitoramento. Para obter informações sobre os recursos disponíveis para cada serviço da AWS, consulte a documentação da AWS para o serviço em questão.

Visibilidade e alertas

AWS Security Hub: o AWS Security Hub oferece uma visão abrangente de seus alertas de segurança de prioridade alta e do status de conformidade em todas as suas contas da AWS. Com o Security Hub, você tem um único local que agrega, organiza e prioriza alertas de segurança ou descobertas de vários serviços da AWS, como o Amazon GuardDuty, o Amazon Inspector e o Amazon Macie, bem como de soluções de parceiros da AWS. As descobertas são resumidas visualmente em painéis integrados com tabelas e grafos práticos. Você também pode monitorar continuamente o ambiente usando verificações de compatibilidade automatizadas com base nas práticas recomendadas da AWS e nos padrões do setor adotados pela organização.

Amazon GuardDuty: o Amazon GuardDuty é um serviço de detecção de ameaças gerenciado que monitora continuamente comportamentos mal-intencionados ou não autorizados para ajudar a proteger contas e workloads da AWS. O serviço monitora atividades como chamadas de API incomuns ou implantações potencialmente não autorizadas que indicam um possível comprometimento da conta. O GuardDuty também detecta instâncias possivelmente comprometidas ou reconhecimento por invasores.

O GuardDuty identifica suspeitas de invasão por meio de feeds integrados de inteligência de ameaças e usa machine learning para detectar anomalias nas atividades das contas e das workloads. Quando uma possível ameaça é detectada, o serviço entrega um alerta de segurança

detalhado ao console do GuardDuty e ao AWS CloudWatch Events. Dessa forma, os alertas ficam acionáveis e fáceis de integrar a sistemas existentes de gerenciamento de eventos e fluxos de trabalho.

Amazon Macie: o Amazon Macie é um serviço de segurança baseado em IA que ajuda a evitar a perda de dados descobrindo, classificando e protegendo automaticamente dados sigilosos armazenados na AWS. O Amazon Macie usa machine learning para reconhecer dados sigilosos, como informações de identificação pessoal (PII) ou propriedade intelectual, atribui um valor empresarial e proporciona visibilidade do local de armazenamento dos dados e de como são usados na organização. O Amazon Macie monitora continuamente atividades de acesso a dados para detectar anomalias e envia alertas quando detecta risco de acesso não autorizado ou vazamento acidental de dados.

Regras do AWS Config: uma regra do AWS Config representa as configurações preferenciais para um recurso e é avaliada com relação às alterações na configuração de recursos relevantes, conforme o registrado pelo AWS Config. Você pode ver os resultados da avaliação de uma regra em relação à configuração de um recurso em um painel. Usando o Config Rules, você pode avaliar sua conformidade geral e o status do risco do ponto de vista da configuração, visualizar tendências de conformidade durante um período e descobrir qual alteração da configuração fez com que um recurso ficasse fora de conformidade com uma regra.

AWS Trusted Advisor: o AWS Trusted Advisor é um recurso online que ajuda você a reduzir custos, aumentar a performance e aprimorar a segurança pela otimização do seu ambiente AWS. O Trusted Advisor fornece orientação em tempo real para ajudar você a provisionar os recursos seguindo as práticas recomendadas da AWS. O conjunto completo de verificações do Trusted Advisor, incluindo a integração com o CloudWatch Events, está disponível para os clientes do plano de suporte dos negócios e da empresa.

Amazon CloudWatch: o Amazon CloudWatch é um serviço de monitoramento para os recursos da Nuvem AWS e as aplicações que você executa na AWS. Você pode usar o Amazon CloudWatch para coletar e rastrear métricas, coletar e monitorar arquivos de log, definir alarmes e reagir automaticamente a alterações nos seus recursos da AWS. O Amazon CloudWatch pode monitorar recursos da AWS como instâncias do Amazon EC2, tabelas do Amazon DynamoDB e instâncias de banco de dados do Amazon RDS, além de métricas personalizadas geradas pelas suas aplicações e serviços, e quaisquer arquivos de log que suas aplicações gerarem. Você pode usar o Amazon CloudWatch para obter visibilidade sobre a utilização de recursos, a performance de aplicações e a integridade em todo o sistema. É possível usar esses insights para reagir rapidamente e manter sua aplicação em execução sem problemas.

AWS Inspector: o Amazon Inspector é um serviço automatizado de avaliação de segurança que ajuda a aprimorar a segurança e a conformidade das aplicações implantadas na AWS. O Amazon Inspector avalia automaticamente as aplicações para detectar vulnerabilidades ou desvios das práticas recomendadas. Depois de fazer uma avaliação, o Amazon Inspector gera uma lista detalhada dos problemas de segurança encontrados priorizados por nível de gravidade. Esses problemas podem ser revisados diretamente ou fazer parte de relatórios de avaliação detalhados que estão disponíveis no console ou na API do Amazon Inspector.

Amazon Detective: o Amazon Detective coleta automaticamente dados de log dos recursos da AWS e usa machine learning, análise estatística e teoria dos grafos para criar um conjunto de dados vinculado que permite conduzir facilmente investigações de segurança mais rápidas e eficientes. O Amazon Detective pode analisar trilhões de eventos de várias fontes dos dados, como logs de fluxo da Virtual Private Cloud (VPC), do AWS CloudTrail e do Amazon GuardDuty, e criar automaticamente uma visualização interativa e unificada de seus recursos e usuários e das interações entre eles ao longo do tempo. Com essa visualização unificada, você pode visualizar todos os detalhes e o contexto em um único local para identificar os motivos subjacentes das descobertas, detalhar as atividades históricas relevantes e determinar rapidamente a causa raiz.

Automação

AWS Lambda: o AWS Lambda é um serviço computacional sem servidor que executa seu código em resposta a eventos e gerencia automaticamente os recursos de computação subjacentes para você. Você pode usar o Lambda para estender outros serviços da AWS com lógica personalizada ou criar seus próprios serviços de back-end que operam na escala, na performance e na segurança da AWS. O Lambda executa o código em uma infraestrutura de computação altamente disponível e executa toda a administração dos recursos de computação para você. Isso inclui manutenção do servidor e do sistema operacional, provisionamento de capacidade e escalabilidade automática, implantação de código e patch de segurança, além de monitoramento e registro em log do código. Tudo o que você precisa fazer é fornecer o código.

AWS Step Functions: o AWS Step Functions permite coordenar os componentes de aplicações e microsserviços distribuídos usando fluxos de trabalho visuais. O Step Functions oferece um console gráfico para organizar e visualizar os componentes da aplicação como uma série de etapas. Isso simplifica a criação e a execução de aplicações com várias etapas. O Step Functions aciona e rastreia automaticamente todas as etapas e tenta executar novamente etapas que apresentaram falha para que a aplicação seja executada na ordem e da forma esperada.

O Step Functions registra em log o estado de cada etapa. Quando ocorre algum erro, você pode diagnosticar e depurar rapidamente os problemas. Você pode alterar e adicionar etapas sem escrever código, para que você possa desenvolver facilmente sua aplicação e inovar mais rapidamente. O AWS Step Functions faz parte da plataforma sem servidor da AWS e simplifica a orquestração de funções do AWS Lambda para aplicações sem servidor. Você também pode usar o Step Functions para orquestração de microsserviços usando recursos de computação como Amazon EC2 e Amazon ECS.

AWS Systems Manager: o AWS Systems Manager oferece visibilidade e controle da sua infraestrutura na AWS. O Systems Manager oferece uma interface do usuário unificada para que você possa visualizar dados operacionais de vários serviços da AWS e permite que você automatize tarefas operacionais em seus recursos da AWS. Com o Systems Manager, é possível agrupar recursos por aplicação, visualizar dados operacionais para monitoramento e resolução de problemas, além de agir nos grupos de recursos. O Systems Manager consegue manter instâncias em seu estado definido, realizar alterações de instância sob demanda, como atualizar aplicações ou executar scripts de shell e realizar outras tarefas de automação e aplicação de patches.

Armazenamento seguro

Amazon S3: o Amazon S3 é um armazenamento de objetos desenvolvido para armazenar e recuperar qualquer quantidade de dados de qualquer local. O serviço foi projetado para oferecer resiliência de 99,999999999% e armazena dados de milhões de aplicações usadas por líderes de mercado em todos os setores. O Amazon S3 oferece segurança abrangente e foi projetado para atender aos seus requisitos regulamentares. Ele proporciona aos clientes flexibilidade nos métodos que eles usam para gerenciar dados de otimização de custo, controle de acesso e conformidade. O Amazon S3 fornece funcionalidade de consulta no local, que permite executar análises avançadas diretamente nos dados em repouso no Amazon S3. O Amazon S3 é o serviço de armazenamento na nuvem que conta com o maior suporte no mercado, integrado à maior comunidade de soluções de terceiros e parceiros integradores de sistemas, bem como a outros serviços da AWS.

Amazon S3 Glacier: o Amazon S3 Glacier é um serviço de armazenamento na nuvem seguro, duradouro e de custo extremamente baixo para arquivamento de dados e backups de longa duração. Ele foi projetado para oferecer durabilidade de 99,999999999%, oferece segurança abrangente e foi projetado para atender aos seus requisitos regulamentares. O Amazon S3 Glacier oferece funcionalidade de consultas no local, o que permite executar análises avançadas diretamente em dados em repouso arquivados. Para manter os custos baixos, mas adequados para várias necessidades de recuperação, o Amazon S3 Glacier fornece três opções de acesso a arquivos, de alguns minutos a várias horas.

Personalizar

Os serviços e recursos acima mencionados não são uma lista completa. A AWS está continuamente adicionando novos recursos. Para obter mais informações, recomendamos que você leia as páginas O que há de novo na AWS e Segurança na Nuvem AWS. Além dos serviços de segurança que a AWS oferece como serviços de nuvem nativos, talvez você tenha interesse em criar seus próprios recursos com base nos serviços da AWS.

Embora seja recomendável habilitar um conjunto básico de serviços de segurança em suas contas, como o AWS CloudTrail, o Amazon GuardDuty e o Amazon Macie, talvez você queira estender esses recursos para obter valor adicional de seus ativos de log. Há várias ferramentas de parceiros disponíveis, como as listadas em nosso Programa de competência em segurança da APN. Você também pode escrever suas próprias consultas para pesquisar seus logs. Com o grande número de serviços gerenciados que a AWS oferece, isso nunca foi tão fácil. Há muitos serviços adicionais da AWS que podem ajudar você com investigações que estão fora do escopo deste documento, como o Amazon Athena, o Amazon OpenSearch Service, o Amazon QuickSight, o Amazon Machine Learning e o Amazon EMR.

Apêndice B: Código de exemplo

Evento de exemplo AWS CloudTrail

O exemplo a seguir mostra que um usuário do IAM chamado `Alice` usou a AWS CLI para chamar o Amazon EC2 `StopInstancesaction` usando o `ec2-stop-instances`.

```
{"Records": [{
    "eventVersion": "1.0",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2014-03-06T21:01:59Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "StopInstances",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "205.251.233.176",
    "userAgent": "ec2-api-tools 1.6.12.2",
    "requestParameters": {
        "instancesSet": {"items": [{"instanceId": "i-ebeaf9e2"}]},
        "force": false
    },
    "responseElements": {"instancesSet": {"items": [{
        "instanceId": "i-ebeaf9e2",
        "currentState": {
            "code": 64,
            "name": "stopping"
        },
        "previousState": {
            "code": 16,
            "name": "running"
        }
    }]}}
}]}
```

Exemplo do AWS CloudWatch Events

O exemplo do Amazon CloudWatch Events a seguir mostra que um usuário do AWS IAM denominado `jane-roe-test` foi publicamente exposto no `www.github.com` e pode ser utilizado indevidamente por usuários não autorizados.

```
{
  "check-name": "Exposed Access Keys",
  "check-item-detail": {
    "Case ID": "02648f3b-e18f-4019-8d68-ce25efe080ff",
    "Usage (USD per Day)": "0",
    "User Name (IAM or Root)": "jane-roe-test",
    "Deadline": "1440453299248",
    "Access Key ID": "AKIAIOSFODNN7EXAMPLE",
    "Time Updated": "1440021299248",
    "Fraud Type": "Exposed",
    "Location": "www.github.com"
  },
  "status": "ERROR",
  "resource_id": "",
  "uuid": "cce6d28f-e44b-4e61-aba1-5b4af96a0f59"
}
```

Exemplo de atividades de CLI de domínio

Os seguintes comandos da AWS CLI mostram um exemplo de resposta a um evento no domínio da infraestrutura. Este exemplo usa as APIs da AWS para realizar muitas das atividades iniciais de resposta a incidentes descritas neste documento.

```
# Anomaly detected on IP X.X.X.X. Capture that instance's metadata
> aws ec2 describe-instances --filters "Name=ip-address,Values=X.X.X.X"
```

```
# Protect that instance from accidental termination
> aws ec2 modify-instance-attribute --instance-id i-abcd1234 --attribute
 disableApiTermination --value true
```

```
# Switch the EC2 instance's Security Group to a restricted Security Group
> aws ec2 modify-instance-attribute --instance-id i-abcd1234 --groups sg-a1b2c3d4
```

```
# Detach from the Auto Scaling Group
> aws autoscaling detach-instances --instance-ids i-abcd1234 --auto-scaling-group-name
 web-asg
```

```
# Deregister the instance from the Elastic Load Balancer
> aws elb deregister-instances-from-load-balancer --instances i-abcd1234 --load-
balancer-name web-load-balancer
```

```
# Create an EBS snapshot
> aws ec2 create-snapshot --volume vol-12xxxx78 --description "ResponderName-Date-
REFERENCE-ID"
```

```
# Create a new EC2 instance from the Forensic Workstation AMI
> aws ec2 run-instances --image-id ami-4n6x4n6x --count 1 --instance-type c4.8xlarge --
key-name forensicPublicKey --security-group-ids sg-1a2b3c4d --subnet-id subnet-6e7f819e
```

```
# Create a new EBS volume copy from the EBS snapshot
> aws ec2 create-volume --region us-east-1 --availability-zone us-east-1a --snapshot-id
 snap-abcd1234 --volume-type io1 --iops 10000
```

```
# Attach the volume to the forensic workstation
> aws ec2 attach-volume --volume-id vol-1234abcd --instance-id i-new4n6x --device /dev/
sdf
```

```
# Create a security group rule to allow the new Forensic Workstation to communicate to
 the contaminated instance.
> aws ec2 authorize-security-group-ingress --group-id sg-a1b2c3d4 --protocol tcp --port
 0-65535 --source-group sg-1a2b3c4d
```

```
# Tag the contaminated instance with the ticket or reference ID
> aws ec2 create-tags -resources i-abcd1234 -tags
 Key=Environment,Value=Quarantine:REFERENCE-ID
```

Apêndice C: Exemplo de runbook

Este exemplo de runbook a seguir representa uma única entrada de um runbook maior. Este runbook não é oficial e é fornecido apenas como exemplo. Conforme você cria seus runbooks, cada um de seus cenários pode evoluir para itens maiores com diferentes começos e indicadores de comprometimento, mas todos têm resultados ou ações semelhantes que precisam ser executadas. Perceber essa mudança também pode criar outras situações para respostas melhores ou mais perspicazes.

Runbook de resposta a incidentes: uso básico

Objetivo

O objetivo deste runbook é fornecer orientações específicas sobre como gerenciar o uso da conta raiz da AWS. Este runbook não substitui uma estratégia detalhada de resposta a incidentes. Este runbook se concentra no ciclo de vida de resposta a incidentes:

- Estabelecer o controle.
- Determinar o impacto.
- Recuperar conforme necessário.
- Investigar a causa raiz.
- Aprimorar.

Os Indicadores de comprometimento (IOC), as etapas iniciais (interromper o sangramento) e os comandos detalhados da CLI necessários para executar essas etapas estão listados abaixo.

Pressuposições

- CLI configurada e instalada.
- O processo de relatório já está em vigor.
- O Trusted Advisor está ativo.
- O Security Hub está ativo.

Indicadores de comprometimento

- Atividade anormal para a conta.
  - Criação de usuários do IAM.
  - O CloudTrail foi desativado.
  - O Cloudwatch foi desligado.
  - SNS pausado.
  - Step Functions pausado.
- Lançamento de AMIs novas ou inesperadas.
- Alterações nos contatos da conta.

Etapas de correção: estabelecer o controle

A documentação da AWS para uma possível conta comprometida destaca as tarefas específicas listadas abaixo. A documentação de uma possível conta comprometida pode ser encontrada em: O que eu faço se notar uma atividade não autorizada na minha conta da AWS?

1. Entre em contato com AWS Support e o TAM o mais rápido possível.
2. Altere e alterne a senha raiz e adicione um dispositivo com MFA associado à raiz.
3. Alterne senhas, chaves de acesso/secretas e comandos da CLI relevantes para as etapas de correção.
4. Revise as ações realizadas pelo usuário raiz.
5. Abra os runbooks para essas ações.
6. Encerre o incidente.
7. Analise o incidente e entenda o que aconteceu.
8. Corrija os problemas subjacentes, implemente melhorias e atualize o runbook conforme necessário.

Outras ações: determinar o impacto

Revise os itens criados e as chamadas mutantes. Pode haver itens que foram criados para permitir o acesso no futuro. Alguns fatores a serem observados:

- Funções entre contas do IAM.

- Usuários do IAM.
- Buckets do S3.
- Instâncias do EC2.
- [Sua aplicação e sua infraestrutura conduzirão essa lista.]

Avisos

Os clientes são responsáveis por fazer sua própria avaliação independente das informações neste documento. Este documento é: (a) fornecido 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 cria nenhum compromisso ou garantia da AWS e suas afiliadas, fornecedores ou licenciadores. Os produtos ou serviços da AWS são fornecidos no “estado em que se encontram”, sem garantias, declarações ou condições de qualquer tipo, explícitas ou implícitas. As responsabilidades e obrigações da AWS com seus clientes são regidas por contratos da AWS, e este documento não modifica nem faz parte de nenhum contrato entre a AWS e seus clientes.

© 2020 Amazon Web Services, Inc. ou suas afiliadas. Todos os direitos reservados.