AWS Security Incident ResponseGuia do usuário do

Versão April 29, 2026

AWS Security Incident ResponseGuia do usuário do:

Table of Contents

O que é o AWS Security Incident Response?

A AWS Security Incident Response ajuda você a se preparar rapidamente, responder de forma eficaz e receber orientações para auxiliar na recuperação de incidentes de segurança. Isso inclui incidentes como aquisição de contas, violações de dados e ataques de ransomware.

A AWS Security Incident Response realiza a triagem das descobertas de ameaças, escala os eventos de segurança e gerencia os casos que requerem sua atenção imediata. Além disso, você tem acesso à engenheiros do Security Incident Response, que investigarão os recursos impactados.

> **Note**
>
> Não há garantia de que os recursos impactados possam ser recuperados. É recomendável que você estabeleça e mantenha backups dos recursos cuja perda possa impactar os requisitos do seu negócio.

A AWS Security Incident Response atua em conjunto com outros serviços de Detecção e Resposta a Incidentes da AWS, orientando você durante todo o ciclo de vida do incidente, desde a detecção até a recuperação.

Conteúdo

Configurações compatíveis

A AWS Security Incident Response fornece suporte para as seguintes configurações de idioma e de região:

- Idioma: a AWS Security Incident Response oferece suporte dedicado em inglês. O suporte em japonês é limitado ao horário comercial do Japão (correspondente ao horário padrão do Japão) e conta com restrições específicas:

- > **Note**
  >
  > O suporte em japonês é fornecido em caráter de melhor esforço durante o horário comercial (que compreende das 9h às 17h, de segunda a sexta-feira, exceto feriados).

- Regiões da AWS com suporte:

  A AWS Security Incident Response está disponível em um subconjunto de Regiões da AWS. Nessas regiões com suporte, você pode criar uma associação, abrir e visualizar casos, além de acessar o painel.

  - Leste dos EUA (Ohio)
  - Oeste dos EUA (Oregon)
  - Leste dos EUA (Virgínia)
  - Europa (Frankfurt)
  - Europa (Irlanda)
  - Europa (Londres)
  - Europa (Milão)
  - Europe (Paris)
  - Europa (Espanha)
  - Europa (Estocolmo)
  - Europa (Zurique)
  - Ásia-Pacífico (Hong Kong)
  - Ásia-Pacífico (Hyderabad)
  - Ásia-Pacífico (Jacarta)
  - Ásia-Pacífico (Melbourne)
  - Ásia-Pacífico (Mumbai)
  - Ásia-Pacífico (Seul)
  - Ásia-Pacífico (Singapura)
  - Ásia-Pacífico (Sydney)
  - Ásia-Pacífico (Tóquio)
  - Canadá (Central)
  - Oriente Médio (Bahrein)
  - Oriente Médio (Emirados Árabes Unidos)

- América do Sul (São Paulo)
- África (Cidade do Cabo)

Quando você habilita o recurso de monitoramento e investigação, a AWS Security Incident Response passa a monitorar as descobertas do Amazon GuardDuty em todas as Regiões da AWS comerciais e ativas. Como uma prática recomendada de segurança, a AWS recomenda habilitar o GuardDuty em todas as regiões da AWS com suporte. Essa configuração permite que o GuardDuty realize a geração de descobertas relacionadas a atividades suspeitas ou não autorizadas, mesmo em Regiões da AWS nas quais você não conta com recursos implantados ativamente. Ao fazer isso, você fortalece sua postura geral de segurança e mantém uma cobertura abrangente de detecção de ameaças em todo o seu ambiente da AWS.

> **Note**
>
> O Amazon GuardDuty gera descobertas para as regiões configuradas. Se você optar por não habilitar o serviço em uma região específica, os alertas não estarão disponíveis.

Resumo dos recursos

Monitoramento e investigação

A AWS Security Incident Response revisa rapidamente os alertas de ameaça de segurança do Amazon GuardDuty e de integrações de terceiros com o AWS Security Hub CSPM, reduzindo a quantidade de alertas que sua equipe precisa analisar. O serviço configura regras de supressão de acordo com o ambiente para reduzir os alertas de baixa prioridade que requerem triagem e análise.

Simplificação da resposta a incidentes

Encaminhe e execute a resposta a incidentes em poucos minutos, envolvendo as partes interessadas, os serviços de entidades externas e as ferramentas relevantes.

Soluções de segurança de autoatendimento

A AWS Security Incident Response disponibiliza APIs que permitem a integração e o desenvolvimento de soluções de segurança personalizadas.

Painel para visibilidade

Monitore e avalie a prontidão para a resposta a incidentes.

Postura de segurança

Acesse as práticas recomendadas da AWS e as ferramentas validadas para avaliação da segurança e investigação rápida da resposta a incidentes.

Assistência prioritária

Entre em contato com os engenheiros de Security Incident Response para investigar, conter e obter orientação sobre modos de realizar a recuperação após os eventos de segurança.

Preparação e prontidão

Implemente notificações simplificadas ao configurar sua equipe de Resposta a Incidentes para acionar alertas a indivíduos ou grupos designados, com políticas de permissão definidas previamente.

Conceitos e terminologia

Os termos e os conceitos apresentados a seguir são importantes para a compreensão do serviço de AWS Security Incident Response e de seu funcionamento.

Escopo: a AWS Security Incident Response está alinhada com o guia NIST 800-61 Computer Security Incident Handling Guide do National Institute of Standards and Technology (NIST), fornecendo uma abordagem consistente para o gerenciamento de eventos de segurança, conforme as práticas recomendadas do setor.

Análise: o processo de investigação e exame detalhados de um evento de segurança para compreender o escopo, o impacto e a causa-raiz.

Portal do serviço AWS Security Incident Response: um portal de autoatendimento para você iniciar e gerenciar casos relacionados aos eventos de segurança. A comunicação contínua e a geração de relatórios são facilitadas por meio do sistema de emissão de tíquetes, notificações automatizadas e interação direta com a equipe do serviço.

Comunicação: o diálogo contínuo e o compartilhamento de informações entre a equipe da Resposta a Incidentes de Segurança da AWS e o cliente durante o processo de resposta a incidentes.

Contenção, erradicação e recuperação: a prevenção de atividades não autorizadas adicionais (contenção), em conjunto com a remoção dos recursos não autorizados e da vulnerabilidade original (erradicação), e a recuperação dos recursos para o retorno às operações normais.

Melhoria contínua: a AWS Security Incident Response incorpora comentários e lições aprendidas de interações anteriores para aprimorar suas funcionalidades de detecção, processos investigativos e ações de remediação. Além disso, a AWS Security Incident Response se mantém atualizada em relação às mais recentes ameaças de segurança e práticas recomendadas para enfrentar os desafios de segurança em constante evolução.

Evento de segurança cibernética: uma ação que usa um sistema ou uma rede de informação para provocar efeitos adversos ao sistema, à rede ou às informações nele presentes.

Incidente de segurança cibernética: uma violação ou ameaça iminente de violação das políticas de segurança de computadores, políticas de uso aceitável ou práticas padrão de segurança.

Engenheiros do Security Incident Response: um grupo que fornece suporte durante os eventos de segurança ativos. Nos casos com o suporte da AWS, o grupo são os engenheiros do Security Incident Response.

Fluxo de trabalho de resposta a incidentes: a sequência definida de etapas e de atividades envolvidas no gerenciamento de ponta a ponta de um evento de segurança, seguindo as diretrizes do padrão NIST 800-61.

Ferramentas de investigação: as ferramentas e os perfis vinculados ao serviço da AWS Security Incident Response usados para analisar a integridade operacional da sua conta e dos recursos.

Lições aprendidas: o processo de análise e de documentação da resposta a um evento de segurança para identificar áreas de melhoria e orientar o planejamento futuro de resposta a incidentes.

Monitoramento e investigação: a AWS Security Incident Response analisa rapidamente os alertas de segurança do Amazon GuardDuty, destacando os alertas mais relevantes que precisam ser analisados por sua equipe. O serviço configura regras de supressão com base nas especificidades do seu ambiente para evitar alertas desnecessários.

Preparação: as atividades realizadas para preparar uma organização para a resposta e para o gerenciamento de eventos de segurança de maneira eficaz, como a elaboração de planos de resposta a incidentes e a realização de testes de procedimentos.

Elaboração de relatórios e comunicação: os procedimentos usados para fornecer a você as informações durante todo o processo de resposta a incidentes, incluindo notificações automatizadas, pontes de conferência e fornecimento de artefatos de investigação. A AWS Security Incident Response disponibiliza um painel único e centralizado no Console de gerenciamento da AWS para gerenciar todos os esforços relacionados ao serviço de AWS Security Incident Response.

Inteligência gerada por respondente: inclui indicadores de comprometimento; táticas, técnicas e procedimentos, e os padrões associados identificados pelas investigações da AWS.

Conhecimento especializado em eventos de segurança: os conhecimentos especializados e as habilidades necessárias para responder e gerenciar de forma eficaz os eventos de segurança, especialmente no contexto da Nuvem AWS.

Modelo de responsabilidade compartilhada: a divisão das responsabilidades de segurança entre a AWS e o cliente, no qual a AWS é responsável pela segurança da nuvem e o cliente é responsável pela segurança na nuvem.

Inteligência de ameaças: os feeds de dados internos e externos que contêm detalhes sobre as atividades não autorizadas, com o objetivo de ajudar na identificação e na resposta a ameaças de segurança em constante evolução.

Sistema de emissão de tíquetes: uma plataforma dedicada de gerenciamento de casos que permite a integração e o gerenciamento de casos de eventos de segurança, a adição de anexos e o acompanhamento do ciclo de vida da resposta ao incidente.

Triagem: a avaliação inicial e a priorização de um evento de segurança com o objetivo de determinar a resposta adequada e as próximas etapas.

Fluxo de trabalho: a sequência definida de etapas e de atividades envolvidas no gerenciamento de ponta a ponta de um evento de segurança.

Introdução

Conceitos básicos do AWS Security Incident Response

Conteúdo

Guia de integração

O AWS Security Incident Response ajuda você a se preparar, responder e se recuperar de eventos de segurança, como aquisição de contas, violações de dados e ataques de ransomware. O serviço realiza a triagem das descobertas do Amazon GuardDuty e do AWS Security Hub CSPM, escala eventos de segurança e gerencia os casos que precisam da sua atenção. Você também tem acesso à equipe de Resposta a Incidentes de Segurança (SIRT) da AWS, que investiga os recursos afetados e fornece orientação durante todo o ciclo de vida do incidente.

Para obter uma visão geral completa do serviço, consulte O que é o AWS Security Incident Response?

Prepare-se para a integração

Recomendamos o uso de uma abordagem de prova de conceito (POC) ao implementar o AWS Security Incident Response. Antes da implantação, conclua as etapas de preparação a seguir com suas equipes internas e sua equipe de contas da AWS.

- Identifique as principais partes interessadas: mapeie os tomadores de decisão de resposta a incidentes em sua organização. Seu envolvimento em atualizações de políticas e alterações de processos é essencial para uma implantação com êxito.
- Valide as fontes de descobertas: confirme se todas as fontes de descobertas de segurança estão configuradas e implantadas adequadamente. O GuardDuty e o Security Hub CSPM são entradas essenciais para a tecnologia de triagem automática do serviço.

- Determine o escopo da conta: decida se o AWS Security Incident Response abrangerá toda a sua organização da AWS ou unidades organizacionais (UOs) específicas. A definição antecipada desse escopo torna a implementação e o escalonamento mais simples.
- Estabeleça protocolos de escalonamento: atualize seus procedimentos de escalonamento existentes para incluir o AWS Security Incident Response. Comunique os protocolos atualizados a todas as partes interessadas e à equipe de resposta.
- Colete pontos de contato e informações críticas: a coleta antecipada de metadados do cliente garante uma experiência de integração tranquila e permite a comunicação oportuna da SIRT da AWS quando necessário. Consulte Apêndice A: pontos de contato e informações críticas para obter as informações necessárias.

Pré-requisitos de integração

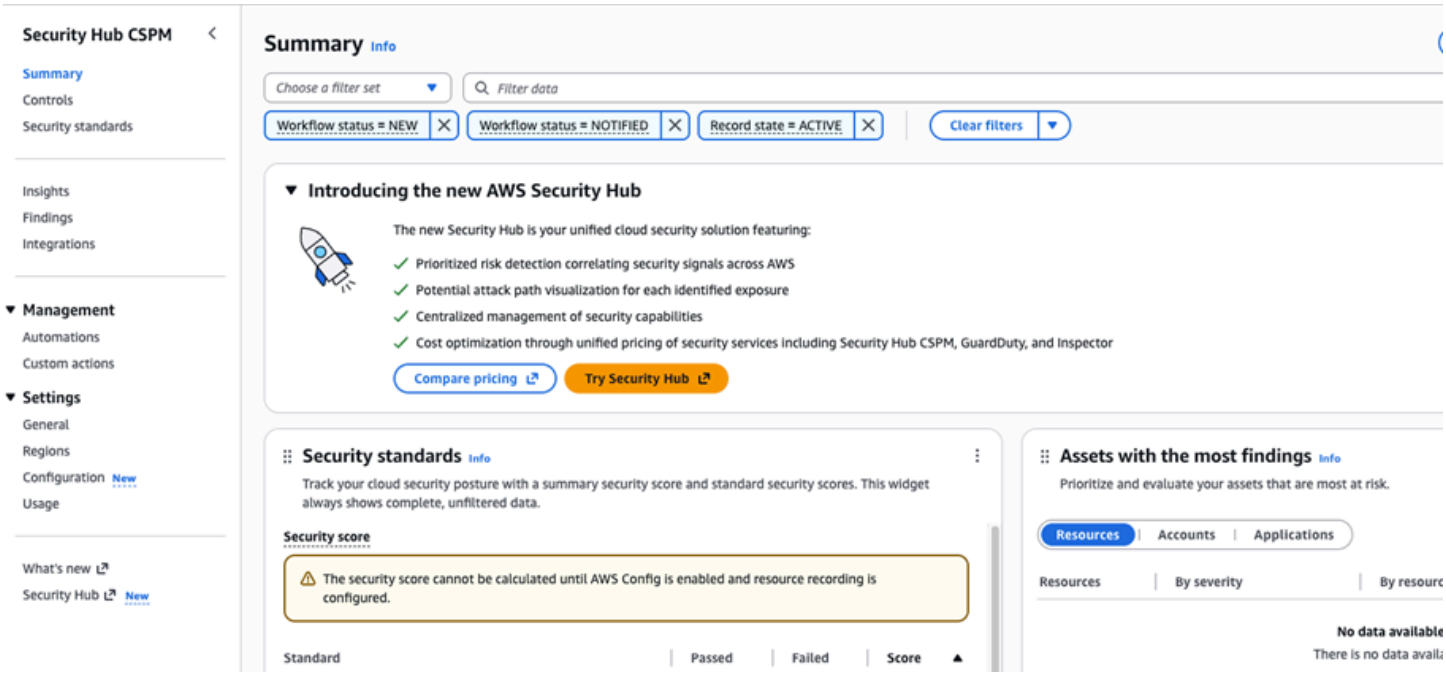
O único pré-requisito necessário é habilitar o AWS Organizations com Todos os atributos habilitados. O faturamento consolidado por si só não é suficiente.

Embora não seja obrigatório, é altamente recomendável habilitar o Amazon GuardDuty e o AWS Security Hub CSPM em todas as contas e ativar as Regiões da AWS para obter o máximo valor do AWS Security Incident Response.

- GuardDuty e AWS Security Incident Response
- Práticas recomendadas do GuardDuty

Integração do EDR de terceiros

O Security Hub CSPM pode ingerir descobertas de fornecedores terceirizados de detecção e resposta de endpoints (EDR). Quando ingeridas, essas descobertas são submetidas à triagem automática do AWS Security Incident Response para a criação proativa de casos. Para configurar uma integração do EDR de terceiros, siga as etapas na documentação de integrações do Security Hub CSPM.



> **Note**
>
> Você não precisa habilitar os padrões ou controles do Security Hub CSPM. Somente as integrações do fornecedor são necessárias para o AWS Security Incident Response ingerir descobertas de terceiros.

Preços: as primeiras 10.000 descobertas do Security Hub CSPM são gratuitas. Depois disso, o custo é de USD 0,00003 por descoberta. Para obter mais informações, consulte Preço do Security Hub CSPM.

Etapa 1: habilitar AWS Security Incident Response

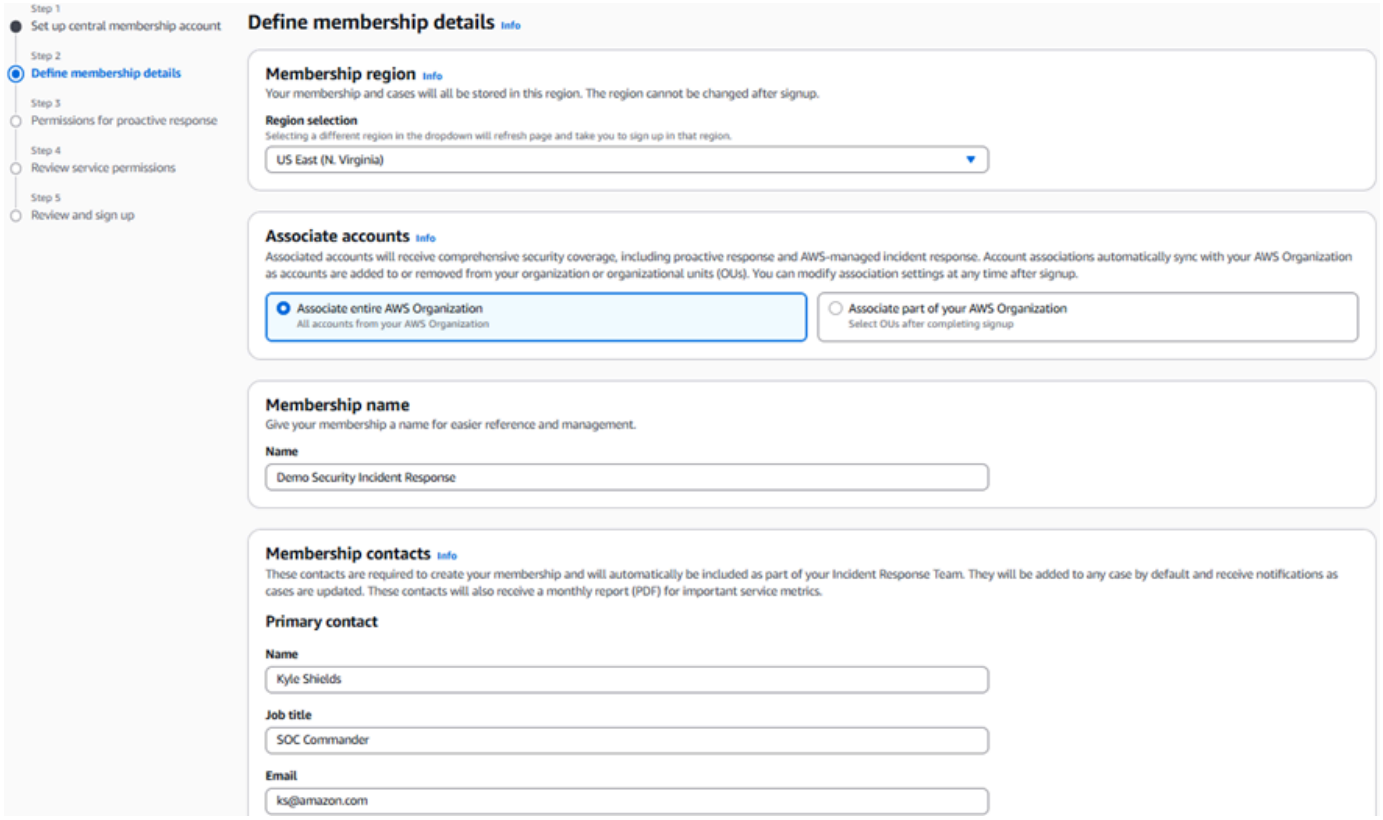
O processo de integração leva aproximadamente de 10 a 15 minutos por organização da AWS. Para ver uma demonstração, assista ao Vídeo de introdução na documentação do serviço.

Como habilitar o AWS Security Incident Response

1. Faça login no Console de Gerenciamento da AWS usando sua conta gerencial.
2. Abra o console do AWS Security Incident Response e clique em Cadastrar.

3. Designe uma conta de ferramenta de segurança como administrador delegado.

   - Para obter orientação, consulte Security Reference Architecture nas Recomendações da AWS e Administrador delegado.

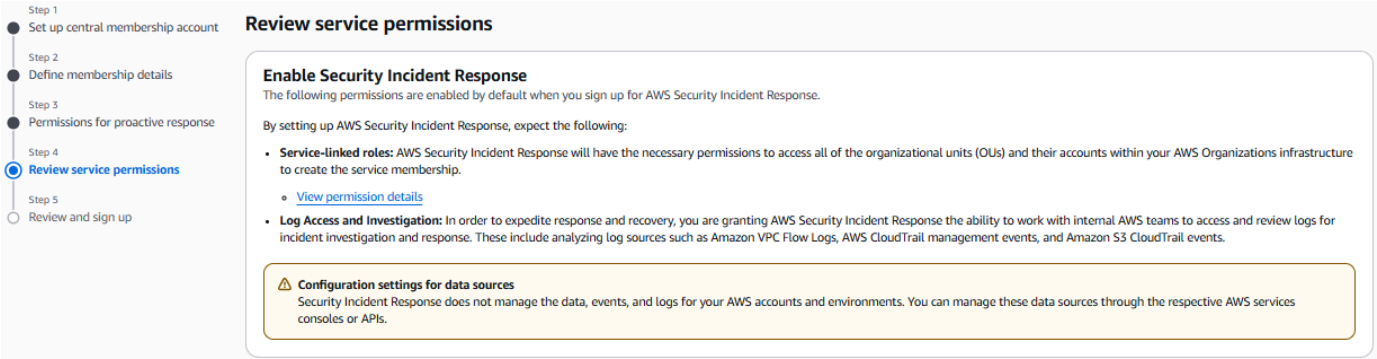


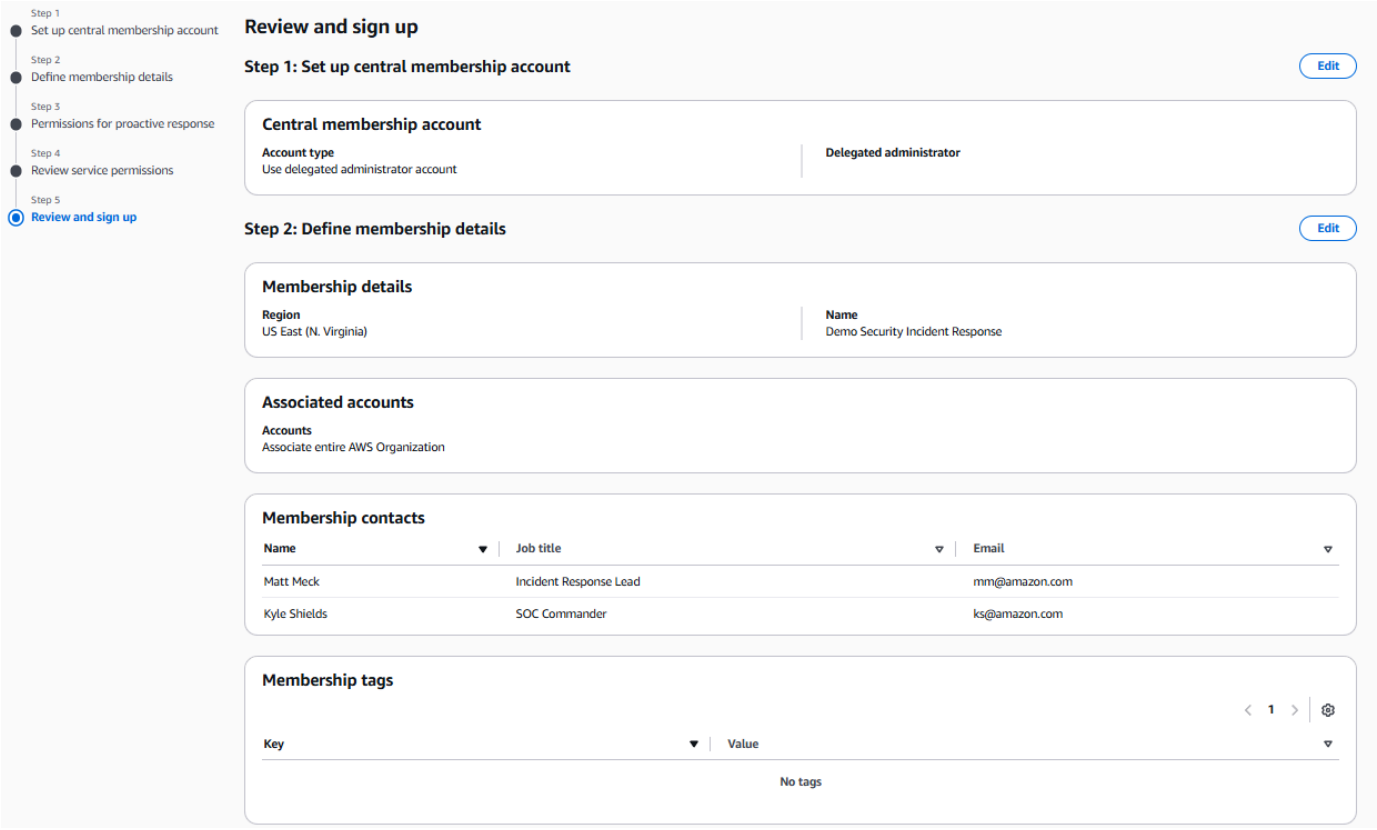
4. Faça login na conta do administrador delegado.

5. Insira os detalhes da associação e associe as contas relevantes.
6. Em Escopo da conta, escolha habilitar o AWS Security Incident Response para toda a sua organização da AWS ou para UOs específicas. Você pode selecionar a cobertura no nível da UO, mas não no nível da conta individual.
7. Para Resposta proativa, confirme se a configuração está habilitada. A resposta proativa é ativada por padrão e cria um perfil vinculado ao serviço que permite à SIRT da AWS ingerir descobertas do GuardDuty e abrir casos de investigação proativa quando ameaças são detectadas. Para obter mais informações, consulte Resposta proativa.

> **Important**
>
> O perfil vinculado ao serviço não é implantado automaticamente na conta gerencial. Você deve configurá-lo manualmente para obter uma cobertura completa. Para instruções, consulte Configuração de fluxos de trabalho de resposta proativa e de triagem de alertas.

8. (Opcional) Escolha pré-autorizar a SIRT da AWS ao realizar ações de contenção em seu nome durante incidentes ativos. As ações de contenção compatíveis incluem runbooks para buckets comprometidos do S3, instâncias do EC2 e entidades principais do IAM. Se você pular essa etapa, a SIRT fornecerá orientação manual durante as investigações. Para obter mais informações, consulte Ações de contenção.
9. Revise as permissões do serviço e a configuração de integração e escolha Cadastrar.



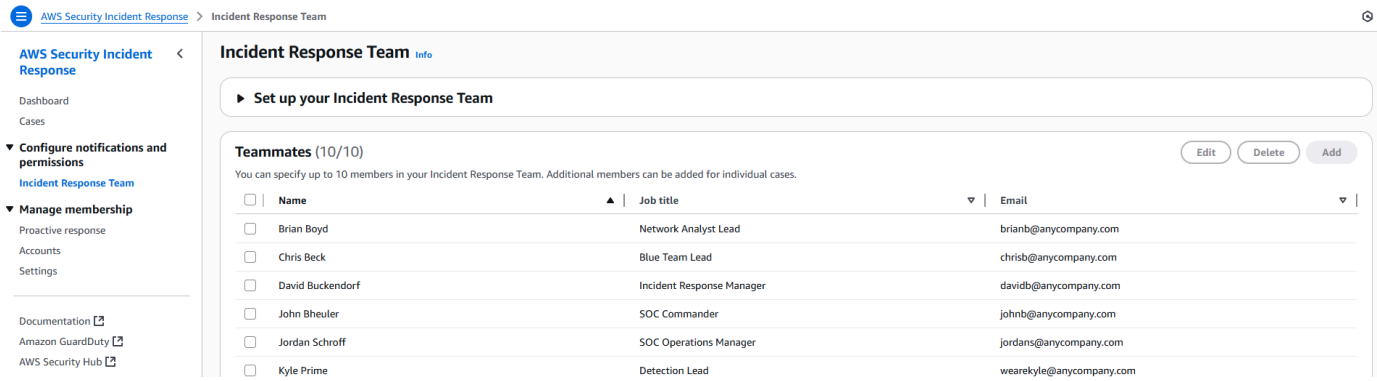


Etapa 2: configure sua equipe de resposta a incidentes

Depois de concluir a implantação, configure sua equipe de resposta a incidentes para garantir a notificação e a escalação adequadas durante eventos de segurança.

Para configurar sua equipe de resposta a incidentes

1. Abra o AWS Security Incident Response Console.
2. No painel de navegação à esquerda, selecione Equipe de resposta a incidentes.
3. Adicione até 10 membros da equipe. Para cada membro, forneça o nome, cargo e endereço de e-mail.



Sua equipe pode incluir liderança organizacional, assessoria jurídica, parceiros gerenciados de detecção e resposta (MDR), engenheiros de nuvem e outras partes interessadas que precisam ser notificadas durante eventos de segurança.

Etapa 3: entenda os tipos e gerenciamento de casos

O AWS Security Incident Response fornece dois tipos de casos para gerenciar eventos de segurança: casos proativos que são criados automaticamente quando ameaças são detectadas e casos reativos que você cria quando precisa da ajuda da SIRT da AWS. Você também pode conceder visibilidade do caso a partes externas, como parceiros, equipes jurídicas ou especialistas no assunto.

Os seguintes tópicos são abordados nesta seção:

- Casos proativos
- Casos reativos
- Observadores

Casos proativos

O atributo de triagem automática analisa continuamente alertas de alto volume para filtrar ruídos e focar ameaças críticas de alto impacto. Quando uma ameaça potencial é detectada, o sistema encaminha a descoberta para um responsável da SIRT da AWS para investigação. Se a descoberta for confirmada como uma ameaça genuína, um caso proativo será criado no portal de gerenciamento de casos e todas as partes interessadas configuradas serão notificadas automaticamente.

Nenhuma configuração manual é necessária para casos proativos além de habilitar o GuardDuty e integrar soluções de segurança de terceiros com o Security Hub CSPM. O serviço também se

integra a um agente investigativo de IA que correlaciona dados de várias fontes para acelerar as investigações. Esse recurso está disponível para casos reativos com suporte da AWS.

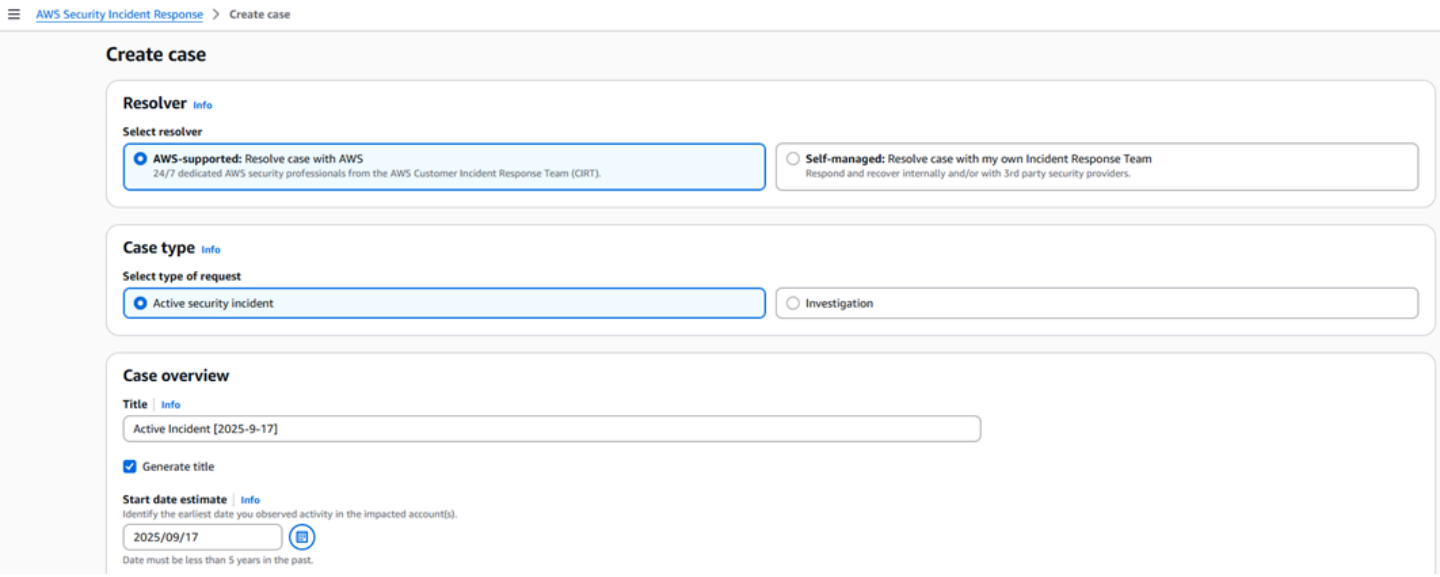
Casos reativos

O AWS Security Incident Response fornece um portal de gerenciamento de casos baseado em assinatura, no qual sua organização trabalha diretamente com a SIRT da AWS. AWS A SIRT auxilia em investigações de segurança e incidentes ativos com um objetivo de nível de serviço (SLO) de 15 minutos. Não há limite para o número de casos reativos que você pode abrir.

Como criar um caso

1. Abra o AWS Security Incident Response Console.
2. Selecione Casos e, depois, Criar caso.
3. Escolha um tipo de caso:
    - Com suporte da AWS: escalado diretamente para a SIRT da AWS para investigação e orientação (SLO de 15 minutos).
    - Autogerenciado: mantido internamente em sua organização para rastreamento e documentação.
4. Preencha todos os campos relevantes. Inclua o máximo de detalhes possível para dar suporte a uma investigação eficiente.

Ambos os tipos de casos usam os mesmos campos de dados. Você pode escalar um caso autogerenciado para a SIRT da AWS a qualquer momento, selecionando Obter ajuda da AWS no canto superior direito do caso.



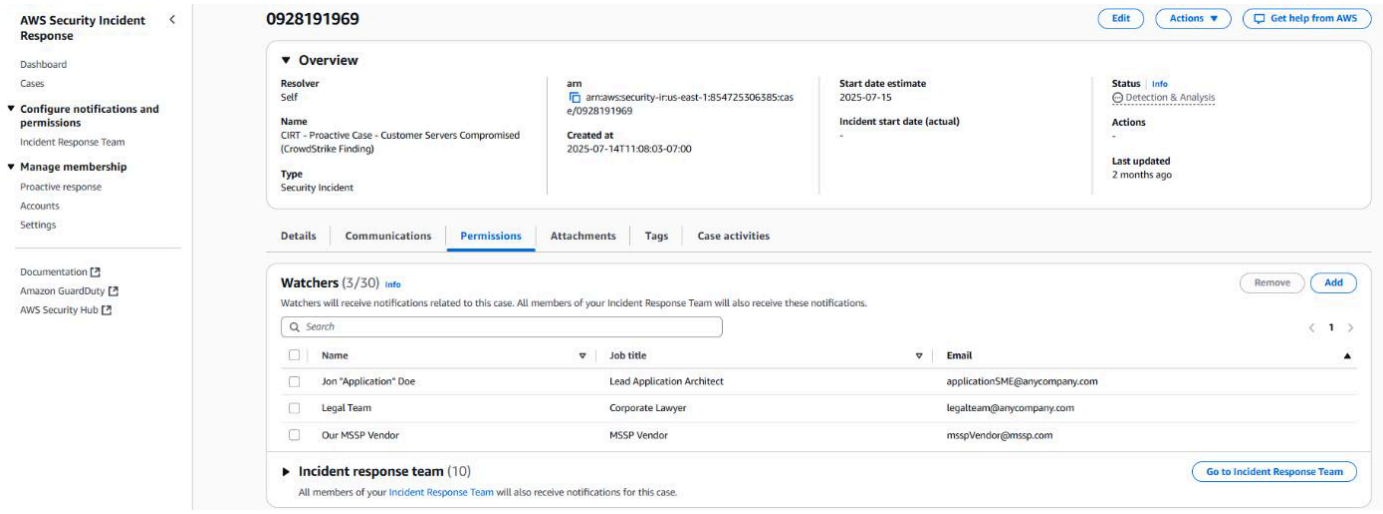
Para obter instruções detalhadas, consulte Criar um caso.

Observadores

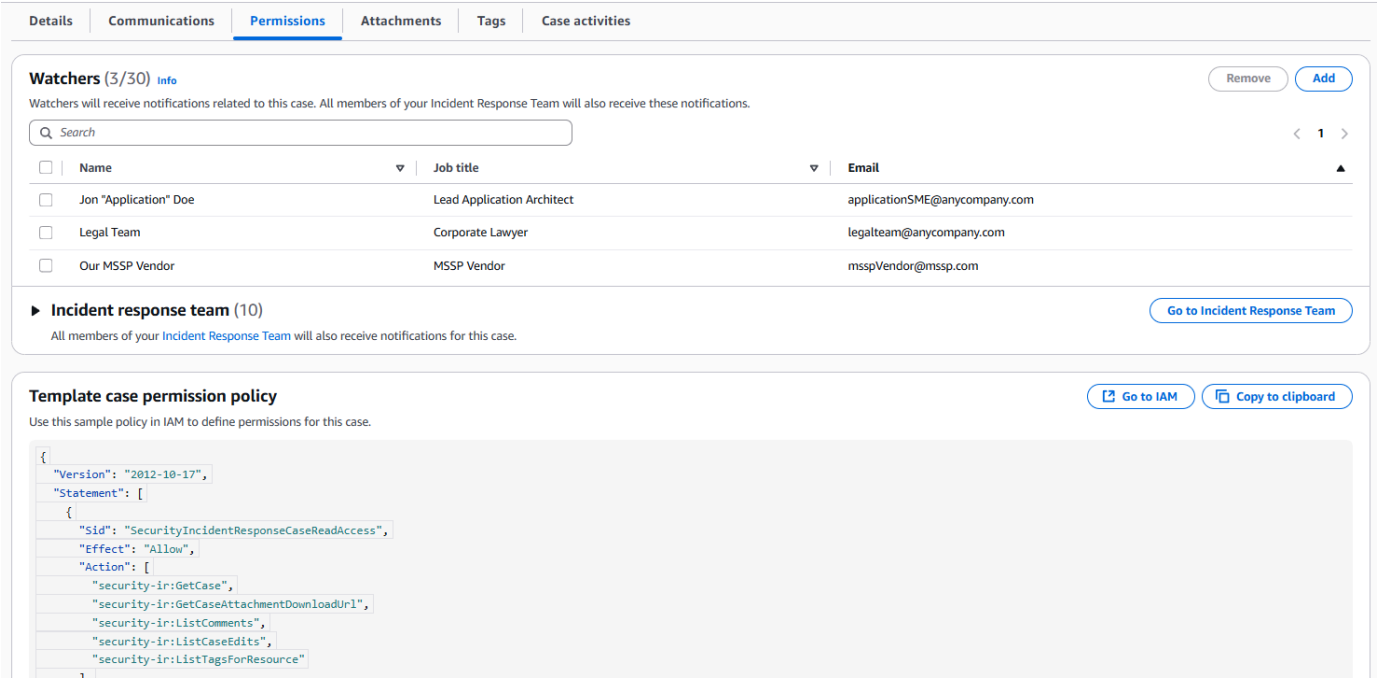
Você pode conceder visibilidade do caso a partes externas usando observadores ou políticas do IAM. Essas opções permitem que você inclua parceiros, equipes de risco e conformidade, consultores jurídicos ou especialistas no assunto em suas investigações. Os observadores recebem notificações para todas as atualizações de um caso específico. As políticas do IAM fornecem acesso direto ao console com permissões de privilégios mínimos.

Para adicionar um observador a um caso

1. Abra o console do AWS Security Incident Response e selecione Casos.
2. Abra o caso que você deseja compartilhar.
3. Selecione a guia Permissões e escolha Adicionar.



4. Copie a política pré-preenchida do IAM e aplique-a aos perfis ou usuários apropriados do IAM.



> **Note**
>
> Cada caso inclui uma política do IAM pré-preenchida com o escopo desse caso específico. Isso mantém o privilégio mínimo de acesso para parceiros terceirizados de MDR e equipes de investigação.

Etapa 4: integre com suas ferramentas existentes

O AWS Security Incident Response se integra às suas ferramentas e fluxos de trabalho de segurança existentes para agilizar as operações de resposta a incidentes. Você pode configurar a ingestão automática de descoberta do GuardDuty, configurar fluxos de trabalho orientados por eventos com o EventBridge, conectar-se a plataformas de ITSM, como Jira e ServiceNow, e colaborar com seus fornecedores de SIEM e MDR.

Os seguintes tópicos são abordados nesta seção:

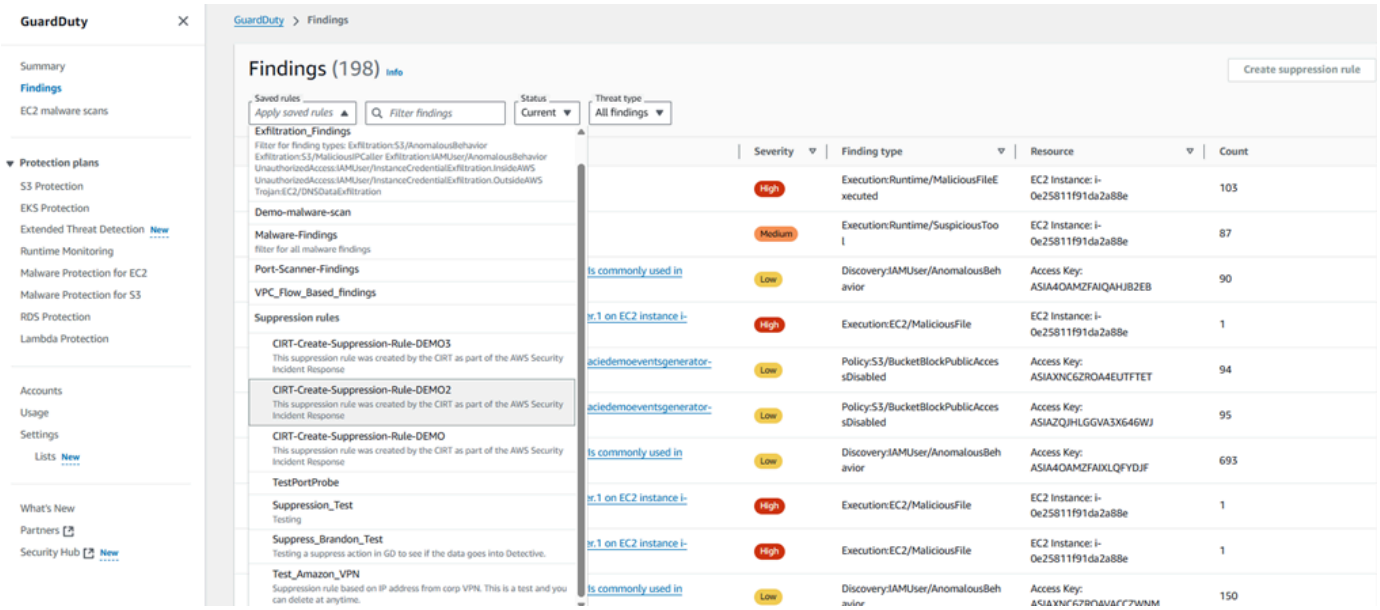
- Descobertas e regras de supressão do GuardDuty
- Amazon EventBridge
- Integrações com Jira, Slack e ServiceNow
- SIEM e ferramentas externas

Descobertas e regras de supressão do GuardDuty

O AWS Security Incident Response ingere, faz a triagem e responde automaticamente às descobertas do GuardDuty e do Security Hub CSPM provenientes de integrações com terceiros. A tecnologia de triagem automática trata a análise como uma camada adicional de detecção e análise. O serviço pode criar regras de arquivamento automático no GuardDuty depois de escalar uma descoberta que é um falso positivo. As equipes de resposta sempre discutirão isso com você antes de implementar a regra.

Para revisar as regras de supressão do GuardDuty

1. Abra o console do GuardDuty.



2. Escolha Descobertas.
3. No painel de navegação, escolha Regras de supressão. A página Regras de supressão exibe uma lista de todas as regras de supressão da sua conta.
4. Para revisar ou alterar as configurações de uma regra, escolha a regra e depois escolha Atualizar regra de supressão no menu Ações.

> **Note**
>
> As organizações que usam a tecnologia SIEM reduzirão os volumes de descoberta do GuardDuty ao longo do tempo, o que melhora a eficiência da AWS Security Incident Response e o desempenho do SIEM.

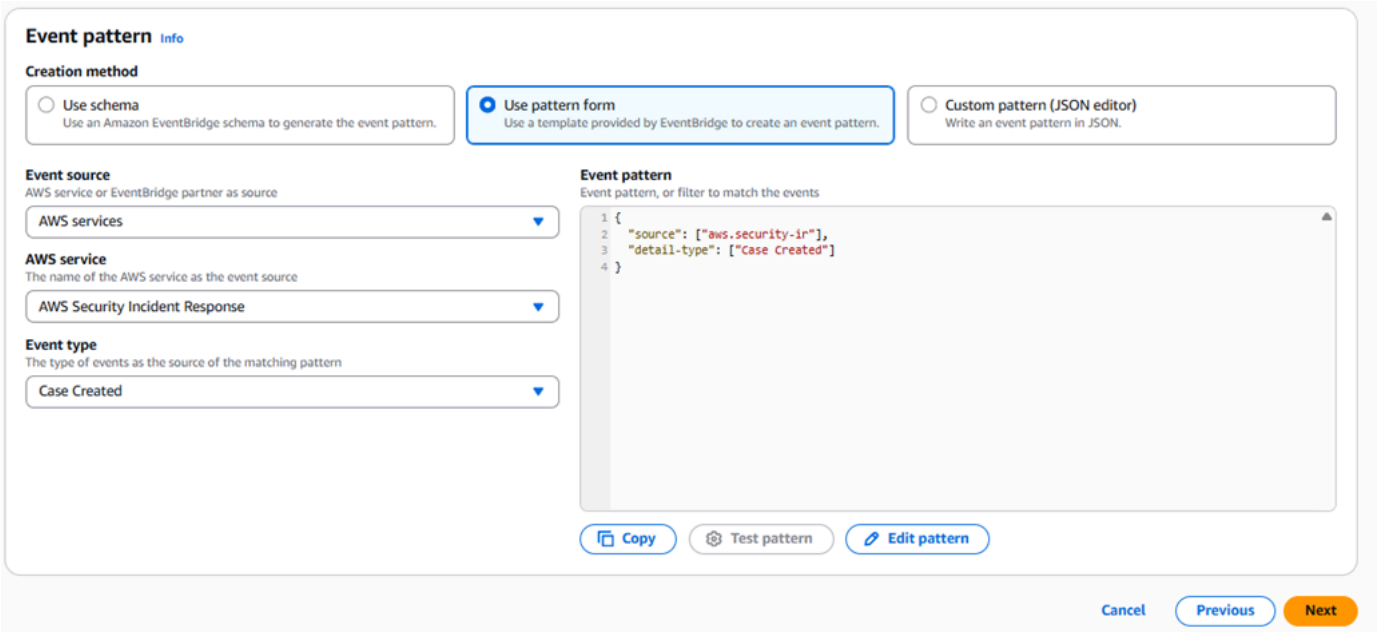
Amazon EventBridge

O Amazon EventBridge permite fluxos de trabalho orientados por eventos para o AWS Security Incident Response. Você pode configurar a atividade do caso para acionar serviços de downstream da AWS (Amazon Simple Notification Service, AWS Lambda, Amazon Simple Queue Service, AWS Step Functions) ou ferramentas externas, como Jira, ServiceNow, Slack e PagerDuty.

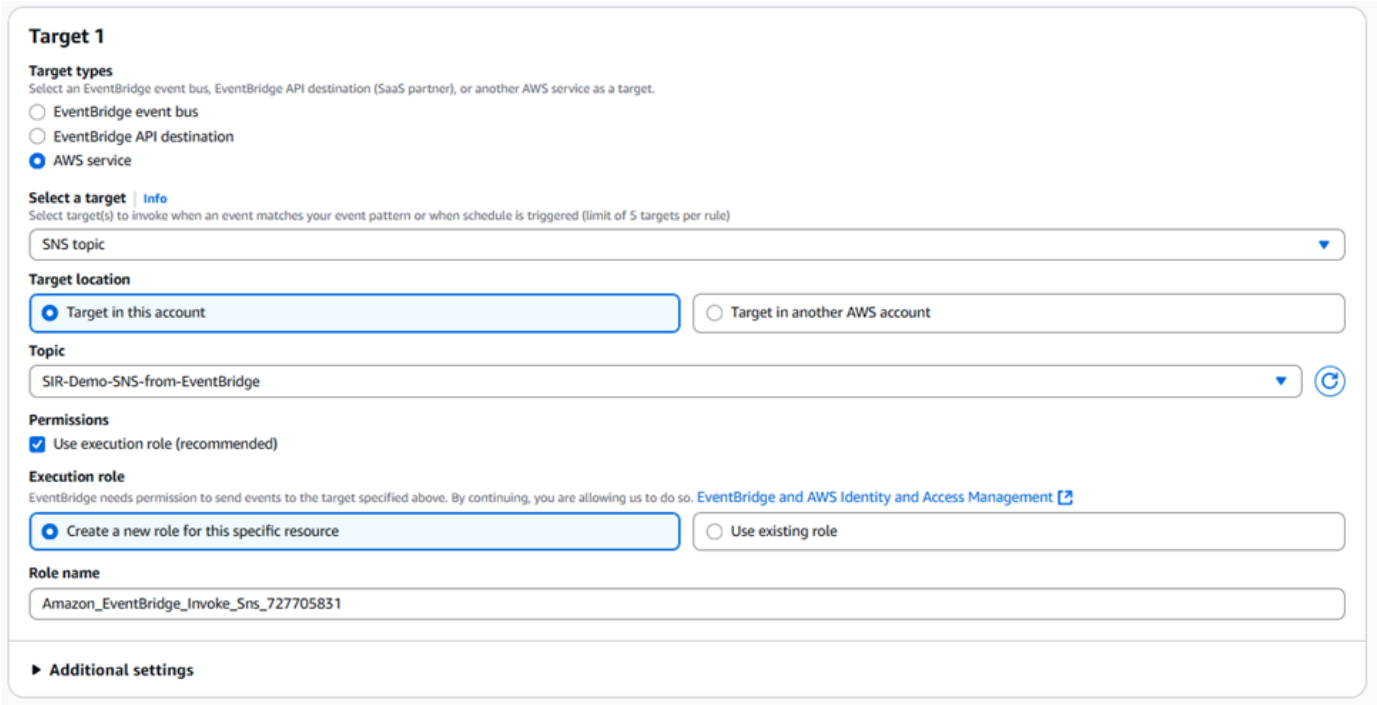
Para configurar uma regras do EventBridge para o AWS Security Incident Response

1. Faça login na conta do administrador delegado no AWS Security Incident Response.
2. Abra o console do EventBridge.

3. No painel de navegação, em Barramentos, selecione Regras.
4. Escolha Criar regra, preencha os detalhes da regra e selecione Avançar.
5. Em Serviço da AWS, selecione o AWS Security Incident Response no menu suspenso.
6. Em Tipo de evento, selecione a chamada de API que você deseja corresponder. É possível editar o padrão manualmente para incluir vários eventos.
7. Escolha Próximo.

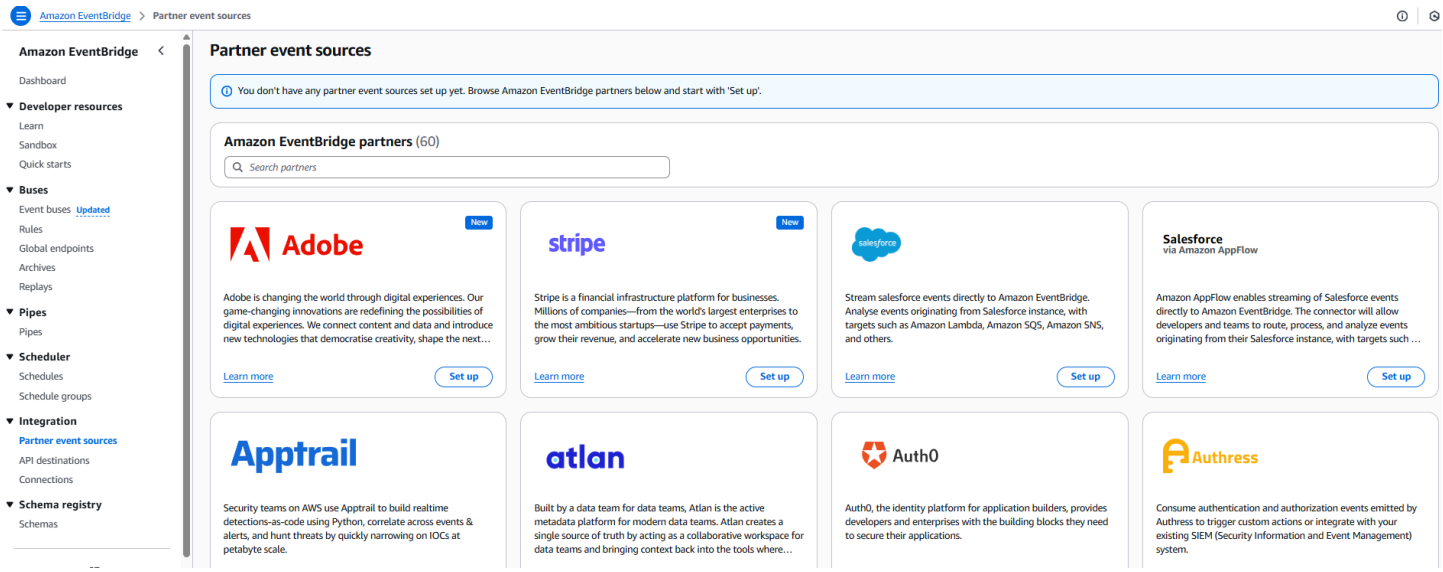


8. Selecione um ou mais destinos para seus eventos, como Amazon SNS, AWS Lambda, um documento do SSM ou Step Functions. Configure destinos entre contas, se necessário.



9. Analise e crie a regra.

Para usar integrações de parceiros pré-criadas, escolha Origens de eventos de parceiros no console do EventBridge. Os parceiros disponíveis incluem Atlassian (Jira), Datadog, New Relic, PagerDuty, Symantec e Zendesk.



Integrações com Jira, Slack e ServiceNow

A AWS fornece soluções totalmente desenvolvidas para integração bidirecional com o Jira, Slack e ServiceNow. Essas integrações mantêm os casos do AWS Security Incident Response e suas

plataformas ITSM ou ChatOps sincronizados. As atualizações em um sistema são refletidas automaticamente no outro.

Vantagens da integração

A integração da AWS Security Incident Response à plataforma de ITSM existente simplifica as operações de segurança centralizando os fluxos de trabalho de rastreamento e resposta a incidentes. Essas soluções prontas eliminam a necessidade de desenvolvimento personalizado, permitindo que as equipes de segurança mantenham a visibilidade dos sistemas de gerenciamento de incidentes nativos da AWS e corporativos. Ao usar o EventBridge para automação orientada por eventos, as atualizações fluem perfeitamente entre as plataformas em tempo real, garantindo que os incidentes de segurança sejam rastreados sistematicamente, qualquer que seja sua origem. Essa abordagem unificada reduz a alternância de contextos para os analistas de segurança, melhora os tempos de resposta e fornece trilhas de auditoria abrangentes em todo o ciclo de vida das respostas a incidentes.

Para obter instruções de implantação, consulte exemplos de soluções da AWS para Jira, Slack e ServiceNow.

SIEM e ferramentas externas

O AWS Security Incident Response não ingere diretamente as descobertas do seu SIEM. No entanto, quando você abre um caso com suporte da AWS, as equipes de resposta pela SIRT da AWS analisam e investigam as descobertas do SIEM em paralelo com sua equipe. A SIRT ajuda a identificar correlações em ambientes híbridos e multinuvem e auxilia no escopo das atividades dos agentes de ameaças em todos os fornecedores.

A SIRT da AWS também colabora diretamente com seus provedores de MDR e equipes de investigação terceirizadas para ajudar a estabelecer processos de coordenação eficazes antes que ocorra um incidente.

Apêndice A: pontos de contato e informações críticas

Preencha a tabela a seguir e entregue-a à sua equipe de contas da AWS antes da implantação. Essas informações permitem que a SIRT da AWS faça contato rapidamente com as pessoas certas durante um evento de segurança.

Informações de contato do pessoal de IR e SOC

Ent	Pessoal IR | SOC: cargo, nome, e-mail	Primá secun o, contat de escalo ento	Interv s CIDR intern conhe s	Interv s CIDR extern conhe s	Prove s de serviç em nuven adicio s	Traba com Regiõ da AWS	IPs do servid DNS (se for difere do Amaz Route Resol	VPN | Soluçõe e IPS de acesso remoto	Nomes dos aplicativ os críticos | Número de conta	Portas incom comu usada	ERD | AV | Ferrame as de gerencia ento de vulnerab lidades usadas	IDP | Locais
1	Comand e SOC, John Smith, jsmith@ amplo.c	Prima	10.0.0 16	5.5.60 20 (Azure	Azure	us-east-1 , us-east-2	N/D	Direct Connect VIF pública 116.32.8 7	Servidor Web Nginx (exempl crítico) | 1234567 0	8080	CrowdSt ke Falcon	Entra, Azure

Para enviar essas informações, conclua as seguintes etapas:

1. Preencha a tabela de metadados anterior com as informações do seu ambiente.
2. Crie um caso do AWS Support com os seguintes detalhes:
   - Tipo de caso: Técnico
   - Serviço: Resposta a Incidentes de Segurança
   - Categoria: Outros
3. Anexe ao caso a tabela de metadados preenchida.

Matriz RACI

A matriz RACI a seguir define perfis e responsabilidades ao longo de todo o processo de implementação do Security Incident Response. RACI são as iniciais das palavras Responsável (R), Responsabilizável (A), Consultado (C) e Informado (I) em inglês.

Atividade	Cliente	Equipe da conta da AWS	Equipe de SIR
Pré-onboarding			
Identificar as principais partes interessadas	R		eu
Validar as fontes de descobertas	R	C	eu
[integração de EDR de terceiros] CSPM do Security Hub	R	C	eu
Validação/verificação de integridade do GuardDuty	C	R	eu
Determinar o escopo da conta	R		
Estabelecer protocolos de escalação	R	eu	C
Habilitar o AWS Organizations	R	C	
Associação de contas com o AWS Organizations	R	eu	
Selecionar uma conta de administr ador delegado/ferramental de segurança	R	eu	
Onboarding			
Configuração dos detalhes da associação	R	eu	

Atividade	Cliente	Equipe da conta da AWS	Equipe de SIR
Passo a passo (configurar fluxos de trabalho proativos de resposta e triagem de alertas; implantar o perfil vinculado ao serviço na conta gerencial; autorizar ações de contenção)	R	C	eu
Configuração de implantação pós-implantação			
Revisar os recursos de integração operacional	R	C	eu
Enviar casos reativos do Security Incident Response	R		
Configurar integrações do Amazon EventBridge	R	C	C
Conectar ferramental de terceiros (Jira, ServiceNow, PagerDuty, Teams etc.)	R	eu	C
Aprofundamento e demonstração do serviço	A	R	C

Definições da matriz RACI:

- Responsável (R): a parte que realiza o trabalho para concluir a tarefa
- Responsabilizável (A): a parte que em última instância responde pela conclusão correta da tarefa
- Consultado (C): a parte cujas opiniões são solicitadas e com quem existe comunicação bidirecional
- Informado (I): a parte que se mantém atualizada sobre o progresso e com quem existe comunicação unidirecional

Seleção de uma conta de associação

Uma conta de associação consiste na conta da AWS usada para configurar detalhes da conta, adicionar e remover informações para sua equipe de resposta a incidentes, além de ser destinada à criação e ao gerenciamento de todos os eventos de segurança, tanto ativos quanto históricos. É recomendável que a conta de associação da AWS Security Incident Response esteja alinhada com a mesma conta habilitada para serviços como o Amazon GuardDuty e o AWS Security Hub CSPM.

Você tem duas opções para selecionar sua conta de associação da AWS Security Incident Response usando o AWS Organizations. É possível criar a associação na conta gerencial do Organizations ou em uma conta de administrador delegado do Organizations.

Uso da conta de administrador delegado: as tarefas administrativas e o gerenciamento de casos da AWS Security Incident Response estão localizados na conta de administrador delegado. Recomendamos usar o mesmo administrador delegado configurado para outros serviços de segurança e de conformidade da AWS. Forneça o ID da conta de administrador delegado, que contém 12 dígitos, e, em seguida, faça login nessa conta para continuar.

Important

Quando você usa uma conta de administrador delegado como parte do processo de configuração, a AWS Security Incident Response não pode criar automaticamente o perfil vinculado ao serviço de triagem necessária em sua conta gerencial do AWS Organizations. Conclua as seguintes etapas para criar manualmente esse perfil em sua conta gerencial do AWS Organizations.

Para criar um perfil vinculado ao serviço (console)

1. Faça login na sua conta gerencial do AWS Organizations.
2. Acesse o Console do AWS CloudShell ou acesse a conta por meio da AWS Command Line Interface usando seu método preferido.
3. Use o comando da CLI: . `aws iam create-service-linked-role --aws-service-name "triage.security-ir.amazonaws.com" --no-cli-pager`.
4. (Opcional) Para verificar se o comando está funcionando, execute o comando `aws iam get-role --role-name AWSServiceRoleForSecurityIncidentResponse_Triage`.

Uso da conta atualmente conectada: selecionar esta conta significa que a conta atual será designada como a conta principal de associação para sua associação à AWS Security Incident Response. Os indivíduos da sua organização precisarão acessar o serviço por meio desta conta para criar, acessar e gerenciar casos ativos e resolvidos.

Certifique-se de ter permissões suficientes para administrar a AWS Security Incident Response.

Consulte Adicionar e remover permissões de identidade do IAM para obter etapas específicas sobre como adicionar permissões.

Consulte AWS Security Incident Response managed policies.

Para verificar as permissões do IAM, você pode seguir estas etapas:

- Verificação da política do IAM: analise a política do IAM associada ao seu usuário, grupo ou perfil para garantir que ela conceda as permissões necessárias. É possível fazer isso ao acessar https://console.aws.amazon.com/iam/, selecionar a opção `Users`, escolher o usuário específico e, em seguida, na página de resumo, acessar a guia `Permissions`, em que você pode visualizar uma lista de todas as políticas anexadas. Você pode expandir cada linha da política para visualizar os detalhes.
- Teste das permissões: tente executar a ação necessária para verificar se as permissões estão corretas. Por exemplo, se você precisa acessar um caso, tente usar o comando `ListCases`. Se você não tiver as permissões necessárias, receberá uma mensagem de erro.
- Uso da AWS CLI ou de um SDK: você pode usar a AWS Command Line Interface ou um AWS SDK na linguagem de programação de sua preferência para testar as permissões. Por exemplo, com a AWS Command Line Interface, você pode executar o comando `aws sts get-caller-identity` para verificar as permissões do usuário atual.
- Verificação dos logs do AWS CloudTrail: analise os logs do CloudTrail para verificar se as ações que você está tentando executar estão sendo registradas em log. Essa verificação pode auxiliar na identificação de problemas relacionados a permissões.
- Uso do simulador de políticas do IAM: o simulador de políticas do IAM é uma ferramenta que permite o teste de políticas do IAM e visualizar o efeito que elas têm sobre suas permissões.

> **Note**
>
> As etapas específicas podem variar dependendo do serviço da AWS e das ações que você está tentando executar.

Configuração dos detalhes da associação

- Selecione uma Região da AWS que será usada para armazenar tanto sua associação quanto os casos associados a ela.

> **Warning**
>
> Após o registro inicial da associação, não será possível alterar a Região da AWS padrão.

- Selecione se você deseja fornecer cobertura total de associados em todo o AWS Organizations ou em parte do AWS Organizations por meio de unidades organizacionais (UOs).
- Opcionalmente, você pode selecionar um nome para esta associação.
- É necessário fornecer um contato principal e um contato secundário como parte do fluxo de criação da associação. Esses contatos são incluídos automaticamente como integrantes da sua equipe de resposta a incidentes. Deve haver, no mínimo, dois contatos para uma única associação, o que também garante a inclusão mínima de dois integrantes na equipe de resposta a incidentes.
- Defina etiquetas opcionais para sua associação. As etiquetas ajudam no monitoramento os custos da AWS e facilitam a pesquisa de recursos.

Associação de contas com o AWS Organizations

Se você optou por associar todo seu AWS Organizations durante a configuração, sua associação dará direito à cobertura de todas as contas de membros na organização. As contas associadas serão atualizadas automaticamente à medida que as contas forem adicionadas ou removidas da sua organização.

Se você optou por associar parte do seu AWS Organizations durante a configuração e tiver restringido sua associação a unidades organizacionais (UOs) específicas, sua associação dará direito à cobertura de todas as contas nas UOs selecionadas. Isso inclui contas em sub-UOs das UOs selecionadas. As contas associadas são atualizadas automaticamente à medida que as contas forem adicionadas ou removidas dessas UOs.

Para obter mais informações sobre as práticas recomendadas envolvendo unidades organizacionais, consulte Organizar seu ambiente da AWS usando várias contas.

Configuração de fluxos de trabalho de resposta proativa e de triagem de alertas

A AWS Security Incident Response monitora e investiga alertas gerados nas integrações com o Amazon GuardDuty e o CSPM do Security Hub. Para usar esse recurso, o Amazon GuardDuty deve estar habilitado. A AWS Security Incident Response realiza uma triagem automatizada de alertas de baixa prioridade, permitindo que sua equipe se concentre nas questões mais importantes. Para obter mais informações sobre como a AWS Security Incident Response funciona com o Amazon GuardDuty e com o AWS Security Hub CSPM, consulte a seção Detecção e análise do guia do usuário.

Se você enfrente algum problema durante o processo de integração, crie um caso no AWS Support para obter assistência adicional. Certifique-se de incluir detalhes, como o ID da Conta da AWS e quaisquer erros observados durante o processo de configuração.

> **Note**
>
> Se tiver dúvidas sobre as regras de supressão do Amazon GuardDuty, configurações de triagem de alertas ou fluxos de trabalho de resposta proativa, crie um caso com o suporte da AWS com o tipo de caso Investigações e consultas para consultar a equipe do AWS Security Incident Response. Para obter mais informações, consulte Criação de um caso com suporte por parte da AWS.

Este atributo permite que a AWS Security Incident Response monitore e investigue descobertas em todas as contas incluídas e em todas as regiões compatíveis da AWS ativas na sua organização. Para viabilizar essa funcionalidade, a AWS Security Incident Response cria automaticamente um perfil vinculado ao serviço em todas as contas de membros cobertas do AWS Organizations. No entanto, na conta gerencial, a criação desse perfil vinculado ao serviço deve ser feita manualmente para habilitar o monitoramento.

O AWS Security Incident Response não pode criar o perfil vinculado ao serviço na conta gerencial. É necessário criar esse perfil manualmente na conta gerencial. Para obter mais informações, consulte a nota Importante em Seleção de uma conta de associação.

Entender arquivamento automático com resposta proativa

Quando você habilita resposta proativa e triagem de alertas, a AWS Security Incident Response automaticamente monitora e faz a triagem das descobertas do Amazon GuardDuty e do CSPM do Security Hub. Como parte desse fluxo de trabalho de triagem automática, as descobertas são arquivadas automaticamente segundo os seguintes critérios:

Comportamento de arquivamento automático:

- Descobertas benignas: quando o processo de triagem automática determina que uma descoberta é benigna (não é uma verdadeira ameaça à segurança), a AWS Security Incident Response automaticamente arquiva a descoberta no Amazon GuardDuty e cria regras de supressão para evitar que descobertas semelhantes gerem alertas no futuro.
- Regras de supressão: o serviço cria regras de supressão e arquivamento automático no Amazon GuardDuty e no CSPM do Security Hub para descobertas que correspondam aos padrões reconhecidos do ambiente, como endereços IP esperados, entidades do IAM e comportamentos operacionais normais.
- Volume de alertas reduzido: as organizações que usam a tecnologia SIEM observarão volumes de descoberta do Amazon GuardDuty significativamente reduzidos ao longo do tempo, à medida que o serviço aprender o ambiente e arquivar automaticamente descobertas benignas. Isso melhora a eficiência do serviço AWS Security Incident Response e do SIEM.

Visualizar descobertas arquivadas:

É possível revisar automaticamente as descobertas arquivadas e as regras de supressão criadas pelo AWS Security Incident Response:

1. Navegue até o console do Amazon GuardDuty
2. Escolha Descobertas
3. Selecione Arquivada no filtro de descobertas
4. Revise as regras de supressão selecionando a seta para baixo ao lado de cada regra

Considerações importantes:

- As descobertas arquivadas são retidas no Amazon GuardDuty por 90 dias e podem ser visualizadas a qualquer momento durante esse período

- Você pode modificar ou excluir regras de supressão a qualquer momento no console do Amazon GuardDuty
- O processo de triagem automática se adapta continuamente ao ambiente, melhorando a precisão ao longo do tempo e reduzindo os falsos positivos

Contenção: no caso de um evento de incidente de segurança, a AWS Security Incident Response pode executar ações de contenção para mitigar rapidamente o impacto, como isolar hosts comprometidos ou alterar credenciais. A Resposta a Incidentes de Segurança não habilita, por padrão, as funcionalidades de contenção. Para executar essas ações de contenção, é necessário primeiro conceder as permissões necessárias ao serviço. Essa concessão pode ser realizada por meio da implantação de um AWS CloudFormation StackSet, que estabelece os perfis necessários.

Tarefas do usuário

Conteúdo

Painel do Resposta a Incidentes de Segurança

No console de AWS Security Incident Response, o painel fornece uma visão geral da sua equipe de resposta a incidentes, do status da resposta proativa e da contagem contínua de casos nas últimas quatro semanas.

Equipe de resposta a incidentes

Selecione Visualizar a equipe de resposta a incidentes para acessar os detalhes de seus colegas da equipe de resposta a incidentes.

Meus casos

A seção Meus casos do painel apresenta o número de casos com suporte por parte da AWS que estão abertos e encerrados, bem como os casos gerenciados por conta própria atribuídos a você durante um período específico. Essa seção também apresenta o tempo médio, em horas, dedicado à resolução dos casos encerrados.

Gerenciamento da equipe de resposta a incidentes

As equipes de resposta a incidentes incluem as partes interessadas responsáveis por participar do processo de resposta a incidentes. É possível configurar até dez partes interessadas como parte da associação.

Os exemplos de partes interessadas internas incluem membros da sua equipe de resposta a incidentes, analistas de segurança, responsáveis pelas aplicações e integrantes da equipe de liderança em segurança.

Os exemplos de partes interessadas externas incluem indivíduos de provedores de software independentes (ISV) e de provedores de serviços gerenciados (MSP) que você deseja integrar ao processo de resposta a incidentes.

> **Note**
>
> A configuração da equipe de resposta a incidentes não concede automaticamente aos integrantes da equipe acesso a recursos do serviço, como associação e casos. Você pode usar as políticas gerenciadas da AWS para a AWS Security Incident Response a fim de conceder permissões de leitura e de gravação aos recursos. Clique aqui para obter mais informações.

Os integrantes da equipe de resposta a incidentes especificados em um nível de associação serão adicionados automaticamente para qualquer caso. É possível adicionar ou remover integrantes da equipe individualmente a qualquer momento após a criação de um caso.

A equipe de resposta a incidentes receberá por e-mail uma notificação sobre os eventos listados nas preferências de comunicação.

Preferências de comunicação

Configure suas preferências de comunicação para controlar como você recebe notificações e interage com o sistema de resposta a incidentes durante incidentes de segurança.

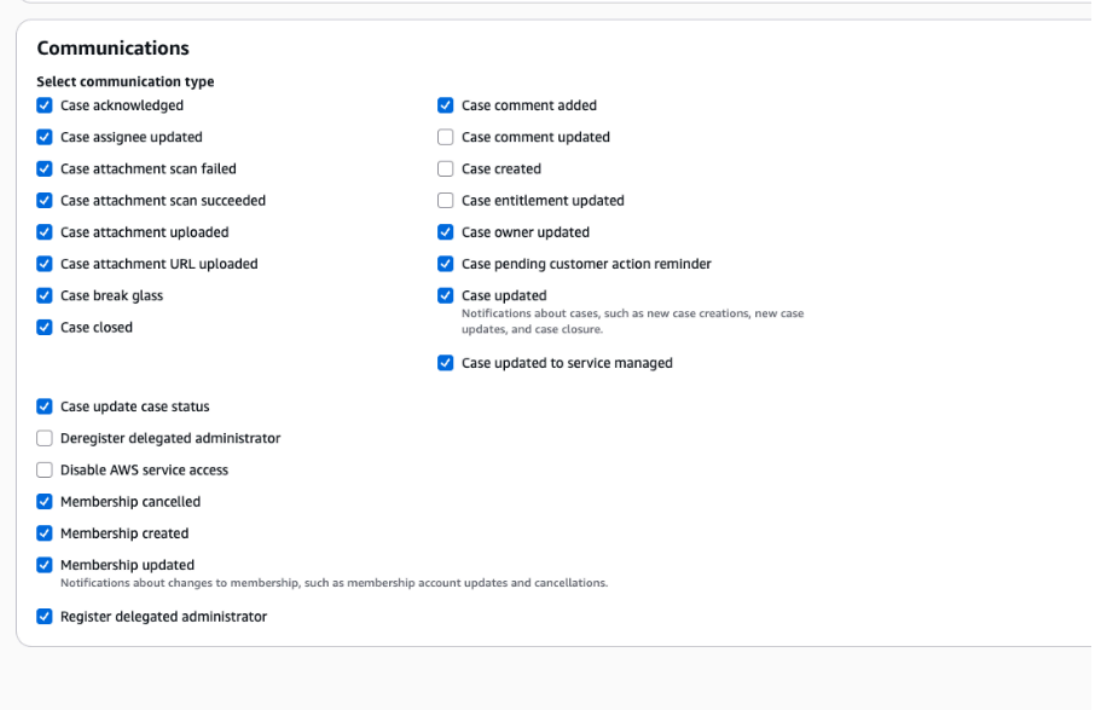
Gerenciar preferências de comunicação da equipe

Você pode configurar as preferências de comunicação para indivíduos da sua equipe de resposta a incidentes na página do painel.

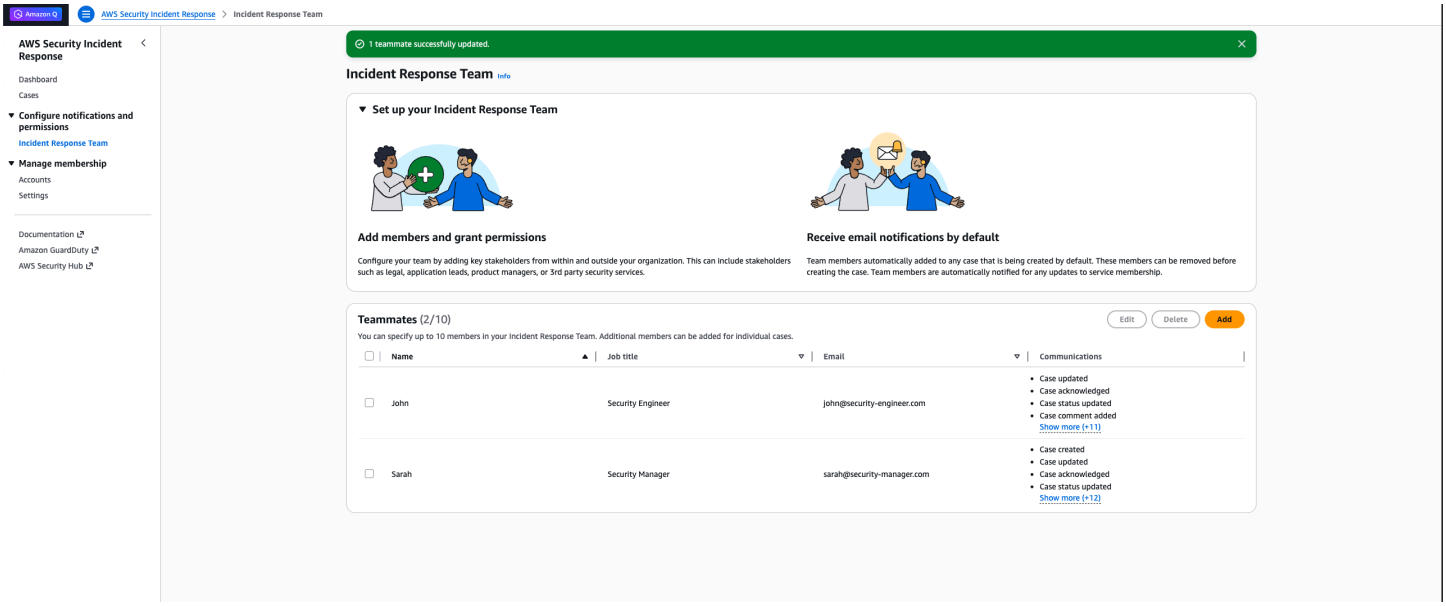
Siga estas etapas para gerenciar as configurações de comunicação dos membros da equipe:

1. Navegue até a página da equipe de resposta a incidentes em seu painel
2. Execute um destes procedimentos:
   - Para atualizar as preferências de um membro existente da equipe: selecione o colega cujas preferências de comunicação você deseja modificar e escolha Editar
   - Para adicionar um novo membro da equipe: escolha Adicionar
3. Na parte inferior da página, você verá as Comunicações
   a. Marque as caixas de seleção das comunicações que você deseja receber

b. Desmarque as caixas de seleção das comunicações que você não deseja receber



4. Salve as alterações



Configurações de comunicação padrão

Por padrão, os membros da equipe de resposta a incidentes têm todas as comunicações habilitadas. É possível modificar essas configurações a qualquer momento seguindo as etapas acima.

Opções de comunicação

Suas preferências de comunicação controlam como você interage com o sistema de resposta a incidentes e como as notificações são entregues a você durante incidentes de segurança.

> **Note**
>
> Essas preferências se aplicam a todas as comunicações futuras dentro do sistema de Resposta a Incidentes de Segurança. Você pode modificar essas configurações a qualquer momento repetindo as etapas acima.

Associação de contas com o AWS Organizations

Ao habilitar o AWS Security Incident Response, você terá a opção de selecionar toda a sua organização ou unidades organizacionais (UOs) específicas. Se UOs específicas forem selecionadas, sua associação cobrirá apenas as contas que se enquadrarem nessas UOs selecionadas. Se toda a organização for selecionada, sua associação cobrirá todas as contas da organização.

Para obter mais detalhes, consulte Gerenciamento de contas da AWS Security Incident Response com o AWS Organizations.

Gerenciar a cobertura da associação

É possível alterar a opção de cobertura da associação a qualquer momento, inclusive para trocar da cobertura de toda a organização para a cobertura de UOs específicas.

Atualizar as associações de UOs

Para gerenciar a cobertura da associação:

1. Navegue até a página de configurações de associação da conta
2. Selecione Adicionar UOs para selecionar as UOs que você deseja incluir na associação
3. Selecionar as UOs que você deseja incluir na associação
4. Clique em Atualizar associação para salvar a inclusão da UO na associação

Depois de atualizar as associações, você pode retornar à mesma página e remover as UOs que não desejar manter na associação. Essa flexibilidade se aplica mesmo que você tenha selecionado

inicialmente toda a organização. Mais tarde, será possível atualizar a associação para incluir somente UOs específicas sem necessidade de cancelar e reabilitar o serviço.

Para saber mais, consulte Gerenciar a associação com unidades organizacionais (UOs).

Considerações importantes

Contas diretamente na raiz: ao selecionar UOs específicas para a associação, as contas que estão diretamente na raiz da organização (que não fazem parte de nenhuma UO) não serão incluídas. Para incluir essas contas na cobertura da associação, primeiro adicione-as a uma UO e depois inclua essa UO na associação.

> **Note**
>
> Aprimoramos continuamente a associação de UOs para tornar o processo mais intuitivo e autoexplicativo para o usuário.

Monitoramento e investigação

O AWS Security Incident Response analisa e faz a triagem dos alertas de segurança do Amazon GuardDuty e do AWS Security Hub CSPM, depois configura regras de supressão com base no ambiente para evitar alertas desnecessários. A equipe do AWS Security Incident Response Engineering (SIRE) investiga as descobertas, e rapidamente escala e orienta sua equipe para conter possíveis problemas. Se desejar, você pode conceder permissão à AWS Security Incident Response para implementar ações de contenção em seu nome.

A AWS Security Incident Response está em conformidade com o guia NIST 800-61r2 Computer Security Event Handling Guide para a resposta a eventos de segurança. Ao estar alinhada com esse padrão do setor, a AWS Security Incident Response fornece uma abordagem consistente para o gerenciamento de eventos de segurança e adota as práticas recomendadas para a proteção e para a resposta a eventos de segurança em seu ambiente da AWS.

Quando o AWS Security Incident Response identifica um alerta de segurança ou quando você solicita assistência de segurança, o AWS SIRE faz uma investigação. A equipe coleta eventos de logs e dados provenientes do serviço, como alertas do GuardDuty, realiza a triagem e a análise dos dados, executa atividades de remediação e de contenção, e fornece um relatório posterior ao incidente.

Conteúdo

Preparar

A equipe de AWS Security Incident Response realiza investigações e trabalha em conjunto com você ao longo de todo o ciclo de vida de resposta a um evento de segurança. É recomendável realizar a configuração dessa equipe e a atribuição das permissões necessárias antes da ocorrência de um evento de segurança.

Detecção e análise

Relatar um evento

É possível criar um evento de segurança no portal do AWS Security Incident Response. Durante a ocorrência de um evento de segurança, é essencial agir sem demora. A AWS Security Incident Response usa técnicas automatizadas e manuais para conduzir investigações de eventos de segurança, analisar logs e procurar padrões anômalos. A sua colaboração e compreensão do seu ambiente acelera esse processo de análise.

Habilitar fontes de detecção compatíveis

> **Note**
>
> Os custos associados ao serviço de AWS Security Incident Response não incluem os custos e as taxas decorrentes do uso das fontes de detecção compatíveis ou de outros serviços da AWS. Consulte as páginas individuais de cada serviço ou recurso para obter mais detalhes sobre os preços.

Amazon GuardDuty

Para habilitar o GuardDuty em toda a sua organização, consulte a seção `Setting up GuardDuty` no Guia do usuário do Amazon GuardDuty.

É altamente recomendável que o GuardDuty seja habilitado em todas as Regiões da AWS com suporte. Com isso, o GuardDuty poderá realizar a geração de descobertas relacionadas a atividades incomuns ou não autorizadas mesmo em regiões que não estejam em uso ativo. Para obter mais informações, consulte Amazon GuardDuty Regions and endpoints.

A habilitação do GuardDuty fornece à AWS Security Incident Response acesso a dados críticos de detecção de ameaças, aprimorando sua capacidade de identificar e de responder a possíveis problemas de segurança em seu ambiente da AWS.

AWS Security Hub CSPM

O AWS Security Hub CSPM pode ingerir descobertas de segurança de diversos serviços da AWS e de soluções de segurança de terceiros compatíveis. Essas integrações podem auxiliar a AWS Security Incident Response no monitoramento e na investigação de descobertas originadas por outras ferramentas de detecção.

Para habilitar o Security Hub CSPM com a integração ao Organizations, consulte o Guia do usuário do AWS Security Hub CSPM.

Existem diversas formas de habilitar as integrações no Security Hub CSPM. Para integrações de produtos de terceiros, talvez seja necessário comprar a integração do AWS Marketplace e, depois, configurar a integração. As informações de integração fornecem links para realizar essas tarefas. Saiba mais informações sobre como habilitar integrações no AWS Security Hub CSPM.

A AWS Security Incident Response pode monitorar e investigar descobertas provenientes das seguintes ferramentas quando essas ferramentas estão integradas ao AWS Security Hub CSPM:

- CrowdStrike: CrowdStrike Falcon
- Lacework: Lacework
- Trend Micro: Cloud One

Ao habilitar essas integrações, é possível aprimorar significativamente o escopo e a eficácia das funcionalidades de monitoramento e de investigação da AWS Security Incident Response.

Detecção

Com a Resposta proativa, o AWS Security Incident Response ingere as descobertas do Amazon GuardDuty e do AWS Security Hub CSPM através das regras do Amazon EventBridge implantadas em suas contas durante a integração.

O AWS Security Incident Response arquiva automaticamente as descobertas do Amazon GuardDuty que, durante a triagem automatizada, são consideradas benignas ou associadas às atividades esperadas. Você pode visualizar as descobertas arquivadas no console do Amazon GuardDuty selecionando Arquivada no filtro Status das descobertas. Para saber mais, consulte Visualizar as descobertas geradas no console do GuardDuty no Guia do usuário do Amazon GuardDuty.

O AWS Security Incident Response arquiva automaticamente as descobertas do Amazon GuardDuty que, durante a triagem automatizada, são consideradas benignas ou associadas às atividades esperadas. Apenas as descobertas que foram triadas e cujo resultado foi designado como “arquivar” são arquivadas. As descobertas sob investigação ativa permanecem visíveis no console do Amazon GuardDuty mesmo após o encerramento da investigação. Você pode visualizar as descobertas arquivadas no console do Amazon GuardDuty selecionando Arquivada no filtro de descobertas. Para saber mais sobre o trabalho com descobertas arquivadas, consulte Trabalhar com descobertas no Guia do usuário do Amazon GuardDuty.

Quando o AWS Security Hub CSPM ingere descobertas de segurança, o sistema atualiza cada descoberta com uma observação indicando que a triagem automatizada foi iniciada. O estado do fluxo de trabalho muda de NOVO para NOTIFICADO, o que remove a descoberta da visualização de descobertas padrão do AWS Security Hub CSPM. Se a triagem determinar que uma descoberta é benigna ou associada às atividades esperadas, o sistema adiciona uma observação à descoberta e atualiza o estado do fluxo de trabalho para SUPRIMIDO.

Análise: triagem automatizada

O AWS Security Incident Response faz a triagem automática das descobertas de segurança. O processo de triagem determina se a atividade detectada representa o comportamento esperado analisando dados de várias fontes, incluindo a carga útil da descoberta, os metadados do serviço da AWS, os dados de registro em log e o monitoramento da AWS (como logs de fluxo do AWS CloudTrail e da VPC), a inteligência de ameaças da AWS e o contexto que você é convidado a fornecer sobre o ambiente da AWS e o ambiente on-premises.

Se a triagem automatizada determinar que a atividade detectada era esperada, o sistema não realizará nenhuma ação investigativa adicional.

Análise: investigação do Incident Response Security

O AWS Security Incident Response Engineering é uma equipe global, sempre disponível, de profissionais de segurança com expertise na AWS e em resposta a incidentes de segurança. Se a triagem automatizada não conseguir determinar se a atividade era esperada, o AWS Security Incident Response Engineering é envolvido para realizar uma investigação de segurança. Se o evento tiver sido ingerido do Security Hub, será postada uma observação na descoberta correspondente informando que a investigação do AWS Security Incident Response Engineering está em andamento.

O AWS Security Incident Response Engineering conduz uma investigação de segurança na prática, analisando outros metadados do serviço e inteligência de ameaças, revisando insights

de descobertas e investigações anteriores no ambiente e aplicando sua expertise em resposta a incidentes. Dependendo de suas preferências de contenção (consulte Conter), o AWS Security Incident Response Engineering pode envolver a equipe de resposta a incidentes de sua organização por meio de um caso do Resposta a Incidente de Segurança no console do AWS Security Incident Response para verificar se a atividade detectada era esperada e autorizada a responder a um caso gerado pela AWS.

Como parte de uma investigação de segurança, o AWS Security Incident Response também pode coletar informações investigativas de dentro das instâncias do Amazon Elastic Compute Cloud usando o EC2 Triage. Quando habilitado, esse recurso permite que os respondentes do AWS Security Incident Response executem o Run Command do AWS Systems Manager em instâncias do Amazon EC2 para coletar dados investigativos, inspecionar processos em execução e analisar o estado do sistema, sem exigir acesso direto à instância.

O EC2 Triage é compatível com os seguintes sistemas operacionais:

Linux

- Amazon Linux 2, Amazon Linux 2023
- Ubuntu 18.04, 20.04, 22.04, 24.04
- Red Hat Enterprise Linux (RHEL) 7.x, 8.x, 9.x
- CentOS 7.x, 8.x
- SUSE Linux Enterprise Server (SLES) 12.x, 15.x
- Debian 10, 11, 12

Windows

- Windows Server 2012 R2
- Windows Server 2016, 2019, 2022

Para usar o EC2 Triage, você deve implantar o modelo Contenção com o EC2 Triage do CloudFormation em suas contas. Para obter mais informações, consulte Trabalhar com o CloudFormation StackSets. As instâncias de destino do Amazon EC2 devem ter o SSM Agent instalado e em execução, e devem estar on-line e gerenciadas pelo AWS Systems Manager. Para obter mais informações sobre configuração, consulte Configuração do Systems Manager para instâncias do EC2.

Comunicar

O AWS Security Incident Response mantém você informado durante as investigações de segurança, interagindo com sua equipe de resposta a incidentes por meio de um caso da Resposta a Incidentes de Segurança. Vários membros do AWS Security Incident Response Engineering podem prestar suporte a uma mesma investigação. A comunicação pode incluir: confirmação ou notificação da criação de uma investigação de segurança; estabelecimento de uma ponte de chamada; análise de artefatos, como arquivos de log; solicitações de confirmação de atividades esperadas e compartilhamento dos resultados das investigações.

Quando o AWS Security Incident Response envolve proativamente sua equipe de resposta a incidentes, é criado um caso na sua Associação do AWS Security Incident Response, que centraliza a comunicação de todas as contas organizacionais em um lugar. Esses casos contêm o prefixo “[Caso proativo]” no título, o que os identifica como iniciados pelo AWS Security Incident Response. Quando se envolve proativamente e fornece respostas oportunas a essas comunicações, sua equipe de resposta a incidentes pode ajudar o AWS Security Incident Response a fazer o seguinte:

- Garantir uma resposta rápida a incidentes de segurança reais.
- Entender o ambiente e os comportamentos esperados.
- Reduzir detecções de falsos positivos ao longo do tempo.

A eficácia do AWS Security Incident Response é maior com a sua colaboração, o que resulta no monitoramento mais eficiente e em um ambiente da AWS mais seguro.

Atualizar descobertas

O modo como o AWS Security Incident Response gerencia as descobertas é diferente, dependendo da origem das descobertas e dos resultados da triagem.

Ajuste do serviço

Quando as cotas de serviço da conta permitirem, o AWS Security Incident Response tenta implantar uma regra de supressão do Amazon GuardDuty ou uma regra de automação do AWS Security Hub CSPM. Essas regras suprimem descobertas futuras que correspondam ao tipo e à origem das atividades autorizadas conhecidas (por exemplo, endereço IP da origem, ASN, entidade principal da identidade ou recurso). As regras do AWS Security Hub CSPM são implantadas com prioridade máxima, o que permite substituir essas automações por regras autodefinidas, se necessário.

Dessa maneira, o AWS Security Incident Response ajusta as origens de detecção com base no comportamento esperado no ambiente da AWS. Sua equipe de resposta a incidentes é notificada sobre modificações nesses conjuntos de regras, e as alterações são revertidas mediante solicitação.

Agente de IA investigativo

Visão geral

O agente de investigação por IA trabalha junto com os clientes e os engenheiros do AWS Security Incident Response para agilizar as investigações de segurança. Quando um cliente cria um caso com o suporte da AWS, o agente automaticamente ativa em paralelo o envolvimento do engenheiro do Security Incident Response, o que reduz o tempo de resolução de dias para horas.

Durante escalações do cliente, os casos do Security Incident Response podem ser criados por você ou proativamente pelo AWS Security Incident Response. Quando um novo caso com o suporte da AWS é criado, o agente de investigação é acionado automaticamente. Você pode gerenciar todos os casos no console, na API ou nas integrações do Amazon EventBridge.

Benefícios principais

- Investigação paralela: o agente trabalha ao mesmo tempo que os respondentes, fornecendo tanto automação por IA quanto expertise humana.
- Coleta automatizada de evidências — elimina a análise manual de logs por meio de consultas automáticas à AWS CloudTrail, IAM, Amazon EC2 e Cost Explorer.
- Interface de linguagem natural — você pode descrever as questões de segurança em linguagem simples, sem precisar de experiência em formatos de log AWS.
- Resposta mais rápida — resumos da investigação ficam disponíveis em minutos na guia Investigação.
- Auditabilidade total — todas as ações do atendente são registradas na AWS CloudTrail sob o perfil `AWSServiceRoleForSupport`.

> **Important**
>
> Esse atributo está disponível somente para os casos suportados pela AWS. Os casos autogerenciados não incluem possibilidades de investigação com IA.

Como funciona

O agente de investigação por IA segue um fluxo de trabalho estruturado ao analisar casos de segurança com o suporte da AWS:

Fluxo de trabalho de investigação

1. Criação de casos: o cliente cria um caso com o suporte da AWS no console do Security Incident Response descrevendo o problema de segurança.
2. Ativação paralela
   - Os engenheiros do Security Incident Response se envolvem no caso.
   - Simultaneamente, o agente de IA inicia seu fluxo de trabalho de investigação.
3. Perguntas contextuais (opcional) — o atendente pode fazer perguntas de esclarecimento para obter detalhes específicos:
   - IDs da conta AWS afetada
   - Entidades principais IAM envolvidas (usuários, perfis, chaves de acesso)
   - Identificadores de recursos específicos (buckets S3, instâncias EC2, ARNs)
   - Período de tempo de atividade suspeita
4. Coleta de evidências — o atendente consulta automaticamente as fontes de dados da AWS:
   - AWS CloudTrail – chamadas de API e atividades associadas ao incidente
   - IAM — permissões de usuário e perfil, mudanças de políticas e criação de novas identidades
   - APIs de instância do Amazon EC2 — Informações sobre recursos computacionais, se eles estiverem envolvidos
   - Explorador de custos — métricas de custo e uso para consumo incomum de recursos
5. Análise e correlação — o atendente correlaciona evidências entre serviços, identifica padrões e cria um cronograma dos eventos.
6. Geração de resumo — em questão de minutos, o atendente apresenta um resumo abrangente da investigação na guia Investigação.

> **Note**
>
> Todos os campos são opcionais. Se nenhuma resposta for fornecida em 10 minutos, a investigação será iniciada automaticamente. Em alguns casos, se já houver informações suficientes disponíveis, o atendente poderá ignorar totalmente as perguntas opcionais.

Como acessar os resultados da investigação

Para ver a análise de IA:

1. Navegue para seu caso no console de Resposta a Incidentes de Segurança
2. Selecione a guia Investigação.
3. Revise o resumo da investigação com suas descobertas, o cronograma e o contexto.

O resumo do agente de investigação por IA é publicado automaticamente como um comentário na seção Comunicação do caso, o que facilita a revisão em conjunto com outras atualizações do caso.

Acesso a dados e permissões

O atendente investigativo de IA usa o perfil vinculado ao serviço `AWSServiceRoleForSupport` para acessar recursos da AWS. Esse recurso fornece permissões somente leitura necessárias para a coleta de evidências.

Todas as ações realizadas pelo atendente são registradas no AWS CloudTrail, permitindo que os clientes auditem exatamente quais dados foram acessados durante a investigação. Nos logs AWS CloudTrail, essas ações são atribuídas à `AWSServiceRoleForSupport`.

Pré-requisitos

Antes de usar as capacidades de investigação potencializadas por IA, certifique-se do seguinte:

Configuração necessária

- AWS Security Incident Response habilitado: o serviço deve ser habilitado por meio da conta gerencial do AWS Organizations.
- Tipo de caso com o suporte da AWS: a investigação por IA está disponível apenas para casos com suporte da AWS (não para casos autogerenciados).
- AWSServiceRoleForSupport — esse perfil vinculado ao serviço é criado automaticamente e fornece as permissões necessárias para o atendente de investigação.

Permissões obrigatórias

Para criar casos com o suporte da AWS e ter acesso aos resultados das investigações, a entidade principal do IAM precisa das seguintes permissões:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": [
                "security-ir:CreateCase",
                "security-ir:GetCase",
                "security-ir:ListCases",
                "security-ir:UpdateCase"
            ],
            "Resource": "*"
        }
    ]
}
```

Como usar o atendente investigativo

O atendente investigativo de IA é ativado automaticamente ao criar um caso suportado pela AWS.

Para monitorar o progresso da investigação de IA

1. Abra seu caso no console AWS Security Incident Response.
2. Escolha a guia Investigação.
3. Visualize o status da investigação (Em andamento ou Concluída).
4. Depois disso, revise o resumo abrangente da investigação com as descobertas, o cronograma e as recomendações.

Aviso de IA responsável

Os resumos das investigações são gerados usando recursos de IA generativa da AWS. Você é responsável por avaliar as recomendações geradas pela IA em seu contexto específico, implementar mecanismos de supervisão apropriados, verificar as descobertas de forma independente e manter a supervisão humana de todas as decisões de segurança.

Uso de dados do cliente

O agente de investigação por IA não usa dados de clientes para treinamento de modelo nem compartilha dados de clientes com terceiros.

Contenção

O AWS Security Incident Response é seu parceiro na contenção de eventos. Em resposta às descobertas de segurança, você pode configurar o serviço para realizar ações de contenção proativa

em sua conta. Você também pode fazer a contenção por conta própria ou em parceria com entidades externas usando os documentos do SSM descritos em Ações de contenção compatíveis.

> **Important**
>
> O AWS Security Incident Response não habilita os recursos de contenção por padrão. São necessárias duas etapas para habilitar recursos de contenção proativa:
>
> 1. Conceda as permissões necessárias ao serviço usando perfis do IAM. Você pode criar esses perfis individualmente em cada conta ou para toda a organização trabalhando com os stacksets do AWS CloudFormation, que criam os perfis necessários.
> 2. Defina suas preferências de contenção conta a conta ou em toda a organização para autorizar ações de contenção proativas. As preferências em nível da conta têm precedência sobre as preferências em nível da organização. Isso pode ser feito criando um caso do AWS Support (Técnico: Serviço Security Incident Response/Outro). As preferências de contenção disponíveis são:
>   - Aprovação necessária (padrão): não faça contenção proativa de nenhum recurso sem autorização explícita, caso a caso.
>   - Conter confirmado: faça a contenção proativa de um recurso cujo comprometimento foi confirmado.
>   - Conter suspeito: faça a contenção proativa de um recurso com grande probabilidade de estar comprometido, com base em análise realizada pelo AWS Security Incident Response Engineering.

Tomada de decisões de contenção

Uma parte essencial da contenção é a tomada de decisões, como, por exemplo, desligar um sistema, isolar um recurso da rede, suspender acessos ou encerrar sessões. Essas decisões ficam mais fáceis quando há estratégias e procedimentos predeterminados para conter o evento. O AWS Security Incident Response fornece a estratégia de contenção, informa sobre os possíveis impactos e orienta sobre a implementação da solução somente depois que você analisou e aceitou os riscos envolvidos.

Ações de contenção compatíveis

A AWS Security Incident Response executa, em seu nome, ações de contenção compatíveis para acelerar a resposta e reduzir o tempo que um agente de ameaça pode dispor para causar

danos em seu ambiente. Essa funcionalidade permite mitigar ameaças identificadas com maior rapidez, minimizando os impactos potenciais e fortalecendo sua postura geral de segurança. Existem diferentes opções de contenção, dependendo dos recursos sendo analisados. As ações de contenção compatíveis são descritas nas subseções abaixo.

Contenção no EC2

A automação de contenção `AWSSupport-ContainEC2Instance` faz uma contenção de rede reversível de uma instância do EC2, mantendo a instância intacta e em execução, mas isolando-a de qualquer nova atividade de rede e impedindo-a de se comunicar com recursos internos e externos à VPC.

> **Important**
>
> É importante notar que as conexões rastreadas existentes não serão encerradas em resultado da alteração dos grupos de segurança. Apenas o tráfego futuro será, de fato, bloqueado pelo novo grupo de segurança e por este documento do SSM. Mais informações estão disponíveis na seção Contenção da origem no guia técnico do serviço.

Contenção no IAM

A automação de contenção `AWSSupport-ContainIAMPrincipal` faz uma contenção de rede reversível de um perfil ou usuário do IAM, mantendo o usuário ou perfil no IAM, mas isolando-o de qualquer comunicação com recursos na sua conta.

Contenção no S3

A automação de contenção `AWSSupport-ContainS3Resource` faz uma contenção de rede reversível de um bucket do S3, mantendo os objetos contidos no bucket e isolando o bucket ou o objeto do Amazon S3 por meio da modificação das suas políticas de acesso.

Desenvolver estratégias de contenção

A AWS Security Incident Response incentiva a definição de estratégias de contenção específicas para cada tipo principal de evento, alinhadas ao seu nível de tolerância ao risco. Documente critérios claros para auxiliar no processo de tomada de decisão durante um evento. Os critérios a serem considerados incluem:

- Potenciais danos aos recursos.
- Preservação de evidências e requisitos regulatórios.

- Indisponibilidade de serviços (por exemplo, conectividade de rede e serviços fornecidos para entidades externas).
- Tempo e recursos necessários para implementar a estratégia.
- Efetividade da estratégia (por exemplo, contenção parcial em comparação com a contenção total).
- Caráter permanente da solução (por exemplo, reversível em comparação com irreversível).
- Duração da solução (por exemplo, solução alternativa de emergência, solução alternativa temporária ou solução definitiva)

Aplique controles de segurança que possam reduzir o risco e dar tempo suficiente para a definição e implementação uma estratégia de contenção mais eficaz.

Abordagem de contenção em etapas

A AWS Security Incident Response recomenda uma abordagem em etapas para alcançar uma contenção eficiente e eficaz, envolvendo estratégias de curto e longo prazo, com base no tipo de recurso.

Estratégia de contenção

A AWS Security Incident Response consegue identificar o escopo do evento de segurança?

- Em caso afirmativo, realize a identificação de todos os recursos afetados (usuários, sistemas e recursos).
- Em caso negativo, realize a investigação simultaneamente à execução da próxima etapa nos recursos previamente identificados.

O recurso pode ser isolado?

- Em caso afirmativo, prossiga com o isolamento dos recursos afetados.
- Em caso negativo, colabore com os responsáveis pelos sistemas e gerentes para determinar as ações necessárias para a contenção do problema.

Todos os recursos afetados estão isolados dos recursos que não foram afetados?

- Em caso afirmativo, prossiga para a próxima etapa.
- Em caso negativo, continue realizando o isolamento dos recursos afetados para concluir a contenção a curto prazo e evitar que o incidente se agrave.

Backup do sistema

Foram criadas cópias de backup dos sistemas afetados para análises posteriores?

As cópias para análises forenses estão devidamente criptografadas e armazenadas em um local seguro?

- Em caso afirmativo, prossiga para a próxima etapa.
- Em caso negativo, criptografe as imagens para análises forenses e, em seguida, armazene-as em um local seguro para evitar uso acidental, danos e adulterações.

Enviar preferências de contenção

Para configurar preferências de contenção para sua conta ou organização, crie um caso do AWS Support.

No caso do suporte, especifique as seguintes informações:

Quando configurado, o AWS Security Incident Response executa as ações de contenção autorizadas durante os incidentes de segurança ativos para ajudar a proteger seu ambiente.

- Seu ID do AWS Organizations ou os IDs das contas específicas em que as ações de contenção devem ser autorizadas.
- Sua opção de contenção preferida.

> **Note**
>
> O AWS Security Incident Response executa ações de contenção apenas quando configurado com as preferências apropriadas e após a implantação do AWS CloudFormation StackSet requerido para conceder as permissões necessárias.

Erradicação

Durante a fase de erradicação, é importante identificar e tratar todas as contas, recursos e instâncias afetados, por exemplo, ao realizar a exclusão de malware, a remoção de contas de usuários comprometidas e a mitigação das vulnerabilidades descobertas, a fim de assegurar uma remediação uniforme em todo o ambiente.

É considerada uma prática recomendada adotar uma abordagem em fases para erradicação e recuperação, além de priorizar as etapas de remediação. O propósito das fases iniciais consiste em aumentar a segurança geral rapidamente (em dias ou semanas), implementando mudanças significativas para evitar incidentes futuros. As fases posteriores, por sua vez, podem se concentrar em alterações de longo prazo (por exemplo, mudanças na infraestrutura) e em trabalhos contínuos para manter a empresa o mais segura possível. Cada caso é único, e os engenheiros do AWS Security Incident Response trabalharão junto com você para avaliar as ações necessárias.

Considere o seguinte:

- É possível instalar novamente o sistema e reforçá-lo com patches ou outras medidas para prevenir ou reduzir o risco de ataques?
- É possível substituir o sistema infectado por uma nova instância ou por um novo recurso, possibilitando uma linha de base íntegra enquanto realiza o encerramento do item comprometido?
- Você realizou a remoção de todos os malwares e artefatos remanescentes do uso não autorizado, e os sistemas afetados foram reforçados contra novos ataques?
- Existe a necessidade de realizar uma análise forense nos recursos impactados?

Recuperar

A AWS Security Incident Response fornece orientações para ajudar na restauração dos sistemas à operação normal, confirmar que estão funcionando corretamente e remediar quaisquer vulnerabilidades, a fim de evitar eventos semelhantes no futuro. Ressalta-se que a AWS Security Incident Response não é responsável pela execução direta do processo de recuperação dos sistemas. As principais considerações incluem:

- Os sistemas afetados foram atualizados com patches e reforçados para prevenir reincidência do ataque recente?
- Qual é o prazo viável para restaurar os sistemas para o ambiente de produção?
- Quais ferramentas serão usadas para testar, monitorar e verificar os sistemas restaurados?

Relatório posterior ao incidente

A AWS Security Incident Response fornece um resumo do evento após a conclusão das atividades de segurança conduzidas em conjunto com sua equipe.

Ao final de cada mês, o serviço de AWS Security Incident Response enviará relatórios mensais para o ponto de contato principal de cada cliente por e-mail. Os relatórios serão fornecidos em um formato PDF, usando as métricas descritas abaixo. Os clientes receberão um relatório por AWS Organizations.

Métricas relacionadas ao caso

- Casos criados
  - Nome da dimensão: tipo
  - Valores da dimensão: com suporte por parte da AWS e com suporte próprio
  - Unidade: Contagem
  - Descrição: o número de casos criados.
- Casos encerrados
  - Nome da dimensão: tipo
  - Valores da dimensão: com suporte por parte da AWS e gerenciado por conta própria
  - Unidade: Contagem
  - Descrição: uma contagem do número total de casos encerrados.
- Casos em aberto
  - Nome da dimensão: tipo
  - Valores da dimensão: com suporte por parte da AWS e com suporte próprio
  - Unidade: Contagem
  - Descrição: o número de casos em aberto.

Métricas relacionadas à triagem

- Descobertas recebidas
  - Unidade: Contagem
  - Descrição: o número de descobertas enviadas para a triagem.
- Descobertas arquivadas
  - Unidade: Contagem
  - Descrição: o número de descobertas arquivadas após o processamento, sem necessidade de investigação manual.
- Descobertas com investigação manual

  - Unidade: Contagem
  - Descrição: o número de descobertas que passaram por investigação manual.
- Investigações arquivadas
  - Unidade: Contagem
  - Descrição: o número de investigações manuais que resultaram em falsos positivos e foram enviadas para o arquivamento.
- Investigações encaminhadas
  - Unidade: Contagem
  - Descrição: o número de investigações manuais que resultaram na identificação de um incidente de segurança.

Casos

A AWS Security Incident Response permite a criação de dois tipos de casos: os casos com suporte por parte da AWS ou os casos gerenciados por conta própria.

Criação de um caso com suporte por parte da AWS

É possível criar um caso com o suporte da AWS para o AWS Security Incident Response no Console, na API ou na AWS Command Line Interface. Os casos com suporte da AWS permitem que você receba suporte dos engenheiros do Security Incident Response.

> **Important**
>
> Casos de demonstração/simulação são encerrados depois de 90 dias.

> **Note**
>
> Os engenheiros do AWS Security Incident Response responderão ao seu caso em até 15 minutos. O tempo de resposta refere-se à primeira resposta dos engenheiros do AWS Security Incident Response. Empregaremos todos os esforços razoáveis para responder à sua solicitação inicial dentro desse período. O tempo de resposta mencionado não se aplica às respostas posteriores.

> **Note**
>
> Você pode criar casos com o suporte da AWS não apenas para incidentes e investigações de segurança ativos, mas também para consultas sobre os recursos do AWS Security Incident Response. Isso inclui perguntas sobre as regras de supressão, as configurações de triagem de alertas, os fluxos de trabalho de resposta proativa do GuardDuty e orientações gerais sobre postura de segurança. Selecione o tipo de caso Investigações e consultas para essas finalidades.

Quando entrar em contato com o AWS Security Incident Response

Você pode entrar em contato com o AWS Security Incident Response com diversas finalidades, dependendo de suas necessidades. A tabela a seguir descreve os diferentes cenários e o método de contato adequado para cada um deles.

Cenário	Quando usar	Tempo de resposta	Tipo de caso
Incidente de segurança ativo	Você tem um incidente de segurança urgente que requer suporte e serviços de resposta a incidentes imediatamente	15 minutos (primeira resposta)	Incidente de segurança ativo
Investigação	Você percebeu um incidente de segurança e precisa de suporte em análise de log e confirmação secundária de investigação de resposta a incidente	15 minutos (primeira resposta)	Investigações e consultas
Consultas e orientaçõ es	Você tem dúvidas sobre as descobertas, as regras de supressão, as configura ções de triagem de alertas, os fluxos de trabalho de resposta proativa do Amazon GuardDuty ou a postura geral	15 minutos (primeira resposta)	Investigações e consultas

Cenário	Quando usar	Tempo de resposta	Tipo de caso
	de segurança relacionada a recursos do AWS Security Incident Response		
Problemas de onboarding	Você tem problemas técnicos durante o processo de onboarding do AWS Security Incident Response	Varia de acordo com o plano de suporte	AWS Support Caso do

Em todos os casos com o suporte da AWS (Incidente ativo de segurança, e Investigações e consultas), os engenheiros do AWS Security Incident Response darão a primeira resposta em até 15 minutos . Esse tempo de resposta se aplica apenas ao contato inicial, não às respostas subsequentes.

O exemplo apresentado a seguir abrange o uso do console.

1. Faça login no AWS Security Incident Response usando o Console de gerenciamento da AWS.
2. Escolha Criar caso.
3. Escolha Resolver caso com a AWS.
4. Selecione o tipo de solicitação:
   a. Incidente de segurança ativo: esse tipo é para suporte e serviços de resposta a incidentes urgentes.
   b. Investigações e consultas: use esse tipo para incidentes de segurança percebidos nos quais os engenheiros do AWS Security Incident Response podem prestar suporte em análise de logs e confirmação secundária da investigação de resposta a incidente. Você pode também usar esse tipo para consultas sobre as descobertas, as regras de supressão, as configurações de triagem de alertas, os fluxos de trabalho de resposta proativa do Amazon GuardDuty e sobre a postura geral de segurança relacionada aos recursos do AWS Security Incident Response.
5. Defina a data estimada de início como a data do seu primeiro indicativo do incidente. Por exemplo, quando você percebeu um comportamento anormal pela primeira vez ou quando recebeu o primeiro alerta de segurança relacionado.
6. Informe um título para o caso.

7. Forneça uma descrição detalhada do caso. Considere os seguintes aspectos, que podem ajudar os responsáveis pela resposta a incidentes na resolução do caso:
   a. O que aconteceu?
   b. Quem descobriu e reportou o incidente?
   c. Quem são as pessoas que estão afetadas pelo caso?
   d. Qual é o impacto conhecido?
   e. Qual é a urgência deste caso?
   f. Adicione um ou mais IDs de Conta da AWS que estejam envolvidos no escopo do caso.
8. Adicione detalhes opcionais ao caso:
   a. Selecione os principais serviços impactados usando a lista suspensa.
   b. Selecione as principais regiões impactadas usando a lista suspensa.
   c. Adicione um ou mais endereços IP de agentes de ameaça que você identificou como parte deste caso.
9. Adicione, opcionalmente, responsáveis pela resposta a incidentes adicionais ao caso para receberem notificações. Para adicionar um indivíduo, execute as seguintes etapas:
   a. Adicione um endereço de e-mail.
   b. Adicione, opcionalmente, um nome e o sobrenome.
   c. Escolha Adicionar novo para adicionar outro indivíduo.
   d. Para remover um indivíduo, escolha a opção Remover correspondente.
   e. Escolha Adicionar para incluir todos os indivíduos listados no caso.
      i. Você pode selecionar diversos indivíduos e escolher Remover para excluí-los da lista.
10. Adicione etiquetas opcionais ao caso.
   a. Para adicionar uma tag, faça o seguinte:
   b. Selecione Adicionar nova tag.
   c. Em Chave, insira o nome da tag.
   d. Em Valor, insira o valor da tag.
   e. Para remover uma tag, clique na opção Remover da tag.

Após a criação de um caso com o suporte da AWS, os engenheiros do AWS Security Incident Response e sua equipe de resposta a incidentes são notificadas imediatamente.

Para criar um caso suportado pela AWS com a investigação de IA

1. Abra o console do AWS Security Incident Response em console.aws.amazon.com/.
2. Escolha Casos no painel de navegação.
3. Escolha Criar caso.
4. Em Tipo de caso, selecione caso suportado pela AWS.
5. Forneça detalhes do caso, incluindo título, data de início do incidente e ID da conta AWS afetada.
6. Na seção Descreva o evento de segurança, forneça uma descrição completa do incidente.
7. Forneça informações adicionais sobre os serviços da AWS afetados, regiões e outros detalhes relevantes.
8. Escolha Criar caso.

Após a criação de um caso, os engenheiros do Security Incident Response e o agente de IA começam a trabalhar simultaneamente.

Para responder às perguntas de esclarecimento da IA (opcional)

1. Navegue até a guia Investigação em seu caso.
2. Analise as perguntas de esclarecimento apresentadas pelo agente de IA.
3. Responda às perguntas ou escolha Ignorar se preferir não responder.
4. Escolha Enviar para continuar. Todos os campos são opcionais.

Aviso de IA responsável

Os resumos das investigações são gerados usando recursos de IA generativa da AWS. Você é responsável por avaliar as recomendações geradas pela IA em seu contexto específico, implementar mecanismos de supervisão apropriados, verificar as descobertas de forma independente e manter a supervisão humana de todas as decisões de segurança.

Criação de um caso gerenciado por conta própria

Você pode criar um caso gerenciado por conta própria para a AWS Security Incident Response por meio do Console, da API ou da AWS Command Line Interface. Esse tipo de caso NÃO envolve engenheiros do AWS Security Incident Response. O exemplo apresentado a seguir abrange o uso do console.

1. Faça login no AWS Security Incident Response via Console de gerenciamento da AWS em https://console.aws.amazon.com/security-ir/.

2. Escolha Criar caso.
3. Escolha Resolver caso com minha própria equipe de resposta a incidentes.
4. Defina a data estimada de início como a data do seu primeiro indicativo do incidente. Por exemplo, quando você percebeu um comportamento anormal pela primeira vez ou quando recebeu o primeiro alerta de segurança relacionado.
5. Informe um título para o caso. É recomendado incluir os dados no título do caso, conforme a sugestão fornecida ao selecionar a opção Gerar título.
6. Insira os IDs de Conta da AWS que fazem parte do caso. Para adicionar um ID de conta, execute as seguintes etapas:
   a. Insira o ID da conta, que contém 12 dígitos, e escolha Adicionar conta.
   b. Para remover uma conta, selecione Remover ao lado da conta que deseja remover do caso.
7. Forneça uma descrição detalhada do caso.
   a. Considere os seguintes aspectos, que podem ajudar os responsáveis pela resposta a incidentes na resolução do caso:
      i. O que aconteceu?
      ii. Quem descobriu e reportou o incidente?
      iii. Quem são as pessoas que estão afetadas pelo caso?
      iv. Qual é o impacto conhecido?
      v. Qual é a urgência deste caso?
8. Adicione detalhes opcionais ao caso:
   a. Selecione os principais serviços impactados usando a lista suspensa.
   b. Selecione as principais regiões impactadas usando a lista suspensa.
   c. Adicione um ou mais endereços IP de agentes de ameaça que você identificou como parte deste caso.
9. Adicione, opcionalmente, responsáveis pela resposta a incidentes adicionais ao caso para receberem notificações. Para adicionar um indivíduo, execute as seguintes etapas:
   a. Adicione um endereço de e-mail.
   b. Adicione, opcionalmente, um nome e o sobrenome.
   c. Escolha Adicionar novo para adicionar outro indivíduo.
   d. Para remover um indivíduo, escolha a opção Remover correspondente.
   e. Escolha Adicionar para incluir todos os indivíduos listados no caso. Você pode selecionar diversos indivíduos e escolher Remover para excluí-los da lista.

10 Adicione etiquetas opcionais ao caso. Para adicionar uma tag, faça o seguinte:

   a. Selecione Adicionar nova tag.
   b. Em Chave, insira o nome da tag.
   c. Em Valor, insira o valor da tag.
   d. Para remover uma tag, clique na opção Remover da tag.

Após a criação do caso, a equipe de resposta a incidentes receberá uma notificação por e-mail.

Trabalhar com os engenheiros do AWS Security Incident Response

Depois que você abre um caso de incidente de segurança, os engenheiros do AWS Security Incident Response começam a trabalhar no incidente. Esta seção explica o que esperar durante a investigação e como colaborar de modo eficaz com nossa equipe.

O que esperar dos engenheiros do AWS Security Incident Response

Quando você abre um caso com o suporte da AWS, um engenheiro do Security Incident Response é designado para o incidente. O respondente designado:

- Revisa as informações iniciais que você forneceu sobre o caso
- Analisa os logs de serviço da AWS e as descobertas de segurança relevantes
- Identifica o escopo e o impacto do incidente de segurança
- Desenvolve um plano de investigação e resposta específico para a situação

Cronograma de resposta: o objetivo do nível de serviço (SLO) para o reconhecimento de novos casos pelos engenheiros da AWS Security Incident Response é de 15 minutos. O cronograma da avaliação inicial pode variar com base na gravidade e complexidade do caso. Se os engenheiros da AWS Security Incident Response não receberem uma resposta ou informações críticas de você dentro de 5 dias úteis, o caso será encerrado.

Fluxo de trabalho de investigação

Os engenheiros do AWS Security Incident Response seguem um processo estruturado de resposta a incidentes alinhado com a estrutura NIST 800-61r2. Durante sua investigação, as seguintes fases são esperadas:

1. Triagem inicial: os engenheiros do Security Incident Response analisam os detalhes do caso e confirmam o escopo do incidente

2. Investigação: os engenheiros do Security Incident Response analisam os logs, identificam os indicadores de comprometimento e determinam a causa primária
3. Contenção: os engenheiros do Security Incident Response recomendam ações para limitar o impacto do incidente
4. Erradicação e recuperação: os engenheiros do Security Incident Response ajudam a remover as ameaças e restaurar as operações normais
5. Análise pós-incidente: os engenheiros do Security Incident Response apresentam as descobertas e as recomendações para evitar futuros incidentes

Durante essas fases, o engenheiro de Security Incident Response mantém você informado por meio de atualizações do caso e pode solicitar informações ou ações adicionais.

Os engenheiros do Information Security Incident Response podem solicitar

Para investigar o incidente de forma eficaz, os engenheiros do AWS Security Incident Response podem solicitar:

- Detalhes cronológicos: quando você detectou pela primeira vez o incidente e quaisquer eventos relevantes que o antecederam
- Recursos afetados: IDs de contas, serviços, regiões específicas da AWS, e ARNs dos recursos envolvidos
- Informações de acesso: detalhes sobre quem tem acesso aos recursos afetados e qualquer alteração de acesso recente
- Contexto de negócios: como os recursos afetados são usados e o possível impacto nos negócios
- Logs e evidências: outros logs, capturas de tela ou artefatos que possam ajudar na investigação
- Autorização: aprovação para realizar ações específicas de contenção ou remediação para você

O engenheiro do Security Incident Response explicará por que cada informação é necessária e como ela ajudará na investigação.

Práticas recomendadas de comunicação

A comunicação eficaz acelera a resolução dos incidentes. Siga estas práticas ao trabalhar com engenheiros do AWS Security Incident Response:

- Responda prontamente às solicitações de informação feitas pelo engenheiro do Security Incident Response

- Forneça informações completas, mesmo que não tenha certeza de sua relevância
- Faça perguntas se não entender uma recomendação ou precisar de esclarecimentos
- Atualize o caso com qualquer novo desenvolvimento ou alteração no incidente
- Designe um contato principal de sua equipe para coordenar com os engenheiros do Security Incident Response

> **Important**
>
> Se os engenheiros da AWS Security Incident Response não receberem uma resposta às solicitações de informações críticas dentro de 5 dias úteis, procederemos ao encerramento do caso. É possível reabrir um caso se novas informações ficarem disponíveis.

Seu papel durante a investigação

Embora os engenheiros da AWS Security Incident Response conduzam a investigação, sua participação é essencial. Você é responsável por realizar as seguintes ações:

- Fornecer respostas às solicitações de informação prontamente
- Implementar as ações recomendadas de contenção e remediação em seu ambiente da AWS
- Autorizar os engenheiros da Resposta a Incidentes de Segurança a realizar ações para você (se a resposta proativa foi habilitada)
- Coordenar com suas equipes internas (segurança, jurídica, conformidade) conforme necessário
- Tomar decisões de negócios sobre prioridades e escolhas compensatórias nas respostas aos incidentes

Os engenheiros da AWS Security Incident Response oferecem expertise e recomendações, mas você mantém o controle de seus recursos da AWS e toma as decisões finais sobre as ações de resposta.

Encerramento do caso

Os engenheiros da AWS Security Incident Response encerram seu caso quando:

- O incidente foi contido e remediado
- Todos os resultados da investigação foram compartilhados com você

- Nenhuma assistência adicional do engenheiro do Security Incident Response é necessária
- Você solicita o encerramento do caso

Antes de encerrar um caso, o engenheiro do Security Incident Response fornece um resumo das descobertas, ações realizadas e recomendações para melhorar a postura de segurança.

Se precisar de assistência adicional após o encerramento do caso, você pode abrir um novo caso ou entrar em contato com o AWS Support.

Como responder a um caso gerado pela AWS

A AWS Security Incident Response pode criar uma notificação externa ou abrir um caso quando for necessário que você realize alguma ação ou esteja ciente de algo que possa impactar sua conta ou seus recursos. Isso só ocorre se você tiver habilitado os fluxos de trabalho de resposta proativa e triagem de alertas como parte da sua assinatura.

Essas notificações é apresentada como casos de Resposta a Incidentes de Segurança com o prefixo “[Caso proativo]” no console de AWS Security Incident Response. Para visualizar e gerenciar esses casos, conclua as seguintes etapas:

- Acesse o console de Resposta a Incidentes de Segurança em https://console.aws.amazon.com/security-ir/.
- Escolha Casos.
- Você vê todos os casos, incluindo aqueles com o prefixo "[Caso proativo]".

É possível atualizar, resolver e reabrir esses casos conforme necessário. É possível se comunicar diretamente com a equipe de AWS Security Incident Response por meio desses casos, garantindo um tratamento eficiente de possíveis questões de segurança.

Gerenciamento de casos

Conteúdo

- Comunicações
- Permissões
- Anexos
- Tags
- Atividades relacionadas ao caso
- Encerramento de um caso

Alteração do status de um caso

Um caso encontra-se em um dos seguintes estados:

- Enviado: representa o status inicial de um caso. Os casos com este status foram enviados por um solicitante, mas ainda não estão sendo processados.
- Detecção e análise: este status indica que o responsável pela resposta a incidentes começou a trabalhar no caso. Esta fase inclui a coleta de dados, a triagem do evento e a realização de análises para formular conclusões orientadas por dados.
- Contenção, erradicação e recuperação: neste status, o responsável pela resposta a incidentes identificou uma atividade suspeita que exige esforços adicionais para ser removida. O responsável pela resposta a incidentes fornecerá recomendações para você executar a análise de riscos ao negócio e a implementação de ações adicionais. Se os recursos opcionais para o serviço estiverem habilitados, o responsável pela resposta a incidentes da AWS solicitará seu consentimento para executar as ações de contenção usando documentos do SSM nas contas impactadas.
- Atividades posteriores ao incidente: neste status, o evento de segurança principal foi contido. O foco passa a ser a recuperação e o restabelecimento das operações empresariais ao seu estado normal. Um resumo e a análise da causa-raiz serão fornecidos, desde que o responsável pela resolução do caso seja a AWS.
- Encerrado: este é o status final do fluxo de trabalho. Os casos com status “encerrado” indicam que o trabalho foi totalmente concluído. Não é possível reabrir casos encerrados, portanto, assegure-se de que todas as ações estejam devidamente finalizadas antes de aplicar essa alteração de status.

Selecione Ação: atualizar status para alterar o status do caso em casos gerenciados por conta própria. Nos casos com o suporte da AWS, o status é definido pelos engenheiros do AWS Security Incident Response.

Alteração do responsável

Para casos gerenciados por conta própria, sua equipe de resposta a incidentes pode solicitar ajuda da AWS. Escolha Obtenha ajuda da AWS para alterar o responsável pelo caso para a AWS. Após a atualização do caso para “suporte por parte da AWS”, o status será alterado para Enviado. O histórico do caso existente ficará disponível para os engenheiros do AWS Security Incident Response. Uma vez solicitada a ajuda da AWS, não será possível retornar o caso ao gerenciamento próprio.

Itens de ação

Um engenheiro do AWS Security Incident Response designado para trabalhar no caso pode solicitar ações de sua equipe interna.

Após a criação de um caso, os itens de ações que podem ser solicitados incluem:

- Solicitação para conceder permissões a um responsável pela resposta a incidentes para acesso a um caso
- Solicitação para fornecer informações adicionais sobre o caso

Quando um caso está pronto para ser encerrado, os itens de ação incluem:

- Solicitação para analisar o relatório do caso
- Solicitação para encerrar o caso

Editar um caso

Selecione Editar para alterar os detalhes de um caso.

Para casos com suporte por parte da AWS e casos gerenciados por conta própria:

É possível alterar os seguintes detalhes referentes ao caso após a criação do caso:

- Cargo
- Descrição

Somente para casos com suporte por parte da AWS:

É possível alterar os campos adicionais:

- Tipos de solicitação:
  - Incidente de segurança ativo: este tipo é destinado ao suporte e aos serviços urgentes de resposta a incidentes.
  - Investigações: as investigações permitem obter suporte em incidentes de segurança percebidos, nos quais os engenheiros do AWS Security Incident Response podem prestar suporte para análise de logs e confirmação secundária de evento de segurança.
- Estimativa da data de início: altere este campo caso tenha identificado indicadores relacionados ao caso que antecedem a data de início inicialmente informada. Considere fornecer detalhes adicionais sobre o novo indicador detectado no campo de descrição ou adicione um comentário na guia de comunicações.

Comunicações

Os engenheiros do AWS Security Incident Response podem adicionar comentários para documentar suas atividades ao trabalharem em um caso. Vários engenheiros do AWS Security Incident Response podem trabalhar em um caso ao mesmo tempo. Esses profissionais são identificados como responsáveis da AWS no log de comunicações.

Permissões

A guia Permissões lista todos os indivíduos que receberão notificações em caso de qualquer alteração no caso. Você pode adicionar e remover indivíduos da lista até que o caso seja encerrado.

> **Note**
>
> Os casos individuais permitem a inclusão de até 30 partes interessadas no total. É necessário configurar permissões adicionais para conceder acesso em nível de caso a essas partes interessadas.

Fornecimento de acesso a um caso no Console

Para fornecer acesso ao caso no Console de gerenciamento da AWS, você pode copiar o modelo de política de permissões do IAM e adicionar essa permissão para um usuário ou perfil.

Como adicionar a política do IAM para um usuário ou para um perfil:

1. Copie a política de permissões do IAM.
2. Acesse o IAM em https://console.aws.amazon.com/iam/.
3. No painel de navegação, selecione Usuários ou Perfis.
4. Selecione um usuário ou um perfil para abrir a página de detalhes.
5. Na guia Permissões, escolha Adicionar permissões.
6. Escolha Anexar política.
7. Selecione a política gerenciada da AWS Security Incident Response mais apropriada.
8. Escolha Add policy.

Anexos

Em casos gerenciados por conta própria, seus responsáveis pela resposta a incidentes podem adicionar anexos ao caso para apoiar outros profissionais responsáveis pela resposta a incidentes durante a investigação.

> **Note**
>
> Nos casos com suporte por parte da AWS, a AWS não pode visualizar os anexos. Todos os detalhes relacionados a casos com suporte por parte da AWS devem ser compartilhados por meio de comentários no caso ou fornecidos por compartilhamento de tela usando a tecnologia de comunicação de sua preferência.

Escolha Fazer upload para selecionar um arquivo do seu computador para ser adicionado ao caso.

> **Note**
>
> Todos os anexos enviados serão excluídos sete dias após um caso ter sido `Closed`.

Tags

Uma etiqueta consiste em um rótulo opcional que você pode atribuir para os seus casos com a finalidade de armazenar metadados sobre esse recurso. Cada tag é um rótulo que consiste em uma chave e um valor opcional. Você pode usar etiquetas para pesquisar, alocar custos e autenticar permissões para o recurso.

Para adicionar uma tag, faça o seguinte:

1. Selecione Adicionar nova tag.
2. Em Chave, insira o nome da tag.
3. Em Valor, insira o valor da tag.

Para remover uma tag, clique na opção Remover da tag.

Atividades relacionadas ao caso

As trilhas de auditoria fornecem registros cronológicos detalhados de todas as atividades relacionadas ao caso. As trilhas oferecem informações importantes para atividades posteriores ao evento e auxiliam na identificação de possíveis melhorias. O horário, o usuário, a ação e os detalhes de qualquer alteração no caso são registrados em log na trilha de auditoria do caso.

Encerramento de um caso

Para casos com suporte por parte da AWS, selecione Encerrar caso na página de detalhes do caso para encerrá-lo permanentemente, independentemente do status atual. Normalmente, um caso atinge o status Pronto para encerrar antes de ser encerrado permanentemente. Se encerrar prematuramente um caso com status que não for Pronto para encerrar, você estará solicitando que os engenheiros do AWS Security Incident Response interrompam o trabalho nesse caso com o suporte da AWS.

Se a sua equipe de resposta a incidentes for a responsável, selecione Ação: encerrar caso na página de detalhes do caso.

> **Note**
>
> O status “Pronto para encerrar” indica que um caso pode ser encerrado permanentemente e que não há trabalho adicional a ser feito em um caso.

Um caso não poderá ser reaberto após ter sido encerrado permanentemente. Todas as informações ficarão disponíveis somente para leitura. Para evitar o encerramento acidental, você receberá uma notificação para confirmar que deseja encerrar o caso.

Trabalhar com o CloudFormation StackSets

Para obter instruções específicas sobre como criar um StackSet com permissões gerenciadas pelo serviço, consulte Criar CloudFormation StackSets com permissões gerenciadas pelo serviço no Guia do usuário do AWS CloudFormation.

O AWS Security Incident Response fornece dois modelos do CloudFormation. Ambos os modelos criam os mesmos dois perfis do AWS Identity and Access Management, `AWSSecurityIncidentResponseContainment` e `AWSSecurityIncidentResponseContainmentExecution`. O modelo Contenção com o EC2 Triage adiciona o `AWSSecurityIncidentResponseInvestigationPolicy` ao perfil do `AWSSecurityIncidentResponseContainment`, o que concede permissões adicionais para o EC2 Triage. Escolha o modelo que corresponde aos seus requisitos de segurança:

- Somente contenção: cria as permissões mínimas necessárias para ações de contenção.
- Contenção com EC2 Triage: inclui todas as permissões de contenção, além de permissões adicionais para EC2 Triage. Esse modelo permite ao AWS Security Incident Response executar o Run Command do AWS Systems Manager em suas instâncias do Amazon Elastic Compute Cloud durante investigações de segurança.

Para obter mais informações sobre o EC2 Triage, consulte Detecção e análise.

Modelos do CloudFormation

Os modelos a seguir criam os perfis do IAM necessários para as ações de contenção do AWS Security Incident Response. Escolha o modelo que melhor atenda aos seus requisitos de segurança.

Conteúdo

Apenas contenção

Este modelo cria os perfis mínimos necessários para ações de contenção. Use este modelo se você não precisar da funcionalidade do EC2 Triage.

```
AWSTemplateFormatVersion: '2010-09-09'
Description: 'Template for production SIR containment roles'
```

```
Resources:
  AWSSecurityIncidentResponseContainment:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSSecurityIncidentResponseContainment
      AssumeRolePolicyDocument:
        {
          'Version': '2012-10-17',
          'Statement':
            [
              {
                'Effect': 'Allow',
                'Principal': { 'Service': 'containment.security-ir.amazonaws.com' },
                'Action': 'sts:AssumeRole',
                'Condition': { 'StringEquals': { 'sts:ExternalId': !Sub
 '${AWS::AccountId}' } },
              },
              {
                'Effect': 'Allow',
                'Principal': { 'Service': 'containment.security-ir.amazonaws.com' },
                'Action': 'sts:TagSession',
              },
            ],
        }
      Policies:
        - PolicyName: AWSSecurityIncidentResponseContainmentPolicy
          PolicyDocument:
            {
              'Version': '2012-10-17',
              'Statement':
                [
                  {
                    'Effect': 'Allow',
                    'Action': ['ssm:StartAutomationExecution'],
                    'Resource':
                      [
                        !Sub 'arn:${AWS::Partition}:ssm:*::document/AWSSupport-
ContainEC2Instance',
                        !Sub 'arn:${AWS::Partition}:ssm:*::document/AWSSupport-
ContainS3Resource',
                        !Sub 'arn:${AWS::Partition}:ssm:*::document/AWSSupport-
ContainIAMPrincipal',
```

```
                        !Sub 'arn:${AWS::Partition}:ssm:*:${AWS::AccountId}:automation-
execution/*',
                    ],
                },
                {
                  'Effect': 'Allow',
                  'Action':
                    ['ssm:DescribeInstanceInformation', 'ssm:GetAutomationExecution',
 'ssm:ListCommandInvocations'],
                  'Resource': '*',
                },
                {
                  'Effect': 'Allow',
                  'Action': ['iam:PassRole'],
                  'Resource': !GetAtt
 AWSSecurityIncidentResponseContainmentExecution.Arn,
                  'Condition': { 'StringEquals': { 'iam:PassedToService':
 'ssm.amazonaws.com' } },
                },
              ],
          }
  AWSSecurityIncidentResponseContainmentExecution:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSSecurityIncidentResponseContainmentExecution
      AssumeRolePolicyDocument:
        {
          'Version': '2012-10-17',
          'Statement':
            [{ 'Effect': 'Allow', 'Principal': { 'Service': 'ssm.amazonaws.com' },
 'Action': 'sts:AssumeRole' }],
        }
      ManagedPolicyArns:
        - !Sub arn:${AWS::Partition}:iam::aws:policy/SecurityAudit
      Policies:
        - PolicyName: AWSSecurityIncidentResponseContainmentExecutionPolicy
          PolicyDocument:
            {
              'Version': '2012-10-17',
              'Statement':
                [
                  {
                    'Sid': 'AllowIAMContainment',
                    'Effect': 'Allow',
```

```
                'Action':
                  [
                    'iam:AttachRolePolicy',
                    'iam:AttachUserPolicy',
                    'iam:DeactivateMFADevice',
                    'iam:DeleteLoginProfile',
                    'iam:DeleteRolePolicy',
                    'iam:DeleteUserPolicy',
                    'iam:GetLoginProfile',
                    'iam:GetPolicy',
                    'iam:GetRole',
                    'iam:GetRolePolicy',
                    'iam:GetUser',
                    'iam:GetUserPolicy',
                    'iam:ListAccessKeys',
                    'iam:ListAttachedRolePolicies',
                    'iam:ListAttachedUserPolicies',
                    'iam:ListMfaDevices',
                    'iam:ListPolicies',
                    'iam:ListRolePolicies',
                    'iam:ListUserPolicies',
                    'iam:ListVirtualMFADevices',
                    'iam:PutRolePolicy',
                    'iam:PutUserPolicy',
                    'iam:TagMFADevice',
                    'iam:TagPolicy',
                    'iam:TagRole',
                    'iam:TagUser',
                    'iam:UntagMFADevice',
                    'iam:UntagPolicy',
                    'iam:UntagRole',
                    'iam:UntagUser',
                    'iam:UpdateAccessKey',
                    'identitystore:CreateGroupMembership',
                    'identitystore:DeleteGroupMembership',
                    'identitystore:IsMemberInGroups',
                    'identitystore:ListUsers',
                    'identitystore:ListGroups',
                    'identitystore:ListGroupMemberships',
                  ],
                'Resource': '*',
              },
              {
                'Sid': 'AllowOrgListAccounts',
```

```
                    'Effect': 'Allow',
                    'Action': 'organizations:ListAccounts',
                    'Resource': '*',
                  },
                  {
                    'Sid': 'AllowSSOContainment',
                    'Effect': 'Allow',
                    'Action':
                      [
                        'sso:CreateAccountAssignment',
                        'sso:DeleteAccountAssignment',
                        'sso:DeleteInlinePolicyFromPermissionSet',
                        'sso:GetInlinePolicyForPermissionSet',
                        'sso:ListAccountAssignments',
                        'sso:ListInstances',
                        'sso:ListPermissionSets',
                        'sso:ListPermissionSetsProvisionedToAccount',
                        'sso:PutInlinePolicyToPermissionSet',
                        'sso:TagResource',
                        'sso:UntagResource',
                      ],
                    'Resource': '*',
                  },
                  {
                    'Sid': 'AllowSSORead',
                    'Effect': 'Allow',
                    'Action': ['sso-directory:SearchUsers', 'sso-
directory:DescribeUser'],
                    'Resource': '*',
                  },
                  {
                    'Sid': 'AllowS3Read',
                    'Effect': 'Allow',
                    'Action':
                      [
                        's3:GetAccountPublicAccessBlock',
                        's3:GetBucketAcl',
                        's3:GetBucketLocation',
                        's3:GetBucketOwnershipControls',
                        's3:GetBucketPolicy',
                        's3:GetBucketPolicyStatus',
                        's3:GetBucketPublicAccessBlock',
                        's3:GetBucketTagging',
                        's3:GetEncryptionConfiguration',
```

```
            's3:GetObject',
            's3:GetObjectAcl',
            's3:GetObjectTagging',
            's3:GetReplicationConfiguration',
            's3:ListBucket',
            's3express:GetBucketPolicy',
          ],
        'Resource': '*',
      },
      {
        'Sid': 'AllowS3Write',
        'Effect': 'Allow',
        'Action':
          [
            's3:CreateBucket',
            's3:DeleteBucketPolicy',
            's3:DeleteObjectTagging',
            's3:PutAccountPublicAccessBlock',
            's3:PutBucketACL',
            's3:PutBucketOwnershipControls',
            's3:PutBucketPolicy',
            's3:PutBucketPublicAccessBlock',
            's3:PutBucketTagging',
            's3:PutBucketVersioning',
            's3:PutObject',
            's3:PutObjectAcl',
            's3express:CreateSession',
            's3express:DeleteBucketPolicy',
            's3express:PutBucketPolicy',
          ],
        'Resource': '*',
      },
      {
        'Sid': 'AllowAutoScalingWrite',
        'Effect': 'Allow',
        'Action':
          [
            'autoscaling:CreateOrUpdateTags',
            'autoscaling:DeleteTags',
            'autoscaling:DescribeAutoScalingGroups',
            'autoscaling:DescribeAutoScalingInstances',
            'autoscaling:DescribeTags',
            'autoscaling:EnterStandby',
            'autoscaling:ExitStandby',
```

```
                'autoscaling:UpdateAutoScalingGroup',
              ],
            'Resource': '*',
          },
          {
            'Sid': 'AllowEC2Containment',
            'Effect': 'Allow',
            'Action':
              [
                'ec2:AuthorizeSecurityGroupEgress',
                'ec2:AuthorizeSecurityGroupIngress',
                'ec2:CopyImage',
                'ec2:CreateImage',
                'ec2:CreateSecurityGroup',
                'ec2:CreateSnapshot',
                'ec2:CreateTags',
                'ec2:DeleteSecurityGroup',
                'ec2:DeleteTags',
                'ec2:DescribeImages',
                'ec2:DescribeInstances',
                'ec2:DescribeSecurityGroups',
                'ec2:DescribeSnapshots',
                'ec2:DescribeTags',
                'ec2:ModifyNetworkInterfaceAttribute',
                'ec2:RevokeSecurityGroupEgress',
              ],
            'Resource': '*',
          },
          {
            'Sid': 'AllowKMSActions',
            'Effect': 'Allow',
            'Action':
              [
                'kms:CreateGrant',
                'kms:DescribeKey',
                'kms:GenerateDataKeyWithoutPlaintext',
                'kms:ReEncryptFrom',
                'kms:ReEncryptTo',
              ],
            'Resource': '*',
          },
          {
            'Sid': 'AllowSSMActions',
            'Effect': 'Allow',
```

```
                    'Action': ['ssm:DescribeAutomationExecutions'],
                    'Resource': '*',
                  },
                ],
            }
```

Contenção com o EC2 Triage

Este modelo cria perfis de contenção com permissões adicionais para a funcionalidade do EC2 Triage. Use esse modelo se precisar do AWS Security Incident Response para executar o Run Command do Systems Manager nas instâncias do Amazon EC2 durante investigações de segurança.

```
AWSTemplateFormatVersion: '2010-09-09'
Description: 'Template for AWS Security Incident Response containment roles'

Resources:
  AWSSecurityIncidentResponseContainment:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSSecurityIncidentResponseContainment
      AssumeRolePolicyDocument:
        {
          'Version': '2012-10-17',
          'Statement':
            [
              {
                'Effect': 'Allow',
                'Principal': { 'Service': 'containment.security-ir.amazonaws.com' },
                'Action': 'sts:AssumeRole',
                'Condition': { 'StringEquals': { 'sts:ExternalId': !Sub
 '${AWS::AccountId}' } },
              },
              {
                'Effect': 'Allow',
                'Principal': { 'Service': 'containment.security-ir.amazonaws.com' },
                'Action': 'sts:TagSession',
              },
            ],
        }
      Policies:
        - PolicyName: AWSSecurityIncidentResponseContainmentPolicy
```

```
          PolicyDocument:
            {
              'Version': '2012-10-17',
              'Statement':
                [
                  {
                    'Effect': 'Allow',
                    'Action': ['ssm:StartAutomationExecution'],
                    'Resource':
                      [
                        !Sub 'arn:${AWS::Partition}:ssm:*::document/AWSSupport-
ContainEC2Instance',
                        !Sub 'arn:${AWS::Partition}:ssm:*::document/AWSSupport-
ContainS3Resource',
                        !Sub 'arn:${AWS::Partition}:ssm:*::document/AWSSupport-
ContainIAMPrincipal',
                        !Sub 'arn:${AWS::Partition}:ssm:*:${AWS::AccountId}:automation-
execution/*',
                      ],
                  },
                  {
                    'Effect': 'Allow',
                    'Action':
                      ['ssm:DescribeInstanceInformation', 'ssm:GetAutomationExecution',
 'ssm:ListCommandInvocations'],
                    'Resource': '*',
                  },
                  {
                    'Effect': 'Allow',
                    'Action': ['iam:PassRole'],
                    'Resource': !GetAtt
 AWSSecurityIncidentResponseContainmentExecution.Arn,
                    'Condition': { 'StringEquals': { 'iam:PassedToService':
 'ssm.amazonaws.com' } },
                  },
                ],
            }
        - PolicyName: AWSSecurityIncidentResponseInvestigationPolicy
          PolicyDocument:
            {
              'Version': '2012-10-17',
              'Statement':
                [
                  {
```

```
                    'Effect': 'Allow',
                    'Action': [
                      'ec2:DescribeInstanceStatus',
                      'ec2:DescribeInstances',
                      'ec2:DescribeRouteTables',
                      'ec2:DescribeSecurityGroupRules',
                      'iam:GetInstanceProfile',
                      'ssm:DescribeInstanceInformation',
                      'ssm:GetCommandInvocation'
                    ],
                    'Resource': '*'
                  },
                  {
                    'Effect': 'Allow',
                    'Action': [
                      'ssm:SendCommand'
                    ],
                    'Resource': '*'
                  }
                ]
              }
  AWSSecurityIncidentResponseContainmentExecution:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSSecurityIncidentResponseContainmentExecution
      AssumeRolePolicyDocument:
        {
          'Version': '2012-10-17',
          'Statement':
            [{ 'Effect': 'Allow', 'Principal': { 'Service': 'ssm.amazonaws.com' },
'Action': 'sts:AssumeRole' }],
        }
      ManagedPolicyArns:
        - !Sub arn:${AWS::Partition}:iam::aws:policy/SecurityAudit
      Policies:
        - PolicyName: AWSSecurityIncidentResponseContainmentExecutionPolicy
          PolicyDocument:
            {
              'Version': '2012-10-17',
              'Statement':
                [
                  {
                    'Sid': 'AllowIAMContainment',
                    'Effect': 'Allow',
```

```
                'Action':
                  [
                    'iam:AttachRolePolicy',
                    'iam:AttachUserPolicy',
                    'iam:DeactivateMFADevice',
                    'iam:DeleteLoginProfile',
                    'iam:DeleteRolePolicy',
                    'iam:DeleteUserPolicy',
                    'iam:GetLoginProfile',
                    'iam:GetPolicy',
                    'iam:GetRole',
                    'iam:GetRolePolicy',
                    'iam:GetUser',
                    'iam:GetUserPolicy',
                    'iam:ListAccessKeys',
                    'iam:ListAttachedRolePolicies',
                    'iam:ListAttachedUserPolicies',
                    'iam:ListMfaDevices',
                    'iam:ListPolicies',
                    'iam:ListRolePolicies',
                    'iam:ListUserPolicies',
                    'iam:ListVirtualMFADevices',
                    'iam:PutRolePolicy',
                    'iam:PutUserPolicy',
                    'iam:TagMFADevice',
                    'iam:TagPolicy',
                    'iam:TagRole',
                    'iam:TagUser',
                    'iam:UntagMFADevice',
                    'iam:UntagPolicy',
                    'iam:UntagRole',
                    'iam:UntagUser',
                    'iam:UpdateAccessKey',
                    'identitystore:CreateGroupMembership',
                    'identitystore:DeleteGroupMembership',
                    'identitystore:IsMemberInGroups',
                    'identitystore:ListUsers',
                    'identitystore:ListGroups',
                    'identitystore:ListGroupMemberships',
                  ],
                'Resource': '*',
              },
              {
                'Sid': 'AllowOrgListAccounts',
```

```
                    'Effect': 'Allow',
                    'Action': 'organizations:ListAccounts',
                    'Resource': '*',
                  },
                  {
                    'Sid': 'AllowSSOContainment',
                    'Effect': 'Allow',
                    'Action':
                      [
                        'sso:CreateAccountAssignment',
                        'sso:DeleteAccountAssignment',
                        'sso:DeleteInlinePolicyFromPermissionSet',
                        'sso:GetInlinePolicyForPermissionSet',
                        'sso:ListAccountAssignments',
                        'sso:ListInstances',
                        'sso:ListPermissionSets',
                        'sso:ListPermissionSetsProvisionedToAccount',
                        'sso:PutInlinePolicyToPermissionSet',
                        'sso:TagResource',
                        'sso:UntagResource',
                      ],
                    'Resource': '*',
                  },
                  {
                    'Sid': 'AllowSSORead',
                    'Effect': 'Allow',
                    'Action': ['sso-directory:SearchUsers', 'sso-
directory:DescribeUser'],
                    'Resource': '*',
                  },
                  {
                    'Sid': 'AllowS3Read',
                    'Effect': 'Allow',
                    'Action':
                      [
                        's3:GetAccountPublicAccessBlock',
                        's3:GetBucketAcl',
                        's3:GetBucketLocation',
                        's3:GetBucketOwnershipControls',
                        's3:GetBucketPolicy',
                        's3:GetBucketPolicyStatus',
                        's3:GetBucketPublicAccessBlock',
                        's3:GetBucketTagging',
                        's3:GetEncryptionConfiguration',
```

```
            's3:GetObject',
            's3:GetObjectAcl',
            's3:GetObjectTagging',
            's3:GetReplicationConfiguration',
            's3:ListBucket',
            's3express:GetBucketPolicy',
          ],
        'Resource': '*',
      },
      {
        'Sid': 'AllowS3Write',
        'Effect': 'Allow',
        'Action':
          [
            's3:CreateBucket',
            's3:DeleteBucketPolicy',
            's3:DeleteObjectTagging',
            's3:PutAccountPublicAccessBlock',
            's3:PutBucketACL',
            's3:PutBucketOwnershipControls',
            's3:PutBucketPolicy',
            's3:PutBucketPublicAccessBlock',
            's3:PutBucketTagging',
            's3:PutBucketVersioning',
            's3:PutObject',
            's3:PutObjectAcl',
            's3express:CreateSession',
            's3express:DeleteBucketPolicy',
            's3express:PutBucketPolicy',
          ],
        'Resource': '*',
      },
      {
        'Sid': 'AllowAutoScalingWrite',
        'Effect': 'Allow',
        'Action':
          [
            'autoscaling:CreateOrUpdateTags',
            'autoscaling:DeleteTags',
            'autoscaling:DescribeAutoScalingGroups',
            'autoscaling:DescribeAutoScalingInstances',
            'autoscaling:DescribeTags',
            'autoscaling:EnterStandby',
            'autoscaling:ExitStandby',
```

```
                'autoscaling:UpdateAutoScalingGroup',
              ],
            'Resource': '*',
          },
          {
            'Sid': 'AllowEC2Containment',
            'Effect': 'Allow',
            'Action':
              [
                'ec2:AuthorizeSecurityGroupEgress',
                'ec2:AuthorizeSecurityGroupIngress',
                'ec2:CopyImage',
                'ec2:CreateImage',
                'ec2:CreateSecurityGroup',
                'ec2:CreateSnapshot',
                'ec2:CreateTags',
                'ec2:DeleteSecurityGroup',
                'ec2:DeleteTags',
                'ec2:DescribeImages',
                'ec2:DescribeInstances',
                'ec2:DescribeSecurityGroups',
                'ec2:DescribeSnapshots',
                'ec2:DescribeTags',
                'ec2:ModifyNetworkInterfaceAttribute',
                'ec2:RevokeSecurityGroupEgress',
              ],
            'Resource': '*',
          },
          {
            'Sid': 'AllowKMSActions',
            'Effect': 'Allow',
            'Action':
              [
                'kms:CreateGrant',
                'kms:DescribeKey',
                'kms:GenerateDataKeyWithoutPlaintext',
                'kms:ReEncryptFrom',
                'kms:ReEncryptTo',
              ],
            'Resource': '*',
          },
          {
            'Sid': 'AllowSSMActions',
            'Effect': 'Allow',
```

```
                'Action': ['ssm:DescribeAutomationExecutions'],
                'Resource': '*',
            },
        ],
    }
```

Cancelamento da associação

Um perfil que contém a permissão CancelMembership para a AWS Security Incident Response pode cancelar a associação pelo console, pela API ou pela AWS Command Line Interface.

> **Important**
>
> Depois de cancelar sua assinatura, você não poderá ver os dados históricos do caso. Ao cancelar uma associação, ela será excluída imediatamente e você não terá mais acesso aos casos da assinatura. Todos os recursos ou investigações com status `Active` ou `ready to close` também serão encerrados no cancelamento da associação.

Ao cancelar uma assinatura:

Sua associação será excluída e você não terá mais acesso aos casos da assinatura.

> **Important**
>
> Caso você opte por reativar a assinatura do serviço, uma nova associação será criada e os recursos de casos vinculados à associação anterior poderão ser acessados somente se tiverem sido previamente baixados antes do cancelamento.

Após o cancelamento da associação, todos os membros da equipe de resposta a incidentes da associação receberão notificações por e-mail.

> **Important**
>
> Se a associação tiver sido criada usando uma conta com permissões de administrador delegado e você remover essa designação de administrador delegado da conta usando a API do AWS Organizations, a associação será encerrada imediatamente.

Marcando atributos AWS Security Incident Response

Uma tag é um rótulo de metadados que você ou AWS atribuem a um atributo da AWS. Cada tag consiste em uma chave e um valor. Em tags atribuídas por você, você mesmo define a chave e o valor. Por exemplo, você pode definir a chave como `stage` e o valor de um atributo como `test`.

As tags ajudam a:

- Identificar e organizar seus atributos AWS. Muitos Serviços da AWS são compatíveis com marcação e permitem que você atribua a mesma tag a atributos de diferentes serviços, para indicar que estes atributos estão relacionados.
- Monitorar seus custos AWS. Você pode ativar essas tags no painel AWS Billing. AWS usa tags para categorizar seus custos e entregar um relatório mensal de alocação de custos a você. Para obter mais informações, consulte Use cost allocation tags no Guia do usuário do Faturamento da AWS.
- Controle o acesso aos recursos da AWS. Para mais informações, consulte Controlar o acesso usando etiquetas no Guia do usuário do IAM.

Consulte a referência da API de AWS Security Incident Response para obter informações sobre a marcação.

Como usar o AWS CloudShell para trabalhar com a Resposta a Incidentes de Segurança da AWS

AWS CloudShell O é um shell pré-autenticado baseado em navegador que você pode iniciar diretamente do Console de gerenciamento da AWS. Você pode executar comandos da AWS CLI em serviços da AWS (incluindo a Resposta a Incidentes de Segurança da AWS) usando o shell de sua preferência (Bash, PowerShell ou Z Shell). E você pode fazer isso sem precisar baixar ou instalar ferramentas de linha de comando.

Você inicia a AWS CloudShell via Console de gerenciamento da AWS, e as credenciais da AWS que usou para fazer login no console estarão automaticamente disponíveis em uma nova sessão do shell. Essa autenticação prévia de usuários do AWS CloudShell permite que você dispense a configuração de credenciais ao interagir com serviços da AWS, como a Resposta a Incidentes de Segurança, usando a AWS CLI na versão 2 (que está instalada previamente no ambiente de computação do shell).

Conteúdo

Obtenção de permissões do IAM para a AWS CloudShell

Usando os recursos de gerenciamento de acesso fornecidos pelo AWS Identity and Access Management, os administradores podem conceder permissões aos usuários do IAM para que eles possam acessar a AWS CloudShell e usar os recursos do ambiente.

A maneira mais rápida de um administrador conceder acesso aos usuários é por meio de uma política gerenciada pela AWS. Uma política gerenciada pela AWS é uma política independente que é criada e administrada pela AWS. A política gerenciada pela AWS a seguir para o CloudShell pode ser anexada às identidades do IAM:

- `AWSCloudShellFullAccess`: concede permissão para uso da AWS CloudShell com acesso total a todos os recursos.

Se você quiser limitar o escopo das ações que um usuário do IAM pode realizar com a AWS CloudShell, crie uma política personalizada que use a política gerenciada

`AWSCloudShellFullAccess` como modelo. Para obter mais informações sobre como limitar as ações que estão disponíveis para os usuários no CloudShell, consulte Gerenciamento de acesso e uso da AWS CloudShell com políticas do IAM no Guia do usuário da AWS CloudShell.

> **Note**
>
> Sua identidade do IAM também requer uma política que conceda permissão para realizar chamadas à Resposta a Incidentes de Segurança.

Interação com a Resposta a Incidentes de Segurança usando o AWS CloudShell

Após iniciar o AWS CloudShell usando o Console de gerenciamento da AWS, você pode começar imediatamente a interagir com a Resposta a Incidentes de Segurança por meio da interface de linha de comando.

> **Note**
>
> Ao usar a AWS Command Line Interface na AWS CloudShell, não é necessário baixar nem instalar nenhum recurso adicional. Além disso, como você já está autenticado no shell, não precisará configurar as credenciais antes de fazer chamadas.

Como trabalhar com o AWS CloudShell em conjunto com a Resposta a Incidentes de Segurança

1. No Console de gerenciamento da AWS, inicie o CloudShell escolhendo opções a seguir disponíveis na barra de navegação:
   - Escolha o ícone do CloudShell.
   - Comece digitando “cloudshell” na caixa Pesquisar e escolha a opção CloudShell.
2. Use a AWS Command Line Interface padrão para interagir com a Resposta a Incidentes de Segurança da AWS. Para obter uma referência completa dos comandos disponíveis da CLI, consulte a Referência de comandos da AWS CLI para Resposta a Incidentes de Segurança da AWS.

Registro em log das chamadas de API da Resposta a Incidentes de Segurança da AWS usando o AWS CloudTrail

A Resposta a Incidentes de Segurança da AWS está integrada com o AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, perfil ou serviço da AWS na Resposta a Incidentes de Segurança. O CloudTrail captura todas as chamadas de API da Resposta a Incidentes de Segurança como eventos. As chamadas capturadas incluem as chamadas realizadas pelo console da Resposta a Incidentes de Segurança e as chamadas de código para as operações da API da Resposta a Incidentes de Segurança. Se você criar uma trilha, poderá habilitar a entrega contínua dos eventos do CloudTrail para um bucket do Amazon S3, incluindo eventos relacionados à Resposta a Incidentes de Segurança. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail no Histórico de eventos. Com as informações coletadas pelo CloudTrail, é possível determinar qual solicitação foi feita à Resposta a Incidentes de Segurança, o endereço IP de origem da solicitação, quem a realizou, quando foi realizada e outros detalhes adicionais.

Para saber mais sobre o CloudTrail, consulte o Guia do usuário do AWS CloudTrail.

Informações da Resposta a Incidentes de Segurança no CloudTrail

O CloudTrail é habilitado em sua Conta da AWS quando ela é criada. Quando ocorre uma atividade na Resposta a Incidentes de Segurança, essa atividade é registrada como um evento do CloudTrail, juntamente com os demais eventos de serviços da AWS no Histórico de eventos. Você pode exibir, pesquisar e baixar eventos recentes em sua Conta da AWS. Para obter mais informações, consulte Como visualizar eventos com o histórico de eventos do CloudTrail.

Para obter um registro contínuo de eventos em sua Conta da AWS nos últimos 90 dias, crie uma trilha ou um armazenamento de dados de eventos do CloudTrail Lake.

Trilhas do CloudTrail

Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket do Amazon S3. As trilhas criadas usando o Console de gerenciamento da AWS são de várias regiões. Só é possível criar uma trilha de região única ou de várias regiões usando a AWS CLI. Criar uma trilha de várias regiões é uma prática recomendada, pois você captura atividades em todas as Regiões da AWS da conta. Ao criar uma trilha de região única, é possível visualizar somente os eventos registrados na Região da AWS da trilha. Para obter mais informações sobre trilhas, consulte Criar

uma trilha para a Conta da AWS e Criar uma trilha para uma organização no Guia do usuário do AWS CloudTrail.

Uma cópia dos eventos de gerenciamento em andamento pode ser entregue no bucket do Amazon S3 sem nenhum custo via CloudTrail com a criação de uma trilha; no entanto, há cobranças de armazenamento do Amazon S3. Para obter mais informações sobre os preços do CloudTrail, consulte Preços do AWS CloudTrail. Para receber informações sobre a definição de preços do Amazon S3, consulte Definição de preços do Amazon S3.

Armazenamentos de dados de eventos do CloudTrail Lake

O CloudTrail Lake permite executar consultas baseadas em SQL nos eventos. O CloudTrail Lake converte eventos existentes em formato JSON baseado em linhas para o formato Apache ORC. O ORC é um formato colunar de armazenamento otimizado para recuperação rápida de dados. Os eventos são agregados em armazenamentos de dados de eventos, que são coleções imutáveis de eventos baseados nos critérios selecionados com a aplicação de seletores de eventos avançados. Os seletores que aplicados a um armazenamento de dados de eventos controlam quais eventos persistem e estão disponíveis para consulta. Para obter mais informações sobre o CloudTrail Lake, consulte Trabalhar com o AWS CloudTrail Lake, no Guia do usuário do AWS CloudTrail.

Os armazenamentos de dados de eventos e consultas do CloudTrail Lake incorrem em custos. Ao criar um armazenamento de dados de eventos, você escolhe a opção de preço que deseja usar para ele. A opção de preço determina o custo para a ingestão e para o armazenamento de eventos, e o período de retenção padrão e máximo para o armazenamento de dados de eventos. Para obter mais informações sobre os preços do CloudTrail, consulte Preços do AWS CloudTrail.

Todas as ações da Resposta a Incidentes de Segurança são registradas em log pelo CloudTrail e estão documentadas na Referência da API da Resposta a Incidentes de Segurança da AWS. Por exemplo, as chamadas às ações `CreateMembership`, `CreateCase` e `UpdateCase` geram entradas nos arquivos de log do CloudTrail.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário-raiz ou usuário do AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.

- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte Elemento userIdentity do CloudTrail.

Noções básicas sobre as entradas de arquivos de log da Resposta a Incidentes de Segurança

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket do Amazon S3 especificado. Os arquivos de log CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte, e inclui informações sobre a ação solicitada, data e hora da ação, parâmetros da solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública, portanto, não são exibidos em uma ordem específica.

O exemplo apresentado a seguir mostra uma entrada de log do CloudTrail que demonstra a ação CreateCase.


```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROA00000000000000000:user",
        "arn": "arn:aws:sts::123412341234:assumed-role/Admin/user",
        "accountId": "123412341234",
        "accessKeyId": "****",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA00000000000000000",
                "arn": "arn:aws:iam::123412341234:role/Admin",
                "accountId": "123412341234",
                "userName": "Admin"
            },
            "attributes": {
                "creationDate": "2024-10-13T06:32:53Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2024-10-13T06:40:45Z",
    "eventSource": "security-ir.amazonaws.com",
```

```
    "eventName": "CreateCase",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "1.2.3.4",
    "userAgent": "aws-cli/2.17.23 md/awscrt#0.20.11 ua/2.0 os/macos#23.6.0 md/
arch#x86_64 lang/python#3.11.9 md/pyimpl#CPython cfg/retry-mode#standard md/
installer#exe md/prompt#off md/command#security-ir.create-case",
    "requestParameters": {
        "impactedServices": [
            "Amazon GuardDuty"
        ],
        "impactedAccounts": [],
        "clientToken": "testToken112345679",
        "resolverType": "Self",
        "description": "***",
        "engagementType": "Investigation",
        "watchers": [
            {
                "email": "***",
                "name": "***",
                "jobTitle": "***"
            }
        ],
        "membershipId": "m-r1abcdabcd",
        "title": "***",
        "impactedAwsRegions": [
            {
                "region": "ap-southeast-1"
            }
        ],
        "reportedIncidentStartDate": 1711553521,
        "threatActorIpAddresses": [
            {
                "ipAddress": "***",
                "userAgent": "browser"
            }
        ]
    },
    "responseElements": {
        "caseId": "0000000001"
    },
    "requestID": "2db4b08d-94a9-457a-9474-5892e6c8191f",
    "eventID": "b3fa3990-db82-43be-b120-c81262cc2f19",
    "readOnly": false,
    "resources": [
```

```
        {
            "accountId": "123412341234",
            "type": "AWS::SecurityResponder::Case",
            "ARN": "arn:aws:security-ir:us-east-1:123412341234:case/*"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123412341234",
    "eventCategory": "Management"
}
```

Gerenciamento de contas da AWS Security Incident Response com o AWS Organizations

AWS Security Incident Response O é integrado ao AWS Organizations. A conta gerencial do AWS Organizations para a organização pode designar uma conta como administrador delegado da AWS Security Incident Response. Essa ação habilita a AWS Security Incident Response como um serviço confiável dentro do AWS Organizations. Para obter informações sobre como essas permissões são concedidas, consulte Using AWS Organizations with other AWS services.

As seções apresentadas a seguir orientam você sobre diversas tarefas que podem ser executadas como uma conta de administrador delegado da Resposta a Incidentes de Segurança.

Conteúdo

Considerações e recomendações para o uso da AWS Security Incident Response com o AWS Organizations

As considerações e recomendações apresentadas a seguir podem ajudar você a compreender como uma conta de administrador delegado da Resposta a Incidentes de Segurança opera na AWS Security Incident Response:

Conta de administrador delegado para a AWS Security Incident Response.

> Você pode designar uma única conta de membro como a conta de administrador delegado do Security Incident Response. Por exemplo, ao designar uma conta-membro *111122223333* na

Europa (Irlanda), não é possível designar outra conta-membro *555555555555* no *Canadá (Central)*. É necessário usar a mesma conta como conta de administrador delegado da Resposta a Incidentes de Segurança em todas as demais regiões.

Você configura a conta de administrador delegado do Security Incident Response em uma Região da AWS específica.

> Você pode designar uma conta de membro como a conta de administrador delegado do Security Incident Response em uma Região da AWS durante a configuração inicial. Embora a configuração seja regional, o AWS Security Incident Response fornece cobertura a toda a organização em todas as Regiões da AWS compatíveis. As descobertas de segurança do Amazon GuardDuty e do AWS Security Hub CSPM são ingeridas de todas as Regiões da AWS compatíveis, e os casos são gerenciados centralmente na região em que você ativou sua assinatura. A conta de administrador delegado da Resposta a Incidentes de Segurança e as contas de membros devem ser adicionadas por meio do AWS Organizations.

Não é recomendável configurar a conta gerencial da organização como a conta de administrador delegado do Security Incident Response.

> A conta gerencial da organização pode ser designada como a conta de administrador delegado do Security Incident Response. Porém, as práticas recomendadas de segurança da AWS seguem o princípio do privilégio mínimo e não recomendam essa configuração.

A remoção de uma conta de administrador delegado da Resposta a Incidentes de Segurança de uma assinatura ativa cancela a assinatura imediatamente.

> Se você remover uma conta de administrador delegado do Security Incident Response, a AWS Security Incident Response removerá todas as contas de membros associadas a essa conta de administrador delegado do Security Incident Response. A AWS Security Incident Response não estará mais habilitada para todas as contas de membros.

Habilitação do acesso confiável para o AWS Account Management

Habilitar o acesso confiável para a AWS Security Incident Response permite que o administrador delegado da conta gerencial modifique as informações e os metadados (por exemplo, os detalhes de contato principais ou alternativos) específicos para cada conta de membro no AWS Organizations.

Use o procedimento apresentado a seguir para habilitar o acesso confiável para a AWS Security Incident Response em sua organização.

Permissões mínimas

Para executar essas tarefas, você deve atender aos seguintes requisitos:

- Você só pode executar essas tarefas na conta de gerenciamento da organização.
- A organização deve ter todos os recursos habilitados.

Console

Para habilitar o acesso confiável para a AWS Security Incident Response

1. Faça login no console do AWS Organizations. É necessário fazer login como um usuário do IAM, assumir uma função do IAM ou fazer login como usuário root (não recomendado) na conta de gerenciamento da organização.
2. No painel de navegação, escolha Serviços.
3. Escolha AWS Security Incident Response na lista de serviços.
4. Escolha Enable trusted access (Habilitar acesso confiável).
5. Na caixa de diálogo Habilitar o acesso confiável para o AWS Security Incident Response, digite habilitar para confirmar e, em seguida, escolha Habilitar o acesso confiável.

API/CLI

Para habilitar o acesso confiável para a AWS Account Management

Depois de executar o comando a seguir, você pode usar as credenciais da conta de gerenciamento da organização para chamar as operações da API de Gerenciamento de Contas que usam o parâmetro `--accountId` para fazer referência às contas-membro de uma organização.

- AWS CLI: enable-aws-service-access

  O exemplo apresentado a seguir habilita o acesso confiável para a AWS Security Incident Response na organização da conta que está realizando a chamada.

```
$ aws organizations enable-aws-service-access \
                                    --service-principal security-
ir.amazonaws.com
```

Se for bem-sucedido, esse comando não produzirá uma saída.

Permissões necessárias para designar uma conta de administrador delegado da Resposta a Incidentes de Segurança

Você pode optar por configurar sua associação à AWS Security Incident Response usando um administrador delegado para o AWS Organizations. Para obter informações sobre como essas permissões são concedidas, consulte Using AWS Organizations with other AWS services.

> **Note**
>
> A AWS Security Incident Response habilita automaticamente o relacionamento confiável com o AWS Organizations ao usar o console para configuração e gerenciamento. Se você usar a CLI ou o SDK, será necessário habilitar manualmente esse relacionamento por meio da API EnableAWSServiceAccess, confiando no domínio `security-ir.amazonaws.com`.

Na qualidade de gerente do AWS Organizations, antes de designar a conta de administrador delegado da Resposta a Incidentes de Segurança para sua organização, verifique se você pode executar as seguintes ações da AWS Security Incident Response: `security-ir:CreateMembership` e `security-ir:UpdateMembership`. Essas ações permitem que você designe a conta de administrador delegado da Resposta a Incidentes de Segurança para sua organização por meio da própria AWS Security Incident Response. Também é preciso garantir que se tenha permissão para executar as AWS Organizations ações que o ajudam a recuperar informações sobre sua organização.

Para conceder essas permissões, inclua a seguinte instrução em uma política AWS Identity and Access Management (IAM) da sua conta:

```
{
    "Sid": "PermissionsForSIRAdmin",
    "Effect": "Allow",
    "Action": [
        "security-ir:CreateMembership",
        "security-ir:UpdateMembership",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
```

```
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts"
            ],
            "Resource": "*"
        }
```

Se você deseja designar sua conta gerencial do AWS Organizations como a conta de administrador delegado de Resposta a Incidentes de Segurança, sua conta também precisará da ação do IAM: `CreateServiceLinkedRole`. Analise a seção Considerações e recomendações para o uso da AWS Security Incident Response com o AWS Organizations antes de prosseguir com a adição das permissões.

Para continuar com a designação da sua conta gerencial do AWS Organizations como a conta de administrador delegado da Resposta a Incidentes de Segurança, adicione a seguinte declaração à política do IAM e substitua *111122223333* pelo ID da Conta da AWS de sua conta gerencial do AWS Organizations:

```
        {
         "Sid": "PermissionsToEnableSecurityIncidentResponse"
         "Effect": "Allow",
         "Action": [
          "iam:CreateServiceLinkedRole"
         ],
         "Resource": "arn:aws:iam::111122223333:role/aws-service-role/security-
ir.amazonaws.com/AWSServiceRoleForSecurityIncidentResponse",
         "Condition": {
          "StringLike": {
           "iam:AWSServiceName": "security-ir.amazonaws.com"
          }
         }
        }
```

Designação de um administrador delegado para a AWS Security Incident Response

Esta seção apresenta as etapas para designar um administrador delegado na organização da AWS Security Incident Response.

Na qualidade de gerente da organização da AWS, certifique-se de ler atentamente as Considerações e recomendações sobre o funcionamento de uma conta de administrador delegado da Resposta a Incidentes de Segurança. Antes de continuar, verifique se você tem Permissões necessárias para designar uma conta de administrador delegado da Resposta a Incidentes de Segurança.

Selecione o método de acesso de sua preferência para designar uma conta de administrador delegado de Resposta a Incidentes de Segurança para sua organização. Somente uma conta gerencial pode executar esta etapa.

Console

1. Acesse o console de Resposta a Incidentes de Segurança em https://console.aws.amazon.com/security-ir/.

   Para fazer login, use as credenciais de gerenciamento da sua organização do AWS Organizations.
2. Ao usar o seletor de Região da AWS, localizado no canto superior direito da página, selecione a região na qual deseja designar a conta de administrador delegado da Resposta a Incidentes de Segurança para sua organização.
3. Siga o assistente de configuração para criar sua associação, incluindo a conta de administrador delegado.

API/CLI

- Execute o comando CreateMembership usando as credenciais da Conta da AWS destinada ao gerenciamento da organização.
  - Outra alternativa é definir isso como AWS Command Line Interface. O comando da AWS CLI apresentado a seguir designa uma conta de administrador delegado da Resposta a Incidentes de Segurança. A seguir, apresentamos as opções de string disponíveis para configurar sua associação:

```
                                    {
                                      "customerAccountId": "stringstring",
                                      "membershipName": "stringstring",
                                      "customerType": "Standalone",
                                      "organizationMetadata": {
                                        "organizationId": "string",
                                        "managementAccountId":
"stringstring",
                                        "delegatedAdministrators": [
                                          "stringstring"
                                        ]
                                      },
                                      "membershipAccountsConfigurations":
{
                                        "autoEnableAllAccounts": true,
                                        "organizationalUnits": [
                                          "string"
                                        ]
                                      },
                                      "incidentResponseTeam": [
                                        {
                                          "name": "string",
                                          "jobTitle": "stringstring",
                                          "email": "stringstring"
                                        }
                                      ],
                                      "internalIdentifier": "string",
                                      "membershipId": "stringstring",
                                      "optInFeatures": [
                                        {
                                          "featureName": "RuleForwarding",
                                          "isEnabled": true
                                        }
                                      ]
                                    }
```

Se a AWS Security Incident Response não estiver habilitada para a sua conta de administrador delegado da Resposta a Incidentes de Segurança, ela não poderá executar nenhuma ação. Caso ainda não tenha sido feito, certifique-se de habilitar a AWS Security Incident Response para a conta de administrador delegado da Resposta a Incidentes de Segurança designada recentemente.

Gerenciar a associação com unidades organizacionais (UOs) para o AWS Security Incident Response

O AWS Security Incident Response oferece suporte à cobertura de associação para unidades organizacionais (UOs) individuais. É possível atualizar sua associação para cobrir UOs específicas a qualquer momento. Todas as contas nas UOs selecionadas, incluindo contas em UOs secundárias, serão cobertas pela associação.

Ao atualizar sua associação de membros, é possível aplicar atualizações para até 5 UOs de cada vez. Se quiser fazer alterações em mais de 5 UOs, conclua as alterações de associação em lotes de 5 UOs, até que todas as atualizações sejam concluídas.

Console

1. Acesse o console de Resposta a Incidentes de Segurança em https://console.aws.amazon.com/security-ir/.

   Para fazer login, use as credenciais de gerenciamento da sua organização do AWS Organizations.
2. Navegue até Gerenciar associação > Contas.
3. Clique em Atualizar associação.
4. Selecione Escolher unidades organizacionais (UOs).
5. Selecione Adicionar UOs ou Remover UOs.
6. Selecione até 5 UOs que você deseja atualizar. Não é possível adicionar e remover UOs ao mesmo tempo.

   > **Note**
   >
   > Todas as contas e UOs secundárias em uma UO selecionada serão associadas.
7. Clique em Atualizar associação.
8. > **Note**
   >
   > Se quiser fazer alterações em mais de 5 UOs, repita as etapas 5 e 6 até que todas as UOs tenham sido associadas.

Para saber mais sobre como fazer alterações em UOs na sua organização da AWS, consulte Gerenciar unidades organizacionais (UOs) com o AWS Organizations.

Adição de membros à AWS Security Incident Response

Existe uma correspondência direta entre o AWS Organizations e sua associação à AWS Security Incident Response. À medida que contas são adicionadas (ou removidas) de suas organizações ou unidades organizacionais (UOs), essas alterações serão refletidas nas contas cobertas pela sua associação do AWS Security Incident Response.

Para adicionar uma conta à sua associação, siga uma das opções apresentadas na seção Managing accounts in an organization with AWS Organizations.

Também é possível acrescentar UOs adicionais à sua associação a qualquer momento. Consulte Gerenciar a associação com unidades organizacionais (UOs).

Remoção de membros da AWS Security Incident Response

Para remover uma conta da sua associação, você pode remover uma conta de membro da sua organização, mover contas de suas UOs selecionadas ou remover UOs da sua associação.

Para remover uma conta da sua associação, siga os procedimentos para a remoção de uma conta de membro de uma organização.

Para mover contas das suas UOs, siga os procedimentos de como Mover contas para uma unidade organizacional (OU) ou entre a raiz e as UOs com o AWS Organizations.

Para remover a UU da sua associação, siga os procedimentos de como Gerenciar a associação com unidades organizacionais (UOs).

Amazon EventBridge

Ao usar o Amazon EventBridge, você pode reagir, monitorar e realizar a orquestração de eventos associados a casos de AWS Security Incident Response e associações. É possível encaminhar esses eventos por meio de Regras (em cenários de disseminação para um ou mais destinos) ou por meio de Pipes (para integrações ponto a ponto com funcionalidades avançadas de filtragem, enriquecimento e transformação).

Você pode criar integrações entre a Resposta a Incidentes de Segurança e ferramentas de entidades externas, bem como agregar dados para análise com o uso de IA generativa e outras ferramentas da AWS. Por exemplo, quando a Resposta a Incidentes de Segurança cria proativamente um caso, você pode usar automações do EventBridge para acionar sistemas que notifiquem as partes interessadas. Além disso, se você gerencia diversos ambientes da AWS, pode usar a integração com o Amazon EventBridge para monitorar as associações da AWS Security Incident Response, garantindo que todos os ambientes mantenham uma postura de segurança robusta.

Para obter mais informações, você pode consultar What is Amazon EventBridge?

> **Note**
>
> Para obter as atualizações mais recentes sobre a integração do Amazon EventBridge com o AWS Security Incident Response, incluindo as integrações do ITSM, consulte AWS Security Incident Response now supports ITSM integrations na página Novidades da AWS.

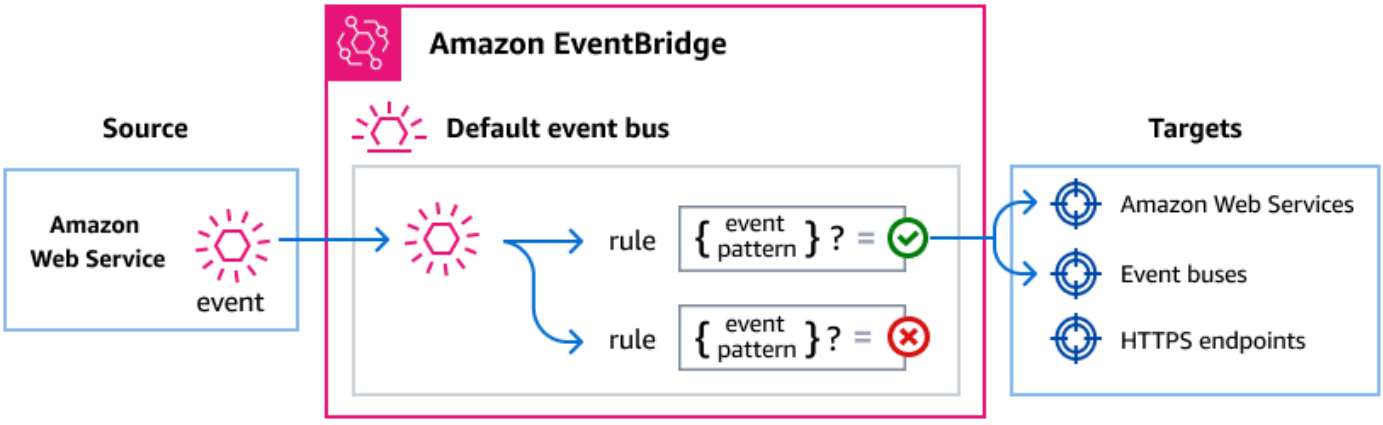
Conteúdo

Gerenciamento de eventos de Resposta a Incidentes de Segurança usando o Amazon EventBridge

O Amazon EventBridge é um serviço sem servidor que usa eventos para conectar os componentes da aplicação, facilitando a criação de aplicações escaláveis orientadas por eventos. A arquitetura orientada por eventos é um estilo de criação de sistemas de software com acoplamento fraco que funcionam juntos emitindo e respondendo a eventos. Os eventos representam uma mudança em um recurso ou ambiente.

Como isso funciona:

Assim como muitos serviços da AWS, a Resposta a Incidentes de Segurança gera e envia eventos para o barramento de eventos padrão do EventBridge. (O barramento de eventos padrão é provisionado automaticamente em sua conta da AWS.) Um barramento de eventos é um roteador que recebe eventos e os entrega a zero ou mais destinos, ou alvos. As regras especificadas para o barramento de eventos avaliam os eventos à medida que eles chegam. Cada regra verifica se um evento corresponde ao padrão do evento. Se o evento corresponder, o barramento de eventos enviará o evento para os destinos especificados.



Distribuição de eventos da Resposta a Incidentes de Segurança usando as regras do EventBridge

Para que o barramento de eventos padrão do EventBridge envie eventos da Resposta a Incidentes de Segurança para um destino, é necessário criar uma regra. Cada regra contém um padrão de evento, que o EventBridge compara a cada evento recebido no barramento de eventos. Se os dados

do evento corresponderem ao padrão de evento especificado, o EventBridge fornecerá o evento aos destinos da regra.

Para obter instruções completas sobre como criar regras para o barramento de eventos, consulte a seção Creating rules that react to events no Guia do usuário do Amazon EventBridge.

Criação de padrões de eventos que correspondem a eventos da Resposta a Incidentes de Segurança

Cada padrão de evento é um objeto JSON que contém:

- Um atributo `source` que identifica o serviço que envia o evento. Para eventos da Resposta a Incidentes de Segurança, a origem é `"aws.security-ir"`.
- (Opcional): um atributo `detail-type` que contém uma matriz dos tipos de eventos a serem correlacionados.
- (Opcional): um atributo `detail` que contém quaisquer outros dados relacionados aos eventos a serem correlacionados.

Por exemplo, o seguinte padrão de evento corresponde a todos os eventos de `Case Updated by AWS Security Incident Response Service` para uma Conta da AWS específica:

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T03:45:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "security-ir.amazonaws.com"
  }
}
```

Consulte mais informações sobre como escrever padrões de eventos, consulte Padrões de eventos no Guia do usuário do EventBridge.

Referência detalhada dos eventos da Resposta a Incidentes de Segurança

Todos os eventos dos serviços da AWS têm um conjunto comum de campos contendo metadados sobre o evento, como o serviço da AWS que é a origem do evento, a hora em que o evento foi gerado, a conta e a região em que o evento ocorreu, e outros. Para obter as definições desses campos gerais, consulte Event structure reference no Guia do usuário do Amazon EventBridge.

Além disso, cada evento tem um campo de `detail` que contém dados específicos desse determinado evento. A referência abaixo define os campos de detalhes para os diversos eventos da Resposta a Incidentes de Segurança.

Ao usar o EventBridge para selecionar e gerenciar eventos da Resposta a Incidentes de Segurança, é útil considerar o seguinte:

- O campo `source` de todos os eventos da Resposta a Incidentes de Segurança é definido como `"aws.security-ir"`.
- O campo do `detail-type` especifica o tipo de evento.

  Por exemplo, `"Case Updated"`.
- O campo de `detail` contém os dados específicos desse determinado evento.

Para obter mais informações sobre como desenvolver padrões de eventos que possibilitam que regras correspondam a eventos da Resposta a Incidentes de Segurança, consulte Event patterns no Guia do usuário do Amazon EventBridge.

Consulte mais informações sobre eventos e como o EventBridge os processa em EventBridge events no Guia do usuário do Amazon EventBridge.

Campos comuns: todos os eventos da AWS Security Incident Response incluem os campos padrão do Amazon EventBridge apresentados abaixo

- version: versão do formato do evento do EventBridge
- id: identificador único para o evento
- detail-type: descrição textual e compreensível do tipo de evento
- source: sempre “aws.security-ir” para eventos da Resposta a Incidentes de Segurança

- account: ID da conta da AWS em que o evento ocorreu
- time: carimbo de data/hora no formato ISO 8601 indicando quando o evento ocorreu
- region: Região da AWS em que o recurso existe
- resources: matriz que contém o ARN do recurso afetado

Campos de detalhes: o objeto `detail` contém informações específicas da Resposta a Incidentes de Segurança

- caseId: identificador exclusivo para o caso (somente para eventos de caso)
- membershipId: identificador exclusivo para a associação (somente para eventos de associação)
- updatedBy: identifica quem realizou a atualização (somente para eventos de atualização de casos e comentários)
- createdBy: identifica quem criou a entidade (somente para eventos de criação de casos e comentários)

Valores possíveis para o ator: os campos `updatedBy` e `createdBy` podem conter

- AWS Responder: indica uma ação executada por um responsável pela segurança da AWS
- *`security-ir.amazonaws.com`*: identifica uma ação executada automaticamente pelo serviço
- Account ID: identifica uma ação executada pelo cliente (por exemplo, “111122223333”)

Valores de ARN de recursos: os recursos da AWS Security Incident Response usam os seguintes formatos de ARN

- Casos: `arn:aws:security-ir:{region}:{account-id}:case/{case-id}`
- Associações: `arn:aws:security-ir:{region}:{account-id}:membership/{membership-id}`

Eventos relacionados ao caso

Caso criado pelo profissional responsável da AWS

```
{
  "version": "0",
```

```
    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "detail-type": "Case Created",
    "source": "aws.security-ir",
    "account": "111122223333",
    "time": "2023-05-12T00:00:00Z",
    "region": "us-west-2",
    "resources": [
      "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
    ],
    "detail": {
      "caseId": "1234567890",
      "createdBy": "AWS Responder"
    }
  }
```

Caso criado pelo serviço

```
  {
    "version": "0",
    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "detail-type": "Case Created",
    "source": "aws.security-ir",
    "account": "111122223333",
    "time": "2023-05-12T00:00:00Z",
    "region": "us-west-2",
    "resources": [
      "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
    ],
    "detail": {
      "caseId": "1234567890",
      "createdBy": "security-ir.amazonaws.com"
    }
  }
```

Caso criado pelo cliente

```
  {
    "version": "0",
    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
```

```
  "detail-type": "Case Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T00:00:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "createdBy": "111122223333"
  }
}
```

Caso atualizado pelo profissional responsável da AWS

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T01:30:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "AWS Responder"
  }
}
```

Caso atualizado pelo cliente da AWS

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Updated",
```

```
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:15:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "111122223333"
  }
}
```

Caso atualizado pelo serviço de AWS Security Incident Response

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T03:45:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "security-ir.amazonaws.com"
  }
}
```

Caso encerrado

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Closed",
  "source": "aws.security-ir",
```

```
  "account": "111122223333",
  "time": "2023-05-15T14:22:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890"
  }
}
```

Eventos relacionados aos comentários do caso

Comentário do caso criado pelo profissional responsável da AWS

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T04:30:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "createdBy": "AWS Responder"
  }
}
```

Comentário do caso criado pelo cliente

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Created",
  "source": "aws.security-ir",
```

```
  "account": "111122223333",
  "time": "2023-05-12T02:15:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "createdBy": "111122223333"
  }
}
```

Comentário do caso criado pelo serviço de AWS Security Incident Response

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:15:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "createdBy": "security-ir.amazonaws.com"
  }
}
```

Comentário do caso atualizado pelo cliente

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
```

```
  "time": "2023-05-12T02:45:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "111122223333"
  }
}
```

Comentário do caso atualizado pelo serviço de AWS Security Incident Response

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:45:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "security-ir.amazonaws.com"
  }
}
```

Comentário do caso criado pelo profissional responsável da AWS

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:45:00Z",
```

```
            "region": "us-west-2",
            "resources": [
              "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
            ],
            "detail": {
              "caseId": "1234567890",
              "updatedBy": "AWS Responder"
            }
          }
```

Eventos relacionados à associação

Associação criada

```
          {
            "version": "0",
            "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "detail-type": "Membership Created",
            "source": "aws.security-ir",
            "account": "111122223333",
            "time": "2023-04-01T10:00:00Z",
            "region": "us-west-2",
            "resources": [
              "arn:aws:security-ir:us-west-2:111122223333:membership/
m-1234567890abcdef0"
            ],
            "detail": {
              "membershipId": "m-1234567890abcdef0"
            }
          }
```

Associação atualizada

```
          {
            "version": "0",
            "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "detail-type": "Membership Updated",
            "source": "aws.security-ir",
            "account": "111122223333",
```

```
            "time": "2023-04-15T16:30:00Z",
            "region": "us-west-2",
            "resources": [
              "arn:aws:security-ir:us-west-2:111122223333:membership/
m-1234567890abcdef0"
            ],
            "detail": {
              "membershipId": "m-1234567890abcdef0"
            }
          }
```

Associação cancelada

```
          {
            "version": "0",
            "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "detail-type": "Membership Closed",
            "source": "aws.security-ir",
            "account": "111122223333",
            "time": "2023-06-30T23:59:59Z",
            "region": "us-west-2",
            "resources": [
              "arn:aws:security-ir:us-west-2:111122223333:membership/
m-1234567890abcdef0"
            ],
            "detail": {
              "membershipId": "m-1234567890abcdef0"
            }
          }
```

Associação encerrada

```
          {
            "version": "0",
            "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "detail-type": "Membership Terminated",
            "source": "aws.security-ir",
            "account": "111122223333",
            "time": "2023-07-01T00:00:00Z",
```

```
            "region": "us-west-2",
            "resources": [
              "arn:aws:security-ir:us-west-2:111122223333:membership/
m-123456s7890abcdef0"
            ],
            "detail": {
              "membershipId": "m-1234567890abcdef0"
            }
          }
```

Usar eventos do AWS Security Incident Response

Você pode criar regras do EventBridge para corresponder a esses eventos e acionar ações automatizadas. Veja a seguir estão alguns casos de uso de exemplo:

Correspondência com todos os eventos de AWS Security Incident Response:

```
{
  "source": ["aws.security-ir"]
}
```

Correspondência somente com eventos relacionados ao caso:

```
{
  "source": ["aws.security-ir"],
  "detail-type": [
    "Case Created",
    "Case Updated",
    "Case Closed",
    "Case Comment Added",
    "Case Comment Updated"
  ]
}
```

Correspondência com casos atualizados pelos profissionais responsáveis da AWS:

```
{
  "source": ["aws.security-ir"],
  "detail-type": ["Case Updated"],
  "detail": {
    "updatedBy": ["AWS Responder"]
  }
}
```

Correspondência com eventos para um caso específico:

```
{
  "source": ["aws.security-ir"],
  "detail": {
    "caseId": ["1234567890"]
  }
}
```

Tutorial: como enviar alertas do Amazon Simple Notification Service para eventos de **`Membership Updated`**

Neste tutorial, você configura uma regra de evento do Amazon EventBridge que captura somente eventos nos quais sua assinatura entra em um status de `Membership Updated`.

Pré-requisitos

Este tutorial presume que sua assinatura está em pleno funcionamento e que há contas ativas da AWS vinculadas à sua associação.

Tópicos

- Tutorial: criar e assinar um tópico do Amazon SNS
- Tutorial: registrar uma regra de evento
- Tutorial: testar sua regra
- Regra alternativa: atualizações realizadas nos casos da Resposta a Incidentes de Segurança

Tutorial: criar e assinar um tópico do Amazon SNS

Neste tutorial, você configura um tópico do Amazon SNS para funcionar como um destino de evento para a nova regra de evento.

Para criar um tópico do Amazon SNS

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. Escolha Topics (Tópicos), Create topic (Criar tópico).
3. Em Tipo, escolha Padrão.
4. Em Nome, insira **`MembershipUpdated`** e selecione Criar tópico.
5. Na tela MembershipUpdated, selecione a opção Criar assinatura.
6. Em Protocolo, escolha Email.
7. Em Endpoint, insira um endereço de e-mail ao qual tenha acesso e escolha Criar assinatura.
8. Verifique sua conta de e-mail e espere para receber uma mensagem de e-mail de confirmação de assinatura. Quando você recebê-la, escolha Confirmar assinatura.

Tutorial: registrar uma regra de evento

Em seguida, registre uma regra de eventos que capture somente eventos do tipo `Membership Updated`.

Para registrar sua regra do EventBridge

1. Abra o console do Amazon EventBridge em https://console.aws.amazon.com/events/.
2. No painel de navegação, escolha Regras.
3. Escolha Create rule.
4. Insira um nome e uma descrição para a regra.

> **Note**
>
> Uma regra não pode ter o mesmo nome que outra na mesma Região e barramento de eventos.

5. Em Barramento de eventos, selecione o barramento de eventos que você deseja associar a essa regra. Se quiser que essa regra faça a correspondência com eventos provenientes da sua

conta, escolha Barramento de eventos padrão da AWS. Quando um serviço AWS em sua conta emite um evento, ele sempre irá para o barramento de eventos padrão da conta.

> **Note**
>
> Essa configuração deve ser realizada na sua conta do AWS Organizations ou na conta de administrador delegado em que você criou a associação à AWS Security Incident Response.

6. Em Rule type, escolha Rule with an event pattern.
7. Escolha Próximo.
8. Em Origem do Evento, escolha Outro.
9. Em Padrão de eventos, selecione Padrões personalizados (editor JSON).
10. Cole o padrão de evento a seguir na área de texto.

```
{
  "source": ["aws.security-ir"],
  "detail-type": ["Membership Updated"]
}
```

Este código define uma regra do EventBridge que corresponde a qualquer evento em que a sua associação de serviço seja atualizada ou modificada. Para obter mais informações sobre padrões de eventos, consulte Eventos e padrões de eventos no Guia do usuário do Amazon EventBridge.

11. Escolha Próximo.
12. Em Tipos de destino, escolha Serviço da AWS.
13. Em Selecionar um destino, escolha Tópico do SNS e, em Tópico, escolha MembershipUpdated.
14. (Opcional) Para Configurações Adicionais, proceda da seguinte forma:

    a. Em Tempo Máximo do Evento, insira um valor entre um minuto (00:01) e 24 horas (24:00).

    b. Em Tentativas de Repetição, insira um número entre 0 e 185.

    c. Em Fila de mensagens não entregues, escolha se será usada uma fila padrão do Amazon SQS como fila de mensagens não entregues. O EventBridge enviará eventos que correspondam a essa regra para a fila de mensagens não entregues caso não sejam entregues com êxito ao destino. Faça um dos procedimentos a seguir:

- Escolha Nenhum para não usar uma fila de mensagens não entregues.
- Escolha Selecionar uma Fila Amazon SQS na Conta AWS Atual para usá-la como fila de mensagens não entregues e então, na lista suspensa, selecione a fila a ser usada.
- Escolha Selecionar uma Fila Amazon SQS em qualquer outra AWS conta como fila de mensagens não entregues e insira o ARN da fila a ser usada. Você deve anexar uma política baseada em recurso à fila responsável por conceder permissão ao EventBridge para enviar mensagens. Para mais informações, consulte Concedendo Permissões à Fila de Mensagens Não Entregues do Guia de usuário Amazon EventBridge.

15. Escolha Próximo.
16. (Opcional) Insira uma ou mais tags para a regra. Para mais informações, consulte Tags Amazon EventBridge em Guia de Usuário Amazon EventBridge.
17. Escolha Próximo.
18. Analise os detalhes da regra e selecione Criar regra.

Tutorial: testar sua regra

Para testar sua regra, envie uma atualização para sua associação à AWS Security Incident Response. Se a regra estiver configurada corretamente, você deverá receber uma mensagem por e-mail em poucos minutos com o texto do evento.

Regra alternativa: atualizações realizadas nos casos da Resposta a Incidentes de Segurança

Para criar uma regra de evento que monitore todas as atualizações realizadas nos casos, repita estes tutoriais com as seguintes alterações:

1. Em Tutorial: criar e assinar um tópico do Amazon SNS, use *`CaseUpdates`* como o nome do tópico.
2. Em Tutorial: registrar uma regra de evento, use o seguinte padrão no editor JSON:

```
{
  "source": ["aws.security-ir"],
  "detail-type": [
    "Case Created",
    "Case Updated",
    "Case Closed",
```

```
                "Case Comment Created",
                "Case Comment Updated"
            ]
        }
```

Solução de problemas

Caso você enfrente problemas relacionados à execução de uma ação específica para a AWS Security Incident Response, consulte os tópicos apresentados nesta seção.

Um ERRO consiste em um status de uma operação que indica uma falha em parte ou na totalidade das operações. De forma alternativa, os avisos são emitidos quando algum problema ocorre, porém a tarefa continua e é concluída.

Conteúdo

Problemas

Envio de solicitações fora do contexto adequado.

Todas as chamadas às APIs da AWS Security Incident Response devem se originar de uma entidade principal do IAM na conta de administrador delegado ou na conta de associação do serviço. Certifique-se de que você está operando da entidade principal do IAM adequada na Conta da AWS que corresponde à conta de administrador delegado da AWS Security Incident Response ou à conta de associação da sua organização.

Erros

AccessDeniedException

Você não tem acesso suficiente para executar esta ação.

Entre em contato com o seu administrador da AWS para garantir que você tenha permissão para assumir um perfil do IAM na conta de administrador delegado ou na conta de associação da AWS Security Incident Response. Além disso, assegure-se de que esse perfil contenha uma política do IAM que permita a execução da ação solicitada. Para obter mais informações, consulte AWS Security Incident Response IAM.

ConflictException

A solicitação gerou um estado de inconsistência.

Verifique se todos os nomes dos arquivos anexados ao caso ou os membros padrão da equipe de resposta especificados são exclusivos. Além disso, verifique se a associação ao serviço de AWS Security Incident Response não foi previamente configurada. Abra o console da Resposta a Incidentes de Segurança em https://console.aws.amazon.com/security-ir/ e navegue até `Membership Details`.

InternalServerException

Ocorreu um erro inesperado durante o processamento da solicitação. Tente novamente em alguns minutos. Se o problema persistir, abra um caso com o Suporte.

ResourceNotFoundException

A solicitação faz referência a um recurso que não existe.

Um ou mais dos recursos especificados na sua solicitação não existem. Verifique se todos os ARNs ou IDs dos recursos fornecidos estão corretos. Isso se aplica a IDs do AWS Organizations, IDs de contas, perfis do IAM, associações, casos, membros da equipe de resposta, responsáveis pelos casos, anexos dos casos e comentários dos casos.

ThrottlingException

A solicitação foi negada devido à limitação da solicitação.

Houve um excesso de solicitações realizadas pela sua entidade principal do IAM para essa função da API em um determinado período. Aguarde um minuto e tente novamente. Se o problema persistir, considere implementar um algoritmo de recuo exponencial e de novas tentativas.

ValidationException

A entrada não atende às restrições especificadas por um serviço da AWS service (Serviço da AWS).

Um ou mais dos campos de dados na sua solicitação não atendem aos requisitos de validação ou de combinação lógica. Verifique se todos os ARNs dos recursos estão completos e se os valores de texto atendem às restrições de tamanho e de formato definidos no Guia de referência da API da AWS Security Incident Response. Confirme também se as alterações de valores são permitidas. Por exemplo, não é possível alterar um caso de “com suporte por parte da AWS” para “gerenciado por conta própria”.

Suporte

Se você precisar de assistência adicional, entre em contato com o Centro de Suporte para obter auxílio na solução dos problemas. Solicitamos que tenha em mãos as seguintes informações:

- A Região da AWS que foi usada
- O ID da Conta da AWS vinculada à associação
- Seu conteúdo de origem, se aplicável e disponível
- Quaisquer outros detalhes sobre o problema que podem ajudar na solução do problema

Segurança

Tópicos

Proteção de dados no AWS Security Incident Response

O modelo de responsabilidade compartilhada da AWS se aplica à proteção de dados para o serviço de Resposta a Incidentes de Segurança da AWS. Conforme descrito neste modelo, a AWS é responsável pela proteção da infraestrutura que executa os serviços oferecidos na Nuvem AWS. Você é responsável por manter o controle sobre o conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para obter mais informações sobre a proteção de dados na Europa, consulte o artigo do blog AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS.

Para finalidades de proteção de dados, as práticas recomendadas de segurança da AWS recomendam que você proteja as credenciais da conta da AWS e configure usuários individuais com o Centro de Identidade do AWS IAM ou com o AWS Identity and Access Management (IAM). Dessa

maneira, a cada usuário são atribuídas somente as permissões essenciais para o desempenho de suas responsabilidades profissionais. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos da AWS. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure o registro em log de atividades da API e dos usuários com o AWS CloudTrail.
- Use as soluções de criptografia da AWS, juntamente com todos os controles de segurança padrão nos serviços da AWS.
- Atualmente, o serviço não é compatível com o padrão FIPS 140-3.

Nunca insira informações confidenciais ou sensíveis, como seus endereços de e-mail, em tags ou em campos de texto livres, como um campo Nome. Isso também vale para o uso do AWS Support ou de outros serviços da AWS com o console, a API, a AWS Command Line Interface ou os AWS SDKs. Quaisquer dados inseridos em tags ou campos de texto de forma livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, recomendamos fortemente que não inclua informações relacionadas às credenciais no URL para validar sua solicitação para esse servidor.

Tópicos

Criptografia de dados

O AWS Security Incident Response protege seus dados usando criptografia em repouso e em trânsito. Todos os dados são criptografados usando protocolos de criptografia padrão do setor para ajudar você a atender os requisitos de segurança e conformidade.

Tópicos

- Gerenciamento de chaves

Criptografia inativa

Os dados são criptografados em repouso usando criptografia transparente do lado do servidor. Isso ajuda a reduzir a carga e a complexidade operacionais necessárias para proteger dados confidenciais. Com a criptografia de dados em repouso, você pode criar aplicativos confidenciais que atendem a requisitos de conformidade e regulamentação de criptografia.

Criptografia em trânsito

Os dados coletados e acessados pelo AWS Security Incident Response são exclusivamente por meio de um canal protegido for Transport Layer Security (TLS).

Gerenciamento de chaves

A AWS Security Incident Response implementa integrações com o AWS KMS para fornecer criptografia em repouso para os dados de casos e de anexos.

A AWS Security Incident Response não oferece suporte para as chaves gerenciadas pelo cliente.

Coleta e uso de dados

O AWS Security Incident Response trabalha com três categorias distintas de dados, cada uma com diferentes métodos de coleta, padrões de armazenamento e comportamento regional. Compreender essas categorias é essencial para avaliar como a Resposta a Incidentes de Segurança se encaixa em seus requisitos de conformidade.

Tópicos

- Dados de investigação de caso
- Dados de descobertas de segurança
- Processamento de agentes de investigação
- Noções básicas sobre a confidencialidade dos metadados

Dados de investigação de caso

Quando você abre um caso de incidente de segurança, a Resposta a Incidentes de Segurança coleta logs e metadados do ambiente da AWS para dar suporte a investigação. Esses dados específicos do caso incluem logs de API, logs de fluxo da VPC, consultas ao DNS do Amazon

Route 53, eventos de acesso do Amazon S3, metadados de recursos (nomes, tags e detalhes de configuração) e informações de casos, como comentários e notas de investigação.

> **Important**
>
> A Resposta a Incidentes de Segurança coleta informações sobre os padrões de atividade e as configurações de recursos do seu ambiente. Ela não coleta o conteúdo real de seus buckets, registros de banco de dados ou dados de aplicações do Amazon S3. A Resposta a Incidentes de Segurança coleta "quem fez o quê e quando" em vez dos dados subjacentes em si.

Estes dados de investigação de caso são coletados sob demanda para incidentes específicos e permanecem associados ao seu caso. A Resposta a Incidentes de Segurança retém esses dados por 90 dias por padrão para permitir que você revise o histórico de investigações, dê suporte as investigações em andamento ou de acompanhamento e atenda aos requisitos de documentação de auditoria e conformidade. Se você precisar excluir dados antes que o período de 90 dias expire, entre em contato o AWS Support para solicitar a exclusão antecipada.

Dados de descobertas de segurança

A Resposta a Incidentes de Segurança ingere continuamente os metadados das descobertas de segurança do Amazon GuardDuty e do AWS Security Hub CSPM e de todas as Regiões da AWS com suporte onde você habilitou esses serviços. Esses dados de descobertas incluem identificadores de recursos, tipos de descobertas, níveis de gravidade, recursos afetados e registros de data e hora de detecção. Diferentemente dos dados de investigação de casos, os dados das descobertas são ingeridos de forma automática e contínua para permitir que o Security Incident Response correlacione ameaças em todo o seu ambiente da AWS.

Os dados das descobertas não incluem os logs detalhados ou os dados brutos que geraram as descobertas, apenas os metadados sobre o que foi detectado, onde foi detectado e a gravidade da detecção. Esses metadados permitem que a Resposta a Incidentes de Segurança identifique padrões, correlacione eventos de segurança relacionados em todas as regiões e forneça uma análise abrangente de ameaças.

Processamento de agentes de investigação

O agente investigativo da Resposta a Incidentes de Segurança, desenvolvido pelo Amazon Bedrock, processa metadados dos dados de investigação do seu caso e dos dados de descobertas para gerar

insights, identificar padrões e recomendar ações de resposta. Esse processamento ocorre na região global do Amazon Bedrock como parte do fluxo de trabalho de análise do agente.

> **Important**
>
> O agente investigativo processa metadados de forma transitória e não armazena esses dados de forma persistente na região global do Amazon Bedrock. Os metadados são usados somente para gerar insights de investigação e não são retidos após a conclusão do processamento.

Noções básicas sobre a confidencialidade dos metadados

Embora a Resposta a Incidentes de Segurança não colete os dados de sua aplicação, os metadados coletados em todas as três categorias podem revelar informações confidenciais sobre seu ambiente e, potencialmente, sobre seus usuários. Considere os seguintes exemplos:

- Nomes de recursos como `patient-database-prod` ou `financial-records-2026` indicam a finalidade e a confidencialidade dos recursos.
- As consultas de DNS como `user12345.internal.app.com` podem conter identificadores de usuário ou informações internas do sistema.
- Os padrões de chamada de API podem revelar processos de negócios e fluxos de trabalho operacionais.

Organizações em setores regulamentados devem avaliar se esses metadados se enquadram em seus requisitos de conformidade, mesmo que não sejam os dados regulamentados em si.

Residência de dados e comportamento regional

As três categorias de dados na Resposta a Incidentes de Segurança têm diferentes locais de armazenamento e padrões regionais de movimentação. Compreender esses padrões é fundamental para organizações com requisitos de residência de dados.

Tópicos

- Armazenamento e movimentação de dados de investigação de casos
- Descobertas de segurança, armazenamento e movimentação de dados
- Local de processamento do agente investigativo

- Disponibilidade regional

Armazenamento e movimentação de dados de investigação de casos

Os dados da investigação do caso permanecem na Região da AWS onde você abre o caso do incidente de segurança. Quando você cria um caso em uma região específica, todos os logs, metadados e informações do caso coletados para essa investigação são armazenados nessa região. Esses dados não são transferidos para outras regiões.

Para Regiões da AWS padrão (regiões disponíveis por padrão), os dados da investigação do caso permanecem na região em que o caso foi criado durante todo o ciclo de vida da investigação e o período de retenção de 90 dias.

Para regiões opcionais da AWS, como Oriente Médio (Bahrein), África (Cidade do Cabo) ou Ásia-Pacífico (Hong Kong), os dados de investigação de caso também permanecem na região em que o caso foi criado. No entanto, se você habilitar a Resposta a Incidentes de Segurança em uma região opcional, todos os dados de casos dessa região são replicados automaticamente para a região Leste dos EUA (Norte da Virgínia) (us-east-1), para gerenciamento e análise centralizados.

> **Important**
>
> Se você opera em regiões opcionais, seus dados de investigação de caso fluem automaticamente para us-east-1. Organizações com requisitos rígidos de residência de dados devem avaliar se essa replicação entre regiões é compatível com suas obrigações de conformidade. Os dados nunca fluem entre diferentes regiões opcionais, e os dados de regiões não opcionais nunca são replicados para regiões opcionais.

Descobertas de segurança, armazenamento e movimentação de dados

Os metadados das descobertas de segurança atravessam regiões, independentemente da origem das descobertas. A Resposta a Incidentes de Segurança ingere descobertas do Amazon GuardDuty e do AWS Security Hub CSPM entre todas as regiões em que você habilitou esses serviços e correlaciona esses metadados entre regiões para identificar ameaças distribuídas e padrões de ataque.

Para Regiões da AWS padrão, os metadados de descobertas de todas as regiões estão acessíveis para correlação e análise. Essa movimentação entre regiões permite que a Resposta a Incidentes

de Segurança detecte ameaças que abrangem várias regiões, como um invasor se movendo lateralmente pela sua infraestrutura.

Para regiões opcionais da AWS, os metadados das descobertas seguem o mesmo padrão de replicação dos dados da investigação de caso. As descobertas das regiões opcionais são replicadas para as Regiões da AWS comerciais (regiões que não sejam as regiões AWS GovCloud (US) e as regiões da China) para análise centralizada junto com as descobertas de outras regiões.

Os metadados das descobertas incluem somente identificadores de recursos, tipos de descobertas e informações de gravidade, não os logs detalhados ou os dados brutos que geraram as descobertas. Esses metadados permitem a correlação de ameaças e, ao mesmo tempo, minimizam o volume de dados que ultrapassa os limites da região.

Local de processamento do agente investigativo

O agente investigativo da Resposta a Incidentes de Segurança processa metadados na região global do Amazon Bedrock, independentemente da região de origem dos dados do seu caso ou das descobertas. Esse processamento é transitório, já que o agente analisa os metadados para gerar insights e recomendações, mas não armazena os metadados de forma persistente na infraestrutura do Amazon Bedrock.

Quando o agente conclui sua análise, os insights e recomendações gerados são armazenados com seus dados de investigação de caso na região em que o caso foi criado. Os metadados usados para processamento não são retidos na região global Amazon Bedrock após a conclusão da análise.

Disponibilidade regional

Para obter informações sobre quais regiões oferecem suporte à Resposta a Incidentes de Segurança, consulte Serviços regionais da AWS.

Acesso a dados e permissões

Dois grupos podem acessar seus dados do AWS Security Incident Response:

- Seus usuários autorizados: os usuários e perfis do IAM aos quais você concede permissões da Resposta a Incidentes de Segurança.
- Equipes de resposta a incidentes na AWS: funcionários da AWS e prestadores de serviços aprovados que investigam seus casos.

Tópicos

- Acesso do responsável por resposta a incidentes da AWS
- Registro em log e auditabilidade de acesso
- Controlar o acesso com o IAM

Acesso do responsável por resposta a incidentes da AWS

A AWS opera a Resposta a Incidentes de Segurança como um serviço “siga o sol”, oferecendo cobertura 24 horas por dia, 7 dias por semana, por meio de equipes de resposta a incidentes localizadas nas Américas, Europa e Ásia-Pacífico. Quando você abre um caso de incidente de segurança, o respondente designado para o caso pode estar localizado em qualquer uma dessas regiões. Todos os respondente de incidentes da AWS passam por verificações de antecedentes e concluem o treinamento de segurança antes de obter acesso aos dados do cliente.

> **Important**
>
> A localização geográfica do responsável pela resposta a incidente que está lidando com seu caso pode variar de acordo com o momento em que você abre o caso e a disponibilidade do respondente. Organizações com requisitos sobre quem pode acessar seus dados devem avaliar se esse modelo de acesso global é compatível com suas políticas.

Registro em log e auditabilidade de acesso

Cada acesso aos seus dados da Resposta a Incidentes de Segurança é registrado em log. Você pode auditar quem acessou seus dados, quais dados foram acessados e quando o acesso ocorreu. Esses logs de auditoria oferecem suporte a seus requisitos de monitoramento de conformidade e segurança.

Controlar o acesso com o IAM

Você controla quais usuários e perfis em sua conta da Conta da AWS podem acessar a Resposta a Incidentes de Segurança por meio de políticas do IAM. Para obter informações sobre como configurar as permissões do IAM para a Resposta a Incidentes de Segurança, consulte Gerenciamento de Identidade e Acesso.

Privacidade do tráfego entre redes

Tráfego entre clientes de serviço e on-premises e as aplicações

Você tem duas opções de conectividade entre sua rede privada e a AWS:

- Uma conexão do AWS Site-to-Site VPN. Para obter mais informações, consulte O que é o AWS Site-to-Site VPN? no Guia do usuário do AWS Site-to-Site VPN.
- Uma conexão do Direct Connect. Para obter mais informações, consulte O que é o Direct Connect? no Guia do usuário do Direct Connect.

O acesso ao AWS Security Incident Response via rede é por meio de APIs publicadas pela AWS. Os clientes devem ser compatíveis com o Transport Layer Security (TLS) 1.2. Recomendamos o TLS 1.3. Os clientes também devem ter suporte a pacotes de criptografia com sigilo de encaminhamento perfeito (PFS) como Ephemeral Diffie-Hellman (DHE) ou Ephemeral Elliptic Curve Diffie-Hellman (ECDHE). A maioria dos sistemas modernos como Java 7 e versões posteriores oferece suporte a esses modos. Além disso, você deve assinar solicitações usando um ID da chave de acesso e uma chave de acesso secreta associados a uma entidade principal do IAM. Ou você pode usar o AWS Security Token Service (STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Tráfego entre recursos da AWS na mesma região

Um endpoint da Amazon Virtual Private Cloud (Amazon VPC) para a AWS Security Incident Response consiste em uma entidade lógica dentro de uma VPC que permite conectividade somente com a AWS Security Incident Response. A Amazon VPC realiza o roteamento das solicitações para a AWS Security Incident Response e encaminha as respostas de volta à VPC. Para obter mais informações, consulte Endpoints da VPC no Guia do usuário da Amazon VPC. Para obter exemplos de políticas que podem ser usadas para controlar o acesso a partir de endpoints da VPC, consulte Usar políticas do IAM para controlar o acesso ao DynamoDB.

> **Note**
>
> Os endpoints da Amazon VPC não podem ser acessados via AWS Site-to-Site VPN ou Direct Connect.

Gerenciamento de Identidade e Acesso

O AWS Identity and Access Management (IAM) é um serviço da AWS que auxilia administradores a controlar o acesso aos recursos da AWS. Os administradores do IAM são responsáveis por controlar quais entidades principais estão autenticadas (com login realizado) e autorizadas (com permissões obtidas) a usar os recursos da AWS Security Incident Response. O IAM é um AWS serviço da que pode ser usado sem custo adicional.

Tópicos

Público

O uso do AWS Identity and Access Management (IAM) varia dependendo do trabalho que for realizado no AWS Security Incident Response.

Administradores responsáveis pela segurança

Recomenda-se que esses usuários usem a política gerenciada AWSSecurityIncidentResponseFullAccess para garantir que tenham acesso de leitura e de gravação aos recursos de associação e de caso.

Observadores de casos

Esses indivíduos não têm acesso autorizado a todos os casos, apenas àqueles casos específicos para os quais foi concedida autorização expressa.

Membros da Equipe de Resposta a Incidentes

Os membros da equipe podem receber tanto a associação completa quanto o acesso aos casos. É recomendado que apenas alguns indivíduos tenham autoridade sobre a associação do serviço, mas que todos tenham acesso irrestrito a todos os casos criados e gerenciados por meio do serviço. Para obter mais informações, consulte AWS Security Incident Response managed policies.

Autenticação com identidades

A autenticação é a forma como fazer login na AWS usando suas credenciais de identidade. É necessário estar autenticado (conectado à AWS) como usuário raiz da conta AWS, como usuário do IAM ou assumindo um perfil do IAM.

É possível fazer login na AWS como uma identidade federada usando credenciais fornecidas por uma fonte de identidades. AWS Os usuários do Centro de Identidade do IAM (IAM Identity Center), a autenticação única da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Quando você acessa a AWS usando a federação, está indiretamente assumindo um perfil.

Dependendo do seu tipo de usuário, você pode acessar o Console de Gerenciamento da AWS ou o portal de acesso da AWS. Para obter mais informações sobre como fazer login na AWS, consulte Como fazer login na sua conta da AWS, no Guia do usuário de Início de Sessão da AWS.

Se você acessar a AWS de forma programática, a AWS fornecerá um kit de desenvolvimento de software (SDK) e uma interface de linha de comandos (CLI) para você assinar de forma criptográfica as solicitações usando as suas credenciais. Se você não utilizar as ferramentas AWS, deverá designar as solicitações por conta própria. Para obter mais informações sobre como usar o método recomendado para designar solicitações por conta própria, consulte Designando solicitações de API AWS no Guia do usuário do IAM.

Independentemente do método de autenticação usado, pode ser necessário fornecer informações adicionais de segurança. Por exemplo, a AWS recomenda o uso da autenticação multifator (MFA) para aumentar a segurança de sua conta. Para saber mais informações, consulte Autenticação multifator no Guia do usuário do Centro de Identidade do AWS IAM e Usar a autenticação multifator (MFA) na AWS no Guia do usuário do IAM.

AWS Usuário raiz de conta da

Ao criar uma conta AWS, você começa com uma identidade de login que tem acesso completo a todos os serviços e recursos da conta AWS. Essa identidade é chamada de usuário-raiz da conta da AWS e é acessada mediante login com o endereço de e-mail e a senha usados para criar a conta. Nunca use o usuário-raiz para a realização das suas tarefas diárias e tome medidas para proteger as credenciais do usuário-raiz. Use-as apenas para executar tarefas que somente o usuário-raiz pode realizar. Para obter a lista completa das tarefas que exigem login como usuário-raiz, consulte Tarefas que exigem credenciais de usuário-raiz no Guia do Usuário do IAM.

Identidade federada

É uma prática recomendada exigir que usuários humanos, incluindo aqueles que necessitam de acesso de administrador, usem federação com um provedor de identidades para acessar os serviços da AWS por meio de credenciais temporárias.

Identidade federada é um usuário de seu diretório de usuários corporativos, um provedor de identidades da Web, AWS Directory Service, o diretório do Centro de Identidade ou qualquer usuário que acesse os serviços da AWS usando credenciais fornecidas por meio de uma fonte de identidade. Quando as identidades federadas acessam as contas da AWS, elas assumem perfis, e os perfis fornecem credenciais temporárias.

Para obter um gerenciamento centralizado de acesso, recomendamos o uso do Centro de Identidade do AWS IAM. É possível criar usuários e grupos diretamente no Centro de Identidade do IAM ou conectar e sincronizar um conjunto de usuários e de grupos usando sua própria fonte de identidades para utilizá-los em todas as suas contas e aplicações da AWS. Para obter mais informações sobre o Centro de Identidade do IAM, consulte O que é o Centro de Identidade do IAM?, no Guia do usuário do Centro de Identidade do AWS IAM.

Grupos e usuários do IAM

Um usuário do IAM é uma identidade dentro da sua conta da AWS que tem permissões específicas para uma única pessoa ou aplicação. É recomendável priorizar o uso de credenciais temporárias, em vez de criar usuários do IAM que usam credenciais de longo prazo, como senhas e chaves de acesso. Caso você tenha um caso de uso específico que exija credenciais de longo prazo com usuários do IAM, recomendamos alterar as chaves de acesso. Para obter mais informações, consulte Alternar as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do Usuário do IAM.

Um grupo do IAM é uma identidade que especifica um conjunto de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdmins e conceder a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar um usuário do IAM (em vez de um perfil) no Guia do usuário do IAM.

Perfis do IAM

Um Perfil do IAM é uma identidade dentro da sua conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. É possível assumir um perfil do IAM temporariamente no Console de Gerenciamento da AWS ao

alterar os perfis. É possível assumir um perfil chamando uma operação da AWS CLI ou da AWS API, ou usando um URL personalizado. Para obter mais informações sobre métodos para o uso de perfis, consulte Utilizar perfis do IAM no Guia do usuário do IAM.

Perfis do IAM com credenciais temporárias são úteis nas situações a seguir:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, é possível criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas por ele. Para obter mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidades de terceiros no Guia do usuário do IAM. Se usar o Centro de Identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de Identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter mais informações sobre os conjuntos de permissões, consulte Conjuntos de permissões no Guia do usuário do Centro de Identidade do AWS IAM.
- Permissões temporárias para usuários do IAM: um usuário ou um perfil do IAM pode presumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, alguns serviços da AWS permitem que você anexe uma política diretamente a um recurso (em vez de usar um perfil como proxy). Para conhecer a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.
- Acesso entre serviços: alguns serviços da AWS usam recursos em outros serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicações no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões da entidade principal da chamada, usando um perfil de serviço ou um perfil vinculado ao serviço.
  - Perfil de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir uma função de serviço do IAM. Para obter mais informações, consulte Criação de uma função para delegar permissões a um AWS serviço no Guia do usuário do IAM.
  - Função vinculada a serviço: uma função vinculada a serviço é um tipo de função de serviço vinculada a um serviço da AWS. O serviço pode assumir o perfil de executar uma ação em seu nome. Os Perfis vinculados a serviços aparecem em sua conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados ao serviço.

- Aplicações em execução no Amazon EC2: é possível usar um perfil do IAM para gerenciar credenciais temporárias para aplicações em execução em uma instância do EC2 e fazer solicitações da AWS CLI ou da AWS API. É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir um perfil da AWS a uma instância do EC2 e torná-lo disponível para todas as suas aplicações, você cria um perfil de instância que é vinculado à instância. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para obter mais informações, consulte Utilizar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para saber se deseja usar perfis do IAM, consulte Quando criar um perfil do IAM (em vez de um usuário) no Guia do usuário do IAM.

Como o AWS Security Incident Response funciona com o IAM

O AWS Identity and Access Management (IAM) é um serviço da AWS que ajuda a controlar o acesso aos atributos da AWS de forma segura. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (ter permissões) a usar os recursos do AWS Security Incident Response. O IAM é um serviço da AWS que pode ser usado sem custo adicional.

Atributos do IAM que você pode usar com o AWS Security Incident Response	
Recurso do IAM	Alinhamento de serviços
Políticas baseadas em identidade	Sim
Políticas baseadas em recurso	Não
Ações de políticas	Sim
Recursos de políticas	Sim
Chaves de condições em políticas	Sim (global)
ACLs	Não
ABAC (tags em políticas)	Sim

Atributos do IAM que você pode usar com o AWS Security Incident Response	
Credenciais temporárias	Sim
Sessões de acesso direto (FAS)	Sim
Perfis de serviço	Não
Perfis vinculados ao serviço	Sim

Tópicos

- Políticas do baseadas em identidade para o AWS Security Incident Response
- Chaves de condição de políticas para AWS Security Incident Response
- Listas de controle de acesso (ACLs) em AWS Security Incident Response

Políticas do baseadas em identidade para o AWS Security Incident Response

As políticas baseadas em identidade são documentos de políticas de permissões JSON que podem ser anexados a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criando políticas do IAM no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elemento de política JSON do IAM no Guia do usuário do IAM.

Tópicos

- Exemplos de políticas baseadas em identidade
- Práticas recomendadas de política
- Usar o console do AWS Security Incident Response
- Permitir que os usuários visualizem suas próprias permissões

- Políticas baseadas em recurso
- Ações de políticas

Exemplos de políticas baseadas em identidade

Por padrão, usuários e perfis não têm permissão para criar ou modificar recursos do AWS Security Incident Response. Além disso, eles não podem executar tarefas ao usar o Console de Gerenciamento da AWS, a AWS Command Line Interface (AWS CLI) ou a API da AWS. Um administrador do IAM pode criar políticas do IAM para conceder permissões aos usuários a fim de que realizem ações relacionadas aos recursos de que necessitam. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem presumir os perfis.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documento de política JSON, consulte Criação de políticas do IAM no Guia do Usuário do IAM.

Para obter mais detalhes sobre as ações e os tipos de recurso definidos pela Resposta a Incidentes de Segurança da AWS, incluindo o formato dos ARNs para cada tipo de recurso, consulte Actions, resources, and condition keys for AWS Security Incident Response na Referência de autorização de serviços.

Práticas recomendadas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do AWS Security Incident Response em sua conta. Essas ações podem incorrer em custos para sua conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo: para começar a conceder permissões a seus usuários e workloads, use as políticas gerenciadas pela AWS, que concedem permissões para muitos casos de uso comuns. Elas estão disponíveis em sua conta AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente da AWS que são específicas para seus casos de uso. Para saber mais, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do IAM.

Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para saber mais sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.

Use condições nas políticas do IAM para restringir ainda mais o acesso: é possível adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, é possível escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso a ações de serviço se elas forem usadas por meio de um serviço específico do AWS, como o AWS CloudFormation. Para saber mais, consulte Elementos da política JSON do IAM: condição no Guia do usuário do IAM.

Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de 100 verificações de política e recomendações acionáveis para ajudá-lo a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do usuário do IAM.

Exigir autenticação multifator (MFA) - se você tiver um cenário que exija usuários do IAM ou um usuário raiz na sua conta AWS, ative a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do Usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte Práticas Recomendadas de Segurança no IAM no Guia do Usuário do IAM.

Usar o console do AWS Security Incident Response

Para acessar https://console.aws.amazon.com/security-ir/, é necessário ter um conjunto mínimo de permissões. Essas permissões dão autorização para que você liste e visualize detalhes sobre os recursos do AWS Security Incident Response na sua conta da AWS. Caso crie uma política baseada em identidade mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Você não precisa conceder permissões mínimas do console para os usuários que estão fazendo chamadas somente com a CLI da AWS ou a API da AWS. Em vez disso, permita o acesso somente a ações que correspondam à operação de API que estiverem tentando executar.

Anexe a política gerenciada pela AWS AWS Security Incident Response Access ou ReadOnly para garantir que usuários e perfis possam usar o console do serviço. Para obter informações, consulte Adicionar permissões a um usuário no Guia do usuário do IAM.

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como criar uma política que permita que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou de forma programática usando a AWS CLI ou a API da AWS.

Políticas baseadas em recurso

Políticas baseadas em recursos na Resposta a Incidentes de Segurança da AWS

Compatibilidade com políticas baseadas em recursos: não

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os principais podem incluir contas, usuários, funções, usuários federados ou serviços da AWS.

Para obter mais informações, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Ações de políticas

Ações de política para a AWS Security Incident Response

Suporte para ações de política: sim

Os administradores podem usar as políticas JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento “Action” de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de políticas geralmente têm o mesmo nome que a operação de API da AWS associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para visualizar a lista de ações da AWS Security Incident Response, consulte “Actions defined by AWS Security Incident Response“ na Referência de autorização de serviços.

As ações de políticas no AWS Security Incident Response usam o seguinte prefixo antes da ação:

AWS Security Incident Response -identity

Para especificar várias ações em uma única declaração, separe-as com vírgulas.

“Action”: [“AWS Security Incident Response -identity:action1”, “AWS Security Incident Response -identity:action2”]

Recursos de política para a Resposta a Incidentes de Segurança da Amazon AWS

Suporte para recursos de política: Sim | Administradores podem usar políticas JSON da AWS para especificar quem tem acesso a quais recursos. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento “Resource” da política JSON especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento Resource ou NotResource. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

"Resource": "*"

Chaves de condição de políticas para AWS Security Incident Response

Compatível com chaves de condição de política específicas de serviço: não

Os administradores podem usar as políticas JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento “Condition” (ou bloco “Condition”) permite especificar as condições sob as quais uma declaração está em vigor. O elemento Condition é opcional. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar diversos elementos “Condition” em uma declaração, ou múltiplas chaves em um único elemento “Condition”, a AWS os avalia usando uma operação lógica E. Se diversos valores

forem especificados para uma única chave de condição, a AWS avalia a condição usando uma operação lógica OU. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um recurso somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos da política do IAM: variáveis e tags no Guia do usuário do IAM.

A AWS oferece compatibilidade com chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição globais da AWS, consulte Chaves de contexto de condição globais da AWS no Guia do usuário do IAM.

Listas de controle de acesso (ACLs) em AWS Security Incident Response

Compatível com ACLs: não

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

Controle de acesso por atributo (ABAC) com a Resposta a Incidentes de Segurança da AWS

Compatível com ABAC (tags em políticas): sim

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define as permissões com base em atributos. Na AWS, esses atributos são chamados de tags. É possível anexar tags a entidades do IAM (usuários ou perfis) e a muitos recursos da AWS. Marcar de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela estiver tentando acessar. O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `AWS:ResourceTag/key-name`, `AWS:RequestTag/key-name` ou chaves de condição `AWS:TagKeys`. Se um serviço for compatível com as três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial Para obter mais informações sobre o ABAC, consulte O que é ABAC? no Guia do Usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso por atributo (ABAC) no Guia do usuário do AWS Identity and Access Management.

Credenciais temporárias com o AWS Security Incident Response

Compatível com credenciais temporárias: sim

Os serviços da AWS não funcionam quando você acessa usando credenciais temporárias. Para obter informações adicionais, incluindo quais serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS compatíveis com o IAM no Guia do usuário do AWS Identity and Access Management. Você está usando credenciais temporárias se fizer login no Console de Gerenciamento da AWS por qualquer método, exceto nome de usuário e uma senha. Por exemplo, quando você acessa a AWS usando o link de autenticação única (SSO) da sua empresa, esse processo cria credenciais temporárias automaticamente. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar funções, consulte Alternar para um perfil (console) no Guia do usuário do IAM.

É possível criar credenciais temporárias de forma manual por meio da AWS CLI ou da API da AWS. Em seguida, você pode usar essas credenciais temporárias para acessar a AWS. A AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte Credenciais de segurança temporárias no IAM.

Sessões de acesso direto para o AWS Security Incident Response

Compatibilidade com o recurso de encaminhamento de sessões de acesso (FAS): sim

O usuário ou perfil do IAM usado para executar ações na AWS é considerado uma entidade principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. A FAS usa as permissões do entidade principal que chama um serviço da AWS, combinadas com o serviço da AWS solicitante, para fazer solicitações a serviços downstream. As solicitações FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros serviços ou recursos do AWS para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.

Solução de problemas de identidade e acesso AWS Security Incident Response

Use as informações apresentadas a seguir para ajudar a diagnosticar e corrigir problemas comuns que podem ocorrer ao trabalhar com a Resposta a Incidentes de Segurança da AWS e o IAM.

Tópicos

- Não tenho autorização para executar uma ação
- Não estou autorizado a executar iam:PassRole
- Quero permitir que pessoas fora da minha conta da AWS acessem meus recursos do AWS Security Incident Response

Não tenho autorização para executar uma ação

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro apresentado no exemplo a seguir ocorre quando o usuário do IAM “mateojackson” tenta usar o console para visualizar detalhes sobre o recurso fictício “my-example-widget”, mas não tem a permissão fictícia “AWS Security Incident Response :GetWidget”.

User: arn:AWS:iam::123456789012:user/mateojackson is not authorized to perform: AWS Security Incident Response :GetWidget on resource: my-example-widget

Nesse caso, a política para o usuário “mateojackson” deve ser atualizada para permitir o acesso ao recurso “my-example-widget” por meio da ação “AWS Security Incident Response :GetWidget”.

Se você precisar de ajuda, entre em contato com seu administrador AWS. Seu administrador é a pessoa que forneceu suas credenciais de login.

Não tenho autorização para executar o **`iam:PassRole`** | Se você receber uma mensagem de erro informando que não tem autorização para executar a ação `iam:PassRole`, suas políticas devem ser atualizadas para permitir que você transmita um perfil ao AWS Security Incident Response.

Alguns serviços da AWS permitem que você passe um perfil existente para o serviço, em vez de criar um novo perfil de serviço ou perfil vinculado ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O erro apresentado no exemplo a seguir ocorre quando um usuário do IAM chamado “marymajor” tenta usar o console para executar uma ação na Resposta a Incidentes de Segurança da AWS. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

User: arn:AWS:iam::123456789012:user/marymajor is not authorized to perform: `iam:PassRole`

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`. Se você precisar de ajuda, entre em contato com seu administrador AWS. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas de fora da minha conta da AWS acessem os recursos do AWS Security Incident Response

Você pode criar uma função que os usuários de outras contas ou pessoas fora da sua organização possam usar para acessar seus recursos. É possível especificar quem é confiável para assumir o perfil.

Para saber mais, consulte:

- Para saber se o Amazon AWS Security Incident Response é compatível com esses recursos, consulte “How AWS Security Incident Response works with IAM”.
- Para saber como conceder acesso a seus recursos em todas as contas da AWS pertencentes a você, consulte Fornecimento de acesso a um usuário do IAM em outra conta da AWS pertencente a você no Guia de Usuário do IAM.
- Para saber como conceder acesso aos recursos para contas da AWS de terceiros, consulte Fornecer acesso a contas da AWS pertencentes a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Uso de perfis de serviço

Compatível com perfis de serviço: não

O perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criação de uma função para delegar permissões a um AWS serviço no Guia do usuário do IAM.

Uso de perfis vinculados ao serviço

Funções vinculadas ao serviço para o AWS Security Incident Response

Tópicos

- SLR da AWS: AWSServiceRoleForSecurityIncidentResponse

- SLR da AWS: AWSServiceRoleForSecurityIncidentResponse_Triage
- Regiões compatíveis com funções vinculadas ao serviço do AWS Security Incident Response

Compatibilidade com perfis vinculados a serviços: sim

Um perfil vinculado ao serviço é um tipo de perfil de serviço vinculado a um serviço da AWS. O serviço pode assumir o perfil de executar uma ação em seu nome. Os Perfis vinculados a serviços aparecem em sua conta da AWS e são de propriedade do serviço. Um administrador do AWS Identity and Access Management pode visualizar, mas não pode editar as permissões para funções vinculadas ao serviço.

Uma perfil vinculada ao serviço facilita a configuração do AWS Security Incident Response porque você não precisa adicionar as permissões necessárias manualmente. AWS Security Incident Response define as permissões de seus perfis vinculados ao serviço e, a menos que definido de outra forma, somente AWS Security Incident Response pode assumir suas perfis. As permissões definidas incluem a política de confiança e a política de permissões. Essa política não pode ser anexada a nenhuma outra entidade do IAM.

Para obter mais informações sobre outros serviços que são compatíveis com perfis vinculados ao serviço, consulte Serviços da AWS que funcionam com o IAM e procure os serviços que apresentam Sim na coluna de perfis vinculados ao serviço. Escolha um Sim com um link para visualizar a documentação do perfil vinculado a esse serviço.

SLR da AWS: AWSServiceRoleForSecurityIncidentResponse

A AWS Security Incident Response faz uso do perfil vinculado ao serviço (SLR, na sigla em inglês) denominado AWSServiceRoleForSecurityIncidentResponse, uma política da AWS Security Incident Response para identificar contas com assinatura, criar casos e etiquetar recursos relacionados.

Permissões

O perfil vinculado ao serviço AWSServiceRoleForSecurityIncidentResponse confia no seguinte serviço para assumir o perfil:

- `triage.security-ir.amazonaws.com`

Anexada a esse perfil está a política gerenciada pela AWS denominada AWSSecurityIncidentResponseServiceRolePolicy. O serviço usa esse perfil para executar ações nos seguintes recursos:

- AWS Organizations: permite que o serviço consulte contas de associação para uso com o serviço.
- CreateCase: permite que o serviço crie casos de serviços em nome das contas de associação.
- ListCases: permite que o agente de IA do serviço visualize casos para fazer a investigação de segurança.
- UpdateCase: permite que o agente de IA do serviço atualize os metadados do caso.
- CreateCaseComment: permite que o agente de IA do serviço publique seus resultados como um comentário do caso.
- ListComments: permite que o agente de IA do serviço visualize os comentários de casos que são necessários para realizar investigações automatizadas.
- TagResource: permite que o serviço marque recursos configurados como parte do serviço.

Gerenciamento do perfil

Não é necessário criar manualmente um perfil vinculado ao serviço. Quando você realiza a integração da AWS Security Incident Response no Console de gerenciamento da AWS, na AWS CLI ou na API da AWS, o serviço cria automaticamente o perfil vinculado ao serviço para você.

> **Note**
>
> Se você criou uma associação usando uma conta de administrador delegado, os perfis vinculados ao serviço precisam ser criados manualmente nas contas gerenciais do AWS Organizations.

Se excluir esse perfil vinculado ao serviço e precisar criá-lo novamente, será possível usar esse mesmo processo para recriar o perfil em sua conta. Quando você realiza a integração do serviço, ele cria novamente o perfil vinculado ao serviço para você.

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua um perfil vinculado a serviço. Para ter mais informações, consulte Permissões de função vinculada a serviços no Guia do usuário do IAM.

SLR da AWS: AWSServiceRoleForSecurityIncidentResponse_Triage

A AWS Security Incident Response usa o perfil vinculado ao serviço (SLR) denominado AWSServiceRoleForSecurityIncidentResponse_Triage, uma política da AWS Security Incident Response para monitorar continuamente seu ambiente em busca de ameaças de segurança, ajustar

serviços de segurança para reduzir o ruído de alertas e coletar informações para investigar possíveis incidentes.

Permissões

O perfil vinculado ao serviço AWSServiceRoleForSecurityIncidentResponse_Triage confia no seguinte serviço para assumir o perfil:

- `triage.security-ir.amazonaws.com`

Anexada a esse perfil está a política gerenciada pela AWS denominada AWSSecurityIncidentResponseTriageServiceRolePolicy. O serviço usa esse perfil para executar ações nos seguintes recursos:

- Eventos: permite que o serviço crie uma regra gerenciada do Amazon EventBridge. Esta regra constitui a infraestrutura necessária em sua conta da AWS para fornecer eventos da sua conta ao serviço. Essa ação é executada em qualquer recurso da AWS gerenciado pelo `triage.security-ir.amazonaws.com`.
- Amazon GuardDuty: permite que o serviço ajuste os serviços de segurança para reduzir o ruído de alertas, coletar informações para investigar possíveis incidentes e iniciar varreduras de malware do GuardDuty.
- AWS Security Hub CSPM: permite que o serviço liste os padrões e as integrações com produtos habilitados, liste os membros e as contas de administradores da organização, e ajuste os serviços de segurança para reduzir o ruído de alertas e coletar informações para investigar possíveis incidentes.
- AWS Identity and Access Management: permite que o serviço recupere informações sobre o perfil vinculado ao serviço `AWSServiceRoleForAmazonGuardDutyMalwareProtection` para verificar se o GuardDuty MalwareProtection está configurado.
- AWS Security Incident Response: permite que o serviço crie e atualize casos, e marque recursos, limitado aos recursos marcados com `SecurityIncidentResponseManaged=true`. Permite que o serviço leia as informações de associação (GetMembership, ListMemberships).

Gerenciamento do perfil

Não é necessário criar manualmente um perfil vinculado ao serviço. Quando você realiza a integração da AWS Security Incident Response no Console de gerenciamento da AWS, na AWS CLI ou na API da AWS, o serviço cria automaticamente o perfil vinculado ao serviço para você.

Se excluir esse perfil vinculado ao serviço e precisar criá-lo novamente, será possível usar esse mesmo processo para recriar o perfil em sua conta. Quando você realiza a integração do serviço, ele cria novamente o perfil vinculado ao serviço para você.

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua um perfil vinculado a serviço. Para ter mais informações, consulte Permissões de função vinculada a serviços no Guia do usuário do IAM.

Regiões compatíveis com funções vinculadas ao serviço do AWS Security Incident Response

O AWS Security Incident Response oferece suporte a funções vinculadas a serviços em todas as regiões em que o serviço está disponível.

- Leste dos EUA (Ohio)
- Oeste dos EUA (Oregon)
- Leste dos EUA (Virgínia)
- Europa (Frankfurt)
- Europa (Irlanda)
- Europa (Londres)
- Europa (Milão)
- Europe (Paris)
- Europa (Espanha)
- Europa (Estocolmo)
- Europa (Zurique)
- Ásia-Pacífico (Hong Kong)
- Ásia-Pacífico (Hyderabad)
- Ásia-Pacífico (Jacarta)
- Ásia-Pacífico (Melbourne)
- Ásia-Pacífico (Mumbai)
- Ásia-Pacífico (Seul)
- Ásia-Pacífico (Singapura)
- Ásia-Pacífico (Sydney)

- Ásia-Pacífico (Tóquio)
- Canadá (Central)
- Oriente Médio (Bahrein)
- Oriente Médio (Emirados Árabes Unidos)
- América do Sul (São Paulo)
- África (Cidade do Cabo)

Políticas gerenciadas pela AWS

Uma política gerenciada pela AWS é uma política autônoma criada e administrada pela AWS. As políticas gerenciadas pela AWS são criadas para fornecer permissões a vários casos de uso comuns e permitir a atribuição de permissões a usuários, grupos e perfis.

Para adicionar permissões a usuários, grupos e perfis, é mais fácil usar políticas gerenciadas pela AWS do que gravar políticas por conta própria. É necessário tempo e experiência para criar políticas gerenciadas pelo cliente do IAM que fornecem à sua equipe apenas as permissões de que precisam. Para começar rapidamente, é possível usar nossas políticas gerenciadas pela AWS. Essas políticas abrangem casos de uso comuns e estão disponíveis na sua conta da AWS. Para obter mais informações sobre políticas gerenciadas pela AWS, consulte Políticas gerenciadas pela AWS no Guia do usuário do IAM.

Os serviços da AWS são responsáveis por manter e atualizar as políticas gerenciadas pela AWS às quais estão associadas. Não é possível alterar as permissões em políticas gerenciadas pela AWS. Os serviços ocasionalmente acrescentam permissões adicionais a uma política gerenciada pela AWS para oferecer suporte a novos recursos. Esse tipo de atualização afeta todas as identidades (usuários, grupos e funções) em que a política está anexada. É mais provável que os serviços atualizem uma política gerenciada pela AWS quando um novo recurso for iniciado ou novas operações se tornarem disponíveis. Os serviços não removem permissões de uma política gerenciada pela AWS, portanto, as atualizações de políticas não suspendem suas permissões existentes.

Além disso, a AWS é compatível com políticas gerenciadas por perfis de trabalho que abrangem vários serviços. Por exemplo, a política ReadOnlyAccess política gerenciada pela AWS fornece acesso somente leitura a todos os serviços e recursos da AWS. Quando um serviço executa um novo atributo, a AWS adiciona permissões somente leitura para novas operações e recursos. Para obter uma lista e descrições das políticas de perfis de trabalho, consulte Políticas gerenciadas pela AWS para perfis de trabalho no Guia do usuário do IAM.

Tópicos

Política gerenciada pela AWS: AWSSecurityIncidentResponseServiceRolePolicy

A AWS Security Incident Response faz uso da política gerenciada pela AWS denominada AWSSecurityIncidentResponseServiceRolePolicy. Essa política gerenciada pela AWS está anexada ao perfil vinculado ao serviço AWSServiceRoleForSecurityIncidentResponse. A política concede acesso à AWS Security Incident Response para identificar contas assinantes, criar casos, atualizar casos, criar comentários de casos, listas casos, listar comentários de casos e etiquetar recursos relacionados.

> **Important**
>
> Não armazene informações de identificação pessoal (PII) ou outras informações confidenciais ou sensíveis em etiquetas. A AWS Security Incident Response usa etiquetas para fornecer serviços de administração. As etiquetas não devem ser usadas para armazenar dados sensíveis ou privados.

Detalhes relacionados às permissões

O serviço usa essa política para executar ações nos seguintes recursos:

- AWS Organizations: permite que o serviço consulte contas de associação para uso com o serviço.
- CreateCase: permite que o serviço crie casos de serviços em nome das contas de associação.
- ListCases: permite que o agente de IA do serviço visualize casos para fazer a investigação de segurança.
- UpdateCase: permite que o agente de IA do serviço atualize os metadados do caso.

- CreateCaseComment: permite que o agente de IA do serviço publique seus resultados como um comentário do caso.
- ListComments: permite que o agente de IA do serviço visualize os comentários de casos que são necessários para realizar investigações automatizadas.
- TagResource: permite que o serviço marque recursos configurados como parte do serviço.

Você pode visualizar as permissões associadas a esta política nas políticas gerenciadas pela AWS para AWSSecurityIncidentResponseServiceRolePolicy.

Política gerenciada pela AWS: AWSSecurityIncidentResponseFullAccess

A AWS Security Incident Response faz uso da política gerenciada pela AWS denominada AWSSecurityIncidentResponseAdmin. Essa política concede acesso total aos recursos do serviço e acesso a Serviços da AWS relacionados. Você pode usar essa política com suas entidades principais do IAM para adicionar permissões à AWS Security Incident Response rapidamente.

> **Important**
>
> Não armazene informações de identificação pessoal (PII) ou outras informações confidenciais ou sensíveis em etiquetas. A AWS Security Incident Response usa etiquetas para fornecer serviços de administração. As etiquetas não devem ser usadas para armazenar dados sensíveis ou privados.

Detalhes relacionados às permissões

O serviço usa essa política para executar ações nos seguintes recursos:

- Acesso somente de leitura para a entidade principal do IAM: concede a um usuário do serviço a capacidade de executar ações somente de leitura em recursos existentes da AWS Security Incident Response.
- Acesso de gravação para a entidade principal do IAM: concede a um usuário do serviço a capacidade de atualizar, modificar, excluir e criar recursos da AWS Security Incident Response.

Você pode visualizar as permissões associadas a esta política nas políticas gerenciadas pela AWS para AWSSecurityIncidentResponseFullAccess.

Política gerenciada pela AWS: AWSSecurityIncidentResponseReadOnlyAccess

A AWS Security Incident Response faz uso da política gerenciada pela AWS denominada AWSSecurityIncidentResponseReadOnlyAccess. A política concede acesso somente de leitura aos recursos de casos de serviços. Você pode usar essa política com suas entidades principais do IAM para adicionar permissões à AWS Security Incident Response rapidamente.

> **Important**
>
> Não armazene informações de identificação pessoal (PII) ou outras informações confidenciais ou sensíveis em etiquetas. A AWS Security Incident Response usa etiquetas para fornecer serviços de administração. As etiquetas não devem ser usadas para armazenar dados sensíveis ou privados.

Detalhes relacionados às permissões

O serviço usa essa política para executar ações nos seguintes recursos:

- Acesso somente de leitura para a entidade principal do IAM: concede a um usuário do serviço a capacidade de executar ações somente de leitura em recursos existentes da AWS Security Incident Response.

Você pode visualizar as permissões associadas a esta política nas políticas gerenciadas pela AWS para AWSSecurityIncidentResponseReadOnlyAccess.

Política gerenciada pela AWS: AWSSecurityIncidentResponseCaseFullAccess

A AWS Security Incident Response faz uso da política gerenciada pela AWS denominada AWSSecurityIncidentResponseCaseFullAccess. A política concede acesso total aos recursos de casos de serviços. Você pode usar essa política com suas entidades principais do IAM para adicionar permissões à AWS Security Incident Response rapidamente.

> **Important**
>
> Não armazene informações de identificação pessoal (PII) ou outras informações confidenciais ou sensíveis em etiquetas. A AWS Security Incident Response usa etiquetas

para fornecer serviços de administração. As etiquetas não devem ser usadas para armazenar dados sensíveis ou privados.

Detalhes relacionados às permissões

O serviço usa essa política para executar ações nos seguintes recursos:

- Acesso somente de leitura a casos para a entidade principal do IAM: concede a um usuário do serviço a capacidade de executar ações somente de leitura em casos existentes da AWS Security Incident Response.
- Acesso de gravação a casos para a entidade principal do IAM: concede a um usuário do serviço a capacidade de atualizar, modificar, excluir e criar casos da AWS Security Incident Response.

Você pode visualizar as permissões associadas a esta política nas políticas gerenciadas pela AWS para AWSSecurityIncidentResponseCaseFullAccess.

Política gerenciada pela AWS: AWSSecurityIncidentResponseTriageServiceRolePolicy

A AWS Security Incident Response faz uso da política gerenciada pela AWS denominada AWSSecurityIncidentResponseTriageServiceRolePolicy. Essa política gerenciada pela AWS está anexada ao perfil vinculado ao serviço AWSServiceRoleForSecurityIncidentResponse_Triage.

A política fornece à AWS Security Incident Response acesso para monitorar continuamente seu ambiente em busca de ameaças de segurança, ajustar serviços de segurança para reduzir o ruído de alertas e coletar informações para investigar possíveis incidentes. Não é possível anexar essa política a suas entidades do IAM.

> **Important**
>
> Não armazene informações de identificação pessoal (PII) ou outras informações confidenciais ou sensíveis em etiquetas. A AWS Security Incident Response usa etiquetas para fornecer serviços de administração. As etiquetas não devem ser usadas para armazenar dados sensíveis ou privados.

Detalhes relacionados às permissões

O serviço usa essa política para executar ações nos seguintes recursos:

- Eventos: permite que o serviço crie uma regra gerenciada do Amazon EventBridge. Esta regra constitui a infraestrutura necessária em sua conta da AWS para fornecer eventos da sua conta ao serviço. Essa ação é executada em qualquer recurso da AWS gerenciado pelo `triage.security-ir.amazonaws.com`.
- Amazon GuardDuty: permite que o serviço ajuste os serviços de segurança para reduzir o ruído de alertas, coletar informações para investigar possíveis incidentes e iniciar varreduras de malware do GuardDuty.
- AWS Security Hub CSPM: permite que o serviço liste os padrões e as integrações com produtos habilitados, liste os membros e as contas de administradores da organização, e ajuste os serviços de segurança para reduzir o ruído de alertas e coletar informações para investigar possíveis incidentes.
- AWS Identity and Access Management: permite que o serviço recupere informações sobre o perfil vinculado ao serviço `AWSServiceRoleForAmazonGuardDutyMalwareProtection` para verificar se o GuardDuty MalwareProtection está configurado.
- AWS Security Incident Response: permite que o serviço crie e atualize casos, e marque recursos, limitado aos recursos marcados com `SecurityIncidentResponseManaged=true`. Permite que o serviço leia as informações de associação (GetMembership, ListMemberships).

Você pode visualizar as permissões associadas a esta política nas políticas gerenciadas pela AWS para AWSSecurityIncidentResponseTriageServiceRolePolicy.

Atualizações da AWS Security Incident Response para SLRs e políticas gerenciadas

Confira detalhes sobre as atualizações nos perfis de SLRs e de políticas gerenciadas da AWS Security Incident Response desde que este serviço começou a monitorar essas alterações.

Alteração	Descrição	Data
Atualizado – `AWSSecurityIncidentResponse`	A política agora inclui a ação `security-ir:ListInvestigations` .	22 de abril de 2026

Alteração	Descrição	Data
ReadOnlyAccess		
Atualizado – AWSSecurityIncidentResponseFullAccess	A política agora usa `security-ir:*` em vez de listar ações `security-ir` explícitas. Oito novas permissões do AWS Organizations foram adicionadas (`organizations:ListAWSServiceAccessForOrganization`, `organizations:ListRoots`, `organizations:ListOrganizationalUnitsForParent`, `organizations:ListAccountsForParent`, `organizations:ListChildren`, `organizations:DescribeOrganizationalUnit`, `organizations:ListAccounts`, `eorganizations:DescribeAccount`) para dar suporte ao seletor de contas do console ao atualizar associações. A condição de MFA foi removida.	22 de abril de 2026
Atualizado – AWSSecurityIncidentResponseCaseFullAccess	A política agora inclui duas novas ações: `security-ir:ListInvestigations` e `security-ir:SendFeedback`. A condição de MFA foi removida.	22 de abril de 2026
Atualizado – AWSSecurityIncidentResponseTriageServiceRolePolicy	A política agora permite que o serviço modifique os filtros do GuardDuty marcados com `SecurityIncidentResponseManaged=true`, atualize as configurações do detector e inicie os varreduras de malware do GuardDuty. Ela permite que o serviço crie e gerencie as regras aplicadas automaticamente às descobertas do Security Hub CSPM e compreenda a estrutura organizacional.	27 de março de 2026

Alteração	Descrição	Data
Atualização: AWSSecurityIncidentResponseServiceRolePolicy	Agora a política executa as seguintes ações nos recursos a seguir: ListCases: permite que o agente de IA do serviço visualize casos para fazer a investigação de segurança UpdateCase: permite que o agente de IA do serviço atualize os metadados do caso. CreateCaseComment: permite que o agente de IA do serviço publique seus resultados como um comentário do caso ListComments: permite que o agente de IA do serviço visualize os comentários de casos que são necessários para realizar investigações automatizadas	Novembro de 2025
Atualização: AWSSecurityIncidentResponseServiceRolePolicy	A política inclui agora duas novas ações para `"organizations:DescribeAccount" "organizations:ListDelegatedAdministrators"` e uma nova condição: `"Condition": { "StringEquals": { "aws:ResourceAccount": "${aws:PrincipalAccount}" } }`	Novembro de 2025

Alteração	Descrição	Data
Atualizações no SLR com a adição de permissões para oferecer suporte aos direitos do serviço.	A política AWSSecurityIncidentResponseTriageServiceRolePolicy foi atualizada para adicionar as permissões security-ir:GetMembership, security-ir:ListMemberships, security-ir:UpdateCase, guardduty:ListFilters, guardduty:UpdateFilter, guardduty:DeleteFilter e guardduty:GetAdministratorAccount. A permissão guardduty:GetAdministratorAccount foi adicionada para facilitar o gerenciamento de filtros de arquivamento automático do GuardDuty em contas delegadas.	2 de junho de 2025
Novo SLR: AWSServiceRoleForSecurityIncidentResponse Nova política gerenciada: AWSSecurityIncidentResponseServiceRolePolicy.	Novo perfil vinculado ao serviço e nova política anexada que permitem o acesso do serviço às suas contas do AWS Organizations para identificar a associação.	1.º de dezembro de 2024

Alteração	Descrição	Data
Novo SLR: AWSServiceRoleForSecurityIncidentResponse_Triage Nova política gerenciada: AWSSecurityIncidentResponseTriageServiceRolePolicy	Novo perfil vinculado ao serviço e nova política anexada que permitem o acesso do serviço às suas contas do AWS Organizations para realizar a triagem de eventos de segurança.	1.º de dezembro de 2024
Nova política gerenciada: AWSSecurityIncidentResponseFullAccess	A AWS Security Incident Response adiciona um novo SLR para ser associado às entidades principais do IAM, permitindo ações de leitura e de gravação para o serviço.	1.º de dezembro de 2024
Novo perfil de política gerenciada: AWSSecurityIncidentResponseReadOnlyAccess	A AWS Security Incident Response adiciona um novo SLR para ser associado às entidades principais do IAM, permitindo ações de leitura.	1.º de dezembro de 2024

Alteração	Descrição	Data
Novo perfil de política gerenciada: AWSSecurityIncidentResponseCaseFullAccess	A AWS Security Incident Response adiciona um novo SLR para ser associado às entidades principais do IAM, permitindo ações de leitura e de gravação para os casos de serviços.	1.º de dezembro de 2024
Início do acompanhamento de alterações.	Início do acompanhamento das alterações nos SLRs e nas políticas gerenciadas da AWS Security Incident Response.	1.º de dezembro de 2024

Resposta a incidentes

Segurança e conformidade são uma responsabilidade compartilhada entre a AWS e o cliente. Esse modelo compartilhado pode ajudar a reduzir os encargos operacionais do cliente porque a AWS opera, gerencia e controla os componentes do sistema operacional do host e a camada de virtualização, incluindo a segurança física das instalações em que o serviço opera. O cliente assume o gerenciamento e a responsabilidade pelo sistema operacional convidado (inclusive por atualizações e correções de segurança) e por outro software de aplicação associado, bem como pela configuração do firewall dos grupos de segurança fornecido pela AWS. Para obter informações adicionais, consulte o Modelo de responsabilidade compartilhada da AWS.

Ao estabelecer uma referência de segurança que atenda aos objetivos de suas aplicações executadas na nuvem, você pode detectar desvios aos quais pode reagir. Como a resposta a incidentes de segurança pode ser um tópico complexo, recomendamos que você analise os seguintes recursos para compreender melhor o impacto que a resposta a incidentes e suas escolhas têm nas metas empresariais: o whitepaper Práticas recomendadas de segurança da AWS e o whitepaper Security Perspective of the AWS Cloud Adoption Framework (CAF).

Validação de conformidade

Auditores externos avaliam a segurança e a conformidade dos serviços da AWS como parte de vários programas de conformidade da AWS. Isso inclui SOC, PCI, FedRAMP, HIPAA e outros.

Para obter uma lista dos serviços da AWS no escopo de programas de conformidade específicos, consulte Serviços da AWS no escopo por programa de conformidade. Para obter informações gerais, consulte os programas de conformidade da AWS.

Você pode fazer download de relatórios de auditoria de terceiros usando o AWS Artifact. Para obter mais informações, consulte Download de relatórios no AWS Artifact.

Sua responsabilidade com relação à conformidade ao usar os serviços da AWS é determinada pela confidencialidade dos dados, pelos objetivos de conformidade da empresa e pelos regulamentos e leis aplicáveis. A AWS fornece os seguintes recursos para ajudar com a conformidade:

- Guias de início rápido sobre segurança e conformidade: esses guias de implantação abordam considerações relacionadas à arquitetura e fornecem etapas para implantar ambientes de referência com foco em segurança e em conformidade na AWS.
- Whitepaper “Architecting for HIPAA security and compliance”: este documento descreve como as empresas podem usar a AWS para criar aplicações compatíveis com a HIPAA.
- Recursos de conformidade da AWS: um conjunto de registros e de guias que são aplicáveis por setor ou por localização.
- Avaliação de recursos com o AWS Config Rules no guia do desenvolvedor do AWS Config: o AWS Config avalia o grau de conformidade das configurações dos seus recursos com práticas internas, diretrizes do setor e regulamentações.
- AWS Security Hub - Esse serviço AWS fornece uma visão abrangente do seu estado de segurança em AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- Amazon GuardDuty - Este serviço AWS detecta possíveis ameaças às suas contas AWS, workloads, contêineres e dados, monitorando seu ambiente em busca de atividades suspeitas e mal-intencionadas. O GuardDuty pode ajudar você a atender a diversos requisitos de conformidade, como o PCI DSS, com o cumprimento dos requisitos de detecção de intrusões requeridos por determinadas estruturas de conformidade.
- AWS Audit Manager: esse serviço da AWS ajuda a auditar continuamente o uso da AWS para simplificar a forma como você gerencia os riscos e a conformidade com regulamentos e padrões do setor.

Responsabilidade compartilhada para conformidade

Sua responsabilidade de conformidade ao usar o AWS Security Incident Response depende da confidencialidade dos seus dados, dos objetivos de conformidade da sua empresa e dos regulamentos e as leis aplicáveis. A AWS fornece a Resposta a Incidentes de Segurança como uma ferramenta para ajudar você a investigar e responder a incidentes de segurança. Você continua responsável por:

- Determinar se a Resposta a Incidentes de Segurança é apropriada para seus requisitos de conformidade.
- Configurar a Resposta a Incidentes de Segurança de acordo com suas políticas.
- Garantir que seu uso da Resposta a Incidentes de Segurança esteja em conformidade com os regulamentos aplicáveis.

Metadados como dados regulamentados

Embora a Resposta a Incidentes de Segurança não colete os dados de sua aplicação, os metadados que ela coleta podem estar de acordo com seus requisitos de conformidade. As organizações devem avaliar:

- Se os nomes e identificadores dos recursos constituem dados regulamentados.
- Se os logs de consulta ao DNS contêm informações pessoais.
- Se os padrões de chamada de API revelam informações comerciais protegidas.

Consulte suas equipes jurídicas e de conformidade para determinar como os metadados da Resposta a Incidentes de Segurança devem ser classificados de acordo com os regulamentos aplicáveis.

Registro em log e monitoramento na Resposta a Incidentes de Segurança da AWS

O monitoramento é uma parte essencial da manutenção da confiabilidade, da disponibilidade e da performance da AWS Security Incident Response e das demais soluções da AWS. Atualmente, a AWS Security Incident Response fornece suporte aos serviços da AWS apresentados a seguir para monitorar sua organização e as atividades que ocorrem dentro dela.

AWS CloudTrail: com o CloudTrail, é possível registrar as chamadas de API realizadas por meio do console da Resposta a Incidentes de Segurança da AWS. Por exemplo, quando um usuário se autentica, o CloudTrail pode registrar detalhes, como o endereço IP na solicitação, quem fez a solicitação e quando ela foi feita.

Métricas do Amazon CloudWatch: com as métricas do CloudWatch, é possível monitorar, relatar e realizar ações automáticas no caso de um evento quase em tempo real. Por exemplo, você pode criar painéis do CloudWatch com base nas métricas fornecidas para monitorar o uso da AWS Security Incident Response, ou configurar alarmes do CloudWatch nas métricas fornecidas para receber notificações caso um limite definido previamente seja ultrapassado.

O namespace para o serviço é AWS/Usage/ServiceName. Os nomes de métricas disponíveis são ActiveManagedCases e SelfManagedCases.

De acordo com os Termos de Serviço da AWS, a equipe de responsáveis pela AWS Security Incident Response terá acesso ao seu histórico de dados de logs do CloudTrail, da VPC, do DNS e do S3. Esses dados podem ser usados durante incidentes de segurança ativos, quando um caso estiver aberto no portal do serviço de Resposta a Incidentes de Segurança da AWS.

Resiliência

A infraestrutura global da AWS é criada com base em regiões e zonas de disponibilidade da AWS. As regiões fornecem várias zonas de disponibilidade separadas e isoladas fisicamente, que são conectadas com baixa latência, alta throughput e redes altamente redundantes. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre AWS Regiões e Zonas de Disponibilidade, consulte AWS global infrastructure.

Segurança da infraestrutura

A AWS Security Incident Response é protegida pela infraestrutura global de segurança da rede da AWS. Para saber mais sobre serviços de segurança da AWS e como a AWS protege a infraestrutura, consulte Segurança na Nuvem AWS. Para projetar seu ambiente da AWS usando as práticas recomendadas de segurança da infraestrutura, consulte Proteção de Infraestrutura em Pilar de Segurança: AWS Well-Architected Framework.

Você usa AWS Security Incident Response chamadas de API publicadas pela para acessarAWS o por meio da rede. Os clientes devem oferecer compatibilidade com:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou você pode usar o serviço de token de segurança da AWS (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Análise de configuração e vulnerabilidade

Você é responsável por gerenciar os perfis de contenção do serviço e os conjuntos de pilhas do CloudFormation associados.

A AWS se encarrega das tarefas básicas de segurança, como a aplicação de patches no sistema operacional (SO) de convidados e em bancos de dados, a configuração de firewalls e a recuperação de desastres. Esses procedimentos foram revisados e certificados por terceiros certificados. Para obter mais detalhes, consulte os seguintes recursos da AWS:

- Modelo de responsabilidade compartilhada
- Práticas recomendadas de segurança, identidade e conformidade

Prevenção do problema do “confused deputy” entre serviços

“Confused deputy” é um problema de segurança no qual uma entidade sem permissão para executar uma ação pode coagir uma entidade mais privilegiada a executá-la. Na AWS, a personificação entre serviços pode resultar no problema do ‘confused deputy’. A personificação entre serviços pode ocorrer quando um serviço (o serviço de chamada) chama outro serviço (o serviço chamado). O serviço de chamada pode ser manipulado de modo a usar suas permissões para atuar nos recursos de outro cliente de uma forma na qual ele não deveria ter permissão para acessar. Para evitar isso, a AWS fornece ferramentas que ajudam você a proteger seus dados para todos os serviços com entidades principais de serviço que receberam acesso aos recursos em sua conta.

Recomendamos usar as chaves de contexto global de condição AWS:SourceArn e AWS:SourceAccount nas políticas de recursos para limitar as permissões que o Amazon Connect concede a outro serviço em relação ao recurso. Caso use ambas as chaves de contexto global de condição, o valor de AWS:SourceAccount e a conta presente no valor de AWS:SourceArn devem corresponder ao mesmo ID de conta quando usadas na mesma declaração de política.

A maneira mais eficaz de se proteger contra o problema de substituto confuso é usar o nome do recurso da Amazon (ARN) exato do recurso que deseja permitir. Se você não souber o ARN completo do recurso ou se estiver especificando diversos recursos, use a chave de contexto global de condição AWS:SourceArn com caracteres curingas (*) para as partes desconhecidas do ARN. Por exemplo: arn:AWS:servicename::region-name::your AWS account ID:*.

Para obter um exemplo de política para assumir o perfil que demonstra como prevenir o problema do confused deputy, consulte Confused deputy prevention policy.

Service Quotas

AWS Security Incident Response

O Guia de referência geral da AWS inclui os Endpoints e cotas da AWS Security Incident Response mais atuais.

Guia técnico da AWS Security Incident Response

Conteúdo

Resumo

Este guia apresenta uma visão geral dos fundamentos para responder a incidentes de segurança dentro do ambiente em nuvem da Amazon Web Services (AWS) de um cliente. Ele fornece uma visão geral dos conceitos de segurança e resposta a incidentes na nuvem e identifica recursos, serviços e mecanismos de nuvem que estão disponíveis para clientes que respondem a problemas de segurança.

Este guia destina-se a profissionais em cargos técnicos e parte do pressuposto de que você tenha familiaridade com os princípios gerais de segurança da informação, conte com uma compreensão básica sobre resposta a incidentes de segurança em seus ambientes on-premises atuais e tenha alguma familiaridade com serviços em nuvem.

Você é Well-Architected?

O Well-Architected Framework da AWS ajuda você a entender os prós e os contras das decisões que você toma ao criar sistemas na nuvem. Os seis pilares do framework permitem a você conhecer as melhores práticas de arquitetura para criar e operar sistemas confiáveis, seguros, econômicos e sustentáveis na nuvem. Ao usar a AWS Well-Architected Tool, disponível gratuitamente no console

da AWS Well-Architected Tool, você pode analisar suas workloads em relação a essas práticas recomendadas ao responder a um conjunto de perguntas para cada pilar.

Para obter orientações especializadas e melhores práticas adicionais para a arquitetura de sua nuvem (implantações de arquitetura de referência, diagramas e whitepapers), consulte o Centro de arquitetura da AWS.

Introdução

A segurança é a principal prioridade na AWS. Os clientes da AWS se beneficiam de data centers e arquiteturas de rede projetados para atender às necessidades das organizações mais sensíveis em termos de segurança. A AWS adota um modelo de responsabilidade compartilhada, no qual a AWS gerencia a segurança da nuvem, enquanto os clientes são responsáveis pela segurança na nuvem. Isso significa que você tem controle total sobre a implementação da sua segurança, incluindo o acesso a diversas ferramentas e serviços que auxiliam no atendimento aos seus objetivos de segurança. Essas funcionalidades ajudam você a estabelecer uma linha de base de segurança para as aplicações que estão em execução na Nuvem AWS.

Quando ocorre uma divergência em relação à linha de base, seja por uma configuração incorreta ou por fatores externos em constante alteração, será necessário responder e investigar. Para alcançar esse objetivo com êxito, é necessário compreender os conceitos básicos de resposta a incidentes de segurança dentro do seu ambiente da AWS e os requisitos para preparar, instruir e treinar as equipes de nuvem antes que ocorram problemas de segurança. É importante saber quais controles e funcionalidades podem ser usados, analisar os exemplos atuais para resolver preocupações potenciais e identificar métodos de remediação que empreguem automação para melhorar a velocidade e a consistência da resposta. Além disso, você deve compreender os requisitos de conformidade e de regulamentação relacionados ao desenvolvimento de um programa de resposta a incidentes de segurança para cumprir essas exigências.

A resposta a incidentes de segurança pode ser complexa, portanto, recomendamos que você adote uma abordagem iterativa. Comece com os serviços principais de segurança, desenvolva as funcionalidades de base de detecção e de resposta, e, em seguida, desenvolva planos de ação para criar uma biblioteca inicial de mecanismos de resposta a incidentes que possa ser aprimorada e iterada continuamente.

Antes de começar

Antes de iniciar o aprendizado sobre a resposta a incidentes em eventos de segurança na AWS, é importante familiarizar-se com os padrões e estruturas relevantes à segurança e à resposta a

incidentes da AWS. Esses fundamentos ajudarão você a compreender os conceitos e as práticas recomendadas apresentados neste guia.

Padrões e estruturas de segurança da AWS

Para começar, recomendamos que você analise as Práticas recomendadas de segurança, identidade e conformidade, o Pilar Segurança: AWS Well-Architected Framework e o whitepaper Security Perspective of the Overview of the AWS Cloud Adoption Framework (AWS CAF).

O AWS CAF fornece orientações para apoiar a coordenação entre diferentes áreas das organizações que estão migrando para a nuvem. As orientações do AWS CAF são divididas em diversas áreas de foco, denominadas perspectivas, que são relevantes para o desenvolvimento de sistemas de TI baseados na nuvem. A perspectiva de segurança descreve como implementar um programa de segurança ao longo dos fluxos de trabalho, incluindo a resposta a incidentes. Este documento é resultado de nossas experiências trabalhando com clientes para ajudá-los a desenvolver programas e funcionalidades eficazes e eficientes de resposta a incidentes de segurança.

Padrões e estruturas do setor destinados a resposta a incidentes

Este whitepaper segue os padrões e as práticas recomendadas de resposta a incidentes do Computer Security Incident Handling Guide SP 800-61 r3, que foi criado pelo National Institute of Standards and Technology (NIST). A leitura e a compreensão dos conceitos apresentados pelo NIST são requisitos prévios úteis. Os conceitos e as práticas recomendadas apresentadas nesse guia do NIST serão aplicados às tecnologias da AWS neste documento. No entanto, cenários de incidentes em ambientes on-premises estão fora do escopo deste guia.

Visão geral da resposta a incidentes da AWS

Para começar, é importante compreender como as operações de segurança e a resposta a incidentes diferem no ambiente de nuvem. Para desenvolver funcionalidades de resposta eficazes na AWS, é necessário compreender as diferenças em relação à resposta tradicional em ambientes on-premises e o impacto dessas diferenças no seu programa de resposta a incidentes. Cada uma dessas diferenças, assim como os princípios fundamentais de concepção da resposta a incidentes da AWS, serão detalhados nesta seção.

Aspectos da resposta a incidentes da AWS

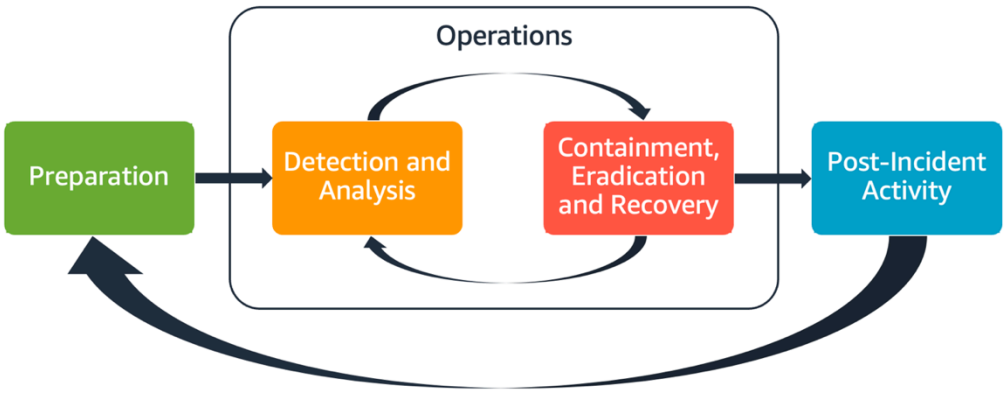
Todos os usuários da AWS de uma organização devem ter uma compreensão básica dos processos de resposta a incidentes de segurança, e a equipe de segurança deve entender como responder aos

problemas de segurança. Educação, treinamento e experiência são essenciais para um programa bem-sucedido de resposta a incidentes na nuvem e são preferencialmente implementados bem antes de precisar lidar com um possível incidente de segurança. A base de um programa bem-sucedido de resposta a incidentes na nuvem é composta por três pilares: Preparação, Operações e Atividades posteriores ao incidente.

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

- Preparação: prepare sua equipe de resposta a incidentes para detectar e responder a incidentes dentro da AWS ao habilitar os controles de detecção e verificar o acesso adequado às ferramentas e aos serviços em nuvem necessários. Além disso, prepare os playbooks necessários, tanto os automatizados quanto os manuais, para garantir respostas confiáveis e consistentes.
- Operações: atue sobre eventos de segurança e possíveis incidentes seguindo as fases de resposta a incidentes estabelecidas pelo NIST: detecção, análise, contenção, erradicação e recuperação.
- Atividades posteriores ao incidente: realize a iteração com base nos resultados de seus eventos de segurança e simulações para melhorar a eficácia da resposta, aumentar o valor obtido das ações de resposta e de investigações, e reduzir ainda mais os riscos. Você precisa aprender com os incidentes e ter uma propriedade consistente das atividades de melhoria.

Cada um desses aspectos será explorado e detalhado neste guia. O diagrama apresentado a seguir mostra o fluxo desses aspectos, alinhando-se ao ciclo de vida da resposta a incidentes estabelecido pelo NIST e comentado anteriormente, mas com a fase de operações abrangendo a detecção e a análise, bem como a contenção, a erradicação e a recuperação.



Aspectos da resposta a incidentes da AWS

Princípios e metas de concepção da resposta a incidentes da AWS

Embora os processos e os mecanismos gerais da resposta a incidentes definidos no guia NIST SP 800-61 – Computer Security Incident Handling Guide sejam consistentes e bem fundamentados, recomendamos que você também considere as seguintes metas específicas de concepção, que são particularmente relevantes para a resposta a incidentes de segurança em ambientes de nuvem:

- Estabelecer objetivos de resposta: trabalhe em conjunto com as partes interessadas, a assessoria jurídica e a liderança da organização para determinar a meta da resposta a um incidente. Algumas metas comuns incluem conter e mitigar o problema, realizar a recuperação dos recursos afetados, preservar dados para fins forenses, restabelecer operações em um estado conhecido como seguro e, por fim, extrair aprendizados dos incidentes.
- Responder usando a nuvem: implemente padrões de resposta diretamente na nuvem, que corresponde ao local em que os eventos e os dados são originados.
- Ter clareza sobre seus recursos e sobre suas necessidades: preserve logs, recursos, snapshots e outras evidências ao copiar e realizar o armazenamento deles em uma conta centralizada na nuvem dedicada à resposta. Use tags, metadados e mecanismos que impõem políticas de retenção. É necessário compreender quais serviços estão em uso e, a partir disso, identificar os requisitos necessários para investigá-los. Para ajudar na compreensão do seu ambiente, você também pode empregar a marcação, conforme descrito posteriormente neste documento, na seção the section called “Desenvolva e implemente uma estratégia de marcação”.
- Usar mecanismos de reimplantação: se uma anomalia de segurança puder ser atribuída a uma configuração incorreta, a remediação pode ser tão simples quanto eliminar a divergência por meio da reimplantação dos recursos com a configuração adequada. Caso seja identificado um possível comprometimento, verifique se a nova implantação inclui a mitigação bem-sucedida e verificada das causas-raiz.
- Automatizar sempre que possível: à medida que surgem problemas ou incidentes recorrentes, desenvolva mecanismos que realizem a triagem e a resposta programática para eventos comuns. Deixe os incidentes complexos, específicos ou sensíveis para resposta humana, visto que a automação não atinge o nível necessário de precisão.
- Escolher soluções escaláveis: busque alinhar a escalabilidade da abordagem da sua organização à computação em nuvem. Implemente mecanismos de detecção e de resposta que escalam com base em diferentes ambientes, a fim de reduzir de forma eficaz o tempo entre a detecção e a resposta.
- Aprender e aprimorar seu processo: adote uma postura proativa na identificação de lacunas em seus processos, ferramentas ou equipe, e implemente um plano para corrigi-las. As simulações

são métodos seguros para realizar a descoberta de falhas e aprimorar os processos. Consulte a seção the section called “Atividade pós-incidente” deste documento para obter mais detalhes sobre como efetuar a iteração dos seus processos.

Essas metas de design são um lembrete para analisar a implementação de sua arquitetura quanto à capacidade de conduzir tanto a resposta a incidentes quanto a detecção de ameaças. Durante o planejamento das implementações na nuvem, considere a necessidade de responder a incidentes, preferencialmente por meio de uma metodologia que preserve a integridade forense. Em alguns casos, isso pode significar a existência de diversas organizações, contas e ferramentas configuradas especificamente para executar essas tarefas de resposta. Essas ferramentas e funções devem ser disponibilizadas para a equipe de atendimento a incidentes por meio do pipeline de implantação. Elas não devem ser estáticas, pois podem causar um risco maior.

Domínios relacionados aos incidentes de segurança na nuvem

Para se preparar e responder a eventos de segurança em seu ambiente da AWS de forma eficaz, é essencial compreender os tipos mais comuns de incidentes de segurança na nuvem. Existem três domínios sob a responsabilidade do cliente nos quais incidentes de segurança podem ocorrer, nomeadamente, serviço, infraestrutura e aplicação. Cada domínio requer conhecimentos, ferramentas e processos de resposta distintos. Considere os seguintes domínios:

- Domínio de serviço: incidentes no domínio de serviço podem afetar a conta da Conta da AWS, as permissões do AWS Identity and Access Management (IAM), os metadados de recursos, o faturamento ou outras áreas. Um evento no domínio de serviço consiste em um evento que é tratado exclusivamente por meio de mecanismos da API da AWS ou cuja causa-raiz está associada à configuração ou às permissões de recursos, podendo envolver registros de log relacionados a serviços.
- Domínio de infraestrutura: incidentes no domínio de infraestrutura incluem atividades relacionadas aos dados ou à rede, como processos e dados em instâncias do Amazon Elastic Compute Cloud (Amazon EC2), tráfego direcionado a essas instâncias do Amazon EC2 dentro de uma nuvem privada virtual (VPC), além de outras áreas, como contêineres ou outros serviços futuros. A resposta aos eventos no domínio de infraestrutura geralmente envolve a aquisição de dados relacionados ao incidente para análise forense. Além disso, a resposta frequentemente requer interação com o sistema operacional da instância e, em diversos casos, pode envolver também mecanismos da API da AWS. No domínio de infraestrutura, é possível combinar o uso de APIs da AWS com ferramentas de resposta a incidentes e forense digital (DFIR, na sigla em inglês) executadas dentro de um sistema operacional convidado, como uma instância do Amazon EC2

dedicada à realização de análises e de investigações forenses. Os incidentes no domínio de infraestrutura podem envolver a análise de capturas de pacotes de rede, blocos de disco em volumes do Amazon Elastic Block Store (Amazon EBS) ou memória volátil adquirida de uma instância.

- Domínio de aplicação: incidentes no domínio de aplicação ocorrem no código da aplicação ou em softwares implantados para os serviços ou para a infraestrutura. Esse domínio deve ser incluído em seus planos de ação de detecção e de resposta a ameaças na nuvem e pode incorporar respostas semelhantes às apresentadas no domínio de infraestrutura. Com uma arquitetura de aplicação bem planejada e adequada, é possível gerenciar esse domínio ao usar ferramentas em nuvem por meio da aquisição, da recuperação e da implantação automatizadas.

Nesses domínios, considere os agentes que podem representar ameaças às contas, aos recursos ou aos dados na AWS. Sejam internos ou externos, use uma estrutura de gerenciamento de riscos para determinar os riscos específicos à organização e se preparar adequadamente. Além disso, você deve realizar o desenvolvimento de modelos de ameaças, que podem auxiliar no planejamento da resposta a incidentes e na criação de arquiteturas com melhor planejamento.

Principais diferenças na resposta a incidentes na AWS

A resposta a incidentes constitui uma parte essencial da estratégia de segurança da cibernética, aplicável tanto em ambientes on-premises quanto na nuvem. Os princípios de segurança, como o privilégio mínimo e a defesa em profundidade, têm o objetivo de proteger a confidencialidade, a integridade e a disponibilidade dos dados tanto em ambientes on-premises quanto na nuvem. Diversos padrões de resposta a incidentes que apoiam esses princípios de segurança seguem esse exemplo, incluindo a retenção de log, a seleção de alertas baseada em modelagem de ameaças, o desenvolvimento de planos de ação e a integração com o gerenciamento de informações e de eventos de segurança (SIEM, na sigla em inglês). As diferenças surgem quando os clientes começam a projetar e a desenvolver esses padrões na nuvem. A seguir, apresentamos as principais diferenças da resposta a incidentes na AWS.

Diferença n.º 1: segurança como uma responsabilidade compartilhada

A responsabilidade pela segurança e pela conformidade é compartilhada entre a AWS e seus clientes. Esse modelo de responsabilidade compartilhada reduz parte da carga operacional do cliente, pois a AWS opera, gerencia e controla os componentes desde o sistema operacional do host e a camada de virtualização até a segurança física das instalações nas quais o serviço é prestado. Para obter mais detalhes sobre o modelo de responsabilidade compartilhada, consulte a documentação do Modelo de responsabilidade compartilhada.

À medida que a sua responsabilidade compartilhada na nuvem evolui, as opções para a resposta a incidentes também se transformam. O planejamento e a compreensão dessas compensações, combinados com suas necessidades de governança, são etapas fundamentais na resposta a incidentes.

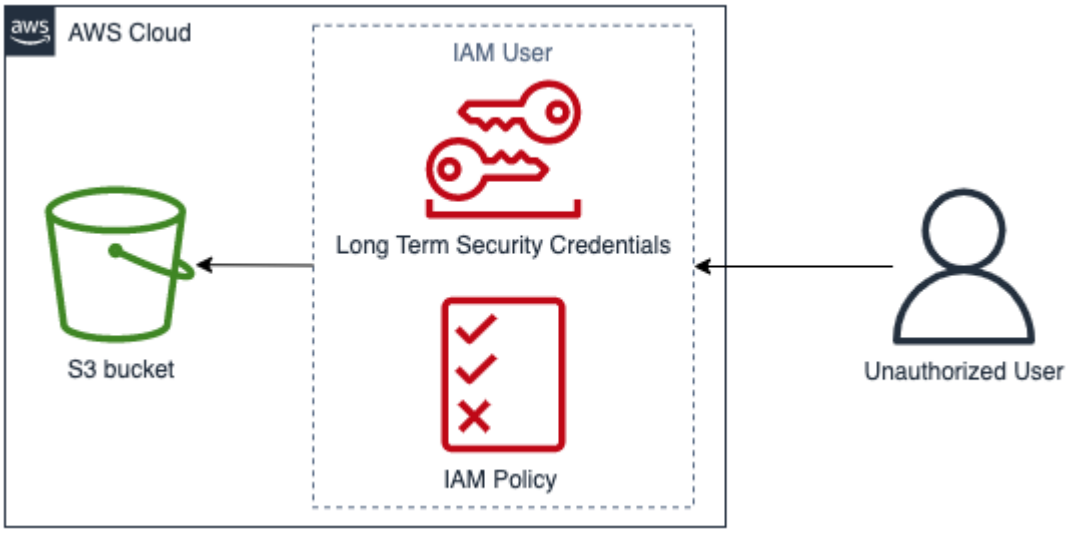
Além da relação direta que você mantém com a AWS, pode haver outras entidades que tenham responsabilidades em seu modelo de responsabilidade específico. Por exemplo, você pode contar com unidades organizacionais internas que assumem a responsabilidade por determinados aspectos de suas operações. Além disso, é possível que você mantenha relações com outras partes que desenvolvem, gerenciam ou operam parte da sua tecnologia em nuvem.

A criação e a realização de testes de um plano de resposta a incidentes adequado, assim como planos de ação apropriados que estejam alinhados ao seu modelo operacional, é de extrema importância.

Diferença n.º 2: domínio de serviço em nuvem

Devido às diferenças presentes nas responsabilidades de segurança existentes nos serviços em nuvem, foi introduzido um novo domínio para incidentes de segurança, denominado o domínio de serviço, conforme explicado anteriormente na seção Domínios relacionados aos incidentes. O domínio de serviço abrange a conta da AWS do cliente, as permissões do IAM, os metadados de recursos, o faturamento e outras áreas. Esse domínio é distinto no contexto da resposta a incidentes devido à forma como a resposta é conduzida. Geralmente, a resposta no domínio de serviço é realizada por meio da análise e da emissão de chamadas de API, em vez de abordagens de respostas tradicionais baseadas em host e em rede. No domínio de serviço, não há interação direta com o sistema operacional de um recurso afetado.

O diagrama apresentado a seguir mostra um exemplo de um evento de segurança no domínio de serviço baseado em um antipadrão de arquitetura. Nesse evento, um usuário não autorizado obtém as credenciais de segurança de longo prazo de um usuário do IAM. O usuário do IAM tem uma política do IAM que permite a recuperação de objetos de um bucket do Amazon Simple Storage Service (Amazon S3). Para responder a esse evento de segurança, você utilizaria as APIs da AWS para analisar os logs da AWS, como o AWS CloudTrail e os logs de acesso do Amazon S3. Além disso, você usaria as APIs da AWS para realizar a contenção e a recuperação do ambiente afetado pelo incidente.



Exemplo de domínio de serviço

Diferença n.º 3: APIs para provisionamento de infraestrutura

Uma outra diferença decorre da natureza sob demanda e de autoatendimento da computação em nuvem. O principal meio de interação dos clientes com a Nuvem AWS é por meio de uma API RESTful, acessível por endpoints públicos e privados disponíveis em diversas regiões geográficas ao redor do mundo. Os clientes podem acessar essas APIs com as credenciais da AWS. Em contraste com o controle de acesso em ambientes on-premises, essas credenciais não estão necessariamente vinculadas a uma rede ou a um domínio do Microsoft Active Directory. Em vez disso, as credenciais estão associadas a uma entidade principal do IAM dentro de uma conta da AWS. Esses endpoints de API podem ser acessados de forma externa a sua rede corporativa, o que é um fator importante a ser compreendido ao responder a um incidente em que as credenciais são utilizadas fora da rede ou da região geográfica esperada.

Devido à natureza baseada em APIs da AWS, uma fonte de log importante para a resposta a eventos de segurança é o AWS CloudTrail, que acompanha as chamadas à API de gerenciamento realizadas em suas contas da AWS e fornece informações sobre a localização de origem dessas chamadas de API.

Diferença n.º 4: natureza dinâmica da nuvem

A nuvem é dinâmica, portanto, ela permite a criação e a exclusão de recursos rapidamente. Com a escalabilidade automática, os recursos podem ser provisionados ou encerrados conforme a demanda de tráfego. Devido à natureza transitória da infraestrutura e à rapidez das alterações, o recurso que está sendo investigado pode já não existir mais ou ter sido modificado. Compreender a

natureza efêmera dos recursos da AWS, bem como saber como acompanhar a criação e a exclusão dos recursos da AWS, será importante para a análise de incidentes. Você pode usar o AWS Config para acompanhar o histórico de configurações dos seus recursos da AWS.

Diferença n.º 5: acesso aos dados

O acesso aos dados também é diferente na nuvem. Não é possível conectar-se diretamente a um servidor para coletar os dados necessários para uma investigação de segurança. Os dados são coletados por meio de tráfego de rede e de chamadas de API. É fundamental praticar e compreender como realizar a coleta de dados por meio de APIs para estar com tudo preparado para essa mudança, além de garantir o armazenamento adequado para uma coleta e para um acesso eficazes.

Diferença n.º 6: importância da automação

Para que os clientes possam aproveitar plenamente os benefícios da adoção da nuvem, sua estratégia operacional deve incorporar a automação. A infraestrutura como código (IaC) consiste em um padrão de ambientes altamente eficientes e automatizados, nos quais os serviços da AWS são implantados, configurados, reconfigurados e destruídos por meio de código, utilizando serviços nativos de IaC, como o AWS CloudFormation, ou soluções de entidades externas. Isso torna a implementação da resposta a incidentes altamente automatizada, o que é desejável para evitar erros humanos, especialmente ao lidar com evidências. Embora a automação seja usada em ambientes on-premises, ela é essencial e mais simples na Nuvem AWS.

Como abordar essas diferenças

Para abordar essas diferenças, siga as etapas descritas na próxima seção para garantir que seu programa de resposta a incidentes, contemplando pessoas, processos e tecnologias, esteja adequadamente preparado.

Preparação

A preparação para um incidente é fundamental para uma resposta oportuna e eficaz a incidentes. A preparação é feita em três domínios:

- Pessoas: a preparação das pessoas para um incidente de segurança envolve a identificação das partes interessadas responsáveis pela resposta a incidentes, bem como o treinamento desses profissionais em resposta a incidentes e em tecnologias de nuvem.
- Processos: a preparação dos processos para um incidente de segurança envolve a documentação das arquiteturas, o desenvolvimento de planos detalhados de resposta a incidentes e a criação de planos de ação que assegurem uma resposta consistente diante de eventos de segurança.

- Tecnologia: a preparação da tecnologia para um incidente de segurança envolve a configuração de acessos, a agregação e o monitoramento dos logs essenciais, a implementação de alertas eficientes e o desenvolvimento de funcionalidades para resposta e investigação.

Cada um desses domínios é igualmente importante para uma resposta eficaz a incidentes. Nenhum programa de resposta a incidentes é completo ou eficaz sem os três. Você precisará preparar pessoas, processos e tecnologias com uma forte integração para se preparar para um incidente.

Pessoas

Para responder a um evento de segurança, é necessário identificar as partes interessadas que fornecerão suporte à resposta para o evento de segurança. Além disso, é fundamental, para uma resposta eficaz, que essas pessoas estejam treinadas em tecnologias da AWS e no seu ambiente da AWS.

Definir funções e responsabilidades

Lidar com eventos de segurança exige disciplina interorganizacional e uma inclinação para a ação. Em sua estrutura organizacional, deve haver muitas pessoas responsáveis, atribuídas, consultadas ou mantidas informadas durante um incidente, como representantes de recursos humanos (RH), da equipe executiva e do setor jurídico. Considere essas funções e responsabilidades e se algum terceiro deve estar envolvido. Vale destacar que, em diversas regiões geográficas, existem legislações locais que regulam as ações permitidas e proibidas. Embora a elaboração de um quadro que compreende o responsável, a autoridade, o consultado e o informado (RACI) para os planos de resposta a incidentes de segurança possa parecer burocrática, essa prática é essencial para viabilizar uma comunicação direta e ágil, além de definir claramente a pessoa responsável por liderar cada etapa do processo durante o evento.

Durante um incidente, incluir os responsáveis e os desenvolvedores das aplicações e dos recursos impactados é fundamental, pois eles são especialistas no assunto (SMEs, na sigla em inglês) e podem fornecer informações e contexto que auxiliam na avaliação do impacto. Pratique e construa relacionamentos com os desenvolvedores e os proprietários de aplicações antes de confiar na experiência deles para responder a incidentes. Proprietários de aplicações ou PMEs, como administradores ou engenheiros de nuvem, podem precisar agir em situações em que o ambiente não seja familiar ou tenha complexidade, ou em que os respondentes não tenham acesso.

Por fim, as relações de confiança podem ser envolvidas na investigação ou na resposta, pois podem oferecer conhecimento especializado adicional e uma análise criteriosa de valor. Se você não tiver essas habilidades em sua própria equipe, contrate uma parte externa para obter assistência.

Treinamento da equipe de resposta a incidentes

O treinamento da sua equipe de resposta a incidentes nas tecnologias usadas pela organização será crucial para que ela possa responder adequadamente a um evento de segurança. As respostas podem ser prolongadas caso os membros da equipe não compreendam as tecnologias subjacentes. Além dos conceitos tradicionais de resposta a incidentes, é importante que a equipe também tenha conhecimento dos serviços da AWS e do ambiente da AWS. Existem diversos mecanismos tradicionais para treinar sua equipe de resposta a incidentes, como treinamentos on-line e presenciais. Você também deve considerar a realização de dias de desafios ou simulações como um mecanismo de treinamento. Para obter mais detalhes sobre como conduzir simulações, consulte a seção the section called “Execução de simulações de forma periódica” deste documento.

Compreensão das tecnologias da Nuvem AWS

Para reduzir dependências e diminuir o tempo de resposta, assegure-se de que suas equipes de segurança e de que seus responsáveis pela resposta a incidentes estejam instruídos sobre os serviços em nuvem e disponham de oportunidades para prática direta com o ambiente de nuvem específico usado pela sua organização. Para que os responsáveis pela resposta a incidentes sejam eficazes, é importante compreender os fundamentos da AWS, o IAM, o AWS Organizations, os serviços de registro em log e monitoramento da AWS, e os serviços de segurança da AWS.

A AWS proporciona workshops de segurança on-line (consulte AWS Security Workshops), nos quais é possível adquirir experiência prática com os serviços de segurança e de monitoramento da AWS. Além disso, a AWS disponibiliza diversas opções de treinamento e trilhas de aprendizado por meio de treinamentos digitais, presenciais, parceiros de treinamento da AWS e certificações. Para saber mais informações, consulte Treinamento e certificação da AWS.

A AWS disponibiliza tanto treinamentos gratuitos quanto baseados em assinatura, atendendo a diversos perfis e focos de atuação. Acesse o AWS Skill Builder para saber mais.

Compreensão do ambiente da AWS

Além de compreender os serviços da AWS, os casos de uso e como esses casos se integram entre si, é igualmente importante entender como o ambiente da AWS da sua organização está realmente arquitetado e quais processos operacionais estão em vigor. Frequentemente, esse tipo de conhecimento técnico interno não está documentado e é compreendido somente por alguns especialistas no assunto, o que pode gerar dependências, dificultar a inovação e aumentar o tempo de resposta.

Para evitar essas dependências e agilizar os tempos de resposta, o conhecimento técnico interno sobre o ambiente da AWS deve ser devidamente documentado, estar acessível e ser compreendido pelos analistas de segurança. A compreensão completa da presença na nuvem da organização exigirá colaboração entre as partes interessadas de segurança relevantes e os administradores da nuvem. Como parte da preparação dos seus processos para a resposta a incidentes, é necessário documentar e centralizar os diagramas de arquitetura, conforme descrito na seção the section called "Documentação e centralização dos diagramas de arquitetura" que será apresentada posteriormente neste whitepaper. No entanto, sob a ótica da área de recursos humanos, é igualmente importante que os analistas possam acessar e compreender os diagramas e os processos operacionais relacionados com o ambiente da AWS.

Compreensão das equipes de resposta da AWS e do suporte fornecido

Suporte

Suporte O AWS oferece uma variedade de planos que permitem conceder acesso a ferramentas e conhecimentos que oferecem suporte ao sucesso e à integridade operacional das soluções da . Se precisar de suporte técnico e mais recursos para ajudar a planejar, implantar e otimizar seu ambiente da AWS, selecione um plano de suporte mais adequado ao seu caso de uso da AWS.

Considere o Support Center no Console de gerenciamento da AWS (é necessário fazer login) como o ponto de contato principal para obter suporte em questões que afetam seus recursos da AWS. O acesso ao Suporte é controlado por meio do IAM. Para obter mais informações sobre como obter acesso aos recursos do AWS Support, consulte Getting started with Suporte.

Além disso, se for necessário relatar um caso de abuso, entre em contato com a equipe de Confiança e Segurança da AWS.

Engenheiros do Security Incident Response

Os engenheiros do Security Incident Response são uma equipe global especializada da AWS, que presta suporte aos clientes durante os eventos de segurança ativos que ocorrem do lado do cliente do Modelo de responsabilidade compartilhada da AWS.

Quando os engenheiros do Security Incident Response prestarem suporte a você, eles ajudarão na triagem e recuperação de um evento de segurança ativo na AWS. A equipe auxiliará na análise da causa-raiz por meio do uso de logs dos serviços da AWS e fornecerá recomendações para a recuperação. Além disso, serão apresentadas recomendações de segurança e práticas recomendadas com o objetivo de evitar a recorrência dos eventos de segurança.

Os clientes da AWS podem entrar em contato com os engenheiros do Security Incident Response abrindo um caso de suporte da AWS.

- Aplicável para todos os clientes:
  1. Conta e faturamento
  2. Serviço: conta
  3. Categoria: segurança
  4. Severidade: dúvidas gerais

- Aplicável para clientes com planos do Developer Suporte:
  1. Conta e faturamento
  2. Serviço: conta
  3. Categoria: segurança
  4. Severidade: dúvidas importantes

- Aplicável para clientes com planos do Business Suporte:
  1. Conta e faturamento
  2. Serviço: conta
  3. Categoria: segurança
  4. Severidade: dúvidas urgentes com impacto nos negócios

- Aplicável para clientes com planos do Enterprise Suporte:
  1. Conta e faturamento
  2. Serviço: conta
  3. Categoria: segurança
  4. Severidade: dúvidas com riscos críticos para os negócios

- Clientes com assinaturas da AWS Security Incident Response: abra o console de Resposta a Incidentes de Segurança ao acessar https://console.aws.amazon.com/security-ir/

Suporte de resposta a DDoS

A AWS oferece o AWS Shield, um serviço gerenciado de proteção contra ataques de negação de serviço distribuída (DDoS) que protege aplicações web executadas na AWS. O AWS Shield fornece detecção contínua e mitigação automática em linha que são capazes de minimizar o tempo de inatividade e a latência das aplicações, eliminando a necessidade de entrar em contato com o Suporte para se beneficiar da proteção contra ataques de DDoS. Existem dois níveis do AWS Shield, o Shield Básico e o Shield Avançado. Para saber mais informações sobre as diferenças entre esses dois níveis, consulte a documentação de recursos do Shield.

AWS Managed Services (AMS)

O AWS Managed Services (AMS) fornece gerenciamento contínuo da sua infraestrutura da AWS, permitindo que você se concentre nas suas aplicações. Ao implementar práticas recomendadas para manter sua infraestrutura, o AMS ajuda a reduzir a sobrecarga e os riscos operacionais. O AMS automatiza atividades comuns, como solicitações de alteração, monitoramento, gerenciamento de patches, segurança e serviços de backup, além de disponibilizar serviços de ciclo de vida total para provisionar, executar e apoiar a sua infraestrutura.

O AMS assume a responsabilidade pela implantação de um conjunto de controles de segurança detectivos e atua diariamente como a primeira linha de resposta a alertas. Quando um alerta é iniciado, o AMS segue um conjunto padrão de guias e playbooks automatizados para verificar uma resposta consistente. Esses playbooks são compartilhados com os clientes do AMS durante a integração para que eles possam desenvolver e coordenar uma resposta com o AMS.

Processar

O desenvolvimento de processos de resposta a incidentes bem estruturados e devidamente definidos é essencial para garantir o êxito e a escalabilidade de um programa de resposta a incidentes. No caso da ocorrência de um evento de segurança, a existência de etapas e fluxos de trabalho claros permitirá uma resposta em tempo hábil. É possível que você já tenha processos existentes de resposta a incidentes. Independentemente do seu estado atual, é importante atualizar, repetir e testar seus processos de resposta a incidentes regularmente.

Desenvolvimento e teste de um plano de resposta a incidentes

O primeiro documento a ser desenvolvido para a resposta a incidentes é o plano de resposta a incidentes. O plano de resposta a incidentes foi projetado para ser a base de seu programa e estratégia de resposta a incidentes. Um plano de resposta a incidentes consiste em um documento de alto nível que, normalmente, inclui as seguintes seções:

- Visão geral da equipe de resposta a incidentes: apresenta as metas e as funções da equipe de resposta a incidentes.
- Perfis e responsabilidades: lista as partes interessadas na resposta a incidentes e detalha os perfis em caso de ocorrência de um incidente.
- Plano de comunicação: detalha as informações de contato e a maneira como será realizada a comunicação durante um incidente.

  É uma prática recomendada dispor de um canal de comunicação externo à banda principal como um backup para comunicação em incidentes. Um exemplo de uma aplicação que fornece um canal de comunicação seguro e externo à banda é o AWS Wickr.
- Fases da resposta a incidentes e ações a serem executadas: enumera as fases da resposta a incidentes, por exemplo, detecção, análise, erradicação, contenção e recuperação, incluindo as ações de alto nível a serem executadas em cada fase.
- Definições relativas à severidade e priorização de incidentes: explicita os critérios para a classificação da severidade de um incidente, a maneira de realizar a priorização dos incidentes e, em seguida, a influência dessas definições de severidade nos procedimentos de encaminhamento.

Embora essas seções sejam comuns em empresas de diferentes tamanhos e setores, o plano de resposta a incidentes de cada organização é único. Será necessário elaborar um plano de resposta a incidentes que seja mais adequado para a sua organização.

Documentação e centralização dos diagramas de arquitetura

Para responder de forma rápida e precisa a um evento de segurança, é necessário compreender como seus sistemas e suas redes estão arquitetados. A compreensão desses padrões internos é essencial não apenas para a resposta a incidentes, mas também para verificar a consistência das aplicações que foram desenvolvidas seguindo esses padrões, de acordo com as práticas recomendadas. Você também deve verificar se essa documentação está atualizada e é regularmente atualizada de acordo com os novos padrões de arquitetura. Recomenda-se desenvolver documentação e repositórios internos que detalhem itens como:

- Estrutura da conta da AWS: informações necessárias:
  - Qual é a quantidade de contas da AWS que você tem?
  - De que maneira essas contas da AWS estão organizadas?
  - Quem são os responsáveis comerciais por cada conta da AWS?

  - Você faz o uso de políticas de controle de serviços (SCPs)? Em caso afirmativo, quais barreiras de proteção organizacionais são implementadas ao usar as SCPs?
  - Você limita as regiões e os serviços que podem ser usados?
  - Quais são as diferenças entre as unidades de negócios e os ambientes (dev/teste/produção)?
- Padrões de serviços da AWS
  - Quais serviços da AWS são usados por você?
  - Quais são os serviços da AWS que apresentam maior adoção?
- Padrões de arquitetura
  - Quais arquiteturas de nuvem são usadas por você?
- Padrões de autenticação da AWS
  - De que maneira seus desenvolvedores geralmente realizam a autenticação na AWS?
  - Você usa usuários ou perfis do IAM, ou uma combinação de ambos? Sua autenticação na AWS está conectada a um provedor de identidades (IdP)?
  - De que maneira é realizado o mapeamento de um usuário por perfil do IAM para um colaborador ou para um sistema?
  - De que maneira ocorre a revogação de acesso quando um indivíduo perde a autorização?
- Padrões de autorização da AWS
  - Quais políticas do IAM são usadas por seus desenvolvedores?
  - Você faz o uso de políticas baseadas em recursos?
- Registro em log e monitoramento
  - Quais fontes de registros em log são usadas e em quais locais essas fontes são armazenadas?
  - Você realiza a agregação de logs do AWS CloudTrail? Em caso afirmativo, em quais locais esses logs são armazenados?
  - De que maneira você realiza a consulta em logs do CloudTrail?
  - O Amazon GuardDuty está habilitado?
  - De que maneira é possível acessar as descobertas do GuardDuty (por exemplo, o console, o sistema de emissão de tíquetes e o SIEM)?
  - As descobertas ou os eventos são agregados em um SIEM?
  - Os tíquetes são criados automaticamente?
  - Quais ferramentas estão em vigor para realizar a análise de logs para uma investigação?
- Topologia de rede

  - De que maneira os dispositivos, os endpoints e as conexões presentes em sua rede estão organizados física ou logicamente?
  - De que maneira sua rede se conecta com a AWS?
  - De que maneira é realizado a filtragem do tráfego de rede entre os diferentes ambientes?
- Infraestrutura externa
  - De que maneira as aplicações voltadas para o público externo são implantadas?
  - Quais recursos da AWS estão disponíveis publicamente?
  - Quais contas da AWS hospedam infraestrutura voltada para o público externo?
  - Que mecanismos de proteção contra ataques de DDoS ou filtragem externa estão implementados?

A documentação de diagramas técnicos e processos internos facilita o trabalho do analista responsável pela resposta a incidentes, permitindo o acesso rápido ao conhecimento técnico institucional necessário para responder a um evento de segurança. A documentação completa dos processos técnicos internos não apenas simplifica as investigações de segurança, como também contribui para a racionalização e para a avaliação desses processos.

Desenvolvimento de planos de ação de resposta a incidentes

Uma parte fundamental da preparação de seus processos de resposta a incidentes é desenvolver playbooks. Os playbooks de resposta a incidentes fornecem uma série de recomendações e etapas a serem seguidas quando um evento de segurança ocorre. Ter uma estrutura e etapas claras simplifica a resposta e reduz a probabilidade de erro humano.

Identificação de situações que requerem a criação de planos de ação

Os playbooks devem ser criados para cenários de incidentes, como:

- Incidentes esperados: é recomendável criar planos de ação para os tipos de incidentes que podem ser antecipados. Isso inclui ameaças como negação de serviço (DoS), ransomware e comprometimento de credenciais.
- Descobertas ou alertas de segurança conhecidos: é recomendável elaborar planos de ação específicos para descobertas e alertas de segurança conhecidos, como as descobertas geradas pelo GuardDuty. Você pode receber uma descoberta do GuardDuty e pensar: “E agora?” Para evitar o tratamento inadequado de uma descoberta do GuardDuty ou a negligência diante dessa descoberta, crie um plano de ação correspondente para cada tipo de descoberta possível do GuardDuty. Alguns detalhes e orientações sobre a correção podem ser encontrados na

documentação do GuardDuty. É importante notar que o GuardDuty não está habilitado por padrão e seu uso gera custos. Mais detalhes sobre o GuardDuty podem ser encontrados no Apêndice A: definições das funcionalidades da nuvem: the section called “Visibilidade e geração de alertas”.

O que deve ser incluso nos planos de ação

Os playbooks devem conter etapas técnicas a serem concluídas por um analista de segurança para investigar e responder adequadamente a um possível incidente de segurança.

Os itens a serem incluídos em um playbook incluem:

- Visão geral do plano de ação: quais cenários de riscos ou de incidentes este plano de ação aborda? Qual é o objetivo do playbook?
- Requisitos prévios: quais logs e mecanismos de detecção são necessários para este cenário de incidente? Qual é a notificação esperada?
- Informações das partes interessadas: quem são as pessoas envolvidas e quais são suas informações de contato? Quais são as responsabilidades de cada parte interessada?
- Etapas de resposta: ao longo das fases da resposta a incidentes, quais etapas táticas devem ser adotadas? Que consultas um analista deve executar? Que código deve ser executado para alcançar o resultado desejado?
  - Detecção: qual será o método de detecção do incidente?
  - Análise: qual será o método de determinação do escopo do impacto?
  - Contenção: qual será o método de isolamento do incidente para limitar o escopo?
  - Erradicação: qual será o método de remoção da ameaça do ambiente?
  - Recuperação: qual será o método de reintegração do sistema ou do serviço afetado para o ambiente de produção?
- Resultados esperados: quais são os resultados esperados após a execução das consultas e do código definido neste plano de ação?

Com a finalidade de verificar a consistência das informações em cada plano de ação, pode ser útil criar um modelo de plano de ação a ser usado nos demais planos de ação de segurança. Alguns dos itens mencionados anteriormente, por exemplo, as informações das partes interessadas, podem ser comuns a vários planos de ação. Se esse for o caso, é possível criar uma documentação centralizada para essas informações e apenas referenciá-la no plano de ação, enumerando as diferenças específicas diretamente no próprio plano de ação. Dessa forma, você evita a necessidade de atualizar repetidamente as mesmas informações em cada plano de ação de forma individual. Ao

criar um modelo e ao identificar informações comuns ou compartilhadas entre os planos de ação, é possível simplificar e agilizar o desenvolvimento dos planos de ação. Por fim, considerando que os planos de ação tendem a evoluir ao longo do tempo, a padronização das etapas permite definir os requisitos necessários para sua automação.

Planos de ação de amostra

Diversos planos de ação de amostra podem ser encontrados no Apêndice B, na seção the section called “Recursos relacionados ao plano de ação”. Os exemplos apresentados podem servir como referência para a criação dos seus próprios planos de ação e para a definição dos elementos que devem ser incluídos nesses planos de ação. No entanto, é fundamental que você elabore planos de ação que incorporem os riscos mais relevantes ao seu negócio. É necessário verificar se as etapas e os fluxos de trabalho definidos nos seus planos de ação estão alinhados às tecnologias e aos processos usados em sua organização.

Execução de simulações de forma periódica

Com o tempo, as organizações se desenvolvem e transformam, assim como o panorama de ameaças. Por isso, é importante analisar continuamente suas funcionalidades de resposta a incidentes. As simulações são um dos métodos que podem ser usados para realizar essa avaliação. As simulações usam cenários de eventos de segurança do mundo real projetados para imitar as táticas, as técnicas e os procedimentos (TTPs) de um agente de ameaças e permitir que uma organização exercite e avalie seus recursos de resposta a incidentes respondendo a esses eventos cibernéticos simulados da mesma forma que em uma situação real.

As simulações fornecem uma variedade de benefícios, incluindo:

- Validar a prontidão cibernética e desenvolver a confiança de seus socorristas.
- Testar a precisão e a eficiência de ferramentas e fluxos de trabalho.
- Refinar os métodos de comunicação e escalação alinhados ao seu plano de resposta a incidentes.
- Proporcionar uma oportunidade de responder a vetores menos comuns.

Tipos de simulações

Existem três tipos principais de simulações:

- Exercícios de simulação: abordagem de exercícios de simulação consiste estritamente em uma sessão baseada em debates, envolvendo as diversas partes interessadas responsáveis pela resposta a incidentes para praticar as atividades atribuídas ao cargo e as responsabilidades, além

de usar as ferramentas de comunicação e os planos de ação estabelecidos. Normalmente, a facilitação do exercício pode ser realizada em um dia inteiro, seja em um ambiente virtual, em um ambiente físico ou em uma combinação de ambos. Devido à sua natureza baseada em debates, o exercício de simulação se concentra em processos, pessoas e colaboração. A tecnologia constitui uma parte essencial da discussão. No entanto, o uso real de ferramentas ou de scripts de resposta a incidentes geralmente não faz parte do exercício de simulação.

- Exercícios de Purple Team: os exercícios de Purple Team aumentam o nível de colaboração entre os responsáveis pela resposta a incidentes (Blue Team) e os agentes de ameaças simulados (Red Team). Geralmente, o Blue Team é composto por membros do Security Operations Center (SOC), mas também pode incluir outras partes interessadas que estariam envolvidas durante um evento cibernético real. O Red Team, por sua vez, é geralmente formado por uma equipe de testes de penetração ou por partes interessadas principais que foram treinadas em segurança ofensiva. O Red Team trabalha de forma colaborativa com os facilitadores do exercício durante a elaboração do cenário, garantindo que este seja preciso e viável. Durante os exercícios de Purple Team, o foco principal está nos mecanismos de detecção, nas ferramentas e nos procedimentos operacionais padrão (SOPs, na sigla em inglês) que fornecem suporte às iniciativas de resposta a incidentes.
- Exercícios de Red Team: durante um exercício de Red Team, a equipe ofensiva (Red Team) conduz uma simulação para atingir um objetivo ou conjunto de objetivos determinado dentro de um escopo determinado previamente. A equipe defensora (Blue Team) nem sempre conhecem o escopo e a duração do exercício, o que proporciona uma avaliação mais realista de como as pessoas reagiriam a um incidente real. Como os exercícios de Red Team podem ser testes invasivos, é recomendável agir com cautela e implementar controles para garantir que o exercício não cause danos reais ao seu ambiente.

> **Note**
>
> A AWS requer que os clientes analisem a política de testes de penetração disponível no site de teste de penetração antes de realizarem exercícios de Purple Team ou de Red Team.

A Tabela 1 apresenta um resumo das principais diferenças entre esses tipos de simulações. É importante destacar que as definições são geralmente consideradas flexíveis e podem ser personalizadas para atender às necessidades da sua organização.

Tabela 1: tipos de simulações

	Exercício de simulação	Exercício de Purple Team	Exercício de Red Team
Resumo	Exercícios baseados em documentos que se concentram em um cenário específico de incidente de segurança. Os exercícios podem ser de nível estratégico ou técnico, e são conduzidos por uma série de informações documentadas.	Uma abordagem mais realista em comparação aos exercícios de simulação. Durante os exercícios de Purple Team, os facilitadores trabalham de forma colaborativa com os participantes para aumentar o engajamento no exercício e oferecer treinamento quando necessário.	Trata-se, em geral, de uma simulação mais complexa. Normalmente há um alto nível de sigilo, de modo que os participantes podem não conhecer todos os detalhes do exercício.
Recursos necessários	Recursos técnicos limitados necessários	Diversas partes interessadas necessárias e alto nível de recursos técnicos necessários	Diversas partes interessadas necessárias e alto nível de recursos técnicos necessários
Complexidade	Baixo	Médio	Alto

Considere facilitar as simulações cibernéticas em intervalos regulares. Cada tipo de exercício pode fornecer benefícios únicos aos participantes e à organização como um todo, por isso pode ser interessante começar com simulações menos complexas (como os exercícios de simulação) e evoluir gradualmente para simulações mais complexas (como os exercícios de Red Team). Você deve selecionar um tipo de simulação com base em sua maturidade de segurança, recursos e resultados desejados. Alguns clientes podem optar por não realizar exercícios de Red Team devido à sua complexidade e ao custo envolvido.

Ciclo de vida do exercício

Independentemente do tipo de simulação que você escolher, as simulações geralmente seguem estas etapas:

1. Definição dos elementos principais do exercício: defina o cenário da simulação e os objetivos da simulação. Ambos devem ter aceitação da equipe de liderança.
2. Identificação das partes interessadas principais: no mínimo, um exercício requer facilitadores e participantes. Dependendo do cenário, outras partes interessadas, como departamento jurídico, de comunicação ou liderança executiva, podem estar envolvidos.
3. Desenvolvimento e teste do cenário: o cenário pode precisar ser redefinido durante sua elaboração, caso determinados elementos não sejam viáveis. Espera-se um cenário finalizado como resultado dessa etapa.
4. Facilitação da simulação: o tipo de simulação determina o método de facilitação adotado (por exemplo, um cenário baseado em documentos comparado a um cenário altamente técnico e simulado). Os facilitadores devem alinhar suas táticas de facilitação aos objetos da simulação e envolver todos os participantes sempre que possível para proporcionar o máximo benefício.
5. Elaboração do relatório posterior à ação (AAR, na sigla em inglês): identifique os pontos que funcionaram bem, aqueles que podem ser aprimorados e possíveis lacunas. O AAR deve medir a eficácia da simulação, bem como a resposta da equipe ao evento simulado, para que o progresso possa ser monitorado ao longo do tempo com simulações futuras.

Tecnologia

Se você desenvolver e implementar as tecnologias apropriadas antes da ocorrência de um incidente de segurança, sua equipe de resposta a incidentes poderá conduzir investigações, compreender o escopo e tomar as devidas medidas em tempo hábil.

Desenvolvimento da estrutura de contas da AWS

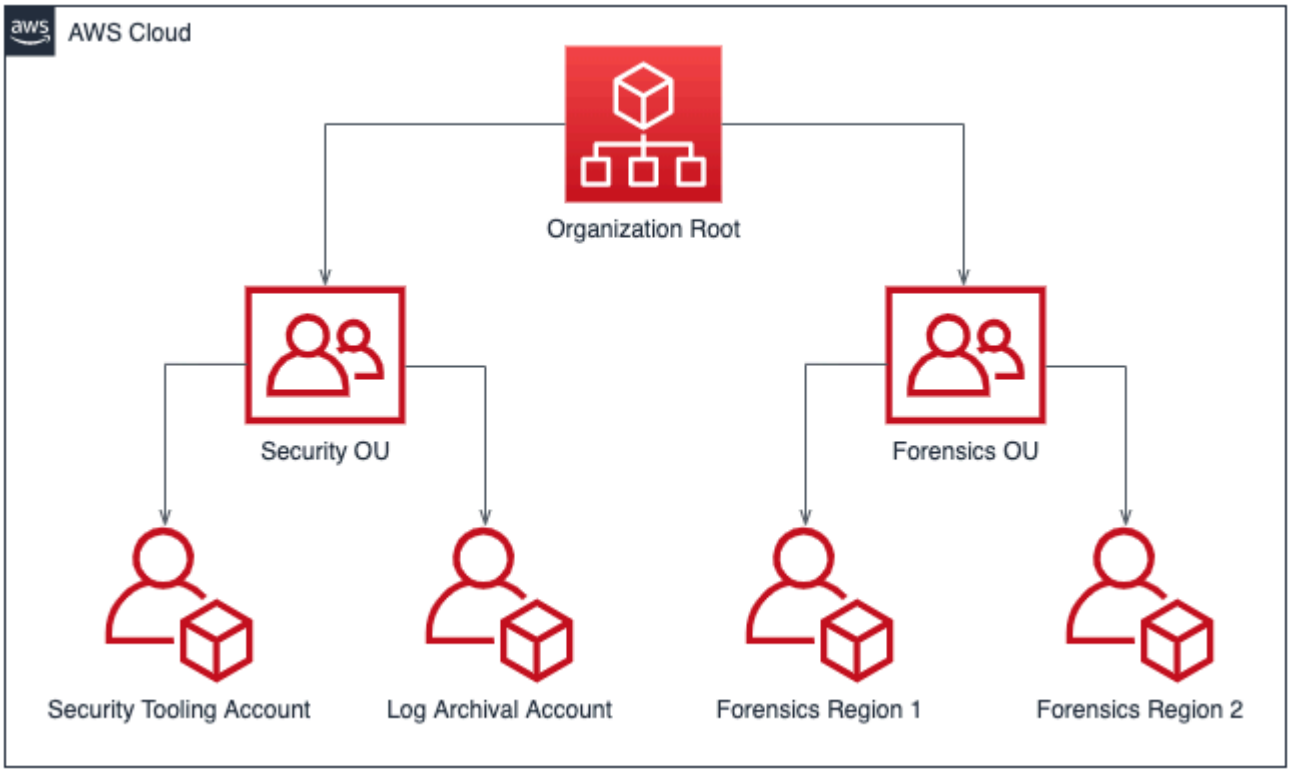
O AWS Organizations auxilia no gerenciamento e governança centralizados de um ambiente da AWS à medida que você expande e escala os recursos da AWS. Uma organização da AWS consolida suas contas da AWS para que possam ser administradas por você como uma única unidade. Você pode usar unidades organizacionais (UOs) para agrupar contas e administrá-las como uma unidade única.

No contexto da resposta a incidentes, é recomendável contar com uma estrutura de contas da AWS que fornece suporte para as funções de resposta a incidentes, incluindo uma UO de segurança e uma UO de análise forense. Dentro da OU de segurança, é necessário ter contas para:

- Arquivamento de log: agregue os logs em uma conta da AWS destinada ao arquivamento de log.
- Ferramentas de segurança: centralize os serviços de segurança em uma conta da AWS dedicada às ferramentas de segurança. Essa conta opera como administrador delegado dos serviços de segurança.

Dentro da UO forense, você tem a opção de implementar uma única conta ou contas forenses para cada região em que opera, dependendo da que funciona melhor para sua empresa e modelo operacional. Para exemplificar a abordagem de contas por região, se você operar somente nas regiões Leste dos EUA (Norte da Virgínia) (us-east-1) e Oeste dos EUA (Oregon) (us-west-2), terá duas contas na UO de análise forense, nomeadamente, uma para us-east-1 e outra para us-west-2. Como é preciso tempo para provisionar novas contas, é imperativo criar e instrumentar as contas forenses bem antes de um incidente, para que os respondentes possam estar preparados para usá-las de forma eficaz em suas respostas.

O diagrama a seguir exibe um exemplo de estrutura de contas, incluindo uma UO forense com contas forenses por região:



Estrutura de contas por região para o gerenciamento da resposta a incidentes

Desenvolva e implemente uma estratégia de marcação

Obter informações contextuais sobre o caso de uso empresarial e as partes interessadas internas relevantes em torno de um recurso da AWS pode ser difícil. Uma forma de fazer isso é na forma de tags, que atribuem metadados aos recursos da AWS e consistem em uma chave e um valor definidos pelo usuário. Você pode criar tags para categorizar os recursos por finalidade, proprietário, ambiente, tipo de dados processados e outros critérios de sua escolha.

Dispor de uma estratégia consistente de marcação pode facilitar a aceleração dos tempos de resposta ao permitir a rápida identificação e análise das informações contextuais relacionadas a um recurso da AWS. As tags também podem servir como um mecanismo para iniciar automações de resposta. Para obter mais informações sobre o que deve ser etiquetado, consulte a documentação referente à marcação de recursos da AWS. Primeiro, você deve definir as tags que deseja implementar em toda a sua organização. Depois disso, você implementará e aplicará essa estratégia de marcação. Mais detalhes sobre a implementação e sobre a aplicação da estratégia podem ser consultados na publicação do blog da AWS "Implement AWS resource tagging strategy using AWS Tag Policies and Service Control Policies (SCPs)".

Atualização das informações de contato vinculadas à conta da AWS

Para cada uma de suas contas da AWS, é importante manter informações de contato precisas e atualizadas, de modo que as partes interessadas adequadas recebam notificações importantes da AWS sobre tópicos como segurança, faturamento e operações. Para cada conta da AWS, há um contato principal e contatos alternativos designados para segurança, faturamento e operações. As diferenças entre esses contatos podem ser consultadas no Guia de referência do AWS Account Management.

Para obter mais detalhes sobre como gerenciar contatos alternativos, consulte a documentação da AWS sobre como adicionar, alterar ou remover contatos alternativos. É uma prática recomendada usar uma lista de distribuição de e-mail caso sua equipe seja responsável por gerenciar questões relacionadas a faturamento, operações e segurança. O uso de uma lista de distribuição de e-mail remove a dependência de uma única pessoa, o que pode causar bloqueios na comunicação em casos de ausência ou de desligamento da empresa. Você também deve verificar se as informações de contato da conta, incluindo o e-mail e o número de telefone, estão bem protegidas, a fim de evitar redefinições indevidas de senha da conta-raiz e restaurações da autenticação multifator (MFA).

Para clientes que usam o AWS Organizations, os administradores da organização podem gerenciar centralmente os contatos alternativos para as contas de membro por meio da conta gerencial ou

de uma conta de administrador delegado, sem a necessidade de credenciais individuais para cada conta da AWS. Além disso, será necessário verificar se as contas criadas recentemente contêm informações de contato precisas. Consulte a publicação do blog Automatically update alternate contacts for newly created Contas da AWS.

Preparação do acesso às contas da Contas da AWS

Durante um incidente, suas equipes de resposta a incidentes devem ter acesso aos ambientes e aos recursos envolvidos no incidente. Certifique-se de que as equipes disponham do acesso apropriado para executar as atividades atribuídas antes da ocorrência de um evento. Para isso, é necessário conhecer o nível de acesso exigido por cada membro da equipe (por exemplo, quais tipos de ações provavelmente precisarão executar) e provisionar previamente o acesso com privilégio mínimo.

Para implementar e provisionar esse acesso, você deve identificar e debater a estratégia de contas da AWS e a estratégia de identidade na nuvem com os arquitetos de nuvem da sua organização, a fim de compreender quais métodos de autenticação e de autorização estão configurados. Devido à natureza privilegiada dessas credenciais, recomenda-se considerar o uso de fluxos de aprovação ou a recuperação de credenciais usando um cofre ou um local seguro como parte de sua implementação. Após a implementação, é essencial documentar e testar o acesso dos membros da equipe com antecedência, garantindo que possam responder sem atrasos em caso de incidente.

Por fim, os usuários que foram criados especificamente para responder a um incidente de segurança costumam ter privilégios elevados, a fim de garantir acesso suficiente. Portanto, o uso dessas credenciais deve ser restrito, monitorado e não empregado em atividades rotineiras.

Compreensão do panorama de ameaças

Desenvolvimento de modelos de ameaças

Ao desenvolver modelos de ameaças, as organizações podem identificar ameaças e mitigações antes que um usuário não autorizado o faça. Existem diversas estratégias e abordagens para a modelagem de ameaças. Para saber mais, consulte a publicação do blog How to approach threat modeling. Para a resposta a incidentes, um modelo de ameaças pode auxiliar na identificação dos vetores de ataque que um agente malicioso possa ter usado durante um incidente. Compreender contra o que você está se defendendo é fundamental para garantir uma resposta em tempo hábil. Além disso, é possível contar com um AWS Partner para modelagem de ameaças. Para localizar um parceiro da AWS, use a AWS Partner Network.

Integração e uso da inteligência de ameaças cibernéticas

A inteligência de ameaças cibernéticas consiste em dados e análises referentes à intenção, à oportunidade e à capacidade de um agente malicioso. A obtenção e o uso da inteligência de ameaças auxiliam na detecção precoce de um incidente e na compreensão aprofundada do comportamento desses agentes maliciosos. A inteligência de ameaças cibernéticas inclui indicadores estáticos, como endereços IP ou hashes de arquivos de malware. Além disso, essa inteligência inclui informações de alto nível, como padrões comportamentais e intenções. É possível coletar a inteligência de ameaças de diversos fornecedores de segurança cibernética e de repositórios de código aberto.

Para integrar e maximizar o uso da inteligência de ameaças em seu ambiente da AWS, é possível usar funcionalidades prontas e também integrar suas próprias listas de inteligência de ameaças. O Amazon GuardDuty usa fontes de inteligência de ameaças provenientes da AWS e de entidades externas. Outros serviços da AWS, como um firewall DNS e as regras do AWS WAF, também operam com base em informações fornecidas pelo grupo avançado de inteligência de ameaças da AWS. Algumas descobertas do GuardDuty são mapeadas para o MITRE ATT&CK Framework, que fornece informações baseadas em observações reais sobre táticas e técnicas usadas por adversários.

Selecione e configure logs para análise e alertas

Durante uma investigação de segurança, você precisa ser capaz de revisar os logs relevantes para registrar e compreender o escopo completo e o cronograma do incidente. Os logs também são necessários para geração de alertas indicando que determinadas ações de interesse ocorreram. É essencial selecionar, ativar, armazenar e configurar mecanismos de consulta e recuperação, bem como definir alertas. Cada uma dessas ações é analisada nesta seção. Para obter mais detalhes, consulte a publicação do blog da AWS Logging strategies for security incident response.

Seleção e habilitação das fontes de log

Antes de conduzir uma investigação de segurança, é essencial capturar previamente logs relevantes que permitam reconstruir de forma retroativa as atividades ocorridas em uma conta da AWS. Selecione e habilite as fontes de log relevantes às workloads da conta da AWS.

O AWS CloudTrail consiste em um serviço de registro em log que rastreia as chamadas de API realizadas em uma conta da AWS, capturando a atividade dos serviços da AWS. Este serviço é habilitado por padrão, com retenção de 90 dias para eventos de gerenciamento, os quais podem ser recuperados por meio do recurso Event History do CloudTrail, usando o Console de gerenciamento da AWS, a AWS CLI ou um AWS SDK. Para obter uma retenção prolongada e uma visibilidade dos

eventos de dados, é necessário criar uma trilha do CloudTrail associada a um bucket do Amazon S3 e, opcionalmente, a um grupo de logs do CloudWatch. Como alternativa, é possível criar um CloudTrail Lake, que armazena os logs do CloudTrail por até sete anos e oferece uma interface de consulta baseada em SQL.

A AWS recomenda que os clientes que usam uma VPC habilitem os logs de tráfego de rede e de DNS, utilizando, respectivamente, os logs de fluxo da VPC e os logs de consulta do Amazon Route 53 Resolver, transmitindo-os para um bucket do Amazon S3 ou para um grupo de logs do CloudWatch. É possível criar um log de fluxo da VPC para uma VPC, uma sub-rede ou uma interface de rede. No caso dos logs de fluxo da VPC, é possível definir de forma seletiva a maneira e o local em que os logs de fluxo serão habilitados, com o objetivo de reduzir custos.

Os logs do AWS CloudTrail, os logs de fluxo da VPC e os logs de consulta do Route 53 Resolver constituem a tríade básica de registro em log para o fornecimento de suporte a investigações de segurança na AWS.

Os serviços da AWS podem gerar logs que não são capturados pela tríade básica de registro em log, como os logs do Elastic Load Balancing, os logs do AWS WAF, os logs do gravador do AWS Config, as descobertas do Amazon GuardDuty, os logs de auditoria do Amazon Elastic Kubernetes Service (Amazon EKS) e os logs do sistema operacional e de aplicações da instância do Amazon EC2. Consulte o the section called “Apêndice A: definições das funcionalidades da nuvem” para obter a lista completa de opções de registro em log e de monitoramento.

Seleção do armazenamento de log

A definição do armazenamento de log depende, em geral, da ferramenta de consulta usada, das necessidades de retenção, da familiaridade dos usuários e das considerações de custo. Ao habilitar os logs de serviços da AWS, é necessário fornecer um local de armazenamento, que geralmente consiste em um bucket do Amazon S3 ou em um grupo de logs do CloudWatch.

Um bucket do Amazon S3 fornece um armazenamento durável e econômico, com a opção de configurar políticas de ciclo de vida. Os logs armazenados em buckets do Amazon S3 podem ser consultados nativamente usando serviços como o Amazon Athena. Um grupo de logs do CloudWatch oferece armazenamento durável e um recurso de consultas incorporado por meio do CloudWatch Logs Insights.

Identificação da retenção de log apropriada

Ao usar um bucket do S3 ou um grupo de logs do CloudWatch para armazenar logs, é necessário estabelecer ciclos de vida adequados para cada fonte de log, a fim de otimizar os custos de

armazenamento e de recuperação. Em geral, os clientes mantêm logs disponíveis para consulta por um período que varia entre 3 e 12 meses, podendo ampliar a retenção por até sete anos. A escolha de disponibilidade e retenção deve se alinhar aos seus requisitos de segurança e um composto de atribuições regulatórias, estatutárias e de negócios.

Seleção e implementação de mecanismos de consulta para logs

Na AWS, os principais serviços que você pode usar para consultar logs são o CloudWatch Logs Insights, para dados armazenados em grupos de logs do CloudWatch, e o Amazon Athena e o Amazon OpenSearch Service, para dados armazenados no Amazon S3. Além disso, é possível usar ferramentas de consulta de entidades externas, como sistemas de gerenciamento de informações e de eventos de segurança (SIEM, na sigla em inglês).

O processo para selecionar uma ferramenta de consulta de log deve considerar as pessoas, o processo e os aspectos de tecnologia de suas operações de segurança. Selecione uma ferramenta que cumpra os requisitos operacionais, empresariais e de segurança, garantindo também acessibilidade e facilidade de manutenção no longo prazo. Lembre-se de que as ferramentas de consulta de logs funcionam da forma ideal quando o número de logs a serem verificados é mantido dentro dos limites da ferramenta. Não é incomum que os clientes tenham diversas ferramentas de consulta em função de limitações técnicas ou orçamentárias. Por exemplo, os clientes podem usar um SIEM proveniente de uma entidade externa para consultar dados dos últimos 90 dias e usar o Athena para consultas além desse período de 90 dias, devido ao custo de ingestão de logs em um SIEM. Independentemente da implementação, verifique se a sua abordagem minimiza o número de ferramentas necessárias, a fim de maximizar a eficiência operacional, especialmente durante as investigações de um evento de segurança.

Uso de logs para geração de alertas

A AWS fornece geração de alertas de forma nativa por meio de serviços de segurança, como o Amazon GuardDuty, o AWS Security Hub CSPM e o AWS Config. Além disso, é possível usar mecanismos personalizados para geração de alertas de segurança que não são cobertos por esses serviços ou para alertas específicos e relevantes para o seu ambiente. A criação desses alertas e detecções é abordada na seção intitulada the section called “Detecção” neste documento.

Desenvolvimento de funcionalidades de análise forense

Antes de um incidente de segurança, considere o desenvolvimento de recursos forenses para contribuir com as investigações de eventos de segurança. O guia Guide to Integrating Forensic Techniques into Incident Response elaborado pelo NIST oferece orientações sobre o tema.

Análise forense na AWS

Os conceitos da análise forense on-premises tradicional se aplicam à AWS. A publicação do blog Forensic investigation environment strategies in the Nuvem AWS fornece informações essenciais para que você possa iniciar a migração do conhecimento técnico forense para a AWS.

Após configurar seu ambiente e a estrutura de contas da AWS para a análise forense, será necessário definir as tecnologias requeridas para executar metodologias que preservem a integridade forense nas quatro fases:

- Coleta: realize a coleta de logs relevantes da AWS, como os logs do AWS CloudTrail, os logs do AWS Config, os logs de fluxo da VPC e os logs em nível de host. Além disso, colete snapshots, backups e despejos de memória dos recursos da AWS impactados.
- Exame: examine os dados coletados ao extrair e ao avaliar as informações relevantes.
- Análise: analise os dados coletados a fim de compreender o incidente e tirar conclusões a partir deles.
- Relatório: apresente as informações resultantes da fase de análise.

Capture backups e snapshots

Configurar backups dos principais sistemas e bancos de dados é essencial para a recuperação de um incidente de segurança e para fins forenses. Com os backups em vigor, você pode restaurar seus sistemas ao estado seguro anterior. Na AWS, é possível criar snapshots de vários recursos. Os snapshots fornecem backups pontuais desses recursos. Há muitos serviços da AWS que podem ajudar em backup e recuperação. Consulte o guia Backup and Recovery Prescriptive Guidance para obter mais detalhes sobre esses serviços e abordagens para backup e para recuperação. Para obter mais detalhes, consulte a publicação do blog Use backups to recover from security incidents.

Especialmente quando se trata de situações como ransomware, é fundamental que os backups estejam bem protegidos. Consulte a publicação do blog Top 10 security best practices for securing backups in AWS para obter orientações sobre como proteger seus backups. Além de proteger os backups, você deve testar regularmente seus processos de backup e restauração para verificar se a tecnologia e os processos implementados funcionam conforme o esperado.

Automação de análise forense na AWS

Durante um evento de segurança, sua equipe de resposta a incidentes deve ser capaz de coletar e de analisar evidências rapidamente, ao mesmo tempo em que mantém a precisão em relação ao

intervalo de tempo relacionado ao incidente. É desafiador e demorado para a equipe de resposta a incidentes coletar manualmente as evidências relevantes em um ambiente de nuvem, especialmente quando há um grande número de instâncias e contas envolvidas. Além disso, a coleta manual pode estar sujeita a erros humanos. Por esses motivos, recomenda-se que os clientes desenvolvam e implementem mecanismos automatizados para a análise forense.

A AWS disponibiliza diversos recursos de automação para a análise forense, os quais estão consolidados no Apêndice na seção the section called “Recursos relacionados à análise forense”. Esses recursos são exemplos de padrões forenses que desenvolvemos e que os clientes implementaram. Embora possam ser uma arquitetura de referência útil para começar, considere modificá-las ou criar padrões de automação forense com base em seu ambiente, requisitos, ferramentas e processos forenses.

Resumo dos itens de preparação

Uma preparação completa para responder a eventos de segurança é essencial para uma resposta a incidentes eficaz e em tempo hábil. A preparação para a resposta a incidentes envolve pessoas, processos e tecnologia. Todos esses três domínios têm igual importância no contexto da preparação. Você deve preparar e aprimorar seu programa de resposta a incidentes considerando todos os três domínios.

A Tabela 2 apresenta um resumo dos itens de preparação detalhados nesta seção.

Tabela 2: itens de preparação para a resposta a incidentes

Domínio	Item de preparação	Itens de ação
Pessoas	Definir atividades a serem atribuídas e responsab ilidades.	• Identificar as partes interessadas relevantes na resposta a incidentes. • Desenvolver um quadro que compreende o responsável, a autoridade, o consultado e o informado (RACI) para um incidente.
Pessoas	Treinar a equipe de resposta a incidentes na AWS.	• Treinar as partes interessa das da resposta a incidente s nos fundamentos da AWS.

Domínio	Item de preparação	Itens de ação
		• Treinar as partes interessadas da resposta a incidentes nos serviços de segurança e de monitoramento da AWS. • Treinar as partes interessadas da resposta a incidentes em seu ambiente da AWS e na forma como o ambiente foi arquitetado.
Pessoas	Compreender as opções de suporte da AWS.	• Entenda as diferenças entre o suporte da AWS, os engenheiros do Security Incident Response e a equipe de resposta a ataques de DDoS (DRT) e o AMS. • Entenda o caminho de triagem e escalação para entrar em contato com os engenheiros de a Security Incident Response durante um evento de segurança ativo, se necessário.

Domínio	Item de preparação	Itens de ação
Processos	Desenvolver um plano de resposta a incidentes.	• Criar um documento de alto nível que defina o programa e a estratégia de resposta a incidentes. • Incluir no plano de resposta a incidentes uma matriz RACI, um plano de comunicação, as definições de incidentes e as fases da resposta a incidentes.
Processos	Documentar e centralizar os diagramas de arquitetura.	• Documentar os detalhes sobre como seu ambiente da AWS está configurado, abrangendo a estrutura de contas, o uso de serviços, os padrões de IAM e outras funcionalidades essenciais da configuração da AWS. • Desenvolver diagramas de arquitetura das suas arquiteturas em nuvem.
Processos	Desenvolver planos de ação de resposta a incidentes.	• Criar um modelo para a estrutura dos seus planos de ação. • Desenvolver planos de ação para os eventos de segurança esperados. • Desenvolver planos de ação para os alertas de segurança conhecidos, como as descobertas do GuardDuty.

Domínio	Item de preparação	Itens de ação
Processos	Executar simulações de forma periódica.	• Desenvolver uma frequênci a sistemática para a execução de simulações de incidentes. • Usar os resultados e as lições aprendidas para realizar a iteração do seu programa de resposta a incidentes.
Tecnologia	Desenvolver uma estrutura de contas da AWS.	• Planejar uma estrutura de contas que defina como as workloads serão separadas por contas da AWS. • Criar uma unidade organizacional (OU) de segurança com uma conta para ferramentas de segurança e arquivamento de log. • Criar uma OU de análise forense com contas de análise forense específicas para cada região em que você opera.
Tecnologia	Desenvolver e implementar uma estratégia de marcação que auxilie os responsáveis pela resposta a incidentes na identificação da propriedade e do contexto para as descobert as.	• Planejar uma estratégia para a marcação e definir quais etiquetas devem ser associadas aos recursos da AWS. • Implementar e aplicar a estratégia de marcação.

Domínio	Item de preparação	Itens de ação
Tecnologia	Atualizar as informações de contato das contas da AWS.	• Verificar se as contas da AWS contam com informaçõ es de contato cadastradas. • Criar listas de distribuição de e-mail para as informaçõ es de contato, a fim de remover pontos únicos de falha. • Proteger as contas de e-mail que estão associadas às informações de contato das contas da AWS.
Tecnologia	Preparar o acesso às contas da AWS.	• Definir os níveis de acesso necessários para que os responsáveis pela resposta a incidentes possam atuar adequadamente a um incidente. • Implementar, testar e monitorar os acessos definidos.
Tecnologia	Compreender o cenário de ameaças.	• Desenvolver modelos de ameaças para seu ambiente e para suas aplicações. • Integrar e usar a inteligência de ameaças cibernéticas.

Domínio	Item de preparação	Itens de ação
Tecnologia	Selecionar e configurar os logs.	• Identificar e habilitar os logs relevantes para as investiga ções. • Selecionar o local de armazenamento dos log. • Identificar e implementar políticas de retenção de log. • Desenvolver um mecanismo para recuperação e consulta de logs e de artefatos. • Usar os logs para geração de alertas.
Tecnologia	Desenvolver funcionalidades de análise forense.	• Identificar os artefatos necessários para a coleta forense. • Capturar e proteger backups dos sistemas essenciais. • Definir mecanismos para análise dos logs e dos artefatos identificados. • Implementar a automação para a análise forense.

Uma abordagem iterativa é recomendada para a preparação da resposta a incidentes. Como não é possível implementar todos os itens de preparação de imediato, é importante estabelecer um plano que comece em pequena escala e evolua gradualmente, com melhorias contínuas nas funcionalidades de resposta a incidentes.

Operações

As operações são a base da resposta a incidentes. É aqui que ocorrem as ações de resposta e atenuação de incidentes de segurança. As operações incluem as seguintes cinco fases: detecção, análise, contenção, erradicação e recuperação. As descrições dessas fases e das metas podem ser encontradas na Tabela 3.

Tabela 3: fases operacionais

Fase	Objetivo
Detecção	Identifique um possível evento de segurança.
Análise	Determinar se um evento de segurança constitui um incidente e avaliar o escopo do incidente.
Contenção	Minimize e limite o escopo do evento de segurança.
Erradicação	Remova recursos ou artefatos não autorizad os relacionados ao evento de segurança. Implemente atenuações para as causas do incidente de segurança.
Recuperação	Restaurar os sistemas para um estado seguro conhecido e monitorar esses sistemas para verificar se não há retorno da ameaça.

As fases devem servir como orientação quando você responde e atua em incidentes de segurança, a fim de responder de forma eficaz e robusta. As ações reais realizadas variam de acordo com o incidente. Um incidente envolvendo ransomware, por exemplo, terá um conjunto de etapas de resposta a serem seguidas diferente do que o de um incidente que envolva um bucket público do Amazon S3. Além disso, essas fases não acontecem necessariamente de modo sequencial. Após a contenção e a erradicação, talvez seja necessário retornar à análise para entender se suas ações foram eficazes.

Detecção

Um alerta corresponde ao componente principal da fase de detecção. Ele gera uma notificação para iniciar o processo de resposta a incidente com base nas atividades de ameaças na conta da AWS em questão.

A precisão dos alertas é um desafio. Não é sempre que é possível determinar com total certeza se um incidente ocorreu, está em andamento ou se ocorrerá no futuro. A seguir, apresentamos alguns motivos:

- Os mecanismos de detecção são baseados na variação em relação à linha de base, em padrões conhecidos e em notificações provenientes de entidades internas ou externas.
- Em virtude da natureza imprevisível da tecnologia e das pessoas, que são respectivamente os meios e os agentes dos incidentes de segurança, as linhas de base se alteram com o tempo. Os padrões anômalos surgem por meio de táticas, técnicas e procedimentos (TTPs) novos ou modificados de agentes de ameaças.
- As alterações relacionadas a pessoas, tecnologia e processos não são incorporadas imediatamente ao processo de resposta a incidentes. Algumas dessas alterações, inclusive, são descobertas durante o andamento de uma investigação.

Fontes de alertas

Você deve considerar o uso das seguintes fontes para definir alertas:

- Descobertas: os serviços da AWS, como o Amazon GuardDuty, o AWS Security Hub CSPM, o Amazon Macie, o Amazon Inspector, o AWS Config, o IAM Access Analyzer e o Analisador de Acesso à Rede, geram descobertas que podem ser usadas para criar alertas.
- Logs: os logs de serviços da AWS, infraestrutura e aplicações armazenados em buckets do Amazon S3 e em grupos de logs do CloudWatch podem ser analisados e correlacionados para gerar alertas.
- Atividade relacionada ao faturamento: uma mudança repentina na atividade relacionada ao faturamento pode indicar um evento de segurança. Siga a documentação Criar um alarme de faturamento para monitorar suas cobranças estimadas da AWS para realizar o monitoramento dessa atividade.
- Inteligência de ameaças cibernéticas: caso você seja assinante de um feed de inteligência de ameaças cibernéticas de entidades externas, é possível realizar a correlação dessas informações

com outras ferramentas de registro em log e de monitoramento para identificar possíveis indicadores de eventos.

- Ferramentas de parceiros: os parceiros da AWS Partner Network (APN) oferecem produtos de alto nível que podem ajudar você a atingir seus objetivos de segurança. Para a resposta a incidentes, os produtos de parceiros com funcionalidades de detecção e de resposta em endpoints (EDR, na sigla em inglês) ou de SIEM podem contribuir para o cumprimento dos objetivos de resposta a incidentes. Para obter mais informações, consulte Soluções de parceiros de competência em segurança e Soluções de segurança no AWS Marketplace.
- Confiança e Segurança da AWS: a equipe de Suporte pode entrar em contato com os clientes caso identifiquemos atividades abusivas ou maliciosas.
- Contato único: como podem ser seus clientes, desenvolvedores ou outros membros da equipe que percebem algo incomum na sua organização, é importante dispor de um método bem divulgado e conhecido para contato com sua equipe de segurança. Entre as opções populares estão sistemas de emissão de tíquetes, endereços de e-mail de contato e formulários na web. Caso sua organização atue com o público em geral, pode ser necessário também dispor de um canal de contato com a segurança voltada ao público externo.

Para obter mais informações sobre as funcionalidades em nuvem que podem ser usadas durante suas investigações, consulte o the section called “Apêndice A: definições das funcionalidades da nuvem” neste documento.

Detecção como parte da engenharia de controles de segurança

Os mecanismos de detecção constituem uma parte essencial do desenvolvimento de controles de segurança. À medida que controles diretivos e preventivos são definidos, controles detectivos e responsivos correspondentes devem ser elaborados. Para exemplificar, uma organização estabelece um controle diretivo relacionado ao usuário-raiz de uma conta da AWS, o qual deve ser usado somente para atividades específicas e muito bem definidas. Esse controle é associado a um controle preventivo, implementado por meio de uma política de controle de serviços (SCP, na sigla em inglês) da organização da AWS. Se ocorrer uma atividade do usuário-raiz que ultrapassa a linha de base esperada, um controle detectivo, implementado com uma regra do EventBridge e um tópico do SNS, alertará o Security Operations Center (SOC). O controle responsivo envolve o SOC ao selecionar o plano de ação mais apropriado, realizar a análise e trabalhar até que o incidente seja resolvido.

Os controles de segurança são melhor definidos por meio da modelagem de ameaças das workloads executadas na AWS. A criticidade dos controles detectivos será determinada pela análise de impacto nos negócios (BIA, na sigla em inglês) para a workload específica. Os alertas gerados pelos

controles detectivos não são tratados à medida que chegam, mas sim com base em sua criticidade inicial, a qual pode ser ajustada durante a análise. A criticidade inicial estabelecida serve como um auxílio para a priorização, no entanto, apenas o contexto em que o alerta ocorreu determinará sua real criticidade. Para exemplificar, uma organização usa o Amazon GuardDuty como um componente do controle detectivo aplicado para as instâncias do EC2 que fazem parte de uma workload. A descoberta `Impact:EC2/SuspiciousDomainRequest.Reputation` é gerada, informando que a instância do Amazon EC2 listada dentro da sua workload está consultando um nome de domínio suspeito de ser malicioso. Esse alerta é configurado por padrão com severidade baixa e, à medida que a fase de análise avança, foi constatado que várias centenas de instâncias do EC2 do tipo `p4d.24xlarge` foram implantadas por um agente não autorizado, aumentando significativamente o custo operacional da organização. Nesse momento, a equipe de resposta a incidentes decide ajustar a criticidade desse alerta para alta, aumentando o senso de urgência e agilizando as ações subsequentes. Vale destacar que a severidade da descoberta do GuardDuty não pode ser alterada.

Implementações de controles detectivos

É importante compreender como os controles detectivos são implementados, pois isso auxilia a determinar como o alerta será usado para o evento específico. Existem duas principais formas de implementação de controles detectivos técnicos:

- A detecção comportamental se baseia em modelos matemáticos, comumente conhecidos como machine learning (ML) ou inteligência artificial (IA). A detecção é realizada por inferência. Portanto, o alerta pode não refletir necessariamente um evento real.
- A detecção baseada em regras é determinística. Dessa forma, os clientes podem definir exatamente os parâmetros das atividades sobre as quais desejam receber alertas, garantindo certeza na detecção.

As implementações modernas de sistemas detectivos, como um sistema de detecção de intrusão (IDS, na sigla em inglês), geralmente incluem ambos os mecanismos. A seguir, apresentamos alguns exemplos de detecções baseadas em regras e comportamentais com o GuardDuty.

- Quando a descoberta `Exfiltration:IAMUser/AnomalousBehavior` é gerada, ela informa que “uma solicitação de API anômala foi observada em sua conta”. Ao analisar a documentação mais detalhadamente, verifica-se que ela informa que “o modelo de ML avalia todas as solicitações de API na sua conta e identifica eventos anômalos associados a técnicas usadas por agentes adversários”, o que demonstra a natureza comportamental dessa descoberta.
- Para a descoberta `Impact:S3/MaliciousIPCaller`, o GuardDuty analisa as chamadas de API do serviço Amazon S3 no CloudTrail, comparando o elemento de log `SourceIPAddress`

com uma tabela de endereços IP públicos que inclui feeds de inteligência de ameaças. Assim que encontra uma correspondência direta com uma entrada, a descoberta é gerada pelo serviço.

Recomendamos a implementação de uma combinação de alertas comportamentais e baseados em regras, pois nem sempre é possível aplicar alertas baseados em regras para todas as atividades dentro do seu modelo de ameaças.

Detecção baseada em pessoas

Até o momento, abordamos a detecção baseada em tecnologia. Outra fonte importante de detecção provém de pessoas internas ou externas à organização do cliente. As pessoas internas podem ser definidas como um colaborador ou prestador de serviços, e as pessoas externas são entidades como pesquisadores que se concentram em segurança, autoridades policiais, meios de comunicação e redes sociais.

Embora a detecção baseada em tecnologia possa ser configurada de forma sistemática, a detecção baseada em pessoas ocorre de diversas formas, como e-mails, tíquetes, correspondências, publicações nos meios de comunicação, telefonemas e interações presenciais. As notificações de detecção tecnológica são geralmente entregues em tempo quase real, enquanto para a detecção baseada em pessoas não há expectativas definidas de prazo. É imprescindível que a cultura de segurança incorpore, facilite e fortaleça os mecanismos de detecção baseados em pessoas, visando uma abordagem de defesa em profundidade para a segurança.

Resumo

Na detecção, é importante contar com uma combinação de alertas baseados em regras e orientados por comportamento. Além disso, devem existir mecanismos para que pessoas, tanto internas quanto externas, possam registrar tickets sobre questões de segurança. Os seres humanos podem ser uma das fontes mais valiosas para eventos de segurança, por isso é importante ter processos implementados que permitam que as pessoas realizem o encaminhamento de preocupações. É possível usar modelos de ameaças do seu ambiente para começar a desenvolver as detecções. Esses modelos de ameaças ajudarão você a desenvolver alertas baseados nas ameaças mais relevantes para o seu ambiente. Por fim, você pode usar estruturas como o MITRE ATT&CK para compreender as táticas, técnicas e procedimentos (TTPs) dos agentes de ameaças. A estrutura MITRE ATT&CK pode ser útil para servir como uma linguagem comum entre seus diversos mecanismos de detecção.

Análise

Os logs, as funcionalidades de consulta e a inteligência de ameaças são alguns dos componentes de apoio necessários para a fase de análise. Diversos logs que são usados na fase de detecção também são aproveitados na análise, sendo necessário incorporá-los e configurar as ferramentas de consulta correspondentes.

Validação, definição de escopo e avaliação do impacto do alerta

Durante a fase de análise, realiza-se uma análise abrangente dos logs com o objetivo de validar os alertas, definir o escopo e avaliar o impacto do possível comprometimento.

- A validação do alerta constitui o ponto de entrada da fase de análise. Os responsáveis pela resposta a incidentes buscarão entradas de log provenientes de diversas fontes e entrarão em contato diretamente com os proprietários da workload afetada.
- A definição do escopo é a etapa seguinte, na qual todos os recursos envolvidos são inventariados e a criticidade do alerta é ajustada após o consenso entre as partes interessadas de que se trata, provavelmente, de um alerta verdadeiro.
- Por fim, a análise de impacto descreve a interrupção real nos negócios.

Uma vez que os componentes da workload afetada forem identificados, os resultados do escopo podem ser correlacionados com o objetivo de ponto de recuperação (RPO) e com o objetivo de tempo de recuperação (RTO) da workload correspondente, ajustando a criticidade do alerta, o que dará início à alocação de recursos e às atividades subsequentes. Não são todos os incidentes que interromperão diretamente as operações de uma workload que fornece suporte a um processo de negócios. Incidentes como a divulgação de dados sensíveis, o roubo de propriedade intelectual ou o sequestro de recursos (como no caso de mineração de criptomoedas) podem não paralisar ou prejudicar imediatamente um processo de negócios, mas podem acarretar consequências em um momento posterior.

Enriquecimento de logs e de descobertas de segurança

Enriquecimento com inteligência de ameaças e contexto organizacional

Ao longo da análise, é necessário enriquecer os observáveis de interesse a fim de proporcionar uma contextualização aprimorada do alerta. Conforme exposto na seção Preparação, a integração e o aproveitamento da inteligência de ameaças cibernéticas podem ser benéficos para a obtenção de uma compreensão mais aprofundada da descoberta de segurança. Os serviços de inteligência de ameaças são usados para atribuir reputação e identificar a titularidade de endereços IP públicos,

nomes de domínio e hashes de arquivos. Essas ferramentas estão disponíveis por meio de serviços gratuitos ou pagos.

Os clientes que adotam o Amazon Athena como uma ferramenta de consulta de log obtêm a vantagem de usar trabalhos do AWS Glue para carregar informações de inteligência de ameaças como tabelas. As tabelas de inteligência de ameaças podem ser usadas em consultas SQL para correlacionar elementos dos logs, como endereços IP e nomes de domínio, proporcionando uma visão enriquecida dos dados a serem analisados.

A AWS não fornece inteligência de ameaças diretamente aos clientes, mas serviços como o Amazon GuardDuty fazem o uso da inteligência de ameaças para enriquecimento e geração de descobertas. Além disso, é possível fazer o upload de listas personalizadas de ameaças no GuardDuty com base em sua própria inteligência de ameaças.

Enriquecimento com automação

A automação constitui uma parte essencial da governança na Nuvem AWS. A automação pode ser usada em todas as diversas fases do ciclo de vida da resposta a incidentes.

Na fase de detecção, a automação baseada em regras realiza a combinação de padrões de interesse definidos no modelo de ameaças com os logs e executa ações apropriadas, como o envio de notificações. A fase de análise pode aproveitar esse mecanismo de detecção para encaminhar o conteúdo do alerta a um mecanismo capaz de consultar os logs e enriquecer os observáveis para a contextualização do evento.

O conteúdo do alerta, em sua forma básica, é composto por um recurso e por uma identidade. Para exemplificar, você poderia implementar uma automação para consultar o CloudTrail sobre a atividade da API da AWS realizada pela identidade ou pelo recurso apresentados no conteúdo do alerta próximo ao momento do alerta, fornecendo informações adicionais como `eventSource`, `eventName`, `SourceIPAddress` e `userAgent` da atividade de API identificada. Ao realizar essas consultas de modo automatizado, os responsáveis pela resposta a incidentes podem economizar tempo durante a triagem e obter contexto adicional para tomar decisões mais bem informadas.

Consulte a publicação do blog How to enrich AWS Security Hub findings with account metadata para obter um exemplo de como usar automação no enriquecimento de descobertas de segurança e na simplificação da análise.

Coleta e análise de evidências forenses

A análise forense, conforme mencionada na seção the section called “Preparação” deste documento, consiste no processo de coleta e de análise de artefatos durante a resposta a incidentes. Na AWS,

essa análise se aplica a recursos do domínio de infraestrutura, como capturas de pacotes de tráfego de rede e despejos de memória do sistema operacional, bem como a recursos do domínio de serviços, como os logs do AWS CloudTrail.

As principais características do processo forense são:

- Consistência: adoção rigorosa das etapas documentadas, sem alterações.
- Repetibilidade: capacidade de gerar exatamente os mesmos resultados ao aplicar novamente o processo ao mesmo artefato.
- Caráter habitual: documentado publicamente e amplamente adotado.

É importante manter uma cadeia de custódia dos artefatos coletados durante a resposta a incidentes. O uso de automação e da geração automática de documentação desse processo de coleta podem ser úteis, além do armazenamento dos artefatos em repositórios com permissão somente de leitura. A análise deve ser realizada apenas em réplicas exatas dos artefatos coletados, a fim de preservar sua integridade.

Coleta de artefatos relevantes

Considerando essas características e com base nos alertas relevantes e na avaliação do impacto e do escopo, será necessário coletar os dados que serão relevantes para as investigações e para as análises posteriores. Diversos tipos e fontes de dados podem ser relevantes para a investigação, incluindo logs do ambiente de gerenciamento e dos serviços (nomeadamente, CloudTrail, eventos de dados do Amazon S3 e fluxo de logs da VPC), dados (por exemplo, metadados e objetos do Amazon S3) e recursos (como bancos de dados e instâncias do Amazon EC2).

Os logs do ambiente de gerenciamento e do serviço podem ser coletados para análise local ou, idealmente, consultados diretamente por meio de serviços nativos da AWS (quando aplicável). Os dados, incluindo metadados, podem ser consultados diretamente para obter informações relevantes ou para adquirir os objetos de origem, por exemplo, usar a AWS CLI CLI para obter metadados do bucket e do objeto do Amazon S3, bem como acessar diretamente os objetos de origem. Os recursos precisam ser coletados de maneira consistente com seu tipo e com o método de análise pretendido. Por exemplo, os bancos de dados podem ser coletados por meio da criação de uma cópia ou de um snapshot do sistema que executa o banco de dados, da cópia ou do snapshot do próprio banco de dados, ou pela consulta e extração de determinados dados e logs relevantes à investigação.

Para instâncias do Amazon EC2, existe um conjunto específico de dados que deve ser coletado e uma ordem definida de coleta que deve ser seguida, a fim de adquirir e preservar a maior quantidade possível de dados para fins de análise e de investigação.

De forma específica, a sequência recomendada de ações para resposta a incidentes, com o objetivo de adquirir e preservar a maior quantidade possível de dados de uma instância do Amazon EC2, é a seguinte:

1. Adquirir metadados da instância: adquira os metadados da instância que sejam relevantes para a investigação e para consultas de dados (nomeadamente, ID da instância, tipo, endereço IP, ID da VPC ou da sub-rede, região, ID da imagem de máquina da Amazon [AMI], grupos de segurança associados e horário de inicialização).
2. Habilitar proteções e etiquetas da instância: habilite as proteções da instância, como a proteção contra rescisão, configure o comportamento de desligamento para a interrupção (caso esteja definido como encerrar), desabilite os atributos Excluir ao Encerrar dos volumes do EBS anexados e aplique etiquetas apropriadas tanto para identificação visual quanto para utilização em possíveis automações de resposta (por exemplo, ao aplicar uma etiqueta com o nome `Status` e o valor `Quarantine`, realizar a aquisição forense dos dados e isolar a instância).
3. Adquirir disco (snapshots do EBS): adquira um snapshot do EBS dos volumes do EBS anexados. Cada snapshot armazena as informações necessárias para restaurar os dados, a partir do momento em que o snapshot foi criado, em um novo volume do EBS. Consulte a etapa para executar a resposta em tempo real e a coleta do artefato, caso esteja usando volumes do armazenamento de instância.
4. Adquirir memória: como os snapshots do EBS capturam somente os dados que foram gravados no volume do Amazon EBS, o que pode excluir dados armazenados ou em cache na memória pelas aplicações ou pelo sistema operacional, é imprescindível adquirir uma imagem da memória do sistema usando uma ferramenta apropriada de uma entidade externa, seja ela de código aberto ou comercial, a fim de obter os dados disponíveis no sistema.
5. (Opcional) Realizar a coleta da resposta e dos artefatos em tempo real: realize a coleta direcionada de dados (para disco, memória e logs) por meio da resposta em tempo real no sistema somente se não for possível adquirir o disco ou a memória por outros meios, ou se houver uma justificativa válida de natureza operacional ou comercial. Essa ação modificará dados e artefatos valiosos do sistema.
6. Descomissionar a instância: realize o desvinculamento da instância dos grupos do Auto Scaling, cancele o registro da instância nos balanceadores de carga e ajuste ou aplique um perfil de instância definido previamente com permissões reduzidas ou inexistentes.

7. Isolar ou realizar a contenção da instância: verifique se a instância está efetivamente isolada de outros sistemas e recursos no ambiente ao realizar o encerramento e evitar conexões atuais e futuras de e para a instância. Consulte a seção the section called “Contenção” deste documento para obter mais detalhes.
8. Opção do responsável pela resposta a incidentes: com base na situação e nas metas, selecione uma das seguintes opções:
   - Desativar e encerrar o sistema (recomendado).

     Encerre o sistema assim que as evidências disponíveis forem adquiridas, a fim de verificar a mitigação mais eficaz contra um possível impacto futuro ao ambiente causado pela instância.
   - Manter a instância em operação em um ambiente isolado com instrumentação para monitoramento.

     Embora não seja recomendado como uma abordagem padrão, se uma situação justificar a observação contínua da instância (como quando dados ou indicadores adicionais são necessários para realizar uma investigação e análise abrangentes da instância), você pode considerar encerrar a instância, criar uma AMI da instância e iniciá-la novamente em sua conta dedicada à análise forense, dentro de um ambiente de sandbox que já esteja instrumentado para ser completamente isolado e configurado com instrumentação para facilitar o monitoramento quase contínuo da instância (por exemplo, os logs de fluxo da VPC ou a VPC Traffic Mirroring).

> **Note**
>
> É essencial capturar a memória antes das atividades de resposta em tempo real ou do isolamento ou desligamento do sistema, a fim de coletar dados voláteis (e valiosos) disponíveis.

Desenvolvimento de narrativas

Durante a análise e a investigação, documente as ações executadas, a análise realizada e as informações identificadas, para serem usadas pelas fases subsequentes e, em última instância, em um relatório final. Essas narrativas devem ser concisas e precisas, confirmando que as informações relevantes estão incluídas para verificar a compreensão eficaz do incidente e para manter uma linha do tempo precisa. As narrativas também são úteis quando você envolve pessoas externas à equipe principal de resposta a incidentes. Aqui está um exemplo:

O departamento de marketing e de vendas recebeu uma nota de resgate em 15 de março de 2022, exigindo o pagamento em criptomoeda para evitar a divulgação pública de possíveis dados sensíveis. O SOC determinou que o banco de dados do Amazon RDS pertencente ao departamento de marketing e de vendas estava acessível ao público em 20 de fevereiro de 2022. O SOC consultou os logs de acesso do RDS e determinou que o endereço IP 198.51.100.23 foi usado em 20 de fevereiro de 2022 com as credenciais `mm03434`, pertencentes à Major Mary, uma das desenvolvedoras web. Ao analisar os logs de fluxo da VPC, o SOC verificou que aproximadamente 256 MB de dados foram transferidos para o mesmo endereço IP na mesma data (carimbo de horário 2022-02-20T15:50+00Z). Por meio de inteligência de ameaças de código aberto, o SOC confirmou que as credenciais estão atualmente disponíveis em texto simples no repositório público *`https[:]// example[.]com/majormary/rds-utils`*.

Contenção

No âmbito da resposta a incidentes, uma definição possível para a contenção é o processo ou a implementação de uma estratégia durante o tratamento de um evento de segurança, que atua para minimizar o escopo do evento de segurança e conter os efeitos do uso não autorizado dentro do ambiente.

Uma estratégia de contenção depende de uma infinidade de fatores e pode variar de uma organização para outra quanto à aplicação das táticas de contenção, ao momento de sua execução e ao seu propósito. O guia NIST SP 800-61 – Computer Security Incident Handling Guide descreve diversos critérios para a determinação da estratégia de contenção apropriada, entre os quais se incluem:

- Danos potenciais e roubo de recursos.
- Necessidade da preservação de evidências.
- Disponibilidade de serviços (como conectividade de rede e serviços prestados a partes externas).
- Tempo e recursos necessários para implementar a estratégia.
- Eficácia da estratégia (por exemplo, contenção parcial ou total).
- Duração da solução (por exemplo, solução de emergência que será removida em quatro horas, solução temporária que será removida em duas semanas ou solução definitiva).

Em relação aos serviços na AWS, no entanto, as etapas essenciais de contenção podem ser resumidas em três categorias principais:

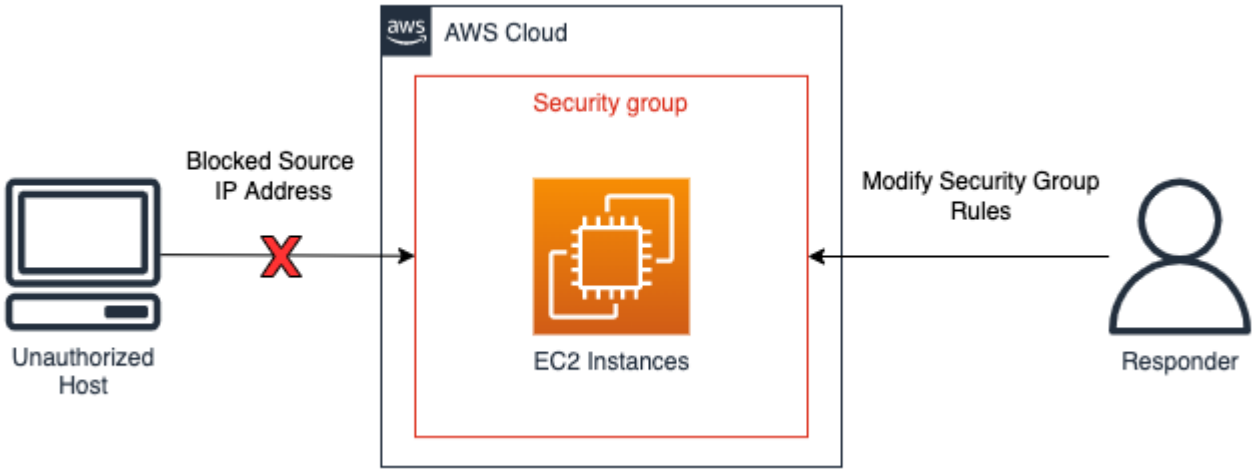
- Contenção da origem: uso de mecanismos de filtragem e de roteamento para restringir o acesso de uma determinada origem.
- Contenção de técnica e de acesso: remoção de acessos para evitar acessos não autorizados aos recursos afetados.
- Contenção do destino: uso de mecanismos de filtragem e de roteamento para restringir o acesso a um recurso de destino.

Contenção da origem

A contenção da origem consiste no uso e na aplicação de mecanismos de filtragem ou roteamento, dentro de um determinado ambiente, com o objetivo de restringir o acesso a recursos provenientes de um endereço IP de origem ou intervalo de rede específico. A seguir, apresentamos exemplos de contenção da origem com o uso de serviços da AWS:

- Grupos de segurança: a criação e a aplicação de grupos de segurança de isolamento para instâncias do Amazon EC2, ou a remoção de regras de um grupo de segurança existente, pode ajudar na contenção do tráfego não autorizado direcionado a uma instância do Amazon EC2 ou a um recurso da AWS. Vale destacar que conexões existentes, que já estejam sendo rastreadas, não serão interrompidas pela alteração dos grupos de segurança. Apenas o tráfego futuro será efetivamente bloqueado pelo novo grupo de segurança (consulte o Plano de ação de Resposta a Incidentes e a seção Rastreamento de conexão de grupo de segurança para obter mais informações sobre as conexões que são rastreadas e as conexões que não rastreadas).
- Políticas: é possível configurar políticas de buckets do Amazon S3 para permitir ou negar tráfego proveniente de um determinado endereço IP, intervalo de rede ou endpoint da VPC. As políticas permitem bloquear endereços suspeitos e restringir o acesso ao bucket do Amazon S3. Você pode encontrar informações adicionais sobre as políticas de bucket em Adicionar uma política de bucket usando o console do Amazon S3.
- AWS WAF: é possível configurar listas de controle de acesso à web (ACLs da web) no AWS WAF para fornecer controle granulado sobre as solicitações web recebidas pelos recursos. Você pode adicionar um endereço IP ou um intervalo de rede a um conjunto de IP configurado no AWS WAF e aplicar condições de correspondência, como bloqueio, ao conjunto de IP. Dessa forma, quaisquer solicitações web serão bloqueadas para um recurso se o endereço IP ou os intervalos de rede provenientes do tráfego de origem corresponderem às regras do conjunto de IP configurado.

Um exemplo de contenção da origem pode ser observado no diagrama apresentado a seguir, no qual um analista responsável pela resposta a incidentes modifica o grupo de segurança de uma instância do Amazon EC2 para restringir novas conexões somente a determinados endereços IP. É importante ressaltar, conforme indicado no tópico sobre grupos de segurança, que conexões existentes, que já estejam sendo rastreadas, não serão interrompidas em decorrência da modificação do grupo de segurança.



Exemplo de contenção de origem

> **Note**
>
> Os grupos de segurança e as ACLs da rede não realizam a filtragem do tráfego direcionado ao Amazon Route 53. Dessa maneira, ao realizar a contenção de uma instância do EC2, é necessário garantir o bloqueio explícito das comunicações DNS, caso o objetivo seja restringir o contato com hosts externos.

Contenção de técnica e de acesso

Restrinja o uso não autorizado de um recurso por meio da limitação das funções e das entidades principais do IAM com acesso ao recurso. Isso inclui restringir as permissões das entidades principais do IAM que têm acesso ao recurso, bem como revogar credenciais de segurança temporárias. A seguir, apresentamos exemplos da contenção de técnica e de acesso com o uso de serviços da AWS:

- Restrição de permissões: as permissões atribuídas a uma entidade principal do IAM devem seguir o princípio de privilégio mínimo. No entanto, durante um evento de segurança ativo, pode ser necessário restringir ainda mais o acesso de uma determinada entidade principal do IAM a um

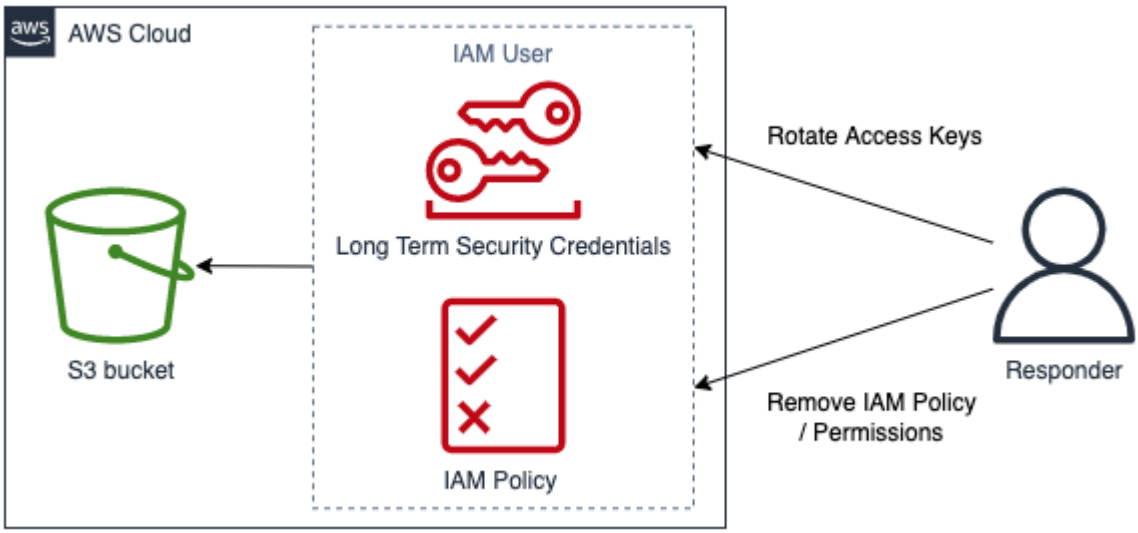
recurso específico. Nesse caso, é possível realizar a contenção do acesso ao recurso ao remover as permissões da entidade principal do IAM em questão. Essa ação é executada com o uso do serviço IAM e pode ser aplicada usando o Console de gerenciamento da AWS, a AWS CLI ou um AWS SDK.

- Revogação de chaves: as chaves de acesso do IAM são usadas pelas entidades principais do IAM para fins de acesso ou de gerenciamento de recursos. Estas são credenciais estáticas de longo prazo usadas para assinar solicitações programáticas à AWS CLI ou à API da AWS, e começam com o prefixo AKIA (para obter informações adicionais, consulte a seção Understanding unique ID prefixes em Identificadores do IAM). Com a finalidade de conter o acesso de uma entidade principal do IAM cuja chave de acesso tenha sido comprometida, é possível desativar ou excluir a chave de acesso. É importante considerar os seguintes pontos:
  - Uma chave de acesso pode ser reativada após ser desativada.
  - Uma chave de acesso não pode ser recuperada após ser excluída.
  - Uma entidade principal do IAM pode ter, no máximo, duas chaves de acesso ativas simultaneamente.
  - Os usuários ou as aplicações que dependem da chave de acesso perderão acesso imediatamente após sua desativação ou exclusão.
- Revogação de credenciais de segurança temporárias: as credenciais de segurança temporárias podem ser empregadas por uma organização para controlar o acesso a recursos da AWS e começam com o prefixo ASIA (para obter informações adicionais, consulte a seção Understanding unique ID prefixes em Identificadores do IAM). As credenciais temporárias são geralmente usadas por perfis do IAM e não necessitam de alteração ou revogação explícita, devido ao seu prazo de validade limitado. Em casos em que ocorra um evento de segurança envolvendo uma credencial de segurança temporária antes da expiração da referida credencial de segurança temporária, pode ser necessário alterar as permissões efetivas das credenciais de segurança temporárias existentes. Essa ação pode ser realizada por meio do serviço IAM no Console de gerenciamento da AWS. As credenciais de segurança temporárias também podem ser emitidas para usuários do IAM (em oposição a perfis do IAM). Entretanto, até o momento da redação desta seção, não existe uma opção para revogar as credenciais de segurança temporárias para um usuário do IAM no Console de gerenciamento da AWS. Para eventos de segurança em que a chave de acesso do IAM de um usuário é comprometida por um usuário não autorizado que criou credenciais de segurança temporárias, as credenciais de segurança temporárias podem ser revogadas usando dois métodos:
  - Realize a anexação de uma política em linha para o usuário do IAM que restrinja o acesso com base no tempo de emissão do token de segurança (consulte a seção Denying access

to temporary security credentials issued before a specific time em Desabilitar permissões de credenciais de segurança temporárias para obter mais detalhes).

  - Realize a exclusão do usuário do IAM proprietário das chaves de acesso comprometidas. É possível criar novamente o usuário, se necessário.
- AWS WAF: determinadas técnicas empregadas por usuários não autorizados incluem padrões comuns de tráfego malicioso, como solicitações que contêm injeção de SQL e cross-site scripting (XSS). O AWS WAF pode ser configurado para corresponder e negar esse tipo de tráfego usando as instruções de regras incorporadas do AWS WAF.

Um exemplo de contenção de técnica e de acesso pode ser observado no diagrama apresentado a seguir, no qual um responsável pela resposta a incidentes altera as chaves de acesso ou remove uma política do IAM para impedir que um usuário do IAM acesse um bucket do Amazon S3.



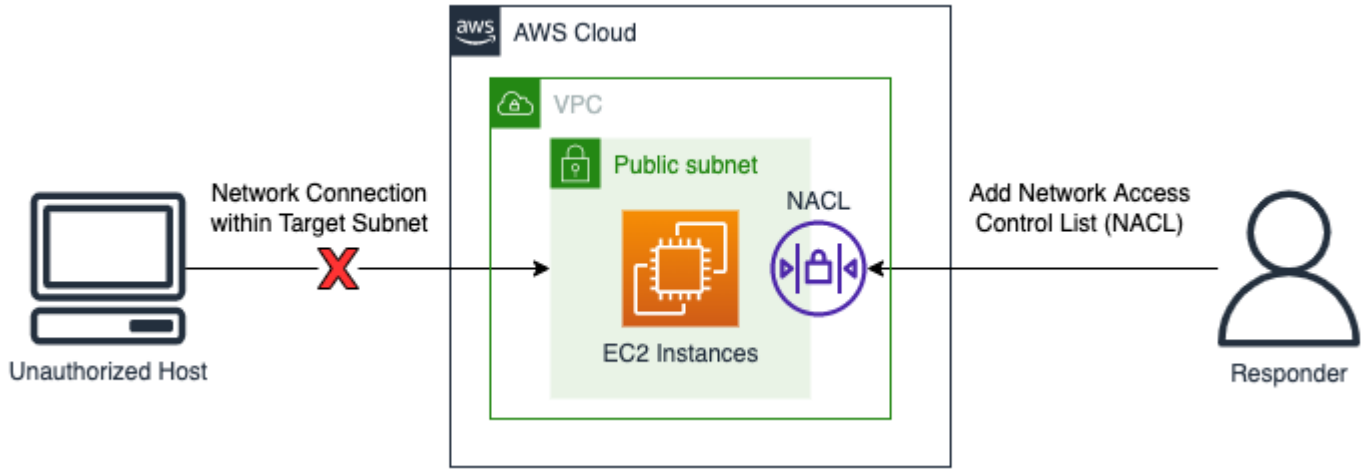
Exemplo de contenção de técnica e de acesso

Contenção de destino

A contenção de destino refere-se à aplicação de mecanismos de filtragem ou roteamento em um ambiente com o objetivo de restringir o acesso a um host ou recurso de destino. Em alguns casos, a contenção de destino também envolve uma forma de resiliência para verificar se os recursos legítimos estão replicados para garantir disponibilidade. Os recursos devem ser desvinculados dessas formas de resiliência para fins de isolamento e de contenção. Entre os exemplos de contenção de destino com o uso de serviços da AWS, destacam-se:

- ACLs da rede: as listas de controle de acesso à rede (ACLs da rede) configuradas em sub-redes que contêm recursos da AWS podem ter regras de negação adicionadas. Essas regras de negação podem ser aplicadas para restringir o acesso a um recurso da AWS específico. No entanto, aplicar uma lista de controle de acesso à rede (ACL da rede) afetará todos os recursos na sub-rede, e não apenas os recursos que estão sendo acessados sem autorização. As regras listadas em uma ACL da rede são processadas na ordem em que aparecem, de cima para baixo. Por isso, a primeira regra em uma ACL da rede existente deve ser configurada para negar o tráfego não autorizado para o recurso e a sub-rede de destino. Como alternativa, uma nova ACL da rede pode ser criada com uma única regra de negação para tráfego de entrada e saída. Em seguida, essa nova ACL da rede pode ser associada à sub-rede que contém o recurso de destino, restringindo o acesso à sub-rede com o uso da nova ACL da rede.
- Encerramento: o encerramento definitivo de um recurso pode ser eficaz para conter os efeitos do uso não autorizado. No entanto, o encerramento um recurso também impedirá o acesso legítimo para as necessidades do negócio e prejudicará a obtenção de dados forenses voláteis. Portanto, essa deve ser uma decisão intencional e deve ser avaliada em relação às políticas de segurança de uma organização.
- VPCs de isolamento: as VPCs de isolamento podem ser usadas para a contenção de recursos de forma eficaz, enquanto ainda permitem o acesso de tráfego legítimo (por exemplo, soluções de antivírus [AV] ou endpoints de detecção e de resposta [EDR] que precisam de acesso à internet ou a um console de gerenciamento externo). As VPCs de isolamento podem ser configuradas previamente antes de um evento de segurança para permitir endereços IP e portas válidos. Durante um incidente de segurança ativo, os recursos de destino podem ser movidos imediatamente para essa VPC de isolamento, com a finalidade de realizar a contenção do recurso enquanto ainda permite que o tráfego legítimo seja enviado e recebido pelo recurso de destino durante as fases subsequentes da resposta ao incidente. Um aspecto importante relacionado ao uso de uma VPC de isolamento é que os recursos, como as instâncias do EC2, precisam ser encerrados e inicializados novamente na nova VPC de isolamento antes do uso. As instâncias do EC2 existentes não podem ser movidas para outra VPC ou outra zona de disponibilidade. Para executar essa ação, siga as etapas descritas em Como mover minha instância do Amazon EC2 para outra sub-rede, zona de disponibilidade ou VPC?.
- Grupos do Auto Scaling e balanceadores de carga: os recursos do AWS anexados a grupos do Auto Scaling e balanceadores de carga devem ser desanexados e removidos do registro como parte dos procedimentos de contenção de destino. A desanexação e a remoção do registro de recursos da AWS podem ser realizadas usando o Console de gerenciamento da AWS, a AWS CLI e o AWS SDK.

Um exemplo de contenção de destino é demonstrado no diagrama apresentado a seguir, em que um analista responsável pela resposta a incidentes adiciona uma ACL da rede para uma sub-rede com a finalidade de bloquear uma solicitação de conexão de rede proveniente de um host não autorizado.



Exemplo de contenção de destino

Resumo

A contenção consiste em uma etapa do processo de resposta a incidentes e pode ser manual ou automatizada. A estratégia geral de contenção deve estar alinhada com as políticas de segurança e as necessidades de negócios de uma organização, além de verificar se os efeitos negativos são mitigados o mais eficientemente possível antes da erradicação e da recuperação.

Erradicação

A erradicação, no contexto da resposta a incidentes de segurança, corresponde à remoção de recursos suspeitos ou não autorizados em um esforço para retornar a conta a um estado seguro conhecido. A estratégia de erradicação depende de diversos fatores, que, por sua vez, dependem dos requisitos de negócios da sua organização.

O guia NIST SP 800-61 Computer Security Incident Handling Guide estabelece diversas etapas para a erradicação:

1. Identificar e mitigar todas as vulnerabilidades que foram exploradas.
2. Remover malwares, materiais impróprios e outros componentes.
3. Caso mais hosts afetados sejam descobertos (por exemplo, novas infecções por malware), repetir as etapas de detecção e de análise para identificar todos os outros hosts afetados, e, em seguida, realizar a contenção e a erradicação do incidente para esses hosts.

Para os recursos da AWS, essas etapas podem ser ainda mais aprimoradas por meio dos eventos detectados e analisados em logs disponíveis ou das ferramentas automatizadas, como o CloudWatch Logs e o Amazon GuardDuty. Esses eventos devem ser a base para determinar quais remediações devem ser realizadas para restaurar adequadamente o ambiente a um estado seguro conhecido.

A primeira etapa da erradicação consiste em determinar quais recursos foram afetados na sua conta da AWS. Isso é realizado por meio da análise das fontes de dados de log, dos recursos e das ferramentas automatizadas disponíveis.

- Identifique ações não autorizadas executadas pelas identidades do IAM na sua conta.
- Identifique acessos ou alterações não autorizadas na sua conta.
- Identifique a criação de recursos ou de usuários do IAM não autorizadas.
- Identifique sistemas ou recursos com alterações não autorizadas.

Após identificar a lista de recursos, você deve avaliar cada um dos recursos para determinar o impacto nos negócios caso o recurso seja excluído ou restaurado. Para exemplificar, se um servidor web está hospedando sua aplicação de negócios e a exclusão dele causaria tempo de inatividade, então você deve considerar recuperar o recurso de backups seguros verificados ou inicializar novamente o sistema usando uma AMI íntegra antes de excluir o servidor impactado.

Após concluir a análise de impacto nos negócios, usando os eventos da análise de logs, você deve acessar as contas e realizar as remediações apropriadas, tais como:

- Alterar ou excluir as chaves, pois essa etapa remove a capacidade do agente de continuar realizando atividades dentro da conta.
- Alterar as credenciais de usuários do IAM que possam estar não autorizadas.
- Excluir recursos não reconhecidos ou não autorizados.

> **Important**
>
> Se você tiver a necessidade de manter recursos para sua investigação, considere fazer um backup desses recursos. Por exemplo, se for necessário reter uma instância do Amazon EC2 por razões regulatórias, de conformidade ou legais, crie um snapshot do Amazon EBS antes de remover a instância.

- No caso de infecções por malware, talvez seja necessário entrar em contato com um parceiro da AWS Partner ou com outro fornecedor. A AWS não disponibiliza ferramentas nativas para análise

ou remoção de malware. No entanto, se você estiver usando o módulo Proteção contra Malware do GuardDuty para o Amazon EBS, recomendações podem estar disponíveis para as descobertas fornecidas.

Após erradicar os recursos afetados identificados, a AWS recomenda que você realize uma análise de segurança da sua conta. Isso pode ser feito usando regras do AWS Config ou soluções de código aberto, como Prowler e ScoutSuite, ou por meio de outros fornecedores. Você também deve considerar a realização de verificações de vulnerabilidade em seus recursos voltados para o público e expostos à internet para avaliar o risco residual.

A erradicação consiste em uma das etapas do processo de resposta a incidentes e pode ser manual ou automatizada, dependendo do incidente e dos recursos afetados. A estratégia geral deve estar alinhada com as políticas de segurança e com as necessidades de negócios de uma organização, e verificar se os efeitos negativos são mitigados à medida que recursos ou configurações inapropriados são removidos.

Recuperação

A recuperação é o processo de restaurar sistemas a um estado seguro conhecido, validar que os backups estão seguros ou não foram afetados pelo incidente antes da restauração, realizar testes para verificar se os sistemas estão funcionando corretamente após a restauração e abordar as vulnerabilidades associadas ao evento de segurança.

A ordem de recuperação depende dos requisitos da sua organização. Como parte do processo de recuperação, você deve realizar uma análise de impacto nos negócios para determinar, no mínimo:

- Prioridades de negócios ou de dependências
- Plano de restauração
- Autenticação e autorização

O guia NIST SP 800-61 Computer Security Incident Handling Guide estabelece diversas etapas para a recuperação de sistemas, incluindo:

- Restauração de sistemas usando backups íntegros.
  - Verifique se os backups são avaliados antes da restauração para os sistemas, a fim de garantir que a infecção não esteja presente e evitar um ressurgimento do evento de segurança.

Os backups devem ser avaliados regularmente como parte dos testes de recuperação de desastres, para verificar se o mecanismo de backup está funcionando corretamente e se a integridade dos dados atende aos objetivos de ponto de recuperação.

  - Se possível, use backups anteriores ao primeiro carimbo de data e horário do evento identificado como parte da análise da causa-raiz.
- Reconstrução de sistemas do zero, o que inclui a reimplantações a partir de uma fonte confiável usando automação, às vezes em uma nova conta da AWS.
- Substituição de arquivos comprometidos por versões íntegras.

  Você deve ter extremo cuidado ao executar essa ação. É necessário ter certeza absoluta de que o arquivo que está recuperando é reconhecidamente seguro e não foi afetado pelo incidente.
- Instalação de patches.
- Alteração de senhas.
  - Isso inclui senhas para entidades principais do IAM que podem ter sido usadas indevidamente.
  - Se possível, recomendamos usar perfis para entidades principais do IAM e para federação como parte de uma estratégia de privilégio mínimo.
- Reforço da segurança do perímetro da rede (por exemplo, com conjuntos de regras de firewall e listas de controle de acesso de roteadores de borda).

Depois que os recursos forem recuperados, é importante registrar as lições aprendidas para atualizar as políticas, os procedimentos e os guias de resposta a incidentes.

Em resumo, é imprescindível implementar um processo de recuperação que facilite o retorno às operações seguras conhecidas. A recuperação pode demorar um longo tempo e requerer uma ligação estreita com as estratégias de contenção para equilibrar o impacto nos negócios com o risco de reinfecção. Os procedimentos de recuperação devem incluir etapas para a restauração de recursos, serviços e entidades principais do IAM, e a realização de uma análise de segurança da conta para avaliar o risco residual.

Conclusão

Cada fase operacional apresenta metas, técnicas, metodologias e estratégias específicas. A Tabela 4 fornece um resumo dessas fases e de algumas das técnicas e das metodologias abordadas nesta seção.

Tabela 4: fases operacionais: metas, técnicas e metodologias

Fase	Objetivo	Técnicas e metodologias
Detecção	Identifique um possível evento de segurança.	• Controles de segurança voltados à detecção • Detecção baseada em comportamento e em regras • Detecção baseada em pessoas
Análise	Determinar se o evento de segurança constitui um incidente e avaliar o escopo do incidente.	• Validação e determinação do escopo do alerta • Logs de consulta • Inteligência de ameaças • Automação
Contenção	Minimizar e limitar o impacto do evento de segurança.	• Contenção da origem • Contenção de técnica e de acesso • Contenção de destino
Erradicação	Remova recursos ou artefatos não autorizados relacionados ao evento de segurança.	• Alteração ou exclusão de credenciais comprometidas ou não autorizadas • Exclusão de recursos não autorizados • Remoção de malware • Escaneamentos de segurança
Recuperação	Restaurar os sistemas para um estado conhecido como íntegro e monitorá-los para garantir que a ameaça não retorne.	• Restauração do sistema com base em backups • Novo desenvolvimento de sistemas desde o zero

Fase	Objetivo	Técnicas e metodologias
		• Substituição de arquivos comprometidos por versões íntegras

Atividade pós-incidente

O cenário de ameaças está mudando constantemente, e é importante ser igualmente dinâmico na capacidade de sua organização de proteger seus ambientes com eficácia. O segredo para a melhoria contínua consiste em realizar uma iteração sobre os resultados dos seus incidentes e simulações, a fim de aprimorar suas funcionalidades para detectar, responder e investigar efetivamente possíveis incidentes de segurança, reduzindo suas vulnerabilidades potenciais, o tempo de resposta e o tempo para restabelecimento seguro das operações. Os mecanismos a seguir podem ajudar você a verificar se sua organização continua preparada com os recursos e os conhecimentos mais recentes para responder com eficácia, independentemente da situação.

Estabelecimento de uma estrutura para aprendizado a partir dos incidentes

A implementação de uma estrutura e de metodologia de lições aprendidas não apenas auxilia na melhoria das funcionalidades de resposta a incidentes, como também contribui para a prevenção da recorrência dos incidentes. Ao extrair lições de cada incidente, é possível evitar a reincidência dos mesmos erros, exposições ou configurações inadequadas, aprimorando a postura de segurança e minimizando o tempo dedicado na resolução de situações que poderiam ser prevenidas.

É importante implementar um framework de lições aprendidas que estabeleça e atinja, em alto nível, os seguintes pontos:

- Quando um processo de lições aprendidas é realizado?
- O que está envolvido no processo de lições aprendidas?
- Como um processo de lições aprendidas é realizado?
- Quem está envolvido no processo e como?
- Como as áreas de melhoria serão identificadas?
- De que maneira você garantirá que as melhorias sejam efetivamente monitoradas e implementadas?

Além dos resultados de alto nível listados, é fundamental assegurar que se formulem as questões adequadas para obter o maior valor possível (ou seja, informações que conduzam a melhorias concretas) a partir do processo. Considere estas perguntas para ajudar você a começar a promover discussões sobre lições aprendidas:

- Como foi o incidente?
- Quando o incidente foi identificado pela primeira vez?
- Como ele foi identificado?
- Que sistemas alertaram sobre a atividade?
- Que sistemas, serviços e dados estiveram envolvidos?
- O que ocorreu especificamente?
- O que funcionou bem?
- O que não funcionou bem?
- Que processos ou procedimentos falharam ou não tiveram a escala ajustada para responder ao incidente?
- O que pode ser melhorado nas seguintes áreas:
  - Pessoas
    - As pessoas que precisavam ser contatadas estavam realmente disponíveis e a lista de contatos estava atualizada?
    - As pessoas estavam perdendo treinamentos ou não tinham os recursos necessários para responder e investigar o incidente de forma eficaz?
    - Os recursos apropriados estavam prontos e disponíveis?
  - Processo
    - Os processos e procedimentos foram seguidos?
    - Os processos e procedimentos foram documentados e estavam disponíveis para esse (tipo de) incidente?
    - Havia processos e procedimentos necessários faltando?
    - Os respondedores conseguiram obter acesso oportuno às informações necessárias para responder ao problema?
  - Tecnologia
    - Os sistemas de alerta existentes identificaram e alertaram efetivamente sobre a atividade?
    - Os alertas existentes precisam ser aprimorados ou novos alertas precisam ser criados para esse (tipo de) incidente?

    - O conjunto de ferramentas existente permitiu a condução eficiente da investigação (pesquisa e análise) do incidente?
- O que pode ser feito para ajudar a identificar esse (tipo de) incidente mais cedo?
- O que pode ser feito para ajudar a evitar que esse (tipo de) incidente ocorra novamente?
- Quem é o proprietário do plano de melhoria e como você testará se ele foi implementado?
- Qual o prazo previsto para implementar e testar os controles, processos ou monitoramentos preventivos adicionais?

Esta lista não é exaustiva. No entanto, ela tem o propósito de servir como ponto de partida para a identificação das necessidades da organização e dos negócios, bem como para a análise dessas necessidades a fim de aprender com os incidentes da forma mais eficaz e promover a melhoria contínua da sua postura de segurança. O mais importante é começar incorporando as lições aprendidas como parte padrão do processo de resposta a incidentes, da documentação e das expectativas das partes interessadas.

Estabelecimento de métricas para o sucesso

As métricas são essenciais para mensurar, avaliar e melhorar de forma eficaz suas funcionalidades de resposta a incidentes. Na ausência de métricas, não existe uma referência contra a qual se possa avaliar de forma precisa a performance da organização, identificando se está adequado ou deficitário. Existem algumas métricas comuns à resposta a incidentes que servem como um bom ponto de partida para organizações que desejam estabelecer expectativas e referências para alcançar a excelência operacional.

Tempo médio para detecção

O tempo médio para detecção consiste no intervalo de tempo médio necessário para identificar um possível incidente de segurança. Mais precisamente, trata-se do tempo decorrido desde a ocorrência do primeiro indicador de comprometimento até a identificação ou geração do alerta inicial.

É possível usar essa métrica para acompanhar a eficácia dos seus sistemas de detecção e de geração de alertas. Mecanismos eficazes de detecção e de geração de alertas são fundamentais para garantir que possíveis incidentes de segurança não permaneçam ativos em seus ambientes.

Quanto maior o tempo médio para detecção, maior a necessidade de desenvolver alertas e mecanismos adicionais ou mais eficazes para identificar e detectar possíveis incidentes de segurança. Por outro lado, um tempo médio para detecção reduzido indica a maior eficácia dos seus mecanismos de detecção e de geração de alertas.

Tempo médio para reconhecimento

O tempo médio para reconhecimento consiste no intervalo de tempo médio necessário para reconhecer e definir a prioridade de um possível incidente de segurança. Mais precisamente, trata-se do tempo decorrido desde a geração do alerta até a identificação e a definição da prioridade do alerta por um integrante do SOC ou da equipe de resposta a incidentes para seu devido tratamento.

É possível usar essa métrica para acompanhar a eficiência da sua equipe no tratamento e na priorização dos alertas. Caso a equipe não consiga identificar e priorizar os alertas de forma eficaz, as respostas terão atraso e baixa efetividade.

Quanto maior o tempo médio para reconhecimento, maior a necessidade de verificar se sua equipe está adequadamente equipada e treinada para reconhecer e priorizar rapidamente um possível incidente de segurança para resposta. Em contrapartida, quanto menor o tempo médio para reconhecimento, melhor é a capacidade da equipe em responder aos alertas de segurança, demonstrando que está efetivamente preparada e apta a priorizá-los corretamente.

Tempo médio para resposta

O tempo médio para resposta consiste no intervalo de tempo médio necessário para dar início às ações de resposta inicial a um possível incidente de segurança. Mais precisamente, trata-se do tempo decorrido entre o alerta inicial ou a identificação de um possível incidente de segurança e a realização das primeiras medidas tomadas como resposta. Trata-se de uma métrica semelhante ao tempo médio para reconhecimento, porém voltada à avaliação de ações de resposta concretas (por exemplo, a coleta de dados do sistema e a contenção do sistema), em contraste com o simples reconhecimento ou confirmação da situação.

É possível usar essa métrica para avaliar o nível de prontidão da sua equipe para responder a incidentes de segurança. Como mencionado anteriormente, a preparação é fundamental para uma resposta eficaz. Consulte a seção the section called “Preparação” deste documento.

Quanto maior o tempo médio para resposta, maior a necessidade de verificar se sua equipe está devidamente treinada para fornecer respostas e se os processos de resposta estão documentados e sendo aplicados de forma eficaz. Por outro lado, quanto menor o tempo médio para resposta, melhor a capacidade da equipe em identificar a resposta adequada aos alertas detectados e executar as ações necessárias para iniciar o retorno às operações seguras.

Tempo médio para contenção

O tempo médio para contenção consiste no intervalo de tempo médio necessário para conter um possível incidente de segurança. Mais precisamente, trata-se do tempo decorrido entre o alerta inicial

ou a descoberta de um possível incidente de segurança e a conclusão das ações de resposta que efetivamente impedem o invasor ou os sistemas comprometidos de causar mais danos.

É possível usar essa métrica para avaliar a capacidade da sua equipe em mitigar ou em realizar a contenção de possíveis incidentes de segurança. A incapacidade de realizar uma contenção rápida e eficaz desses possíveis incidentes de segurança aumenta o impacto, o escopo e a exposição a possíveis comprometimentos adicionais.

Quanto maior o tempo médio para contenção, maior a necessidade de desenvolver conhecimento e funcionalidades para mitigar e realizar a contenção, de forma rápida e eficaz, dos incidentes de segurança enfrentados. Por outro lado, quanto menor o tempo médio para contenção, melhor é a capacidade da equipe em compreender e aplicar as medidas necessárias para mitigar e realizar a contenção das ameaças identificadas, reduzindo o impacto, o escopo e os riscos para o negócio.

Tempo médio para recuperação

O tempo médio para recuperação consiste no intervalo de tempo médio necessário para retomar completamente as operações seguras após um possível incidente de segurança. Mais precisamente, trata-se do tempo decorrido entre o alerta inicial ou a descoberta de um possível incidente de segurança e o momento em que a operação da empresa retorna ao normal e em segurança, sem impactos residuais do incidente.

É possível usar essa métrica para monitorar a eficácia da sua equipe na restauração de sistemas, contas e ambientes às condições de operação segura após um incidente de segurança. A incapacidade de restabelecer as operações seguras de forma rápida ou eficaz pode não apenas impactar a segurança, mas também aumentar os impactos e os custos para o negócio e suas operações.

Quanto maior o tempo médio para recuperação, maior a necessidade de preparar as equipes e os ambientes com os mecanismos apropriados (por exemplo, processos de failover e pipelines de CI/CD para reimplantação segura de sistemas íntegros) a fim de minimizar o impacto dos incidentes de segurança sobre as operações e sobre o negócio. Por outro lado, quanto menor o tempo médio para recuperação, mais eficazes são suas equipes em minimizar o impacto dos incidentes de segurança nas operações e no negócio.

Tempo de permanência do invasor

O tempo de permanência do invasor consiste no tempo médio durante o qual um usuário não autorizado mantém acesso a um sistema ou a um ambiente. Esse conceito é semelhante ao tempo

médio para contenção, com a diferença de que o intervalo de tempo começa no momento em que o invasor obtém acesso inicial ao sistema ou ao ambiente, o que pode ocorrer antes do alerta ou da descoberta inicial.

É possível usar essa métrica para monitorar a eficácia conjunta de seus sistemas e mecanismos na redução do tempo, do acesso e das oportunidades que um invasor ou que uma ameaça tem para comprometer seu ambiente. A redução do tempo de permanência do invasor deve ser uma prioridade máxima para suas equipes e para a empresa.

Quanto maior o tempo de permanência do invasor, maior será a necessidade de identificar quais etapas do processo de resposta a incidentes requerem melhorias, a fim de garantir a capacidade das suas equipes de minimizar o impacto e o escopo de ameaças ou de ataques em seus ambientes. Por outro lado, quanto menor o tempo de permanência do invasor, mais eficazes são suas equipes na minimização do tempo e das oportunidades que uma ameaça ou que um invasor tem dentro dos seus ambientes, reduzindo, assim, o risco e o impacto às suas operações e ao seu negócio.

Resumo das métricas

O estabelecimento e o monitoramento das métricas de resposta a incidentes permite medir, avaliar e aprimorar de forma eficaz as funcionalidades de resposta a incidentes da organização. Para alcançar isso, diversas métricas comuns de resposta a incidentes foram destacadas nesta seção. A Tabela 5 apresenta um resumo dessas métricas.

Tabela 5: métricas de resposta a incidentes

Métrica	Descrição
Tempo médio para detecção	Tempo médio necessário para a detecção de um possível incidente de segurança
Tempo médio para reconhecimento	Tempo médio necessário para o reconhecimento e para a priorização de um possível incidente de segurança
Tempo médio para resposta	Tempo médio necessário para o início da resposta a um possível incidente de segurança
Tempo médio para contenção	Tempo médio necessário para a contenção de um possível incidente de segurança

Métrica	Descrição
Tempo médio para recuperação	Tempo médio necessário para o restabele cimento total das operações seguras após um possível incidente de segurança
Tempo de permanência do invasor	Tempo médio durante o qual um invasor mantém acesso a um sistema ou a um ambiente

Uso de indicadores de comprometimento (IOCs)

Um indicador de comprometimento (IOC, na sigla em inglês) refere-se a um artefato detectado em uma rede, em um sistema ou em um ambiente que possibilita, com elevado nível de confiança, a identificação de atividades maliciosas ou de um incidente de segurança. Os IOCs podem se manifestar em várias formas, incluindo endereços IP, domínios, artefatos em nível de rede como sinalizadores TCP ou cargas úteis, artefatos em nível de sistema ou host, como executáveis, nomes de arquivos e hashes, entradas em arquivos de log, entradas no registro, entre outros. Além disso, os IOCs podem ser uma combinação de itens ou de atividades, como a existência de arquivos ou artefatos específicos em um sistema (por exemplo, um determinado arquivo ou conjunto de arquivos e itens no registro), ações executadas em uma sequência específica (por exemplo, um login em um sistema usando um IP determinado, seguido por comandos anômalos específicos) ou atividades na rede (por exemplo, tráfego anômalo de entrada ou de saída para ou a partir de determinados domínios), que podem indicar uma ameaça, um ataque ou uma metodologia de invasor específica.

À medida que você aprimora iterativamente seu programa de resposta a incidentes, deve implementar uma estrutura para coletar, gerenciar e usar os IOCs como um mecanismo para desenvolver e aprimorar continuamente as detecções e as gerações de alertas, além de aumentar a rapidez e a eficácia das investigações. É possível começar ao incorporar a coleta e o gerenciamento de IOCs às fases de análise e de investigação dos seus processos de resposta a incidentes. Ao identificar, coletar e armazenar proativamente os IOCs como um procedimento padrão em seus processos, é possível desenvolver um repositório de dados integrado a um programa de inteligência de ameaças mais abrangente. Este repositório, por sua vez, pode ser empregado para aprimorar detecções e alertas existentes, desenvolver detecções e alertas adicionais, identificar o momento e o local da ocorrência prévia de um artefato, elaborar e consultar documentação sobre investigações anteriores envolvendo IOCs correspondentes, entre outras aplicações.

Instrução e treinamento contínuos

A instrução e o treinamento são iniciativas contínuas e em constante evolução que devem ser visados e mantidos de forma deliberada. Existe uma variedade de mecanismos para garantir que sua equipe mantenha a conscientização, o conhecimento e as funcionalidades compatíveis com o estado em evolução da tecnologia, bem como do cenário de ameaças.

Um dos mecanismos consiste em empregar a educação continuada como um componente regular das metas e das atividades operacionais das equipes. Conforme mencionado na seção Preparação, sua equipe de resposta a incidentes e as partes interessadas devem ser treinadas de forma eficaz para detectar, responder e investigar incidentes dentro do ambiente da AWS. Entretanto, a educação não é um esforço pontual. A educação deve ser continuamente visada para garantir que sua equipe mantenha a conscientização sobre os avanços tecnológicos, as atualizações e as melhorias mais recentes que possam ser aproveitados para aumentar a eficácia e a eficiência da resposta, bem como sobre acréscimos ou atualizações de dados que possam ser usados para aprimorar a investigação e a análise.

Outro mecanismo consiste em garantir que simulações sejam realizadas regularmente (por exemplo, trimestralmente) e que estejam focadas em resultados específicos para o negócio. Consulte a seção the section called “Execução de simulações de forma periódica” deste documento.

Apesar de os exercícios de simulação iniciais representarem uma maneira eficaz de gerar uma linha de base inicial para aprimoramentos, a realização constante de testes é essencial para a manutenção das melhorias contínuas e para assegurar uma representação atualizada e fiel do estado operacional vigente. Realizar testes baseados nas situações de segurança mais atuais e críticas, além das funcionalidades mais relevantes ou recentes para resposta, e integrar as lições aprendidas na educação, nas operações e nos processos e procedimentos, garantirá a capacidade de aprimorar continuamente os processos de resposta e o programa em sua totalidade.

Conclusão

À medida que você avança em sua jornada para a nuvem, é importante considerar os conceitos fundamentais de resposta a incidentes de segurança para o seu ambiente da AWS. É possível combinar os controles disponíveis, as funcionalidades da nuvem e as opções de remediação para ajudar a aprimorar a segurança do seu ambiente na nuvem. Você também pode começar em pequena escala e realizar iterações conforme incorpora funcionalidades de automação que aprimoram a rapidez da resposta, garantindo melhor preparo diante da ocorrência de eventos de segurança.

Colaboradores

Entre as pessoas que contribuíram para este documento, tanto atualmente quanto no passado, estão:

- Anna McAbee, arquiteta sênior de soluções de segurança, Amazon Web Services
- Freddy Kasprzykowski, consultor sênior de segurança da Amazon Web Services
- Jason Hurst, engenheiro sênior de segurança da Amazon Web Service
- Jonathon Poling, consultor principal de segurança da Amazon Web Services
- Josh Du Lac, gerente sênior de arquitetura de soluções de segurança da Amazon Web Services
- Paco Hope, engenheiro principal de segurança da Amazon Web Services
- Ryan Tick, engenheiro sênior de segurança da Amazon Web Services
- Steve de Vera, engenheiro sênior de segurança da Amazon Web Services

Apêndice A: definições das funcionalidades da nuvem

A AWS disponibiliza mais de 200 serviços em nuvem e milhares de recursos. Diversos desses serviços fornecem funcionalidades nativas de detecção, prevenção e resposta, e outros podem ser empregados na arquitetura de soluções de segurança personalizadas. Esta seção inclui um subconjunto de serviços que têm maior relevância para atividades de resposta a incidentes em ambientes de nuvem.

Tópicos

Registro em log e eventos

AWS CloudTrail: serviço da AWS CloudTrail que possibilita a governança, a conformidade, a auditoria operacional e a auditoria de riscos em contas da AWS. Com o CloudTrail, é possível registrar em log, monitorar continuamente e reter a atividade da conta relacionada a ações

executadas nos serviços da AWS. O CloudTrail fornece um histórico de eventos da atividade da sua conta da AWS, incluindo ações realizadas por meio do Console de gerenciamento da AWS, dos AWS SDKs, das ferramentas de linha de comando e de outros serviços da AWS. Esse histórico de eventos facilita a análise de segurança, o rastreamento de alterações em recursos e a solução de problemas. O CloudTrail registra dois tipos diferentes de ações da API da AWS:

- Os eventos de gerenciamento do CloudTrail (também conhecidos como operações do ambiente de gerenciamento) mostram as operações de gerenciamento realizadas em recursos da sua conta da AWS. Isso inclui ações como a criação de um bucket do Amazon S3 e a configuração de registros de log.
- Os eventos de dados do CloudTrail (também conhecidos como operações do plano de dados) mostram as operações realizadas sobre ou dentro de um recurso na sua conta da AWS. Essas operações geralmente são atividades de alto volume. Isso inclui ações como a atividade de API em nível de objeto no Amazon S3 (por exemplo, as operações de API `GetObject`, `DeleteObject` e `PutObject`) e a atividade de invocação de função do Lambda.

AWS Config: serviço da AWS Config que possibilita aos clientes realizar avaliações, auditorias e monitoramento das configurações dos recursos em sua conta da AWS. O AWS Config monitora e registra continuamente as configurações dos seus recursos da AWS, permitindo automatizar a avaliação das configurações registradas em relação às configurações desejadas. Com o AWS Config, os clientes podem analisar alterações nas configurações e nas relações entre os recursos da AWS, de forma manual ou automática, acessar um histórico detalhado das configurações dos recursos e determinar a conformidade geral em relação às configurações especificadas nas diretrizes do cliente. Isso possibilita a simplificação da auditoria de conformidade, da análise de segurança, do gerenciamento de alterações e da solução de problemas operacionais.

Amazon EventBridge: o Amazon EventBridge fornece uma transmissão quase em tempo real dos eventos do sistema que descrevem as alterações nos recursos da AWS ou quando chamadas de API são registradas pelo AWS CloudTrail. Com regras simples que você pode configurar rapidamente, é possível corresponder eventos e roteá-los para um ou mais streams ou funções de destino. O EventBridge se torna ciente das alterações operacionais no momento em que elas ocorrem. O EventBridge é capaz de responder a essas alterações operacionais e executar ações corretivas quando necessário, por meio do envio de mensagens para interagir com o ambiente, ativação de funções, execução de modificações e captura de informações de estado. Alguns serviços de segurança, como o Amazon GuardDuty, geram suas saídas na forma de eventos do EventBridge. Diversos serviços de segurança também disponibilizam a opção de encaminhar suas saídas para o Amazon S3.

Logs de acesso do Amazon S3: se houver informações sensíveis armazenadas em um bucket do Amazon S3, os clientes podem habilitar os logs de acesso do Amazon S3 para acompanhar todas as operações de upload, download e alteração desses dados. Este log é distinto e adicional aos logs do CloudTrail, que registram alterações no próprio bucket, como modificações nas políticas de acesso e nas políticas de ciclo de vida. Vale destacar que os registros de logs de acesso são fornecidos na base do melhor esforço. A maioria das solicitações para um bucket configurado corretamente para registro em log tem como resultado um registro do log entregue. A integralidade e a pontualidade do registro em log do servidor não são garantidas.

Amazon CloudWatch Logs: os clientes podem usar o Amazon CloudWatch Logs para monitorar, armazenar e acessar arquivos de log provenientes de sistemas operacionais, aplicações e outras fontes em execução em instâncias do Amazon EC2 com um agente do CloudWatch Logs instalado. O CloudWatch Logs pode servir como destino para logs do AWS CloudTrail, consultas ao DNS do Route 53, logs de fluxo da VPC, funções do Lambda e outros. Posteriormente, os clientes podem recuperar os dados de log associados diretamente do CloudWatch Logs.

Logs de fluxo da Amazon VPC: os logs de fluxo da VPC habilitam os clientes a capturar informações relativas ao tráfego IP direcionado para e proveniente das interfaces de rede nas VPCs. Após a habilitação dos logs de fluxo, eles podem ser transmitidos para o Amazon CloudWatch Logs e para o Amazon S3. Os logs de fluxo da VPC auxiliam os clientes em diversas tarefas, como solucionar o motivo pelo qual um tráfego específico não está alcançando uma instância, identificar regras excessivamente restritivas em um grupo de segurança e utilizá-lo como ferramenta de segurança para monitorar o tráfego destinado às instâncias do EC2. Use a versão mais recente dos logs de fluxo da VPC para obter os campos mais completos e robustos.

Logs do AWS WAF: o AWS WAF fornece suporte ao registro em log completo de todas as solicitações web inspecionadas pelo serviço. Os clientes podem armazenar esses registros em log no Amazon S3 para atender a requisitos de conformidade e de auditoria, além de auxiliar na depuração e nas análises forenses. Esses logs ajudam os clientes a determinar a causa-raiz das regras acionadas e das solicitações web bloqueadas. É possível integrar esses logs a ferramentas de SIEM e análise de logs de fornecedores externos.

Logs de consulta do Route 53 Resolver: os logs de consulta do Route 53 Resolver permitem registrar todas as consultas ao DNS realizadas por recursos dentro da Amazon Virtual Private Cloud (Amazon VPC). Independentemente de ser uma instância do Amazon EC2, uma função do AWS Lambda ou um contêiner, se estiver dentro da sua Amazon VPC e emitir uma consulta ao DNS, esse recurso realizará o registro em log, permitindo que você analise e compreenda de forma mais detalhada a operação das suas aplicações.

Outros logs da AWS: a AWS lança continuamente novos recursos e funcionalidades para clientes, incluindo funcionalidades aprimoradas de registro em log e de monitoramento. Para obter mais informações sobre os recursos disponíveis para cada serviço da AWS, consulte nossa documentação pública.

Visibilidade e geração de alertas

AWS Security Incident Response: o AWS Security Incident Response é um serviço abrangente que ajuda as organizações a lidar com eventos de segurança ao longo de todo o ciclo de vida, combinando recursos automatizados com suporte humano especializado. O serviço utiliza recursos automatizados de monitoramento e investigação para liberar recursos organizacionais, mantendo uma supervisão de segurança vigilante. Quando ocorrem eventos de segurança, ele facilita a comunicação e a coordenação aceleradas entre as partes interessadas para tempos de resposta rápidos. O serviço é compatível com vários casos de uso, incluindo preparação e simulação de eventos de segurança, resposta a incidentes ativos e relatórios e análises pós-incidente simplificados, garantindo que as organizações estejam bem equipadas para lidar com os desafios de segurança em todas as etapas.

AWS Security Hub CSPM: o AWS Security Hub CSPM fornece aos clientes uma visão abrangente dos alertas de segurança de alta prioridade e dos status de conformidade em diversas contas da AWS. O CSPM do Security Hub agrega, organiza e prioriza as descobertas dos serviços da AWS, como o Amazon GuardDuty, o Amazon Inspector, o Amazon Macie e as soluções da AWS Partner. As descobertas são apresentadas de forma visual em painéis integrados, contendo gráficos e tabelas que permitem ações diretas. É possível realizar monitoramento contínuo do seu ambiente por meio de verificações automáticas de conformidade fundamentadas nas práticas recomendadas da AWS e nos padrões do setor seguidos pela sua organização.

Amazon GuardDuty: o Amazon GuardDuty é um serviço gerenciado de detecção de ameaças que monitora continuamente comportamentos maliciosos ou não autorizados para auxiliar os clientes na proteção de contas e de workloads da AWS. O serviço monitora atividades como chamadas de API incomuns ou implantações potencialmente não autorizadas, que podem indicar comprometimento da conta ou de recursos, como instâncias do Amazon EC2 e buckets do Amazon S3, ou atividades de reconhecimento por agentes mal-intencionados.

O GuardDuty identifica supostos agentes mal-intencionados por meio de feeds integrados de inteligência de ameaças usando machine learning para detectar anomalias na atividade da conta e da workload. Quando uma ameaça potencial é detectada, o serviço envia um alerta de segurança detalhado para o console do GuardDuty e para o CloudWatch Events. Isso torna os alertas

acionáveis e fáceis de integrar aos sistemas de gerenciamento de eventos e de fluxo de trabalho existentes.

Além disso, o GuardDuty disponibiliza dois complementos para o monitoramento de ameaças com serviços específicos: o Amazon GuardDuty para proteção do Amazon S3 e o Amazon GuardDuty para proteção do Amazon EKS. A proteção do Amazon S3 possibilita que o GuardDuty monitore operações de API em nível de objeto para identificar possíveis riscos de segurança para dados em buckets do Amazon S3. A proteção do Kubernetes, por sua vez, possibilita que o GuardDuty detecte atividades suspeitas e possíveis comprometimentos de clusters do Kubernetes no Amazon EKS.

Amazon Macie: o Amazon Macie é um serviço de segurança com tecnologia de IA que auxilia na prevenção de perda de dados ao descobrir, classificar e proteger automaticamente dados sensíveis armazenados na AWS. O Macie usa machine learning (ML) para identificar dados sensíveis, como informações de identificação pessoal (PII) ou de propriedade intelectual, atribuir um valor de negócios, e fornecer visibilidade sobre o local em que esses dados estão armazenados e como são utilizados em sua organização. O Amazon Macie realiza monitoramento constante das atividades de acesso a dados para identificar anomalias, emitindo alertas quando detecta risco de acessos não autorizados ou vazamentos acidentais de dados.

Regras do AWS Config: uma regra do AWS Config representa as configurações de sua preferência para um recurso e é avaliada com base nas alterações de configuração desses recursos, conforme registradas pelo AWS Config. É possível visualizar os resultados da avaliação de uma regra em relação à configuração de um recurso em um painel. Com as regras do AWS Config, você pode avaliar o status geral de conformidade e de riscos sob a perspectiva de configuração, acompanhar as tendências de conformidade ao longo do tempo e identificar qual alteração de configuração fez com que um recurso deixasse de estar em conformidade com uma regra.

AWS Trusted Advisor: o AWS Trusted Advisor é um recurso on-line que auxilia na redução de custos, no aumento de performance e na melhoria da segurança por meio da otimização do seu ambiente da AWS. O Trusted Advisor fornece orientações em tempo real para auxiliar você no provisionamento de recursos com base nas práticas recomendadas da AWS. O conjunto completo de verificações do Trusted Advisor, incluindo a integração com CloudWatch Events, está disponível para clientes dos planos de suporte Business e Enterprise.

Amazon CloudWatch: o Amazon CloudWatch é um serviço destinado ao monitoramento de recursos da Nuvem AWS, bem como das aplicações executadas na AWS. O CloudWatch pode ser usado para a coleta e o acompanhamento de métricas, monitoramento de arquivos de log, definição de alarmes e resposta automática a alterações nos recursos da AWS. O CloudWatch pode monitorar recursos da AWS, como instâncias do Amazon EC2, tabelas do Amazon DynamoDB e instâncias de

banco de dados do Amazon RDS, bem como métricas personalizadas geradas por suas aplicações e serviços, além de quaisquer arquivos de log gerados por suas aplicações. É possível usar o Amazon CloudWatch para obter visibilidade em todo o sistema quanto à utilização de recursos, performance das aplicações e integridade operacional. Com essas informações, você pode tomar as medidas necessárias para garantir o funcionamento estável da aplicação.

Amazon Inspector: o Amazon Inspector é um serviço automatizado de avaliação de segurança que auxilia na melhoria da segurança e da conformidade de aplicações implantadas na AWS. O Amazon Inspector avalia os aplicativos automaticamente para detectar vulnerabilidades ou desvios das melhores práticas. Depois de executar uma avaliação, o Amazon Inspector fornece uma lista detalhada das descobertas de segurança, priorizadas de acordo com seu nível de severidade. Essas descobertas podem ser analisadas diretamente ou como parte de relatórios de avaliação detalhados, disponíveis por meio do console do Amazon Inspector ou por meio da API.

Amazon Detective: o Amazon Detective é um serviço de segurança que coleta automaticamente dados de log dos seus recursos da AWS e usa machine learning, análise estatística e teoria dos grafos para desenvolver um conjunto de dados correlacionados, possibilitando a realização de investigações de segurança de forma mais rápida e eficiente. O Detective pode analisar trilhões de eventos provenientes de diversas fontes de dados, como dos logs de fluxo da VPC, do CloudTrail e do GuardDuty, e criar automaticamente uma visão unificada e interativa dos seus recursos, usuários e das interações entre eles ao longo do tempo. Com essa visão unificada, é possível visualizar todos os detalhes e o contexto em um único local para identificar as causas subjacentes das descobertas, aprofundar-se nas atividades históricas relevantes e determinar rapidamente a causa-raiz.

Automação

AWS Lambda – AWS Lambda o é um serviço de computação com tecnologia 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 ampliar as funcionalidades de outros serviços da AWS por meio de lógica personalizada, ou para criar seus próprios serviços backend que funcionem com a escala, a performance e a segurança proporcionadas pela AWS. O Lambda executa seu código em uma infraestrutura de computação de alta disponibilidade e realiza a administração dos recursos computacionais para você. Isso inclui a manutenção do servidor e do sistema operacional, o provisionamento de capacidade e a escalabilidade automática, a implantação de código e de atualizações de segurança, bem como o monitoramento e o registro em log do código. A única responsabilidade do usuário é fornecer o código.

AWS Step Functions – AWS Step Functions o facilita a coordenação dos componentes de aplicações distribuídas e microsserviços por meio de fluxos de trabalho visuais. O Step Functions disponibiliza

um console gráfico para que você organize e visualize os componentes da sua aplicação como uma sequência de etapas. Isso simplifica a criação e a execução de aplicações em várias etapas. O Step Functions inicia e monitora automaticamente cada etapa, além de realizar tentativas em caso de erros, garantindo que sua aplicação seja executada na ordem correta e conforme o esperado.

O Step Functions registra o estado de cada etapa, de modo que, quando algo dá errado, é possível diagnosticar e depurar problemas rapidamente. Você pode modificar e adicionar etapas sem a necessidade de escrever código, permitindo evoluir sua aplicação e inovar com maior rapidez. O AWS Step Functions faz parte do AWS Serverless e facilita a orquestração de funções do AWS Lambda para aplicações com tecnologia sem servidor. Além disso, o Step Functions pode ser usado para a orquestração de microsserviços utilizando recursos computacionais como o Amazon EC2 e o Amazon ECS.

AWS Systems Manager: o AWS Systems Manager proporciona visibilidade e controle da sua infraestrutura na AWS. O Systems Manager disponibiliza uma interface do usuário unificada que permite a visualização de dados operacionais de diversos serviços da AWS, além de possibilitar a automação de tarefas operacionais em seus recursos da AWS. Com o Systems Manager, é possível agrupar recursos por aplicação, visualizar dados operacionais para monitoramento e solução de problemas, e executar ações sobre esses grupos de recursos. O Systems Manager pode manter suas instâncias no estado definido, realizar alterações sob demanda, como a atualização de aplicações ou a execução de scripts shell, além de executar outras tarefas de automação e aplicação de patches.

Armazenamento seguro

Amazon Simple Storage Service: o Amazon S3 é um serviço de armazenamento de objetos projetado para armazenar e recuperar qualquer volume de dados de qualquer lugar. O serviço foi desenvolvido para fornecer durabilidade de 99,999999999% e armazena dados para milhões de aplicações usadas por empresas líderes de mercado em diversos setores. O Amazon S3 fornece segurança abrangente e foi concebido para auxiliar no atendimento a requisitos regulatórios.
O serviço proporciona aos clientes flexibilidade nos métodos usados para gerenciar dados visando otimização de custos, controle de acesso e conformidade. O Amazon S3 disponibiliza a funcionalidade de consulta direta, que possibilita a execução de analytics avançadas diretamente em seus dados em repouso armazenados no Amazon S3. O Amazon S3 é um serviço de armazenamento em nuvem com suporte abrangente e ampla integração junto a uma das maiores comunidades de soluções de entidades externas, parceiros integradores de sistemas e outros serviços da AWS.

Amazon Glacier: o Amazon Glacier é um serviço de armazenamento em nuvem seguro, durável e de custo extremamente reduzido, voltado para arquivamento de dados e para o backup de longo prazo. O serviço foi projetado para fornecer 99,999999999% de durabilidade, além de proporcionar segurança abrangente e auxiliar no atendimento a requisitos regulatórios. O Amazon Glacier disponibiliza a funcionalidade de consulta direta, que possibilita a execução de analytics avançadas diretamente em seus dados em repouso armazenados. Para manter os custos baixos e atender diferentes necessidades de recuperação, o Amazon Glacier disponibiliza três opções de acesso aos arquivos, com tempos que variam de alguns minutos a várias horas.

Funcionalidades de segurança futuras e personalizadas

Os serviços e recursos mencionados não representam uma lista exaustiva. A AWS está continuamente adicionando novas funcionalidades. Para obter mais informações, recomendamos que você consulte as páginas Quais as novidades da AWS e Segurança na Nuvem AWS. Além dos serviços de segurança nativos oferecidos pela AWS, você pode se interessar em desenvolver suas próprias funcionalidades com base nos serviços da AWS.

Embora recomendemos habilitar um conjunto básico de serviços de segurança em suas contas, como AWS CloudTrail, Amazon GuardDuty e Amazon Macie, você pode desejar expandir essas funcionalidades para obter maior valor dos seus ativos de logs. Existem diversas ferramentas de parceiros disponíveis, como as listadas no nosso programa APN Security Competency. Além disso, você pode desejar desenvolver suas próprias consultas para pesquisar seus logs. Graças à ampla gama de serviços gerenciados disponíveis na AWS, essa tarefa tornou-se mais simples do que nunca. Existem diversos outros serviços da AWS que podem auxiliar em investigações, mas que estão fora do escopo deste documento, como Amazon Athena, Amazon OpenSearch Service, Amazon Quick, Amazon Machine Learning e Amazon EMR.

Apêndice B: recursos de resposta a incidentes da AWS

A AWS publica recursos para auxiliar os clientes no desenvolvimento de funcionalidades de resposta a incidentes. A maioria dos exemplos de código e dos procedimentos pode ser encontrada no repositório público externo da AWS no GitHub. A seguir, são apresentados alguns recursos que fornecem exemplos de como realizar a resposta a incidentes.

Recursos relacionados ao plano de ação

- Framework for Incident Response Playbooks: uma estrutura de exemplo destinado a auxiliar os clientes na criação, no desenvolvimento e na integração de planos de ação de segurança em preparação para cenários potenciais de ataque ao usar os serviços da AWS.

- Incident Response Playbook Samples: planos de ação que abrangem cenários comuns enfrentados por clientes da AWS.
- A AWS anuncia o lançamento de cinco novas workshops disponíveis ao público.

Recursos relacionados à análise forense

- Automated Incident Response and Forensics Framework: esta estrutura e solução fornece um processo forense digital e padronizado, que consiste nas seguintes fases: contenção, aquisição, exame e análise. A estrutura usa funções da AWS para acionar o processo de resposta a incidentes de forma automatizada e repetível. Além disso, a estrutura promove a segmentação de contas para execução das etapas automatizadas, armazenamento de artefatos e criação de ambientes forenses.
- Automated Forensics Orchestrator for Amazon EC2: este guia de implementação disponibiliza uma solução de autoatendimento para capturar e examinar dados de instâncias do EC2 e de volumes conectados, com o objetivo de realizar análises forenses em caso de detecção de um possível incidente de segurança. A implantação da solução é realizada por meio de um modelo do AWS CloudFormation.
- How to automate forensic disk collection in AWS: esta publicação do blog da AWS detalha como configurar um fluxo de trabalho de automação para capturar evidências em disco, com o objetivo de realizar análises que permitam determinar o escopo e o impacto de possíveis incidentes de segurança. A solução inclui um modelo do AWS CloudFormation para implantação.

Notices

Os clientes são responsáveis por fazer a própria avaliação independente das informações contidas neste documento. Este documento: (a) é apenas para fins informativos, (b) representa as ofertas e práticas de produtos atuais da AWS, que estão sujeitas a alterações sem aviso prévio e (c) não criam nenhum compromisso ou garantia da AWS e de suas afiliadas, fornecedores ou licenciadores. Os produtos ou serviços da AWS são fornecidos “no estado em que se encontram”, sem garantias, representações ou condições de qualquer tipo, expressas ou implícitas. As responsabilidades e as obrigações da AWS com os seus clientes são controladas por contratos da AWS, e este documento não é parte, nem modifica, qualquer contrato entre a AWS e seus clientes.

Histórico do documento

A tabela a seguir descreve adições importantes feitas na documentação da Resposta a Incidentes de Segurança da AWS, a partir de 1 janeiro de 2026. Para receber notificações sobre atualizações dessa documentação, você pode se inscrever em o feed RSS.

Alteração	Descrição	Data
Foram adicionados sistemas operacionais compatíveis com o EC2 Triage	Foi adicionada uma lista de sistemas operacionais compatíveis com o recurso do EC2 Triage, incluindo distribuições Linux (Amazon Linux 2, Amazon Linux 2023, Ubuntu, RHEL, CentOS, SLES e Debian) e versões do Windows Server.	29 de abril de 2026
Atualização da descrição da política para `AWSSecurityIncidentResponseReadOnlyAccess`	Política atualizada para adicionar a ação `security-ir:ListInvestigations` .	22 de abril de 2026
Atualização da descrição da política para `AWSSecurityIncidentResponseFullAccess`	Política atualizada para adicionar as permissões do AWS Organizations e remover a condição de MFA.	22 de abril de 2026
Atualização da descrição da política para `AWSSecurityIncidentResponseCaseFullAccess`	Política atualizada para adicionar as ações `security-ir:ListInvestigations` e `security-ir:SendFeedback` e remover a condição de MFA.	22 de abril de 2026

Atributo do EC2 Triage para a Resposta a Incidentes de Segurança da AWS	Foi adicionado o recurso do EC2 Triage que permite que a Resposta a Incidentes de Segurança da AWS colete informações investigativas de instâncias do Amazon Elastic Compute Cloud usando o Run Command do AWS Systems Manager durante as investiga ções de segurança. Página detectar e analisar atualizad a para documentar os pré-requisitos e recursos do EC2 Triage.	20 de abril de 2026
Atributo do EC2 Triage para a Resposta a Incidentes de Segurança da AWS	Documentação atualizada do CloudFormation StackSets para fornecer duas opções de modelo: somente contenção e contenção com o EC2 Triage. O modelo contenção com o EC2 Triage inclui permissõe s adicionais para coleta de dados investigativos de instâncias do Amazon EC2.	20 de abril de 2026

Coleta de dados, comportamento regional e orientação de conformidade para clientes regulamentados	Foram adicionadas novas seções sobre coleta e uso de dados, residência de dados e comportamento regional, além de acesso e permissões de dados. Seção de validação de conformidade expandida com orientação sobre responsabilidade compartilhada e classificação de metadados para clientes em setores regulamentados.	17 de abril de 2026
Guia de integração atualizado	O guia de integração foi atualizado com uma nova estrutura passo a passo, incluindo etapas de preparação, pré-requisitos e fluxos de trabalho de configuração simplificados para equipes de resposta a incidentes, tipos de casos e integrações de ferramentas.	7 de abril de 2026
Atualizar a descrição da política de perfil de serviço de triagem do AWS Security Incident Response	Atualize a descrição da política de perfil de serviço de triagem do AWS Security Incident Response para refletir as alterações que permitem ao serviço melhorar o ajuste do serviço e a coleta de informações para investigar possíveis incidentes.	27 de março de 2026
Enviar metadados	Adicionadas instruções para o envio de metadados por meio de casos do AWS Support.	27 de março de 2026

Enviar preferências de contenção	Adicionadas instruções para o envio de preferências de contenção por meio de casos do AWS Support.	27 de março de 2026
Modelo de StackSet de contenção	Atualizado o modelo do CloudFormation StackSet de contenção.	27 de março de 2026
Esclarecidas as considera ções sobre Região da AWS para contas de administrador delegado	Esclarecido que, embora você designe uma conta de administrador delegado do AWS Security Incident Response em uma Região da AWS durante a configura ção inicial, o serviço fornecerá cobertura a toda a organizaç ão em todas as Regiões da AWS compatíveis.	20 de março de 2026
Definir preferências de ações de contenção	Atualizada a seção de preferências da ação de contenção para corresponder às opções atuais.	19 de março de 2026
Resposta proativa e triagem de alertas	As referências ao fluxo de trabalho de resposta proativa e triagem de alertas como opcional foram removidas.	3 de março de 2026
Cronograma de resposta	Cronograma de resposta atualizado para especificar o SLO de 15 minutos para confirmação do caso e 5 dias úteis para a resposta ao cliente antes do encerramento do caso.	24 de fevereiro de 2026

Práticas recomendadas de comunicação	Cronograma de encerramento de casos atualizado para especificar 5 dias úteis para a resposta ao cliente para solicitações de informações críticas.	24 de fevereiro de 2026
AWS CLI Referência a adicionada em Interação com a Resposta a Incidentes de Segurança usando o AWS CloudShell	Foi adicionado um link para a Referência da AWS Command Line Interface na Resposta a Incidentes de Segurança da AWS.	24 de fevereiro de 2026
Matriz RACI	A opção “Autorizar ações de contenção do CIRT” foi atualizada para “Autorizar ações de contenção” na matriz RACI.	13 de fevereiro de 2026
Preferências de contenção	Opções de preferência de contenção atualizadas de “Nenhuma ação de contenção”, “Contenção com aprovação” e “Contenção automática” para “Aprovação necessária”, “Contém confirmado” e “Contém suspeitos” com descrições revisadas.	13 de fevereiro de 2026
Pós-Implantação da Resposta a Incidentes de Segurança	Foi adicionado um link para a demonstração AWS Security Incident Response: New Integrations and OU-Level Subscription.	4 de fevereiro de 2026
Monitoramento e investigação	Foi adicionado conteúdo revisado à introdução e às subseções desta página.	4 de fevereiro de 2026

Detecção e análise	Foi adicionado conteúdo revisado à introdução e às subseções desta página.	4 de fevereiro de 2026
Contenção	Foi adicionado conteúdo revisado a esta página.	4 de fevereiro de 2026
Agente de IA investigativo	Foi adicionada a isenção de responsabilidade Uso de dados do cliente a esta página. Isenção de responsabilidade: O agente de investigação por AI não usa dados de clientes para treinamento de modelo em compartilha dados de clientes com terceiros.	4 de fevereiro de 2026

Alteração	Descrição	Data
Cancelamento da associação	Foi atualizada a página de cancelamento da associação para indicar que a associação e o serviço serão terminados imediatamente após o cancelamento, não no fim do ciclo de cobrança.	20 de novembro de 2025
Políticas gerenciadas pela AWS	Foram adicionados atualizar casos, criar comentários de casos, listar casos, listar comentários de casos à lista de ações que o serviço fornece.	19 de novembro de 2025
Uso de perfis vinculados ao serviço	Foram adicionados atualizar casos, criar comentários de casos, listar casos, listar	19 de novembro de 2025

Alteração	Descrição	Data
	comentários de casos à lista de ações que o serviço fornece.	
Preferências de comunicação	Foi criada e atualizada a seção Preferências de Comunicação Adicionadas para a documentação de novos atributos.	12 de novembro de 2025

Alteração	Descrição	Data
Adição e atualizações do guia de integração	Guia de integração adicionado criado e atualizado, incluindo as seguintes seções Foi adicionada a seção Habilitar o Security Incident Response. Foi adicionada a seção Autorizar engenheiros do Security Incident Response a realizar ações de contenção de ameaças. Foi adicionada a seção Pós-implantação do Security Incident Response. Foi adicionada a seção Atualizar a equipe de resposta a incidentes. Foi adicionada a seção Descobertas e regras de supressão do GuardDuty. Foi adicionada a seção Amazon EventBridge. Foi adicionada a seção Integrações e fluxo de trabalho de ferramentas externas. Foi adicionada a seção Fluxo de trabalho de ferramentas externas.	12 de novembro de 2025

Alteração	Descrição	Data
	Foi adicionado a seção Apêndice A: Pontos de Contato.	
Atualizações na linguagem de conformidade e cobrança	Atualização: Foi removida a declaração de que o AWS Security Incident Response não tem cobertura por nenhum dos framework s. AWS Agora, o Security Incident Response tem cobertura do HITRUST, com cobertura adicional plenajda no futuro. Atualização de Visibilidade e controle para adicionar o AWS Security Incident Response Atualização de Cancelar associação para esclarecer os períodos de cobrança dos serviços. Adição de um vídeo de Primeiros passos que fornece contexto adicional para tarefas típicas para começar a usar o AWS Security Incident Response.	15 de agosto de 2025

Alteração	Descrição	Data
Atualização: AWSSecurityIncidentResponseServiceRolePolicy	A política inclui agora duas novas ações para `"organizations:DescribeAccount" "organizations:ListDelegatedAdministrators"` e uma nova condição: `"Condition": { "StringEquals": { "aws:ResourceAccount": "${aws:PrincipalAccount}" } }`	A ser definido
Atualização de recurso: assinatura de unidades organizacionais (UOs) especificadas ou de toda a organização da AWS	Painéis de ajuda na interface do usuário foram atualizados para refletir uma atualização para a assinatura de unidades organizacionais (UOs) específicas ou de toda a organização da AWS. Nova página criada para Gerenciar a associação com unidades organizacionais (UOs) Páginas relacionadas ao AWS Organizations, atualizadas para refletir os novos recursos de gerenciamento de UO.	7 de agosto de 2025

Alteração	Descrição	Data
Service Quotas atualizadas	Página do Service Quotas atualizada para orientar os usuários ao Guia de referência geral da AWS para Endpoints e cotas do AWS Security Incident Response	7 de agosto de 2025
Atualizações do feedback dos usuários	Adição de hiperlinks do serviço para Casos do AWS Security Incident Response Atualização para refletir o Computer Security Incident Handling Guide SP 800-61 r3 no Guia técnico de segurança.	7 de agosto de 2025
Adição de uma página sobre a integração entre o Amazon EventBridge e a Resposta a Incidentes de Segurança da AWS.	Nova seção de conteúdo para descrever como o Amazon EventBridge se integra à Resposta a Incidentes de Segurança da AWS.	26 de junho de 2025

Alteração	Descrição	Data
Atualizações no SLR com a adição de permissões para oferecer suporte aos direitos do serviço.	A política AWSSecurityIncidentResponseTriageServiceRolePolicy foi atualizada para adicionar as permissões security-ir:GetMembership, security-ir:ListMemberships, security-ir:UpdateCase, guardduty:ListFilters, guardduty:UpdateFilter, guardduty:DeleteFilter e guardduty:GetAdministratorAccount. A permissão guardduty:GetAdministratorAccount foi adicionada para facilitar o gerenciamento de filtros de arquivamento automático do GuardDuty em contas delegadas.	2 de junho de 2025
Atualizações de recursos.	A página https://docs.aws.amazon.com/security-ir/latest/userguide/appendix-b-incident-response-resources.html#playbook-resources foi atualizada para refletir os workshops ativos disponíveis para os clientes.	23 de maio de 2025
O serviço passou a oferecer suporte ao idioma japonês.	As configurações com suporte foram atualizadas para indicar o suporte ao idioma japonês no horário local do Japão. O idioma inglês permanece com suporte em nível global.	13 de maio de 2025

Alteração	Descrição	Data
Atualizações de conteúdo e de comentários dos clientes.	Uma observação foi adicionada em https://docs.aws.amazon.com/security-ir/latest/userguide/select-a-membership-account.html para refletir uma tarefa adicional ao usar uma conta de administrador delegado durante a configuração. A experiência do cliente foi atualizada ao trabalhar com um caso gerado pelo serviço e com as funcionalidades de detecção e análise. Os detalhes sobre o cancelamento de contas foram atualizados para fornecer maior clareza sobre as implicações de faturamento ao realizar o cancelamento de uma associação.	9 de maio de 2025
Adição de suporte para três novas regiões.	Ocorreu a ação de três novas regiões em https://docs.aws.amazon.com/security-ir/latest/userguide/supported-configs.html. Nomeadamente, Mumbai, Paris e São Paulo.	7 de maio de 2025

Alteração	Descrição	Data
Atualização: atualizações baseadas em comentários dos clientes sobre a documentação.	Correções de erros ortográficos e gramaticais foram aplicadas em diversas páginas. A página https://docs.aws.amazon.com/en_us/security-ir/latest/userguide/organizations_permissions.html foi atualizada para refletir corretamente o prefixo do serviço security-ir. Ocorreu a adição de uma observação em https://docs.aws.amazon.com/security-ir/latest/userguide/source-containment.html referente ao Route 53 e ao DNS.	7 de fevereiro de 2025

Alteração	Descrição	Data
Atualização: atualizações baseadas em comentários dos clientes sobre a documentação.	A página https://docs.aws.amazon.com/security-ir/latest/userguide/setup-monitoring-and-investigation-workflows.html foi atualizada para o modelo de conjunto de pilhas. As entradas de triage.security-ir.com foram corrigidas para triage.security-ir.amazonaws.com. Ocorreu a adição de uma observação sobre as conexões rastreadas para AWSSupport-ContainEC2Reversible em https://docs.aws.amazon.com/security-ir/latest/userguide/contain.html. O link inativo foi corrigido em https://docs.aws.amazon.com/security-ir/latest/userguide/managing-associated-accounts.html. Ocorreu a adição de uma definição para a conta de associação em https://docs.aws.amazon.com/security-ir/latest/userguide/select-a-membership-account.html. Ocorreu a adição de uma nota de esclarecimento em https://	20 de dezembro de 2024

Alteração	Descrição	Data
	docs.aws.amazon.com/en_us/security-ir/latest/userguide/using-service-linked-roles.html para as contas gerenciais do AWS Organizations.	

Alteração	Descrição	Data
Atualização: atualizações baseadas em comentários dos clientes sobre a documenta ção.	Diversas duplicações de “AWS AWS” foram removidas no texto. Os links inativos foram corrigidos em https://d ocs.aws.amazon.com/ security-ir/latest/userguide/ sir_tagging.html e https://d ocs.aws.amazon.com/security -ir/latest/userguide/service- name-info-in-cloudtrail.html. Ocorreram atualizações em https://docs.aws.amazon.com /security-ir/latest/usergui de/contain.html. O símbolo “**>**” foi removido do primeiro parágrafo. AWSSupport- ContainEC2Reversible foi substituído por AWSSuppor t-ContainEC2Instance. AWSSupport-Contain IAMReversible foi substituí do por AWSSupport-Contain IAMPrincipal. AWSSuppor t-ContainS3Reversible foi substituído por AWSSupport- ContainS3Resource. Os formatos foram atualizad os em https://docs.aws.a mazon.com/en_us/security-ir/ latest/userguide/issues.html.	10 de dezembro de 2024

Alteração	Descrição	Data
	Ao orientar os clientes a entrar em contato com a equipe do Security Incident Response por meio de um tíquetes do suporte, https://docs.aws.amazon.com/security-ir/latest/userguide/understand-response-teams-and-support.html agora apresenta opções a serem selecionadas seleção nos formulários de suporte. O CloudWatch Events foi removido e substituído por EventBridge em https://docs.aws.amazon.com/security-ir/latest/userguide/logging-and-events.html. Ocorreram atualizações gramaticais em https://docs.aws.amazon.com/security-ir/latest/userguide/technique-access-containment.html. A data de publicação foi removida de https://docs.aws.amazon.com/security-ir/latest/userguide/security-incident-response-guide.html e substituída pelas atualizações indicadas nesta tabela.	
Atualização: políticas gerenciadas pela AWS e perfis vinculados ao serviço.	Atualizações em políticas gerenciadas e perfis vinculados ao serviço.	1.º de dezembro de 2024

Alteração	Descrição	Data
Inicialização do serviço	Publicação da documentação inicial referente ao lançamento do serviço no re:Invent 2024.	1.º de dezembro de 2024