AWS Well-Architected Framework

Pilar Segurança

Pilar Segurança: AWS Well-Architected Framework

Table of Contents

Pilar Segurança: AWS Well-Architected Framework

Data de publicação: 6 de dezembro de 2023 (Revisões do documento)

O foco deste whitepaper é o pilar Segurança do AWS Well-Architected Framework. Ele contém orientações para ajudá-lo a aplicar melhores práticas e recomendações atuais ao projeto, entrega e manutenção de cargas de trabalho seguras da AWS.

Introdução

O AWS Well-Architected Framework ajuda você a entender as vantagens e desvantagens das decisões que você toma ao criar cargas de trabalho na AWS. Ao usar o Framework, você aprenderá as práticas recomendadas atualmente de arquitetura para projetar e operar workloads confiáveis, seguras, eficientes, econômicas e sustentáveis na nuvem. Com ele, você consegue avaliar consistentemente sua workload em relação às práticas recomendadas e identificar áreas de melhoria. Acreditamos que ter as workloads bem arquitetadas aumenta muito a probabilidade de sucesso nos negócios.

A estrutura é baseada em seis pilares:

- Excelência Operacional
- Segurança
- Confiabilidade
- Eficiência de performance
- Otimização de custos
- Sustentabilidade

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

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

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

Fundamentos de segurança

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

Princípios de design

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

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

Definição

A segurança na nuvem é composta por sete áreas:

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

Responsabilidade compartilhada

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

Responsabilidade da AWS com a “segurança da nuvem” : a AWS é responsável pela proteção da infraestrutura que executa todos os serviços oferecidos na Nuvem AWS. Essa infraestrutura abrange o hardware, o software, as redes e as instalações que executam os serviços da Nuvem AWS.

Responsabilidade do cliente com a “segurança na nuvem” : a responsabilidade do cliente será determinada pelos serviços da Nuvem AWS que ele selecionar. Isso define o volume do trabalho de configuração que o cliente deve executar como parte de suas responsabilidades com a segurança.

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

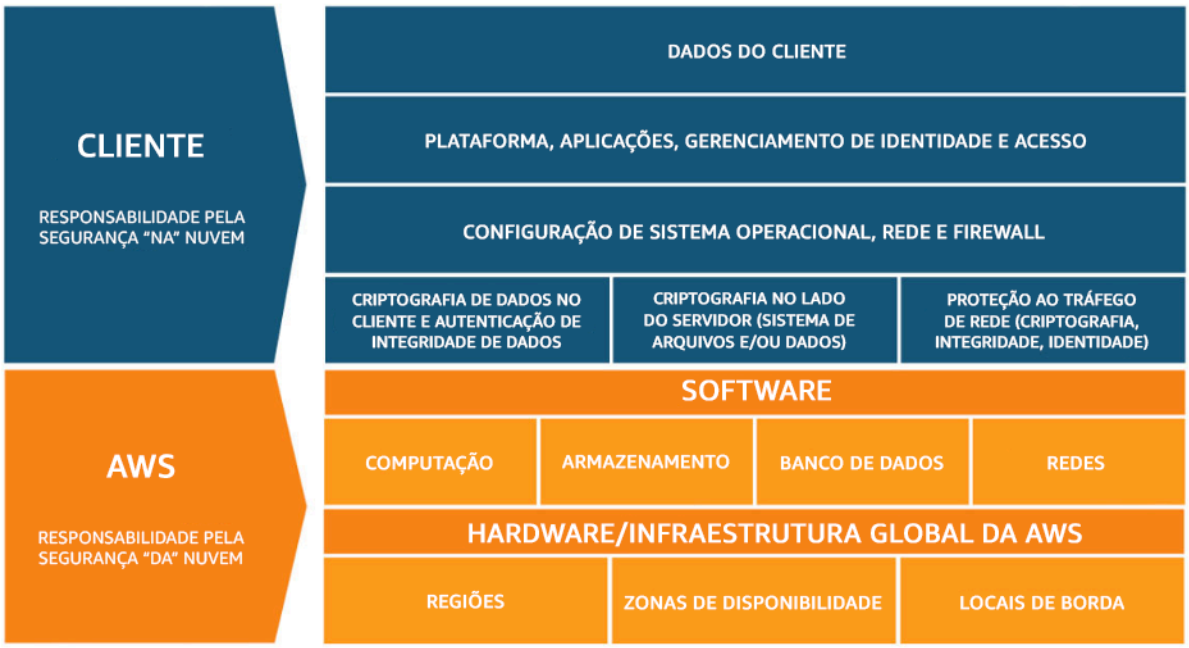


Figura 1: modelo de responsabilidade compartilhada da AWS.

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

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

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

- Controles físicos e ambientais

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

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

Específico para o cliente : controles que são de responsabilidade exclusiva do cliente com base na aplicação que está sendo implantada nos serviços da AWS. Por exemplo:

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

Governança

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

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

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

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

Probabilidade	Nível de risco				
Muito provável	Baixo	Médio	Alto	Crítica	Crítica
Provável	Baixo	Médio	Médio	Alto	Crítica
Possível	Baixo	Baixo	Médio	Médio	Alto
Improvável	Baixo	Baixo	Médio	Médio	Alto
Muito improvável	Baixo	Baixo		Médio	Alto
Consequência	Mínima	Baixo	Médio	Alto	Grave

Figura 2: Matriz de probabilidade de nível de risco

Gerenciamento e separação de contas da AWS

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

Gerenciar contas de maneira centralizada: o AWS Organizations automatiza a criação e o gerenciamento de contas da AWS, bem como o controle dessas contas depois que elas são criadas. Quando você cria uma conta por meio do AWS Organizations, é importante considerar o endereço de e-mail usado, pois esse será o usuário root que permite que a senha seja redefinida. O Organizations permite agrupar contas em unidades organizacionais (UOs), que podem representar ambientes diferentes com base nos requisitos e na finalidade da carga de trabalho.

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

em nível de organização, unidade organizacional ou conta, que se aplicam a todos os usuários e funções do AWS Identity and Access Management (IAM). Por exemplo, você pode aplicar uma SCP que restrinja os usuários de iniciar recursos em regiões que você não tenha permitido explicitamente. O AWS Control Tower oferece uma maneira simplificada de configurar e controlar várias contas. Ele automatiza a configuração de contas na organização da AWS, automatiza o provisionamento e aplica barreiras de proteção (que incluem prevenção e detecção) e fornece um painel para visibilidade.

Configurar serviços e recursos de forma centralizada: o AWS Organizations ajuda você a configurar os serviços da AWS que se aplicam a todas as suas contas. Por exemplo, você pode configurar o registro em log centralizado de todas as ações executadas em toda a organização usando o AWS CloudTraile evite que as contas dos membros desativem o registro em log. Você também pode agregar dados centralmente para regras definidas usando o AWS Config, permitindo auditar workloads em busca de conformidade e reagir rapidamente a alterações. O AWS CloudFormation StackSets permitem que você gerencie centralmente pilhas do AWS CloudFormation entre contas e UOs na sua organização. Isso permite provisionar automaticamente uma nova conta para atender aos seus requisitos de segurança.

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

Práticas recomendadas

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

SEC01-BP01 Separar as workloads usando contas

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

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

Antipadrões comuns:

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

Benefícios do estabelecimento desta prática recomendada:

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

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: alto

Orientação de implementação

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

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

O AWS Organizations e o AWS Control Tower são dois serviços que você pode utilizar para implementar e gerenciar essa estrutura de várias contas em seu ambiente da AWS. O AWS Organizations possibilita organizar as contas em uma hierarquia definida por uma ou mais camadas

de UOs, em que cada UO contém uma série de contas membros. As políticas de controle de serviços (SCPs) permitem que o administrador da organização estabeleça controles preventivos detalhados nas contas membros, e o AWS Config pode ser utilizado para estabelecer controles proativos e de detecção nessas contas. Muitos serviços da AWS integram-se ao AWS Organizations para oferecer controles administrativos delegados e realizar tarefas específicas do serviço em todas as contas membros da organização.

Estruturado sobre o AWS Organizations, o AWS Control Tower oferece práticas recomendadas de um clique para um ambiente da AWS de várias contas com uma zona de pouso. A zona de pouso é o ponto de entrada para o ambiente de várias contas estabelecido pelo Control Tower. O Control Tower oferece vários benefícios em comparação com o AWS Organizations. Três benefícios que oferecem governança aprimorada de contas são:

- Barreiras de proteção de segurança obrigatórias e integradas que são aplicadas automaticamente às contas admitidas na organização.
- Barreiras de proteção opcionais que podem ser ativadas ou desativadas em determinado conjunto de UOs.
- O AWS Control Tower Account Factory oferece implantação automatizada de contas que contêm linhas de base aprovadas e opções de configuração em sua organização.

Etapas da implementação

1. Projetar uma estrutura de unidade organizacional: uma estrutura de unidade organizacional projetada adequadamente reduz o trabalho de gerenciamento necessário para criar e manter políticas de controle de serviços e outros controles de segurança. Sua estrutura de unidade organizacional deve estar alinhada com as necessidades, a confidencialidade dos dados e a estrutura de workload de sua empresa.
2. Criar uma zona de pouso para seu ambiente de várias contas: uma zona de pouso oferece uma base consistente de infraestrutura e segurança na qual sua organização pode desenvolver, executar e implantar workloads com rapidez. É possível usar uma zona de pouso personalizada ou o AWS Control Tower para orquestrar seu ambiente.
3. Estabelecer barreiras de proteção: implemente barreiras de proteção consistentes para seu ambiente por meio da zona de pouso. O AWS Control Tower oferece uma lista de controles obrigatórios e opcionais que podem ser implantados. Os controles obrigatórios são implantados automaticamente na implementação do Control Tower. Leia a lista de controles opcionais e altamente recomendados e implemente controles adequados às suas necessidades.

4. Restringir o acesso a regiões adicionadas recentemente: para novas Regiões da AWS, recursos do IAM, como usuários e perfis, serão propagados somente para as regiões especificadas. Essa ação pode ser realizada por meio do console ao usar o Control Tower ou ajustando as políticas de permissões do IAM no AWS Organizations.
5. Considerar o AWS CloudFormation StackSets: o StackSets ajuda você a implantar recursos, como grupos, políticas e perfis do IAM em diferentes regiões e Contas da AWS por meio de um modelo aprovado.

Recursos

Práticas recomendadas relacionadas:

- SEC02-BP04 Contar com um provedor de identidades centralizado

Documentos relacionados:

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

Vídeos relacionados:

- Habilitar a adoção da AWS em grande escala com automação e governança
- Práticas recomendadas de segurança de acordo com o Well-Architected
- Criar e administrar várias contas com o uso do AWS Control Tower
- Habilitar o Control Tower para organizações existentes

Workshops relacionados:

- Dia de imersão no Control Tower

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

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

Resultado desejado: proteger o usuário raiz ajuda a reduzir a chance de danos acidentais ou intencionais decorrentes do mau uso das respectivas credenciais. Estabelecer controles de detecção também pode alertar o pessoal apropriado quando se realizam ações utilizando o usuário raiz.

Antipadrões comuns:

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

Benefícios do estabelecimento desta prática recomendada: proteger o acesso ao usuário raiz cria a confiança de que as ações em sua conta estão controladas e auditadas.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: alto

Orientação de implementação

A AWS oferece muitas ferramentas para ajudar a proteger sua conta. No entanto, como algumas dessas medidas não estão habilitadas por padrão, é necessário implementá-las diretamente. Leve em consideração essas recomendações como etapas fundamentais para proteger sua Conta da

AWS. Ao implementar essas etapas, é importante criar um processo para avaliar e monitorar os controles de segurança de forma contínua.

Ao criar uma Conta da AWS pela primeira vez, você começa com uma identidade que tem acesso completo a todos os recursos e serviços da AWS na conta. Essa identidade é chamada de usuário raiz da Conta da AWS. É possível fazer login como usuário raiz usando o endereço de e-mail e a senha utilizados para criar a conta. Devido ao acesso elevado concedido ao usuário raiz da AWS, é necessário limitar o uso do usuário raiz da AWS à realização de tarefas que o exijam especificamente. As credenciais de login do usuário raiz devem ser bem protegidas, e a autenticação multifator (MFA) sempre deve ser habilitada para o usuário raiz da Conta da AWS.

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

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

Etapas da implementação

As etapas de implementação a seguir são recomendadas para estabelecer controles para o usuário raiz. Quando aplicável, as recomendações têm referências cruzadas com o Benchmark do CIS AWS Foundations versão 1.4.0. Além dessas etapas, consulte as Diretrizes de práticas recomendadas da AWS para proteger os recursos e a Conta da AWS.

Controles preventivos

1. Configure informações de contato precisos para a conta.

   a. Essas informações são usadas para o fluxo de recuperação de senha perdida, o fluxo de recuperação de conta de dispositivo MFA perdida e para comunicações com sua equipe sobre segurança crítica.

   b. Utilize um endereço de e-mail hospedado por seu domínio corporativo, preferencialmente uma lista de distribuição, como o endereço de e-mail do usuário raiz. O uso de uma lista de distribuição em vez da conta de e-mail de um indivíduo oferece redundância e continuidade adicionais para o acesso à conta raiz por longos períodos.

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

2. Não crie chaves de acesso para o usuário raiz. Se houver chaves de acesso, remova-as (CIS 1.4).

   a. Elimine todas as credenciais programáticas de longa duração (chaves de acesso e secretas) para o usuário raiz.

   b. Se já houver chaves de acesso do usuário raiz, será necessário fazer a transição dos processos que utilizam essas chaves para utilizar chaves de acesso temporárias de um perfil do AWS Identity and Access Management (IAM), depois excluir as chaves de acesso do usuário raiz.

3. Determine se você precisa armazenar credenciais para o usuário raiz.

   a. Ao usar o AWS Organizations para criar contas membros, a senha inicial do usuário raiz em novas contas membros é definida como um valor aleatório que não é exposto a você. Se necessário, considere utilizar o fluxo de redefinição de senha de sua conta de gerenciamento do AWS Organizations para obter acesso à conta membro.

   b. Para Contas da AWS autônomas ou a conta de gerenciamento do AWS Organizations, considere criar e armazenar de forma segura as credenciais do usuário raiz. Ativar a MFA para o usuário raiz

4. Ative os controles preventivos para os usuários raiz das contas membros em ambientes de várias contas da AWS.

   a. Considere habilitar a barreira de proteção preventiva Desautorizar criação de chaves de acesso raiz para o usuário raiz para contas membros.

   b. Considere habilitar a barreira de proteção preventiva Desautorizar criação como um usuário raiz para contas membros.

5. Se você precisar de credenciais para o usuário raiz:

   a. Use uma senha complexa.

b. Ative a autenticação multifator (MFA) para o usuário raiz, especialmente para contas (pagantes) de gerenciamento do AWS Organizations (CIS 1.5).

c. Considere o uso de dispositivos de MFA de hardware para ter resiliência e segurança, pois os dispositivos de uso único reduzem as chances de os dispositivos que contêm seus códigos de MFA serem reutilizados para outros fins. Garanta que os dispositivos de MFA de hardware alimentados por bateria sejam substituídos regularmente. (CIS 1.6)

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

d. Considere registrar vários dispositivos de MFA para backup. Até oito dispositivos de MFA são permitidos por conta.

   - Registrar mais de um dispositivo de MFA para o usuário raiz desabilita automaticamente o fluxo para recuperar sua conta se o dispositivo de MFA for perdido.

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

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

   - As práticas recomendadas de gerenciamento de credenciais dependem de seus requisitos regulatórios e de política. Os usuários raiz protegidos por MFA não dependem da senha como um único fator de autenticação.
   - A alteração periódica da senha de usuário raiz reduz o risco de mau uso de uma senha exposta acidentalmente.

Controles de detecção

- Crie alarmes para detectar o uso das credenciais raiz (CIS 1.7). Quando habilitado, o Amazon GuardDuty monitora e alerta o uso de credenciais da API do usuário raiz por meio da descoberta RootCredentialUsage.
- Avalie e implemente os controles de detecção incluídos no pacote de conformidade do Pilar de segurança do AWS Well-Architected para AWS Config ou, se usar o AWS Control Tower, os controles altamente recomendados disponíveis no Control Tower.

Orientação operacional

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

Recursos

Práticas recomendadas relacionadas:

- SEC01-BP01 Separar as workloads usando contas
- SEC02-BP01 Usar mecanismos de login fortes
- SEC03-BP02 Conceder acesso com privilégio mínimo
- SEC03-BP03 Estabelecer processo de acesso de emergência
- SEC10-BP05 Acesso pré-provisionado

Documentos relacionados:

- AWS Control Tower
- Diretrizes de auditoria de segurança da AWS
- Práticas recomendadas do IAM
- Amazon GuardDuty: alerta de uso de credenciais raiz
- Orientações passo a passo sobre como monitorar o uso de credenciais raiz por meio do CloudTrail
- Tokens de MFA aprovados para uso com a AWS
- Implementar o acesso de quebra de vidro na AWS
- Os dez principais itens de segurança para aprimorar sua Conta da AWS
- O que fazer se eu notar atividade não autorizada em minha Conta da AWS?

Vídeos relacionados:

- Habilitar a adoção da AWS em grande escala com automação e governança
- Práticas recomendadas de segurança de acordo com o Well-Architected
- Limitar o uso de credenciais raiz da AWS do AWS re:inforce 2022: Práticas recomendadas de segurança com o AWS IAM

Exemplos e laboratórios relacionados:

- Laboratório: Conta da AWS e usuário raiz

Operar workloads com segurança

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

Para operar sua carga de trabalho com segurança, você deve aplicar as melhores práticas gerais a todas as áreas de segurança. Use os requisitos e os processos que você definiu em excelência operacional em nível de carga de trabalho e também organizacional e aplique-os a todas as áreas. Manter-se atualizado com as recomendações da AWS e do setor e a inteligência de ameaças ajuda você a desenvolver seu modelo de ameaças e objetivos de controle. A automação de processos, testes e validação de segurança ajuda a escalar suas operações de segurança.

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

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

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

Práticas recomendadas

- SEC01-BP03 Identificar e validar objetivos de controle
- SEC01-BP04 Manter-se atualizado sobre as ameaças à segurança

- SEC01-BP05 Manter-se atualizado com as recomendações de segurança
- SEC01-BP06 Automatizar testes e validação de controles de segurança em pipelines
- SEC01-BP07 Identificar ameaças e priorizar mitigações com o uso de um modelo de ameaça
- SEC01-BP08 Avaliar e implementar regularmente novos serviços e recursos de segurança

SEC01-BP03 Identificar e validar objetivos de controle

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

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

Orientação de implementação

- Identificar requisitos de conformidade: descubra os requisitos organizacionais, legais e de conformidade que a sua workload precisa cumprir.
- Identificar recursos de conformidade da AWS: identifique os recursos da AWS disponíveis para ajudar você com a conformidade.
  - https://aws.amazon.com/compliance/
  - https://aws.amazon.com/artifact/

Recursos

Documentos relacionados:

- AWS Security Audit Guidelines (Diretrizes de auditoria de segurança da AWS)
- Boletins de segurança

Vídeos relacionados:

- AWS Security Hub: Manage Security Alerts and Automate Compliance (AWS Security Hub: gerenciamento de alertas de segurança e automatização da governança)
- Security Best Practices the Well-Architected Way

SEC01-BP04 Manter-se atualizado sobre as ameaças à segurança

Para ajudar a definir e implementar os controles apropriados, reconheça vetores de ataque mantendo-se a par das ameaças de segurança mais recentes. Consuma o AWS Managed Services para facilitar o recebimento de notificações de comportamentos inesperados ou incomuns em suas contas da AWS. Investigue usando ferramentas de parceiros da AWS ou feeds de informações sobre ameaças de terceiros como parte de seu fluxo de informações de segurança. A lista de vulnerabilidades e exposições comuns (CVEs) contém vulnerabilidades de segurança cibernética divulgadas publicamente que você pode usar para se manter atualizado.

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

Orientação de implementação

- Inscreva-se em fontes de inteligência de ameaças: analise regularmente as informações de inteligência de ameaças de várias fontes relevantes sobre as tecnologias usadas na sua workload.
  - Lista de vulnerabilidades e exposições comuns
- Considerar AWS Shield Advanced : oferece visibilidade quase em tempo real das fontes de inteligência, se sua workload for acessível pela Internet.

Recursos

Documentos relacionados:

- AWS Security Audit Guidelines (Diretrizes de auditoria de segurança da AWS)
- AWS Shield
- Boletins de segurança

Vídeos relacionados:

- Security Best Practices the Well-Architected Way

SEC01-BP05 Manter-se atualizado com as recomendações de segurança

Mantenha-se atualizado com as recomendações de segurança da AWS e do setor para evoluir a postura de segurança de sua workload. Boletins de segurança da AWS contêm informações importantes sobre notificações de segurança e privacidade.

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

Orientação de implementação

- Siga as atualizações da AWS: inscreva-se ou verifique regularmente novas recomendações e dicas.
  - Laboratórios do AWS Well-Architected
  - Blog de segurança da AWS
  - Documentação do serviço da AWS
- Inscreva-se para receber as novidades do setor: consulte regularmente os feeds de notícias de várias fontes relevantes às tecnologias usadas na sua workload.
  - Exemplo: lista de vulnerabilidade e exposições comuns

Recursos

Documentos relacionados:

- Boletins de segurança

Vídeos relacionados:

- Security Best Practices the Well-Architected Way

SEC01-BP06 Automatizar testes e validação de controles de segurança em pipelines

Estabeleça linhas de base e modelos seguros para mecanismos de segurança que são testados e validados como parte de sua compilação, pipelines e processos. Use ferramentas e automação para testar e validar todos os controles de segurança continuamente. Por exemplo, verifique itens, como imagens de máquina e modelos de infraestrutura como código, para detectar vulnerabilidades de segurança, irregularidades e desvios da uma linha de base estabelecida em cada estágio. O AWS CloudFormation Guard pode ajudar você a verificar se os modelos do CloudFormation são seguros, economizar tempo e reduzir o risco de erro de configuração.

É fundamental reduzir o número de configurações incorretas de segurança introduzidas em um ambiente de produção. Portanto, quanto mais você puder controlar a qualidade e reduzir os defeitos

no processo de construção, melhor. Projete pipelines de integração e implantação contínua (CI/CD) para testar problemas de segurança sempre que possível. Os pipelines de CI/CD oferecem a oportunidade de aumentar a segurança em cada estágio de criação e entrega. As ferramentas de segurança de CI/CD também devem estar sempre atualizadas para mitigar as ameaças em constante evolução.

Acompanhe as alterações na configuração de workload para ajudar na auditoria de conformidade, gerenciamento de alterações e investigações que possam ser aplicáveis. Você pode usar o AWS Config para registrar e avaliar seus recursos da AWS e de terceiros. Ele permite auditar e avaliar continuamente a conformidade geral com regras e pacotes de conformidade, que são coleções de regras com ações de correção.

O rastreamento de alterações deve incluir alterações planejadas, que fazem parte do processo de controle de alterações da sua organização [às vezes chamado de MACD, de Move, Add, Change, Delete (Mover, Adicionar, Alterar, Excluir)], alterações não planejadas e alterações inesperadas, como incidentes. Podem ocorrer alterações na infraestrutura, mas também podem estar relacionadas a outras categorias, como alterações em repositórios de código, imagens de máquina e alterações de inventário de aplicações, alterações de processos e políticas ou alterações de documentação.

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

Orientação de implementação

- Automatize o gerenciamento de configuração: aplique e valide configurações seguras automaticamente usando uma ferramenta ou um serviço de gerenciamento de configuração.
  - AWS Systems Manager
  - AWS CloudFormation
  - Configurar um pipeline CI/CD na AWS

Recursos

Documentos relacionados:

- Como usar políticas de controle de serviço para definir barreiras de proteção de permissão entre contas no AWS Organization

Vídeos relacionados:

- Como gerenciar ambientes da AWS de várias contas usando o AWS Organizations
- Security Best Practices the Well-Architected Way

SEC01-BP07 Identificar ameaças e priorizar mitigações com o uso de um modelo de ameaça

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

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: alto

Orientações para a implementação

O que é modelagem de ameaças?

“A modelagem de ameaças serve para identificar, comunicar e compreender as ameaças e as mitigações no contexto de proteção de algo de valor.” The Open Web Application Security Project (OWASP) Application Threat Modeling

Por que você deve ter um modelo de ameaças?

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

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

Quando a modelagem de ameaças deve ser realizada?

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

Etapas da implementação

Como podemos realizar a modelagem de ameaças?

Há muitas formas diferentes de realizar a modelagem de ameaças. Muito semelhante às linguagens de programação, há vantagens e desvantagens em cada uma, e é necessário escolher a forma mais adequada para você. Uma abordagem é começar com o Shostack's 4 Question Frame for Threat Modeling (Estrutura de quatro perguntas do Shostack para modelagem de ameaças), que apresenta perguntas abertas a fim de oferecer estrutura ao seu exercício de modelagem de ameaças:

1. Em que você está trabalhando?

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

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

Não há uma lista canônica do que pode dar errado. A criação dessa lista exige etapas de brainstorming e colaboração entre todas as pessoas de sua equipe e as pessoas relevantes envolvidas no exercício de modelagem de ameaças. Você pode auxiliar suas etapas de brainstorming utilizando um modelo para identificar ameaças, como o STRIDE, que sugere categorias diferentes para avaliar: Spoofing (Falsificação), Tampering (Violação), Repudiation (Repúdio), Information disclosure (Divulgação de informações), Denial of service (Negação de serviço) e Elevation of privilege (Elevação de privilégio). Além disso, talvez você queira auxiliar as etapas de brainstorming revisando as listas existentes e a pesquisa para inspiração, como o OWASP Top 10, o HiTrust Threat Catalog e o catálogo de ameaças de sua própria organização.

3. O que estamos fazendo a respeito?

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

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

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

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

suas dependências e pensar nos controles que você poderia implementar para resolver essas ameaças. Esses controles podem ser fatores como validação de entrada, processamento de sessões e processamento de limites. Com frequência, a maioria das vulnerabilidades é introduzida em código personalizado, então concentre-se nessa área.

4. Fizemos um bom trabalho?

   O objetivo é a sua equipe e a organização aprimorarem a qualidade dos modelos de ameaças e a velocidade na qual você está realizando a modelagem de ameaças no decorrer do tempo. Essas melhorias vêm de uma combinação de prática, aprendizado, instrução e revisão. Para se aprofundar e trabalhar, é recomendável que você e sua equipe concluam o curso de treinamento Threat modeling the right way for builders (Modelagem de ameças da maneira certa para desenvolvedores) ou o respectivo workshop. Além disso, se você estiver procurando orientações sobre como integrar a modelagem de ameaças ao ciclo de vida do desenvolvimento de aplicações da organização, consulte a publicação Como abordar a modelagem de ameaças no Blog de segurança da AWS.

Threat Composer

Para ajudar e fornecer orientações ao criar a modelagem de ameaças, considere usar a ferramenta Threat Composer, que visa reduzir o tempo de maturação na modelagem de ameaças. Essa ferramenta ajuda a fazer o seguinte:

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

Para obter mais referências, acesse o Threat Composer e alterne para o Example Workspace definido pelo sistema.

Recursos

Práticas recomendadas relacionadas:

- SEC01-BP03 Identificar e validar objetivos de controle
- SEC01-BP04 Manter-se atualizado sobre as ameaças à segurança
- SEC01-BP05 Manter-se atualizado com as recomendações de segurança
- SEC01-BP08 Avaliar e implementar regularmente novos serviços e recursos de segurança

Documentos relacionados:

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

Vídeos relacionados:

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

Treinamento relacionado:

- Threat modeling the right way for builders (Modelagem de ameaças da maneira certa para desenvolvedores): treinamento autoguiado virtual do AWS Skill Builder
- Threat modeling the right way for builders – AWS Workshop (Modelagem de ameaças da maneira certa para desenvolvedores)

Ferramentas relacionadas:

- Threat Composer

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

Avalie e implemente serviços e recursos de segurança da AWS e parceiros da AWS que permitem que você desenvolva a postura de segurança da sua workload. O blog de segurança da AWS destaca novos serviços e recursos, guias de implementação e orientações gerais de segurança da AWS. Quais as novidades da AWS? é uma ótima forma de se manter atualizado com todos os novos recursos, serviços e anúncios da AWS.

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

Orientação de implementação

- Planeje revisões regulares: crie um calendário de atividades de análise que inclua os requisitos de conformidade, avaliar novos recursos e serviços de segurança da AWS e manter-se atualizado sobre as novidades do setor.
- Descubra os serviços e recursos da AWS: descubra os recursos de segurança disponíveis para os serviços que você está usando e analise os novos recursos à medida que são lançados.
  - Blog de segurança da AWS
  - Boletins de segurança da AWS
  - Documentação do serviço da AWS
- Definir processo de integração de serviços da AWS: defina processos para integração de novos serviços da AWS. Inclua como você avalia os novos serviços da AWS em termos de funcionalidade e os requisitos de conformidade para sua workload.
- Teste novos serviços e recursos: teste novos serviços e recursos à medida que são lançados em um ambiente que não seja de produção que replica bem o ambiente de produção.
- Implemente outros mecanismos de defesa: implemente mecanismos automatizados para defender sua workload e explore as opções disponíveis.
  - Como corrigir recursos não compatíveis da AWS pelo Regras do AWS Config

Recursos

Vídeos relacionados:

- Security Best Practices the Well-Architected Way

Gerenciamento de identidade e acesso

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

Tópicos

Gerenciamento de identidades

Há dois tipos de identidade que você precisa gerenciar para operar workloads seguras da AWS.

- Identidades humanas: administradores, desenvolvedores, operadores e clientes de suas aplicações precisam de uma identidade para acessar seus ambientes e aplicações da AWS. Eles podem ser membros da sua organização ou usuários externos com quem você colabora e que interagem com seus recursos da AWS por meio de um navegador da web, uma aplicação cliente, um aplicativo móvel ou de ferramentas interativas de linha de comando.
- Identidades de máquina: aplicações de workload, ferramentas operacionais e componentes precisam de uma identidade para solicitar serviços da AWS, como ler dados. Essas identidades incluem máquinas em execução em seu ambiente da AWS, como instâncias do Amazon EC2 ou funções do AWS Lambda. Você também pode gerenciar identidades de máquina para partes externas que precisam de acesso. Além disso, você pode ter máquinas fora da AWS que precisam de acesso ao seu ambiente da AWS.

Práticas recomendadas

- SEC02-BP01 Usar mecanismos de login fortes
- SEC02-BP02 Usar credenciais temporárias
- SEC02-BP03 Armazenar e usar segredos com segurança
- SEC02-BP04 Contar com um provedor de identidades centralizado

- SEC02-BP05 Fazer a auditoria e a alternância periódica das credenciais
- SEC02-BP06 Utilizar grupos e atributos de usuários

SEC02-BP01 Usar mecanismos de login fortes

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

Resultado desejado: reduzir os riscos de acesso acidental a credenciais na AWS usando mecanismos de login fortes para usuários do AWS Identity and Access Management (IAM), o usuário raiz da Conta da AWS, o AWS IAM Identity Center (sucessor do AWS Single Sign-On), e provedores de identidades de terceiros. Isso significa exigir MFA, impor políticas de senhas fortes e detectar comportamento de login anômalo.

Antipadrões comuns:

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

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: alto

Orientação de implementação

Há muitas formas de identidades humanas fazerem login na AWS. É prática recomendada da AWS depender de um provedor de identidades centralizado utilizando federação (federação direta ou usando AWS IAM Identity Center) ao realizar a autenticação na AWS. Nesse caso, você deve estabelecer um processo de login seguro com seu provedor de identidades ou o Microsoft Active Directory.

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

Se você criar usuários no AWS IAM Identity Center, proteja o processo de login nesse serviço. Para identidades dos consumidores, é possível usar o Amazon Cognito user pools e proteger o processo de login nesse serviço ou usar os provedores de identidades compatíveis com o Amazon Cognito user pools.

Se estiver usando usuários do AWS Identity and Access Management (IAM), você protegerá o processo de login com o IAM.

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

Etapas da implementação

Veja a seguir as recomendações gerais de login forte. As configurações reais devem ser definidas pela política de sua empresa ou usando um padrão como NIST 800-63.

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

Recomendações do IAM Identity Center:

- O IAM Identity Center oferece uma política de senha predefinida ao usar o diretório padrão que estabelece o comprimento da senha, a complexidade e requisitos de reutilização.
- Ative a MFA e defina a configuração de reconhecimento de contexto ou sempre ativo da MFA quando a origem da identidade for o diretório padrão, o AWS Managed Microsoft AD ou o AD Connector.
- Permita que os usuários registrem seus próprios dispositivos de MFA.

Recomendações de diretório do Amazon Cognito user pools:

- Defina as configurações de força da senha.
- Exija MFA dos usuários.
- Use as configurações de segurança avançadas do Amazon Cognito user pools para recursos como autenticação adaptável que podem bloquear logins suspeitos.

Recomendações para usuários do IAM:

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

Recursos

Práticas recomendadas relacionadas:

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

Documentos relacionados:

- Política de senha do AWS IAM Identity Center (sucessor do AWS Single Sign-On)
- Política de senha do usuário do IAM
- Definir a senha do usuário raiz da Conta da AWS
- Política de senha do Amazon Cognito
- Credenciais da AWS
- Práticas recomendadas de segurança no IAM

Vídeos relacionados:

- Gerenciar permissões de usuário em grande escala com o AWS IAM Identity Center

- Dominar a identidade em todos os aspectos

SEC02-BP02 Usar credenciais temporárias

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

Resultado desejado: para reduzir o risco de credenciais de longo prazo, use credenciais temporárias sempre que possível para identidades humanas e de máquina. Credenciais de longo prazo criam muitos riscos, por exemplo, é possível fazer upload delas em código para repositórios públicos do GitHub. Ao utilizar credenciais temporárias, você reduz significativamente as chances de comprometimento das credenciais.

Antipadrões comuns:

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

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: alto

Orientação de implementação

Utilize credenciais de segurança temporárias em vez de credenciais de longo prazo para todas as solicitações da AWS CLI e API. As solicitações de API e CLI para serviços da AWS devem, em quase todos os casos, ser assinadas com chaves de acesso da AWS. Essas solicitações podem ser assinadas com credenciais temporárias ou de longo prazo. A única vez que você deve usar credenciais de longo prazo, também conhecidas como chaves de acesso de longo prazo, é se você estiver utilizando um usuário do IAM ou o usuário raiz da Conta da AWS. Quando você usa

federação na AWS ou assume um perfil do IAM por outros métodos, são geradas credenciais temporárias. Mesmo quando você acessa o AWS Management Console utilizando credenciais de login, credenciais temporárias são geradas para você fazer chamadas para serviços da AWS. Há poucas situações nas quais você precisa de credenciais de longo prazo, e é possível realizar quase todas as tarefas usando credenciais temporárias.

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

Etapas da implementação

Para identidades humanas, como funcionários, administradores, desenvolvedores, operadores e clientes:

- Você deve contar com um provedor de identidades centralizado e exigir que usuários humanos usem federação com um provedor de identidades para acessar a AWS utilizando credenciais temporárias. A federação para seus usuários pode ser realizada com federação direta para cada Conta da AWS ou usando o AWS IAM Identity Center (sucessor do AWS IAM Identity Center) e o provedor de identidades de sua escolha. A federação oferece uma série de vantagens em comparação com a utilização de usuários do IAM além de eliminar credenciais de longo prazo. Seus usuários também podem solicitar credenciais temporárias da linha de comando para federação direta ou utilizando o IAM Identity Center. Isso significa que há poucos casos de uso que exigem usuários do IAM ou credenciais de longo prazo para seus usuários.
- Ao conceder acesso a recursos em sua Conta da AWS a terceiros, como provedores de software como serviço (SaaS), você pode utilizar perfis entre contas e políticas baseadas em recursos.
- Se você precisar conceder a aplicações de consumidores ou clientes acesso aos seus recursos da AWS, você pode utilizar grupos de identidade do Amazon Cognito ou Amazon Cognito user pools para fornecer credenciais temporárias. As permissões para as credenciais são configuradas por meio de perfis do IAM. Você também pode definir um perfil do IAM separado com permissões limitadas para usuários convidados que não são autenticados.

Para identidades de máquina, talvez seja necessário utilizar credenciais de longo prazo. Nesses casos, você deve exigir que as workloads utilizem credenciais temporárias com perfis da IAM para acessar a AWS.

- Para Amazon Elastic Compute Cloud (Amazon EC2), é possível usar perfis do Amazon EC2.

- O AWS Lambda permite configurar um perfil de execução do Lambda para conceder permissões de serviço a fim de executar ações da AWS usando credenciais temporárias. Há muitos outros modelos semelhantes para os serviços da AWS concederem credenciais temporárias utilizando perfis do IAM.
- Para serviços de IoT, é possível usar o provedor de credenciais de AWS IoT Core para solicitar credenciais temporárias.
- Para sistemas on-premises ou sistemas executados fora da AWS que precisem acessar os recursos da AWS, é possível utilizar o IAM Roles Anywhere.

Há cenários em que credenciais temporárias não são uma opção e talvez seja necessário usar credenciais de longo prazo. Nessas situações, faça auditoria e alterne as credenciais periodicamente e alterne as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo. Alguns exemplos que podem exigir credenciais de longo prazo incluem plug-ins do WordPress e clientes da AWS de terceiros. Em situações em que você precisa utilizar credenciais de longo prazo ou para credenciais que não sejam chaves de acesso da AWS, como logins de banco de dados, é possível usar um serviço projetado para lidar com o gerenciamento de segredos, como AWS Secrets Manager. O Secrets Manager torna simples gerenciar, alternar e armazenar com segurança segredos criptografados utilizando serviços compatíveis. Para ter mais informações sobre a alternância de credenciais de longo prazo, consulte Alternar chave de acesso.

Recursos

Práticas recomendadas relacionadas:

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

Documentos relacionados:

- Credenciais de segurança temporárias
- Credenciais da AWS
- Práticas recomendadas de segurança no IAM

- Perfis do IAM
- IAM Identity Center
- Provedores de identidades e federação
- Alternar chaves de acesso
- Soluções de parceiros de segurança: acesso e controle de acesso
- Usuário raiz da Conta da AWS

Vídeos relacionados:

- Gerenciar permissões de acesso em grande escala com o AWS IAM Identity Center (sucessor do AWS IAM Identity Center
- Dominar a identidade em todos os aspectos

SEC02-BP03 Armazenar e usar segredos com segurança

Uma workload exige um recurso automatizado para comprovar a identidade dela em bancos de dados, recursos e serviços de terceiros. Isso é realizado com o uso de credenciais de acesso secretas, como chaves de acesso de API, senhas e tokens do OAuth. Utilizar um serviço com propósito específico para armazenar, gerenciar e alternar essas credenciais ajuda a reduzir a probabilidade de comprometimento dessas credenciais.

Resultado desejado: implementar um mecanismo para gerenciar com segurança credenciais de aplicações que concretize os seguintes objetivos:

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

Antipadrões comuns:

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

Benefícios do estabelecimento desta prática recomendada:

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

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: alto

Orientação de implementação

Antes, as credenciais usadas para realizar a autenticação em bancos de dados, APIs de terceiros, tokens e outros segredos podiam ser incorporadas em código-fonte ou em arquivos do ambiente. A AWS oferece vários mecanismos para armazenar essas credenciais com segurança, alterná-las automaticamente e auditar o uso delas.

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

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

Alguns segredos duradouros podem não ser removidos ou substituídos. Esses segredos podem ser armazenados em um serviço, como o AWS Secrets Manager, no qual eles podem ser armazenados centralmente, gerenciados e alternados regularmente.

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

Credential type	Description	Suggested strategy
IAM access keys	AWS IAM access and secret keys used to assume IAM roles inside of a workload	Replace: Use Perfis do IAM assigned to the compute instances (such as Amazon EC2 or AWS Lambda) instead. For interoperability with third parties that require access to resources in your Conta da AWS, ask if they support Acesso entre contas da AWS. For mobile apps, consider using temporary credentials through Grupos de identidades (identidades federadas) do Amazon Cognito. For workloads running outside of AWS, consider IAM Roles Anywhere or AWS Systems Manager Hybrid Activations.
SSH keys	Secure Shell private keys used to log into Linux EC2 instances, manually or as part of an automated process	Replace: Use AWS Systems Manager or EC2 Instance Connect to provide programmatic and human access to EC2 instances using IAM roles.
Application and database credentials	Passwords – plain text string	Rotate: Store credentials in AWS Secrets Manager and

Credential type	Description	Suggested strategy
		establish automated rotation if possible.
Amazon RDS and Aurora Admin Database credentials	Passwords – plain text string	Replace: Use the Integração do Secrets Manager ao Amazon RDS or Amazon Aurora. In addition, some RDS database types can use IAM roles instead of passwords for some use cases (for more detail, see Autenticação de banco de dados do IAM).
OAuth tokens	Secret tokens – plain text string	Rotate: Store tokens in AWS Secrets Manager and configure automated rotation.
API tokens and keys	Secret tokens – plain text string	Rotate: Store in AWS Secrets Manager and establish automated rotation if possible.

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

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

O AWS Secrets Manager oferece cinco recursos principais para proteger o armazenamento e o processamento de credenciais sigilosas: criptografia em repouso, criptografia em trânsito, auditoria abrangente, controle de acesso detalhado e alternância de credenciais extensíveis. Outros serviços de gerenciamento de segredos de parceiros da AWS ou soluções desenvolvidas localmente que oferecem recursos e garantias semelhantes também são aceitáveis.

Etapas da implementação

1. Identifique caminhos de código que contenham credenciais codificadas usando ferramentas automatizadas, como o Amazon CodeGuru.
   - Utilize o Amazon CodeGuru para verificar seus repositórios de código. Depois de concluir a revisão, filtre `Type=Secrets` no CodeGuru para encontrar linhas de código problemáticas.
2. Identifique credenciais que possam ser removidas ou substituídas.
   a. Identifique credenciais não mais necessárias e marque-as para remoção.
   b. Para chaves secretas da AWS incorporadas ao código-fonte, substitua-as por perfis do IAM associados aos recursos necessários. Se parte de sua workload estiver fora do AWS, mas exigir credenciais do IAM para acessar recursos da AWS, considere o IAM Roles Anywhere ou o AWS Systems Manager Hybrid Activations.
3. Para outros terceiros, segredos duradouros que exijam o uso da estratégia de alternância, integre o Secrets Manager ao seu código para recuperar segredos de terceiros no tempo de execução.
   a. O console do CodeGuru pode criar um segredo automaticamente no Secrets Manager utilizando as credenciais descobertas.
   b. Integre a recuperação de segredos do Secrets Manager ao código de sua aplicação.
      - Funções do Lambda Sem Servidor podem usar uma extensão do Lambda independente de linguagem.
      - Para instâncias ou contêineres do EC2, a AWS oferece código do lado do cliente de exemplo para recuperar segredos do Secrets Manager em várias linguagens de programação conhecidas.
4. Revise periodicamente sua base de código e verifique novamente para confirmar se não há novos segredos adicionados ao código.
   - Considere usar uma ferramenta como o git-secrets para impedir a confirmação de novos segredos em seu repositório de código-fonte.
5. Monitore a atividade do Secrets Manager quanto a indicações de uso inesperado, acesso inadequado a segredos ou tentativas de excluir segredos.

6. Reduza a exposição humana às credenciais. Restrinja o acesso a credenciais de leitura, gravação e modificação a um perfil do IAM dedicado a esse fim, e apenas forneça acesso para assumir o perfil a um pequeno subconjunto de usuários operacionais.

Recursos

Práticas recomendadas relacionadas:

- SEC02-BP02 Usar credenciais temporárias
- SEC02-BP05 Fazer a auditoria e a alternância periódica das credenciais

Documentos relacionados:

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

Vídeos relacionados:

- Práticas recomendadas para gerenciar, recuperar e alternar segredos em grande escala
- Encontre segredos codificados com o Amazon CodeGuru Secrets Detector
- Proteger segredos para workloads híbridas usando o AWS Secrets Manager

Workshops relacionados:

- Armazenar, recuperar e gerenciar credenciais sigilosas no AWS Secrets Manager
- Ativações híbridas do AWS Systems Manager

SEC02-BP04 Contar com um provedor de identidades centralizado

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

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

Antipadrões comuns:

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

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

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

Orientação para implementação

Orientação para usuários da força de trabalho que acessam a AWS

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

- Para federar os usuários da sua força de trabalho diretamente com cada Conta da AWS, você pode usar um provedor de identidade centralizado para federar o AWS Identity and Access Management nessa conta. A flexibilidade do IAM permite que você habilite um SAML 2.0 ou um provedor de identidade Open ID Connect (OIDC) para cada Conta da AWS e use atributos de usuário federados para controle de acesso. Os usuários da sua força de trabalho usarão o navegador da web para fazer login no provedor de identidade fornecendo suas respectivas credenciais (como senhas e códigos de token MFA). O provedor de identidade emite uma declaração SAML para o navegador, que é enviada ao URL de login do AWS Management Console para permitir que o usuário faça autenticação única no AWS Management Console assumindo uma função do IAM. Seus usuários também podem obter credenciais temporárias de API da AWS para uso na AWS CLI ou em AWS SDKs pelo AWS STS assumindo a função do IAM usando uma declaração SAML do provedor de identidade.
- Para federar seus usuários da força de trabalho com várias contas em sua organização da AWS, você pode usar o AWS IAM Identity Center para gerenciar centralmente o acesso dos usuários de sua força de trabalho a Contas da AWS e aplicações. Você ativa o Centro de Identidade para sua organização e configura sua fonte de identidade. O IAM Identity Center fornece um diretório de origem de identidade padrão que você pode usar para gerenciar seus usuários e grupos. Como alternativa, você pode escolher uma fonte de identidade externa conectando-se ao seu provedor de identidade externo usando SAML 2.0 e provisionando automaticamente usuários e grupos usando o SCIM ou conectando-se ao diretório do Microsoft AD com o uso do AWS Directory Service. Depois que uma fonte de identidade é configurada, você pode atribuir acesso a usuários e grupos a Contas da AWS definindo políticas de privilégios mínimos em seus conjuntos de permissões. Os usuários da sua força de trabalho podem se autenticar por meio de seu provedor de identidade central para entrar no portal de acesso da AWS e autenticação única em Contas da AWS e aplicações em nuvem atribuídas a eles. Seus usuários podem configurar a AWS CLI v2

para se autenticar com o Centro de Identidade e obter credenciais para executar comandos da AWS CLI. O Centro de Identidade também permite acesso com autenticação única a aplicações da AWS, como o Amazon SageMaker Studio e portais do AWS IoT Sitewise Monitor.

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

Orientação para usuários de suas aplicações

Você pode gerenciar as identidades dos usuários de suas aplicações, como um aplicativo móvel, usando o Amazon Cognito como seu provedor de identidade centralizado. O Amazon Cognito permite autenticação, autorização e gerenciamento de usuários de seus aplicativos móveis e da web. O Amazon Cognito fornece um repositório de identidades que pode ser expandido para milhões de usuários, oferece suporte à federação de identidades sociais e corporativas e oferece recursos avançados de segurança para ajudar a proteger seus usuários e sua empresa. Você pode integrar seu aplicativo web ou móvel personalizado ao Amazon Cognito para adicionar autenticação de usuário e controle de acesso aos seus aplicativos em minutos. Desenvolvido com base em padrões de identidade abertos, como SAML e Open ID Connect (OIDC), o Amazon Cognito oferece suporte a vários regulamentos de conformidade e se integra aos recursos de desenvolvimento de front-end e back-end.

Etapas da implementação

Etapas para usuários da força de trabalho acessarem a AWS

- Federe os usuários da sua força de trabalho à AWS usando um provedor de identidade centralizado de acordo com uma das seguintes abordagens:
  - Use o IAM Identity Center para habilitar a autenticação única para várias Contas da AWS em sua organização da AWS, federando com seu provedor de identidade.

    - Use o IAM para conectar seu provedor de identidade diretamente a cada Conta da AWS, permitindo acesso federado refinado.
- Identifique e remova IAM users e grupos que são substituídos por identidades federadas.

Etapas para usuários de suas aplicações

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

Recursos

Práticas recomendadas relacionadas ao Well-Architected:

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

Documentos relacionados:

- Federação de identidades na AWS
- Práticas recomendadas de segurança no IAM
- Práticas recomendadas do AWS Identity and Access Management
- Introdução à administração delegada do IAM Identity Center
- Como usar políticas gerenciadas pelo cliente no IAM Identity Center para casos de uso avançados
- AWS CLI v2: provedor de credenciais do IAM Identity Center

Vídeos relacionados:

- AWS re:Inforce 2022 - AWS Identity and Access Management (IAM) deep dive (AWS re:Inforce 2022: aprofundamento no AWS Identity and Access Management (IAM))
- AWS re:Invent 2022 - Simplify your existing workforce access with IAM Identity Center (AWS re:Invent 2022: simplifique o acesso existente de sua força de trabalho com o IAM Identity Center)

- AWS re:Invent 2018: Mastering Identity at Every Layer of the Cake (AWS re:Invent 2018: dominar a identidade em todos os aspectos)

Exemplos relacionados:

- Workshop: Using AWS IAM Identity Center to achieve strong identity management (Uso do AWS IAM Identity Center para conseguir um forte gerenciamento de identidade)
- Workshop: Serverless identity (Identidade sem servidor)

Ferramentas relacionadas:

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

SEC02-BP05 Fazer a auditoria e a alternância periódica das credenciais

Audite e alterne as credenciais periodicamente para limitar o período durante o qual as credenciais podem ser usadas para acessar seus recursos. Credenciais de longo prazo criam muitos riscos, e estes podem ser reduzidos alternando credenciais de longo prazo regularmente.

Resultado desejado: implementar a alternância de credenciais para ajudar a reduzir os riscos associados ao uso de credenciais de longo prazo. Auditar e corrigir regularmente a não conformidade com políticas de alternância de credenciais.

Antipadrões comuns:

- Não auditar o uso de credenciais.
- Utilizar credenciais de longo prazo desnecessariamente.
- Utilizar credenciais de longo prazo e não alterná-las regularmente.

Nível de risco exposto se esta prática recomendada não é estabelecida: médio

Orientação de implementação

Quando você não puder contar com credenciais temporárias e exigir credenciais de longo prazo, faça uma auditoria das credenciais para garantir que os controles definidos, por exemplo,

autenticação multifator (MFA), sejam aplicados, alternados regularmente e que tenham o nível de acesso apropriado.

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

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

Etapas da implementação

- Fazer auditoria nas credenciais regularmente: a auditoria das identidades configuradas em seu provedor de identidades e no IAM ajuda a garantir que somente identidades autorizadas tenham acesso à sua workload. Essas identidades podem incluir, entre outros, usuários do IAM, do AWS IAM Identity Center, do Active Directory ou usuários em um provedor de identidades upstream diferente. Por exemplo, remova as pessoas que saem da organização e as funções entre contas que não são mais necessárias. Estabeleça um processo para auditar periodicamente as permissões para os serviços acessados por uma entidade do IAM. Isso ajuda a identificar as políticas que você precisa modificar a fim de remover todas as permissões não utilizadas. Use relatórios de credenciais e o AWS Identity and Access Management Access Analyzer para auditar credenciais e permissões do IAM. É possível utilizar o Amazon CloudWatch para configurar alarmes para chamadas de API específicas chamadas em seu ambiente da AWS. O Amazon GuardDuty também pode alertar você sobre atividade inesperada, que pode indicar acesso excessivamente permissivo ou acesso acidental às credenciais do IAM.
- Alternar credenciais regularmente: quando você não pode utilizar credenciais temporárias, alterne as chaves de acesso do IAM de longo prazo regularmente (no máximo, a cada 90 dias). Se uma chave de acesso for divulgada acidentalmente sem seu conhecimento, isso limitará o período de uso das credenciais para acessar seus recursos. Para ter informações sobre a alternância de chaves de acesso para usuários do IAM, consulte Alternar chaves de acesso.

- Revisar as permissões do IAM: para melhorar a segurança de sua Conta da AWS, revise e monitore regularmente cada uma das políticas do IAM. Verifique se as políticas seguem o princípio de privilégio mínimo.
- Considerar automatizar a criação e as atualizações dos recursos do IAM:o IAM Identity Center automatiza muitas tarefas do IAM, como o gerenciamento de perfis e políticas. Como alternativa, o AWS CloudFormation pode ser usado para automatizar a implantação de recursos do IAM, como perfis e políticas, para reduzir a chance de erros humanos, pois os modelos podem ser verificados e ter controle de versão.
- Utilizar o IAM Roles Anywhere para substituir os usuários do IAM para identidades de máquina: o IAM Roles Anywhere possibilita usar perfis em áreas onde não seria possível tradicionalmente, como em servidores on-premises. O IAM Roles Anywhere utiliza um certificado X.509 confiável para realizar a autenticação na AWS e receber credenciais temporárias. O uso do IAM Roles Anywhere evita a necessidade de alternar essas credenciais, pois credenciais de longo prazo não são mais armazenadas em seu ambiente on-premises. Você precisará monitorar e alternar o certificado X.509 ao aproximar-se da validade.

Recursos

Práticas recomendadas relacionadas:

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

Documentos relacionados:

- Conceitos básicos do AWS Secrets Manager
- Práticas recomendadas do IAM
- Provedores de identidades e federação
- Soluções de parceiros de segurança: acesso e controle de acesso
- Credenciais de segurança temporárias
- Obter relatórios de credenciais da sua Conta da AWS

Vídeos relacionados:

- Práticas recomendadas para gerenciar, recuperar e alternar segredos em grande escala

- Gerenciar permissões de usuário em grande escala com o AWS IAM Identity Center
- Dominar a identidade em todos os aspectos

Exemplos relacionados:

- Well-Architected Lab: Limpeza automatizada de usuários do IAM
- Well-Architected Lab: Implantação automatizada de grupos e perfis do IAM

SEC02-BP06 Utilizar grupos e atributos de usuários

À medida que o número de usuários gerenciados cresce, você precisará determinar maneiras de organizá-los para que você possa gerenciá-los em grande escala. Coloque usuários com requisitos de segurança comuns em grupos definidos pelo provedor de identidade e implemente mecanismos para garantir que os atributos de usuário que podem ser usados para controle de acesso (por exemplo, departamento ou localização) estejam corretos e atualizados. Use esses grupos e atributos para controlar o acesso em vez de usuários individuais. Isso permite que você gerencie o acesso centralmente, alterando a associação ao grupo ou os atributos de um usuário uma vez com um conjunto de permissões, em vez de atualizar várias políticas individuais quando as necessidades de acesso de um usuário mudarem. Você pode usar o AWS IAM Identity Center (IAM Identity Center) para gerenciar grupos e atributos de usuários. O IAM Identity Center oferece suporte aos atributos mais usados, quer eles sejam inseridos manualmente durante a criação do usuário ou provisionados automaticamente usando um mecanismo de sincronização, como definido na especificação System for Cross-Domain Identity Management (SCIM).

Coloque usuários com requisitos de segurança comuns em grupos definidos pelo provedor de identidade e implemente mecanismos para garantir que os atributos de usuário que podem ser usados para controle de acesso (por exemplo, departamento ou localização) estejam corretos e atualizados. Use esses grupos e atributos, em vez de usuários individuais, para controlar o acesso. Com isso, você pode gerenciar o acesso centralmente. Basta alterar uma vez a associação ou os atributos do grupo de um usuário. Ou seja, não será preciso atualizar muitas políticas individuais quando as necessidades de acesso de um usuário mudarem.

Nível de exposição a riscos quando esta prática recomendada não for estabelecida: Baixo

Orientações para a implementação

- Se estiver usando o AWS IAM Identity Center (IAM Identity Center), configure grupos: o IAM Identity Center permite configurar grupos de usuários e atribuir aos grupos o nível desejado de permissão.
  - AWS Single Sign-On: gerenciar identidades
- Saiba mais sobre o controle de acesso por atributo (ABAC): o ABAC é uma estratégia de autorização que define permissões com base em atributos.
  - O que é ABAC para a AWS?
  - Laboratório: Controle de acesso baseado em tags do IAM para o EC2

Recursos

Documentos relacionados:

- Conceitos básicos do AWS Secrets Manager
- Práticas recomendadas do IAM
- Provedores de identidade e federação
- O usuário raiz da conta da AWS

Vídeos relacionados:

- Best Practices for Managing, Retrieving, and Rotating Secrets at Scale (Práticas recomendadas para gerenciar, recuperar e alternar segredos em grande escala)
- Managing user permissions at scale with AWS IAM Identity Center (Gerenciar permissões de usuário em grande escala com o AWS SSO)
- Mastering identity at every layer of the cake

Exemplos relacionados:

- Laboratório: Controle de acesso baseado em tags do IAM para o EC2

Gerenciamento de permissões

Gerencie permissões para controlar o acesso a identidades de humanos e máquinas que precisam de acesso à AWS e à suas workloads. As permissões controlam quem pode acessar o quê e em quais condições. Defina permissões para identidades humanas e de máquina específicas para conceder acesso a ações de serviço específicas em recursos específicos. Além disso, especifique condições que devem ser verdadeiras para que o acesso seja concedido. Por exemplo, você pode permitir que os desenvolvedores criem novas funções do Lambda, mas apenas em uma Região específica. Ao gerenciar seus ambientes da AWS em escala, siga as práticas recomendadas a seguir para garantir que as identidades tenham apenas o acesso de que precisam e nada mais.

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

Políticas baseadas em identidade no IAM são gerenciadas ou em linha, e se agregam a identidades do IAM, incluindo usuários, grupos e funções. Essas políticas permitem especificar o que essa identidade pode fazer (permissões). As políticas baseadas em identidade podem ser subdivididas em outras categorias.

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

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

As políticas gerenciadas são o método preferencial para aplicar permissões. No entanto, também é possível usar políticas em linha adicionadas diretamente a um único usuário, grupo ou função. As políticas em linha mantêm uma relação um para um estrita entre uma política e uma identidade. As políticas em linha são excluídas quando você exclui a identidade.

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

Políticas baseadas em recursos são anexadas ao recurso. Por exemplo, uma política de bucket do S3 é uma política baseada em recursos. Essas políticas concedem permissão a uma entidade principal que pode estar na mesma conta que o recurso ou em outra conta. Para obter uma lista de

serviços que oferecem suporte a políticas baseadas em recursos, consulte AWS services that work with IAM (Serviços da AWS que funcionam com IAM).

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

Controle de acesso baseado em atributos (ABAC) permite que você conceda permissões com base em atributos. Na AWS, elas são chamadas de tags. As tags podem ser anexadas a entidades principais (usuários ou funções) do IAM e a recursos da AWS. Usando políticas do IAM, os administradores podem criar uma política reutilizável que aplique permissões com base nos atributos da entidade principal do IAM. Por exemplo, como administrador, você pode usar uma única política do IAM que concede aos desenvolvedores em sua organização acesso a recursos da AWS que correspondam às tags de projeto dos desenvolvedores. À medida que a equipe de desenvolvedores adiciona recursos aos projetos, as permissões são aplicadas automaticamente com base em atributos. Como resultado, nenhuma atualização de política é necessária para cada novo recurso.

Políticas de controle de serviço (SCP) definem as permissões máximas para membros da conta de uma organização ou unidade organizacional (UO). As SCPs limitam as permissões que as políticas baseadas em identidade ou as políticas baseadas em recursos concedem a entidades (usuários ou funções) dentro da conta, mas não concedem permissões.

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

Práticas recomendadas

- SEC03-BP01 Definir requisitos de acesso
- SEC03-BP02 Conceder acesso com privilégio mínimo
- SEC03-BP03 Estabelecer processo de acesso de emergência
- SEC03-BP04 Reduzir as permissões continuamente
- SEC03-BP05 Definir barreiras de proteção de permissões para sua organização
- SEC03-BP06 Gerenciar o acesso com base no ciclo de vida

- SEC03-BP07 Analisar o acesso público e entre contas
- SEC03-BP08 Compartilhar recursos com segurança em sua organização
- SEC03-BP09 Compartilhar recursos com segurança com terceiros

SEC03-BP01 Definir requisitos de acesso

Cada componente ou recurso de sua workload precisa ser acessado por administradores, usuários finais ou outros componentes. É necessário ter uma definição clara de quem ou do que deve ter acesso a cada componente, escolher o tipo de identidade apropriado e o método de autenticação e autorização.

Antipadrões comuns:

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

Nível de risco exposto se essa prática recomendada não for estabelecida: alto

Orientação para implementação

Cada componente ou recurso de sua workload precisa ser acessado por administradores, usuários finais ou outros componentes. É necessário ter uma definição clara de quem ou do que deve ter acesso a cada componente, escolher o tipo de identidade apropriado e o método de autenticação e autorização.

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

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

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

Você pode usar o AWS Identity and Access Management Roles Anywhere para obter credenciais de segurança temporárias no IAM para workloads executadas fora da AWS. As workloads podem usar as mesmas políticas do IAM e perfis do IAM que você usa com as aplicações da AWS para acessar os recursos da AWS.

Quando possível, prefira credenciais temporárias de curta duração em vez de credenciais estáticas de longa duração. Para cenários em que você precisa de usuários da IAM com acesso programático e credenciais de longa duração, use as últimas informações usadas da chave de acesso para alternar e remover chaves de acesso.

Recursos

Documentos relacionados:

- Controle de acesso por atributo (ABAC)
- AWS IAM Identity Center
- IAM Roles Anywhere
- AWS Managed policies for IAM Identity Center (Políticas gerenciadas pela AWS para o IAM Identity Center)
- AWS IAM policy conditions (Condições de políticas do AWS IAM)
- IAM use cases (Casos de uso do IAM)
- Remova credenciais desnecessárias
- Trabalhando com políticas
- How to control access to AWS resources based on Conta da AWS, OU, or organization (Como controlar o acesso aos recursos da AWS baseados em Conta da AWS, UO ou organização)
- Identify, arrange, and manage secrets easily using enhanced search in AWS Secrets Manager (Identificar, organizar e gerenciar segredos facilmente usando a pesquisa avançada no AWS Secrets Manager)

Vídeos relacionados:

- Become an IAM Policy Master in 60 Minutes or Less (Torne-se um mestre em políticas do IAM em 60 minutos ou menos)
- Separation of Duties, Least Privilege, Delegation, and CI/CD (Separação de tarefas, privilégio mínimo, delegação e CI/CD)
- Streamlining identity and access management for innovation (Simplificação do gerenciamento de identidade e acesso para inovação)

SEC03-BP02 Conceder acesso com privilégio mínimo

É prática recomendada conceder somente o acesso de que as identidades precisam para realizar ações em recursos específicos e sob condições específicas. Use grupos e atributos de identidade para definir permissões dinamicamente em escala, em vez de definir permissões para usuários individuais. Por exemplo, você pode permitir o acesso de um grupo de desenvolvedores para gerenciar apenas recursos de seu próprio projeto. Dessa forma, se um desenvolvedor sair do projeto, o acesso dele é automaticamente revogado sem alterar as políticas de acesso adjacentes.

Resultado desejado: os usuário somente têm permissões necessárias para fazerem seus respectivos trabalhos. Os usuários devem ter acesso apenas a ambientes de produção para realizar uma tarefa específica dentro de um período limitado e o acesso deve ser revogado quando a tarefa for concluída. As permissões devem ser revogadas quando não forem mais necessárias, incluindo quando um usuário for para um projeto diferente ou mudar de cargo. Privilégios de administrador devem ser concedidos apenas a um grupo pequeno de administradores confiáveis. As permissões devem ser revistas regularmente para evitar desvios de permissão. Contas de máquina ou sistema devem ter apenas o mínimo de permissões necessárias para concluir as tarefas.

Antipadrões comuns:

- Usar como padrão a concessão de permissões de administrador aos usuários.
- Usar o usuário raiz para atividades diárias.
- Criar políticas permissivas demais, mas sem privilégios completos de administrador.
- Não revisar as permissões para entender se elas permitem o acesso de privilégio mínimo.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: alto

Orientações para a implementação

O princípio de estados privilégio mínimo para as identidades deve ser apenas permitido para realizar o mínimo de ações necessárias para cumprir uma tarefa específica. Isso equilibra a usabilidade, eficiência e segurança. Operar sobre esse princípio ajuda a limitar acesso não intencional e a rastrear quem tem acesso a quais recursos. Usuários e perfis do IAM não têm permissões por padrão. O usuário raiz tem acesso total e deve ser controlado e monitorado rigidamente, além de usado apenas para tarefas que necessitam acesso raiz.

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

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

Você também pode controlar as solicitações feitas pelos serviços da AWS em seu nome, como a criação, pelo AWS CloudFormation, de uma função do AWS Lambda, usando a chave de condição `CalledVia`. Tipos diferentes de política devem estar em camadas para estabelecer a defesa em profundidade e limitar as permissões gerais de seus usuários. Você pode restringir as permissões que podem ser concedidas e sob quais condições. Por exemplo, você pode permitir que suas equipes de aplicação criem suas próprias políticas do IAM para os sistemas que criam, mas deve também aplicar uma Fronteira de permissão para limitar o máximo de permissões que o sistema pode receber.

Etapas da implementação

- Implementar políticas de privilégio mínimo: atribua políticas de acesso com privilégio mínimo a grupos e perfis do IAM para refletir a função ou o perfil do usuário que você definiu.
  - Basear as políticas no uso da API: uma maneira de determinar as permissões necessárias é analisar os logs do AWS CloudTrail. Essa análise permite que você crie permissões personalizadas para as ações do usuário dentro da AWS. O IAM Access Analyzer pode gerar automaticamente uma IAM política com base na atividade. Você pode usar o IAM Access Advisor no nível da organização ou da conta para rastrear as últimas informações acessadas para determinada política.

- Considerar o uso de políticas gerenciadas da AWS para cargos. Pode ser difícil saber por onde começar ao criar políticas de permissões mais estritas. A AWS gerencia políticas para cargos comuns, como faturamento, administradores de banco de dados e cientistas de dados. Essas políticas podem ajudar a diminuir o acesso dos usuários ao determinar como implementar as políticas de privilégio mínimo.
- Remover permissões desnecessárias: remova permissões que não são necessárias e ajuste políticas muito permissivas. A geração de política pelo IAM Access Analyzer pode ajudar a ajustar as políticas de permissão.
- Garantir que os usuários tenham acesso limitado a ambientes de produção: os usuários devem ter acesso a ambientes de produção apenas com um caso de uso válido. Depois de o usuário realizar as tarefas específicas para as quais foi necessário o acesso à produção, o acesso deve ser revogado. Limitar o acesso a ambientes de produção evita eventos não intencionais e que causam impacto à produção, além de diminuir o escopo do impacto do acesso não intencional.
- Considerar os limites de permissões: um limite de permissões é um recurso para usar uma política gerenciada que define o número máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM. O limite de permissões de uma entidade permite que ela execute apenas as ações aceitas por suas políticas baseadas em identidade e seus limites de permissões.
- Considerar tags de recursos para permissões: um modelo de controle de acesso baseado em atributo que usa tags de recursos permite conceder acesso com base no propósito do recurso, proprietário, ambiente ou outros critérios. Por exemplo, você pode usar tags de recurso para diferenciar entre ambientes de desenvolvimento e produção. Ao usar essas tags, é possível restringir os desenvolvedores ao ambiente de desenvolvimento. Ao combinar as tags e as políticas de permissões, você consegue alcançar um acesso restrito ao recurso sem precisar definir políticas complicadas e personalizadas para cada cargo.
- Use políticas de controle de serviço para AWS Organizations. As políticas de controle de serviço controlam centralmente o máximo de permissões disponíveis para contas de membros em sua organização. É importante notar que as políticas de controle de serviço permitem que você restrinja as permissões do usuário raiz nas contas de membros. Considere também o uso do AWS Control Tower, que fornece controles gerenciados prescritivos que enriquecem o AWS Organizations. Também é possível definir os seus próprios controles no Control Tower.
- Estabelecer uma política de ciclo de vida para sua organização: as políticas de ciclo de vida do usuário definem tarefas a serem realizadas quando os usuários entram na AWS, mudam de cargo ou escopo de trabalho ou não precisam mais de acesso à AWS. As análises de permissão devem

ser feitas durante todas as etapas do ciclo de vida do usuário para verificar se as permissões estão adequadamente restritas e para evitar desvios nas permissões.

- Estabelecer uma programação regular para rever as permissões e remover as permissões desnecessárias: frequentemente, você deve verificar o acesso do usuário para garantir que ele não tenha acesso muito permissivo. O AWS Config e o IAM Access Analyzer podem ajudar ao auditar as permissões do usuário.
- Estabelecer uma matriz de cargos: uma matriz de cargos exibe os diversos cargos e níveis de acesso necessários dentro de sua área da AWS. Com uma matriz de cargos, você pode definir e separar as permissões com base nas responsabilidades do usuário dentro da sua organização. Use grupos em vez de aplicar permissões diretamente a usuários ou cargos individuais.

Recursos

Documentos relacionados:

- Conceder privilégio mínimo
- Permissions boundaries for IAM entities (Limites de permissões para entidades do IAM)
- Techniques for writing least privilege IAM policies (Técnicas para escrever políticas do IAM de privilégio mínimo)
- IAM Access Analyzer makes it easier to implement least privilege permissions by generating IAM policies based on access activity (IAM Access Analyzer facilita a implementação de permissões de privilégio mínimo gerando políticas do IAM baseadas na atividade de acesso)
- Delegate permission management to developers by using IAM permissions boundaries (Delegar gerenciamento de permissões para desenvolvedores usando os limites de permissões do IAM)
- Refining Permissions using last accessed information (Refinar permissões usando as últimas informações acessadas)
- IAM policy types and when to use them (Tipos de política do IAM e quando usá-las)
- Testing IAM policies with the IAM policy simulator (Testar políticas do IAM com o simulador de política do IAM)
- Guardrails in AWS Control Tower (Barreiras de proteção no AWS Control Tower)
- Zero Trust architectures: An AWS perspective (Arquiteturas de confiança zero: uma perspectiva da AWS)
- How to implement the principle of least privilege with CloudFormation StackSets (Como implementar o princípio de privilégio mínimo com o CloudFormation StackSets)

- Controle de acesso baseado em atributos (ABAC)
- Redução do escopo da política ao exibir a atividade do usuário
- Visualizar acesso do cargo
- Use a marcação para organizar seu ambiente e gerar responsabilidade
- Estratégias de marcação da AWS
- Marcação de recursos da AWS

Vídeos relacionados:

- Next-generation permissions management (Gerenciamento de permissões de última geração)
- Zero Trust: An AWS perspective (Confiança zero: uma perspectiva da AWS)
- How can I use permissions boundaries to limit users and roles to prevent privilege escalation? (Como posso usar limites de permissões para limitar usuários e funções e evitar escalação do privilégio?)

Exemplos relacionados:

- Lab: IAM permissions boundaries delegating role creation (Laboratório: limites de permissões do IAM que delegam a criação de perfis)
- Lab: IAM tag based access control for EC2 (Laboratório: controle de acesso baseado em tags do IAM para EC2)

SEC03-BP03 Estabelecer processo de acesso de emergência

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

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

configuração de federação ou workloads. O processo de acesso de emergência é usado até que o mecanismo normal de federação seja restaurado.

Resultado desejado:

- Você definiu e documentou os modos de falha que são considerados uma emergência: considere suas circunstâncias normais e os sistemas dos quais seus usuários dependem para gerenciar suas workloads. Pense em como cada uma dessas dependências pode falhar e causar uma situação de emergência. Você pode encontrar as perguntas e as práticas recomendadas no Pilar Confiabilidade útil para identificar modos de falha e arquitetar sistemas mais resilientes com o objetivo de minimizar a probabilidade de falhas.
- Você documentou as etapas que devem ser seguidas para confirmar uma falha como emergência. Por exemplo, é possível exigir que os administradores de identidade confiram o status de seus provedores de identidade primário e de reserva e, se nenhum dos dois estiver disponível, declarar um evento de emergência por falha do provedor de identidades.
- Você definiu um processo de acesso de emergência específico de cada tipo de modo de emergência ou falha. Ser específico pode reduzir a tentação de seus usuários de abusar de um processo geral para todos os tipos de emergência. Seus processos de acesso de emergência descrevem as circunstâncias em que cada processo deve ser usado e, inversamente, as situações em que o processo não deve ser usado e apontam para processos alternativos que podem ser aplicados.
- Seus processos são bem documentados com instruções detalhadas e manuais que podem ser seguidos com rapidez e eficiência. Lembre-se de que um evento de emergência pode ser um momento estressante para os usuários e eles podem estar sob extrema pressão de tempo, portanto, projete o processo para ser o mais simples possível.

Antipadrões comuns:

- Você não tem processos de acesso de emergência bem documentados e bem testados. Os usuários não estão preparados para uma emergência e seguem processos improvisados quando surge um evento de emergência.
- Seus processos de acesso de emergência dependem dos mesmos sistemas (como um provedor de identidades centralizado) que seus mecanismos de acesso normais. Isso significa que a falha desse sistema pode afetar os mecanismos de acesso normal e de emergência e prejudicar sua capacidade de se recuperar da falha.

- Seus processos de acesso de emergência são usados em situações não emergenciais. Por exemplo, os usuários frequentemente usam de forma indevida os processos de acesso de emergência, pois acham mais fácil fazer alterações diretamente do que enviá-las por meio de um pipeline.
- Seus processos de acesso de emergência não geram logs suficientes para auditar os processos, ou os logs não são monitorados para alertar sobre o possível uso indevido dos processos.

Benefícios de estabelecer esta prática recomendada:

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

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

Orientação para implementação

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

Orientação comum para todos os modos de falha

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

- Documente as pré-condições e as suposições do processo: quando o processo deve ou não ser usado. Isso ajuda a detalhar o modo de falha e documentar suposições, como o estado de outros sistemas relacionados. Por exemplo, o processo do Modo de falha 2 pressupõe que o provedor de identidades está disponível, mas a configuração na AWS foi modificada ou expirou.
- Pré-crie os recursos necessários para o processo de acesso de emergência (SEC10-BP05). Por exemplo, crie previamente a Conta da AWS de acesso de emergência com IAM users e perfis e os perfis entre contas do IAM em todas as contas da workload. Isso verifica se esses recursos estão prontos e disponíveis quando ocorre um evento de emergência. Ao pré-criar recursos, você não depende das APIs do ambiente de gerenciamento da AWS (usadas para criar e modificar recursos

da AWS) que podem ficar indisponíveis em caso de emergência. Além disso, ao pré-criar recursos do IAM, você não precisa contabilizar possíveis atrasos devido à eventual consistência.

- Inclua processos de acesso de emergência como parte dos planos de gerenciamento de incidentes (SEC10-BP02). Documente como os eventos de emergência são acompanhados e comunicados a outras pessoas na organização, como equipes de colegas, sua liderança e, quando aplicável, externamente a seus clientes e parceiros de negócios.
- Defina o processo de solicitação de acesso de emergência no sistema de fluxo de trabalho de solicitação de serviço existente, caso haja um. Normalmente, esses sistemas de fluxo de trabalho permitem criar formulários de admissão para coletar informações sobre a solicitação, acompanhar a solicitação em cada estágio do fluxo de trabalho e adicionar etapas de aprovação automatizadas e manuais. Relacione cada solicitação a um evento de emergência correspondente acompanhado no sistema de gerenciamento de incidentes. Ter um sistema uniforme para acessos de emergência permite que você acompanhe essas solicitações em um único sistema, analise as tendências de uso e melhore os processos.
- Verifique se os processos de acesso de emergência só podem ser iniciados por usuários autorizados e exigem aprovações dos colegas ou da gerência do usuário, conforme apropriado. O processo de aprovação deve operar de forma eficaz dentro e fora do horário comercial. Defina como as solicitações de aprovação permitirão aprovadores secundários se os aprovadores primários não estiverem disponíveis e forem encaminhadas para a cadeia de gerenciamento até serem aprovadas.
- Verifique se o processo gera logs e eventos de auditoria detalhados para tentativas bem-sucedidas e fracassadas de obter acesso de emergência. Monitore o processo de solicitação e o mecanismo de acesso de emergência para detectar uso indevido ou acessos não autorizados. Correlacione a atividade com eventos de emergência contínuos do sistema de gerenciamento de incidentes e alerte quando as ações ocorrerem fora dos períodos esperados. Por exemplo, você deve monitorar e alertar sobre atividades na Conta da AWS de acesso de emergência, pois ela nunca deve ser usada em operações normais.
- Teste os processos de acesso de emergência periodicamente para verificar se as etapas estão claras e garantir o nível correto de acesso com rapidez e eficiência. Os processos de acesso de emergência devem ser testados como parte das simulações de resposta a incidentes (SEC10-BP07) e testes de recuperação de desastres (REL13-BP03).

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

Conforme descrito em SEC02-BP04 Contar com um provedor de identidades centralizado, recomendamos confiar em um provedor de identidades centralizado para federar os usuários de

sua força de trabalho e conceder acesso a Contas da AWS. Você pode federar em várias Contas da AWS na organização da AWS usando o IAM Identity Center ou federar em Contas da AWS individuais usando o IAM. Nos dois casos, os usuários da força de trabalho se autenticam com seu provedor de identidades centralizado antes de serem redirecionados a um endpoint de login da AWS para SSO.

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

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

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

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

- Você pode pré-criar um conjunto de IAM users para seus administradores de emergência na conta de acesso de emergência com senhas fortes e tokens de MFA associados. Esses IAM users têm permissões para assumir os perfis do IAM que permitem o acesso entre contas à Conta da AWS onde o acesso de emergência é necessário. Recomendamos criar o menor número possível de usuários e atribuir cada um a um único administrador de emergência. Durante uma emergência, um usuário administrador de emergência entra na conta de acesso de emergência usando sua senha e código de token MFA, muda para a função do IAM de acesso de emergência na conta de emergência e, por fim, muda para a função do IAM de acesso de emergência na conta da

workload para realizar a ação de alteração de emergência. A vantagem dessa abordagem é que cada IAM user é atribuído a um administrador de emergência, e você pode saber qual usuário fez login analisando os eventos do CloudTrail. A desvantagem é que você precisa manter vários IAM users com as respectivas senhas de longa duração e tokens de MFA associados.

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

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

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

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

Nesse evento de emergência, você pode fornecer aos seus administradores de identidade acesso à AWS para resolver os problemas de federação. Por exemplo, seu administrador de identidade usa o processo de acesso de emergência para fazer login na Conta da AWS de acesso de emergência, muda para um perfil na conta de administrador do Centro de Identidade e atualiza a configuração do

provedor de identidades externo importando o documento XML de metadados SAML mais recente do provedor de identidades para reativar a federação. Depois que a federação for corrigida, os usuários da sua força de trabalho continuarão usando o processo operacional normal para federar em suas contas da workload.

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

Modo de falha 3: interrupção do Centro de Identidade

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

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

Etapas da implementação

Etapas comuns para todos os modos de falha

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

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

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

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

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

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

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

Recursos

Práticas recomendadas relacionadas ao Well-Architected:

- SEC02-BP04 Contar com um provedor de identidades centralizado
- SEC03-BP02 Conceder acesso com privilégio mínimo
- SEC10-BP02 Desenvolver planos de gerenciamento de incidentes
- SEC10-BP07 Promover dias de jogo

Documentos relacionados:

- Configurar o acesso de emergência ao AWS Management Console
- Permitir que usuários federados do SAML 2.0 acessem o AWS Management Console
- Acesso de emergência

Vídeos relacionados:

- AWS re:Invent 2022 - Simplify your existing workforce access with IAM Identity Center
- AWS re:Inforce 2022 - AWS Identity and Access Management (IAM) deep dive

Exemplos relacionados:

- Perfil de acesso de emergência da AWS
- AWS customer playbook framework
- AWS incident response playbook samples

SEC03-BP04 Reduzir as permissões continuamente

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

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

Antipadrões comuns:

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

Nível de risco exposto se esta prática recomendada não é estabelecida: médio

Orientação de implementação

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

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

Etapas da implementação

- Utilizar o AWS Identity and Access Management Access Analyzer: o IAM Access Analyzer ajuda a identificar os recursos na organização e nas contas, como buckets do Amazon Simple Storage Service (Amazon S3) ou perfis do IAM, que são compartilhados com uma entidade externa.
- Utilizar a geração de políticas do IAM Access Analyzer: a geração de políticas do IAM Access Analyzer ajuda você a criar políticas de permissão detalhadas com base em um usuário do IAM ou na atividade de acesso de um perfil.
- Determinar um cronograma e uma política de uso aceitáveis para usuários e perfis do IAM: utilize o carimbo de data e hora de último acesso para identificar usuários e perfis não utilizados e removê-los. Revise as informações de serviço e ação acessadas mais recentemente para identificar e definir o escopo das permissões para usuários e perfis específicos. Por exemplo, você pode usar as informações acessadas mais recentemente para identificar as ações específicas do Amazon S3 exigidas pelo perfil da aplicação e restringir o acesso do perfil apenas a essas ações. Os recursos de informações acessadas mais recentemente estão disponíveis no AWS Management

Console e de maneira programática para permitir que você os incorpore aos fluxos de trabalho de infraestrutura e ferramentas automatizadas.

- Considerar o registro em log dos eventos de dados no AWS CloudTrail: por padrão, o CloudTrail não registra eventos de dados, como atividade em nível de objeto do Amazon S3 (por exemplo, `GetObject` e `DeleteObject`) ou atividades de tabelas do Amazon DynamoDB (por exemplo, `PutItem` e `DeleteItem`). Considere ativar o registro em log desses eventos para determinar quais usuários e perfis precisam acessar objetos do Amazon S3 ou itens de tabelas do DynamoDB específicos.

Recursos

Documentos relacionados:

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

Vídeos relacionados:

- Torne-se um mestre em políticas do IAM em 60 minutos ou menos
- Separação de tarefas, privilégio mínimo, delegação e CI/CD
- AWS re:Inforce 2022: Aprofundamento no AWS Identity and Access Management (IAM)

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

Estabeleça controles comuns que restrinjam o acesso a todas as identidades na organização. Por exemplo, é possível restringir o acesso a Regiões da AWS específicas ou impedir que os operadores excluam recursos comuns, como um perfil do IAM usado pela equipe de segurança central.

Antipadrões comuns:

- Execução de workloads em sua conta de administrador organizacional.
- Execução de workloads de produção e não produção na mesma conta.

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

Orientação para implementação

Com a expansão e o gerenciamento de workloads adicionais na AWS, você deve separá-las usando contas e gerenciá-las usando o AWS Organizations. Recomendamos que você estabeleça barreiras de proteção de permissões comuns que restrinjam o acesso a todas as identidades na sua organização. Por exemplo, você pode restringir o acesso a Regiões da AWS específicas ou impedir que a equipe exclua recursos comuns, como um perfil do IAM usado pela equipe de segurança central.

Você pode começar implementando exemplos de políticas de controle de serviço, como impedir que os usuários desabilitem os principais serviços. As SCPs usam a linguagem de políticas do IAM e permitem que você estabeleça controles aos quais todas as entidades principais (usuários e perfis) do IAM aderem. Você pode restringir o acesso a ações de serviço, recursos específicos e com base em condições específicas para atender às necessidades de controle de acesso de sua organização. Se necessário, você pode definir exceções para suas barreiras de proteção. Por exemplo, você pode restringir ações de serviço para todas as entidades do IAM na conta, exceto para um perfil de administrador específico.

Recomendamos evitar a execução de workloads em sua conta de gerenciamento. A conta de gerenciamento deve ser usada para gerir e implantar barreiras de proteção de segurança que afetarão as contas-membro. Alguns serviços da AWS permitem o uso de uma conta de administrador delegada. Quando disponível, você deve usar essa conta delegada em vez da conta de gerenciamento. Você deve limitar estritamente o acesso à conta de administrador organizacional.

O uso de uma estratégia de várias contas permite ter maior flexibilidade na aplicação de barreiras de proteção às suas workloads. O AWS Security Reference Architecture dá orientações prescritivas sobre como projetar a estrutura da conta. Os serviços da AWS, como o AWS Control Tower, fornece recursos para gerenciar centralmente os controles de prevenção e detecção em sua organização. Defina um objetivo claro para cada conta ou UO em sua organização e limite os controles de acordo com esse objetivo.

Recursos

Documentos relacionados:

- AWS Organizations
- Service control policies (SCPs) (Políticas de controle de serviços (SCPs))
- Get more out of service control policies in a multi-account environment (Aproveite ao máximo as políticas de controle de serviços em um ambiente de várias contas)
- AWS Security Reference Architecture (AWS SRA)

Vídeos relacionados:

- Enforce Preventive Guardrails using Service Control Policies (Aplique barreiras de proteção preventivas usando políticas de controle de serviços)
- Building governance at scale with AWS Control Tower (Criação de governança em escala com o AWS Control Tower)
- AWS Identity and Access Management deep dive (Análise aprofundada do AWS Identity and Access Management)

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

Integre controles de acesso ao ciclo de vida do operador e da aplicação e ao seu provedor de federação centralizado. Por exemplo, remova o acesso do usuário que sair da organização ou mudar de funções.

À medida que você gerencia cargas de trabalho usando contas separadas, haverá casos em que você precisará compartilhar recursos entre essas contas. Recomendamos que você compartilhe recursos usando o AWS Resource Access Manager (AWS RAM). Esse serviço permite que você compartilhe, com facilidade e segurança, os recursos da AWS dentro da AWS Organizations e das unidades organizacionais. Usando o AWS RAM, o acesso a recursos compartilhados é concedido ou revogado automaticamente à medida que as contas são movidas para dentro e para fora da organização ou da unidade organizacional com a qual são compartilhadas. Isso ajuda a garantir que os recursos sejam compartilhados apenas com as contas que você determinar.

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

Orientação de implementação

Ciclo de vida de acesso de usuário: implemente uma política de ciclo de vida de acesso para novos usuários, alterações de função de trabalho e usuários que saem, para que apenas os usuários atuais tenham acesso.

Recursos

Documentos relacionados:

- AttributeControle de acesso baseado em atributos (ABAC)
- Grant least privilege
- IAM Access Analyzer
- Remova credenciais desnecessárias
- Trabalhando com políticas

Vídeos relacionados:

- Become an IAM Policy Master in 60 Minutes or Less (Torne-se um mestre em políticas do IAM em 60 minutos ou menos)
- Separation of Duties, Least Privilege, Delegation, and CI/CD (Separação de tarefas, privilégio mínimo, delegação e CI/CD)

SEC03-BP07 Analisar o acesso público e entre contas

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

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

Antipadrões comuns:

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

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: baixo

Orientação de implementação

Se a sua conta estiver no AWS Organizations, você poderá conceder acesso aos recursos à toda a organização, a unidades organizacionais específicas ou a contas individuais. Se sua conta não for

membro de uma organização, você poderá compartilhar recursos com contas individuais. Você pode conceder acesso direto entre contas usando políticas baseadas em recursos, por exemplo, políticas de buckets do Amazon Simple Storage Service (Amazon S3) ou permitindo que uma identidade principal em outra conta assuma um perfil do IAM em sua conta. Ao utilizar políticas de recursos, verifique se o acesso é concedido apenas a entidades principais autorizadas. Defina um processo para aprovar todos os recursos que devem ser acessíveis publicamente.

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

O AWS Config pode relatar recursos configurados incorretamente, e por meio de verificações de politica do AWS Config, pode detectar recursos que tenham acesso público configurado. Serviços, como AWS Control Tower e AWS Security Hub simplificam a implantação de controles de detecção e barreiras de proteção nos AWS Organizations para identificar e corrigir recursos publicamente expostos. Por exemplo, o AWS Control Tower tem uma barreira de proteção gerenciada que pode detectar se algum snapshot do Amazon EBS é restaurado por Contas da AWS.

Etapas da implementação

- Pensar em ativar o AWS Config para AWS Organizations: o AWS Config permite que você agregue as descobertas de várias contas em um AWS Organizations em uma conta de administrador delegada. Isso oferece uma visão abrangente e permite que você implante o Regras do AWS Config nas contas para detectar recursos acessíveis ao público.
- Configurar o AWS Identity and Access Management Access Analyzer o IAM Access Analyzer ajuda a identificar os recursos na organização e nas contas, como buckets do Amazon S3 ou perfis do IAM, que são compartilhados com uma entidade externa.
- Usar autocorreção no AWS Config para responder a alterações na configuração do acesso público de buckets do Amazon S3: é possível reativar automaticamente as configurações de acesso público de bloco para buckets do Amazon S3.

- Implementar o monitoramento e os alertas para identificar se os buckets do Amazon S3 se tornaram públicos: é necessário ter o monitoramento e os alertas implementados para identificar quando o acesso público de blocos do Amazon S3 foi desativado e se os buckets do Amazon S3 se tornaram públicos. Além disso, se você estiver usando o AWS Organizations, poderá criar uma política de controle de serviços que impeça alterações nas políticas de acesso público do Amazon S3. O AWS Trusted Advisor confere se há buckets do Amazon S3 com permissões de acesso abertas. As permissões de bucket que concedem, upload ou excluem acesso a todos criam possíveis problemas de segurança, pois permitem que qualquer pessoa adicione, modifique ou remova itens em um bucket. A verificação do Trusted Advisor examina as permissões de bucket explícitas e as políticas de bucket associadas que podem substituir as permissões de bucket. Você também pode utilizar o AWS Config para monitorar seus buckets do Amazon S3 para acesso público. Para ter mais informações, consulte Como usar o AWS Config para monitorar e responder a buckets do Amazon S3 que possibilitam acesso público. Ao revisar o acesso, é importante considerar quais tipos de dados estão contidos em buckets do Amazon S3. O Amazon Macie ajuda a descobrir e proteger dados sigilosos, como PII, PHI e credenciais, como chaves privadas ou da AWS.

Recursos

Documentos relacionados:

- Usar o AWS Identity and Access Management Access Analyzer
- Biblioteca de controles do AWS Control Tower
- Norma de práticas de segurança básicas da AWS
- Regras gerenciadas do AWS Config
- Referência de verificação do AWS Trusted Advisor
- Monitorar resultados da verificação do AWS Trusted Advisor com o Amazon EventBridge
- Gerenciar regras do AWS Config em todas as contas de sua organização
- AWS Config e AWS Organizations

Vídeos relacionados:

- Práticas recomendadas para proteger seu ambiente de várias contas
- Análise aprofundada do IAM Access Analyzer

SEC03-BP08 Compartilhar recursos com segurança em sua organização

À medida que o número de workloads aumenta, talvez você precise compartilhar o acesso aos recursos nessas workloads ou fornecer os recursos várias vezes nas contas. Você pode ter estruturas para fragmentar seu ambiente, como ter ambientes de desenvolvimento, teste e produção. No entanto, ter estruturas de separação não limita o compartilhamento seguro. Ao compartilhar componentes que se sobrepõem, você pode reduzir a sobrecarga operacional e possibilitar uma experiência consistente sem precisar adivinhar o que ignorou ao criar o mesmo recurso várias vezes.

Resultado desejado: minimizar o acesso acidental utilizando métodos seguros para compartilhar recursos com sua organização e ajudar com sua iniciativa de prevenção de perda de dados. Reduza sua sobrecarga operacional em comparação com o gerenciamento de componentes individuais, reduza os erros gerados pela criação manual do mesmo componente várias vezes e aumente a escalabilidade de suas workloads. É possível se beneficiar da redução de tempo para a resolução em cenários de falhas em vários pontos e aumentar sua confiança na determinação de quando um componente não é mais necessário. Para ter orientações prescritivas sobre como analisar recursos compartilhados externamente, consulte SEC03-BP07 Analisar o acesso público e entre contas.

Antipadrões comuns:

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

Nível de risco exposto se esta prática recomendada não é estabelecida: médio

Orientação de implementação

Projete seus controles e padrões de acesso para reger o consumo de recursos compartilhados com segurança e somente com entidades confiáveis. Monitore recursos compartilhados e revise o acesso a eles de forma contínua e seja alertado sobre o compartilhamento inadequado ou inesperado. Leia Analisar o acesso público e entre contas para ajudar você a estabelecer a governança a fim de reduzir o acesso externo apenas aos recursos que precisem dele e estabelecer um processo para monitorar de forma contínua e alertar automaticamente.

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

Para restringir sua conta para somente compartilhar recursos em sua organização, utilize políticas de controle de serviços (SCPs) para impedir o acesso a entidades principais externas. Ao compartilhar recursos, combine controles baseados em identidade e controles de rede para criar um perímetro de dados para sua organização a fim de ajudar a proteger contra o acesso acidental. Um perímetro de dados é um conjunto de barreiras de proteção preventivas que ajudam a garantir que apenas suas identidades confiáveis acessem recursos confiáveis das redes esperadas. Esses controles impõem limites apropriados sobre quais recursos podem ser compartilhados e impedir o compartilhamento ou a exposição de recursos que não devem ser permitidos. Por exemplo, como parte de um perímetro de dados, é possível usar políticas de endpoint de VPC e a condição `AWS:PrincipalOrgId` para garantir que as identidades que acessam seus buckets do Amazon S3 pertençam à sua organização. É importante observar que as SCPs não se aplicam a perfis vinculados a serviço (LSR) nem a entidades principais de serviços da AWS.

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

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

Etapas da implementação

1. Utilize o AWS Organizations.

   O AWS Organizations é um serviço de gerenciamento de contas que permite consolidar várias Contas da AWS em uma organização que você cria e gerencia centralmente. É possível agrupar

suas contas em unidades organizacionais (UOs) e anexar políticas diferentes a cada UO a fim de ajudar a atender às suas necessidades orçamentárias, de segurança e conformidade. Também é possível controlar como serviços de inteligência artificial (IA) e machine learning (ML) da AWS podem coletar e armazenar dados e usar o gerenciamento de várias contas dos serviços da AWS integrados ao Organizations.

2. Integre o AWS Organizations aos serviços da AWS.

   Ao ativar um serviço da AWS para realizar tarefas em seu nome nas contas membros de sua organização, o AWS Organizations cria um perfil vinculado a serviço do IAM para esse serviço em cada conta membro. Você deve gerenciar o acesso confiável usando o AWS Management Console, as APIs da AWS ou a AWS CLI. Para ter orientações prescritivas sobre como ativar o acesso confiável, consulte Usar o AWS Organizations com outros serviços da AWS e Serviços da AWS que podem ser usados com o Organizations.

3. Estabeleça um perímetro de dados.

   O perímetro da AWS, geralmente, é representado como uma organização gerenciada pelo AWS Organizations. Junto com redes e sistemas on-premises, o acesso a recursos da AWS é o que muitos consideram o perímetro de My AWS. O objetivo do perímetro é garantir que o acesso seja permitido se a identidade e o recurso forem confiáveis e a rede for esperada.

   a. Defina e implante os perímetros.

      Siga as etapas descritas em Implementação do perímetro do whitepaper Criar um perímetro na AWS para cada condição de autorização. Para ter orientações prescritivas sobre como proteger a camada de rede, consulte Proteção de redes.

   b. Monitore e alerte de forma contínua.

      O AWS Identity and Access Management Access Analyzer ajuda a identificar os recursos na organização e nas contas que são compartilhados com entidades externas. É possível integrar o IAM Access Analyzer ao AWS Security Hub para enviar e agregar as descobertas para um recurso do IAM Access Analyzer para o Security Hub a fim de ajudar a analisar o procedimento de segurança de seu ambiente. Para ativar a integração, ative o IAM Access Analyzer e o Security Hub em cada região em cada conta. Também é possível utilizar o Regras do AWS Config para fazer auditoria da configuração e alertar a parte adequada utilizando o AWS Chatbot com o AWS Security Hub. Depois, você pode utilizar Documentos de automação do AWS Systems Manager para corrigir os recursos sem conformidade.

   c. Para ter orientações prescritivas sobre como monitorar e alertar de forma contínua sobre recursos compartilhados externamente, consulte Analisar o acesso público e entre contas.

4. Utilize o compartilhamento de recursos em serviços da AWS e restrinja-o adequadamente.

   Muitos serviços da AWS possibilitam compartilhar recursos com outra conta ou almejar um recurso em outra conta, como Imagens de máquina da Amazon (AMIs) e AWS Resource Access Manager (AWS RAM). Restrinja a API `ModifyImageAttribute` para especificar as contas confiáveis com as quais compartilhar a AMI. Especifique a condição `ram:RequestedAllowsExternalPrincipals` ao utilizar o AWS RAM para restringir o compartilhamento somente à sua organização, a fim de ajudar a impedir o acesso de identidades não confiáveis. Para ter orientações prescritivas e considerações, consulte Compartilhamento de recursos e destinos externos.

5. Utilize o AWS RAM para compartilhar com segurança em uma conta ou com outras Contas da AWS.

   O AWS RAM ajuda você a compartilhar com segurança os recursos criados com perfis e usuários em sua conta e com outras Contas da AWS. Em um ambiente de várias contas, o AWS RAM possibilita criar um recurso uma vez e compartilhá-lo com outras contas. Essa abordagem ajuda a reduzir sua sobrecarga operacional ao oferecer consistência, visibilidade e capacidade de auditoria por meio de integrações com o Amazon CloudWatch e o AWS CloudTrail, o que você não recebe ao utilizar o acesso entre contas.

   Se você tiver recursos compartilhados anteriormente com o uso de uma política baseada em recurso, é possível utilizar a API `PromoteResourceShareCreatedFromPolicy` ou equivalente a fim de promover o compartilhamento de recursos para um compartilhamento completo de recursos do AWS RAM.

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

Recursos

Práticas recomendadas relacionadas:

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

Documentos relacionados:

- Proprietário do bucket concede permissão entre contas a objetos que não possui
- Como usar políticas de confiança com o IAM
- Criar um perímetro de dados na AWS
- Como usar um ID externo ao conceder acesso aos seus recursos da AWS para terceiros
- Serviços da AWS que podem ser usados com o AWS Organizations
- Estabelecer um perímetro de dados na AWS: permitir apenas que identidades confiáveis acessem os dados da empresa

Vídeos relacionados:

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

Ferramentas relacionadas:

- Exemplos de política de perímetro de dados

SEC03-BP09 Compartilhar recursos com segurança com terceiros

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

Resultado desejado: credenciais do AWS Identity and Access Management (IAM) de longo prazo, chaves de acesso do IAM e chaves secretas associadas a um usuário podem ser usadas por qualquer pessoa desde que as credenciais sejam válidas e ativas. O uso de um perfil do IAM e credenciais temporárias ajuda você a melhorar seu procedimento de segurança geral reduzindo o esforço para manter credenciais de longo prazo, inclusive o gerenciamento e a sobrecarga operacional dessas informações sigilosas. Ao utilizar um identificador universalmente exclusivo (UUID) para o ID externo na política de confiança do IAM e manter as políticas do IAM anexadas ao perfil do IAM sob seu controle, é possível fazer auditoria e garantir que o acesso concedido a

terceiros não seja permissivo demais. Para ter orientações prescritivas sobre como analisar recursos compartilhados externamente, consulte SEC03-BP07 Analisar o acesso público e entre contas.

Antipadrões comuns:

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

Nível de risco exposto se esta prática recomendada não é estabelecida: médio

Orientação de implementação

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

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

Se o parceiro não precisar mais de acesso ao seu ambiente, remova o perfil. Evite fornecer credenciais de longo prazo para terceiros. Esteja ciente de outros serviços da AWS compatíveis com o compartilhamento. Por exemplo, o AWS Well-Architected Tool possibilita o compartilhamento de uma workload com outras Contas da AWS, e o AWS Resource Access Manager ajuda você a compartilhar com segurança um recurso da AWS que você possua com outras contas.

Etapas da implementação

1. Utilize perfis entre contas para fornecer acesso a contas externas.

   Os perfis entre contas reduzem a quantidade de informações sigilosas armazenadas por contas externas e terceiros para atender aos clientes. Os perfis entre contas possibilitam a você conceder acesso a recursos da AWS em sua conta de forma segura a terceiros, como AWS Partners ou

outras contas em sua organização e, ao mesmo tempo, manter a capacidade de gerenciar e auditar esse acesso.

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

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

2. Utilize um ID externo com terceiros.

   O uso de um ID externo possibilita designar quem pode assumir um perfil em uma política de confiança do IAM. A política de confiança pode exigir que o usuário que assume o perfil imponha a condição e o destino no qual ele está operando. Ele também fornece uma maneira para que o proprietário da conta permita que a função seja assumida somente em circunstâncias específicas. A função principal do ID externo é resolver e evitar o problema de substituto confuso.

   Utilize um ID externo se você for proprietário de uma Conta da AWS e tiver configurado um perfil para terceiros que acesse outras Contas da AWS além da sua, ou quando você pode assumir perfis em nome de clientes diferentes. Trabalhe com terceiros ou a AWS Partner para estabelecer uma condição de ID externo a ser incluída na política de confiança do IAM.

3. Utilize IDs externos universalmente exclusivos.

   Implemente um processo que gere um valor exclusivo aleatório para um ID externo, como um identificador universalmente exclusivo (UUID). Um parceiro que reutilize IDs externos entre diferentes clientes não resolve o problema de substituto confuso porque o cliente A pode ser capaz de visualizar dados do cliente B utilizando o ARN do perfil do cliente B junto com o ID externo duplicado. Em um ambiente de vários locatários, em que um parceiro atende a vários clientes com diferentes Contas da AWS, o parceiro deve usar um ID exclusivo diferente como o ID externo de cada Conta da AWS. O parceiro é responsável por detectar IDs externos duplicados e mapear de forma segura cada cliente ao seu respectivo ID externo. O parceiro deve testar para verificar se ele pode assumir o perfil somente ao especificar o ID externo. O parceiro deve evitar armazenar o ARN do perfil do cliente e o ID externo até que este seja necessário.

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

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

4. Deprecie credenciais de longo prazo fornecidas pelo cliente.

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

5. Verifique se a configuração tem orientações prescritivas ou é automatizada.

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

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

6. Considere alterações.

   Sua estrutura de contas, sua necessidade de terceiros ou a oferta de serviço pode ser alterada. Você deve antecipar alterações e falhas e planejar adequadamente com as pessoas, o processo e a tecnologia corretos. Audite o nível de acesso que você concede periodicamente e implemente métodos de detecção para alertar você de alterações inesperadas. Monitore e audite o uso do perfil e o datastore dos IDs externos. Você deve estar preparado para revogar o acesso de terceiros, seja de forma temporária ou permanente, como resultado de alterações ou padrões

de acesso inesperados. Além disso, meça o impacto de sua operação de revogação, inclusive o tempo para realizá-la, as pessoas envolvidas, o custo e o impacto de outros recursos.

Para ter orientações prescritivas sobre métodos de detecção, consulte as Práticas recomendadas de detecção.

Recursos

Práticas recomendadas relacionadas:

- SEC02-BP02 Usar credenciais temporárias
- SEC03-BP05 Definir barreiras de proteção de permissões para sua organização
- SEC03-BP06 Gerenciar o acesso com base no ciclo de vida
- SEC03-BP07 Analisar o acesso público e entre contas
- SEC04 Detecção

Documentos relacionados:

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

Vídeos relacionados:

- Como permito que usuários ou perfis em uma Conta da AWS separada acessem minha Conta da AWS?

- AWS re:Invent 2018: Torne-se um mestre em políticas do IAM em 60 minutos ou menos
- AWSPráticas recomendadas do IAM e decisões de design

Exemplos relacionados:

- Well-Architected Lab: Assumir perfil do IAM entre contas do Lambda (Nível 300)
- Configurar o acesso entre contas ao Amazon DynamoDB
- AWS STS Network Query Tool

Detecção

A detecção consiste em duas partes: a detecção de alterações de configuração inesperadas ou indesejadas e a detecção de comportamento inesperado. A primeira pode ocorrer em vários locais em um ciclo de vida de entrega de aplicações. Usando a infraestrutura como código (por exemplo, um modelo do CloudFormation), é possível verificar a configuração indesejada antes que uma workload seja implantada ao aplicar as verificações nos pipelines de CI/CD ou controle de origem. Em seguida, ao implantar uma workload em ambientes de não produção e de produção, você pode verificar a configuração usando ferramentas nativas da AWS, de código aberto ou de parceiros da AWS. Essas verificações podem ser para configuração que não atende aos princípios de segurança ou práticas recomendadas, ou para alterações que foram feitas entre uma configuração testada e implementada. Para uma aplicação em execução, é possível verificar se a configuração foi alterada de maneira inesperada, inclusive fora de uma implantação conhecida ou de um evento de escalabilidade automatizada.

Para a segunda parte da detecção, comportamento inesperado, é possível usar ferramentas ou alertar sobre um aumento em um tipo específico de chamada de API. Usando o Amazon GuardDuty, você pode receber um alerta quando ocorrer atividade inesperada e potencialmente não autorizada ou maliciosa em suas contas da AWS. Monitore também explicitamente as chamadas de API mutantes que você não espera que sejam usadas na workload e as chamadas de API que alteram a postura de segurança.

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

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

Práticas recomendadas

- SEC04-BP01 Configurar registro em log de serviço e aplicação
- SEC04-BP02 Analisar logs, descobertas e métricas de forma centralizada
- SEC04-BP03 Automatizar a resposta a eventos
- SEC04-BP04 Implementar eventos de segurança acionáveis

SEC04-BP01 Configurar registro em log de serviço e aplicação

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

Resultado desejado: uma organização deve ser capaz de recuperar de forma confiável e consistente logs de ventos de segurança de serviços e aplicações da AWS de modo pontual quando necessário a fim de cumprir um processo ou obrigação interna, como resposta a incidentes de segurança. Considere centralizar os logs para ter melhores resultados operacionais.

Antipadrões comuns:

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

Benefícios do estabelecimento desta prática recomendada: implementar um mecanismo de análise da causa raiz (RCA) para incidentes de segurança e uma fonte de evidências para suas obrigações de governança, risco e conformidade.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: alto

Orientação de implementação

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

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

Etapas da implementação

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

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

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

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

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

  Os serviços da AWS podem gerar logs não capturados pelas fontes de log básicas, como logs do Elastic Load Balancing, logs do AWS WAF, logs de gravador do AWS Config, descobertas do Amazon GuardDuty, logs de auditoria do Amazon Elastic Kubernetes Service (Amazon EKS)

e logs de aplicações e do sistema de instâncias do Amazon EC2. Para ter uma lista completa de opções de registro em log e monitoramento, consulte Apêndice A: Definições de recursos de nuvem: registro em log e eventos do Guia de resposta a incidentes de segurança da AWS.

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

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

  Um grupo de logs do CloudWatch oferece armazenamento durável e um recurso de consultas incorporado por meio do CloudWatch Logs Insights.
- Identifique a retenção de logs apropriada: quando você utiliza um bucket do Amazon S3 ou o grupo de logs do CloudWatch para armazenar logs, é necessário estabelecer ciclos de vida adequados para cada fonte de logs a fim de otimizar os custos de armazenamento e recuperação. Os clientes geralmente têm entre três meses a um ano de logs prontamente disponíveis para consultas, com retenção de até sete anos. A escolha de disponibilidade e retenção deve se alinhar aos seus requisitos de segurança e um composto de atribuições regulatórias, estatutárias e de negócios.
- Ative o registro em log para cada serviço e aplicação da AWS com políticas adequadas de retenção e ciclo de vida: para cada serviço ou aplicação da AWS em sua organização, procure as orientações específicas de configuração de registro em log:
  - Configurar a trilha do AWS CloudTrail
  - Configurar logs de fluxo de VPC
  - Configurar as exportações de descobertas do Amazon GuardDuty
  - Configurar os registros do AWS Config

  - Configurar o tráfego de ACL da web do AWS WAF
  - Configurar os logs de tráfego de rede do AWS Network Firewall
  - Configurar logs de acesso do Elastic Load Balancing
  - Configurar logs de consulta do Amazon Route 53 resolver
  - Configurar logs do Amazon RDS
  - Configurar logs do ambiente de gerenciamento Amazon EKS
  - Configurar o agente do Amazon CloudWatch para instâncias do Amazon EC2 e servidores on-premises
- Selecione e implemente os mecanismos de consulta para logs: para consultas de log, você pode usar 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. Também é possível usar ferramentas de consulta de terceiros, como um serviço de gerenciamento de eventos e informações de segurança (SIEM).

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

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

fluxo de VPC e logs do Amazon EKS Audit. O GuardDuty extrai fluxos de dados independentes diretamente do CloudTrail, de logs de fluxo de VPC, logs de consulta ao DNS e do Amazon EKS. Não é necessário gerenciar políticas de bucket do Amazon S3 nem modificar a forma de coletar e armazenar logs. Ainda é recomendável reter esses logs para sua própria investigação e fins de conformidade.

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

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

Recursos

Práticas recomendadas relacionadas:

- SEC04-BP02 Analisar logs, descobertas e métricas de forma centralizada
- SEC07-BP04 Definir o gerenciamento do ciclo de vida de dados
- SEC10-BP06 Pré-implantação de ferramentas

Documentos relacionados:

- Guia de resposta a incidentes de segurança da AWS
- Conceitos básicos do Amazon Security Lake
- Conceitos básicos: Amazon CloudWatch Logs
- Soluções de segurança parceiros: registro em log e monitoramento

Vídeos relacionados:

- AWS re:Invent 2022: Introdução ao Amazon Security Lake

Exemplos relacionados:

- Assisted Log Enabler for AWS

- Exportação histórica de descobertas do AWS Security Hub

Ferramentas relacionadas:

- Snowflake for Cybersecurity

SEC04-BP02 Analisar logs, descobertas e métricas de forma centralizada

as equipes de operações de segurança confiam na coleta de logs e no uso de ferramentas de pesquisa para descobrir possíveis eventos de interesse, que podem indicar atividade não autorizada ou alteração não intencional. No entanto, a simples análise de dados coletados e o processamento manual de informações são insuficientes para acompanhar o volume de informações provenientes de arquiteturas complexas. Somente a análise e os relatórios não facilitam a atribuição dos recursos certos para trabalhar um evento em tempo hábil.

Uma prática recomendada para montar uma equipe madura de operações de segurança é integrar profundamente o fluxo de eventos e descobertas de segurança em um sistema de notificação e fluxo de trabalho, como um sistema de emissão de tíquetes, um sistema de erros ou problemas, ou outro sistema de gerenciamento de informações e eventos de segurança (SIEM). Isso remove o fluxo de trabalho de e-mails e relatórios estáticos, o que permite rotear, escalar e gerenciar eventos ou descobertas. Muitas organizações também estão integrando alertas de segurança em suas plataformas de bate-papo ou colaboração e de produtividade do desenvolvedor. Para organizações que estão iniciando com automações, um sistema de emissão de tíquetes orientado por APIs e de baixa latência oferece flexibilidade considerável para o planejamento de o que automatizar primeiro.

Essa prática recomendada aplica-se não só a eventos de segurança gerados a partir de mensagens de log que representam atividades do usuário ou eventos de rede, como também a alterações detectadas na própria infraestrutura. A capacidade de detectar alterações, determinar se uma alteração foi apropriada e, em seguida, rotear essas informações para o fluxo de trabalho de correção correto é essencial para manter e validar uma arquitetura segura, no contexto de alterações em que a natureza de sua indesejabilidade é suficientemente sutil para que sua execução não possa ser impedida com uma combinação de configuração do AWS Identity and Access Management(IAM) e do AWS Organizations.

O Amazon GuardDuty e o AWS Security Hub fornecem mecanismos de agregação, desduplicação e análise para registros de log que também são disponibilizados a você por meio de outros serviços da

AWS. O GuardDuty ingere, agrega e analisa informações de fontes como gerenciamento e eventos de dados do AWS CloudTrail, logs de DNS de VPC e logs de fluxo de VPC. O Security Hub pode ingerir, agregar e analisar a saída do GuardDuty AWS Config, do Amazon Inspector, Amazon Macie, do AWS Firewall Manager e de um número significativo de produtos de segurança de terceiros disponíveis no AWS Marketplace e, se criado adequadamente, no seu próprio código. Tanto o GuardDuty quanto o Security Hub têm um modelo de membro administrador que pode agregar descobertas e insights em várias contas. O Security Hub geralmente é usado por clientes que têm um SIEM on-premises como um log do lado da AWS e um pré-processador e agregador de logs e alertas nos quais eles podem consumir o Amazon EventBridge por meio de um processador e encaminhador com base no AWS Lambda.

Nível de exposição a riscos quando esta prática recomendada não for estabelecida: Alto

Orientações para a implementação

- Avaliar os recursos de processamento de log: avalie as opções disponíveis para o processamento de logs.
  - Use Amazon OpenSearch Service to log and monitor (almost) everything (Usar o Amazon OpenSearch Service para registrar e monitorar (quase) tudo)
  - Encontre um parceiro especializado em soluções de registro e monitoramento
- Para começar a analisar logs do CloudTrail, experimente o Amazon Athena.
  - Como configurar o Athena para analisar logs do CloudTrail
- Implementar o login centralizado na AWS: consulte a solução de exemplo da AWS a seguir para centralizar o log de várias fontes.
  - Centralizar a solução de registro em log
- Implementar o registro em log centralizado com o parceiro: os parceiros da APN têm soluções para ajudar você a analisar os logs de forma centralizada.
  - Registro em log e monitoramento

Recursos

Documentos relacionados:

- AWS Answers: registro em log centralizado
- AWS Security Hub

- Amazon CloudWatch
- Amazon EventBridge
- Conceitos básicos: Amazon CloudWatch Logs
- Soluções de segurança parceiros: registro em log e monitoramento

Vídeos relacionados:

- Centrally Monitoring Resource Configuration and Compliance (Monitoramento centralizado de configuração e conformidade de recursos)
- Remediating Amazon GuardDuty and AWS Security Hub Findings (Correção do Amazon GuardDuty e descobertas do AWS Security Hub)
- Threat management in the cloud: Amazon GuardDuty and AWS Security Hub (Gerenciamento de ameaças na nuvem: Amazon GuardDuty e AWS Security Hub)

SEC04-BP03 Automatizar a resposta a eventos

O uso de automação para investigar e corrigir eventos reduz o esforço humano e erros e permite escalar recursos de investigação. Análises regulares ajudarão você a ajustar ferramentas de automação e iterar continuamente.

Na AWS, a investigação de eventos de interesse e informações sobre alterações potencialmente inesperadas em um fluxo de trabalho automatizado pode ser obtida com o Amazon EventBridge. Esse serviço fornece um mecanismo de regras escalável, projetado para processar formatos de eventos da AWS nativos (como eventos do AWS CloudTrail) e personalizados, que você pode gerar com base em sua aplicação. O Amazon GuardDuty também permite rotear eventos em um sistema de fluxo de trabalho para usuários que criam sistemas de resposta a incidentes (AWS Step Functions), uma conta de segurança central ou um bucket para análise posterior.

A detecção de alterações e o roteamento dessas informações para o fluxo de trabalho correto podem ser realizados com o uso do Regras do AWS Config e de pacotes de conformidade. O AWS Config detecta alterações nos serviços em escopo (embora com maior latência do que o EventBridge) e gera eventos que podem ser analisados usando o Regras do AWS Config para reversão, aplicação da política de conformidade e encaminhamento de informações aos sistemas, como plataformas de gerenciamento de alterações e sistemas operacionais de emissão de tíquetes. Além de escrever suas próprias funções do Lambda para responder a eventos do AWS Config, você também pode aproveitar o kit de desenvolvimento do Regras do AWS Confige uma biblioteca de código aberto

do Regras do AWS Config. Os pacotes de conformidade são uma coleção de ações de correção e do Regras do AWS Config que você implanta como uma única entidade criada como um modelo YAML. O modelo de pacote de conformidade de amostra está disponível no pilar Segurança do Well-Architected.

Nível de exposição a riscos quando esta prática recomendada não for estabelecida: Médio

Orientações para a implementação

- Implementar alertas automatizados com o GuardDuty: o GuardDuty é um serviço de detecção de ameaças que monitora continuamente atividades mal-intencionadas e comportamentos não autorizados para proteger suas workloads e Contas da AWS. Habilite o GuardDuty e configure alertas automatizados.
- Automatizar o processo de investigação: desenvolva processos automatizados que investigam um evento e relatam informações a um administrador para economizar tempo.
  - Laboratório: Amazon GuardDuty na prática

Recursos

Documentos relacionados:

- AWS Answers: registro em log centralizado
- AWS Security Hub
- Amazon CloudWatch
- Amazon EventBridge
- Conceitos básicos: Amazon CloudWatch Logs
- Soluções de segurança parceiros: registro em log e monitoramento
- Como configurar o Amazon GuardDuty

Vídeos relacionados:

- Centrally Monitoring Resource Configuration and Compliance (Monitoramento centralizado de configuração e conformidade de recursos)
- Remediating Amazon GuardDuty and AWS Security Hub Findings (Correção do Amazon GuardDuty e descobertas do AWS Security Hub)

- Threat management in the cloud: Amazon GuardDuty and AWS Security Hub (Gerenciamento de ameaças na nuvem: Amazon GuardDuty e AWS Security Hub)

Exemplos relacionados:

- Laboratório: Implantação automatizada de controles de detecção

SEC04-BP04 Implementar eventos de segurança acionáveis

Crie alertas para serem enviados à sua equipe para ação. Certifique-se de que os alertas incluam informações relevantes para a equipe agir. Para cada mecanismo de detecção existente, você também deve ter um processo, na forma de um runbook ou playbook, para investigar. Por exemplo, quando você habilita o Amazon GuardDuty, ele gera diferentes descobertas. Você deve ter uma entrada de runbook para cada tipo de descoberta, por exemplo, se um cavalo de Troia for descoberto, seu runbook terá instruções simples que instruem alguém a investigar e corrigir o problema.

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

Orientação de implementação

- Descubra as métricas disponíveis para serviços da AWS: descubra as métricas disponíveis por meio do Amazon CloudWatch para os serviços que você está usando.
  - Documentação do serviço da AWS
  - Uso de métricas do Amazon CloudWatch
- Configure os alarmes do Amazon CloudWatch.
  - Como usar os alarmes do Amazon CloudWatch

Recursos

Documentos relacionados:

- Amazon CloudWatch
- Amazon EventBridge
- Soluções de segurança parceiros: registro em log e monitoramento

Vídeos relacionados:

- Centrally Monitoring Resource Configuration and Compliance (Monitoramento centralizado de configuração e conformidade de recursos)
- Remediating Amazon GuardDuty and AWS Security Hub Findings (Correção do Amazon GuardDuty e descobertas do AWS Security Hub)
- Threat management in the cloud: Amazon GuardDuty and AWS Security Hub (Gerenciamento de ameaças na nuvem: Amazon GuardDuty e AWS Security Hub)

Proteção de infraestrutura

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

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

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

É necessário estar familiarizado com regiões, zonas de disponibilidade, zonas locais da AWSe aos AWS Outposts, que são componentes da infraestrutura global segura da AWS.

A AWS tem o conceito de região, que é um local físico em algum lugar do mundo onde os datacenters são agrupados. Os grupos de datacenters lógicos são chamados de zona de disponibilidade (AZ). Cada região da AWS consiste em várias AZs isoladas e fisicamente separadas em uma área geográfica. Se você tiver requisitos de residência de dados, será possível escolher a região da AWS mais próxima do local desejado. Você mantém controle e propriedade totais sobre a região em que seus dados estão localizados fisicamente, o que pode ser útil para atender aos requisitos regionais de conformidade e residência de dados. Cada AZ tem fontes de energia, refrigeração e segurança física independentes. Se uma aplicação for particionada em AZs, você estará mais bem isolado e protegido contra problemas como queda de energia, raios, tornados, terremotos, entre outros. As AZs estão separadas fisicamente por uma distância significativa, a muitos quilômetros de qualquer outra AZ, embora todas estejam a 100 km (60 milhas) uma da outra. Todas as AZs em uma região da AWS são interconectadas com rede de alta largura de banda e baixa latência, usando fibra metropolitana dedicada totalmente redundante, fornecendo rede de alto throughput e baixa latência entre as AZs. Todo tráfego entre AZs é criptografado. Os clientes da AWS focados em alta disponibilidade podem projetar suas aplicações para serem executadas em várias AZs para obter uma tolerância a falhas ainda maior. As regiões da AWS atendem aos mais altos níveis de segurança, conformidade e proteção de dados.

As zonas locais da AWS colocam computação, armazenamento, banco de dados e outros serviços selecionados da AWS mais próximos dos usuários finais. Com as zonas locais da AWS, é possível executar facilmente aplicações altamente exigentes que requerem latências de milissegundos de um dígito para os usuários finais, como criação de conteúdo de mídia e entretenimento, jogos em tempo real, simulações de reservatórios, automação de projetos eletrônicos e machine learning. Cada zona local da AWS é uma extensão de uma região da AWS onde é possível executar as simulações de reservatórios sensíveis à latência, usando serviços da AWS como Amazon EC2, Amazon VPC, Amazon EBS, Amazon File Storage e Elastic Load Balancing na proximidade geográfica dos usuários finais. As zonas locais da AWS fornecem uma conexão segura e de alta largura de banda entre as workloads locais e aquelas executadas na região da AWS, permitindo se conectar perfeitamente a toda a gama de serviços na região por meio das mesmas APIs e conjuntos de ferramentas.

O AWS Outposts inclui serviços nativos, infraestrutura e modelos operacionais da AWS para praticamente qualquer datacenter, espaço de colocalização ou instalação on-premises. Você pode usar as mesmas APIs, ferramentas e infraestrutura da AWS em instalações on-premises e na Nuvem AWS para oferecer uma experiência híbrida verdadeiramente consistente. O AWS Outposts foi projetado para ambientes conectados e pode ser usado para oferecer suporte a workloads que devem permanecer no ambiente on-premises devido à baixa latência ou às necessidades de processamento de dados locais.

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

Tópicos

Proteção de redes

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

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

Práticas recomendadas

- SEC05-BP01 Criar camadas de rede
- SEC05-BP02 Controlar tráfego de todas as camadas
- SEC05-BP03 Automatizar a proteção da rede:
- SEC05-BP04 Implementar inspeção e proteção

SEC05-BP01 Criar camadas de rede

Agrupe os componentes que compartilham requisitos de confidencialidade em camadas para minimizar o possível escopo do impacto do acesso não autorizado. Por exemplo, um cluster de banco de dados em uma nuvem privada virtual (VPC) sem necessidade de acesso à Internet deve ser colocado em sub-redes sem nenhuma rota para/ou proveniente da Internet. O tráfego só deve fluir do próximo recurso menos sigiloso adjacente. Considere uma aplicação da web atrás de um balanceador de carga. Seu banco de dados não deve ser acessível diretamente do balanceador de carga. Somente a lógica de negócios ou o servidor da web tem acesso direto ao seu banco de dados.

Resultado desejado: criar uma rede em camadas. Redes em camadas ajudam a agrupar logicamente componentes de rede semelhantes. Elas também reduzem o possível escopo de impacto do acesso não autorizado à rede. Uma rede configurada adequadamente em camadas dificulta que usuários não autorizados adaptem recursos adicionais em seu ambiente da AWS. Além de garantir caminhos de rede internos, você também deve proteger sua borda de rede, como aplicações da web e endpoints de API.

Antipadrões comuns:

- Criar todos os recursos em uma única VPC ou sub-rede.
- Utilizar grupos de segurança excessivamente permissivos.

- Não utilizar sub-redes.
- Permitir o acesso direto aos armazenamentos de dados, como bancos de dados.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: alto

Orientação de implementação

Os componentes como instâncias do Amazon Elastic Compute Cloud (Amazon EC2), clusters de banco de dados do Amazon Relational Database Service (Amazon RDS) e funções do AWS Lambda que compartilham requisitos de acessibilidade podem ser segmentados em camadas formadas por sub-redes. Considere implantar workloads sem servidor, como funções do Lambda, em uma VPC ou atrás de um Amazon API Gateway. As tarefas do AWS Fargate (Fargate) que não têm necessidade de acesso à Internet devem ser colocadas em sub-redes sem rota para ou proveniente da Internet. Essa abordagem em camadas reduz o impacto da configuração incorreta de uma única camada, o que pode permitir o acesso não intencional. Para o AWS Lambda, você pode executar as funções em sua VPC para utilizar os controles baseados em VPC.

Para a conectividade de rede que pode incluir milhares de VPCs, Contas da AWS e redes on-premises, você deve utilizar o AWS Transit Gateway. O Transit Gateway age como um hub que controla como o tráfego é roteado entre todas as redes conectadas, que agem como raios. O tráfego entre o Amazon Virtual Private Cloud (Amazon VPC) e o Transit Gateway permanece na rede privada da AWS, o que reduz a exposição externa a usuários não autorizados e possíveis problemas de segurança. O emparelhamento entre regiões do Transit Gateway também criptografa o tráfego entre regiões sem nenhum ponto único de falha ou gargalo de largura de banda.

Etapas da implementação

- Utilize o Reachability Analyzer para analisar o caminho entre uma origem e um destino com base na configuração: o Reachability Analyzer permite a você automatizar a verificação da conectividade para e proveniente de recursos conectados à VPC. Observe que essa análise é realizada analisando a configuração (nenhum pacote de rede é enviado na realização da análise).
- Utilize o Analisador de Acesso à Rede Amazon VPC para identificar o acesso acidental à rede aos recursos: o Analisador de Acesso à Rede Amazon VPC possibilita especificar seus requisitos de acesso à rede identificar possíveis caminhos de rede.
- Considere se os recursos precisam estar em uma sub-rede pública: não coloque os recursos em sub-redes públicas de sua VPC a menos que eles devam receber tráfego de rede de entrada de origens públicas.

- Crie sub-redes em suas VPCs: crie sub-redes para cada camada de rede (em grupos que incluam várias zonas de disponibilidade) para melhorar a microssegmentação. Verifique também se você associou as tabelas de rotas corretas com suas sub-redes para controlar o roteamento e a conectividade de rede.
- Utilize o AWS Firewall Manager para gerenciar seus grupos de segurança de VPC: o AWS Firewall Manager ajuda a reduzir o trabalho de usar vários grupos de segurança.
- Utilize o AWS WAF para proteger contra vulnerabilidades comuns da web: o AWS WAF pode ajudar a melhorar a segurança de borda inspecionando o tráfego quanto a vulnerabilidades comuns da web, como injeção de SQL. Ele também permite restringir o tráfego de endereços IP originários de determinados países ou locais geográficos.
- Utilize o Amazon CloudFront como uma rede de distribuição de conteúdo (CDN): o Amazon CloudFront pode ajudar a acelerar sua aplicação da web armazenando dados mais perto de seus usuários. Ele também pode melhorar a segurança de borda aplicando HTTPS, restringindo o acesso a áreas geográficas e garantindo que o tráfego de rede possa acessar somente recursos roteados por meio do CloudFront.
- Utilize o Amazon API Gateway ao criar interfaces de programação de aplicações (APIs): o Amazon API Gateway ajuda a publicar, monitorar e proteger APIs REST, HTTPS e de WebSocket.

Recursos

Documentos relacionados:

- AWS Firewall Manager
- Amazon Inspector
- Segurança na Amazon VPC
- Reachability Analyzer
- Analisador de Acesso à Rede Amazon VPC

Vídeos relacionados:

- Arquiteturas de referência do AWS Transit Gateway para várias VPCs
- Aceleração e proteção de aplicações com o Amazon CloudFront, o AWS WAF e o AWS Shield
- AWS re:Inforce 2022: Validar controles de acesso à rede eficazes na AWS
- AWS re:Inforce 2022: Proteções avançadas contra bots usando o AWS WAF

Exemplos relacionados:

- Well-Architected Lab: Implantação automatizada de VPC
- Workshop: Analisador de Acesso à Rede Amazon VPC

SEC05-BP02 Controlar tráfego de todas as camadas

ao projetar sua topologia de rede, você deve examinar os requisitos de conectividade de cada componente. Por exemplo, se um componente precisa de acesso à Internet (entrada e saída), conectividade com VPCs, serviços de borda e datacenters externos.

Uma VPC permite que você defina a topologia de rede que abrange uma Região da AWS com um intervalo de endereços IPv4 privados que você define ou um intervalo de endereços IPv6 que a AWS seleciona. Você deve aplicar vários controles com uma abordagem detalhada de defesa para tráfego de entrada e saída, incluindo o uso de grupos de segurança (firewall de inspeção com estado), Network ACLs, sub-redes e tabelas de rotas. Você pode criar sub-redes em uma zona de disponibilidade dentro de uma VPC. Cada sub-rede tem uma tabela de rotas associada que define regras de roteamento para gerenciar os caminhos do tráfego dentro da sub-rede. Você pode definir uma sub-rede roteável na Internet com uma rota que siga até um gateway da Internet ou gateway NAT associado à VPC ou que passe por outra VPC.

Quando uma instância, um banco de dados do Amazon Relational Database Service(Amazon RDS) ou outro serviço é executado em uma VPC, ela tem seu próprio grupo de segurança por interface de rede. Esse firewall está fora da camada do sistema operacional e pode ser usado para definir regras para o tráfego permitido de entrada e saída. Você também pode definir relacionamentos entre grupos de segurança. Por exemplo, as instâncias em um grupo de segurança no nível do banco de dados aceitam somente o tráfego de instâncias no nível do aplicativo, por referência aos grupos de segurança aplicados às instâncias envolvidas. A menos que você esteja usando protocolos não baseados em TCP, não deve ser necessário ter uma instância do Amazon Elastic Compute Cloud(Amazon EC2) diretamente acessível pela Internet (mesmo com portas restritas por grupos de segurança) sem um balanceador de carga ou o CloudFront. Isso ajuda a protegê-lo contra acesso não intencional surgido por um problema de sistema operacional ou aplicativo. Uma sub-rede também pode ter uma Network ACL anexada a ela, que atua como um firewall sem estado. Você deve configurar a Network ACL para restringir a abrangência do tráfego permitido entre camadas. Observe que é preciso definir regras de entrada e de saída.

Alguns serviços da AWS requerem componentes para acessar a Internet para fazer chamadas de API, onde os endpoints de API da AWS estão localizados. Outros serviços da AWS usam VPC

endpoints dentro das suas Amazon VPCs. Muitos serviços da AWS, incluindo o Amazon S3 e o Amazon DynamoDB, oferecem suporte a endpoints da VPC, e essa tecnologia foi generalizada no AWS PrivateLink. Recomendamos o uso dessa abordagem para acessar serviços da AWS, serviços de terceiros e seus próprios serviços hospedados em outras VPCs com segurança. Todo o tráfego de rede do AWS PrivateLink permanece no backbone global da AWS e nunca atravessa a Internet. A conectividade só pode ser iniciada pelo consumidor do serviço e não pelo provedor do serviço. O uso do AWS PrivateLink para acesso a serviços externos permite criar VPCs air-gapped sem acesso à Internet e ajuda a proteger suas VPCs de vetores de ameaças externas. Os serviços de terceiros podem usar o AWS PrivateLink para permitir que os clientes se conectem aos serviços de suas VPCs por meio de endereços IP privados. Para ativos da VPC que precisam estabelecer conexões de saída com a Internet, elas podem ser feitas somente de saída (unidirecional) por meio de um gateway NAT gerenciado pela AWS, de um gateway da Internet somente de saída ou de proxies de Web criados e gerenciados por você.

Nível de exposição a riscos quando esta prática recomendada não for estabelecida: Alto

Orientações para a implementação

- Controlar o tráfego de rede em uma VPC: implemente as práticas recomendadas de VPC para controlar o tráfego.
  - Segurança da Amazon VPC
  - VPC endpoints
  - Grupo de segurança da Amazon VPC
  - ACLs de rede
- Controlar o tráfego na borda: implemente serviços de borda, como o Amazon CloudFront, para fornecer uma camada adicional de proteção e outros recursos.
  - Casos de uso do Amazon CloudFront
  - AWS Global Accelerator
  - AWS Web Application Firewall (AWS WAF)
  - Amazon Route 53
  - Roteamento de entrada da Amazon VPC
- Controlar o tráfego de rede privada: implemente serviços que protegem o tráfego privado da sua workload.
  - Emparelhamento de Amazon VPC
  - Serviços de endpoint da Amazon VPC (AWS PrivateLink)

- Amazon VPC Transit Gateway
- AWS Direct Connect
- AWS Site-to-Site VPN
- AWS Client VPN
- Pontos de acesso do Amazon S3

Recursos

Documentos relacionados:

- AWS Firewall Manager
- Amazon Inspector
- Conceitos básicos do AWS WAF

Vídeos relacionados:

- AWS Transit Gateway reference architectures for many VPCs (Arquiteturas de referência do AWS Transit Gateway para várias VPCs)
- Application Acceleration and Protection with Amazon CloudFront, AWS WAF, and AWS Shield (Aceleração e proteção de aplicações com o Amazon CloudFront, o AWS WAF e o AWS Shield)

Exemplos relacionados:

- Laboratório: Implantação automatizada da VPC

SEC05-BP03 Automatizar a proteção da rede:

Automatize os mecanismos de proteção para fornecer uma rede de autodefesa com base em inteligência de ameaças e detecção de anomalias. Por exemplo, ferramentas de detecção e prevenção de intrusão que podem se adaptar às ameaças atuais e reduzir seu impacto. Um firewall de aplicação Web é um exemplo de onde você pode automatizar a proteção de rede; por exemplo, usando a solução AWS WAF Security Automations (https://github.com/awslabs/aws-waf-security-automations) para bloquear automaticamente solicitações originadas de endereços IP associados a agentes de ameaças conhecidos.

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

Orientação de implementação

- Automatize a proteção para tráfego baseado na Web: a AWS oferece uma solução que usa o AWS CloudFormation para implantar automaticamente um conjunto de regras do AWS WAF projetadas para filtrar ataques comuns baseados na Web. Os usuários podem selecionar entre recursos de proteção pré-configurados que definem as regras incluídas em uma lista de controle de acesso da Web (ACL da Web) do AWS WAF.
  - Automações de segurança do AWS WAF
- Considere as soluções de AWS Partner: os parceiros da AWS oferecem centenas de produtos líderes do setor que são equivalentes, idênticos ou se integram aos controles existentes nos seus ambientes on-premises. Esses produtos complementam os serviços da AWS já existentes para que os clientes possam implantar uma arquitetura de segurança abrangente e obter uma experiência mais uniforme na nuvem e no ambiente on-premises.
  - Segurança da infraestrutura

Recursos

Documentos relacionados:

- AWS Firewall Manager
- Amazon Inspector
- Segurança da Amazon VPC
- Conceitos básicos do AWS WAF

Vídeos relacionados:

- AWS Transit Gateway reference architectures for many VPCs (Arquiteturas de referência do AWS Transit Gateway para várias VPCs)
- Application Acceleration and Protection with Amazon CloudFront, AWS WAF, and AWS Shield (Aceleração e proteção de aplicações com o Amazon CloudFront, o AWS WAF e o AWS Shield)

Exemplos relacionados:

- Laboratório: Implantação automatizada da VPC

SEC05-BP04 Implementar inspeção e proteção

Inspecione e filtre o tráfego em cada camada. É possível inspecionar suas configurações de VPC quanto a possíveis acessos não intencionais usando o VPC Network Access Analyzer. Especifique seus requisitos de acesso à rede e identifique possíveis caminhos de rede que não os atendem. Para componentes que fazem transações por meio de protocolos baseados em HTTP, um firewall de aplicativo Web pode ajudar a proteger contra ataques comuns. AWS WAF é um firewall para aplicativos web que permite monitorar e bloquear solicitações HTTP(s) que correspondem às regras configuráveis que são encaminhadas para uma API do Amazon API Gateway, o Amazon CloudFront ou um Application Load Balancer. Para começar a usar o AWS WAF, você pode usar o AWS Managed Rules em combinação com as suas próprias ou usar integrações de parceiros existentes.

Para gerenciar o AWS WAF, proteções do AWS Shield Advanced e grupos de segurança do Amazon VPC no AWS Organizations, você pode usar o AWS Firewall Manager. Ele permite configurar e gerenciar centralmente regras de firewall entre contas e aplicativos, simplificando a imposição de regras comuns em escala. Ele também permite que você responda rapidamente a ataques, usando o AWS Shield Advancedou soluções capazes de bloquear automaticamente solicitações indesejadas para suas aplicações Web. O Firewall Manager também funciona com o AWS Network Firewall. O AWS Network Firewall é um serviço gerenciado que usa um mecanismo de regras para fornecer controle refinado sobre o tráfego de rede com e sem estado. Ele oferece suporte às especificações do sistema de prevenção de intrusões (IPS) de código aberto compatível com Suricata para regras para ajudar a proteger sua workload.

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

Orientação de implementação

- Configure o Amazon GuardDuty: o GuardDuty é um serviço de detecção de ameaças que monitora continuamente atividades mal-intencionadas e comportamentos não autorizados para proteger suas workloads e Contas da AWS. Habilite o GuardDuty e configure alertas automatizados.
  - Amazon GuardDuty
  - Laboratório: Implantação automatizada de controles de detecção
- Configure os logs de fluxo da nuvem privada virtual (VPC): os logs de fluxo da VPC é um recurso que permite capturar informações sobre o tráfego de IP direcionado e proveniente de interfaces de rede na sua VPC. Os dados de log de fluxo podem ser publicados no Amazon CloudWatch Logs e no Amazon Simple Storage Service (Amazon S3). Depois de criar um log de fluxo, você pode recuperar e visualizar seus dados no destino escolhido.

- Considere o espelhamento de tráfego da VPC: o espelhamento de tráfego é um recurso da Amazon VPC que pode ser usado para copiar o tráfego de rede de uma interface de rede elástica de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) e enviá-lo para dispositivos de segurança e monitoramento fora de banda para inspeção de conteúdo, monitoramento de ameaças e solução de problemas.
  - Espelhamento de tráfego de VPC

Recursos

Documentos relacionados:

- AWS Firewall Manager
- Amazon Inspector
- Segurança da Amazon VPC
- Conceitos básicos do AWS WAF

Vídeos relacionados:

- AWS Transit Gateway reference architectures for many VPCs (Arquiteturas de referência do AWS Transit Gateway para várias VPCs)
- Application Acceleration and Protection with Amazon CloudFront, AWS WAF, and AWS Shield (Aceleração e proteção de aplicações com o Amazon CloudFront, o AWS WAF e o AWS Shield)

Exemplos relacionados:

- Laboratório: Implantação automatizada da VPC

Proteção da computação

Os recursos de computação incluem instâncias do EC2, contêineres, funções do AWS Lambda, serviços de banco de dados, dispositivos de IoT e muito mais. Cada um desses tipos de recursos de computação requer abordagens diferentes para protegê-los. No entanto, eles compartilham estratégias comuns que devem ser consideradas: defesa em profundidade, gerenciamento de vulnerabilidades, redução na superfície de ataque, automação de configuração e operação e execução de ações à distância. Nesta seção, você encontrará orientações gerais para proteger seus

recursos de computação para os principais serviços. Para cada serviço da AWS usado, é importante verificar as recomendações de segurança específicas na documentação do serviço.

Práticas recomendadas

- SEC06-BP01 Fazer o gerenciamento de vulnerabilidades
- SEC06-BP02 Reduzir a superfície de ataque
- SEC06-BP03 Implementar serviços gerenciados
- SEC06-BP04 Automatizar a proteção da computação
- SEC06-BP05 Permitir que as pessoas executem ações a uma distância
- SEC06-BP06 Validar a integridade do software

SEC06-BP01 Fazer o gerenciamento de vulnerabilidades

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

Resultado desejado: criar e manter um programa de gerenciamento de vulnerabilidade. Verificar regularmente e corrigir recursos, como instâncias do Amazon EC2, contêineres do Amazon Elastic Container Service (Amazon ECS) e workloads do Amazon Elastic Kubernetes Service (Amazon EKS). Configurar janelas de manutenção para recursos gerenciados da AWS, como bancos de dados Amazon Relational Database Service (Amazon RDS). Utilizar a verificação de código estático para inspecionar a existência de problemas comuns no código-fonte da aplicação. Considerar testes de penetração de aplicações da web se sua organização tiver as habilidades obrigatórias ou puder contratar assistência externa.

Antipadrões comuns:

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

Benefícios do estabelecimento desta prática recomendada:

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: alto

Orientação de implementação

Um programa de gerenciamento de vulnerabilidades inclui avaliação de segurança, identificação de problemas, priorização e realização de operações de patch como parte da solução dos problemas. A automação é a chave para verificar de forma contínua as workloads quanto a problemas e exposição acidental à rede e realização de remediação. Automatizar a criação e atualizar os recursos economiza tempo e reduz o risco de erros de configuração que criam mais problemas. Um programa de gerenciamento de vulnerabilidades bem projetado também deve considerar testes de vulnerabilidades durante o desenvolvimento e os estágios de implantação do ciclo de vida do software. Implementar o gerenciamento de vulnerabilidades durante o desenvolvimento e a implantação ajuda a reduzir a chance de uma vulnerabilidade atingir seu ambiente de produção.

Implementar um programa de gerenciamento de vulnerabilidades exige um bom entendimento do Modelo de responsabilidade compartilhada da AWS e como ele se relaciona com suas workloads específicas. Segundo o modelo de responsabilidade compartilhada, a AWS é responsável por proteger a infraestrutura da Nuvem AWS. Essa infraestrutura abrange o hardware, o software, as redes e as instalações que executam os serviços da Nuvem AWS. Você é responsável pela segurança na nuvem, por exemplo, os dados reais, a configuração de segurança e as tarefas de gerenciamento de instâncias do Amazon EC2 e por garantir que seus objetos do Amazon S3 sejam classificados e configurados corretamente. Sua abordagem ao gerenciamento de vulnerabilidades também pode variar dependendo dos serviços consumidos. Por exemplo, a AWS gerencia a aplicação de patches para nosso serviço de banco de dados relacional gerenciado, o Amazon RDS, mas você seria responsável pela colocação de patches em bancos de dados auto-hospedados.

A AWS tem uma série de serviços para ajudar com seu programa de gerenciamento de vulnerabilidades. O Amazon Inspector verifica de forma contínua as workloads da AWS quanto a problemas de software e acesso acidental à rede. O AWS Systems Manager Patch Manager ajuda a gerenciar a aplicação de patches em suas instâncias do Amazon EC2. O Amazon Inspector e o Systems Manager podem ser visualizados no AWS Security Hub, um serviço de gerenciamento de procedimentos de segurança na nuvem que ajuda a automatizar verificações de segurança da AWS e centralizar alertas de segurança.

O Amazon CodeGuru pode ajudar a identificar possíveis problemas em aplicações Java e Python utilizando análise de código estático.

Etapas da implementação

- Configurar o Amazon Inspector: o Amazon Inspector detecta automaticamente instâncias do Amazon EC2 recém-executadas, funções do Lambda e imagens de contêiner elegíveis enviadas

ao Amazon ECR e as verifica imediatamente quanto a problemas de software, possíveis defeitos e exposição acidental à rede.

- Verificar o código-fonte: verifique as bibliotecas e as dependências quanto a problemas e defeitos. O Amazon CodeGuru pode verificar e fornecer recomendações para corrigir problemas de segurança comuns para aplicações Java e Python. A OWASP Foundation publica uma lista de ferramentas de análise de código-fonte (também conhecidas como ferramentas SAST).
- Implementar um mecanismo para verificar e aplicar patches ao seu ambiente existente, bem como verificação como parte de um processo de construção de pipeline de CI/CD: implemente um mecanismo para verificar e aplicar patches quanto a problemas em suas dependências e sistemas operacionais a fim de ajudar a proteger-se contra novas ameaças. Execute esse mecanismo regularmente. O gerenciamento de vulnerabilidade de software é essencial ao entendimento de onde é necessário aplicar patches ou resolver problemas de software. Priorize a remediação de possíveis problemas de segurança incorporando avaliações de vulnerabilidade no início de seu pipeline de integração/entrega contínua (CI/CD). Sua abordagem pode variar com base nos serviços da AWS que você está consumindo. Para conferir a existência de possíveis problemas no software em execução em instâncias do Amazon EC2, adicione o Amazon Inspector ao seu pipeline para alertar e interromper o processo de compilação se forem detectados problemas ou possíveis defeitos. O Amazon Inspector monitora recursos de forma contínua. Você também pode utilizar produtos de código aberto, como OWASP Dependency-Check, Snyk, OpenVAS, gerenciadores de pacotes e ferramentas de AWS Partner para gerenciamento de vulnerabilidades.
- Utilize o AWS Systems Manager: você é responsável pelo gerenciamento de patches para seus recursos do AWS, incluindo instâncias do Amazon Elastic Compute Cloud (Amazon EC2), imagens de máquina da Amazon (AMIs) e outros recursos de computação. O AWS Systems Manager Patch Manager automatiza o processo de aplicação de patches em instâncias gerenciadas com atualizações relacionadas à segurança e outros tipos de atualizações. O Patch Manager pode ser utilizado para aplicar patches em instâncias do Amazon EC2 para sistemas operacionais e aplicações, como aplicações da Microsoft, pacotes de serviços Windows e atualizações de versão secundária para instâncias baseadas em Linux. Além do Amazon EC2, o Patch Manager também pode ser utilizado para aplicar patches em servidores on-premises.

  Para ter uma lista de sistemas operacionais compatíveis, consulte Sistemas operacionais compatíveis no Guia do usuário do Systems Manager. Você pode verificar instâncias para ver apenas um relatório de patches ausentes ou verificar e instalar automaticamente todos os patches ausentes.
- Utilize do AWS Security Hub: o Security Hub oferece uma visão abrangente do estado de seu sistema na AWS. Ele coleta dados de segurança em vários serviços da AWS e oferece essas

descobertas em um formato personalizado, possibilitando priorizar as descobertas de segurança em serviços da AWS.

- Utilize o AWS CloudFormation: o AWS CloudFormation é um serviço de infraestrutura como código (IaC) que pode ajudar com o gerenciamento de vulnerabilidades automatizando a implantação de recursos e padronizando a arquitetura de recursos em várias contas e ambientes.

Recursos

Documentos relacionados:

- AWS Systems Manager
- Visão geral de segurança do AWS Lambda
- Amazon CodeGuru
- Gerenciamento aprimorado e automatizado de vulnerabilidades para workloads de nuvem com um novo Amazon Inspector
- Automatizar o gerenciamento e a remediação de vulnerabilidades na AWS usando o Amazon Inspector e o AWS Systems Manager: Parte 1

Vídeos relacionados:

- Proteção de serviços com tecnologia sem servidor e de contêiner
- Práticas recomendadas de segurança para o serviço de metadados de instância do Amazon EC2

SEC06-BP02 Reduzir a superfície de ataque

Reduza a exposição ao acesso não intencional protegendo os sistemas operacionais e minimizando componentes, bibliotecas e serviços consumíveis externamente em uso. Primeiro, diminua o número de componentes não utilizados, sejam eles pacotes de sistema operacional ou aplicações para workloads baseadas no Amazon Elastic Compute Cloud (Amazon EC2), sejam eles módulos de software externos no código, para todas as workloads. Encontre muitos guias de configuração de proteção e segurança para sistemas operacionais comuns e software de servidor. Por exemplo, você pode começar com o Center for Internet Security e iterar.

No Amazon EC2, e possível criar as próprias imagens de máquina da Amazon (AMIs), corrigidas e reforçadas, para ajudar você a atender aos requisitos de segurança específicos da sua organização.

Os patches e outros controles de segurança aplicados na AMI são efetivos no momento em que foram criados. Eles não são dinâmicos, a menos que você modifique após a inicialização, por exemplo, com o AWS Systems Manager.

É possível simplificar o processo de criação de AMIs seguras com o EC2 Image Builder. O EC2 Image Builder reduz significativamente o esforço necessário para criar e manter imagens douradas sem escrever e manter a automação. Quando as atualizações de software ficam disponíveis, o Image Builder produz automaticamente uma nova imagem sem exigir que os usuários iniciem manualmente as compilações de imagem. O EC2 Image Builder permite validar facilmente a funcionalidade e a segurança de suas imagens antes de usá-las na produção com testes fornecidos pela AWS e seus próprios testes. Também é possível aplicar as configurações de segurança fornecidas pela AWS para proteger ainda mais suas imagens para atender aos critérios de segurança internos. Por exemplo, você pode produzir imagens em conformidade com o padrão do Guia de implementação técnica de segurança (STIG) usando modelos fornecidos pela AWS.

Com ferramentas de análise de código estático de terceiros é possível identificar problemas de segurança comuns, como limites de entrada de função não verificados, bem como vulnerabilidades e exposições comuns (CVEs) aplicáveis. Você pode usar o Amazon CodeGuru para os idiomas compatíveis. As ferramentas de verificação de dependência também podem ser usadas para determinar se as bibliotecas com as quais o código está vinculado são as versões mais recentes, estão livres de CVEs e têm condições de licenciamento que atendem aos requisitos da política de software.

Usando o Amazon Inspector, você pode executar avaliações de configuração de CVEs conhecidas em suas instâncias, avaliar parâmetros de segurança e automatizar a notificação de defeitos. O Amazon Inspector é executado em instâncias de produção ou em um pipeline de compilação e notifica desenvolvedores e engenheiros quando descobertas estão presentes. Você pode acessar as descobertas programaticamente e direcionar sua equipe para os registros em atraso e os sistemas de rastreamento de bugs. EC2 Image Builder pode ser usado para manter imagens de servidor (AMIs) com aplicação automática de patches, aplicação de políticas de segurança fornecidas pela AWS e outras personalizações. Ao usar contêineres, implemente a Verificação de imagens do ECR no pipeline de compilação e regularmente no repositório de imagens para procurar CVEs nos contêineres.

Embora o Amazon Inspector e outras ferramentas sejam eficazes na identificação de configurações e CVEs presentes, outros métodos são necessários para testar a carga de trabalho no nível do aplicativo. Fuzzing é um método conhecido de encontrar erros usando automação para injetar dados malformados em campos de entrada e outras áreas do aplicativo.

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

Orientação de implementação

- Configure os sistemas operacionais: configure os sistemas operacionais para atender às práticas recomendadas.
  - Securing Amazon Linux
  - Securing Microsoft Windows Server
- Configure recursos em contêiner para atender às práticas recomendadas de segurança.
- Implemente as práticas recomendadas do AWS Lambda.
  - Práticas recomendadas do AWS Lambda

Recursos

Documentos relacionados:

- AWS Systems Manager
- Replacing a Bastion Host with Amazon EC2 Systems Manager (Como substituir um host traga a sua própria licença pelo Amazon EC2 Systems Manager)
- Security Overview of AWS Lambda (Visão geral de segurança do AWS Lambda)

Vídeos relacionados:

- Running high-security workloads on Amazon EKS (Execução de workloads de alta segurança no Amazon EKS)
- Securing Serverless and Container Services (Proteção de serviços com tecnologia sem servidor e de contêiner)
- Security best practices for the Amazon EC2 instance metadata service (Práticas recomendadas de segurança para o serviço de metadados de instância do Amazon EC2

Exemplos relacionados:

- Laboratório: Implantação automatizada do firewall de aplicações Web

SEC06-BP03 Implementar serviços gerenciados

Implemente serviços que gerenciam recursos, como o Amazon Relational Database Service (Amazon RDS), o AWS Lambda e o Amazon Elastic Container Service (Amazon ECS), para reduzir as tarefas de manutenção de segurança como parte do modelo de responsabilidade compartilhada. Por exemplo, o Amazon RDS ajuda você a configurar, operar e escalar um banco de dados relacional, automatiza tarefas de administração, como provisionamento de hardware, configuração de banco de dados, aplicação de patches e backups. Isso significa que você tem mais tempo livre para se concentrar na proteção da aplicação de outras maneiras descritas no AWS Well-Architected Framework. O Lambda permite executar código sem provisionar nem gerenciar servidores e, portanto, você só precisa se concentrar na conectividade, na invocação e na segurança em nível de código, e não na infraestrutura ou no sistema operacional.

Nível de exposição a riscos quando esta prática recomendada não for estabelecida: Médio

Orientações para a implementação

- Explorar os serviços disponíveis: explore, teste e implemente serviços que gerenciam recursos, como Amazon RDS, AWS Lambda e Amazon ECS.

Recursos

Documentos relacionados:

- Site da AWS
- AWS Systems Manager
- Replacing a Bastion Host with Amazon EC2 Systems Manager (Como substituir um bastion host com o Amazon EC2 Systems Manager)
- Security Overview of AWS Lambda (Visão geral de segurança do AWS Lambda)

Vídeos relacionados:

- Running high-security workloads on Amazon EKS (Execução de workloads de alta segurança no Amazon EKS)
- Securing Serverless and Container Services (Proteção de serviços com tecnologia sem servidor e de contêiner)

- Security best practices for the Amazon EC2 instance metadata service (Práticas recomendadas de segurança para o serviço de metadados de instância do Amazon EC2)

Exemplos relacionados:

- Laboratório: AWS Certificate Manager Request Public Certificate

SEC06-BP04 Automatizar a proteção da computação

Automatize seus mecanismos de computação de proteção, incluindo gerenciamento de vulnerabilidades, redução da superfície de ataque e gerenciamento de recursos. A automação ajudará você a investir tempo para proteger outros aspectos da carga de trabalho e reduzir o risco de erros humanos.

Nível de exposição a riscos quando esta prática recomendada não for estabelecida: Médio

Orientações para a implementação

- Automatizar o gerenciamento de configuração: aplique e valide configurações seguras automaticamente usando uma ferramenta ou um serviço de gerenciamento de configuração.
  - AWS Systems Manager
  - AWS CloudFormation
  - Laboratório: Implantação automatizada da VPC
  - Laboratório: Implantação automatizada da aplicação Web no EC2

- Automatizar a aplicação de patches para instâncias do Amazon Elastic Compute Cloud(Amazon EC2): o Patch Manager do AWS Systems Manager automatiza o processo de aplicação de patches em instâncias gerenciadas com atualizações relacionadas à segurança e com outros tipos de atualizações. Você pode usar o gerenciador de patches para aplicar patches a sistemas operacionais e aplicações.
  - AWS Systems Manager Patch Manager
  - Correção centralizada de várias contas e várias regiões com automação do AWS Systems Manager

- Implementar detecção e prevenção de intrusão: implemente uma ferramenta de detecção e prevenção de invasões para monitorar e interromper atividades maliciosas nas instâncias.

- Considerar as soluções de AWS Partner: os parceiros da AWS oferecem centenas de produtos líderes do setor que são equivalentes, idênticos ou se integram aos controles existentes nos seus ambientes on-premises. Esses produtos complementam os serviços da AWS já existentes para que os clientes possam implantar uma arquitetura de segurança abrangente e obter uma experiência mais uniforme na nuvem e no ambiente on-premises.
  - Segurança da infraestrutura

Recursos

Documentos relacionados:

- AWS CloudFormation
- AWS Systems Manager
- AWS Systems Manager Patch Manager
- Correção centralizada de várias contas e várias regiões com automação do AWS Systems Manager
- Segurança da infraestrutura
- Replacing a Bastion Host with Amazon EC2 Systems Manager (Como substituir um bastion host com o Amazon EC2 Systems Manager)
- Security Overview of AWS Lambda (Visão geral de segurança do AWS Lambda)

Vídeos relacionados:

- Running high-security workloads on Amazon EKS (Execução de workloads de alta segurança no Amazon EKS)
- Securing Serverless and Container Services (Proteção de serviços com tecnologia sem servidor e de contêiner)
- Security best practices for the Amazon EC2 instance metadata service (Práticas recomendadas de segurança para o serviço de metadados de instância do Amazon EC2)

Exemplos relacionados:

- Laboratório: Implantação automatizada do firewall de aplicações Web
- Laboratório: Implantação automatizada da aplicação Web no EC2

SEC06-BP05 Permitir que as pessoas executem ações a uma distância

A remoção da capacidade de acesso interativo reduz o risco de erro humano e o potencial de configuração ou gerenciamento manual. Por exemplo, use um fluxo de trabalho de gerenciamento de alterações para implantar instâncias do Amazon Elastic Compute Cloud (Amazon EC2) usando infraestruturas como código e gerenciar instâncias do Amazon EC2 com ferramentas, como o AWS Systems Manager, em vez de permitir acesso direto, ou por meio de um host traga a sua própria licença. O AWS Systems Managerpode automatizar uma variedade de tarefas de manutenção e implantação, usando recursos que incluem fluxos de trabalho de automação ,, documentos (playbooks) e o Run Command. O AWS CloudFormation empilha a compilação com base em pipelines e pode automatizar tarefas de implantação e gerenciamento de infraestrutura sem usar diretamente o AWS Management Console ou APIs.

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

Orientação de implementação

- Substitua o acesso ao controle: substitua o acesso ao console (SSH ou RDP) a instâncias com o Run Command do AWS Systems Manager para automatizar tarefas de gerenciamento.

- AWS Systems Manager Run Command

Recursos

Documentos relacionados:

- AWS Systems Manager
- AWS Systems Manager Run Command
- Replacing a Bastion Host with Amazon EC2 Systems Manager (Como substituir um host traga a sua própria licença pelo Amazon EC2 Systems Manager)
- Security Overview of AWS Lambda (Visão geral de segurança do AWS Lambda)

Vídeos relacionados:

- Running high-security workloads on Amazon EKS (Execução de workloads de alta segurança no Amazon EKS)

- Securing Serverless and Container Services (Proteção de serviços com tecnologia sem servidor e de contêiner)
- Security best practices for the Amazon EC2 instance metadata service (Práticas recomendadas de segurança para o serviço de metadados de instância do Amazon EC2

Exemplos relacionados:

- Laboratório: Implantação automatizada do firewall de aplicações Web

SEC06-BP06 Validar a integridade do software

Implemente mecanismos (por exemplo, assinatura de código) para validar se o software, o código e as bibliotecas usados na workload são de fontes confiáveis e não foram adulterados. Por exemplo, você deve verificar o certificado de assinatura de código de binários e scripts para confirmar o autor e garantir que ele não tenha sido adulterado desde que foi criado pelo autor. AWS Signer pode ajudar a garantir a confiança e a integridade do código gerenciando centralmente o ciclo de vida de assinatura de código, incluindo certificação de assinatura e chaves públicas e privadas. Você pode aprender a usar padrões avançados e práticas recomendadas para assinatura de código com o AWS Lambda. Além disso, uma soma de verificação do software que você faz download, em comparação com a soma de verificação do provedor, pode ajudar a garantir que ela não tenha sido adulterada.

Nível de exposição a riscos quando esta prática recomendada não for estabelecida: Baixo

Orientações para a implementação

- Investigar os mecanismo: a assinatura de código é um mecanismo que pode ser usado para validar a integridade do software.
  - NIST: Considerações de segurança para assinatura de código

Recursos

Documentos relacionados:

- AWS Signer
- New – Code Signing, a Trust and Integrity Control for AWS Lambda (Novo: assinatura de código, um controle de confiança e integridade para o AWS Lambda)

Proteção de dados

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

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

Tópicos

Classificação de dados

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

Práticas recomendadas

SEC07-BP01 Identificar os dados em sua workload

É essencial compreender o tipo e a classificação de dados que sua workload está processando, os processos de negócios associados, onde os dados são armazenados e quem é o proprietário dos dados. Você também deve ter uma compreensão dos requisitos legais e de conformidade aplicáveis

de sua workload e quais controles de dados precisam ser implementados. A identificação dos dados é a primeira etapa da jornada da classificação de dados.

Benefícios do estabelecimento desta prática recomendada:

A classificação dos dados possibilita que os proprietários da workload identifiquem os locais que armazenam dados sigilosos e determinem como esses dados devem ser acessados e compartilhados.

A classificação dos dados tem como objetivo responder às seguintes perguntas:

- Qual tipo de dados você tem?

  Podem ser dados como:

  - Propriedade intelectual (IP), como segredos comerciais, patentes ou contratos.
  - Informações de saúde protegidas (PHI), como registros médicos que contêm informações do histórico médico referente a um indivíduo.
  - Informações de identificação pessoal (PII), como nome, endereço, data de nascimento e ID nacional ou número de registro.
  - Dados do cartão de crédito, como o Número da conta principal (PAN), nome do titular do cartão, data de validade e número do código de serviço.
  - Onde os dados sigilosos são armazenados?
  - Quem pode acessar, modificar e excluir dados?
  - A compreensão das permissões do usuário é essencial na proteção contra o possível uso indevido de dados.
- Quem pode realizar operações de criação, leitura, atualização e exclusão (CRUD)?
  - Considere a possível escalação de privilégios compreendendo quem pode gerenciar permissões aos dados.
- Qual impacto nos negócios poderá ocorrer se os dados forem divulgados de forma acidental, alterados ou excluídos?
  - Entenda a consequência do risco se os dados forem modificados, excluídos ou divulgados acidentalmente.

Ao responder a estas perguntas, você pode realizar as seguintes ações:

- Reduzir o escopo de dados sigilosos (como o número de locais de dados sigilosos) e limitar o acesso aos dados sigilosos somente para usuários aprovados.
- Obtenha um entendimento de diferentes tipos de dados para que você possa implementar técnicas e mecanismos de proteção de dados apropriados, como criptografia, prevenção da perda de dados e gerenciamento de identidade e acesso.
- Otimize os custos entregando os objetivos de controle certos para os dados.
- Responda às perguntas de modo confidencial de reguladores e auditores sobre os tipos e a quantidade de dados e como os dados de diferentes níveis de confidencialidade são isolados uns dos outros.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: alto

Orientação de implementação

Classificação dos dados é o ato de identificar a confidencialidade dos dados. Ela pode envolver marcação para tornar os dados facilmente acessíveis e rastreáveis. A classificação de dados também reduz a duplicação de dados, o que pode ajudar a reduzir os custos de armazenamento e backup enquanto acelera o processo de pesquisa.

Utilize serviços, como o Amazon Macie para automatizar em grande escala a descoberta e a classificação de dados sigilosos. Outros serviços, como Amazon EventBridge e AWS Config, podem ser utilizados para automatizar a remediação de problemas de segurança de dados, como buckets do Amazon Simple Storage Service (Amazon S3) não criptografados e volumes do Amazon EC2 EBS ou recursos de dados não marcados. Para ter uma lista completa de integrações de serviços da AWS, consulte a documentação do EventBridge.

A detecção de PII em dados não estruturados, como e-mails de clientes, tickets de suporte, análises de produtos e redes sociais, é possível com o uso do Amazon Comprehend, que é um serviço de processamento de linguagem natural (PLN) que utiliza machine learning (ML) para encontrar insights e relacionamentos, como pessoas, locais, sentimentos e tópicos em texto não estruturado. Para ter uma lista de serviços da AWS que podem auxiliar na identificação dos dados, consulte Técnicas comuns para detectar dados PHI e PII com o uso de serviços da AWS.

Outro método compatível com a classificação e a proteção de dados é a marcação de recursos da AWS. A marcação possibilita atribuir metadados aos seus recursos da AWS que você pode utilizar para gerenciar, identificar, organizar, procurar e filtrar recursos.

Em alguns casos, você pode optar por marcar recursos inteiros (como um bucket do S3), especialmente quando uma workload ou um serviço específico deve armazenar processos ou transmissões de classificação de dados já conhecidos.

Quando apropriado, é possível marcar um bucket do S3 em vez de objetos individuais para facilidade de administração e manutenção de segurança.

Etapas da implementação

Detectar dados sigilosos no Amazon S3:

1. Antes de começar, você deve ter permissões apropriadas para acessar o console do Amazon Macie e as operações de API. Para ter detalhes adicionais, consulte Conceitos básicos do Amazon Macie.
2. Utilize o Amazon Macie para realizar a descoberta de dados automatizada quando seus dados sigilosos residem no Amazon S3.
   - Utilize o guia Conceitos básicos do Amazon Macie para configurar um repositório para os resultados da descoberta de dados sigilosos e criar um trabalho de descoberta de dados sigilosos.
   - Como utilizar o Amazon Macie para visualizar dados sigilosos em buckets do S3.

     Por padrão, o Macie analisa objetos utilizando o conjunto de identificadores de dados gerenciados que recomendamos para a descoberta automatizada de dados sigilosos. É possível ajustar a análise configurando o Macie para utilizar identificadores de dados gerenciados específicos, identificadores de dados personalizados e listas de permissões quando ele realiza a descoberta automatizada de dados sigilosos para a sua conta ou organização. Você pode ajustar o escopo da análise excluindo buckets específicos (por exemplo, buckets do S3 que geralmente armazenam dados de registro em log da AWS).
3. Para configurar e utilizar a descoberta automatizada de dados sigilosos, consulte Realizar a descoberta automatizada de dados sigilosos com o Amazon Macie.
4. Você também pode considerar Descoberta automatizada de dados para o Amazon Macie.

Detectar dados sigilosos no Amazon RDS:

Para ter mais informações sobre a descoberta de dados em bancos de dados Amazon Relational Database Service (Amazon RDS), consulte Habilitar a classificação de dados para o banco de dados Amazon RDS com o Macie.

Detectar dados sigilosos no DynamoDB:

- Detectar dados sigilosos no DynamoDB com Macie explica como utilizar o Amazon Macie para detectar dados sigilosos em tabelas do Amazon DynamoDB exportando os dados para o Amazon S3 para verificação.

Soluções de parceiros da AWS:

- Considere utilizar nossa AWS Partner Network extensiva. Os parceiros da AWS têm ferramentas e frameworks de conformidade extensas que se integram diretamente aos serviços da AWS. Os parceiros podem oferecer uma solução de governança e conformidade personalizada para ajudar você a atender às suas necessidades organizacionais.
- Para saber sobre as soluções personalizadas em classificação de dados, consulte Governança de dados na era dos requisitos de regulamento e conformidade.

É possível aplicar automaticamente os padrões de marcação que sua organização adota criando e implantando políticas com o uso do AWS Organizations. As políticas de tag possibilitam especificar regras que definem nomes de chave válidas e quais valores são válidos para cada chave. É possível optar somente por monitorar, que oferece a você uma oportunidade de avaliar e limpar suas tags existentes. Depois que suas tags estiverem em conformidade com seus padrões escolhidos, você poderá ativar a aplicação nas políticas de tag a fim de impedir que tags sem conformidade sejam criadas. Para ter mais detalhes, consulte Proteger tags de recursos utilizadas para autorização utilizando uma política de controle de serviço no AWS Organizations e o exemplo de política em Impedir que as tags sejam modificadas, exceto por principais autorizados.

- Para começar a utilizar políticas de tag no AWS Organizations, é altamente recomendável que você siga o fluxo de trabalho em Conceitos básicos de políticas de tag antes de passar para políticas de tag mais avançadas. Compreender os efeitos de anexar uma política de tag simples a uma conta antes de expandir para uma unidade organizacional (UO) ou uma organização inteira permite ver os efeitos de uma política de tag antes de aplicar a conformidade com a política de tag. Conceitos básicos de políticas de tag oferece links para instruções de tarefas relacionadas a política mais avançadas.
- Considere a avaliação de outros serviços e recursos do AWS compatíveis com a classificação de dados, que estão listados no whitepaper Classificação de dados.

Recursos

Documentos relacionados:

- Conceitos básicos do Amazon Macie
- Descoberta automatizada de dados com o Amazon Macie
- Conceitos básicos de políticas de tag
- Detectar entidades de PII

Blogs relacionados:

- Como utilizar o Amazon Macie para visualizar dados sigilosos em buckets do S3.
- Realizar a descoberta automatizada de dados sigilosos com o Amazon Macie
- Técnicas comuns para detectar dados PHI e PII com o uso de serviços da AWS
- Detectar e editar PII com o uso do Amazon Comprehend
- Proteger tags de recursos usadas para autorização utilizando uma política de controle de serviços no AWS Organizations
- Habilitar a classificação do banco de dados Amazon RDS com o Macie
- Detectar dados sigilosos no DynamoDB com o Macie
-

Vídeos relacionados:

- Segurança dos dados orientada a eventos com o uso do Amazon Macie
- Amazon Macie para proteção e governança de dados
- Ajustar descobertas de dados sigilosos com listas de permissão

SEC07-BP02 Definir controles de proteção de dados

Proteja os dados de acordo com seu nível de classificação. Por exemplo, proteja dados classificados como públicos usando recomendações relevantes enquanto protege dados confidenciais com controles adicionais.

Usando tags de recursos, separar contas da AWS por confidencialidade (e potencialmente também por advertência, enclave ou comunidade de interesse), políticas do IAM, SCPs do AWS

Organizations, AWS Key Management Service (AWS KMS) e AWS CloudHSM, você pode definir e implementar as políticas de classificação e proteção de dados com criptografia. Por exemplo, se você tiver buckets do S3 que contêm dados altamente críticos ou instâncias do Amazon Elastic Compute Cloud (Amazon EC2) que processam dados confidenciais, eles poderão ser marcados com uma tag `Project=ABC` . Somente a equipe imediata sabe o que o código do projeto significa e fornece meios de usar o controle de acesso baseado em atributos. Você pode definir os níveis de acesso às chaves de criptografia do AWS KMS por meio de políticas de chave e concessões para garantir que somente os serviços apropriados tenham acesso ao conteúdo confidencial por meio de um mecanismo seguro. Se você estiver tomando decisões de autorização com base em tags, certifique-se de que as permissões nas tags sejam definidas adequadamente usando políticas de tags no AWS Organizations.

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

Orientação de implementação

- Defina o esquema de identificação e classificação de dados: a identificação e a classificação de seus dados são realizadas para avaliar o potencial impacto e o tipo de dados que você está armazenando e quem deve acessá-los.
  - Documentação da AWS
- Descubra os controles disponíveis da AWS: descubra os controles de segurança para os serviços da AWS que você usa ou planeja usar. Muitos serviços têm uma seção de segurança em sua documentação.
  - Documentação da AWS
- Identificar recursos de conformidade da AWS: identifique os recursos da AWS disponíveis para ajudar.
  - https://aws.amazon.com/compliance/

Recursos

Documentos relacionados:

- Documentação da AWS
- Whitepaper Classificação de dados
- Conceitos básicos do Amazon Macie
- Texto ausente

Vídeos relacionados:

- Introducing the New Amazon Macie (Apresentação do novo Amazon Macie)

SEC07-BP03 Automatizar a identificação e a classificação

automatizar a identificação e a classificação de dados pode ajudar a implementar os controles corretos. O uso de automação para isso, em vez de acesso direto de uma pessoa, reduz o risco de erros humanos e exposição. Você deve avaliar o uso de uma ferramenta, como o Amazon Macie, que usa machine learning para descobrir, classificar e proteger automaticamente dados confidenciais na AWS. O Amazon Macie reconhece dados confidenciais, como informações de identificação pessoal (PII) ou propriedade intelectual, e fornece painéis e alertas que dão visibilidade sobre como esses dados estão sendo acessados ou movidos.

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

Orientação de implementação

- Use o Amazon Simple Storage Service (Amazon S3) Inventory: o Amazon S3 Inventory é uma das ferramentas que você pode usar para auditar e gerar relatórios sobre o status de replicação e criptografia de seus objetos.
  - Amazon S3 Inventory
- Considere o Amazon Macie: O Amazon Macie usa o machine learning para descobrir e classificar automaticamente os dados armazenados no Amazon S3.
  - Amazon Macie

Recursos

Documentos relacionados:

- Amazon Macie
- Amazon S3 Inventory
- Whitepaper Classificação de dados
- Conceitos básicos do Amazon Macie

Vídeos relacionados:

- Introducing the New Amazon Macie (Apresentação do novo Amazon Macie)

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

sua estratégia de ciclo de vida definida deve ser baseada no nível de confidencialidade, bem como nos requisitos legais e organizacionais. Aspectos como a duração pela qual você retém dados, processos de destruição de dados, gerenciamento de acesso a dados, transformação de dados e compartilhamento de dados devem ser considerados. Ao escolher uma metodologia de classificação de dados, equilibre usabilidade e acesso. Considere também os vários níveis de acesso e nuances para implementar uma abordagem segura, mas utilizável, para cada nível. Sempre use uma abordagem de defesa detalhada e reduza o acesso humano a dados e mecanismos para transformar, excluir ou copiar dados. Por exemplo, exija que os usuários se autentiquem fortemente em uma aplicação e conceda a ela, e não aos usuários, a permissão de acesso necessária para executar uma ação a distância. Além disso, garanta que os usuários venham de um caminho de rede confiável e exijam acesso às chaves de descriptografia. Use ferramentas como painéis ou relatórios automatizados para fornecer aos usuários informações extraídas dos dados e não acesso direto aos dados.

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

Orientação de implementação

- Identificar tipos de dados: identifique os tipos de dados que você está armazenando ou processando em sua workload. Esses dados podem ser texto, imagens, bancos de dados binários, entre outros.

Recursos

Documentos relacionados:

- Whitepaper Classificação de dados
- Conceitos básicos do Amazon Macie

Vídeos relacionados:

- Introducing the New Amazon Macie (Apresentação do novo Amazon Macie)

Proteção de dados em repouso

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

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

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

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

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

Práticas recomendadas

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

- SEC08-BP04 Impor o controle de acesso
- SEC08-BP05 Usar mecanismos para evitar que as pessoas acessem os dados

SEC08-BP01 Implementar gerenciamento de chaves seguro

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

Resultado desejado: um mecanismo de gerenciamento de chaves escalável, repetível e automatizado. O mecanismo deve fornecer a capacidade de impor o acesso de privilégio mínimo ao material essencial e fornecer o equilíbrio correto entre disponibilidade, confidencialidade e integridade das chaves. O acesso às chaves deve ser monitorado e o material da chave deve ser rotacionado por meio de um processo automatizado. O material de chave nunca deve estar acessível a identidades humanas.

Antipadrões comuns:

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

Benefícios de estabelecer esta prática recomendada: Ao estabelecer um mecanismo seguro de gerenciamento de chaves para sua workload, você pode ajudar a proteger seu conteúdo contra acesso não autorizado. Além disso, você pode estar sujeito aos requisitos regulamentares para criptografar seus dados. Uma solução eficaz de gerenciamento de chaves pode fornecer mecanismos técnicos alinhados a essas regulamentações para proteger o material chave.

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

Orientação para implementação

Muitos requisitos regulatórios e práticas recomendadas incluem a criptografia de dados em repouso como um controle de segurança fundamental. Para cumprir esse controle, sua workload precisa de um mecanismo para armazenar e gerenciar com segurança o material chave usado para criptografar seus dados em repouso.

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

Ao implantar workloads usando uma estratégia de várias contas, isso é considerado prática recomendada para manter chaves do AWS KMS na mesma conta da workload que as usa. Nesse modelo distribuído, a responsabilidade pelo gerenciamento das chaves do AWS KMS é da equipe de aplicações. Em outros casos de uso, as organizações podem optar por armazenar as chaves do AWS KMS em uma conta centralizada. Essa estrutura centralizada requer políticas adicionais para permitir o acesso entre contas necessário para que a conta da workload acesse as chaves armazenadas na conta centralizada, mas pode ser mais aplicável em casos de uso em que uma única chave é compartilhada entre várias Contas da AWS.

Independentemente de onde o material da chave esteja armazenado, o acesso à chave deve ser rigorosamente controlado por meio do uso de políticas de chave e políticas do IAM. Políticas de chave são a principal forma de controlar o acesso a uma chave do AWS KMS. Além disso, concessões à chave do AWS KMS podem fornecer acesso a serviços da AWS para criptografar e descriptografar dados em seu nome. Reserve um tempo para revisar as práticas recomendadas para controle de acesso às chaves do AWS KMS.

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

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

Etapas da implementação

1. Determine as opções adequadas de gerenciamento de chaves (gerenciado pela AWS ou gerenciado pelo cliente) para a chave.
   - Para facilitar o uso, a AWS oferece, para a maioria dos serviços, chaves de propriedade da AWS e gerenciadas por ela, que fornecem capacidade de criptografia em repouso sem a necessidade de gerenciar materiais ou políticas de chaves.
   - Ao usar chaves gerenciadas pelo cliente, considere o armazenamento de chaves padrão para fornecer o melhor equilíbrio entre agilidade, segurança, soberania de dados e disponibilidade. Outros casos de uso podem exigir o uso de armazenamentos de chaves personalizadas com AWS CloudHSM ou o armazenamento de chaves externo.
2. Analise a lista de serviços que você está usando para sua workload para entender como o AWS KMS se integra ao serviço. Por exemplo, as instâncias do EC2 podem usar volumes criptografados do EBS, verificando se os snapshots do Amazon EBS criados a partir desses volumes também são criptografados usando uma chave gerenciada pelo cliente e mitigando a divulgação acidental de dados de snapshots não criptografados.
   - Como os serviços da AWS são usados no AWS KMS
   - Para obter informações detalhadas sobre as opções de criptografia que um serviço da AWS oferece, consulte o tópico Criptografia em repouso no guia do usuário ou no guia do desenvolvedor do serviço.
3. Implemente o AWS KMS: o AWS KMS simplifica a criação e o gerenciamento de chaves e o controle do uso da criptografia em uma ampla variedade de serviços da AWS e em suas aplicações.
   - Conceitos básicos: AWS Key Management Service (AWS KMS)
   - Revise as práticas recomendadas para controle de acesso às chaves do AWS KMS.
4. Considere o AWS Encryption SDK: use a integração do AWS Encryption SDK com o AWS KMS quando sua aplicação precisar criptografar dados no lado do cliente.
   - AWS Encryption SDK
5. Habilite o IAM Access Analyzer para revisar e notificar automaticamente se houver políticas de chave do AWS KMS excessivamente amplas.
6. Habilite o Security Hub para receber notificações se houver políticas de chaves configuradas incorretamente, chaves programadas para exclusão ou chaves sem a rotação automática ativada.

7. Determine o nível de registro em log apropriado para suas chaves do AWS KMS. Como as chamadas para o AWS KMS, incluindo eventos somente para leitura, são registradas em log, os logs do CloudTrail associados ao AWS KMS podem se tornar volumosos.
   - Algumas organizações preferem registrar a atividade de log do AWS KMS em uma trilha separada. Para obter mais detalhes, consulte a seção Registro em log de chamadas de API do AWS KMS com CloudTrail do guia do desenvolvedor do AWS KMS.

Recursos

Documentos relacionados:

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

Vídeos relacionados:

- How Encryption Works in AWS (Como funciona a criptografia na AWS)
- Securing Your Block Storage on AWS (Proteger seu armazenamento em bloco na AWS)
- AWS data protection: Using locks, keys, signatures, and certificates (Proteção de dados da AWS: uso de travas, chaves, assinaturas e certificados)

Exemplos relacionados:

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

SEC08-BP02 Aplicar criptografia em repouso

É necessário implementar o uso de criptografia para dados em repouso. A criptografia mantém a confidencialidade dos dados sigilosos em caso de acesso não autorizado ou divulgação acidental.

Resultado desejado: os dados privados devem ser criptografados por padrão quando em repouso. A criptografia ajuda a manter a confidencialidade dos dados e oferece uma camada adicional de proteção contra a divulgação intencional ou acidental de dados ou exfiltração. Dados criptografados não podem ser lidos nem acessados sem primeiro descriptografá-los. Todos os dados armazenados não criptografados devem ser inventariados e controlados.

Antipadrões comuns:

- Não utilizar configurações de criptografia por padrão.
- Conceder acesso excessivamente permissivo para chaves de descriptografia.
- Não monitorar o uso de chaves de criptografia e descriptografia.
- Armazenar dados não criptografados.
- Utilizar a mesma chave de criptografia para todos os dados, seja qual for o uso, os tipos e a classificação de dados.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: alto

Orientação de implementação

Mapeie as chaves de criptografia às classificações de dados em suas workloads. Essa abordagem ajuda a proteger-se contra o acesso excessivamente permissivo ao utilizar uma chave única ou um número muito pequeno de chaves de criptografia para seus dados (consulte SEC07-BP01 Identificar os dados em sua workload).

O AWS Key Management Service (AWS KMS) integra-se a muitos serviços da AWS para facilitar a criptografia de seus dados em repouso. Por exemplo, no Amazon Simple Storage Service (Amazon S3), você pode definir a criptografia padrão em um bucket para que os novos objetos sejam criptografados automaticamente. Ao utilizar o AWS KMS, considere o nível de restrição necessário para os dados. Chaves do AWS KMS controladas por serviço e padrão são gerenciadas e utilizadas em seu nome pelo AWS. Para dados sigilosos que exijam acesso refinado à chave de criptografia subjacente, considere chaves gerenciadas pelo cliente (CMKs). Você tem total controle sobre as CMKs, como gerenciamento de alternância e acesso pelo uso de políticas de chave.

Além disso, o Amazon Elastic Compute Cloud (Amazon EC2) e o Amazon S3 são compatíveis com a imposição de criptografia ao definir a criptografia padrão. Você pode usar o Regras do AWS Config para conferir automaticamente se está usando criptografia, por exemplo, volumes do Amazon Elastic Block Store (Amazon EBS), instâncias do Amazon Relational Database Service (Amazon RDS) e buckets do Amazon S3.

A AWS também oferece operações de criptografia do lado do cliente, possibilitando que você criptografe os dados antes de fazer upload deles para a nuvem. O AWS Encryption SDKoferece uma forma de criptografar seus dados utilizando a criptografia envelopada. Você fornece a chave de encerramento, e o AWS Encryption SDK gera uma chave de dados exclusiva para cada objeto de dados que ele criptografa. Considere utilizar o AWS CloudHSM se precisar de um módulo de segurança de hardware de um locatário (HSM) gerenciado. O AWS CloudHSM possibilita gerar, importar e gerenciar chaves criptográficas em um HSM validado de nível 3 FIPS 140-2. Alguns casos de uso do AWS CloudHSM incluem proteger chaves privadas para emitir uma autoridade de certificado (CA) e ativar a criptografia de dados transparente (TDE) para bancos de dados Oracle. O AWS CloudHSM Client SDK oferece software que possibilita criptografar dados do lado do cliente com chaves armazenadas no AWS CloudHSM antes de fazer upload de seus dados para AWS. O Amazon DynamoDB Encryption Client também possibilita criptografar e assinar itens antes de fazer upload para uma tabela do DynamoDB.

Etapas da implementação

- Impor criptografia em repouso para o Amazon S3: implemente a criptografia padrão do bucket do Amazon S3.

  Configurar a criptografia padrão para volumes do Amazon EBS: especifique que você deseja que todos os volumes do Amazon EBS recém-criados sejam criados em formato criptografado, com a opção de usar a chave padrão fornecida pela AWS ou uma chave que você criar.

  Configurar imagens de máquina da Amazon (AMIs) criptografadas: a cópia de uma AMI existente com criptografia habilitada criptografará automaticamente os volumes raiz e os snapshots.

  Configurar a criptografia do Amazon RDS: configure a criptografia para seus clusters de banco de dados Amazon RDS e snapshots em repouso utilizando a opção de criptografia.

  Criar e configurar chaves do AWS KMS com políticas que limitem o acesso às entidades principais apropriadas para cada classificação de dados: por exemplo, crie uma chave do AWS KMS para criptografar dados de produção e uma chave diferente para criptografar dados de desenvolvimento ou teste. Você também pode conceder acesso de chave a outras Contas da AWS. Considere ter contas diferentes para seus ambientes de desenvolvimento e produção. Se seu ambiente de produção precisar descriptografar artefatos na conta de desenvolvimento, você poderá editar a política de CMK utilizada para criptografar os artefatos de desenvolvimento a fim de conferir à conta de produção a capacidade de descriptografar esses artefatos. O ambiente de produção pode, então, ingerir os dados descriptografados para uso na produção.

Configurar a criptografia em serviços da AWS adicionais: para outros serviços da AWS utilizados, leia a documentação de segurança do serviço em questão para determinar as opções de criptografia do serviço.

Recursos

Documentos relacionados:

- Ferramentas de criptografia da AWS
- Documentação da AWS
- AWS Encryption SDK
- Whitepaper de detalhes criptográficos do AWS KMS
- AWS Key Management Service
- Ferramentas e serviços criptográficos da AWS
- Criptografia do Amazon EBS
- Criptografia padrão de volumes do Amazon EBS
- Criptografar recursos do Amazon RDS
- Como ativo a criptografia padrão para um bucket do Amazon S3?
- Proteger dados do Amazon S3 com o uso de criptografia

Vídeos relacionados:

- Como a criptografia funciona na AWS
- Proteger o armazenamento em bloco na AWS

SEC08-BP03 Automatizar a proteção de dados em repouso

Use ferramentas automatizadas para validar e impor controles de dados em repouso continuamente, por exemplo, verificar se há apenas recursos de armazenamento criptografados. Você pode automatizar a validação de que todos os volumes do EBS são criptografados com o uso do Regras do AWS Config. AWS Security Hub também pode verificar vários controles diferentes por meio de verificações automatizadas em relação a padrões de segurança. Além disso, o Regras do AWS Config pode corrigir recursos não compatíveis automaticamente.

Nível de exposição a riscos quando esta prática recomendada não for estabelecida: Médio

Orientações para a implementação

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

Garantir a criptografia em repouso: garanta que a única maneira de armazenar dados seja usando a criptografia. O AWS KMS se integra perfeitamente a muitos serviços da AWS para facilitar a criptografia de todos os seus dados em repouso. Por exemplo, no Amazon Simple Storage Service (Amazon S3), você pode definir a criptografia padrão em um bucket para que todos os novos objetos sejam criptografados automaticamente. Além disso, o Amazon EC2 e Amazon S3 oferecem suporte à imposição de criptografia ao definir a criptografia padrão. Você pode usar o AWS Managed Config Rules para verificar automaticamente se você está usando criptografia, por exemplo, para Volumes do EBS, instâncias do Amazon Relational Database Service (Amazon RDS)e aos Amazon S3.

Recursos

Documentos relacionados:

- Ferramentas de criptografia da AWS
- SDK de criptografia da AWS

Vídeos relacionados:

- How Encryption Works in AWS (Como a criptografia funciona na AWS)
- Securing Your Block Storage on AWS (Como proteger o armazenamento em bloco na AWS)

SEC08-BP04 Impor o controle de acesso

Para ajudar a proteger seus dados em repouso, implemente o controle de acesso utilizando mecanismos, como isolamento e versionamento, e aplique o princípio de privilégio mínimo. Evite conceder acesso público aos seus dados.

Resultado desejado: garantir que somente usuários autorizados possam acessar os dados conforme a necessidade. Proteger seus dados com backups regulares e versionamento a fim de impedir a

modificação ou a exclusão de dados intencionais ou acidentais. Isolar dados críticos de outros dados a fim de proteger a confidencialidade e a integridade deles.

Antipadrões comuns:

- Armazenar dados com requisitos de confidencialidade ou classificações diferentes juntos.
- Utilizar permissões excessivamente permissivas em chaves de descriptografia.
- Classificar dados de modo inadequado.
- Não reter backups detalhados de dados importantes.
- Conceder acesso persistente a dados de produção.
- Não auditar o acesso aos dados nem rever as permissões regularmente

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: baixo

Orientação de implementação

Vários controles podem ajudar a proteger seus dados em repouso, por exemplo, acesso (utilizando privilégio mínimo), isolamento e versionamento. Deve ser feita a auditoria de acesso aos seus dados com os mecanismos de detecção, como AWS CloudTrail e os logs de nível de serviço, como os logs de acesso do Amazon Simple Storage Service (Amazon S3). Você deve inventariar quais dados são acessíveis publicamente e criar um plano para reduzir a quantidade de dados disponíveis ao longo do tempo.

O Amazon S3 Glacier Vault Lock e o Amazon S3 Object Lock fornecem controle de acesso obrigatório para os objetos no Amazon S3. Assim que uma política de cofre é bloqueada com a opção de conformidade, nem mesmo o usuário raiz pode alterá-la até que o bloqueio expire.

Etapas da implementação

- Aplicar o controle de acesso: aplique o controle de acesso com privilégios mínimos, incluindo acesso a chaves de criptografia.
- Dados separados com base em diferentes níveis de classificação: use diferentes Contas da AWS para níveis de classificação de dados e gerencie essas contas com o AWS Organizations.
- Analisar as políticas do AWS Key Management Service (AWS KMS): analise o nível de acesso concedido nas políticas do AWS KMS.
- Revisar as permissões de objeto e de bucket do Amazon S3: revise regularmente o nível de acesso concedido nas políticas de bucket do S3. Uma das práticas recomendadas é evitar buckets

que possam ser lidos ou gravados publicamente. Considere o uso do AWS Config para detectar buckets que estão disponíveis publicamente e do Amazon CloudFront para fornecer conteúdo do Amazon S3. Garanta que os buckets que não devem permitir acesso público sejam configurados adequadamente para evitar o acesso público. Por padrão, todos os buckets do S3 são privados e só ser acessados por usuários que receberam explicitamente esse acesso.

- Ativar o AWS IAM Access Analyzer: o IAM Access Analyzer analisa os buckets do Amazon S3 e gera uma descoberta quando uma política do S3 concede acesso a uma entidade externa.
- Habilitar o versionamento do Amazon S3 e o bloqueio de objetos quando apropriado.
- Utilizar o Amazon S3 Inventory: o Amazon S3 Inventory pode ser usado para auditar e gerar relatórios sobre o status de replicação e criptografia de seus objetos do S3.
- Revisar as permissões do Amazon EBS e do compartilhamento de AMIs: as permissões de compartilhamento podem permitir que imagens e volumes sejam compartilhados com Contas da AWS externas à sua workload.
- Revise os compartilhamentos do AWS Resource Access Manager periodicamente para determinar se os recursos devem continuar a ser compartilhados. O Resource Access Manager possibilita compartilhar recursos, como políticas do AWS Network Firewall, regras do Amazon Route 53 Resolver e sub-redes em suas Amazon VPCs. Faça auditoria em recursos compartilhados regularmente e interrompa o compartilhamento dos que não precisem mais ser compartilhados.

Recursos

Práticas recomendadas relacionadas:

- SEC03-BP01 Definir requisitos de acesso
- SEC03-BP02 Conceder acesso com privilégio mínimo

Documentos relacionados:

- Whitepaper de detalhes criptográficos do AWS KMS
- Introdução ao gerenciamento de permissões de acesso aos seus recursos do Amazon S3
- Visão geral do gerenciamento de acesso dos recursos do AWS KMS
- Regras do AWS Config
- Amazon S3 + Amazon CloudFront: uma combinação perfeita na nuvem
- Usar versionamento

- Bloquear objetos usando o Bloqueio de objetos do Amazon S3
- Compartilhar um snapshot do Amazon EBS
- AMIs compartilhadas
- Hospedar uma aplicação de uma página no Amazon S3

Vídeos relacionados:

- Proteger o armazenamento em bloco na AWS

SEC08-BP05 Usar mecanismos para evitar que as pessoas acessem os dados

Impeça que os usuários acessem dados e sistemas confidenciais diretamente em circunstâncias operacionais normais. Por exemplo, use um fluxo de trabalho de gerenciamento de alterações para gerenciar instâncias do Amazon Elastic Compute Cloud (Amazon EC2) usando ferramentas em vez de permitir acesso direto ou um host traga a sua própria licença. Isso pode ser obtido usando o AWS Systems Manager Automation, que usa documentos de automação que contêm etapas que você usa para realizar tarefas. Esses documentos podem ser armazenados no controle de origem, analisados por pares antes da execução e testados detalhadamente para minimizar os riscos em comparação com o acesso ao shell. Os usuários empresariais podem ter um painel em vez de acesso direto a um armazenamento de dados para executar consultas. Quando os pipelines de CI/CD não forem usados, determine quais controles e processos são necessários para fornecer adequadamente um mecanismo de acesso break-glass normalmente desabilitado.

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

Orientação de implementação

- Implemente mecanismos para manter as pessoas longe dos dados: os mecanismos incluem o uso de painéis, como o Amazon QuickSight, para exibir dados aos usuários em vez de consultar diretamente.
  - Amazon QuickSight
- Automatize o gerenciamento de configuração: execute ações remotas, aplique e valide configurações seguras automaticamente usando uma ferramenta ou um serviço de gerenciamento de configuração. Evite usar hosts traga a sua própria licença ou acessar diretamente instâncias do EC2.

- AWS Systems Manager
- AWS CloudFormation
- Pipeline de CI/CD do AWS CloudFormation para modelos na AWS

Recursos

Documentos relacionados:

- Whitepaper de detalhes criptográficos do AWS KMS

Vídeos relacionados:

- How Encryption Works in AWS (Como a criptografia funciona no AWS Backup)
- Securing Your Block Storage on AWS (Como proteger o armazenamento em bloco na AWS)

Proteção de dados em trânsito

Dados em trânsito são quaisquer dados enviados de um sistema para outro. Isso inclui a comunicação entre recursos em sua carga de trabalho, bem como a comunicação entre outros serviços e seus usuários finais. Ao fornecer o nível apropriado de proteção para os dados em trânsito, você protege a confidencialidade e a integridade dos dados de sua carga de trabalho.

Proteja dados entre VPC ou locais on-premises: Você pode usar o AWS PrivateLink para criar uma conexão de rede segura e privada entre Amazon Virtual Private Cloud (Amazon VPC) ou conectividade on-premises para serviços hospedados na AWS. Você pode acessar serviços da AWS, serviços de terceiros e serviços em outras Contas da AWS como se estivessem em sua rede privada. Com o AWS PrivateLink, é possível acessar serviços em contas com CIDRs de IP sobrepostos sem precisar de um Gateway de Internet ou NAT. Você também não precisa configurar regras de firewall, definições de caminho ou tabelas de rotas. O tráfego permanece no backbone da Amazon e não atravessa a internet, portanto, seus dados estão protegidos. É possível manter a conformidade com os regulamentos de conformidade específicos do setor, como HIPAA e EU/US Privacy Shield. O AWS PrivateLink funciona perfeitamente com soluções de terceiros para criar uma rede global simplificada, permitindo acelerar a migração para a nuvem e aproveitar os serviços disponíveis da AWS.

Práticas recomendadas

- SEC09-BP01 Implementar o gerenciamento seguro de chaves e certificados
- SEC09-BP02 Aplicar a criptografia em trânsito
- SEC09-BP03 Automatizar a detecção de acesso não intencional a dados
- SEC09-BP04 Autenticar as comunicações de rede

SEC09-BP01 Implementar o gerenciamento seguro de chaves e certificados

Os certificados Transport Layer Security (TLS) são usados para proteger as comunicações de rede e estabelecer a identidade de sites, recursos e workloads na internet, bem como em redes privadas.

Resultado desejado: Um sistema seguro de gerenciamento de certificados que pode provisionar, implantar, armazenar e renovar certificados em uma infraestrutura de chave pública (PKI). Um mecanismo seguro de gerenciamento de chaves e certificados evita que o material da chave privada do certificado seja divulgado e renova automaticamente o certificado periodicamente. Ele também se integra a outros serviços para fornecer comunicações de rede seguras e identidade para os recursos da máquina na workload. O material de chave nunca deve estar acessível a identidades humanas.

Antipadrões comuns:

- Executar etapas manuais durante os processos de implantação ou renovação de certificado.
- Não prestar a devida atenção à hierarquia da autoridade de certificação (CA) ao criar uma CA privada.
- Usar certificados autoassinados para recursos públicos.

Benefícios de estabelecer esta prática recomendada:

- Simplificar o gerenciamento de certificados por meio de implantação e renovação automatizadas.
- Incentivar a criptografia de dados em trânsito usando certificados TLS.
- Aumentar a segurança e a auditabilidade das ações de certificação realizadas pela autoridade de certificação.
- Organizar as tarefas de gerenciamento em diferentes camadas da hierarquia da CA.

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

Orientação para implementação

As workloads modernas fazem uso extensivo de comunicações de rede criptografadas usando protocolos de PKI, como TLS. O gerenciamento de certificados PKI pode ser complexo, mas o provisionamento, a implantação e a renovação automatizados de certificados podem reduzir o atrito associado ao gerenciamento deles.

A AWS oferece dois serviços para gerenciar certificados de PKI de uso geral: AWS Certificate Manager e AWS Private Certificate Authority (AWS Private CA). O ACM é o principal serviço que os clientes usam para provisionar, gerenciar e implantar certificados para uso em workloads públicas e privadas da AWS. O ACM emite certificados usando o AWS Private CA e integra-se a muitos outros serviços gerenciados da AWS para fornecer certificados TLS seguros para workloads.

A AWS Private CA permite estabelecer a própria autoridade de certificação raiz ou subordinada e emitir certificados TLS por meio de uma API. É possível usar esses tipos de certificado em cenários em que você controla e gerencia a cadeia de confiança do lado do cliente da conexão TLS. Além dos casos de uso do TLS, a AWS Private CA pode ser usada para emitir certificados para pods do Kubernetes, atestados de produtos de dispositivos Matter, assinatura de código e outros casos de uso com um modelo personalizado. Você também pode usar IAM Roles Anywhere para fornecer credenciais do IAM temporárias para workloads on-premises que receberam certificados X.509 assinados pela CA privada.

Além do ACM e do AWS Private CA, o AWS IoT Core oferece suporte especializado para provisionar, gerenciar e implantar certificados de PKI em dispositivos de IoT. O AWS IoT Core fornece mecanismos especializados para integração de dispositivos de IoT à infraestrutura de chave pública em grande escala.

Considerações para estabelecer uma hierarquia de CA privada

Quando precisar estabelecer uma CA privada, é importante tomar cuidado especial para projetar adequadamente a hierarquia da CA com antecedência. É uma prática recomendada implantar cada nível de sua hierarquia de CA em Contas da AWS separadas ao criar uma hierarquia de CA privada. Essa etapa intencional reduz a área de superfície de cada nível na hierarquia da CA, simplificando a descoberta de anomalias nos dados de log do CloudTrail e reduzindo o escopo de acesso ou impacto se houver acesso não autorizado a uma das contas. A CA raiz deve residir em uma própria conta separada e deve ser usada somente para emitir um ou mais certificados de CA intermediários.

Depois, crie uma ou mais CAs intermediárias em contas separadas da conta da CA raiz para emitir certificados para usuários finais, dispositivos ou outras workloads. Por fim, emita certificados da CA raiz para as CAs intermediárias, que, por sua vez, emitirão certificados para os usuários finais ou

dispositivos. Para obter mais informações sobre como planejar a implantação de CA e projetar a hierarquia de CA, incluindo planejamento de resiliência, replicação entre regiões, compartilhamento de CAs na organização e muito mais, consulte Planning your AWS Private CA deployment.

Etapas da implementação

1. Determine os serviços da AWS relevantes e necessários para seu caso de uso:
   - Muitos casos de uso podem aproveitar a infraestrutura de chave pública da AWS existente usando o AWS Certificate Manager. O ACM pode ser usado para implantar certificados TLS para servidores web, balanceadores de carga ou outros usos para certificados publicamente confiáveis.
   - Considere AWS Private CA quando precisar estabelecer a própria hierarquia de autoridade de certificação privada ou precisar acessar certificados exportáveis. O ACM pode então ser usado para emitir muitos tipos de certificados de entidade final usando a AWS Private CA.
   - Para casos de uso em que os certificados devem ser provisionados em grande escala para dispositivos incorporados de Internet das Coisas (IoT), pense no AWS IoT Core.
2. Implemente a renovação automática do certificado sempre que possível:
   - Use a renovação gerenciada pelo ACM para certificados emitidos pelo ACM junto com serviços gerenciados da AWS integrados.
3. Estabeleça trilhas de auditoria e registro:
   - Habilite o Logs do CloudTrail para monitorar o acesso às contas que têm autoridades de certificação. Considere configurar a validação da integridade do arquivo de log no CloudTrail para verificar a autenticidade dos dados de log.
   - Gere e revise periodicamente relatórios de auditoria que listam os certificados que a CA privada emitiu ou revogou. Esses relatórios podem ser exportados para um bucket do S3.
   - Ao implantar uma CA privada, você também precisará estabelecer um bucket do S3 para armazenar a lista de revogação de certificados (CRL). Para obter orientação sobre como configurar esse bucket do S3 com base nos requisitos da workload, consulte Planejar uma lista de revogação de certificados (CRL).

Recursos

Práticas recomendadas relacionadas:

- SEC02-BP02 Usar credenciais temporárias
- SEC08-BP01 Implementar gerenciamento de chaves seguro

- SEC09-BP04 Autenticar as comunicações de rede

Documentos relacionados:

- How to host and manage an entire private certificate infrastructure in AWS
- How to secure an enterprise scale ACM Private CA hierarchy for automotive and manufacturing
- Práticas recomendadas de CA privada
- How to use AWS RAM to share your ACM Private CA cross-account

Vídeos relacionados:

- Activating AWS Certificate Manager Private CA (workshop)

Exemplos relacionados:

- Workshop de CA privada
- IOT Device Management Workshop (incluindo provisionamento de dispositivos)

Ferramentas relacionadas:

- Plug-in para o gerenciador de certificados do Kubernetes para usar a AWS Private CA

SEC09-BP02 Aplicar a criptografia em trânsito

Aplique os requisitos de criptografia definidos com base em políticas, obrigações regulatórias e padrões da organização para cumprir os requisitos organizacionais, legais e de conformidade. Utilize somente protocolos com criptografia ao transmitir dados sigilosos para fora da sua nuvem privada virtual (VPC). A criptografia ajuda a manter a confidencialidade dos dados mesmo quando os dados passam por redes não confiáveis.

Resultado desejado: todos os dados devem ser criptografados em trânsito com pacotes de criptografia e protocolos TLS seguros. O tráfego de rede entre seus recursos e a Internet deve ser criptografado para reduzir o acesso não autorizado aos dados. O tráfego de rede exclusivamente em seu ambiente interno da AWS deve ser criptografado com TLS sempre que possível. A rede interna da AWS é criptografada por padrão e o tráfego de rede em uma VPC não pode ser adulterado nem interceptado a menos que uma parte não autorizada tenha obtido acesso ao recurso que esteja

gerando o tráfego (como instâncias do Amazon EC2 e contêineres do Amazon ECS). Considere proteger o tráfego de rede para rede com uma rede privada virtual (VPN) IPsec.

Antipadrões comuns:

- Utilizar versões obsoletas de SSL, TLS e componentes do pacote de criptografia (por exemplo, SSL v3.0, chaves RSA de 1024 bits e criptografia RC4).
- Permitir tráfego não criptografado (HTTP) para ou de recursos voltados para o público.
- Não monitorar e substituir certificados X.509 antes da validade.
- Utilizar certificados X.509 autoassinados para TLS.

Nível de exposição a riscos quando esta prática recomendada não é estabelecida: alto

Orientação de implementação

Os serviços da AWS fornecem endpoints HTTPS usando TLS para comunicação, fornecendo criptografia em trânsito quando se comunicam com as APIs da AWS. Protocolos não seguros, como HTTP, podem ser auditados e bloqueados em uma VPC por meio do uso de grupos de segurança. Solicitações HTTP também podem ser redirecionadas automaticamente para HTTPS no Amazon CloudFront ou em um Application Load Balancer. Você tem controle total sobre seus recursos de computação para implementar a criptografia em trânsito em seus serviços. Além disso, você pode usar a conectividade VPN em sua VPC a partir de uma rede externa ou AWS Direct Connect para facilitar a criptografia do tráfego. Verifique se os seus clientes estão fazendo chamadas para APIs da AWS utilizando pelo menos TLS 1.2, pois a AWS tornará obsoleto o uso de TLS 1.0 e 1.1 em junho de 2023. Soluções de terceiros estão disponíveis no AWS Marketplace, caso você tenha requisitos especiais.

Etapas da implementação

- Aplicar a criptografia em trânsito: os requisitos de criptografia definidos devem se basear nos mais recentes padrões e práticas recomendadas e permitir apenas protocolos seguros. Por exemplo, configure apenas um grupo de segurança para permitir o protocolo HTTPS a um Application Load Balancer ou instância do Amazon EC2.
- Configurar protocolos seguros em serviços de borda: configure o HTTPS com Amazon CloudFront e utilize um perfil de segurança apropriado para seu procedimento de segurança e caso de uso.
- Utilizar uma VPN para conectividade externa: considere usar uma VPN IPsec para proteger conexões ponto a ponto ou rede a rede para fornecer privacidade e integridade dos dados.

- Configurar protocolos seguros em balanceadores de carga: selecione uma política de segurança que ofereça os pacotes de criptografia mais fortes compatíveis com os clientes que se conectarão ao receptor. Criar um receptor de HTTPS para seu Application Load Balancer.
- Configurar protocolos seguros no Amazon Redshift: configure o cluster para exigir uma conexão Secure Socket Layer (SSL) ou Transport Layer Security (TLS).
- Configurar protocolos seguros: leia a documentação do serviço da AWS para determinar os recursos de criptografia em trânsito.
- Configurar o acesso seguro ao fazer upload para buckets do Amazon S3: utilize controles de política de bucket do Amazon S3 para implementar acesso seguro aos dados.
- Considerar o uso do AWS Certificate Manager: o ACM permite fornecer, gerenciar e implantar certificados TLS públicos para uso com serviços da AWS.
- Considerar o uso do AWS Private Certificate Authority para necessidades de PKI privada: o AWS Private CA permite criar hierarquias de autoridade de certificado privada (CA) para emitir certificados X.509 entidade final que podem ser usados para criar canais de TLS criptografados.

Recursos

Documentos relacionados:

- Documentação da AWS
- Utilizar HTTPS com o CloudFront
- Conectar sua VPC a redes remotas usando a AWS Virtual Private Network
- Criar um receptor de HTTPS para seu Application Load Balancer
- Tutorial: configurar o SSL/TLS no Amazon Linux 2
- Usar SSL/TLS para criptografar uma conexão com uma instância de banco de dados
- Configurar as opções de segurança para conexões

SEC09-BP03 Automatizar a detecção de acesso não intencional a dados

Use ferramentas como o Amazon GuardDuty para detectar automaticamente atividades suspeitas ou tentativas de mover dados para fora dos limites definidos. Por exemplo, o GuardDuty pode detectar atividade de leitura do Amazon Simple Storage Service (Amazon S3) que é incomum com a descoberta Exfiltration:S3/AnomalousBehavior. Além do GuardDuty, Logs de fluxo da Amazon VPC, que capturam informações de tráfego de rede, podem ser usados com o Amazon EventBridge

para acionar a detecção de conexões anormais, bem-sucedidas e recusadas. Amazon S3 Access Analyzer pode ajudar a avaliar quais dados podem ser acessados por quem nos buckets do Amazon S3.

Nível de exposição a riscos quando esta prática recomendada não for estabelecida: Médio

Orientações para a implementação

- Automatizar a detecção de acesso não intencional a dados: use uma ferramenta ou um mecanismo de identificação para detectar automaticamente tentativas de mover dados fora dos limites definidos; por exemplo, para descobrir um sistema de banco de dados que esteja copiando dados para um host desconhecido.
  - Logs de fluxo da VPC
- Considerar o Amazon Macie: o Amazon Macie é um serviço de privacidade e segurança de dados totalmente gerenciado que usa machine learning e correspondência de padrões para descobrir e proteger seus dados sigilosos na AWS.
  - Amazon Macie

Recursos

Documentos relacionados:

- Logs de fluxo da VPC
- Amazon Macie

SEC09-BP04 Autenticar as comunicações de rede

Verifique a identidade das comunicações usando protocolos que oferecem suporte à autenticação, como Transport Layer Security (TLS) ou IPsec.

Projete a workload para usar protocolos de rede seguros e autenticados sempre que for feita uma comunicação entre serviços, aplicações ou usuários. O uso de protocolos de rede compatíveis com a autenticação e a autorização fornece maior controle sobre os fluxos de rede e reduz o impacto do acesso não autorizado.

Resultado desejado: uma workload com fluxos de tráfego bem definidos do plano de dados e do ambiente de gerenciamento entre os serviços. Os fluxos de tráfego usam protocolos de rede autenticados e criptografados quando tecnicamente viáveis.

Antipadrões comuns:

- Fluxos de tráfego não criptografados ou não autenticados na workload.
- Reutilizar credenciais de autenticação entre vários usuários ou entidades.
- Confiar apenas nos controles de rede como um mecanismo de controle de acesso.
- Criar um mecanismo de autenticação personalizado em vez de depender de mecanismos de autenticação padrão do setor.
- Fluxos de tráfego excessivamente permissivos entre componentes de serviço ou outros recursos na VPC.

Benefícios do estabelecimento desta prática recomendada:

- Limita o escopo do impacto do acesso não autorizado a uma parte da workload.
- Fornece um nível mais alto de garantia de que as ações são executadas somente por entidades autenticadas.
- Melhora o desacoplamento de serviços definindo e aplicando claramente as interfaces de transferência de dados pretendidas.
- Melhora o monitoramento, o log e a resposta a incidentes por meio da atribuição de solicitações e interfaces de comunicação bem definidas.
- Oferece defesa profunda para as workloads combinando controles de rede com controles de autenticação e de autorização.

Nível de exposição a riscos se esta prática recomendada não for estabelecida: baixo

Orientações para a implementação

Os padrões de tráfego de rede da workload podem ser caracterizados em duas categorias:

- O tráfego leste-oeste representa fluxos de tráfego entre serviços que compõem uma workload.
- O tráfego norte-sul representa fluxos de tráfego entre a workload e os consumidores.

Embora seja uma prática comum criptografar o tráfego norte-sul, é menos comum proteger o tráfego leste-oeste usando protocolos autenticados. As práticas modernas de segurança recomendam que o design da rede por si só não conceda um relacionamento confiável entre duas entidades. Quando

dois serviços puderem residir dentro de um limite de rede comum, criptografar, autenticar e autorizar as comunicações ainda são práticas recomendadas entre esses serviços.

Como exemplo, as APIs de serviços da AWS usam o protocolo de assinatura do Signature Version 4 (SigV4) da AWS para autenticar o chamador, independentemente da rede de origem da solicitação. Essa autenticação garante que as APIs da AWS possam verificar a identidade que solicitou a ação e que essa identidade possa ser combinada com políticas para tomar uma decisão de autorização a fim de determinar se a ação deve ser permitida ou não.

Serviços, como o Amazon VPC Lattice e o Amazon API Gateway permitem usar o mesmo protocolo de assinatura SigV4 para adicionar autenticação e autorização ao tráfego leste-oeste em suas próprias workloads. Se os recursos fora do ambiente da AWS precisarem se comunicar com os serviços que exigem autenticação e autorização baseadas em SigV4, você poderá usar o AWS Identity and Access Management (IAM) Roles Anywhere no recurso que não é da AWS para adquirir credenciais temporárias da AWS. Essas credenciais podem ser usadas para assinar solicitações para serviços que usam o SigV4 para autorizar o acesso.

Outro mecanismo comum para autenticar o tráfego leste-oeste é a autenticação mútua TLS (mTLS). Muitas aplicações da Internet das Coisas (IoT), aplicações business to business e microsserviços usam o mTLS para validar a identidade de ambos os lados de uma comunicação TLS por meio do uso de certificados X.509 do lado do cliente e do servidor. Esses certificados podem ser emitidos por AWS Private Certificate Authority (AWS Private CA). É possível usar serviços como o Amazon API Gateway e o AWS App Mesh para fornecer autenticação mTLS para comunicação entre workloads ou dentro da workload. Embora o mTLS forneça informações de autenticação aos dois lados de uma comunicação TLS, ele não fornece um mecanismo de autorização.

Por fim, o OAuth 2.0 e o OpenID Connect (OIDC) são dois protocolos normalmente usados para controlar o acesso aos serviços pelos usuários, mas agora também estão se tornando populares para o tráfego entre serviços. O API Gateway fornece um autorizador JSON Web Token (JWT), que permite que as workloads restrinjam o acesso às rotas de API usando JWTs emitidos por provedores de identidades OIDC ou OAuth 2.0. Os escopos do OAuth2 podem ser usados como uma fonte para decisões básicas de autorização, mas as verificações de autorização ainda precisam ser implementadas na camada da aplicação, e os escopos do OAuth2 por si sós não atendem a necessidades de autorização mais complexas.

Etapas da implementação

- Definir e documentar os fluxos de rede da workload: a primeira etapa na implementação de uma estratégia de defesa profunda é definir os fluxos de tráfego da workload.

  - Crie um diagrama de fluxo de dados que defina claramente como os dados são transmitidos entre os diferentes serviços que compõem a workload. Esse diagrama é a primeira etapa para aplicar esses fluxos por meio de canais de rede autenticados.
  - Instrumente a workload nas fases de desenvolvimento e testes para validar se o diagrama de fluxo de dados reflete com precisão o comportamento da workload em tempo de execução.
  - Um diagrama de fluxo de dados também pode ser útil ao realizar um exercício de modelagem de ameaças, conforme descrito em SEC01-BP07 Identificar ameaças e priorizar mitigações com o uso de um modelo de ameaça.
- Estabeleça controles de rede: considere os recursos da AWS para estabelecer controles de rede alinhados aos fluxos de dados. Embora os limites da rede não devam ser o único controle de segurança, eles fornecem uma camada na estratégia de defesa profunda para proteger a workload.
  - Use grupos de segurança para estabelecer, definir e restringir fluxos de dados entre recursos.
  - Considere usar o AWS PrivateLink para se comunicar com os serviços da AWS e de terceiros que são compatíveis com o AWS PrivateLink. Os dados enviados por meio de um endpoint da interface do AWS PrivateLink permanecem na estrutura da rede da AWS e não atravessam a internet pública.
- Implementar autenticação e autorização entre os serviços na workload: escolha o conjunto de serviços da AWS mais apropriado para fornecer fluxos de tráfego autenticados e criptografados na workload.
  - Considere o Amazon VPC Lattice para proteger a comunicação entre serviços. O VPC Lattice pode usar a autenticação do SigV4 combinada com políticas de autenticação para controlar o acesso entre serviços.
  - Para comunicação entre serviços usando mTLS, considere o API Gateway ou o App Mesh. O AWS Private CA pode ser usado para estabelecer uma hierarquia de CA privada capaz de emitir certificados para uso com o mTLS.
  - Ao fazer a integração com serviços que usam OAuth 2.0 ou OIDC, considere o API Gateway usando o autorizador JWT.
  - Para comunicação entre a workload e dispositivos de IoT, considere o AWS IoT Core, que fornece várias opções para criptografia e autenticação de tráfego de rede.
- Monitorar o acesso não autorizado: monitore continuamente os canais de comunicação não intencionais, entidades principais não autorizadas que tentam acessar recursos protegidos e outros padrões de acesso inadequados.

- Se estiver usando o VPC Lattice para gerenciar o acesso aos serviços, considere ativar e monitorar os logs de acesso do VPC Lattice. Esses logs de acesso incluem informações sobre a entidade solicitante, informações de rede que incluem a VPC de origem e de destino e os metadados da solicitação.
- Considere a ativação dos Logs de fluxo da VPC para capturar metadados nos fluxos de rede e analisar se há anomalias periodicamente.
- Consulte o AWS Security Incident Response Guide e a seção Resposta a incidentes do Pilar Segurança: AWS Well-Architected Framework para obter mais orientações sobre planejamento, simulação e resposta a incidentes de segurança.

Recursos

Práticas recomendadas relacionadas:

- SEC03-BP07 Analisar o acesso público e entre contas
- SEC02-BP02 Usar credenciais temporárias
- SEC01-BP07 Identificar ameaças e priorizar mitigações com o uso de um modelo de ameaça

Documentos relacionados:

- Evaluating access control methods to secure Amazon API Gateway APIs
- Configurar a autenticação TLS mútua para uma API REST
- How to secure API Gateway HTTP endpoints with JWT authorizer
- Authorizing direct calls to AWS services using AWS IoT Core credential provider
- Guia de resposta a incidentes de segurança da AWS

Vídeos relacionados:

- AWS re:invent 2022: Introducing VPC Lattice
- AWS re:invent 2020: Serverless API authentication for HTTP APIs on AWS

Exemplos relacionados:

- Workshop do Amazon VPC Lattice
- Workshop Zero-Trust Episode 1 – The Phantom Service Perimeter

Resposta a incidentes

Mesmo com controles preventivos e de detecção consolidados, sua organização deve implementar mecanismos para responder e atenuar o impacto potencial de incidentes de segurança.
Sua preparação afeta muito a capacidade das equipes de operar com eficácia durante um incidente, isolar, conter e analisar problemas e restaurar as operações para um estado adequado conhecido. Implementar as ferramentas e o acesso antes de um incidente de segurança e praticar rotineiramente dias de jogos para validar a resposta a incidentes ajudam a garantir que você possa se recuperar enquanto minimiza interrupções empresariais.

Tópicos

Aspectos da resposta a incidentes da AWS

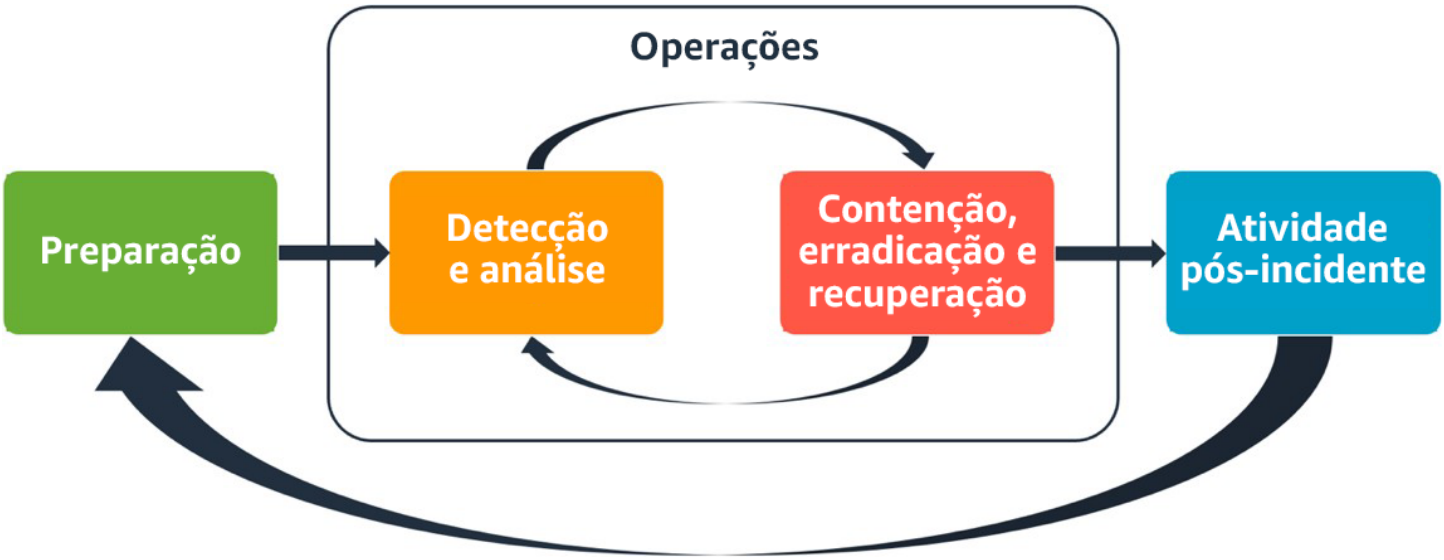
Todos os usuários da AWS de uma organização devem ter uma compreensão básica dos processos de resposta a incidentes de segurança, e a equipe de segurança deve entender como responder aos problemas de segurança. Educação, treinamento e experiência são essenciais para um programa bem-sucedido de resposta a incidentes na nuvem e são preferencialmente implementados bem antes de precisar lidar com um possível incidente de segurança. A base de um programa bem-sucedido de resposta a incidentes na nuvem é Preparação, Operaçõese Atividade pós-incidente.

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

- Preparação: prepare sua equipe de resposta a incidentes para detectar e responder aos incidentes na AWS ativando controles de detecção e verificando o acesso adequado às ferramentas e aos serviços de nuvem necessários. Além disso, prepare os manuais necessários, tanto os automatizados quanto os manuais, para garantir respostas confiáveis e consistentes.
- Operações: opere em eventos de segurança e possíveis incidentes seguindo as fases de resposta a incidentes do NIST: detectar, analisar, conter, erradicar e recuperar.

- Atividade pós-incidente: itere o resultado de seus eventos e simulações de segurança para melhorar a eficácia da resposta, aumentar o valor derivado da resposta e da investigação e reduzir ainda mais os riscos. Você precisa aprender com os incidentes e ter uma propriedade consistente das atividades de melhoria.

O diagrama a seguir mostra o fluxo desses aspectos, alinhando-se ao ciclo de vida de resposta a incidentes do NIST mencionado anteriormente, mas com operações que abrangem detecção e análise com contenção, erradicação e recuperação.



Aspectos da resposta a incidentes da AWS

Elaborar objetivos da resposta da nuvem

Embora os processos e mecanismos gerais de resposta a incidentes, como os definidos no Guia de tratamento de incidentes de segurança de computadores NIST SP 800-61, continuem válidos, recomendamos que você avalie estes objetivos específicos de design que são relevantes para responder a incidentes de segurança em um ambiente de nuvem:

- Estabelecer objetivos de resposta: trabalhe com as partes interessadas, a assessoria jurídica e a liderança organizacional para determinar o objetivo da resposta a um incidente. Alguns objetivos comuns são: conter e atenuar o problema, recuperar os recursos afetados, preservar dados para análise forense, retornar às operações seguras conhecidas e, finalmente, aprender com os incidentes.
- Responder usando a nuvem: Implemente padrões de resposta na nuvem, onde o evento e os dados ocorrem.

- Saber o que você tem e do que precisa: Preserve logs, recursos, instantâneos e outras evidências copiando e armazenando-os em uma conta centralizada na nuvem dedicada à resposta. Use tags, metadados e mecanismos que impõem políticas de retenção. Você precisará entender quais serviços são usados e identificar os requisitos para investigar esses serviços. Para ajudar você a entender seu ambiente, você também pode usar a marcação.
- Usar mecanismos de reimplantação: se uma anomalia de segurança puder ser atribuída a uma configuração incorreta, a correção poderá ser tão simples quanto a remoção da variação com a reimplantação dos recursos com a configuração apropriada. Se um possível comprometimento for identificado, verifique se sua redistribuição inclui a atenuação bem-sucedida e verificada das causas principais.
- Automatizar sempre que possível: À medida que surgem problemas ou incidentes se repetem, crie mecanismos para fazer a triagem programática e responder a eventos comuns. Use respostas humanas para incidentes exclusivos, complexos ou confidenciais em que as automações são insuficientes.
- Escolher soluções escaláveis: Esforce-se para combinar a escalabilidade da abordagem de sua organização com a computação em nuvem. Implemente mecanismos de detecção e resposta que se expandam em seus ambientes para reduzir efetivamente o tempo entre a detecção e a resposta.
- Conhecer e melhorar seu processo: Seja proativo na identificação de déficits em seus processos, ferramentas ou pessoas e implemente um plano para corrigi-los. Simulações são métodos seguros para encontrar déficits e melhorar processos.

Essas metas de design são um lembrete para analisar a implementação de sua arquitetura quanto à capacidade de conduzir tanto a resposta a incidentes quanto a detecção de ameaças. Ao planejar suas implementações de nuvem, pense em responder a um incidente, de preferência, com uma metodologia de resposta sólida em termos forenses. Em alguns casos, isso significa que você pode ter várias organizações, contas e ferramentas configuradas especificamente para essas tarefas de resposta. Essas ferramentas e funções devem ser disponibilizadas para a equipe de atendimento a incidentes por meio do pipeline de implantação. Elas não devem ser estáticas, pois podem causar um risco maior.

Preparação

A preparação para um incidente é fundamental para uma resposta oportuna e eficaz a incidentes. A preparação é feita em três domínios:

- Pessoas: preparar seu pessoal para um incidente de segurança envolve identificar as partes interessadas relevantes para a resposta a incidentes e treiná-las em resposta a incidentes e tecnologias de nuvem.
- Processo: preparar seus processos para um incidente de segurança envolve documentar arquiteturas, desenvolver planos completos de resposta a incidentes e criar manuais para uma resposta consistente a eventos de segurança.
- Tecnologia: preparar sua tecnologia para um incidente de segurança envolve configurar o acesso, agregar e monitorar os logs necessários, implementar mecanismos de alerta eficazes e desenvolver recursos de resposta e investigação.

Cada um desses domínios é igualmente importante para uma resposta eficaz a incidentes. Nenhum programa de resposta a incidentes está completo ou é eficaz sem os três. Você precisará preparar pessoas, processos e tecnologias com uma forte integração para se preparar para um incidente.

Práticas recomendadas

- SEC10-BP01 Identify key personnel and external resources
- SEC10-BP02 Desenvolver planos de gerenciamento de incidentes
- SEC10-BP03 Prepare recursos forenses
- SEC10-BP04 Desenvolva e teste manuais de resposta a incidentes de segurança
- SEC10-BP05 Acesso pré-provisionado
- SEC10-BP06 Pré-implantação de ferramentas
- SEC10-BP07 Execute simulações

SEC10-BP01 Identify key personnel and external resources

Identifique o pessoal, as obrigações legais e os recursos internos e externos que ajudariam sua organização a responder a um incidente.

Para definir sua abordagem de resposta a incidentes na nuvem, com a participação de outras equipes (como consultoria jurídica, liderança, partes interessadas de negócios, serviços do AWS Support e outras), você deve identificar as principais partes interessadas, pessoal e contatos relevantes. Para reduzir a dependência e diminuir o tempo de resposta, certifique-se de que sua equipe, equipes de segurança especializadas e respondentes sejam instruídos sobre os serviços que você usa e tenham a oportunidade de praticar.

É recomendável identificar parceiros externos de segurança da AWS que possam fornecer experiência externa e uma perspectiva diferente para aumentar seus recursos de resposta. Os parceiros de segurança confiáveis podem ajudá-lo a identificar possíveis riscos ou ameaças com os quais você talvez não esteja familiarizado.

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

Orientação para implementação

- Identificar o pessoal-chave da organização: Mantenha uma lista de contatos da sua organização que você precisaria acionar para responder e recuperar-se de um incidente.
- Identificar parceiros externos: Entre em contato com parceiros externos, se necessário, que possam ajudá-lo a responder e se recuperar de um incidente.

Recursos

Documentos relacionados:

- AWS Incident Response Guide (Guia de resposta a incidentes da AWS)

Vídeos relacionados:

- Prepare for and respond to security incidents in your AWS environment (Prepare-se e responda a incidentes de segurança no ambiente da AWS)

Exemplos relacionados:

SEC10-BP02 Desenvolver planos de gerenciamento de incidentes

O primeiro documento a ser desenvolvido para resposta a incidentes é o plano de resposta a incidentes. O plano de resposta a incidentes foi projetado para ser a base de seu programa e estratégia de resposta a incidentes.

Benefícios de estabelecer esta prática recomendada: O desenvolvimento de processos de resposta a incidentes completos e claramente definidos é fundamental para um programa de resposta a incidentes bem-sucedido e escalável. Quando ocorre um evento de segurança, etapas e fluxos de trabalho claros poderão ajudar você a responder em tempo hábil. Talvez você já tenha processos

de resposta a incidentes existentes. Independentemente do seu estado atual, é importante atualizar, repetir e testar seus processos de resposta a incidentes regularmente.

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

Orientação para implementação

Um plano de gerenciamento de incidentes é fundamental para responder, mitigar e se recuperar de possíveis impactos de incidentes de segurança. Um plano de gerenciamento de incidentes é um processo estruturado de identificação, correção e resposta em tempo hábil a incidentes de segurança.

A nuvem tem muitos dos mesmos requisitos e perfis operacionais encontrados em um ambiente on-premises. Ao criar um plano de gerenciamento de incidentes, é importante definir estratégias de resposta e recuperação que se alinhem melhor aos seus resultados empresariais e requisitos de conformidade. Por exemplo, se você opera workloads na AWS em conformidade com o FedRAMP nos Estados Unidos, é útil aderir ao Guia de tratamento de segurança de computadores NIST SP 800-61. Da mesma forma, ao operar workloads com informações de identificação pessoal (PII) da Europa, considere cenários como a maneira como você deve se proteger e responder a incidentes relacionados à residência de dados, conforme exigido pela Regulamentação Geral de Proteção de Dados (GDPR) da UE.

Ao criar um plano de gerenciamento de incidentes para suas workloads na AWS, comece com o Modelo de responsabilidade compartilhada da AWS , para elaborar uma abordagem de defesa profunda em relação à resposta a incidentes. Nesse modelo, a AWS gerencia a segurança da nuvem, e você é responsável pela segurança na nuvem. Isso significa que você mantém o controle e é responsável pelos controles de segurança que escolhe implementar. O AWS Security Incident Response Guide (Guia de resposta a incidentes de segurança da AWS) detalha os conceitos e as orientações básicas para criar um plano de gerenciamento de incidentes centrado na nuvem.

Um plano de gerenciamento de incidentes eficaz deve ser continuamente iterado e permanecer atualizado com relação às suas metas de operações de nuvem. Considere o uso dos planos de implementação detalhados abaixo, à medida que cria e evolui seu plano de gerenciamento de incidentes.

Etapas da implementação

Defina 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. Observe que muitas regiões têm leis locais que regem o que deve e o que não deve ser feito. Embora possa parecer burocrático criar um grafo de pessoas responsáveis, atribuídas, consultadas e informadas (RACI) para seus planos de resposta de segurança, isso facilita a comunicação rápida e direta e descreve claramente a liderança em diferentes estágios do evento.

Durante um incidente, incluir os proprietários e os desenvolvedores de aplicações e recursos afetados é fundamental porque eles são especialistas no assunto (PMEs) que podem fornecer informações e contexto para ajudar a medir o 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, parceiros confiáveis podem estar envolvidos na investigação ou na resposta, pois podem oferecer experiência adicional e um controle valioso. Se você não tiver essas habilidades em sua própria equipe, contrate uma parte externa para obter assistência.

Entender as equipes de resposta e o suporte da AWS

- AWS Support
  - O AWS Support oferece uma variedade de planos que concedem acesso a ferramentas e conhecimentos que apoiam o êxito e a saúde operacional de suas soluções da AWS. Se precisar de suporte técnico e mais recursos para ajudar a planejar, implantar e otimizar seu ambiente da AWS, selecione um plano de suporte mais adequado ao seu caso de uso da AWS.
  - Considere o Support Center entre AWS Management Console (é necessário fazer login) como ponto central de contato para obter suporte para problemas que afetam seus recursos da AWS. O acesso ao AWS Support é controlado pelo AWS Identity and Access Management. Para ter mais informações sobre como obter acesso aos recursos da AWS Support, consulte Conceitos básicos do AWS Support.
- Equipe de Resposta a Incidentes de Clientes (CIRT) da AWS
  - A Equipe de Resposta a Incidentes de Clientes (CIRT) da AWS é uma equipe global da AWS especializada 24 horas por dia, 7 dias por semana, que presta assistência aos clientes durante eventos de segurança ativos do cliente do Modelo de responsabilidade compartilhada da AWS.

  - Ao apoiar você, a AWS CIRT presta assistência na triagem e na recuperação de um evento de segurança ativo na AWS. Eles podem ajudar na análise da causa raiz por meio do uso de logs de serviço da AWS e fornecer recomendações para recuperação. Eles também podem fornecer recomendações de segurança e práticas recomendadas para ajudar você a evitar eventos de segurança no futuro.
  - Os clientes da AWS podem contratar a AWS CIRT por meio de um caso do AWS Support.
- Suporte de resposta a DDoS
  - A AWS oferece o AWS Shield, que fornece um serviço gerenciado de proteção distribuída de negação de serviço (DDoS) que protege as aplicações web em execução na AWS. O Shield oferece detecção contínua e mitigações automáticas em linha que podem minimizar o tempo de inatividade e a latência da aplicação, portanto, não há necessidade de contratar o AWS Support para se beneficiar da proteção contra DDoS. Existem dois níveis de Shield: AWS Shield Standard e AWS Shield Advanced. Para saber mais sobre as diferenças entre esses dois níveis, consulte a documentação de recursos do Shield.
- AWS Managed Services (AMS)
  - O AWS Managed Services (AMS) oferece gerenciamento contínuo de sua infraestrutura da AWS para que você possa se concentrar em suas aplicações. Ao implementar as práticas recomendadas para manter sua infraestrutura, o AMS ajuda a reduzir sua sobrecarga operacional e os riscos. O AMS automatiza atividades comuns, como solicitações de mudança, monitoramento, gerenciamento de patches, serviços de segurança e backup, e fornece serviços de ciclo de vida completo para provisionar, executar e oferecer compatibilidade com sua infraestrutura.
  - O AMS assume a responsabilidade de implantar um pacote de controles de detecção de segurança e fornece uma primeira linha de resposta aos alertas 24 horas por dia, 7 dias por semana. Quando um alerta é iniciado, o AMS segue um conjunto padrão de guias e manuais automatizados para verificar uma resposta consistente. Esses guias são compartilhados com os clientes do AMS durante a integração para que eles possam desenvolver e coordenar uma resposta com o AMS.

Desenvolva o plano de resposta a incidentes

O plano de resposta a incidentes foi projetado para ser a base de seu programa e estratégia de resposta a incidentes. O plano de resposta a incidentes deve estar em um documento formal. Um plano de resposta a incidentes geralmente inclui as seguintes seções:

- Uma visão geral da equipe de resposta a incidentes: Descreve as metas e as funções da equipe de resposta a incidentes.
- Funções e responsabilidades: Lista as partes interessadas na resposta a incidentes e detalha suas funções quando ocorre um incidente.
- Um plano de comunicação: Detalha as informações de contato e como você se comunica durante um incidente.
- Métodos de comunicação de backup: É prática recomendada ter a comunicação fora de banda como backup para a comunicação de incidentes. Um exemplo de aplicação que fornece um canal seguro de comunicação fora de banda é AWS Wickr.
- Fases da resposta a incidentes e ações a serem realizadas: Enumera as fases da resposta a incidentes (por exemplo, detectar, analisar, erradicar, conter e recuperar), incluindo ações de alto nível a serem realizadas nessas fases.
- Definições de severidade e priorização do incidente: Detalha como classificar a severidade de um incidente, como priorizar o incidente e, depois, como as definições de severidade afetam os procedimentos de escalonamento.

Embora essas seções sejam comuns em empresas de diferentes tamanhos e setores, o plano de resposta a incidentes de cada organização é único. Você precisa criar um plano de resposta a incidentes que funcione melhor para a organização.

Recursos

Práticas recomendadas relacionadas:

- SEC04 (Como você detecta e investiga eventos de segurança?)

Documentos relacionados:

- AWS Security Incident Response Guide (Guia de resposta a incidentes de segurança da AWS)
- NIST: Guia de tratamento de incidentes de segurança de computadores

SEC10-BP03 Prepare recursos forenses

Antes de um incidente de segurança, considere o desenvolvimento de recursos forenses para apoiar as investigações de eventos de segurança.

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

Os conceitos da análise forense on-premises tradicional se aplicam à AWS. Para obter informações importantes para começar a desenvolver recursos forenses na Nuvem AWS, consulte Forensic investigation environment strategies in the Nuvem AWS.

Depois de configurar o ambiente e a estrutura da Conta da AWS para análise forense, defina as tecnologias necessárias para executar com eficácia metodologias forenses sólidas nas quatro fases:

- Coleta: Colete logs relevantes da AWS, como logs do AWS CloudTrail, do AWS Config, logs de fluxo da VPC e log em nível de host. Colete snapshots, backups e despejos de memória dos recursos afetados da AWS, quando disponíveis.
- Exame: Examine os dados coletados extraindo e avaliando as informações relevantes.
- Análises: Analise os dados coletados para entender o incidente e tirar conclusões dele.
- Relatórios: Apresente as informações resultantes da fase de análise.

Etapas da implementação

Prepare o ambiente forense

AWS Organizations ajuda a gerenciar e reger centralmente um ambiente da AWS à medida que você expande e escala os recursos da AWS. Uma organização da AWS consolida suas Contas da AWS para que você possa administrá-las como uma única unidade. Você pode usar unidades organizacionais (UOs) para agrupar contas e administrá-las como uma única unidade.

Para resposta a incidentes, é útil ter uma estrutura da Conta da AWS compatível com as funções de resposta a incidentes, que inclui uma UO de segurança e uma UO forense. Dentro da OU de segurança, você deve ter contas para:

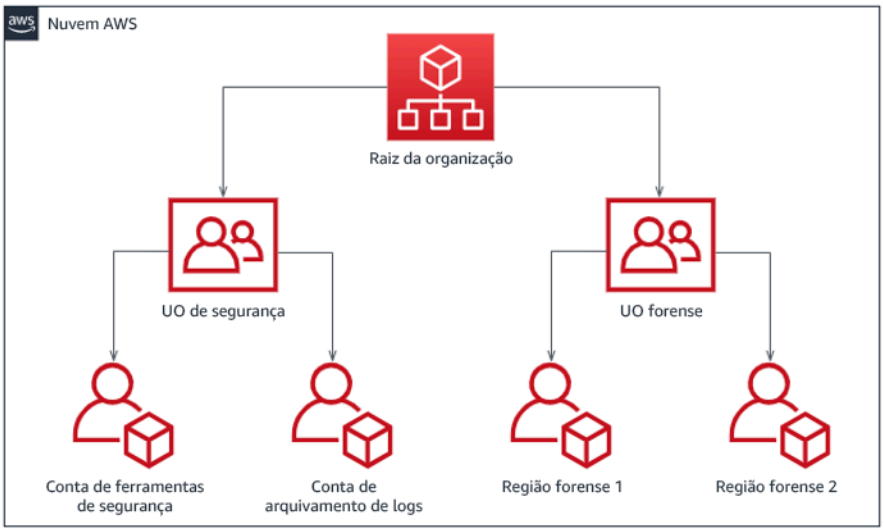
- Arquivamento de logs: Agregue logs em uma Conta da AWS de arquivamento de logs com permissões limitadas.
- Ferramentas de segurança: Centralize os serviços de segurança em uma Conta da AWS de ferramenta de segurança. Essa conta opera como administrador delegado dos serviços de segurança.

Dentro da UO forense, você tem a opção de implementar uma única conta ou contas forenses para cada região em que opera, dependendo da que funciona melhor para sua empresa e modelo

operacional. Se você criar uma conta forense por região, poderá bloquear a criação de recursos da AWS fora dessa região e reduzir o risco de os recursos serem copiados para uma região não pretendida. Por exemplo, se você opera apenas em US East (N. Virginia) Region (`us-east-1`) e US West (Oregon) (`us-west-2`), então você teria duas contas na UO forense: uma para `us-east-1` e uma para `us-west-2`.

Você pode criar uma Conta da AWS de análise forense para várias regiões. Você deve ter cuidado ao copiar recursos da AWS para essa conta para verificar se está de acordo com seus requisitos de soberania de dados. Como é preciso tempo para provisionar novas contas, é imperativo criar e instrumentar as contas forenses bem antes de um incidente, para que os respondentes possam estar preparados para usá-las de forma eficaz em suas respostas.

O diagrama a seguir exibe um exemplo de estrutura de contas, incluindo uma UO forense com contas forenses por região:



Estrutura de contas por região para resposta a incidentes

Capture backups e snapshots

Configurar backups dos principais sistemas e bancos de dados é essencial para a recuperação de um incidente de segurança e para fins forenses. Com os backups em vigor, você pode restaurar seus sistemas ao estado seguro anterior. Na AWS, você pode criar snapshots de vários recursos. Os snapshots fornecem backups pontuais desses recursos. Há muitos serviços da AWS que podem ajudar em backup e recuperação. Para obter detalhes sobre esses serviços e abordagens para backup e recuperação, consulte Backup and Recovery Prescriptive Guidance e Use backups to recover from security incidents.

Especialmente quando se trata de situações como ransomware, é fundamental que os backups estejam bem protegidos. Para obter orientações sobre como proteger os backups, consulte Top 10 security best practices for securing backups in AWS. Além de proteger os backups, você deve testar regularmente seus processos de backup e restauração para verificar se a tecnologia e os processos implementados funcionam conforme o esperado.

Automatize a análise forense

Durante um evento de segurança, sua equipe de resposta a incidentes deve ser capaz de coletar e analisar evidências rapidamente, mantendo a precisão durante o período em torno do evento (como capturar registros relacionados a um evento ou recurso específico ou coletar o despejo de memória de uma instância do Amazon EC2). É desafiador e demorado para a equipe de resposta a incidentes coletar manualmente as evidências relevantes, especialmente em um grande número de instâncias e contas. Além disso, a coleta manual pode estar sujeita a erros humanos. Por esses motivos, você deve desenvolver e implementar a automação para perícia o máximo possível.

A AWS oferece vários recursos de automação para análise forense, que estão listados na seção de recursos a seguir. Esses recursos são exemplos de padrões forenses que desenvolvemos e que os clientes implementaram. Embora possam ser uma arquitetura de referência útil para começar, considere modificá-las ou criar padrões de automação forense com base em seu ambiente, requisitos, ferramentas e processos forenses.

Recursos

Documentos relacionados:

- AWS Security Incident Response Guide - Develop Forensics Capabilities
- AWS Security Incident Response Guide - Forensics Resources
- Forensic investigation environment strategies in the Nuvem AWS
- How to automate forensic disk collection in AWS
- AWS Prescriptive Guidance - Automate incident response and forensics

Vídeos relacionados:

- Automatização de resposta a incidentes e forense

Exemplos relacionados:

- Automated Incident Response and Forensics Framework (Estrutura forense e de resposta automatizada a incidentes)
- Automated Forensics Orchestrator for Amazon EC2

SEC10-BP04 Desenvolva e teste manuais de resposta a incidentes de segurança

Uma parte fundamental da preparação de seus processos de resposta a incidentes é desenvolver manuais. Os manuais de resposta a incidentes fornecem uma série de orientações prescritivas e etapas a serem seguidas quando ocorre um evento de segurança. Ter uma estrutura e etapas claras simplifica a resposta e reduz a probabilidade de erro humano.

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

Orientação para implementação

Os manuais devem ser criados para cenários de incidentes, como:

- Incidentes esperados: os manuais devem ser criados para os incidentes previstos. Isso inclui ameaças como negação de serviço (DoS), ransomware e comprometimento de credenciais.
- Descobertas ou alertas de segurança conhecidos: os manuais devem ser criados para descobertas e alertas de segurança conhecidos, como descobertas do GuardDuty. Você pode receber uma descoberta do GuardDuty e pensar: “E agora?” Para evitar que você trate incorretamente ou ignore uma descoberta do GuardDuty, crie um manual para cada possível descoberta 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 tem um custo. Para obter mais detalhes sobre o GuardDuty, consulte Appendix A: Cloud capability definitions - Visibility and alerting.

Os manuais devem conter etapas técnicas a serem concluídas por um analista de segurança para investigar e responder adequadamente a um possível incidente de segurança.

Etapas da implementação

Os itens a serem incluídos em um manual incluem:

- Visão geral do manual: qual cenário de risco ou incidente esse manual aborda? Qual é o objetivo do manual?

- Pré-requisitos: quais logs, mecanismos de detecção e ferramentas automatizadas são necessários para esse cenário de incidente? Qual é a notificação esperada?
- Informações de comunicação e escalonamento: quem está envolvido e quais são suas informações de contato? Quais são as responsabilidades de cada parte interessada?
- Etapas de resposta: em todas as fases da resposta a incidentes, quais etapas táticas devem ser seguidas? Quais consultas um analista deve executar? Qual código deve ser executado para alcançar o resultado desejado?
  - Detectar: como o incidente será detectado?
  - Análise: como o escopo do impacto será determinado?
  - Contêm: como o incidente será isolado para limitar o escopo?
  - Erradicar: como a ameaça será removida do ambiente?
  - Recuperar: como o sistema ou o recurso afetado voltará à produção?
- Resultados esperados: depois que as consultas e o código forem executados, qual é o resultado esperado do manual?

Recursos

Práticas recomendadas relacionadas ao Well-Architected:

- SEC10-BP02 - Develop incident management plans (SEC10-BP02 – Desenvolver planos de gerenciamento de incidentes)

Documentos relacionados:

- Framework for Incident Response Playbooks (Estrutura para manuais de resposta a incidentes)
- Develop your own Incident Response Playbooks (Desenvolva seus próprios manuais de resposta a incidentes)
- Incident Response Playbook Samples (Amostras do manual de resposta a incidentes)
- Building an AWS incident response runbook using Jupyter playbooks and CloudTrail Lake

SEC10-BP05 Acesso pré-provisionado

Verifique se os respondentes a incidentes têm o acesso correto pré-provisionado na AWS para reduzir o tempo de investigação necessário até a recuperação.

Antipadrões comuns:

- Uso da conta raiz para a resposta a incidentes.
- Alteração de contas de usuário existentes.
- Manipulação de permissões do IAM diretamente ao fornecer elevação de privilégios just-in-time.

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

Orientação para implementação

A AWS recomenda reduzir ou eliminar a dependência de credenciais de longa duração sempre que possível, dando preferência a credenciais temporárias e a mecanismos de escalação de privilégios just-in-time. As credenciais de longa duração são propensas a riscos de segurança e aumentam a sobrecarga operacional. Para a maioria das tarefas de gerenciamento, bem como tarefas de resposta a incidentes, recomendamos a implementação da federação de identidades junto com a escalação temporária para acesso administrativo. Nesse modelo, um usuário solicita elevação a um nível superior de privilégio (como um perfil de resposta a incidentes) e, considerando que ele seja elegível para a elevação, a solicitação é enviada a um aprovador. Se a solicitação for aprovada, o usuário receberá um conjunto de credenciais temporárias da AWS, que podem ser usadas para concluir suas tarefas. Depois que essas credenciais expirarem, o usuário deve enviar uma nova solicitação de elevação.

Recomendamos o uso da escalação de privilégio temporária para a maioria dos cenários de resposta a incidentes. A maneira correta de fazer isso é com o uso do AWS Security Token Service e de políticas de sessão para definir o escopo de acesso.

Há cenários em que as identidades federadas não estão disponíveis, como:

- Interrupção relacionada a um provedor de identidades (IdP) comprometido.
- Erro de configuração ou erro humano causando uma falha no sistema de gerenciamento de acesso federado.
- Atividade mal-intencionada, como um evento de negação de serviço distribuído (DDoS) ou indisponibilidade de renderização do sistema.

Nos casos anteriores, deverá haver um acesso de emergência de breaking-glass configurado para permitir a investigação e a correção em tempo hábil dos incidentes. Recomendamos a utilização de um usuário do IAM com as permissões apropriadas para realizar tarefas e acessar os

recursos da AWS. Use as credenciais raiz somente para tarefas que exijam o acesso do usuário raiz. Para verificar se os respondentes de um incidente têm o nível de acesso correto à AWS e a outros sistemas relevantes, recomendamos o pré-provisionamento de contas de usuário dedicadas. As contas de usuário exigem acesso privilegiado e devem ser estritamente controladas e monitoradas. As contas devem ser criadas com os menores privilégios exigidos para realizar as tarefas necessárias, e o nível de acesso deve ser baseado nos manuais criados como parte do plano de gerenciamento de incidentes.

Utilize perfis e usuários dedicados e com propósito específico como uma prática recomendada. Escalar temporariamente o acesso de usuários ou perfis por meio da adição de políticas do IAM não deixa claro qual é o acesso que os usuários tinham durante o incidente, e há um risco de que os privilégios escalados não sejam revogados.

É importante remover o máximo de dependências possível para verificar se o acesso pode ser obtido com o maior número possível de cenários de falha. Para apoiar isso, crie um manual para verificar se os usuários de resposta a incidentes são criados como usuários do AWS Identity and Access Management em uma conta de segurança dedicada, e não são gerenciados por nenhuma solução de autenticação única (SSO) ou federação. Cada respondente individual deve ter sua própria conta nomeada. A configuração da conta deve aplicar uma política de senha forte e a autenticação multifator (MFA). Se os manuais de resposta a incidentes só exigem acesso ao AWS Management Console, o usuário não deve ter chaves de acesso configuradas e deve ser proibido explicitamente de criar chaves de acesso. Isso pode ser configurado com políticas do IAM ou políticas de controle de serviços (SCPs), conforme mencionado nas Práticas recomendadas de segurança da AWS para SCPs do AWS Organizations. Os usuários não devem ter privilégios além da capacidade de assumir perfis de resposta a incidentes em outras contas.

Durante um incidente, pode ser necessário conceder acesso a outros indivíduos internos ou externos para apoiar a investigação, a correção ou as atividades de recuperação. Nesse caso, use o mecanismo do manual mencionado anteriormente, e deve haver um processo para verificar se qualquer acesso adicional foi revogado imediatamente após a conclusão do incidente.

Para verificar se o uso de perfis de resposta a incidentes pode ser monitorado e auditado corretamente, é essencial que as contas de usuário do IAM criadas para esse fim não sejam compartilhadas entre indivíduos e que o usuário raiz da Conta da AWS não seja utilizado, a menos que isso seja exigido para uma tarefa específica. Se o usuário raiz for exigido (por exemplo, quando o acesso do IAM a uma conta específica estiver indisponível), use um processo distinto com um manual disponível para verificar a disponibilidade da senha e do token de MFA do usuário raiz.

Para configurar as políticas do IAM para os perfis de resposta a incidentes, considere o uso do IAM Access Analyzer para gerar políticas baseadas em logs do AWS CloudTrail. Para fazer isso, conceda acesso de administrador ao perfil de resposta a incidentes em uma conta de não produção e execute de acordo com os manuais. Depois da conclusão, pode ser criada uma política que permita somente as ações realizadas. Essa política pode ser então aplicada a todos os perfis de resposta a incidentes em todas as contas. Você pode criar uma política do IAM separada para cada manual a fim de facilitar o gerenciamento e a auditoria. Exemplos de manuais podem incluir planos de resposta para ransomware, violações de dados, perda de acesso da produção, dentre outros cenários.

Use as contas de usuário de resposta a incidentes para assumir funções do IAM de resposta a incidentes em outras Contas da AWS. Esses perfis também devem ser configurados para só poderem ser assumidos por usuários na conta de segurança, e o relacionamento de confiança deve exigir que a entidade principal que está fazendo a chamada seja autenticada com MFA. Os perfis devem usar políticas do IAM com escopo estritamente definido para controlar o acesso. Garanta que todas as solicitações `AssumeRole` para esses perfis estejam conectadas no CloudTrail e sejam alertadas, e que as ações realizadas usando esses perfis sejam registradas.

É altamente recomendável que as contas de usuário do IAM e os perfis do IAM sejam claramente nomeados para permitir que sejam encontrados com facilidade nos logs do CloudTrail. Um exemplo disso seria nomear as contas do IAM como *<USER_ID>*`-BREAK-GLASS` e os perfis do IAM como `BREAK-GLASS-ROLE`.

O CloudTrail é usado para registrar as atividades da API em suas contas da AWS e deve ser usado para configurar alertas sobre o uso dos perfis de resposta a incidentes. Consulte a publicação do blog sobre como configurar alertas quando as chaves raiz são usadas. As instruções podem ser modificadas para configurar a métrica do Amazon CloudWatch filtro a filtro em eventos `AssumeRole` relacionados ao perfil do IAM de resposta a incidentes:

```
{ $.eventName = "AssumeRole" && $.requestParameters.roleArn =
 "<INCIDENT_RESPONSE_ROLE_ARN>" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !
= "AwsServiceEvent" }
```

Como é provável que os perfis de resposta a incidentes tenham um alto nível de acesso, é importante que esses alertas sejam transmitidos a um grande grupo e que sejam tomadas atitudes rapidamente.

Durante um incidente, é possível que um respondente possa exigir acesso a sistemas que não são protegidos diretamente pelo IAM. Isso pode incluir instâncias do Amazon Elastic Compute Cloud, bancos de dados do Amazon Relational Database Service ou plataformas de software como serviço

(SaaS). É altamente recomendável que, em vez de usar protocolos nativos, como SSH ou RDP, o AWS Systems Manager Session Manager seja usado para todo acesso administrativo a instâncias do Amazon EC2. Esse acesso pode ser controlado usando o IAM, que é protegido e auditado. Também pode ser possível automatizar partes de seus manuais usando os documentos do AWS Systems Manager Run Command, o que pode reduzir os erros do usuário e melhorar o tempo de recuperação. Para acesso aos bancos de dados e a ferramentas de terceiros, recomendamos armazenar as credenciais de acesso no AWS Secrets Manager e conceder acesso aos perfis de respondente a incidentes.

Por fim, o gerenciamento das contas de usuário do IAM de resposta a incidentes deve ser adicionado aos seus processos de junção, migração e saída, além de ser revisado e testado periodicamente visando confirmar se somente o acesso pretendido é permitido.

Recursos

Documentos relacionados:

- Managing temporary elevated access to your AWS environment (Gerenciamento de acesso elevado temporário ao seu ambiente da AWS)
- AWS Security Incident Response Guide (Guia de resposta a incidentes de segurança da AWS)
- AWS Elastic Disaster Recovery
- AWS Systems Manager Incident Manager
- Setting an account password policy for IAM users (Definição de uma política de senhas de contas para usuários do IAM)
- Using multi-factor authentication (MFA) in AWS (Uso da autenticação multifator (MFA) na AWS)
- Configuring Cross-Account Access with MFA (Configuração do acesso entre contas com MFA)
- Using IAM Access Analyzer to generate IAM policies (Uso do IAM Access Analyzer para gerar políticas do IAM)
- Best Practices for AWS Organizations Service Control Policies in a Multi-Account Environment (Práticas recomendadas para políticas de controle de serviço do AWS Organizations em um ambiente de várias contas)
- How to Receive Notifications When Your AWS Account's Root Access Keys Are Used (Como receber notificações quando as chaves de acesso raiz da sua conta da AWS são usadas)
- Create fine-grained session permissions using IAM managed policies (Criar permissões de sessão refinadas usando políticas gerenciadas pelo IAM)

Vídeos relacionados:

- Automating Incident Response and Forensics in AWS (Automação de resposta a incidentes e investigações forenses na AWS)
- Guia DIY (faça você mesmo) para runbooks, relatórios de incidentes e resposta a incidentes
- Prepare for and respond to security incidents in your AWS environment (Prepare-se e responda a incidentes de segurança no ambiente da AWS)

Exemplos relacionados:

- Lab: AWS Account Setup and Root User (Laboratório: usuário raiz e configuração de conta da AWS)
- Lab: Incident Response with AWS Console and CLI (Laboratório: resposta a incidentes com o console e a CLI da AWS)

SEC10-BP06 Pré-implantação de ferramentas

Verifique se o pessoal de segurança tem as ferramentas certas pré-implantadas para reduzir o tempo de investigação até a recuperação.

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

Orientação para implementação

Para automatizar as funções de resposta e operações de segurança, você pode usar um conjunto abrangente de APIs e ferramentas da AWS. Você pode automatizar totalmente os recursos de gerenciamento de identidade, segurança de rede, proteção de dados e monitoramento e disponibilizá-los com métodos populares de desenvolvimento de software já em vigor. Quando você cria a automação da segurança, seu sistema pode monitorar, analisar e iniciar uma resposta, em vez de fazer com que as pessoas monitorem a sua posição de segurança e reajam manualmente a eventos.

Se as equipes de resposta a incidentes continuarem a responder aos alertas da mesma forma, há o risco de se acostumarem aos alertas. Com o passar do tempo, a equipe pode se tornar dessensibilizada para alertas e cometer erros ao lidar com situações comuns ou perder alertas incomuns. A automação ajuda a evitar a exaustão de alertas usando funções que processam alertas repetitivos e comuns, permitindo que as pessoas lidem com incidentes confidenciais e exclusivos.

A integração de sistemas de detecção de anomalias, como Amazon GuardDuty, AWS CloudTrail Insights e Amazon CloudWatch Anomaly Detection, pode reduzir a carga de alertas baseados em limites comuns.

Você pode melhorar os processos manuais com a automatização programática das etapas do processo. Depois de definir o padrão de correção para um evento, você pode decompor esse padrão em lógica acionável e desenvolver o código para executar essa lógica. Os respondentes podem executar esse código para corrigir o problema. Com o passar do tempo, você pode automatizar mais e mais etapas e, por fim, lidar automaticamente com classes inteiras de incidentes comuns.

Durante uma investigação de segurança, você precisa ser capaz de analisar 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 ocorreram determinadas ações de interesse. É essencial selecionar, ativar, armazenar e configurar mecanismos de consulta, recuperação e definir alertas. Além disso, uma forma eficaz de fornecer ferramentas para pesquisar dados de log é o Amazon Detective.

A AWS oferece mais de 200 serviços em nuvem e milhares de recursos. Recomendamos que você analise os serviços que podem apoiar e simplificar sua estratégia de resposta a incidentes.

Além do registro em log, você deve desenvolver e implementar uma estratégia consistente de marcação. A marcação pode ajudar a fornecer contexto sobre a finalidade de um recurso da AWS. A marcação também pode ser usada para automação.

Etapas da implementação

Selecione e configure logs para análise e alertas

Consulte a documentação a seguir sobre como configurar logs para resposta a incidentes:

- Logging strategies for security incident response (Estratégias de registro para resposta a incidentes de segurança)
- SEC04-BP01 Configurar registro em log de serviço e aplicação

Habilite serviços de segurança para oferecer suporte à detecção e resposta

A AWS fornece recursos nativos de detecção, prevenção e resposta, e outros serviços podem ser usados para arquitetar soluções de segurança personalizadas. Para obter uma lista dos serviços mais relevantes para resposta a incidentes de segurança, consulte Definições de capacidade de nuvem.

Desenvolva e implemente uma estratégia de marcação

Obter informações contextuais sobre o caso de uso empresarial e as partes interessadas internas relevantes em torno de um recurso da AWS pode ser difícil. Uma forma de fazer isso é na forma de tags, que atribuem metadados aos recursos da AWS e consistem em uma chave e um valor definidos pelo usuário. Você pode criar tags para categorizar os recursos por finalidade, proprietário, ambiente, tipo de dados processados e outros critérios de sua escolha.

Ter uma estratégia de marcação consistente pode acelerar os tempos de resposta e minimizar o tempo gasto no contexto organizacional, permitindo identificar e discernir rapidamente as informações contextuais sobre um recurso da AWS. As tags também podem servir como um mecanismo para iniciar automações de resposta. Para obter mais detalhes sobre o que marcar, consulte Tagging your AWS resources. Primeiro, você deve definir as tags que deseja implementar em toda a sua organização. Depois disso, você implementará e aplicará essa estratégia de marcação. Para obter mais detalhes sobre implementação e aplicação, consulte Implement AWS resource tagging strategy using AWS Tag Policies and Service Control Policies (SCPs).

Recursos

Práticas recomendadas relacionadas ao Well-Architected:

- SEC04-BP01 Configurar registro em log de serviço e aplicação
- SEC04-BP02 Analisar logs, descobertas e métricas de forma centralizada

Documentos relacionados:

- Logging strategies for security incident response (Estratégias de registro para resposta a incidentes de segurança)
- Incident response cloud capability definitions (Definições de recursos de nuvem de resposta a incidentes)

Exemplos relacionados:

- Threat Detection and Response with Amazon GuardDuty and Amazon Detective
- Security Hub Workshop (Workshop do Security Hub)
- Vulnerability Management with Amazon Inspector

SEC10-BP07 Execute simulações

À medida que as organizações crescem e evoluem com o tempo, o mesmo acontece com o cenário de ameaças, o que torna importante analisar continuamente seus recursos de resposta a incidentes. Executar simulações (também conhecidas como dias de teste) é um método que pode ser usado para realizar essa avaliação. As simulações usam cenários de eventos de segurança do mundo real projetados para imitar as táticas, as técnicas e os procedimentos (TTPs) de um agente de ameaças e permitir que uma organização exercite e avalie seus recursos de resposta a incidentes respondendo a esses eventos cibernéticos simulados da mesma forma que em uma situação real.

Benefícios do estabelecimento dessa prática recomendada: as simulações têm vários benefícios:

- Validar a prontidão cibernética e desenvolver a confiança de seus socorristas.
- Testar a precisão e a eficiência de ferramentas e fluxos de trabalho.
- Refinar os métodos de comunicação e escalonamento alinhados com seu plano de resposta a incidentes.
- Proporcionar uma oportunidade de responder a vetores menos comuns.

Nível de exposição a riscos se esta prática recomendada não for estabelecida: médio

Orientações para a implementação

Existem três tipos principais de simulações:

- Simulações teóricas: a abordagem de simulações teóricas é uma sessão baseada em discussões que envolvem as várias partes interessadas na resposta a incidentes para exercer funções e responsabilidades e usar ferramentas de comunicação e manuais estabelecidos. A facilitação das simulações normalmente pode ser realizada em um dia inteiro em um local virtual, local físico ou uma combinação de ambos. Por ser baseada em discussões, a simulação teórica se concentra em processos, pessoas e colaboração. A tecnologia é parte integrante da discussão, mas o uso real de ferramentas ou scripts de resposta a incidentes geralmente não faz parte da simulação teórica.
- Simulações da equipe roxa: as simulações da equipe roxa aumentam o nível de colaboração entre os respondentes ao incidente (equipe azul) e os agentes de ameaças simuladas (equipe vermelha). A equipe azul é composta por membros do centro de operações de segurança (SOC), mas também pode incluir outras partes interessadas que estariam envolvidas durante um evento cibernético real. A equipe vermelha é composta por uma equipe de testes de penetração ou pelas principais partes interessadas treinadas em segurança ofensiva. A equipe vermelha trabalha em

colaboração com os facilitadores da simulação ao projetar um cenário para que este seja preciso e viável. Durante as simulações da equipe roxa, o foco principal está nos mecanismos de detecção, nas ferramentas e nos procedimentos operacionais padrão (SOPs) que apoiam os esforços de resposta a incidentes.

- Simulações da equipe vermelha: durante uma simulação da equipe vermelha, o infrator (equipe vermelha) realiza uma simulação para atingir um determinado objetivo ou conjunto de objetivos a partir de um escopo predeterminado. Os defensores (equipe azul) não necessariamente terão conhecimento do escopo e da duração da simulação, o que oferece uma avaliação mais realista de como eles responderiam a um incidente real. Como as simulações da equipe vermelha podem ser testes invasivos, tenha cuidado e implemente controles para verificar se a simulação não causa danos reais ao ambiente.

Considere facilitar as simulações cibernéticas em intervalos regulares. Cada tipo de simulação pode oferecer benefícios exclusivos aos participantes e à organização como um todo. Portanto, você pode optar por começar com tipos de simulação menos complexos (como simulações teóricas) e avançar para tipos de simulação mais complexos (simulações da equipe vermelha). Você deve selecionar um tipo de simulação com base em sua maturidade de segurança, recursos e resultados desejados. Alguns clientes podem não optar por realizar simulações da equipe vermelha devido à complexidade e ao custo.

Etapas da implementação

Independentemente do tipo de simulação que você escolher, as simulações geralmente seguem estas etapas de implementação:

1. Defina os principais elementos do exercício: defina o cenário e os objetivos da simulação. Ambos devem ter aceitação da liderança.
2. Identifique as principais partes interessadas: no mínimo, um exercício precisa de facilitadores e participantes. Dependendo do cenário, outras partes interessadas, como departamento jurídico, de comunicação ou liderança executiva, podem estar envolvidos.
3. Crie e teste o cenário: talvez o cenário precise ser redefinido durante a criação se elementos específicos não forem viáveis. Espera-se um cenário finalizado como resultado dessa etapa.
4. Facilite a simulação: o tipo de simulação determina a facilitação usada (um cenário impresso em comparação a um cenário simulado altamente técnico). Os facilitadores devem alinhar suas táticas de facilitação aos objetos da simulação e envolver todos os participantes sempre que possível para proporcionar o máximo benefício.

5. Desenvolva o relatório pós-ação (AAR): identifique as áreas que funcionaram bem, aquelas que podem ser melhoradas e possíveis déficits. O AAR deve medir a eficácia da simulação, bem como a resposta da equipe ao evento simulado, para que o progresso possa ser monitorado ao longo do tempo com simulações futuras.

Recursos

Documentos relacionados:

- AWS Incident Response Guide (Guia de resposta a incidentes da AWS)

Vídeos relacionados:

- AWS GameDay - Security Edition (Dia de jogo da AWS: edição de segurança)

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 estas cinco fases: detecção, análise, contenção, erradicaçãoe recuperação. As descrições dessas fases e dos objetivos podem ser encontradas na tabela a seguir.

Fase	Objetivo
Detecção	Identifique um possível evento de segurança.
Análise	Determine se o evento de segurança é um incidente e avalie o escopo do incidente.
Contenção	Minimize e limite o escopo do evento de segurança.
Erradicação	Remova recursos ou artefatos não autorizad os relacionados ao evento de segurança . Implemente atenuações que causaram o incidente de segurança.

Fase	Objetivo
Recuperação	Restaure os sistemas ao estado seguro conhecido e monitore esses sistemas para verificar se não há retorno da ameaça.

As fases devem servir como orientação quando você responde e atua em incidentes de segurança, a fim de responder de forma eficaz e robusta. As ações reais realizadas vão variar de acordo com o incidente. Um incidente envolvendo ransomware, por exemplo, terá um conjunto de etapas de resposta a serem seguidas diferente do que o de um incidente que envolva um bucket público do Amazon S3. Além disso, essas fases não acontecem necessariamente de modo sequencial. Após a contenção e a erradicação, talvez seja necessário retornar à análise para entender se suas ações foram eficazes.

A preparação completa de seu pessoal, processos e tecnologia é fundamental para ser eficaz nas operações. Dessa forma, siga as práticas recomendadas da seção Preparação para poder responder com eficácia a um evento de segurança ativo.

Para saber mais, consulte a seção Operações do Guia de resposta a incidentes de segurança da AWS.

Atividade pós-incidente

O cenário de ameaças está mudando constantemente, e é importante ser igualmente dinâmico na capacidade de sua organização de proteger seus ambientes com eficácia. A chave para a melhoria contínua é iterar os resultados de seus incidentes e simulações a fim de melhorar seus recursos para detectar, responder e investigar com eficácia possíveis incidentes de segurança, reduzindo suas possíveis vulnerabilidades, o tempo de resposta e o retorno às operações seguras. Os mecanismos a seguir podem ajudar você a verificar se sua organização continua preparada com os recursos e os conhecimentos mais recentes para responder com eficácia, independentemente da situação.

Práticas recomendadas

- SEC10-BP08 Estabeleça uma estrutura para aprender com os incidentes

SEC10-BP08 Estabeleça uma estrutura para aprender com os incidentes

A implementação de uma framework de lições aprendidas e da capacidade de análise da causa raiz não só ajudará a melhorar os recursos de resposta a incidentes, mas também ajudará a evitar que o incidente se repita. Ao aprender com cada incidente, você pode ajudar a evitar a repetição dos mesmos erros, exposições ou configurações incorretas, não apenas melhorando seu procedimento de segurança, mas também minimizando o tempo perdido em situações evitáveis.

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

Orientação para implementação

É importante implementar uma framework de lições aprendidas que estabeleça e alcance, em nível geral, os seguintes pontos:

- Quando as lições são aprendidas?
- O que está envolvido no processo de lições aprendidas?
- Como as lições aprendidas são colocadas em prática?
- Quem está envolvido no processo e como?
- Como as áreas de melhoria serão identificadas?
- Como você garantirá que as melhorias sejam monitoradas e implementadas de forma eficaz?

A estrutura não deve se concentrar em culpar os indivíduos, mas sim na melhoria de ferramentas e processos.

Etapas da implementação

Além dos resultados de alto nível listados acima, é importante garantir que você faça as perguntas certas para obter o máximo valor (informações que levem a melhorias práticas) do processo. Considere estas perguntas para ajudar você a começar a promover discussões sobre as lições aprendidas:

- Qual foi o incidente?
- Quando o incidente foi identificado pela primeira vez?
- Como ele foi identificado?
- Quais sistemas alertaram sobre a atividade?

- Quais sistemas, serviços e dados estavam envolvidos?
- O que ocorreu especificamente?
- O que funcionou bem?
- O que não funcionou bem?
- Quais 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 com eficácia?
    - 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?
    - Estavam faltando processos e procedimentos necessários?
    - Os respondentes conseguiram obter acesso oportuno às informações necessárias para responder ao problema?
  - Tecnologia
    - Os sistemas de alerta existentes identificaram e alertaram efetivamente sobre a atividade?
    - Como poderíamos ter reduzido o tempo de detecção em 50%?
    - Os alertas existentes precisam ser aprimorados ou novos alertas precisam ser criados para esse (tipo de) incidente?
    - As ferramentas existentes permitiram uma investigação (pesquisa/análise) eficaz do incidente?
    - O que pode ser feito para ajudar a identificar esse (tipo de) incidente mais cedo?
    - O que pode ser feito para ajudar a evitar que esse (tipo de) incidente ocorra novamente?
    - Quem é o proprietário do plano de melhoria e como você testará se ele foi implementado?
    - Qual é o cronograma para que os controles e processos adicionais de monitoramento ou prevenção sejam implementados e testados?

Essa lista não inclui tudo, mas serve como ponto de partida para identificar quais são as necessidades da organização e da empresa e como você pode analisá-las para aprender com os incidentes de forma mais eficaz e melhorar constantemente seu procedimento de segurança. O mais importante é começar incorporando as lições aprendidas como parte padrão do processo de resposta a incidentes, da documentação e das expectativas das partes interessadas.

Recursos

Documentos relacionados:

- AWS Security Incident Response Guide - Establish a framework for learning from incidents
- NCSC CAF guidance - Lessons learned (Orientações do NCSC CAF: lições aprendidas)

Segurança de aplicações

A segurança de aplicações (AppSec) retrata o processo geral de como projetar, criar e testar as propriedades de segurança das workloads desenvolvidas. Você precisa treinar a equipe adequadamente em sua organização, entender as propriedades de segurança de sua infraestrutura de compilação e lançamento e utilizar a automação para identificar problemas de segurança.

Adotar testes de segurança de aplicações como parte regular do ciclo de vida de desenvolvimento de software (SDLC) e processos de pós-lançamento ajuda a garantir que você tenha um mecanismo estruturado para identificar, corrigir e impedir que problemas de segurança de aplicações entrem no ambiente de produção.

Sua metodologia de desenvolvimento de aplicações deve incluir controles de segurança à medida que você projeta, cria, implanta e opera suas workloads. Ao fazer isso, alinhe o processo para redução contínua de defeitos e redução da dívida técnica. Por exemplo, o uso de modelagem de ameaças na fase de design ajuda a detectar falhas de design precocemente, o que torna mais fácil e menos caro corrigi-las em contraposição a aguardar e mitigá-las posteriormente.

O custo e a complexidade para resolver defeitos geralmente serão menores quanto mais no princípio você estiver no SDLC. A forma mais fácil de resolver problemas é não os ter. Por isso, começar com um modelo de ameaças ajuda você a se concentrar nos resultados corretos da fase de design. À medida que seu programa de AppSec amadurece, é possível aumentar a quantidade de testes realizados usando automação, aumentar a fidelidade do feedback para os criadores e reduzir o tempo necessário para as avaliações de segurança. Todas essas ações melhoram a qualidade do software desenvolvido e aumentam a velocidade de entrega de recursos à produção.

Essas diretrizes de implementação concentram-se em quatro áreas: organização e cultura, segurança do pipeline, segurança no pipeline e gerenciamento de dependências. Cada área oferece um conjunto de princípios que você pode implementar, bem como uma visão completa de como projetar, desenvolver, criar, implantar e operar workloads.

Na AWS, há várias abordagens para lidar com seu programa de segurança de aplicações. Algumas dessas abordagens dependem de tecnologia, enquanto outras se concentram na equipe e em aspectos organizacionais do programa de segurança de aplicações.

Práticas recomendadas

- SEC11-BP01 Treinar para segurança de aplicações
- SEC11-BP02 Automatizar o teste durante o ciclo de vida de desenvolvimento e lançamento

- SEC11-BP03 Realizar teste de penetração regular
- SEC11-BP04 Análises manuais de código
- SEC11-BP05 Centralizar serviços para pacotes e dependências
- SEC11-BP06 Implantar software programaticamente
- SEC11-BP07 Avaliar regularmente as propriedades de segurança dos pipelines
- SEC11-BP08 Criar um programa que incorpore a propriedade de segurança nas equipes de workload

SEC11-BP01 Treinar para segurança de aplicações

Forneça treinamento aos criadores em sua organização sobre práticas comuns para promover a segurança no desenvolvimento e na operação de aplicações. A adoção de práticas de desenvolvimento com foco na segurança ajuda a diminuir a probabilidade de problemas que são detectados somente no estágio de avaliação da segurança.

Resultado desejado: o software deve ser projetado e criado com a segurança em mente. Quando os criadores em uma organização são treinados em práticas de desenvolvimento seguras que começam com um modelo de ameaças, isso melhora a qualidade e a segurança gerais do software produzido. Essa abordagem pode reduzir o tempo de entrega do software ou de recursos porque não é necessário tanto retrabalho após o estágio de avaliação da segurança.

Para as finalidades desta prática recomendada, desenvolvimento seguro refere-se ao software que está sendo criado e às ferramentas ou aos sistemas compatíveis com o ciclo de vida de desenvolvimento de software (SDLC).

Antipadrões comuns:

- Aguardar uma avaliação da segurança e, depois, considerar as propriedades de segurança de um sistema.
- Deixar todas as decisões de segurança para a equipe de segurança.
- Não comunicar como as decisões tomadas no SDLC se relacionam às expectativas ou as políticas de segurança gerais da organização.
- Iniciar o processo de avaliação da segurança muito tardiamente.

Benefícios do estabelecimento desta prática recomendada:

- Melhor conhecimento dos requisitos organizacionais para a segurança na fase inicial do ciclo de desenvolvimento.
- Ser capaz de identificar e solucionar possíveis problemas de segurança com maior rapidez, promovendo uma entrega de recursos mais rápida.
- Maior qualidade do software e dos sistemas.

Nível de exposição a riscos se esta prática recomendada não for estabelecida: médio

Orientações para a implementação

Ofereça treinamento aos criadores em sua organização. Iniciar um curso sobre modelagem de ameaças é uma boa base para ajudar a treinar para segurança. Preferencialmente, os criadores devem ser capazes de acessar de forma independente as informações relevantes às respectivas workloads. Esse acesso os ajuda a tomar decisões embasadas sobre as propriedades de segurança dos sistemas criados por eles sem a necessidade de solicitar outra equipe. O processo para envolver a equipe de segurança para avaliações deve ser claramente definido e simples de seguir. As etapas do processo de avaliação devem ser incluídas no treinamento de segurança. Quando houver padrões ou modelos de implementação disponíveis, eles deverão ser simples de encontrar e vincular aos requisitos de segurança gerais. Considere usar o AWS CloudFormation, as estruturas do AWS Cloud Development Kit (AWS CDK), o Service Catalog ou outras ferramentas de modelo para reduzir a necessidade de configuração personalizada.

Etapas da implementação

- Oferecer aos criadores um curso sobre modelagem de ameaças para criar uma boa base e ajudar a treiná-los a pensar em segurança.
- Conceder acesso ao treinamento do Treinamento da AWS and Certification, do setor ou de parceiros da AWS.
- Fornecer treinamento sobre o processo de avaliação da segurança de sua organização, que esclarece a divisão de responsabilidades entre a equipe de segurança, as equipes de workload e outras partes interessadas.
- Publicar orientações de autoatendimento sobre como atender aos seus requisitos de segurança, inclusive códigos de exemplo e modelos, se disponíveis.
- Obter feedback regularmente de equipes de criadores sobre a experiência deles com o processo e o treinamento de processo de avaliação da segurança e usar esse feedback para promover melhorias.

- Utilizar dias de jogo ou campanhas de bug bash para ajudar a reduzir o número de problemas e aumentar as habilidades de seus criadores.

Recursos

Práticas recomendadas relacionadas:

- SEC11-BP08 Criar um programa que incorpore a propriedade de segurança nas equipes de workload

Documentos relacionados:

- Treinamento da AWS and Certification
- Como pensar sobre governança de segurança na nuvem
- Como abordar a modelagem de ameaças
- Como acelerar o treinamento: o AWS Skills Guild

Vídeos relacionados:

- Segurança proativa: considerações e abordagens

Exemplos relacionados:

- Workshop sobre modelagem de ameaças
- Conscientização do setor para desenvolvedores

Serviços relacionados:

- AWS CloudFormation
- Estruturas do AWS Cloud Development Kit (AWS CDK) (AWS CDK)
- Service Catalog
- AWS BugBust

SEC11-BP02 Automatizar o teste durante o ciclo de vida de desenvolvimento e lançamento

Automatize o teste das propriedades de segurança durante o ciclo de vida de desenvolvimento e lançamento. Com a automação, é mais fácil identificar de forma consistente e repetível possíveis problemas no software antes do lançamento, o que reduz o risco de problemas de segurança no software que está sendo fornecido.

Resultado esperado: o objetivo do teste automatizado é oferecer uma forma programática de detectar possíveis problemas precocemente e com frequência ao longo do ciclo de vida de desenvolvimento. Ao automatizar o teste de regressão, você pode executar novamente testes funcionais e não funcionais para verificar se o software testado anteriormente ainda funciona da forma esperada após uma alteração. Ao definir testes de unidade de segurança para conferir configurações incorretas comuns, como uma autenticação ausente ou danificada, é possível identificar e resolver esses problemas logo no início do processo de desenvolvimento.

A automação de testes utiliza casos de teste para um propósito específico para validação de aplicações, com base nos requisitos e na funcionalidade desejada da aplicação. O resultado dos testes automatizados baseia-se na comparação da saída do teste gerado com a respectiva saída esperada, o que acelera o ciclo de vida dos testes em geral. As metodologias de teste, como teste de regressão e pacotes de teste de unidade, são mais adequadas para automação. A automação dos testes de propriedades de segurança possibilita aos criadores receber feedback automatizado sem precisar esperar por uma avaliação da segurança. Os testes automatizados em forma de análise de código estático ou dinâmico podem melhorar a qualidade do código e ajudar a detectar possíveis problemas de software no ciclo de vida de desenvolvimento.

Antipadrões comuns:

- Não comunicar os casos de teste e os resultados dos testes automatizados.
- Realizar os testes automatizados somente antes de um lançamento.
- Automatizar casos de teste com requisitos que mudam com frequência.
- Não fornecer orientações sobre como abordar os resultados dos testes de segurança.

Benefícios do estabelecimento desta prática recomendada:

- Redução da dependência de pessoas que avaliam as propriedades de segurança dos sistemas.

- Descobertas consistentes em vários fluxos de trabalho que melhoram a consistência.
- Redução da probabilidade de introduzir problemas de segurança no software de produção.
- Redução do período de tempo entre a detecção e a correção devido à detecção mais antecipada de problemas de software.
- Maior visibilidade do problema sistêmico ou repetido entre os vários fluxos de trabalho, o que pode ser utilizado para promover melhorias em toda a organização.

Nível de exposição a riscos se esta prática recomendada não for estabelecida: médio

Orientação de implementação

Ao criar um software, adote vários mecanismos de teste para garantir que você esteja testando os requisitos funcionais da aplicação, com base na respectiva lógica de negócios e em requisitos não funcionais, os quais se concentram na confiabilidade, performance e segurança da aplicação.

O teste de segurança de aplicação estática (SAST) analisa padrões de segurança anômalos no código-fonte e fornece indicações de código propenso a defeitos. O SAST depende de entradas estáticas, como documentação (especificação de requisitos, documentação e especificações de design) e código-fonte da aplicação, para testar uma série de problemas de segurança conhecidos. Os analisadores de código estático podem ajudar a acelerar a análise de grandes volumes de código. O NIST Quality Group oferece uma comparação de analisadores de segurança de código-fonte, o que inclui ferramentas de código aberto para leitores de código de byte e leitores de código binário.

Complemente seu teste estático com metodologias de teste de segurança de análise dinâmica (DAST), que realizam testes na aplicação em execução a fim de identificar comportamento possivelmente inesperado. O teste dinâmico pode ser utilizado para detectar possíveis problemas que não são detectáveis por meio de análise estática. Por meio dos testes nos estágios de repositório de código, compilação e pipeline, é possível impedir que diferentes tipos de problema em potencial ocorram no código. O Amazon CodeWhisperer oferece recomendações de código, como verificação de segurança, no IDE do criador. O Amazon CodeGuru Reviewer pode identificar problemas críticos, problemas de segurança e bugs difíceis de detectar durante o desenvolvimento da aplicação e oferece recomendações para melhorar a qualidade do código.

O workshop Segurança para desenvolvedores utiliza ferramentas de desenvolvedor da AWS, como AWS CodeBuild, AWS CodeCommit e AWS CodePipeline, para automação de pipeline de lançamento que inclui as metodologias de teste SAST e DAST.

À medida que você avançar no SDLC, estabeleça um processo iterativo que inclua avaliações de aplicação periódicas com sua equipe de segurança. O feedback coletado dessas avaliações de segurança deve ser abordado e validado como parte de sua avaliação de prontidão do lançamento. Essas avaliações estabelecem um procedimento de segurança robusto de aplicações e fornecem aos criadores feedback útil para resolver possíveis problemas.

Etapas da implementação

- Implementar um IDE consistente, análise de código e ferramentas de CI/CD que incluam teste de segurança.
- Considerar quando no SDLC é adequado bloquear pipelines em vez de apenas notificar os criadores de que problemas precisam ser corrigidos.
- O workshop Segurança para desenvolvedores fornece um exemplo de como integrar testes estáticos e dinâmicos a um pipeline de lançamento.
- Realizar testes ou análise de código com ferramentas automatizadas, como o Amazon CodeWhisperer integrado a IDEs de desenvolvedores e o Amazon CodeGuru Reviewer para verificação do código na confirmação, ajuda os criadores a obter feedback no momento certo.
- Ao criar com o AWS Lambda, é possível usar o Amazon Inspector para verificar o código de aplicação em suas funções.
- O workshop CI/CD na AWS fornece um ponto de partida para criar pipelines de CI/CD na AWS.
- Quando testes automatizados são incluídos em pipelines de CI/CD, você precisa usar um sistema de emissão de tíquetes para rastrear a notificação e a correção de problemas de software.
- Para testes de segurança que podem gerar descobertas, a vinculação com orientações para correção ajuda os criadores a melhorar a qualidade do código.
- Analise regularmente as descobertas das ferramentas automatizadas para priorizar a próxima automação, o treinamento de criadores ou a campanha de conscientização.

Recursos

Documentos relacionados:

- Entrega contínua e implantação contínua

- Parceiros com competência em DevOps da AWS
- Parceiros de competência em segurança da AWS para segurança da aplicação

- Como escolher uma abordagem de CI/CD do Well-Arquitected
- Monitorar eventos do CodeCommit no Amazon EventBridge e no Amazon CloudWatch Events
- Análise da detecção de segredos no Amazon CodeGuru Review
- Acelerar implantações na AWS com governança efetiva
- Como a AWS aborda a automação de implantações seguras e sem intervenção manual

Vídeos relacionados:

- Sem intervenção manual: como automatizar os pipelines de entrega contínua na Amazon
- Como automatizar pipelines CI/CD entre contas

Exemplos relacionados:

- Conscientização do setor para desenvolvedores
- Governança do AWS CodePipeline
- Workshop Segurança para desenvolvedores
- Workshop sobre CI/CD da AWS

SEC11-BP03 Realizar teste de penetração regular

Realize teste de penetração regular do software. Esse mecanismo ajuda a identificar possíveis problemas de software que não podem ser detectados pelo teste automatizado ou por uma análise manual do código. Ele também ajuda você a entender a eficácia dos controles de detecção. O teste de penetração deve tentar determinar se o software pode ser executado de formas inesperadas; por exemplo, expondo dados que devem ser protegidos ou concedendo permissões mais amplas que o esperado.

Resultado desejado: o teste de penetração é usado para detectar, corrigir e validar as propriedades de segurança da aplicação. O teste de penetração regular e programado deve ser realizado como parte do ciclo de vida de desenvolvimento de software (SDLC). As descobertas do teste de penetração devem ser abordadas antes do lançamento do software. Você precisa analisar as descobertas do teste de penetração para identificar se há problemas que podem ser encontrados usando a automação. Ter um processo de teste de penetração regular e repetível que inclua um

mecanismo de feedback ativo ajuda a transmitir as orientações aos criadores e melhora a qualidade do software.

Antipadrões comuns:

- Realizar um teste de penetração somente para problemas de segurança conhecidos ou prevalentes.
- Realizar um teste de penetração em aplicações sem ferramentas e bibliotecas de terceiro dependentes.
- Realizar um teste de penetração em aplicações em busca de problemas de segurança de pacote e não avaliar a lógica de negócios implementada.

Benefícios do estabelecimento desta prática recomendada:

- Maior confiança nas propriedades de segurança do software antes do lançamento.
- Oportunidade de identificar padrões de aplicação preferenciais, o que aumenta a qualidade do software.
- Um ciclo de feedback que identifica mais cedo no ciclo de desenvolvimento quando a automação ou treinamento adicional pode melhorar as propriedades de segurança do software.

Nível de exposição a riscos se esta prática recomendada não for estabelecida: alto

Orientação de implementação

O teste de penetração é um exercício de teste de segurança estruturado em que você executa cenários de violação de segurança planejados a fim de detectar, corrigir e validar controles de segurança. Os testes de penetração começam com o reconhecimento, durante o qual os dados são coletados com base no design atual da aplicação e nas respectivas dependências. Uma lista selecionada de cenários de teste específicos de segurança é criada e executada. A principal finalidade desses testes é revelar problemas de segurança em sua aplicação, que podem ser explorados para obter acesso não intencional ao seu ambiente ou acesso não autorizado aos dados. Você precisa realizar o teste de penetração ao lançar novos recursos ou sempre que sua aplicação passar por alterações importantes na implementação técnica ou de funções.

É necessário identificar o estágio mais apropriado do ciclo de vida de desenvolvimento para realizar o teste de penetração. Esse teste deve ocorrer em uma fase tardia o suficiente para que

a funcionalidade do sistema esteja próxima ao estado de lançamento pretendido, mas com tempo suficiente para corrigir todos os problemas.

Etapas da implementação

- Ter um processo estruturado sobre como definir o escopo do teste de penetração. Basear esse processo no modelo de ameaças é uma boa forma de manter o contexto.
- Identificar o estágio apropriado do ciclo de vida de desenvolvimento para realizar o teste de penetração, que deve ser quando houver o mínimo de alterações esperadas na aplicação e houver tempo suficiente para realizar a correção.
- Treinar os criadores sobre o que esperar das descobertas do teste de penetração e como ter informações sobre correção.
- Utilizar ferramentas para acelerar o processo de testes de penetração automatizando testes comuns ou repetíveis.
- Analisar as descobertas do teste de penetração para identificar problemas de segurança sistêmicos e utilizar esses dados para embasar testes automatizados adicionais e a instrução contínua dos criadores.

Recursos

Práticas recomendadas relacionadas:

- SEC11-BP01 Treinar para segurança de aplicações
- SEC11-BP02 Automatizar o teste durante o ciclo de vida de desenvolvimento e lançamento

Documentos relacionados:

- O teste de penetração da AWS fornece orientações detalhadas para teste de penetração na AWS
- Acelerar implantações na AWS com governança efetiva
- Parceiros de competência em segurança da AWS
- Modernize sua arquitetura de teste de penetração no AWS Fargate
- AWS Fault injection Simulator

Exemplos relacionados:

- Como automatizar testes de API com o AWS CodePipeline (GitHub)
- Assistente de segurança automatizado (GitHub)

SEC11-BP04 Análises manuais de código

Realize uma análise manual do código do software que você produz. Esse processo ajuda a verificar se a pessoa que escreveu o código não é a única que está conferindo a qualidade dele.

Resultado desejado: a inclusão de uma etapa de análise de código manual durante o desenvolvimento melhora a qualidade do software que está sendo criado, ajuda a melhorar as habilidades de membros menos experientes da equipe e oferece uma oportunidade de identificar locais onde a automação pode ser usada. É possível oferecer compatibilidade com as análises de código manuais com ferramentas e testes automatizados.

Antipadrões comuns:

- Não realizar análises de código antes da implantação.
- Ter a mesma pessoa para escrever e analisar o código.
- Não utilizar a automação para auxiliar ou orquestrar as análises de código.
- Não treinar os criadores em segurança de aplicações antes de analisarem o código.

Benefícios do estabelecimento desta prática recomendada:

- Código de melhor qualidade.
- Maior consistência do desenvolvimento do código por meio da reutilização de abordagens comuns.
- Redução no número de problemas descobertos durante o teste de penetração e em estágios posteriores.
- Maior transferência de conhecimentos na equipe.

Nível de exposição a riscos se esta prática recomendada não for estabelecida: médio

Orientações para a implementação

A etapa de análise deve ser implementada como parte do fluxo de gerenciamento de código geral. Os detalhes dependem da abordagem utilizada para ramificação, solicitações de pull e mesclagem.

Você pode utilizar o AWS CodeCommit ou soluções de terceiros, como GitHub, GitLab ou Bitbucket. Seja qual for o método utilizado, é importante verificar se seus processos precisam de análise de código antes da implantação em um ambiente de produção. O uso de ferramentas, como o Amazon CodeGuru Reviewer, pode facilitar a orquestração do processo de análise do código.

Etapas da implementação

- Implementar uma etapa de análise manual como parte do fluxo de gerenciamento de código e realizar essa análise antes de prosseguir.
- Considerar o Amazon CodeGuru Reviewer para gerenciar e auxiliar nas análises de código.
- Implementar um fluxo de aprovação que exija a realização de uma análise de código antes de avançá-lo para o próximo estágio.
- Verificar se há um processo para identificar problemas encontrados durante as análises de código manuais que possam ser detectados automaticamente.
- Integrar a etapa de análise de código manual de forma que se alinhe às suas práticas de desenvolvimento de código.

Recursos

Práticas recomendadas relacionadas:

- SEC11-BP02 Automatizar o teste durante o ciclo de vida de desenvolvimento e lançamento

Documentos relacionados:

- Trabalhar com solicitações de pull em repositórios do AWS CodeCommit
- Trabalhar com modelos de regra de aprovação no AWS CodeCommit
- Sobre solicitações de pull no GitHub
- Análises de código automatizadas com o Amazon CodeGuru Reviewer
- Automatizar a detecção de vulnerabilidades de segurança e bugs em pipelines de CI/CD com o uso da CLI do Amazon CodeGuru Reviewer

Vídeos relacionados:

- Melhoria contínua da qualidade do código com o Amazon CodeGuru

Exemplos relacionados:

- Workshop Segurança para desenvolvedores

SEC11-BP05 Centralizar serviços para pacotes e dependências

Forneça serviços centralizados a equipes de criadores para obter pacotes de software e outras dependências. Isso permite a validação de pacotes antes que eles sejam incluídos no software que você escreve e fornece uma fonte de dados para a análise do software que está sendo usado na sua organização.

Resultado desejado: o software é composto de um conjunto de outros pacotes de software além do código que está sendo escrito. Isso simplifica o consumo de implementações de funcionalidades que são utilizadas repetidamente, como um analisador JSON ou uma biblioteca de criptografia. A centralização lógica das fontes desses pacotes e dependências oferece um mecanismo para as equipes de segurança validarem as propriedades dos pacotes antes de eles serem utilizados. Essa abordagem também reduz o risco de um problema inesperado ser provocado por uma alteração em um pacote existente ou pela inclusão de pacotes arbitrários diretamente da Internet pelas equipes de criadores. Utilize essa abordagem em conjunto com os fluxos de testes manuais e automatizados para aumentar a confiança na qualidade do software que está sendo desenvolvido.

Antipadrões comuns:

- Extrair pacotes de repositórios arbitrários na Internet.
- Não testar novos pacotes antes de disponibilizá-los aos criadores.

Benefícios do estabelecimento desta prática recomendada:

- Melhor entendimento de quais pacotes estão sendo utilizados no software que está sendo criado.
- Capacidade de notificar as equipes de workload quando um pacote precisa ser atualizado com base no entendimento de quem está usando o quê.
- Redução do risco de um pacote com problemas ser incluído em seu software.

Nível de exposição a riscos se esta prática recomendada não for estabelecida: médio

Orientação de implementação

Forneça serviços centralizados para pacotes e dependências de uma forma simples para os criadores consumirem. Serviços centralizados podem ser centralizados logicamente em vez de implementados como um sistema monolítico. Essa abordagem possibilita fornecer serviços de uma forma que atenda às necessidades dos criadores. Você precisa implementar uma forma eficiente de adicionar pacotes ao repositório quando ocorrem atualizações ou surgem novos requisitos. Serviços da AWS como o AWS CodeArtifact ou soluções semelhantes de parceiros da AWS oferecem uma forma de entregar esse recurso.

Etapas da implementação:

- Implementar um serviço de repositório centralizado logicamente disponível em todos os ambientes onde o software é desenvolvido.
- Incluir acesso ao repositório como parte do processo de provisionamento de Conta da AWS.
- Criar automação para testar pacotes antes de serem publicados em um repositório.
- Manter métricas dos pacotes mais utilizados, das linguagens e das equipes com a maior quantidade de alterações.
- Fornecer um mecanismo automatizado para as equipes de criadores solicitarem novos pacotes e fornecerem feedback.
- Verificar regularmente os pacotes em seu repositório para identificar o possível impacto de problemas recém-descobertos.

Recursos

Práticas recomendadas relacionadas:

- SEC11-BP02 Automatizar o teste durante o ciclo de vida de desenvolvimento e lançamento

Documentos relacionados:

- Acelerar implantações na AWS com governança efetiva
- Aumentar a segurança de seu pacote com o kit de ferramentas CodeArtifact Package Origin Control
- Detectar problemas de segurança no registro em log com o Amazon CodeGuru Reviewer
- Níveis de cadeia de suprimentos para artefatos de software (SLSA)

Vídeos relacionados:

- Segurança proativa: considerações e abordagens
- A filosofia de segurança da AWS (re:Invent 2017)
- Quando a segurança, a proteção e a urgência importam: lidar com o Log4Shell

Exemplos relacionados:

- Pipeline de publicação de pacotes de várias regiões (GitHub)
- Publicar módulos Node.Js no AWS CodeArtifact usando o AWS CodePipeline (GitHub)
- Exemplo de pipeline do AWS CDK Java CodeArtifact (GitHub)
- Distribuir pacotes privados do .NET NuGet com o AWS CodeArtifact (GitHub)

SEC11-BP06 Implantar software programaticamente

Faça implantações de software de forma programática quando possível. Essa abordagem diminui a probabilidade de falha em uma implantação ou da introdução de um problema inesperado devido a erro humano.

Resultado desejado: manter as pessoas longe dos dados é um princípio essencial da criação segura na Nuvem AWS. Esse princípio inclui como implantar seu software.

Os benefícios de não contar com pessoas para implantar software é a maior confiança de que o componente testado é o que será implantado e de que a implantação sempre é realizada de forma consistente. O software não deve precisar de alterações para funcionar em diferentes ambientes. O uso dos princípios de desenvolvimento de aplicações de 12 fatores, especificamente a externalização da configuração, possibilita implantar o mesmo código em vários ambientes sem a necessidade de alterações. Assinar de forma criptográfica os pacotes de software é uma boa maneira de garantir que nada tenha sido alterado entre os ambientes. O resultado geral dessa abordagem é reduzir o risco em seu processo de alterações e melhorar a consistência das versões do software.

Antipadrões comuns:

- Implantar software manualmente em produção.
- Realizar alterações manualmente no software para suprir diferentes ambientes.

Benefícios do estabelecimento desta prática recomendada:

- Maior confiança no processo de lançamento de software.
- Redução do risco de uma alteração com falha afetar a funcionalidade dos negócios.
- Maior cadência de lançamentos devido ao menor risco de alterações.
- Recurso de reversão automática para eventos inesperados durante a implantação.
- Capacidade de comprovar de forma criptográfica que o software testado é o software implantado.

Nível de exposição a riscos se esta prática recomendada não for estabelecida: alto

Orientações para a implementação

Crie a infraestrutura de sua Conta da AWS para remover o acesso humano persistente dos ambientes e use ferramentas de CI/CD para realizar implantações. Projete suas aplicações de forma que os dados da configuração específica do ambiente sejam obtidos de uma fonte externa, como o AWS Systems Manager Parameter Store. Assine pacotes depois de testados e valide essas assinaturas durante a implantação. Configure seus pipelines de CI/CD para enviar código da aplicação e usar canários para confirmar a implantação bem-sucedida. Utilize ferramentas como o AWS CloudFormation ou o AWS CDK para definir sua infraestrutura; depois, use o AWS CodeBuild e o AWS CodePipeline para realizar operações de CI/CD.

Etapas da implementação

- Criar pipelines de CI/CD bem definidos para simplificar o processo de implantação.
- O uso do AWS CodeBuild e do AWS Code Pipeline para oferecer recurso de CI/CD simplifica a integração de teste de segurança aos seus pipelines.
- Seguir as orientações sobre separação de ambientes no whitepaper Organizar seu ambiente da AWS com o uso de várias contas.
- Garantir que não haja nenhum acesso humano persistente aos ambientes nos quais as workloads de produção estão em execução.
- Projetar as aplicações para oferecer compatibilidade com a externalização de dados de configuração.
- Considerar a implantação com o uso do modelo de implantação azul/verde.
- Implementar canários para validar a implantação bem-sucedida do software.
- Utilizar ferramentas criptográficas, como o AWS Signer ou o AWS Key Management Service (AWS KMS), para assinar e confirmar os pacotes de software que você está implantando.

Recursos

Práticas recomendadas relacionadas:

- SEC11-BP02 Automatizar o teste durante o ciclo de vida de desenvolvimento e lançamento

Documentos relacionados:

- Workshop sobre CI/CD da AWS
- Acelerar implantações na AWS com governança efetiva
- Automatizar uma implantação prática e sem intervenção manual
- Assinatura de código com o uso de CA privada do AWS Certificate Manager e chaves assimétricas do AWS Key Management Service)
- Assinatura de código: um controle de integridade e confiança para o AWS Lambda

Vídeos relacionados:

- Sem intervenção manual: como automatizar os pipelines de entrega contínua na Amazon

Exemplos relacionados:

- Implantações azul/verde com o AWS Fargate

SEC11-BP07 Avaliar regularmente as propriedades de segurança dos pipelines

Aplique os princípios do pilar Segurança do Well-Architected aos seus pipelines, com atenção especial à separação das permissões. Avalie as propriedades de segurança de sua infraestrutura de pipelines. O gerenciamento eficaz da segurança dos pipelines permite que você forneça segurança ao software que passa pelos pipelines.

Resultado desejado: os pipelines utilizados para criar e implantar o software devem seguir as mesmas práticas recomendadas que qualquer outra workload em seu ambiente. Os testes implementados nos pipelines não devem ser editáveis pelos criadores que os estão utilizando. Os pipelines só devem ter as permissões necessárias para as implantações que eles estão realizando e devem implementar proteções para evitar a implantação em ambientes errados. Os pipelines não

devem contar com credenciais de longo prazo e devem ser configurados para emitir o estado de forma que a integridade dos ambientes de compilação possa ser validada.

Antipadrões comuns:

- Testes de segurança que podem ser ignorados pelos criadores.
- Permissões excessivamente amplas para pipelines de implantação.
- Pipelines não configurados para validar entradas.
- Ausência de análise regular das permissões associadas à infraestrutura de CI/CD.
- Uso de credenciais de longo prazo ou codificadas.

Benefícios do estabelecimento desta prática recomendada:

- Maior confiança na integridade do software que está sendo criado e implantado pelos pipelines.
- Capacidade de interromper uma implantação quando há atividade suspeita.

Nível de exposição a riscos se esta prática recomendada não for estabelecida: alto

Orientação de implementação

Iniciar com serviços de CI/CD gerenciados que ofereçam compatibilidade com perfis do IAM reduz o risco de vazamento de credenciais. Aplicar os princípios do pilar Segurança à sua infraestrutura de pipeline de CI/CD pode ajudar você a determinar onde é possível realizar melhorias de segurança. Seguir a Arquitetura de referência de pipelines de implantação da AWS é um bom ponto de partida para criar seus ambientes de CI/CD. Analisar regularmente a implementação de pipelines e analisar comportamentos inesperados nos logs pode ajudar você a entender os padrões de uso dos pipelines que estão sendo utilizados para implantar o software.

Etapas da implementação

- Iniciar com a Arquitetura de referência de pipeline de implantação da AWS.
- Considerar o uso do AWS IAM Access Analyzer para gerar de forma programática as políticas de privilégio mínimo do IAM para os pipelines.
- Integrar seus pipelines ao monitoramento e aos alertas de forma que você seja notificado de atividade inesperada ou anormal. Para serviços gerenciados da AWS, o Amazon EventBridge possibilita rotear dados para destinos, como o AWS Lambda ou o Amazon Simple Notification Service (Amazon SNS).

Recursos

Documentos relacionados:

- Arquitetura de referência de pipeline de implantação da AWS
- Monitorar o AWS CodePipeline
- Práticas recomendadas de segurança para o AWS CodePipeline

Exemplos relacionados:

- Painel de monitoramento de DevOps (GitHub)

SEC11-BP08 Criar um programa que incorpore a propriedade de segurança nas equipes de workload

Crie um programa ou mecanismo que capacite as equipes de criadores a tomar decisões de segurança sobre o software que elas estão criando. Ainda assim é necessário que sua equipe de segurança valide essas decisões durante uma avaliação, mas a incorporação da propriedade de segurança nas equipes de criadores aumenta a velocidade e segurança do processo de criação de workloads. Esse mecanismo também promove uma cultura de propriedade que afeta de forma positiva a operação dos sistemas que você cria.

Resultado desejado: para incorporar a propriedade de segurança e a tomada de decisão às equipes de criadores, você pode treinar os criadores a pensar sobre segurança ou incrementar o treinamento deles com pessoal de segurança incorporado ou associado às equipes de criadores. As duas abordagens são válidas e possibilitam à equipe tomar decisões de segurança de melhor qualidade logo no início do ciclo de desenvolvimento. Esse modelo de propriedade é baseado em treinamento para segurança de aplicações. Iniciar com o modelo de ameaças para a workload específica ajuda a direcionar o design thinking (pensamento de design) para o contexto apropriado. Outro benefício de ter uma comunidade de criadores concentrados em segurança ou um grupo de engenheiros de segurança que trabalhem com equipes de criadores é que você pode entender mais profundamente como o software é escrito. Esse entendimento ajuda você a determinar as próximas áreas de melhoria em seu recurso de automação.

Antipadrões comuns:

- Deixar todas as decisões de design de segurança para a equipe de segurança.
- Não abordar os requisitos de segurança cedo o suficiente no processo de desenvolvimento.
- Não obter feedback dos criadores e do pessoal de segurança sobre a operação do programa.

Benefícios do estabelecimento desta prática recomendada:

- Redução do tempo para concluir as avaliações de segurança.
- Redução dos problemas de segurança que são detectados apenas no estágio de avaliação da segurança.
- Melhoria da qualidade geral do software que está sendo escrito.
- Oportunidade de identificar e entender problemas sistêmicos ou áreas de melhoria de alto valor.
- Redução da quantidade de revisão necessária devido às descobertas da avaliação da segurança.
- Melhoria da percepção da função de segurança.

Nível de exposição a riscos se esta prática recomendada não for estabelecida: baixo

Orientações para a implementação

Comece com as orientações em SEC11-BP01 Treinar para segurança de aplicações. Depois, identifique o modelo operacional para o programa que você acredita ser o melhor para a sua organização. Os dois padrões principais são treinar os criadores ou incorporar o pessoal de segurança às equipes de criadores. Depois de decidir sobre a abordagem inicial, você precisa criar um piloto com uma equipe de workload ou um grupo pequeno de equipes de workload para comprovar que o modelo funciona para sua organização. O apoio de liderança dos criadores e da segurança da organização contribui para a entrega e o sucesso do programa. À medida que você criar esse programa, é importante selecionar as métricas que podem ser utilizadas para mostrar o valor dele. Saber como a AWS resolveu esse problema é uma boa experiência de aprendizado. A prática recomendada é muito concentrada na mudança e cultura organizacionais. As ferramentas que você utiliza devem ser compatíveis com a colaboração entre as comunidades de criadores e de segurança.

Etapas da implementação

- Começar com o treinamento dos criadores para segurança de aplicações.
- Criar uma comunidade e um programa de integração para instruir os criadores.

- Selecionar um nome para o programa. Guardiões, patrocinadores ou defensores são utilizados com frequência.
- Identificar o modelo a ser utilizado: treinar criadores, incorporar engenheiros de segurança e ter perfis de segurança de afinidade.
- Identificar patrocinadores do projeto em grupos de segurança e de criadores e possivelmente em outros grupos relevantes.
- Rastrear as métricas do número de pessoas envolvidas no programa, o tempo gasto em avaliações e o feedback dos criadores e do pessoal de segurança. Utilizar essas métricas para realizar melhorias.

Recursos

Práticas recomendadas relacionadas:

- SEC11-BP01 Treinar para segurança de aplicações
- SEC11-BP02 Automatizar o teste durante o ciclo de vida de desenvolvimento e lançamento

Documentos relacionados:

- Como abordar a modelagem de ameaças
- Como pensar sobre governança de segurança na nuvem

Vídeos relacionados:

- Segurança proativa: considerações e abordagens

Conclusão

A segurança é um esforço contínuo. Quando ocorrem incidentes, eles devem ser tratados como oportunidades de melhorar a segurança da arquitetura. Ter controles fortes de identidade, automatizar respostas a eventos de segurança, proteger a infraestrutura em vários níveis e usar criptografia para gerenciar dados bem classificados proporcionam a defesa profunda que todas as empresas devem implementar. Esse trabalho é facilitado graças às funções programáticas e aos recursos e serviços da AWS discutidos neste documento.

A AWS se esforça para ajudá-lo a criar e operar arquiteturas que protegem informações, sistemas e ativos, enquanto agregam valor de negócios.

Colaboradores

Os indivíduos e empresas a seguir contribuíram para este documento:

- Sarita Dharankar, líder do pilar Segurança do Well-Architected, Amazon Web Services
- Adam Cerini, arquiteto sênior de soluções, Amazon Web Services
- Bill Shinn, diretor sênior no escritório do CISO, Amazon Web Services
- Brigid Johnson, gerente sênior de desenvolvimento de software, AWS Identity, Amazon Web Services
- Byron Pogson, arquiteto sênior de soluções, Amazon Web Services
- Charlie Hammell, arquiteto-chefe empresarial, Amazon Web Services
- Darran Boyd, arquiteto principal de soluções de segurança, serviços financeiros, Amazon Web Services
- Dave Walker, arquiteto de soluções, segurança e conformidade, Amazon Web Services
- John Formento, arquiteto sênior de soluções, Amazon Web Services
- Paul Hawkins, diretor sênior no Escritório do CISO, Amazon Web Services
- Sam Elmalak, líder sênior de tecnologia, Amazon Web Services
- Pat Gaw, consultor de segurança sênior, Amazon Web Services
- Daniel Begimher, consultor sênior, segurança, Amazon Web Services
- Danny Cortegaca, arquiteto sênior de soluções de segurança, Amazon Web Services
- Ana Malhotra, arquiteta de soluções de segurança, Amazon Web Services
- Debashis Das, diretor sênior no Escritório do CISO, Amazon Web Services
- Reef Dsouza, arquiteto-chefe de soluções, Amazon Web Services
- Brad Burnett, arquiteto de soluções de segurança, Identity, Amazon Web Services
- Anna McAbee, arquiteta sênior de soluções de segurança, detecção de ameaças e resposta a incidentes, Amazon Web Services
- Jason Garman, arquiteto principal de soluções de segurança, Amazon Web Services

Leitura adicional

Para obter mais ajuda, consulte as seguintes fontes:

- Whitepaper do AWS Well-Architected Framework
- Centro de Arquitetura da AWS

Revisões do documento

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

Alteração	Descrição	Data
Orientação sobre práticas recomendadas atualizada	As práticas recomendadas foram atualizadas com novas orientações nas seguintes áreas: Operar as workloads com segurança e Proteger os dados em trânsito.	December 6, 2023
Orientação sobre práticas recomendadas atualizada	Principais atualizações nas orientações e nas práticas recomendadas na Resposta a incidentes. Várias práticas recomendadas atualizadas na Preparação. Duas novas áreas adicionad as à Resposta a incidente s: Operações e Atividades pós-incidente. Nova prática recomendada adicionada: SEC10-BP08 Estabeleça uma estrutura para aprender com os incidentes.	October 3, 2023
Orientação sobre práticas recomendadas atualizada	As práticas recomendadas foram atualizadas com novas orientações nas seguintes áreas: Preparar e Simular.	July 13, 2023
Atualizações para o novo Framework.	Práticas recomendadas atualizadas com orientações prescritivas e novas práticas	April 10, 2023

	recomendadas adicionadas. Nova área de práticas recomendadas de segurança de aplicações (AppSec) adicionada.	
Whitepaper atualizado	Práticas recomendadas atualizadas com novas orientações para implementação.	December 15, 2022
Whitepaper atualizado	Práticas recomendadas ampliadas e planos de melhoria adicionados.	October 20, 2022
Atualização secundária	Informações do IAM atualizadas para refletir as práticas recomendadas atuais.	June 28, 2022
Atualização secundária	Informações adicionais do AWS PrivateLink incluídas e links quebrados corrigidos.	May 19, 2022
Atualização secundária	AWS PrivateLink adicionado.	May 6, 2022
Atualização secundária	Remoção de linguagem não inclusiva.	April 22, 2022
Atualização secundária	Adicionadas informações sobre o Analisador de Acesso à Rede VPC.	February 2, 2022
Atualização secundária	Pilar Sustentabilidade adicionado à introdução.	December 2, 2021
Atualização secundária	Link quebrado corrigido.	May 27, 2021
Atualização secundária	Alterações editoriais de modo geral.	May 17, 2021

Atualização principal	Seção adicionada sobre governança, detalhes adicionados a várias seções, novos recursos e serviços adicionados.	May 7, 2021
Atualização secundária	Links atualizados.	March 10, 2021
Atualização secundária	Link quebrado corrigido.	July 15, 2020
Atualizações para a nova estrutura de trabalho	Orientações atualizadas sobre gerenciamento de contas, identidades e permissões.	July 8, 2020
Atualizações para a nova estrutura de trabalho	Atualizado para estender orientações a todas as áreas, novas práticas recomendadas, serviços e recursos.	April 30, 2020
Whitepaper atualizado	Atualizações para refletir novos serviços e recursos da AWS e referências atualizad as.	July 1, 2018
Whitepaper atualizado	Seção Configuração e manutenção da segurança do sistema atualizada para refletir os novos serviços e recursos da AWS.	May 1, 2017
Publicação inicial	Publicação do “Pilar Segurança: AWS Well-Arch itected Framework”.	November 1, 2016

Avisos

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