Construindo um programa escalável de gerenciamento de vulnerabilidades em AWS

AWS Orientação prescritiva

AWS Orientação prescritiva: Construindo um programa escalável de gerenciamento de vulnerabilidades em AWS

Table of Contents

Construindo um programa escalável de gerenciamento de vulnerabilidades em AWS

Anna McAbee e Megan O'Neil, Amazon Web Services ()AWS

Outubro de 2023 (histórico do documento)

Dependendo da tecnologia subjacente que você está usando, uma variedade de ferramentas e verificações podem gerar descobertas de segurança em um ambiente de nuvem. Sem processos implementados para lidar com essas descobertas, elas podem começar a se acumular, muitas vezes levando a milhares a dezenas de milhares de descobertas em um curto espaço de tempo. No entanto, com um programa estruturado de gerenciamento de vulnerabilidades e a operacionalização adequada de suas ferramentas, sua organização pode lidar e fazer a triagem de um grande número de descobertas de diversas fontes.

O gerenciamento de vulnerabilidades se concentra em descobrir, priorizar, avaliar, remediar e relatar vulnerabilidades. O gerenciamento de patches, por outro lado, se concentra em corrigir ou atualizar o software para remover ou remediar vulnerabilidades de segurança. O gerenciamento de patches é apenas um aspecto do gerenciamento de vulnerabilidades. Geralmente, recomendamos estabelecer um patch-in-place processo (também conhecido como mitigate-in-placeprocesso) para lidar com cenários críticos, que já estão corretos, e um processo padrão que você execute regularmente para liberar Amazon Machine Images (AMIs), contêineres ou pacotes de software corrigidos. Esses processos ajudam a preparar sua organização para responder rapidamente a uma vulnerabilidade de dia zero. Para sistemas críticos em um ambiente de produção, usar um patch-in-place processo pode ser mais rápido e confiável do que implantar uma nova AMI em toda a frota. Para patches programados regularmente, como patches de sistema operacional (SO) e software, recomendamos que você crie e teste usando processos de desenvolvimento padrão, como faria com qualquer alteração no nível do software. Isso proporciona melhor estabilidade para os modos operacionais padrão. Você pode usar o Patch Manager, um recurso ou outros produtos de terceiros como patch-in-place soluções. AWS Systems Manager Para obter mais informações sobre como usar o Patch Manager, consulte Gerenciamento de patches no AWS Cloud Adoption Framework: Operations Perspective. Além disso, você pode usar o EC2 Image Builder para automatizar a criação, o gerenciamento e a implantação de imagens personalizadas up-to-date e de servidor.

A criação de um programa escalável de gerenciamento de vulnerabilidades AWS envolve o gerenciamento de vulnerabilidades tradicionais de software e rede, além dos riscos de configuração da nuvem. Um risco de configuração na nuvem, como um bucket não criptografado do Amazon

Simple Storage Service (Amazon S3), deve seguir um processo de triagem e remediação semelhante ao de uma vulnerabilidade de software. Em ambos os casos, a equipe de aplicativos deve possuir e ser responsável pela segurança de seu aplicativo, incluindo a infraestrutura subjacente. Essa distribuição de propriedade é fundamental para um programa de gerenciamento de vulnerabilidades eficaz e escalável.

Este guia discute como simplificar a identificação e a correção de vulnerabilidades para reduzir o risco geral. Use as seções a seguir para criar e iterar seu programa de gerenciamento de vulnerabilidades:

1. Prepare-se — prepare seu pessoal, seus processos e sua tecnologia para identificar, avaliar e corrigir vulnerabilidades em seu ambiente.
2. Triagem e correção — encaminhe as descobertas de segurança para as partes interessadas relevantes, identifique a ação de remediação apropriada e, em seguida, execute a ação de remediação.
3. Relate e melhore — Use mecanismos de geração de relatórios para identificar oportunidades de melhoria e, em seguida, repita seu programa de gerenciamento de vulnerabilidades.

A criação de um programa de gerenciamento de vulnerabilidades na nuvem geralmente envolve iteração. Priorize as recomendações deste guia e revise regularmente sua lista de pendências para se manter atualizado com as mudanças tecnológicas e os requisitos de seus negócios.

Público-alvo

Este guia é destinado a grandes empresas que têm três equipes principais responsáveis pelas descobertas relacionadas à segurança: uma equipe de segurança, uma equipe do Cloud Center of Excellence (CCoE) ou equipe de nuvem e equipes de aplicativos (ou desenvolvedores). Este guia usa os modelos operacionais corporativos mais comuns e se baseia nesses modelos operacionais para permitir uma resposta mais eficiente às descobertas de segurança e melhorar os resultados de segurança. As organizações que usam AWS podem ter estruturas e modelos operacionais diferentes; no entanto, você pode modificar muitos dos conceitos deste guia para se adequar a diferentes modelos operacionais e organizações menores.

Objetivos

Este guia pode ajudar você e sua organização a:

- Desenvolva políticas para simplificar o gerenciamento de vulnerabilidades e garantir a responsabilidade
- Estabeleça mecanismos para distribuir a responsabilidade pela segurança às equipes de aplicativos
- Configure as informações relevantes de Serviços da AWS acordo com as melhores práticas para gerenciamento escalável de vulnerabilidades
- Distribua a propriedade das descobertas de segurança
- Estabeleça mecanismos para relatar e iterar seu programa de gerenciamento de vulnerabilidades
- Melhore a visibilidade das descobertas de segurança e melhore a postura geral de segurança

Prepare seu programa escalável de gerenciamento de vulnerabilidades

A preparação para criar um programa escalável de gerenciamento de vulnerabilidades envolve educar as pessoas, desenvolver processos e implementar a tecnologia adequada de acordo com as melhores práticas. Pessoas, processos e tecnologia são igualmente importantes para um programa eficaz de gerenciamento de vulnerabilidades, e você deve integrá-los totalmente para gerenciar vulnerabilidades em grande escala.

Esta seção do guia analisa as ações fundamentais que você pode tomar para preparar seu programa escalável de gerenciamento de vulnerabilidades. AWS

Tópicos

Defina um plano de gerenciamento de vulnerabilidades

A primeira etapa ao preparar seu programa de gerenciamento de vulnerabilidades na nuvem é definir seu plano de gerenciamento de vulnerabilidades. Esse plano inclui as políticas e os processos que sua organização segue. Esse plano deve ser documentado e acessível a todas as partes interessadas. Um plano de gerenciamento de vulnerabilidades é um documento de alto nível que normalmente inclui as seguintes seções:

- Metas e escopo — descreva as metas, as funções e o escopo do gerenciamento de vulnerabilidades.
- Funções e responsabilidades — Liste as partes interessadas no gerenciamento de vulnerabilidades e detalhe suas responsabilidades.

- Definições de gravidade e priorização da vulnerabilidade — determine como classificar a gravidade de uma vulnerabilidade e como priorizá-la.
- Acordos de nível de serviço (SLAs) para remediação — Para cada nível de gravidade, defina a quantidade máxima de tempo que o proprietário da remediação tem para resolver uma descoberta de segurança. Como a conformidade com o SLA é parte integrante de um programa de gerenciamento de vulnerabilidades eficaz e escalável, considere como monitorar se você está cumprindo esses SLAs.
- Processo de exceção — detalhe o processo de envio, aprovação e atualização de exceções. Esse processo deve garantir que as exceções sejam legítimas, com limite de tempo e rastreadas.
- Fontes de informações sobre vulnerabilidades — Liste as fontes ou ferramentas que geram descobertas de segurança. Para obter mais informações sobre Serviços da AWS essas fontes de descobertas de segurança, consulte Configurar serviços AWS de segurança este guia.

Embora essas seções sejam comuns em empresas de diferentes tamanhos e setores, o plano de gerenciamento de vulnerabilidades de cada organização é único. Você precisa criar um plano de gerenciamento de vulnerabilidades que funcione melhor para sua organização. Espere iterar seu plano ao longo do tempo para incorporar as lições aprendidas e as tecnologias em evolução.

Distribua a propriedade da segurança

O modelo de responsabilidade AWS compartilhada define como AWS seus clientes compartilham a responsabilidade pela segurança e conformidade na nuvem. Nesse modelo, AWS protege a infraestrutura que executa todos os serviços oferecidos no Nuvem AWS, e AWS os clientes são responsáveis por proteger seus dados e aplicativos.

Você pode espelhar esse modelo em sua organização e distribuir as responsabilidades entre suas equipes de nuvem e aplicativos. Isso ajuda você a escalar seus programas de segurança na nuvem com mais eficiência, pois as equipes de aplicativos se apropriam de certos aspectos de segurança de seus aplicativos. A interpretação mais simples do modelo de responsabilidade compartilhada é que, se você tiver acesso para configurar o recurso, será responsável pela segurança desse recurso.

Uma parte fundamental da distribuição de responsabilidades de segurança às equipes de aplicativos é criar ferramentas de segurança de autoatendimento que ajudem suas equipes de aplicativos a se automatizarem. Inicialmente, isso pode ser um esforço conjunto. A equipe de segurança pode traduzir os requisitos de segurança em ferramentas de verificação de código e, em seguida, as equipes de aplicativos podem usar essas ferramentas para criar e compartilhar soluções com sua

comunidade interna de desenvolvedores. Isso contribui para uma maior eficiência em outras equipes que precisam atender a requisitos de segurança semelhantes.

A tabela a seguir descreve as etapas para distribuir a propriedade às equipes de aplicativos e fornece exemplos.

Etapa	Ação	Exemplo
1	Defina seus requisitos de segurança — O que você está tentando alcançar? Isso pode vir de um padrão de segurança ou de um requisito de conformidade.	Um exemplo de requisito de segurança é o acesso com privilégios mínimos para identidades de aplicativos.
2	Enumerar controles para um requisito de segurança — O que esse requisito realmente significa do ponto de vista do controle? O que eu preciso fazer para conseguir isso?	Para obter o menor privilégio para identidades de aplicativos, a seguir estão dois exemplos de controles: • Use funções AWS Identity and Access Management (IAM) • Não use curingas nas políticas do IAM
3	Orientações de documentos para os controles — Com esses controles, que orientação você pode fornecer a um desenvolvedor para ajudá-lo a cumprir o controle?	Inicialmente, você pode começar documentando exemplos de políticas simples, incluindo políticas de IAM seguras e não seguras e políticas de bucket do Amazon Simple Storage Service (Amazon S3). Em seguida, você pode incorporar soluções de análise de políticas em pipelines de integração

Etapa	Ação	Exemplo
		contínua e entrega contínua (CI/CD), como o uso de regras para avaliação proativa.AWS Config
4	Desenvolva artefatos reutilizáveis — Com a orientação, você pode facilitar ainda mais as coisas e desenvolver artefatos reutilizáveis para desenvolvedores?	Você pode criar infraestrutura como código (IaC) para implantar políticas do IAM que sigam o princípio do menor privilégio. Você pode armazenar esses artefatos reutilizáveis em um repositório de código.

O autoatendimento pode não funcionar para todos os requisitos de segurança, mas pode funcionar para cenários padrão. Ao seguir essas etapas, as organizações podem capacitar suas equipes de aplicativos para lidar com mais responsabilidades de segurança de forma escalável. No geral, o modelo de responsabilidade distribuída leva a práticas de segurança mais colaborativas em muitas organizações.

Desenvolva um programa de divulgação de vulnerabilidades

Para uma defense-in-depthabordagem ao gerenciamento de vulnerabilidades, crie um programa de divulgação de vulnerabilidades para que pessoas dentro ou fora da sua organização possam relatar vulnerabilidades ou riscos de segurança.

Para as pessoas da sua organização, estabeleça um processo para apresentar riscos ou vulnerabilidades. Isso pode ser feito por meio de um sistema de bilhetagem ou e-mail. Independentemente do processo escolhido, é essencial que seus funcionários estejam cientes do processo e possam facilmente apresentar quaisquer vulnerabilidades ou riscos que encontrarem.

Para pessoas fora da sua organização, estabeleça uma página da Web externa para enviar possíveis vulnerabilidades de segurança. Como exemplo, consulte a página do Relatório de AWS Vulnerabilidades. Essa página da web também deve conter diretrizes de divulgação para ajudar a proteger os dados e ativos da sua organização. Um programa de divulgação de vulnerabilidades

não deve incentivar atividades potencialmente prejudiciais, por isso é essencial que você tenha uma política clara com diretrizes. Criar um programa de divulgação maduro e responsável é uma meta a ser alcançada à medida que você amadurece seu programa. A maioria não começa com um programa externo de divulgação e leva tempo para acertar.

Prepare seu AWS ambiente

Antes de implementar qualquer ferramenta de gerenciamento de vulnerabilidades, certifique-se de que seu AWS ambiente seja arquitetado para suportar um programa escalável de gerenciamento de vulnerabilidades. A estrutura das políticas de marcação de sua empresa Contas da AWS e da sua organização pode simplificar o processo de criação de um programa escalável de gerenciamento de vulnerabilidades.

Desenvolva uma Conta da AWS estrutura

AWS Organizationsajuda a gerenciar e governar centralmente um AWS ambiente à medida que sua empresa cresce e expande seus AWS recursos. Uma organização AWS Organizations consolida você Contas da AWS em grupos lógicos, ou unidades organizacionais, para que você possa administrá-los como uma única unidade. Você AWS Organizations gerencia a partir de uma conta dedicada, chamada de conta de gerenciamento. Para obter mais informações, consulte Terminologia e conceitos do AWS Organizations.

Recomendamos que você gerencie seu ambiente AWS de várias contas em AWS Organizations. Isso ajuda a criar um inventário completo das contas e recursos da sua empresa. Esse inventário completo de ativos é um aspecto essencial do gerenciamento de vulnerabilidades. As equipes de aplicativos não devem usar contas que estejam fora da organização.

AWS Control Towerajuda você a configurar e administrar um ambiente AWS com várias contas, seguindo as melhores práticas prescritivas. Se você ainda não estabeleceu um ambiente com várias contas, AWS Control Tower é um bom ponto de partida.

Recomendamos usar a estrutura de conta dedicada e as melhores práticas descritas na Arquitetura AWS de Referência de Segurança (AWS SRA). A conta do Security Tooling deve servir como administrador delegado para seus serviços de segurança. Mais informações sobre como configurar suas ferramentas de gerenciamento de vulnerabilidades nessa conta serão fornecidas posteriormente neste guia. Hospede aplicativos em contas dedicadas na unidade organizacional de cargas de trabalho (OU). Isso estabelece um forte isolamento no nível da carga de trabalho e limites

de segurança explícitos para cada aplicativo. Para obter informações sobre os princípios de design e os benefícios do uso de uma abordagem de várias contas, consulte Organizando seu AWS ambiente usando várias contas (AWS whitepaper).

Ter uma estrutura de contas intencional e gerenciar centralmente os serviços de segurança a partir de uma conta dedicada são aspectos essenciais de um programa escalável de gerenciamento de vulnerabilidades.

Defina, implemente e aplique tags

As tags são pares de valores-chave que atuam como metadados para organizar seus recursos. AWS Para obter mais informações, consulte Marcar seus recursos do AWS. Você pode usar tags para fornecer contexto comercial, como unidade de negócios, proprietário do aplicativo, ambiente e centro de custos. A tabela a seguir mostra um conjunto de exemplos de tags.

Chave	Valor
BusinessUnit	HumanResources
CostCenter	CC101
ApplicationTeam	HumanResourcesTechnology
Ambiente	Produção

As tags podem ajudar você a priorizar as descobertas. Por exemplo, ele pode ajudar você a:

- Identifique o proprietário de um recurso responsável por corrigir uma vulnerabilidade
- Acompanhe quais aplicativos ou unidades de negócios têm um grande número de descobertas
- Aumente a severidade das descobertas para determinadas classificações de dados, como informações de identificação pessoal (PII) ou dados do setor de cartões de pagamento (PCI)
- Identifique o tipo de dados no ambiente, como dados de teste em um ambiente de desenvolvimento de nível inferior ou dados de produção

Para ajudar você a obter uma marcação eficaz em grande escala, siga as instruções em Como criar sua estratégia de marcação em Best Practices for Tagging AWS Resources (AWS whitepaper).

Monitore boletins AWS de segurança

É altamente recomendável monitorar os boletins de AWS segurança de forma regular e frequente. Os boletins de segurança podem notificá-lo sobre novas vulnerabilidades relacionadas à segurança, serviços afetados e atualizações aplicáveis. Você também pode assinar um feed RSS para os boletins de segurança e criar um processo para ingerir e tratar esses boletins como parte do seu programa de gerenciamento de vulnerabilidades.

Configurar serviços AWS de segurança

AWS oferece uma variedade de serviços de segurança projetados para ajudar a proteger seu AWS ambiente. Para seu programa de gerenciamento de vulnerabilidades, recomendamos que você habilite o seguinte Serviços da AWS em cada conta:

- GuardDutyA Amazon ajuda a detectar ameaças ativas em seu ambiente. Uma GuardDuty descoberta pode ajudá-lo a identificar uma vulnerabilidade desconhecida que foi explorada em seu ambiente. Também pode ajudar você a entender os efeitos de uma vulnerabilidade não corrigida.
- AWS Healthfornece visibilidade contínua do desempenho de seus recursos e da disponibilidade de suas Serviços da AWS contas.
- AWS Identity and Access Management Access Analyzeranalisa as políticas baseadas em recursos em seu AWS ambiente para identificar recursos que são compartilhados com uma entidade externa. Isso pode ajudá-lo a identificar vulnerabilidades associadas ao acesso não intencional aos seus recursos e dados. Para cada instância de um recurso compartilhado fora de sua conta, o IAM Access Analyzer gera uma descoberta.
- O Amazon Inspector é um serviço de gerenciamento de vulnerabilidades que verifica continuamente suas AWS cargas de trabalho em busca de vulnerabilidades de software e exposição não intencional na rede.
- AWS Security Hubajuda você a verificar seu AWS ambiente em relação aos padrões do setor de segurança e pode identificar riscos de configuração na nuvem. Ele também fornece uma visão abrangente do seu estado de AWS segurança ao agregar descobertas de outros serviços de AWS segurança e ferramentas de segurança de terceiros.

Esta seção discute como habilitar e configurar o Amazon Inspector e o Security Hub para ajudá-lo a estabelecer um programa escalável de gerenciamento de vulnerabilidades.

Usando o Amazon Inspector em seu programa de gerenciamento de vulnerabilidades

O Amazon Inspector é um serviço de gerenciamento de vulnerabilidades que verifica continuamente suas instâncias do Amazon Elastic Compute Cloud (Amazon EC2), imagens de contêineres do Amazon Elastic Container Registry (Amazon ECR) e funções em busca de vulnerabilidades de software e exposição não intencional na rede. AWS Lambda Você pode usar o Amazon Inspector para obter visibilidade e priorizar a resolução de vulnerabilidades de software em seus ambientes. AWS

O Amazon Inspector avalia continuamente seu ambiente durante todo o ciclo de vida de seus recursos. Ele verifica automaticamente os recursos em resposta às mudanças que podem introduzir uma nova vulnerabilidade. Por exemplo, ele verifica novamente quando você instala um novo pacote em uma instância do EC2, quando você instala um patch ou quando uma nova vulnerabilidade e exposição comum (CVE) que afeta o recurso é publicada. Quando o Amazon Inspector identifica uma vulnerabilidade ou um caminho de rede aberto, ele produz uma descoberta que você pode investigar. A descoberta fornece informações abrangentes sobre a vulnerabilidade, incluindo o seguinte:

- Pontuação de risco do Amazon Inspector
- Pontuação do Common Vulnerability Scoring System (CVSS)
- Recurso afetado
- Dados de inteligência de vulnerabilidade sobre o CVE da Amazon, Recorded Future, e Cybersecurity and Infrastructure Security Agency (CISA)
- Recomendações de remediação

Para obter instruções sobre como configurar o Amazon Inspector, consulte Introdução ao Amazon Inspector. A etapa Ativar o Amazon Inspector neste tutorial fornece duas opções de configuração: um ambiente de conta independente e um ambiente de várias contas. Recomendamos usar a opção de ambiente de várias contas se você quiser monitorar várias pessoas Contas da AWS que são membros de uma organização em AWS Organizations.

Quando você configura o Amazon Inspector para um ambiente de várias contas, você designa uma conta na organização para ser o administrador delegado do Amazon Inspector. O administrador delegado pode gerenciar as descobertas e algumas configurações dos membros da organização. Por exemplo, o administrador delegado pode visualizar os detalhes das descobertas agregadas de

todas as contas dos membros, ativar ou desativar as verificações das contas dos membros e revisar os recursos escaneados. A AWS SRA recomenda que você crie uma conta do Security Tooling e a use como administrador delegado do Amazon Inspector.

Usando AWS Security Hub em seu programa de gerenciamento de vulnerabilidades

A criação de um programa escalável de gerenciamento de vulnerabilidades AWS envolve o gerenciamento de vulnerabilidades tradicionais de software e rede, além dos riscos de configuração da nuvem. AWS Security Hubajuda você a verificar seu AWS ambiente em relação aos padrões do setor de segurança e pode identificar riscos de configuração na nuvem. O Security Hub também fornece uma visão abrangente do seu estado de segurança AWS ao agregar descobertas de segurança de outros serviços de AWS segurança e ferramentas de segurança de terceiros.

Nas seções a seguir, fornecemos as melhores práticas e recomendações para configurar o Security Hub para dar suporte ao seu programa de gerenciamento de vulnerabilidades:

- Configurar o Security Hub
- Habilitando os padrões do Security Hub
- Gerenciando as descobertas do Security Hub
- Agregando descobertas de outros serviços e ferramentas de segurança

Configurar o Security Hub

Para obter instruções de configuração, consulte Configuração AWS Security Hub. Para usar o Security Hub, você deve habilitar AWS Config. Para obter mais informações, consulte Habilitando e configurando AWS Config na documentação do Security Hub.

Se você estiver integrado com AWS Organizations, a partir da conta de gerenciamento da organização, você designa uma conta para ser o administrador delegado do Security Hub. Para obter instruções, consulte Designação do administrador delegado do Security Hub. O AWS SRA recomenda que você crie uma conta do Security Tooling e a use como administrador delegado do Security Hub.

O administrador delegado tem acesso automático para configurar o Security Hub para todas as contas dos membros na organização e para visualizar as descobertas associadas a essas contas. Recomendamos que você habilite o AWS Config Security Hub em todos Regiões da AWS os

seus Contas da AWS. Você pode configurar o Security Hub para tratar automaticamente as novas contas da organização como contas de membros do Security Hub. Para obter instruções, consulte Gerenciamento de contas de membros que pertencem a uma organização.

Habilitando os padrões do Security Hub

O Security Hub gera descobertas executando verificações de segurança automatizadas e contínuas em relação aos controles de segurança. Os controles estão associados a um ou mais padrões de segurança. Os controles ajudam a determinar se os requisitos de um padrão estão sendo atendidos.

Quando você habilita um padrão no Security Hub, o Security Hub ativa automaticamente os controles que se aplicam ao padrão. O Security Hub usa AWS Config regras para realizar a maioria das verificações de segurança dos controles. Você pode ativar ou desativar os padrões do Security Hub a qualquer momento. Para obter mais informações, consulte Controles e padrões de segurança em AWS Security Hub. Para obter uma lista completa de padrões, consulte a referência de padrões do Security Hub.

Se sua organização ainda não tiver um padrão de segurança preferencial, recomendamos usar o padrão AWS Foundational Security Best Practices (FSBP). Esse padrão foi projetado para detectar quando Contas da AWS um recurso se desvia das melhores práticas de segurança. AWS organiza esse padrão e o atualiza regularmente para abranger novos recursos e serviços. Depois de fazer a triagem das descobertas do FSBP, considere habilitar outros padrões.

Gerenciando as descobertas do Security Hub

O Security Hub fornece vários recursos que ajudam você a lidar com grandes volumes de descobertas de toda a organização e a entender o estado de segurança do seu AWS ambiente. Para ajudá-lo a gerenciar as descobertas, recomendamos habilitar os dois recursos do Security Hub a seguir:

- Use a agregação entre regiões para agregar descobertas, encontrar atualizações, insights, controlar status de conformidade e pontuações de segurança de várias regiões Regiões da AWS para uma única região de agregação.
- Use descobertas de controle consolidadas para reduzir o ruído de descoberta removendo descobertas duplicadas. Quando as descobertas de controle consolidadas são ativadas em sua conta, o Security Hub gera uma única nova descoberta ou atualização de descoberta para cada verificação de segurança de um controle, mesmo que um controle se aplique a vários padrões habilitados.

Agregando descobertas de outros serviços e ferramentas de segurança

Além de gerar descobertas de segurança, você pode usar o Security Hub para agregar dados de localização de várias soluções Serviços da AWS de segurança de terceiros compatíveis. Esta seção se concentra em enviar descobertas de segurança para o Security Hub. A próxima seção,Prepare-se para atribuir descobertas de segurança, discute como você pode integrar o Security Hub com produtos que podem receber descobertas do Security Hub.

Há muitos produtos Serviços da AWS de terceiros e soluções de código aberto disponíveis que você pode integrar ao Security Hub. Se você está apenas começando, recomendamos fazer o seguinte:

1. Habilitar a integração Serviços da AWS— A maioria das Serviço da AWS integrações que enviam descobertas para o Security Hub é ativada automaticamente depois que você ativa o Security Hub e o serviço integrado. Para o seu programa de gerenciamento de vulnerabilidades, recomendamos habilitar o Amazon Inspector GuardDuty AWS Health, o Amazon e o IAM Access Analyzer em cada conta. Esses serviços enviam automaticamente suas descobertas para o Security Hub. Para obter uma lista completa das Serviço da AWS integrações suportadas, consulte Serviços da AWS a seção Enviar descobertas para o Security Hub.

   > **Note**
   >
   > AWS Health envia as descobertas para o Security Hub se uma das seguintes condições for atendida:
   >
   > - A descoberta está associada a um serviço AWS de segurança
   > - O código de tipo de descoberta contém as palavras`security`,`abuse`, ou `certificate`
   > - O AWS Health serviço de busca é `risk` ou `abuse`

2. Configurar integrações de terceiros — Para obter uma lista das integrações atualmente suportadas, consulte Integrações de produtos de parceiros terceirizados disponíveis. Selecione qualquer ferramenta adicional que possa enviar ou receber descobertas do Security Hub. Talvez você já tenha algumas dessas ferramentas de terceiros. Siga as instruções do produto para configurar a integração com o Security Hub.

Prepare-se para atribuir descobertas de segurança

Nesta seção, você configura as ferramentas que suas equipes usam para gerenciar e atribuir descobertas de segurança. Esta seção inclui as seguintes opções:

- Gerencie descobertas em ferramentas e fluxos de trabalho existentes— Essa opção se integra AWS Security Hub aos sistemas existentes que suas equipes usam para gerenciar suas tarefas diárias, como um backlog de produtos. Essa opção é recomendada para equipes que estabeleceram ferramentas para gerenciar seus fluxos de trabalho.
- Gerencie descobertas no Security Hub— Essa opção configura notificações para eventos do Security Hub para que a equipe apropriada receba um alerta e possa abordar a descoberta no Security Hub.

Decida qual fluxo de trabalho funcionaria melhor para suas equipes e garanta que as descobertas de segurança cheguem prontamente aos respectivos proprietários.

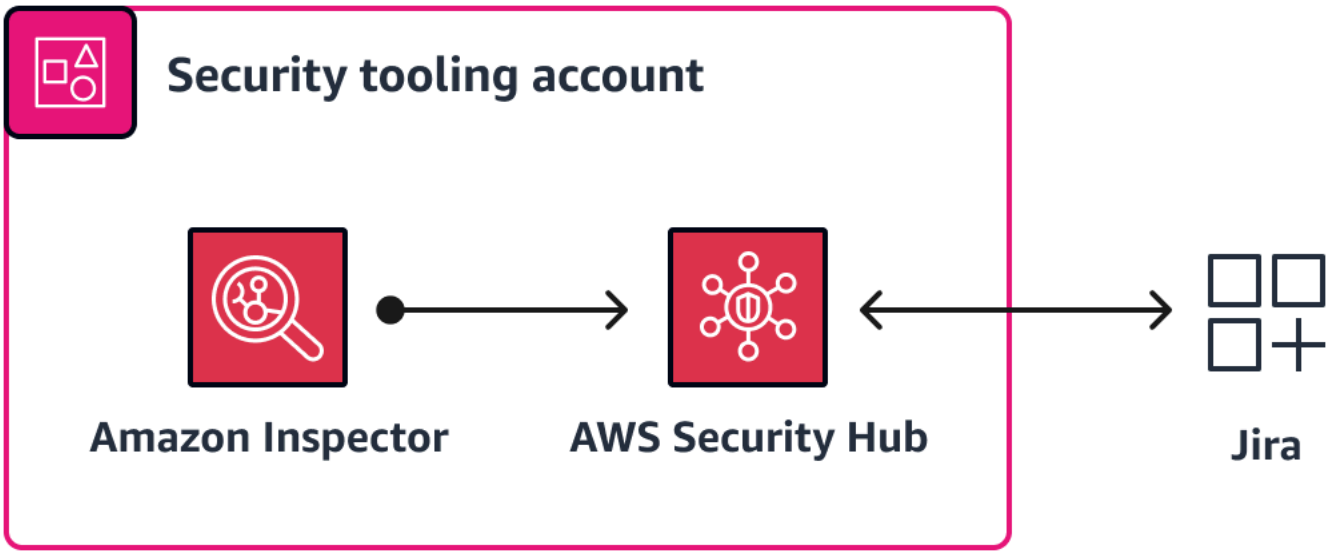
Gerencie descobertas em ferramentas e fluxos de trabalho existentes

Recomendamos integrações adicionais do Security Hub para organizações corporativas que estabeleceram ferramentas que as equipes usam para gerenciar ou realizar suas tarefas diárias. Você pode importar dados de localização do Security Hub em várias plataformas de tecnologia. Os exemplos incluem:

- Os sistemas de gerenciamento de informações e eventos de segurança (SIEM) ajudam as equipes de segurança a fazer a triagem de eventos de segurança operacional. Os sistemas SIEM fornecem análise em tempo real dos alertas de segurança gerados por aplicativos e hardware de rede.
- Os sistemas de governança, risco e conformidade (GRC) ajudam as equipes de conformidade e governança a monitorar e relatar dados de gerenciamento de riscos. As ferramentas GRC são aplicativos de software que as empresas podem usar para gerenciar políticas, avaliar riscos, controlar o acesso dos usuários e otimizar a conformidade. Você pode usar ferramentas de GRC para integrar processos de negócios, reduzir custos e melhorar a eficiência.
- Os sistemas de backlog e emissão de tíquetes de produtos ajudam as equipes de aplicativos e nuvem a gerenciar recursos e priorizar as tarefas de desenvolvimento. Atlassian Jirae Microsoft Azure DevOpssão exemplos desses sistemas.

Integrar as descobertas do Security Hub diretamente com esses sistemas corporativos existentes pode melhorar o tempo médio de recuperação (MTTR) e os resultados de segurança, pois o fluxo de trabalho operacional diário não precisa mudar. As equipes podem responder e aprender com as descobertas de segurança com muito mais rapidez porque não precisam usar ferramentas e fluxos de trabalho separados. A integração faz com que abordar as descobertas de segurança faça parte do fluxo de trabalho normal e padrão.

O Security Hub se integra a vários produtos de parceiros terceirizados. Para obter uma lista completa e instruções, consulte Integrações de produtos de parceiros terceirizados disponíveis na documentação do Security Hub. As integrações comuns incluem Atlassian - Jira Service Managementintegração bidirecional AWS Security Hub com Jira software e. ServiceNow – ITSM O diagrama a seguir mostra como você pode configurar o Amazon Inspector para enviar descobertas para o Security Hub e, em seguida, configurar o Security Hub para enviar todas as descobertas. Jira



Gerencie descobertas no Security Hub

Você pode criar um sistema de notificação baseado em nuvem para as descobertas do Security Hub usando EventBridge as regras da Amazon e os tópicos do Amazon Simple Notification Service (Amazon SNS). Esse sistema notifica a equipe apropriada sobre uma descoberta quando ela é criada. Para essa abordagem, a estratégia de várias contas descrita em Desenvolva uma Conta da AWS estrutura é fundamental porque os aplicativos são separados em contas dedicadas. Isso ajuda você a notificar as equipes corretas para cada descoberta.

As equipes de segurança ou de nuvem podem optar por receber eventos de todos Contas da AWS. Nesse caso, crie uma EventBridge regra na conta de administrador delegado do Security Hub e assine um tópico do Amazon SNS que notifique essas equipes. Para equipes de aplicativos, configure uma EventBridge regra e um tópico do SNS em suas respectivas contas de aplicativos. Quando uma descoberta do Security Hub ocorre em uma conta de aplicativo, a equipe responsável é notificada sobre a descoberta.

O Security Hub já envia automaticamente todas as novas descobertas e todas as atualizações das descobertas existentes EventBridge como eventos importados do Security Hub Findings. Cada evento Security Hub Findings - Imported contém uma única descoberta. Você pode aplicar filtros nas EventBridge regras para que uma descoberta inicie a regra somente se a descoberta corresponder aos filtros. Para obter instruções, consulte Configuração de uma EventBridge regra para descobertas enviadas automaticamente. Para obter mais informações sobre como criar e assinar tópicos do Amazon SNS, consulte Configurando o Amazon SNS.

Considere o seguinte ao usar essa abordagem:

- Para equipes de aplicativos, crie EventBridge regras dentro de cada uma Conta da AWS e Região da AWS onde o aplicativo está hospedado.
- Para equipes de segurança e nuvem, crie EventBridge regras na conta de administrador delegado do Security Hub. Isso notifica as equipes sobre todas as descobertas nas contas dos membros.
- O Amazon SNS envia uma notificação todos os dias se o status da descoberta de segurança for. `NEW` Se quiser desativar as notificações diárias, você pode criar uma AWS Lambda função personalizada que altera o status da descoberta de `NEW` para `NOTIFIED` após o assinante do Amazon SNS receber a notificação.

Faça a triagem e corrija as descobertas de segurança em seu ambiente AWS

A triagem de uma descoberta de segurança envolve encaminhar a descoberta para a parte interessada apropriada, avaliar e priorizar a descoberta e, em seguida, corrigi-la. Esta seção analisa cada uma dessas etapas em detalhes e fornece recomendações para escalabilidade e eficiência. Também inclui exemplos para ajudar a ilustrar o processo de triagem e remediação.

Tópicos

Defina a propriedade das descobertas de segurança

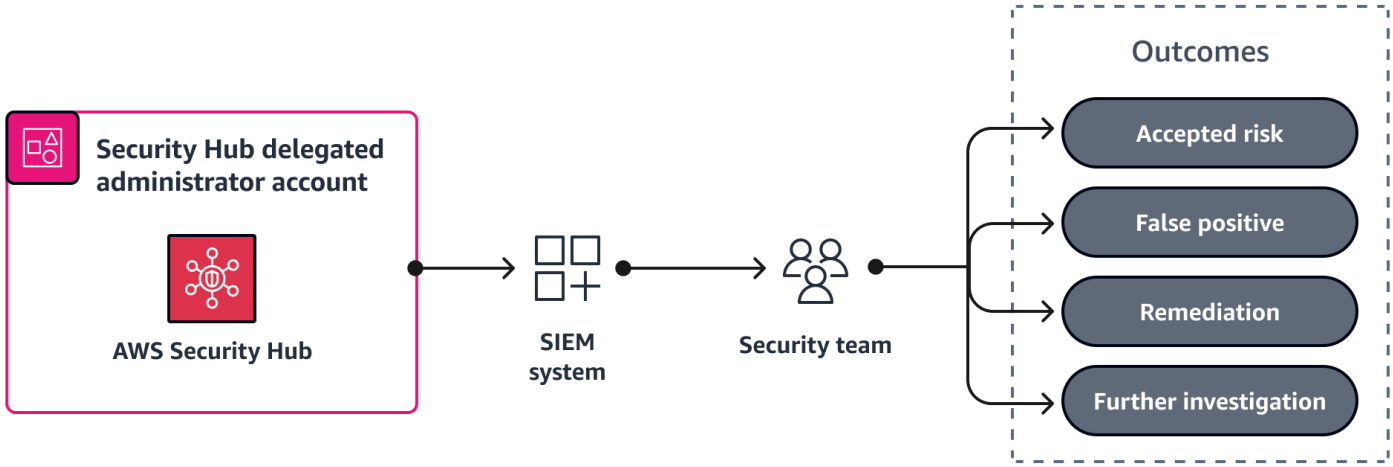
Definir um modelo de propriedade para fazer a triagem das descobertas de segurança pode ser um desafio, mas não precisa ser. O cenário de segurança muda constantemente, e os profissionais devem ser flexíveis para se adaptar a essas mudanças. Adote uma abordagem flexível para desenvolver seu modelo de propriedade para descobertas de segurança. Seu modelo inicial deve permitir que suas equipes ajam imediatamente. Recomendamos começar com a lógica básica de propriedade e refinar essa lógica ao longo do tempo. Se você demorar para definir os critérios de propriedade perfeitos, o número de descobertas de segurança continuará crescendo.

Para facilitar a atribuição das descobertas às equipes e recursos apropriados, recomendamos a integração AWS Security Hub com qualquer sistema existente que suas equipes usem para gerenciar suas tarefas diárias. Por exemplo, você pode integrar o Security Hub com sistemas de gerenciamento de eventos e informações de segurança (SIEM) ou sistemas de backlog e emissão de bilhetes de produtos. Para obter mais informações, consulte Prepare-se para atribuir descobertas de segurança neste guia.

Veja a seguir um exemplo de um modelo de propriedade que você pode usar como ponto de partida:

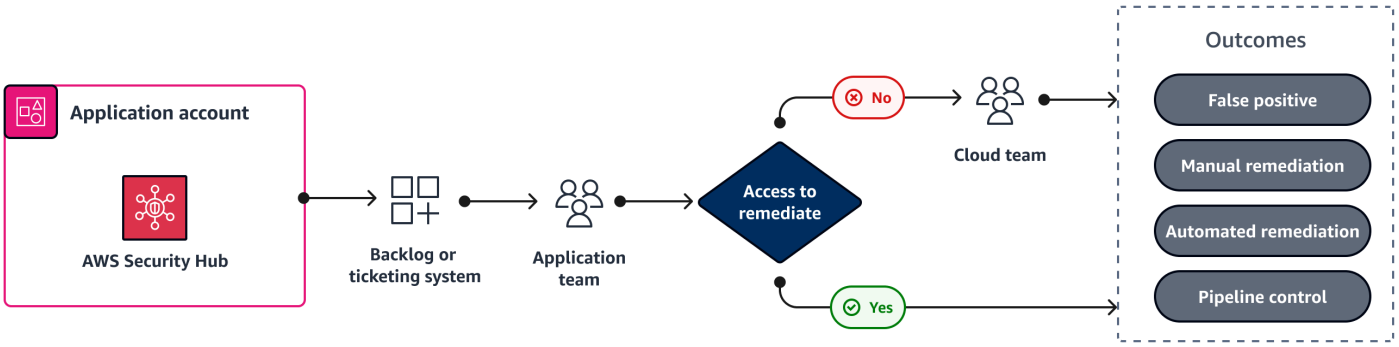
- A equipe de segurança analisa ameaças potencialmente ativas e ajuda a avaliar e priorizar as descobertas de segurança. A equipe de segurança tem a experiência e as ferramentas para

avaliar adequadamente o contexto. Eles entendem os dados adicionais relacionados à segurança que os ajudam a avaliar e priorizar vulnerabilidades e investigar eventos de detecção de ameaças. Se for necessário encontrar severidade ou ajuste adicional, consulte a Avalie e priorize as descobertas de segurança seção deste guia. Veja um exemplo Exemplo de equipe de segurança neste guia.



- Distribua as descobertas de segurança entre as equipes de nuvem e de aplicativos — Conforme discutido na Distribua a propriedade da segurança seção, a equipe que tem acesso para configurar o recurso é responsável por sua configuração segura. As equipes de aplicativos são responsáveis pelas descobertas de segurança relacionadas aos recursos que elas criam e configuram, e a equipe de nuvem é responsável pelas descobertas de segurança relacionadas às configurações de amplo alcance. Na maioria dos casos, as equipes de aplicativos não têm acesso para alterar configurações abrangentes Serviços da AWS, como políticas de controle de serviços (SCPs) AWS Control Tower, configurações de VPC AWS Organizations relacionadas à rede e o IAM Identity Center.AWS

  Para ambientes com várias contas que separam aplicativos em contas dedicadas, geralmente é possível integrar as descobertas relacionadas à segurança da conta no sistema de backlog ou emissão de tíquetes do aplicativo. A partir desse sistema, a equipe de nuvem ou a equipe de aplicativos podem abordar a descoberta. Para obter exemplos, consulte Exemplo de equipe de nuvem ou Exemplo de equipe de aplicativos neste guia.



- Atribua as descobertas restantes e não resolvidas à equipe de nuvem — As descobertas residuais podem estar relacionadas a configurações padrão ou a configurações abrangentes que a equipe de nuvem pode abordar. Essa equipe provavelmente tem o maior conhecimento histórico e acesso para resolver a descoberta. No geral, esse é normalmente um subconjunto significativamente menor do total de descobertas.

Avalie e priorize as descobertas de segurança

Um componente essencial de um programa eficaz de gerenciamento de vulnerabilidades é a capacidade de avaliar e priorizar as descobertas de segurança. É aqui que entra o contexto, o histórico organizacional e o ajuste dos sistemas de detecção. A priorização das descobertas de segurança ajuda a estabelecer a velocidade apropriada para o nível de resposta.

Para o Amazon Inspector e a Amazon AWS Security Hub GuardDuty, as descobertas contêm um rótulo ou pontuação de severidade. Recomendamos priorizar a investigação de todas as descobertas críticas e de alta severidade no Security Hub, incluindo descobertas relacionadas ao padrão Foundational Security Best Practices (FSBP), Amazon Inspector e. GuardDuty Para encontrar rótulos de severidade, as pontuações são determinadas da seguinte forma:

- A pontuação do Amazon Inspector é uma pontuação altamente contextualizada para cada descoberta. É calculado correlacionando as informações de pontuação básica do Common Vulnerability Scoring System (CVSS) com os resultados de acessibilidade da rede e dados de explorabilidade. Usando essa pontuação, você pode priorizar as descobertas para se concentrar nas descobertas mais críticas e nos recursos vulneráveis. Além da pontuação, o Amazon Inspector também fornece inteligência de vulnerabilidade aprimorada sobre vulnerabilidades e exposições comuns (CVE). Este é um resumo da inteligência disponível sobre o CVE da Amazon, bem como de fontes de inteligência de segurança padrão do setor, como Recorded Future e Cybersecurity and Infrastructure Security Agency (CISA). Por exemplo, o Amazon Inspector pode fornecer os

nomes de kits de malware conhecidos usados para explorar uma vulnerabilidade. Para obter mais informações, consulte Inteligência de vulnerabilidade.

- Cada GuardDuty descoberta tem um nível de severidade e um valor atribuídos que refletem o risco potencial da descoberta para seu ambiente. Esse nível e valor são determinados pelos engenheiros AWS de segurança. Por exemplo, um nível de `High` severidade indica que um recurso está comprometido e está sendo usado ativamente para fins não autorizados. Recomendamos que você trate uma GuardDuty constatação de `High` gravidade como uma prioridade e corrija imediatamente para evitar mais uso não autorizado.
- A severidade de uma descoberta de controle do Security Hub é determinada pela dificuldade de exploração e pela probabilidade de comprometimento. A dificuldade é determinada pela quantidade de sofisticação ou complexidade necessária para usar a fraqueza para realizar um cenário de ameaça. A probabilidade de comprometimento indica a probabilidade de o cenário de ameaça resultar em uma interrupção ou violação de seus recursos ou de seus recursos Serviços da AWS .

Para ajustar as descobertas, você pode suprimir ou arquivar descobertas específicas diretamente no respectivo console de serviço ou usando a API do serviço. Além disso, você pode fazer alterações nas descobertas no Security Hub usando regras de automação. GuardDuty e as descobertas do Amazon Inspector são enviadas automaticamente para o Security Hub. Você pode usar regras de automação para atualizar automaticamente (como alterar a gravidade) ou suprimir descobertas quase em tempo real, com base nos critérios definidos por você. Ao criar regras de automação, recomendamos adicionar contexto à descrição da regra, como a data de criação ou modificação, quem a criou e por que a regra é necessária. Essas informações geralmente são úteis para referência futura.

Corrija as descobertas de segurança

Depois de avaliar e priorizar uma descoberta, a próxima ação é remediar a descoberta. Há muitas ações diferentes que você pode tomar para remediar uma descoberta. Para vulnerabilidades de software, você pode atualizar o sistema operacional ou aplicar um patch. Para descobrir a configuração da nuvem, você pode atualizar a configuração do recurso. Em geral, as ações que você toma para remediar podem ser agrupadas em um dos seguintes resultados:

- Remediação manual — Você fornece manualmente uma correção para a vulnerabilidade, como modificar as propriedades de um AWS recurso para ativar a criptografia. Se a descoberta for de

uma verificação gerenciada no Security Hub, a descoberta incluirá um link para instruções para remediar manualmente a descoberta.

- Artefato reutilizável — Você atualiza a infraestrutura como código (IaC) para corrigir a vulnerabilidade e sabe que outras pessoas poderiam se beneficiar de uma solução semelhante. Considere fazer o upload do IaC atualizado e de um breve resumo da resolução em um repositório interno de código compartilhado.
- Remediação automatizada — A vulnerabilidade é corrigida automaticamente por meio de mecanismos que você criou.
- Controle de pipeline — Você aplica um controle em seu pipeline de integração contínua e entrega contínua (CI/CD) que impede a implantação se a vulnerabilidade estiver presente.
- Risco aceito — Você não realiza nenhuma ação nem implementa um controle compensatório e aceita o risco que a vulnerabilidade apresenta. Rastreie o risco aceito em um local dedicado, como um registro de riscos.
- Falso positivo — Você não realiza nenhuma ação porque determinou que a descoberta não identificou corretamente uma vulnerabilidade.

Uma lista completa das várias ações que você pode tomar e das ferramentas que você pode usar para corrigir uma vulnerabilidade está fora do escopo deste guia. No entanto, há alguns serviços e ferramentas que você pode ajudar a corrigir vulnerabilidades em grande escala que merecem destaque, incluindo:

- O Patch Manager, um recurso do AWS Systems Manager, automatiza o processo de correção de nós gerenciados com atualizações relacionadas à segurança e outros tipos de atualizações. Você pode usar o Patch Manager para aplicar patches de sistemas operacionais e aplicativos.
- AWS Firewall Managerajuda você a configurar e gerenciar centralmente as regras de firewall em todas as suas contas e aplicativos em AWS Organizations. À medida que novos aplicativos são criados, o Firewall Manager facilita a conformidade de novos aplicativos e recursos ao impor um conjunto comum de regras de segurança.
- O Automated Security Response on AWS é uma AWS solução que funciona com o Security Hub e fornece ações predefinidas de resposta e remediação com base nos padrões de conformidade do setor e nas melhores práticas para ameaças à segurança.

Exemplos de triagem e correção de descobertas de segurança

Esta seção fornece exemplos do processo de triagem para as equipes de segurança, nuvem e aplicativos. Ele discute os tipos de descobertas que cada equipe geralmente aborda e fornece um exemplo de como responder. Orientações de remediação de alto nível também estão incluídas.

Os exemplos a seguir estão incluídos nesta seção:

- Exemplo de equipe de segurança: criação de uma regra de automação do Security Hub
- Exemplo de equipe de nuvem: alteração das configurações de VPC
- Exemplo de equipe de aplicativos: criação de uma AWS Config regra

Exemplo de equipe de segurança: criação de uma regra de automação do Security Hub

A equipe de segurança recebe descobertas relacionadas à detecção de ameaças, incluindo GuardDuty descobertas da Amazon. Para obter uma lista completa dos tipos de GuardDuty descoberta que são categorizados por tipo de AWS recurso, consulte Tipos de busca na GuardDuty documentação. As equipes de segurança devem estar familiarizadas com todos esses tipos de descobertas.

Neste exemplo, a equipe de segurança está aceitando o nível de risco associado às descobertas de segurança em um Conta da AWS documento que é usado estritamente para fins de aprendizado e não inclui dados importantes ou confidenciais. O nome dessa conta é e `sandbox` o ID da conta é`123456789012`. A equipe de segurança pode criar uma regra de AWS Security Hub automação que suprime todas as GuardDuty descobertas dessa conta. Eles podem criar uma regra a partir de um modelo, que abrange muitos casos de uso comuns, ou criar uma regra personalizada. No Security Hub, recomendamos visualizar os resultados dos critérios para confirmar se a regra retorna as descobertas pretendidas.

> **Note**
>
> Este exemplo destaca a funcionalidade das regras de automação. Não recomendamos a supressão de todas as GuardDuty descobertas de uma conta. O contexto é importante, e cada organização deve escolher quais descobertas suprimir com base no tipo de dados, na classificação e nos controles de mitigação.

A seguir estão os parâmetros usados para criar essa regra de automação:

- Regra:
  - O nome da regra é `Suppress findings from Sandbox account`
  - A descrição da regra é `Date: 06/25/23 Authored by: John Doe Reason: Suppress GuardDuty findings from the sandbox account`
- Critérios:
  - `AwsAccountId` = `123456789012`
  - `ProductName` = `GuardDuty`
  - `WorkflowStatus` = `NEW`
  - `RecordState` = `ACTIVE`
- Ação automatizada:
  - `Workflow.status` é `SUPPRESSED`

Para obter mais informações, consulte Regras de automação na documentação do Security Hub. As equipes de segurança têm muitas opções para investigar e corrigir as descobertas das ameaças detectadas. Para obter orientações abrangentes, consulte o Guia de Resposta a Incidentes de AWS Segurança. Recomendamos revisar este guia para confirmar que você estabeleceu processos sólidos de resposta a incidentes.

Exemplo de equipe de nuvem: alteração das configurações de VPC

A equipe de nuvem é responsável por fazer a triagem e corrigir as descobertas de segurança que têm tendências comuns, como alterações nas configurações AWS padrão que podem não se adequar ao seu caso de uso. Essas descobertas tendem a afetar muitos Contas da AWS recursos, como configurações de VPC, ou incluem uma restrição que deve ser colocada em todo o ambiente. Na maioria das vezes, a equipe de nuvem faz alterações manuais e únicas, como adicionar ou atualizar uma política.

Depois que sua organização tiver usado um AWS ambiente por algum tempo, você poderá encontrar um conjunto de antipadrões em desenvolvimento. Um antipadrão é uma solução frequentemente usada para um problema recorrente em que a solução é contraproducente, ineficaz ou menos eficaz do que uma alternativa. Como alternativa a esses antipadrões, sua organização pode usar restrições ambientais que sejam mais eficazes, como políticas de controle de AWS Organizations serviços (SCPs) ou conjuntos de permissões do IAM Identity Center. SCPs e conjuntos de permissões podem

fornecer restrições adicionais para tipos de recursos, como impedir que os usuários configurem um bucket público do Amazon Simple Storage Service (Amazon S3). Embora possa ser tentador restringir todas as configurações de segurança possíveis, há limites de tamanho de política para SCPs e conjuntos de permissões. Recomendamos uma abordagem equilibrada para os controles preventivos e de detetive.

A seguir estão alguns controles do padrão AWS Security Hub Foundational Security Best Practices (FSBP) pelos quais a equipe de nuvem pode ser responsável:

- [EC2.2] O grupo de segurança padrão da VPC não deve permitir tráfego de entrada e saída
- [EC2.6] O registro de fluxo de VPC deve ser ativado em todas as VPCs
- [EC2.23] Os Amazon EC2 Transit Gateways não devem aceitar automaticamente solicitações de anexos de VPC
- [CloudTrail.1] CloudTrail deve ser habilitado e configurado com pelo menos uma trilha multirregional que inclua eventos de gerenciamento de leitura e gravação
- [Config.1] AWS Config deve estar habilitado

Neste exemplo, a equipe de nuvem está abordando uma descoberta sobre o controle EC2.2 do FSBP. A documentação desse controle recomenda não usar o grupo de segurança padrão porque ele permite amplo acesso por meio das regras padrão de entrada e saída. Como o grupo de segurança padrão não pode ser excluído, a recomendação é alterar as configurações da regra para restringir o tráfego de entrada e saída. Para resolver esse problema de forma eficiente, a equipe de nuvem deve usar mecanismos estabelecidos para modificar as regras do grupo de segurança para todas as VPCs, pois cada VPC tem esse grupo de segurança padrão. Na maioria dos casos, as equipes de nuvem gerenciam as configurações de VPC usando AWS Control Towerpersonalizações ou uma ferramenta de infraestrutura como código (IaC), como ou. HashiCorp TerraformAWS CloudFormation

Exemplo de equipe de aplicativos: criação de uma AWS Config regra

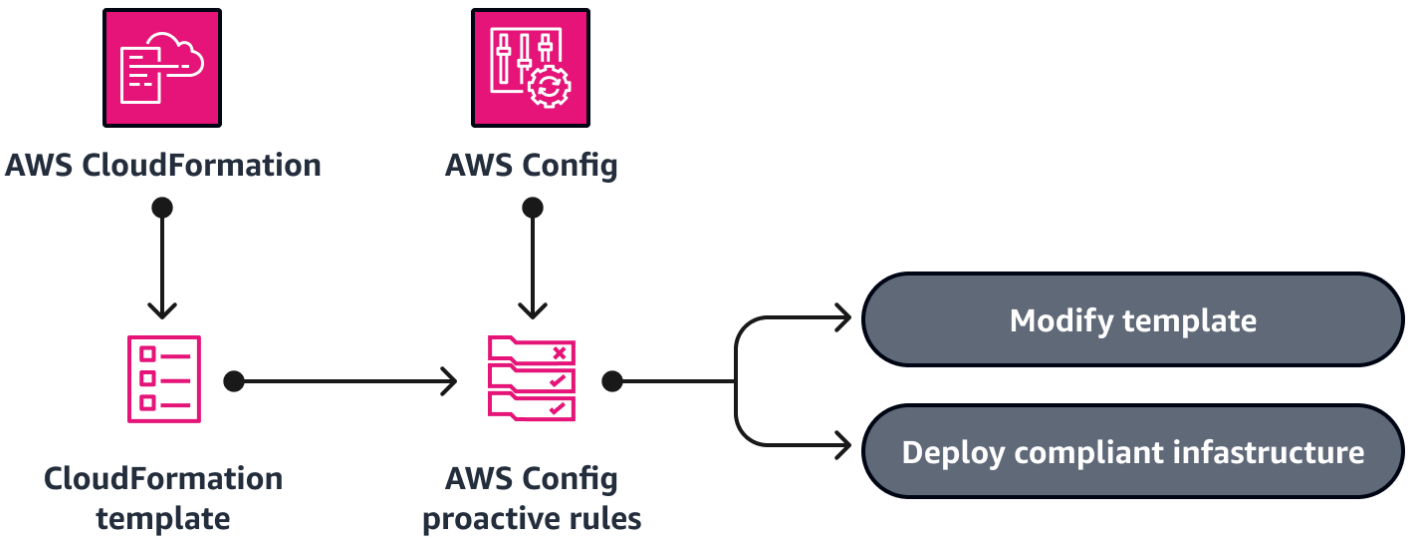
A seguir estão alguns controles do padrão de segurança Security Hub Foundational Security Best Practices (FSBP) pelos quais o aplicativo ou a equipe de desenvolvimento podem ser responsáveis:

- [CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado
- [EC2.19] Grupos de segurança não devem permitir acesso irrestrito a portas com alto risco

- [CodeBuild.1] CodeBuild GitHub ou os URLs do repositório de origem do Bitbucket devem usar OAuth
- [ECS.4] Os contêineres do ECS devem ser executados sem privilégios
- [ELB.1] O Application Load Balancer deve ser configurado para redirecionar todas as solicitações HTTP para HTTPS

Neste exemplo, a equipe de aplicação está abordando uma descoberta para o controle FSBP EC2.19. Esse controle verifica se o tráfego de entrada irrestrito dos grupos de segurança é acessível para as portas especificadas que o maior risco. Esse controle falhará se alguma das regras em um grupo de segurança permitir tráfego de entrada de `0.0.0.0/0` ou `::/0` para essas portas. A documentação desse controle recomenda excluir as regras que permitem esse tráfego.

Além de abordar a regra do grupo de segurança individual, esse é um ótimo exemplo de uma descoberta que deve resultar em uma nova AWS Config regra. Ao usar o modo de avaliação proativa, você pode ajudar a evitar a implantação de regras arriscadas de grupos de segurança no futuro. O modo proativo avalia os recursos antes de serem implantados para que você possa evitar recursos mal configurados e suas descobertas de segurança associadas. Ao implementar um novo serviço ou uma nova funcionalidade, as equipes de aplicativos podem executar regras no modo proativo como parte de seu pipeline de integração contínua e entrega contínua (CI/CD) para identificar recursos não compatíveis. A imagem a seguir mostra como você pode usar uma AWS Config regra proativa para confirmar se a infraestrutura definida em um AWS CloudFormation modelo está em conformidade.



Outra eficiência importante pode ser obtida neste exemplo. Quando uma equipe de aplicativos cria uma AWS Config regra proativa, ela pode compartilhá-la em um repositório de código comum para que outras equipes de aplicativos possam usá-la.

Cada descoberta associada a um controle do Security Hub contém detalhes sobre a descoberta e um link para as instruções para corrigir o problema. Embora as equipes de nuvem possam encontrar descobertas que exijam uma correção manual e única, quando apropriado, recomendamos criar verificações proativas que identifiquem os problemas o mais cedo possível no processo de desenvolvimento.

Relate e melhore seu programa de gerenciamento de vulnerabilidades

Relatórios eficazes para o gerenciamento de vulnerabilidades envolvem a análise de dados, o monitoramento de tendências e o compartilhamento de conhecimento. Isso fornece visibilidade e ajuda as equipes a melhorar a postura de segurança de suas organizações no Nuvem AWS.

Conduza reuniões mensais de operações de segurança

As reuniões mensais de operações de segurança são um mecanismo eficaz para promover a propriedade, a responsabilidade e o alinhamento contínuos entre as equipes. Na reunião, as partes interessadas das equipes de segurança, nuvem e aplicativos analisam os dados em busca de descobertas de segurança excepcionais, descobertas fora dos acordos de nível de serviço (SLAs) e as equipes que obtiveram mais descobertas.

Essas reuniões ajudam suas equipes a identificar antipadrões, como oportunidades de adicionar mais restrições. Controles preventivos e oportunidades de automação também podem ser descobertos e compartilhados. As reuniões também ajudam a identificar o que está funcionando e o que não está funcionando bem no programa de gerenciamento de vulnerabilidades, para que você possa fazer melhorias.

Ao analisar dados, identificar antipadrões e problemas e compartilhar informações sobre controles e automações, as equipes podem obter informações valiosas e fazer refinamentos contínuos que podem fortalecer sua postura de segurança e reduzir seus SLAs relacionados à segurança.

Use os insights do Security Hub para identificar antipadrões

AWS Security Hub os insights também podem ajudá-lo a identificar antipadrões e acompanhar seu progresso na correção das descobertas. Uma visão do Security Hub é uma coleção de descobertas relacionadas. Identifica uma área de segurança que requer atenção e intervenção. Os insights do Security Hub podem ajudar você a identificar requisitos específicos e desenvolver relatórios. O Security Hub oferece vários insights gerenciados integrados. Para rastrear problemas de segurança exclusivos de seu AWS ambiente e uso, você pode criar insights personalizados.

Conclusão e próximas etapas

Em resumo, um programa eficaz de gerenciamento de vulnerabilidades exige uma preparação minuciosa e exige que você habilite as ferramentas e integrações certas, ajuste essas ferramentas, faça a triagem eficiente dos problemas e relate e melhore continuamente. Seguindo as melhores práticas deste guia, as organizações podem criar um programa escalável de gerenciamento de vulnerabilidades AWS para ajudar a proteger seus ambientes de nuvem.

Você pode expandir esse programa para incluir outras vulnerabilidades e descobertas relacionadas à segurança, como vulnerabilidades de segurança de aplicativos. AWS Security Hub oferece suporte a integrações personalizadas de produtos. Considere usar o Security Hub como ponto de integração para ferramentas e produtos de segurança adicionais. Essa integração permite que você aproveite os processos e fluxos de trabalho que você já estabeleceu em seu programa de gerenciamento de vulnerabilidades, como a integração direta com os backlogs de produtos e as reuniões mensais de revisão de segurança.

A tabela a seguir resume as fases e os itens de ação descritos neste guia.

Fase	Itens de ação
Preparar	• Defina um plano de gerenciamento de vulnerabilidades. • Distribua a propriedade das descobertas. • Desenvolva um programa de divulgação de vulnerabilidades. • Desenvolva uma Conta da AWS estrutura. • Defina, implemente e aplique tags. • Monitore os boletins de AWS segurança. • Habilite o Amazon Inspector com um administrador delegado. • Ative o Security Hub com um administrador delegado. • Ative os padrões do Security Hub. • Configure a agregação entre regiões do Security Hub.

Fase	Itens de ação
	• Habilite descobertas de controle consolidadas no Security Hub. • Configure e gerencie integrações do Security Hub, incluindo integrações posteriores aplicáveis com SIEM, GRC ou sistemas de backlog ou emissão de tíquetes de produtos
Faça a triagem e a remediação	• Direcione as descobertas com base na estratégia de várias contas. • Direcione as descobertas para equipes de segurança, nuvem e aplicativos ou desenvolvedores. • Ajuste as descobertas de segurança para garantir que elas sejam acionáveis para seu ambiente específico. • Desenvolva mecanismos automatizados de remediação, quando possível. • Implemente controles de pipeline de CI/CD ou outras barreiras que ajudem a evitar descobertas de segurança, quando possível. • Use as regras de automação do Security Hub para escalar ou suprimir descobertas.
Relate e melhore	• Realize reuniões mensais de operações de segurança. • Use os insights do Security Hub para identificar antipadrões.

Recursos

AWS documentação de serviço

- Integrações de produtos ()AWS Security Hub
- Integrando AWS Security Hub em Jira Service Management Cloud ()AWS Security Hub
- Regras de automação (AWS Security Hub)
- Regras de avaliação proativa ()AWS Config
- Gerenciador de patches (AWS Systems Manager)

Outros AWS recursos

- Práticas recomendadas para marcar AWS recursos (AWS whitepaper)
- Resposta de segurança automatizada ativada AWS (Biblioteca de AWS soluções)
- AWS Guia de resposta a incidentes de segurança (guiaAWS técnico)
- AWS boletins de segurança

Histórico do documento

A tabela a seguir descreve alterações significativas feitas neste guia. Se desejar receber notificações sobre futuras atualizações, inscreva-se em um feed RSS.

Alteração	Descrição	Data
Publicação inicial	—	12 de outubro de 2023

AWS Glossário de orientação prescritiva

A seguir estão os termos comumente usados em estratégias, guias e padrões fornecidos pela Orientação AWS Prescritiva. Para sugerir entradas, use o link Fornecer feedback no final do glossário.

Números

7 Rs

Sete estratégias comuns de migração para mover aplicações para a nuvem. Essas estratégias baseiam-se nos 5 Rs identificados pela Gartner em 2011 e consistem em:

- Refatorar/rearquitetar: mova uma aplicação e modifique sua arquitetura aproveitando ao máximo os recursos nativos de nuvem para melhorar a agilidade, a performance e a escalabilidade. Isso normalmente envolve a portabilidade do sistema operacional e do banco de dados. Exemplo: migre seu banco de dados Oracle local para a edição compatível com o Amazon Aurora PostgreSQL.
- Redefinir a plataforma (mover e redefinir [mover e redefinir (lift-and-reshape]): mova uma aplicação para a nuvem e introduza algum nível de otimização a fim de aproveitar os recursos da nuvem. Exemplo: Migre seu banco de dados Oracle local para o Amazon Relational Database Service (Amazon RDS) for Oracle no. Nuvem AWS
- Recomprar (drop and shop): mude para um produto diferente, normalmente migrando de uma licença tradicional para um modelo SaaS. Exemplo: migre seu sistema de gerenciamento de relacionamento com o cliente (CRM) para a Salesforce.com.
- Redefinir a hospedagem (mover sem alterações [lift-and-shift])mover uma aplicação para a nuvem sem fazer nenhuma alteração a fim de aproveitar os recursos da nuvem. Exemplo: Migre seu banco de dados Oracle local para o Oracle em uma instância do EC2 no. Nuvem AWS
- Realocar (mover o hipervisor sem alterações [hypervisor-level lift-and-shift]): mover a infraestrutura para a nuvem sem comprar novo hardware, reescrever aplicações ou modificar suas operações existentes. Você migra servidores de uma plataforma local para um serviço em nuvem para a mesma plataforma. Exemplo: migrar um Microsoft Hyper-V aplicativo para o. AWS
- Reter (revisitar): mantenha as aplicações em seu ambiente de origem. Isso pode incluir aplicações que exigem grande refatoração, e você deseja adiar esse trabalho para um

momento posterior, e aplicações antigas que você deseja manter porque não há justificativa comercial para migrá-las.

- Retirar: desative ou remova aplicações que não são mais necessárias em seu ambiente de origem.

A

ABAC

Consulte controle de acesso baseado em atributos.

serviços abstratos

Veja os serviços gerenciados.

ACID

Veja atomicidade, consistência, isolamento, durabilidade.

migração ativa-ativa

Um método de migração de banco de dados no qual os bancos de dados de origem e de destino são mantidos em sincronia (por meio de uma ferramenta de replicação bidirecional ou operações de gravação dupla), e ambos os bancos de dados lidam com transações de aplicações conectadas durante a migração. Esse método oferece suporte à migração em lotes pequenos e controlados, em vez de exigir uma substituição única. É mais flexível, mas exige mais trabalho do que a migração ativa-passiva.

migração ativa-passiva

Um método de migração de banco de dados no qual os bancos de dados de origem e de destino são mantidos em sincronia, mas somente o banco de dados de origem manipula as transações das aplicações conectadas enquanto os dados são replicados no banco de dados de destino. O banco de dados de destino não aceita nenhuma transação durante a migração.

função agregada

Uma função SQL que opera em um grupo de linhas e calcula um único valor de retorno para o grupo. Exemplos de funções agregadas incluem `SUM` e. `MAX`

AI

Veja inteligência artificial.

AIOps

Veja as operações de inteligência artificial.

anonimização

O processo de excluir permanentemente informações pessoais em um conjunto de dados. A anonimização pode ajudar a proteger a privacidade pessoal. Dados anônimos não são mais considerados dados pessoais.

antipadrões

Uma solução frequentemente usada para um problema recorrente em que a solução é contraproducente, ineficaz ou menos eficaz do que uma alternativa.

controle de aplicativos

Uma abordagem de segurança que permite o uso somente de aplicativos aprovados para ajudar a proteger um sistema contra malware.

portfólio de aplicações

Uma coleção de informações detalhadas sobre cada aplicação usada por uma organização, incluindo o custo para criar e manter a aplicação e seu valor comercial. Essas informações são fundamentais para o processo de descoberta e análise de portfólio e ajudam a identificar e priorizar as aplicações a serem migradas, modernizadas e otimizadas.

inteligência artificial (IA)

O campo da ciência da computação que se dedica ao uso de tecnologias de computação para desempenhar funções cognitivas normalmente associadas aos humanos, como aprender, resolver problemas e reconhecer padrões. Para obter mais informações, consulte O que é inteligência artificial?

operações de inteligência artificial (AIOps)

O processo de usar técnicas de machine learning para resolver problemas operacionais, reduzir incidentes operacionais e intervenção humana e aumentar a qualidade do serviço. Para obter mais informações sobre como as AIOps são usadas na estratégia de migração para a AWS , consulte o guia de integração de operações.

criptografia assimétrica

Um algoritmo de criptografia que usa um par de chaves, uma chave pública para criptografia e uma chave privada para descriptografia. É possível compartilhar a chave pública porque ela não é usada na descriptografia, mas o acesso à chave privada deve ser altamente restrito.

atomicidade, consistência, isolamento, durabilidade (ACID)

Um conjunto de propriedades de software que garantem a validade dos dados e a confiabilidade operacional de um banco de dados, mesmo no caso de erros, falhas de energia ou outros problemas.

controle de acesso por atributo (ABAC)

A prática de criar permissões minuciosas com base nos atributos do usuário, como departamento, cargo e nome da equipe. Para obter mais informações, consulte ABAC AWS na documentação AWS Identity and Access Management (IAM).

fonte de dados autorizada

Um local onde você armazena a versão principal dos dados, que é considerada a fonte de informações mais confiável. Você pode copiar dados da fonte de dados autorizada para outros locais com o objetivo de processar ou modificar os dados, como anonimizá-los, redigi-los ou pseudonimizá-los.

Availability Zone (zona de disponibilidade)

Um local distinto dentro de um Região da AWS que está isolado de falhas em outras zonas de disponibilidade e fornece conectividade de rede barata e de baixa latência a outras zonas de disponibilidade na mesma região.

AWS Estrutura de adoção da nuvem (AWS CAF)

Uma estrutura de diretrizes e melhores práticas AWS para ajudar as organizações a desenvolver um plano eficiente e eficaz para migrar com sucesso para a nuvem. AWS O CAF organiza a orientação em seis áreas de foco chamadas perspectivas: negócios, pessoas, governança, plataforma, segurança e operações. As perspectivas de negócios, pessoas e governança têm como foco habilidades e processos de negócios; as perspectivas de plataforma, segurança e operações concentram-se em habilidades e processos técnicos. Por exemplo, a perspectiva das pessoas tem como alvo as partes interessadas que lidam com recursos humanos (RH), funções de pessoal e gerenciamento de pessoal. Nessa perspectiva, o AWS CAF fornece orientação para desenvolvimento, treinamento e comunicação de pessoas para ajudar a preparar a organização

para a adoção bem-sucedida da nuvem. Para obter mais informações, consulte o site da AWS CAF e o whitepaper da AWS CAF.

AWS Estrutura de qualificação da carga de trabalho (AWS WQF)

Uma ferramenta que avalia as cargas de trabalho de migração do banco de dados, recomenda estratégias de migração e fornece estimativas de trabalho. AWS O WQF está incluído com AWS Schema Conversion Tool ()AWS SCT. Ela analisa esquemas de banco de dados e objetos de código, código de aplicações, dependências e características de performance, além de fornecer relatórios de avaliação.

B

bot ruim

Um bot destinado a perturbar ou causar danos a indivíduos ou organizações.

BCP

Veja o planejamento de continuidade de negócios.

gráfico de comportamento

Uma visualização unificada e interativa do comportamento e das interações de recursos ao longo do tempo. É possível usar um gráfico de comportamento com o Amazon Detective para examinar tentativas de login malsucedidas, chamadas de API suspeitas e ações similares. Para obter mais informações, consulte Dados em um gráfico de comportamento na documentação do Detective.

sistema big-endian

Um sistema que armazena o byte mais significativo antes. Veja também endianness.

classificação binária

Um processo que prevê um resultado binário (uma de duas classes possíveis). Por exemplo, seu modelo de ML pode precisar prever problemas como “Este e-mail é ou não é spam?” ou “Este produto é um livro ou um carro?”

filtro de bloom

Uma estrutura de dados probabilística e eficiente em termos de memória que é usada para testar se um elemento é membro de um conjunto.

blue/green deployment (implantação azul/verde)

Uma estratégia de implantação em que você cria dois ambientes separados, mas idênticos. Você executa a versão atual do aplicativo em um ambiente (azul) e a nova versão do aplicativo no outro ambiente (verde). Essa estratégia ajuda você a reverter rapidamente com o mínimo de impacto.

bot

Um aplicativo de software que executa tarefas automatizadas pela Internet e simula a atividade ou interação humana. Alguns bots são úteis ou benéficos, como rastreadores da Web que indexam informações na Internet. Alguns outros bots, conhecidos como bots ruins, têm como objetivo perturbar ou causar danos a indivíduos ou organizações.

botnet

Redes de bots infectadas por malware e sob o controle de uma única parte, conhecidas como pastor de bots ou operador de bots. As redes de bots são o mecanismo mais conhecido para escalar bots e seu impacto.

ramo

Uma área contida de um repositório de código. A primeira ramificação criada em um repositório é a ramificação principal. Você pode criar uma nova ramificação a partir de uma ramificação existente e, em seguida, desenvolver recursos ou corrigir bugs na nova ramificação. Uma ramificação que você cria para gerar um recurso é comumente chamada de ramificação de recurso. Quando o recurso estiver pronto para lançamento, você mesclará a ramificação do recurso de volta com a ramificação principal. Para obter mais informações, consulte Sobre filiais (GitHub documentação).

acesso em vidro quebrado

Em circunstâncias excepcionais e por meio de um processo aprovado, um meio rápido para um usuário obter acesso a um Conta da AWS que ele normalmente não tem permissão para acessar. Para obter mais informações, consulte o indicador Implementar procedimentos de quebra de vidro na orientação do Well-Architected AWS .

estratégia brownfield

A infraestrutura existente em seu ambiente. Ao adotar uma estratégia brownfield para uma arquitetura de sistema, você desenvolve a arquitetura de acordo com as restrições dos sistemas e da infraestrutura atuais. Se estiver expandindo a infraestrutura existente, poderá combinar as estratégias brownfield e greenfield.

cache do buffer

A área da memória em que os dados acessados com mais frequência são armazenados.

capacidade de negócios

O que uma empresa faz para gerar valor (por exemplo, vendas, atendimento ao cliente ou marketing). As arquiteturas de microsserviços e as decisões de desenvolvimento podem ser orientadas por recursos de negócios. Para obter mais informações, consulte a seção Organizados de acordo com as capacidades de negócios do whitepaper Executar microsserviços conteinerizados na AWS.

planejamento de continuidade de negócios (BCP)

Um plano que aborda o impacto potencial de um evento disruptivo, como uma migração em grande escala, nas operações e permite que uma empresa retome as operações rapidamente.

C

CAF

Consulte Estrutura de adoção da AWS nuvem.

implantação canária

O lançamento lento e incremental de uma versão para usuários finais. Quando estiver confiante, você implanta a nova versão e substituirá a versão atual em sua totalidade.

CCoE

Veja o Centro de Excelência em Nuvem.

CDC

Veja a captura de dados de alterações.

captura de dados de alterações (CDC)

O processo de rastrear alterações em uma fonte de dados, como uma tabela de banco de dados, e registrar metadados sobre a alteração. É possível usar o CDC para várias finalidades, como auditar ou replicar alterações em um sistema de destino para manter a sincronização.

engenharia do caos

Introduzir intencionalmente falhas ou eventos disruptivos para testar a resiliência de um sistema. Você pode usar AWS Fault Injection Service (AWS FIS) para realizar experimentos que estressam suas AWS cargas de trabalho e avaliar sua resposta.

CI/CD

Veja a integração e a entrega contínuas.

classificação

Um processo de categorização que ajuda a gerar previsões. Os modelos de ML para problemas de classificação predizem um valor discreto. Os valores discretos são sempre diferentes uns dos outros. Por exemplo, um modelo pode precisar avaliar se há ou não um carro em uma imagem.

criptografia no lado do cliente

Criptografia de dados localmente, antes que o alvo os Serviço da AWS receba.

Centro de Excelência da Nuvem (CCoE)

Uma equipe multidisciplinar que impulsiona os esforços de adoção da nuvem em toda a organização, incluindo o desenvolvimento de práticas recomendas de nuvem, a mobilização de recursos, o estabelecimento de cronogramas de migração e a liderança da organização em transformações em grande escala. Para obter mais informações, consulte as postagens do CCoE no blog de estratégia Nuvem AWS corporativa.

computação em nuvem

A tecnologia de nuvem normalmente usada para armazenamento de dados remoto e gerenciamento de dispositivos de IoT. A computação em nuvem geralmente está conectada à tecnologia de computação de ponta.

modelo operacional em nuvem

Em uma organização de TI, o modelo operacional usado para criar, amadurecer e otimizar um ou mais ambientes de nuvem. Para obter mais informações, consulte Criar seu modelo operacional de nuvem.

estágios de adoção da nuvem

As quatro fases pelas quais as organizações normalmente passam quando migram para o Nuvem AWS:

- Projeto: executar alguns projetos relacionados à nuvem para fins de prova de conceito e aprendizado
- Fundação: realizar investimentos fundamentais para escalar sua adoção da nuvem (por exemplo, criar uma zona de pouso, definir um CCoE, estabelecer um modelo de operações)
- Migração: migrar aplicações individuais
- Reinvenção: otimizar produtos e serviços e inovar na nuvem

Esses estágios foram definidos por Stephen Orban na postagem do blog The Journey Toward Cloud-First & the Stages of Adoption no blog de estratégia Nuvem AWS empresarial. Para obter informações sobre como eles se relacionam com a estratégia de AWS migração, consulte o guia de preparação para migração.

CMDB

Consulte o banco de dados de gerenciamento de configuração.

repositório de código

Um local onde o código-fonte e outros ativos, como documentação, amostras e scripts, são armazenados e atualizados por meio de processos de controle de versão. Os repositórios de nuvem comuns incluem GitHub ou AWS CodeCommit. Cada versão do código é chamada de ramificação. Em uma estrutura de microsserviços, cada repositório é dedicado a uma única peça de funcionalidade. Um único pipeline de CI/CD pode usar vários repositórios.

cache frio

Um cache de buffer que está vazio, não está bem preenchido ou contém dados obsoletos ou irrelevantes. Isso afeta a performance porque a instância do banco de dados deve ler da memória principal ou do disco, um processo que é mais lento do que a leitura do cache do buffer.

dados frios

Dados que raramente são acessados e geralmente são históricos. Ao consultar esse tipo de dados, consultas lentas geralmente são aceitáveis. Mover esses dados para níveis ou classes de armazenamento de baixo desempenho e menos caros pode reduzir os custos.

visão computacional (CV)

Um campo da IA que usa aprendizado de máquina para analisar e extrair informações de formatos visuais, como imagens e vídeos digitais. Por exemplo, AWS Panorama oferece dispositivos que adicionam CV às redes de câmeras locais, e a Amazon SageMaker fornece algoritmos de processamento de imagem para CV.

desvio de configuração

Para uma carga de trabalho, uma alteração de configuração em relação ao estado esperado. Isso pode fazer com que a carga de trabalho se torne incompatível e, normalmente, é gradual e não intencional.

banco de dados de gerenciamento de configuração (CMDB)

Um repositório que armazena e gerencia informações sobre um banco de dados e seu ambiente de TI, incluindo componentes de hardware e software e suas configurações. Normalmente, os dados de um CMDB são usados no estágio de descoberta e análise do portfólio da migração.

pacote de conformidade

Um conjunto de AWS Config regras e ações de remediação que você pode montar para personalizar suas verificações de conformidade e segurança. Você pode implantar um pacote de conformidade como uma entidade única em uma Conta da AWS região ou em uma organização usando um modelo YAML. Para obter mais informações, consulte Pacotes de conformidade na documentação. AWS Config

integração contínua e entrega contínua (CI/CD)

O processo de automatizar os estágios de origem, criação, teste, preparação e produção do processo de lançamento do software. O CI/CD é comumente descrito como um pipeline. O CI/CD pode ajudar você a automatizar processos, melhorar a produtividade, melhorar a qualidade do código e entregar com mais rapidez. Para obter mais informações, consulte Benefícios da entrega contínua. CD também pode significar implantação contínua. Para obter mais informações, consulte Entrega contínua versus implantação contínua.

CV

Veja visão computacional.

D

dados em repouso

Dados estacionários em sua rede, por exemplo, dados que estão em um armazenamento.

classificação de dados

Um processo para identificar e categorizar os dados em sua rede com base em criticalidade e confidencialidade. É um componente crítico de qualquer estratégia de gerenciamento de riscos de

segurança cibernética, pois ajuda a determinar os controles adequados de proteção e retenção para os dados. A classificação de dados é um componente do pilar de segurança no AWS Well-Architected Framework. Para obter mais informações, consulte Classificação de dados.

desvio de dados

Uma variação significativa entre os dados de produção e os dados usados para treinar um modelo de ML ou uma alteração significativa nos dados de entrada ao longo do tempo. O desvio de dados pode reduzir a qualidade geral, a precisão e a imparcialidade das previsões do modelo de ML.

dados em trânsito

Dados que estão se movendo ativamente pela sua rede, como entre os recursos da rede.

malha de dados

Uma estrutura arquitetônica que fornece propriedade de dados distribuída e descentralizada com gerenciamento e governança centralizados.

minimização de dados

O princípio de coletar e processar apenas os dados estritamente necessários. Praticar a minimização de dados no Nuvem AWS pode reduzir os riscos de privacidade, os custos e a pegada de carbono de sua análise.

perímetro de dados

Um conjunto de proteções preventivas em seu AWS ambiente que ajudam a garantir que somente identidades confiáveis acessem recursos confiáveis das redes esperadas. Para obter mais informações, consulte Construindo um perímetro de dados em. AWS

pré-processamento de dados

A transformação de dados brutos em um formato que seja facilmente analisado por seu modelo de ML. O pré-processamento de dados pode significar a remoção de determinadas colunas ou linhas e o tratamento de valores ausentes, inconsistentes ou duplicados.

proveniência dos dados

O processo de rastrear a origem e o histórico dos dados ao longo de seu ciclo de vida, por exemplo, como os dados foram gerados, transmitidos e armazenados.

titular dos dados

Um indivíduo cujos dados estão sendo coletados e processados.

data warehouse

Um sistema de gerenciamento de dados que oferece suporte à inteligência comercial, como análises. Os data warehouses geralmente contêm grandes quantidades de dados históricos e geralmente são usados para consultas e análises.

linguagem de definição de dados (DDL)

Instruções ou comandos para criar ou modificar a estrutura de tabelas e objetos em um banco de dados.

linguagem de manipulação de dados (DML)

Instruções ou comandos para modificar (inserir, atualizar e excluir) informações em um banco de dados.

DDL

Consulte a linguagem de definição de banco de dados.

deep ensemble

A combinação de vários modelos de aprendizado profundo para gerar previsões. Os deep ensembles podem ser usados para produzir uma previsão mais precisa ou para estimar a incerteza nas previsões.

Aprendizado profundo

Um subcampo do ML que usa várias camadas de redes neurais artificiais para identificar o mapeamento entre os dados de entrada e as variáveis-alvo de interesse.

defense-in-depth

Uma abordagem de segurança da informação na qual uma série de mecanismos e controles de segurança são cuidadosamente distribuídos por toda a rede de computadores para proteger a confidencialidade, a integridade e a disponibilidade da rede e dos dados nela contidos. Ao adotar essa estratégia AWS, você adiciona vários controles em diferentes camadas da AWS Organizations estrutura para ajudar a proteger os recursos. Por exemplo, uma defense-in-depth abordagem pode combinar autenticação multifatorial, segmentação de rede e criptografia.

administrador delegado

Em AWS Organizations, um serviço compatível pode registrar uma conta de AWS membro para administrar as contas da organização e gerenciar as permissões desse serviço. Essa conta

é chamada de administrador delegado para esse serviço Para obter mais informações e uma lista de serviços compatíveis, consulte Serviços que funcionam com o AWS Organizations na documentação do AWS Organizations .

implantação

O processo de criar uma aplicação, novos recursos ou correções de código disponíveis no ambiente de destino. A implantação envolve a implementação de mudanças em uma base de código e, em seguida, a criação e execução dessa base de código nos ambientes da aplicação

ambiente de desenvolvimento

Veja o ambiente.

controle detectivo

Um controle de segurança projetado para detectar, registrar e alertar após a ocorrência de um evento. Esses controles são uma segunda linha de defesa, alertando você sobre eventos de segurança que contornaram os controles preventivos em vigor. Para obter mais informações, consulte Controles detectivos em Como implementar controles de segurança na AWS.

mapeamento do fluxo de valor de desenvolvimento (DVSM)

Um processo usado para identificar e priorizar restrições que afetam negativamente a velocidade e a qualidade em um ciclo de vida de desenvolvimento de software. O DVSM estende o processo de mapeamento do fluxo de valor originalmente projetado para práticas de manufatura enxuta. Ele se concentra nas etapas e equipes necessárias para criar e movimentar valor por meio do processo de desenvolvimento de software.

gêmeo digital

Uma representação virtual de um sistema real, como um prédio, fábrica, equipamento industrial ou linha de produção. Os gêmeos digitais oferecem suporte à manutenção preditiva, ao monitoramento remoto e à otimização da produção.

tabela de dimensões

Em um esquema em estrela, uma tabela menor que contém atributos de dados sobre dados quantitativos em uma tabela de fatos. Os atributos da tabela de dimensões geralmente são campos de texto ou números discretos que se comportam como texto. Esses atributos são comumente usados para restringir consultas, filtrar e rotular conjuntos de resultados.

desastre

Um evento que impede que uma workload ou sistema cumpra seus objetivos de negócios em seu local principal de implantação. Esses eventos podem ser desastres naturais, falhas técnicas ou o resultado de ações humanas, como configuração incorreta não intencional ou ataque de malware.

Recuperação de desastres (RD)

A estratégia e o processo que você usa para minimizar o tempo de inatividade e a perda de dados causados por um desastre. Para obter mais informações, consulte Recuperação de desastres de cargas de trabalho em AWS: Recuperação na nuvem no AWS Well-Architected Framework.

DML

Consulte linguagem de manipulação de banco de dados.

design orientado por domínio

Uma abordagem ao desenvolvimento de um sistema de software complexo conectando seus componentes aos domínios em evolução, ou principais metas de negócios, atendidos por cada componente. Esse conceito foi introduzido por Eric Evans em seu livro, Design orientado por domínio: lidando com a complexidade no coração do software (Boston: Addison-Wesley Professional, 2003). Para obter informações sobre como usar o design orientado por domínio com o padrão strangler fig, consulte Modernizar incrementalmente os serviços web herdados do Microsoft ASP.NET (ASMX) usando contêineres e o Amazon API Gateway.

DR

Veja a recuperação de desastres.

detecção de deriva

Rastreando desvios de uma configuração básica. Por exemplo, você pode usar AWS CloudFormation para detectar desvios nos recursos do sistema ou AWS Control Tower para detectar mudanças em seu landing zone que possam afetar a conformidade com os requisitos de governança.

DVSM

Veja o mapeamento do fluxo de valor do desenvolvimento.

E

EDA

Veja a análise exploratória de dados.

computação de borda

A tecnologia que aumenta o poder computacional de dispositivos inteligentes nas bordas de uma rede de IoT. Quando comparada à computação em nuvem, a computação de ponta pode reduzir a latência da comunicação e melhorar o tempo de resposta.

Criptografia

Um processo de computação que transforma dados de texto simples, legíveis por humanos, em texto cifrado.

chave de criptografia

Uma sequência criptográfica de bits aleatórios que é gerada por um algoritmo de criptografia. As chaves podem variar em tamanho, e cada chave foi projetada para ser imprevisível e exclusiva.

endianismo

A ordem na qual os bytes são armazenados na memória do computador. Os sistemas big-endian armazenam o byte mais significativo antes. Os sistemas little-endian armazenam o byte menos significativo antes.

endpoint

Veja o endpoint do serviço.

serviço de endpoint

Um serviço que pode ser hospedado em uma nuvem privada virtual (VPC) para ser compartilhado com outros usuários. Você pode criar um serviço de endpoint com AWS PrivateLink e conceder permissões a outros diretores Contas da AWS ou a AWS Identity and Access Management (IAM). Essas contas ou entidades principais podem se conectar ao serviço de endpoint de maneira privada criando endpoints da VPC de interface. Para obter mais informações, consulte Criar um serviço de endpoint na documentação do Amazon Virtual Private Cloud (Amazon VPC).

planejamento de recursos corporativos (ERP)

Um sistema que automatiza e gerencia os principais processos de negócios (como contabilidade, MES e gerenciamento de projetos) para uma empresa.

criptografia envelopada

O processo de criptografar uma chave de criptografia com outra chave de criptografia. Para obter mais informações, consulte Criptografia de envelope na documentação AWS Key Management Service (AWS KMS).

environment (ambiente)

Uma instância de uma aplicação em execução. Estes são tipos comuns de ambientes na computação em nuvem:

- ambiente de desenvolvimento: uma instância de uma aplicação em execução que está disponível somente para a equipe principal responsável pela manutenção da aplicação. Ambientes de desenvolvimento são usados para testar mudanças antes de promovê-las para ambientes superiores. Esse tipo de ambiente às vezes é chamado de ambiente de teste.
- ambientes inferiores: todos os ambientes de desenvolvimento para uma aplicação, como aqueles usados para compilações e testes iniciais.
- ambiente de produção: uma instância de uma aplicação em execução que os usuários finais podem acessar. Em um pipeline de CI/CD, o ambiente de produção é o último ambiente de implantação.
- ambientes superiores: todos os ambientes que podem ser acessados por usuários que não sejam a equipe principal de desenvolvimento. Isso pode incluir um ambiente de produção, ambientes de pré-produção e ambientes para testes de aceitação do usuário.

epic

Em metodologias ágeis, categorias funcionais que ajudam a organizar e priorizar seu trabalho. Os epics fornecem uma descrição de alto nível dos requisitos e das tarefas de implementação. Por exemplo, os épicos de segurança AWS da CAF incluem gerenciamento de identidade e acesso, controles de detetive, segurança de infraestrutura, proteção de dados e resposta a incidentes. Para obter mais informações sobre epics na estratégia de migração da AWS , consulte o guia de implementação do programa.

ERP

Consulte planejamento de recursos corporativos.

análise exploratória de dados (EDA)

O processo de analisar um conjunto de dados para entender suas principais características. Você coleta ou agrega dados e, em seguida, realiza investigações iniciais para encontrar padrões,

detectar anomalias e verificar suposições. O EDA é realizado por meio do cálculo de estatísticas resumidas e da criação de visualizações de dados.

F

tabela de fatos

A tabela central em um esquema em estrela. Ele armazena dados quantitativos sobre operações comerciais. Normalmente, uma tabela de fatos contém dois tipos de colunas: aquelas que contêm medidas e aquelas que contêm uma chave externa para uma tabela de dimensões.

falham rapidamente

Uma filosofia que usa testes frequentes e incrementais para reduzir o ciclo de vida do desenvolvimento. É uma parte essencial de uma abordagem ágil.

limite de isolamento de falhas

No Nuvem AWS, um limite, como uma zona de disponibilidade, Região da AWS um plano de controle ou um plano de dados, que limita o efeito de uma falha e ajuda a melhorar a resiliência das cargas de trabalho. Para obter mais informações, consulte Limites de isolamento de AWS falhas.

ramificação de recursos

Veja a filial.

recursos

Os dados de entrada usados para fazer uma previsão. Por exemplo, em um contexto de manufatura, os recursos podem ser imagens capturadas periodicamente na linha de fabricação.

importância do recurso

O quanto um recurso é importante para as previsões de um modelo. Isso geralmente é expresso como uma pontuação numérica que pode ser calculada por meio de várias técnicas, como Shapley Additive Explanations (SHAP) e gradientes integrados. Para obter mais informações, consulte Interpretabilidade do modelo de aprendizado de máquina com:AWS.

transformação de recursos

O processo de otimizar dados para o processo de ML, incluindo enriquecer dados com fontes adicionais, escalar valores ou extrair vários conjuntos de informações de um único

campo de dados. Isso permite que o modelo de ML se beneficie dos dados. Por exemplo, se a data “2021-05-27 00:15:37” for dividida em “2021”, “maio”, “quinta” e “15”, isso poderá ajudar o algoritmo de aprendizado a aprender padrões diferenciados associados a diferentes componentes de dados.

FGAC

Veja o controle de acesso refinado.

Controle de acesso refinado (FGAC)

O uso de várias condições para permitir ou negar uma solicitação de acesso.

migração flash-cut

Um método de migração de banco de dados que usa replicação contínua de dados por meio da captura de dados alterados para migrar dados no menor tempo possível, em vez de usar uma abordagem em fases. O objetivo é reduzir ao mínimo o tempo de inatividade.

G

bloqueio geográfico

Veja as restrições geográficas.

restrições geográficas (bloqueio geográfico)

Na Amazon CloudFront, uma opção para impedir que usuários em países específicos acessem distribuições de conteúdo. É possível usar uma lista de permissões ou uma lista de bloqueios para especificar países aprovados e banidos. Para obter mais informações, consulte Restringir a distribuição geográfica do seu conteúdo na CloudFront documentação.

Fluxo de trabalho do GitFlow

Uma abordagem na qual ambientes inferiores e superiores usam ramificações diferentes em um repositório de código-fonte. O fluxo de trabalho do Gitflow é considerado legado, e o fluxo de trabalho baseado em troncos é a abordagem moderna e preferida.

estratégia greenfield

A ausência de infraestrutura existente em um novo ambiente. Ao adotar uma estratégia greenfield para uma arquitetura de sistema, é possível selecionar todas as novas tecnologias sem a

restrição da compatibilidade com a infraestrutura existente, também conhecida como brownfield. Se estiver expandindo a infraestrutura existente, poderá combinar as estratégias brownfield e greenfield.

barreira de proteção

Uma regra de alto nível que ajuda a gerenciar recursos, políticas e conformidade em todas as unidades organizacionais (UOs). Barreiras de proteção preventivas impõem políticas para garantir o alinhamento a padrões de conformidade. Elas são implementadas usando políticas de controle de serviço e limites de permissões do IAM. Barreiras de proteção detectivas detectam violações de políticas e problemas de conformidade e geram alertas para remediação. Eles são implementados usando AWS Config, AWS Security Hub, Amazon GuardDuty AWS Trusted Advisor, Amazon Inspector e verificações personalizadas AWS Lambda .

H

HA

Veja a alta disponibilidade.

migração heterogênea de bancos de dados

Migrar seu banco de dados de origem para um banco de dados de destino que usa um mecanismo de banco de dados diferente (por exemplo, Oracle para Amazon Aurora). A migração heterogênea geralmente faz parte de um esforço de redefinição da arquitetura, e converter o esquema pode ser uma tarefa complexa. O AWS fornece o AWS SCT para ajudar nas conversões de esquemas.

alta disponibilidade (HA)

A capacidade de uma workload operar continuamente, sem intervenção, em caso de desafios ou desastres. Os sistemas AH são projetados para realizar o failover automático, oferecer consistentemente desempenho de alta qualidade e lidar com diferentes cargas e falhas com impacto mínimo no desempenho.

modernização de historiador

Uma abordagem usada para modernizar e atualizar os sistemas de tecnologia operacional (OT) para melhor atender às necessidades do setor de manufatura. Um historiador é um tipo de banco de dados usado para coletar e armazenar dados de várias fontes em uma fábrica.

migração homogênea de bancos de dados

Migrar seu banco de dados de origem para um banco de dados de destino que compartilha o mesmo mecanismo de banco de dados (por exemplo, Microsoft SQL Server para Amazon RDS para SQL Server). A migração homogênea geralmente faz parte de um esforço de redefinição da hospedagem ou da plataforma. É possível usar utilitários de banco de dados nativos para migrar o esquema.

dados quentes

Dados acessados com frequência, como dados em tempo real ou dados translacionais recentes. Esses dados normalmente exigem uma camada ou classe de armazenamento de alto desempenho para fornecer respostas rápidas às consultas.

hotfix

Uma correção urgente para um problema crítico em um ambiente de produção. Devido à sua urgência, um hotfix geralmente é feito fora do fluxo de trabalho típico de uma DevOps versão.

período de hipercuidados

Imediatamente após a substituição, o período em que uma equipe de migração gerencia e monitora as aplicações migradas na nuvem para resolver quaisquer problemas. Normalmente, a duração desse período é de 1 a 4 dias. No final do período de hipercuidados, a equipe de migração normalmente transfere a responsabilidade pelas aplicações para a equipe de operações de nuvem.

I

IaC

Veja a infraestrutura como código.

Política baseada em identidade

Uma política anexada a um ou mais diretores do IAM que define suas permissões no Nuvem AWS ambiente.

aplicação ociosa

Uma aplicação que tem um uso médio de CPU e memória entre 5 e 20% em um período de 90 dias. Em um projeto de migração, é comum retirar essas aplicações ou retê-las on-premises.

IIoT

Veja a Internet das Coisas industrial.

infraestrutura imutável

Um modelo que implanta uma nova infraestrutura para cargas de trabalho de produção em vez de atualizar, corrigir ou modificar a infraestrutura existente. Infraestruturas imutáveis são inerentemente mais consistentes, confiáveis e previsíveis do que infraestruturas mutáveis. Para obter mais informações, consulte as melhores práticas de implantação usando infraestrutura imutável no Well-Architected AWS Framework.

VPC de entrada (admissão)

Em uma arquitetura de AWS várias contas, uma VPC que aceita, inspeciona e roteia conexões de rede de fora de um aplicativo. A Arquitetura de referência de segurança da AWS recomenda configurar sua conta de rede com VPCs de entrada, saída e inspeção para proteger a interface bidirecional entre a aplicação e a Internet em geral.

migração incremental

Uma estratégia de substituição na qual você migra a aplicação em pequenas partes, em vez de realizar uma única substituição completa. Por exemplo, é possível mover inicialmente apenas alguns microsserviços ou usuários para o novo sistema. Depois de verificar se tudo está funcionando corretamente, mova os microsserviços ou usuários adicionais de forma incremental até poder descomissionar seu sistema herdado. Essa estratégia reduz os riscos associados a migrações de grande porte.

Indústria 4.0

Um termo que foi introduzido por Klaus Schwab em 2016 para se referir à modernização dos processos de fabricação por meio de avanços em conectividade, dados em tempo real, automação, análise e IA/ML.

infraestrutura

Todos os recursos e ativos contidos no ambiente de uma aplicação.

Infraestrutura como código (IaC)

O processo de provisionamento e gerenciamento da infraestrutura de uma aplicação por meio de um conjunto de arquivos de configuração. A IaC foi projetada para ajudar você a centralizar

o gerenciamento da infraestrutura, padronizar recursos e escalar rapidamente para que novos ambientes sejam reproduzíveis, confiáveis e consistentes.

Internet das Coisas Industrial (IIoT)

O uso de sensores e dispositivos conectados à Internet nos setores industriais, como manufatura, energia, automotivo, saúde, ciências biológicas e agricultura. Para obter mais informações, consulte Construir uma estratégia de transformação digital para a Internet das Coisas Industrial (IIoT).

VPC de inspeção

Em uma arquitetura de AWS várias contas, uma VPC centralizada que gerencia as inspeções do tráfego de rede entre VPCs (na mesma ou em diferentes Regiões da AWS), a Internet e as redes locais. A Arquitetura de referência de segurança da AWS recomenda configurar sua conta de rede com VPCs de entrada, saída e inspeção para proteger a interface bidirecional entre a aplicação e a Internet em geral.

Internet das Coisas (IoT)

A rede de objetos físicos conectados com sensores ou processadores incorporados que se comunicam com outros dispositivos e sistemas pela Internet ou por uma rede de comunicação local. Para obter mais informações, consulte O que é IoT?

interpretabilidade

Uma característica de um modelo de machine learning que descreve o grau em que um ser humano pode entender como as previsões do modelo dependem de suas entradas. Para obter mais informações, consulte Interpretabilidade do modelo de machine learning com a AWS.

IoT

Consulte Internet das Coisas.

Biblioteca de informações de TI (ITIL)

Um conjunto de práticas recomendadas para fornecer serviços de TI e alinhar esses serviços a requisitos de negócios. A ITIL fornece a base para o ITSM.

Gerenciamento de serviços de TI (ITSM)

Atividades associadas a design, implementação, gerenciamento e suporte de serviços de TI para uma organização. Para obter informações sobre a integração de operações em nuvem com ferramentas de ITSM, consulte o guia de integração de operações.

ITIL

Consulte a biblioteca de informações de TI.

ITSM

Veja o gerenciamento de serviços de TI.

L

controle de acesso baseado em etiqueta (LBAC)

Uma implementação do controle de acesso obrigatório (MAC) em que os usuários e os dados em si recebem explicitamente um valor de etiqueta de segurança. A interseção entre a etiqueta de segurança do usuário e a etiqueta de segurança dos dados determina quais linhas e colunas podem ser vistas pelo usuário.

zona de pouso

Uma landing zone é um AWS ambiente bem arquitetado, com várias contas, escalável e seguro. Um ponto a partir do qual suas organizações podem iniciar e implantar rapidamente workloads e aplicações com confiança em seu ambiente de segurança e infraestrutura. Para obter mais informações sobre zonas de pouso, consulte Configurar um ambiente da AWS com várias contas seguro e escalável.

migração de grande porte

Uma migração de 300 servidores ou mais.

LBAC

Veja controle de acesso baseado em etiquetas.

privilégio mínimo

A prática recomendada de segurança de conceder as permissões mínimas necessárias para executar uma tarefa. Para obter mais informações, consulte Aplicar permissões de privilégios mínimos na documentação do IAM.

mover sem alterações (lift-and-shift)

Veja 7 Rs.

sistema little-endian

Um sistema que armazena o byte menos significativo antes. Veja também endianness.

ambientes inferiores

Veja o ambiente.

M

machine learning (ML)

Um tipo de inteligência artificial que usa algoritmos e técnicas para reconhecimento e aprendizado de padrões. O ML analisa e aprende com dados gravados, por exemplo, dados da Internet das Coisas (IoT), para gerar um modelo estatístico baseado em padrões. Para obter mais informações, consulte Machine learning.

ramificação principal

Veja a filial.

malware

Software projetado para comprometer a segurança ou a privacidade do computador. O malware pode interromper os sistemas do computador, vazar informações confidenciais ou obter acesso não autorizado. Exemplos de malware incluem vírus, worms, ransomware, cavalos de Tróia, spyware e keyloggers.

serviços gerenciados

Serviços da AWS para o qual AWS opera a camada de infraestrutura, o sistema operacional e as plataformas, e você acessa os endpoints para armazenar e recuperar dados. O Amazon Simple Storage Service (Amazon S3) e o Amazon DynamoDB são exemplos de serviços gerenciados. Eles também são conhecidos como serviços abstratos.

sistema de execução de manufatura (MES)

Um sistema de software para rastrear, monitorar, documentar e controlar processos de produção que convertem matérias-primas em produtos acabados no chão de fábrica.

MAP

Consulte Migration Acceleration Program.

mecanismo

Um processo completo no qual você cria uma ferramenta, impulsiona a adoção da ferramenta e, em seguida, inspeciona os resultados para fazer ajustes. Um mecanismo é um ciclo que se reforça e se aprimora à medida que opera. Para obter mais informações, consulte Construindo mecanismos no AWS Well-Architected Framework.

conta-membro

Todos, Contas da AWS exceto a conta de gerenciamento, que fazem parte de uma organização em AWS Organizations. Uma conta só pode ser membro de uma organização de cada vez.

MES

Veja o sistema de execução de manufatura.

Transporte de telemetria de enfileiramento de mensagens (MQTT)

Um protocolo de comunicação leve machine-to-machine (M2M), baseado no padrão de publicação/assinatura, para dispositivos de IoT com recursos limitados.

microsserviço

Um serviço pequeno e independente que se comunica por meio de APIs bem definidas e normalmente pertence a equipes pequenas e autônomas. Por exemplo, um sistema de seguradora pode incluir microsserviços que mapeiam as capacidades comerciais, como vendas ou marketing, ou subdomínios, como compras, reclamações ou análises. Os benefícios dos microsserviços incluem agilidade, escalabilidade flexível, fácil implantação, código reutilizável e resiliência. Para obter mais informações, consulte Integração de microsserviços usando serviços sem AWS servidor.

arquitetura de microsserviços

Uma abordagem à criação de aplicações com componentes independentes que executam cada processo de aplicação como um microsserviço. Esses microsserviços se comunicam por meio de uma interface bem definida usando APIs leves. Cada microsserviço nessa arquitetura pode ser atualizado, implantado e escalado para atender à demanda por funções específicas de uma aplicação. Para obter mais informações, consulte Implementação de microsserviços em. AWS

Programa de Aceleração da Migração (MAP)

Um AWS programa que fornece suporte de consultoria, treinamento e serviços para ajudar as organizações a criar uma base operacional sólida para migrar para a nuvem e ajudar a

compensar o custo inicial das migrações. O MAP inclui uma metodologia de migração para executar migrações legadas de forma metódica e um conjunto de ferramentas para automatizar e acelerar cenários comuns de migração.

migração em escala

O processo de mover a maior parte do portfólio de aplicações para a nuvem em ondas, com mais aplicações sendo movidas em um ritmo mais rápido a cada onda. Essa fase usa as práticas recomendadas e lições aprendidas nas fases anteriores para implementar uma fábrica de migração de equipes, ferramentas e processos para agilizar a migração de workloads por meio de automação e entrega ágeis. Esta é a terceira fase da estratégia de migração para a AWS.

fábrica de migração

Equipes multifuncionais que simplificam a migração de workloads por meio de abordagens automatizadas e ágeis. As equipes da fábrica de migração geralmente incluem operações, analistas e proprietários de negócios, engenheiros de migração, desenvolvedores e DevOps profissionais que trabalham em sprints. Entre 20 e 50% de um portfólio de aplicações corporativas consiste em padrões repetidos que podem ser otimizados por meio de uma abordagem de fábrica. Para obter mais informações, consulte discussão sobre fábricas de migração e o guia do Cloud Migration Factory neste conjunto de conteúdo.

metadados de migração

As informações sobre a aplicação e o servidor necessárias para concluir a migração. Cada padrão de migração exige um conjunto de metadados de migração diferente. Exemplos de metadados de migração incluem a sub-rede, o grupo de segurança e AWS a conta de destino.

padrão de migração

Uma tarefa de migração repetível que detalha a estratégia de migração, o destino da migração e a aplicação ou o serviço de migração usado. Exemplo: rehospede a migração para o Amazon EC2 AWS com o Application Migration Service.

Avaliação de Portfólio para Migração (MPA)

Uma ferramenta on-line que fornece informações para validar o caso de negócios para migrar para o. Nuvem AWS O MPA fornece avaliação detalhada do portfólio (dimensionamento correto do servidor, preços, comparações de TCO, análise de custos de migração), bem como planejamento de migração (análise e coleta de dados de aplicações, agrupamento de aplicações, priorização de migração e planejamento de ondas). A ferramenta MPA (requer login) está disponível gratuitamente para todos os AWS consultores e consultores parceiros da APN.

Avaliação de Preparação para Migração (MRA)

O processo de obter insights sobre o status de prontidão de uma organização para a nuvem, identificar pontos fortes e fracos e criar um plano de ação para fechar as lacunas identificadas, usando o CAF. AWS Para mais informações, consulte o guia de preparação para migração. A MRA é a primeira fase da estratégia de migração para a AWS.

estratégia de migração

A abordagem usada para migrar uma carga de trabalho para o. Nuvem AWS Para obter mais informações, consulte a entrada de 7 Rs neste glossário e consulte Mobilize sua organização para acelerar migrações em grande escala.

ML

Veja o aprendizado de máquina.

modernização

Transformar uma aplicação desatualizada (herdada ou monolítica) e sua infraestrutura em um sistema ágil, elástico e altamente disponível na nuvem para reduzir custos, ganhar eficiência e aproveitar as inovações. Para obter mais informações, consulte Estratégia para modernizar aplicativos no Nuvem AWS.

avaliação de preparação para modernização

Uma avaliação que ajuda a determinar a preparação para modernização das aplicações de uma organização. Ela identifica benefícios, riscos e dependências e determina o quão bem a organização pode acomodar o estado futuro dessas aplicações. O resultado da avaliação é um esquema da arquitetura de destino, um roteiro que detalha as fases de desenvolvimento e os marcos do processo de modernização e um plano de ação para abordar as lacunas identificadas. Para obter mais informações, consulte Avaliação da prontidão para modernização de aplicativos no. Nuvem AWS

aplicações monolíticas (monólitos)

Aplicações que são executadas como um único serviço com processos fortemente acoplados. As aplicações monolíticas apresentam várias desvantagens. Se um recurso da aplicação apresentar um aumento na demanda, toda a arquitetura deverá ser escalada. Adicionar ou melhorar os recursos de uma aplicação monolítica também se torna mais complexo quando a base de código cresce. Para resolver esses problemas, é possível criar uma arquitetura de microsserviços. Para obter mais informações, consulte Decompor monólitos em microsserviços.

MAPA

Consulte Avaliação do portfólio de migração.

MQTT

Consulte Transporte de telemetria de enfileiramento de mensagens.

classificação multiclasse

Um processo que ajuda a gerar previsões para várias classes (prevendo um ou mais de dois resultados). Por exemplo, um modelo de ML pode perguntar “Este produto é um livro, um carro ou um telefone?” ou “Qual categoria de produtos é mais interessante para este cliente?”

infraestrutura mutável

Um modelo que atualiza e modifica a infraestrutura existente para cargas de trabalho de produção. Para melhorar a consistência, confiabilidade e previsibilidade, o AWS Well-Architected Framework recomenda o uso de infraestrutura imutável como uma prática recomendada.

O

OAC

Veja o controle de acesso de origem.

CARVALHO

Veja a identidade de acesso de origem.

OCM

Veja o gerenciamento de mudanças organizacionais.

migração offline

Um método de migração no qual a workload de origem é desativada durante o processo de migração. Esse método envolve tempo de inatividade prolongado e geralmente é usado para workloads pequenas e não críticas.

OI

Veja a integração de operações.

OLA

Veja o contrato em nível operacional.

migração online

Um método de migração no qual a workload de origem é copiada para o sistema de destino sem ser colocada offline. As aplicações conectadas à workload podem continuar funcionando durante a migração. Esse método envolve um tempo de inatividade nulo ou mínimo e normalmente é usado para workloads essenciais para a produção.

OPC-UA

Consulte Comunicação de processo aberto — Arquitetura unificada.

Comunicação de processo aberto — Arquitetura unificada (OPC-UA)

Um protocolo de comunicação machine-to-machine (M2M) para automação industrial. O OPC-UA fornece um padrão de interoperabilidade com esquemas de criptografia, autenticação e autorização de dados.

acordo de nível operacional (OLA)

Um acordo que esclarece o que os grupos funcionais de TI prometem oferecer uns aos outros para apoiar um acordo de serviço (SLA).

análise de prontidão operacional (ORR)

Uma lista de verificação de perguntas e melhores práticas associadas que ajudam você a entender, avaliar, prevenir ou reduzir o escopo de incidentes e possíveis falhas. Para obter mais informações, consulte Operational Readiness Reviews (ORR) no Well-Architected AWS Framework.

tecnologia operacional (OT)

Sistemas de hardware e software que funcionam com o ambiente físico para controlar operações, equipamentos e infraestrutura industriais. Na manufatura, a integração dos sistemas OT e de tecnologia da informação (TI) é o foco principal das transformações da Indústria 4.0.

integração de operações (OI)

O processo de modernização das operações na nuvem, que envolve planejamento de preparação, automação e integração. Para obter mais informações, consulte o guia de integração de operações.

trilha organizacional

Uma trilha criada por ela AWS CloudTrail registra todos os eventos de todos Contas da AWS em uma organização em AWS Organizations. Essa trilha é criada em cada Conta da AWS que faz parte da organização e monitora a atividade em cada conta. Para obter mais informações, consulte Criação de uma trilha para uma organização na CloudTrail documentação.

gerenciamento de alterações organizacionais (OCM)

Uma estrutura para gerenciar grandes transformações de negócios disruptivas de uma perspectiva de pessoas, cultura e liderança. O OCM ajuda as organizações a se prepararem e fazerem a transição para novos sistemas e estratégias, acelerando a adoção de alterações, abordando questões de transição e promovendo mudanças culturais e organizacionais. Na estratégia de AWS migração, essa estrutura é chamada de aceleração de pessoas, devido à velocidade de mudança exigida nos projetos de adoção da nuvem. Para obter mais informações, consulte o guia do OCM.

controle de acesso de origem (OAC)

Em CloudFront, uma opção aprimorada para restringir o acesso para proteger seu conteúdo do Amazon Simple Storage Service (Amazon S3). O OAC oferece suporte a todos os buckets S3 Regiões da AWS, criptografia do lado do servidor com AWS KMS (SSE-KMS) e solicitações dinâmicas ao bucket S3. `PUT` `DELETE`

Identidade do acesso de origem (OAI)

Em CloudFront, uma opção para restringir o acesso para proteger seu conteúdo do Amazon S3. Quando você usa o OAI, CloudFront cria um principal com o qual o Amazon S3 pode se autenticar. Os diretores autenticados podem acessar o conteúdo em um bucket do S3 somente por meio de uma distribuição específica. CloudFront Veja também OAC, que fornece um controle de acesso mais granular e aprimorado.

OU

Veja a análise de prontidão operacional.

NÃO

Veja a tecnologia operacional.

VPC de saída (egresso)

Em uma arquitetura de AWS várias contas, uma VPC que gerencia conexões de rede que são iniciadas de dentro de um aplicativo. A Arquitetura de referência de segurança da AWS

recomenda configurar sua conta de rede com VPCs de entrada, saída e inspeção para proteger a interface bidirecional entre a aplicação e a Internet em geral.

P

limite de permissões

Uma política de gerenciamento do IAM anexada a entidades principais do IAM para definir as permissões máximas que o usuário ou perfil podem ter. Para obter mais informações, consulte Limites de permissões na documentação do IAM.

Informações de identificação pessoal (PII)

Informações que, quando visualizadas diretamente ou combinadas com outros dados relacionados, podem ser usadas para inferir razoavelmente a identidade de um indivíduo. Exemplos de PII incluem nomes, endereços e informações de contato.

PII

Veja informações de identificação pessoal.

manual

Um conjunto de etapas predefinidas que capturam o trabalho associado às migrações, como a entrega das principais funções operacionais na nuvem. Um manual pode assumir a forma de scripts, runbooks automatizados ou um resumo dos processos ou etapas necessários para operar seu ambiente modernizado.

PLC

Consulte controlador lógico programável.

AMEIXA

Veja o gerenciamento do ciclo de vida do produto.

política

Um objeto que pode definir permissões (consulte a política baseada em identidade), especificar as condições de acesso (consulte a política baseada em recursos) ou definir as permissões máximas para todas as contas em uma organização em AWS Organizations (consulte a política de controle de serviços).

persistência poliglota

Escolher de forma independente a tecnologia de armazenamento de dados de um microsserviço com base em padrões de acesso a dados e outros requisitos. Se seus microsserviços tiverem a mesma tecnologia de armazenamento de dados, eles poderão enfrentar desafios de implementação ou apresentar baixa performance. Os microsserviços serão implementados com mais facilidade e alcançarão performance e escalabilidade melhores se usarem o armazenamento de dados mais bem adaptado às suas necessidades. Para obter mais informações, consulte Habilitar a persistência de dados em microsserviços.

avaliação do portfólio

Um processo de descobrir, analisar e priorizar o portfólio de aplicações para planejar a migração. Para obter mais informações, consulte Avaliar a preparação para a migração.

predicado

Uma condição de consulta que retorna `true` ou`false`, normalmente localizada em uma `WHERE` cláusula.

pressão de predicados

Uma técnica de otimização de consulta de banco de dados que filtra os dados na consulta antes da transferência. Isso reduz a quantidade de dados que devem ser recuperados e processados do banco de dados relacional e melhora o desempenho das consultas.

controle preventivo

Um controle de segurança projetado para evitar que um evento ocorra. Esses controles são a primeira linha de defesa para ajudar a evitar acesso não autorizado ou alterações indesejadas em sua rede. Para obter mais informações, consulte Controles preventivos em Como implementar controles de segurança na AWS.

principal (entidade principal)

Uma entidade AWS que pode realizar ações e acessar recursos. Essa entidade geralmente é um usuário raiz para um Conta da AWS, uma função do IAM ou um usuário. Para obter mais informações, consulte Entidade principal em Termos e conceitos de perfis na documentação do IAM.

Privacidade por design

Uma abordagem em engenharia de sistemas que leva em consideração a privacidade em todo o processo de engenharia.

zonas hospedadas privadas

Um contêiner que armazena informações sobre como você quer que o Amazon Route 53 responda a consultas ao DNS para um domínio e seus subdomínios dentro de uma ou mais VPCs. Para obter mais informações, consulte Como trabalhar com zonas hospedadas privadas na documentação do Route 53.

controle proativo

Um controle de segurança projetado para impedir a implantação de recursos não compatíveis. Esses controles examinam os recursos antes de serem provisionados. Se o recurso não estiver em conformidade com o controle, ele não será provisionado. Para obter mais informações, consulte o guia de referência de controles na AWS Control Tower documentação e consulte Controles proativos em Implementação de controles de segurança em AWS.

gerenciamento do ciclo de vida do produto (PLM)

O gerenciamento de dados e processos de um produto em todo o seu ciclo de vida, desde o design, desenvolvimento e lançamento, passando pelo crescimento e maturidade, até o declínio e a remoção.

ambiente de produção

Veja o ambiente.

controlador lógico programável (PLC)

Na fabricação, um computador altamente confiável e adaptável que monitora as máquinas e automatiza os processos de fabricação.

pseudonimização

O processo de substituir identificadores pessoais em um conjunto de dados por valores de espaço reservado. A pseudonimização pode ajudar a proteger a privacidade pessoal. Os dados pseudonimizados ainda são considerados dados pessoais.

publicar/assinar (pub/sub)

Um padrão que permite comunicações assíncronas entre microsserviços para melhorar a escalabilidade e a capacidade de resposta. Por exemplo, em um MES baseado em microsserviços, um microsserviço pode publicar mensagens de eventos em um canal no qual outros microsserviços possam se inscrever. O sistema pode adicionar novos microsserviços sem alterar o serviço de publicação.

Q

plano de consulta

Uma série de etapas, como instruções, usadas para acessar os dados em um sistema de banco de dados relacional SQL.

regressão de planos de consultas

Quando um otimizador de serviço de banco de dados escolhe um plano menos adequado do que escolhia antes de uma determinada alteração no ambiente de banco de dados ocorrer. Isso pode ser causado por alterações em estatísticas, restrições, configurações do ambiente, associações de parâmetros de consulta e atualizações do mecanismo de banco de dados.

R

Matriz RACI

Veja responsável, responsável, consultado, informado (RACI).

ransomware

Um software mal-intencionado desenvolvido para bloquear o acesso a um sistema ou dados de computador até que um pagamento seja feito.

Matriz RASCI

Veja responsável, responsável, consultado, informado (RACI).

RCAC

Veja o controle de acesso por linha e coluna.

réplica de leitura

Uma cópia de um banco de dados usada somente para leitura. É possível encaminhar consultas para a réplica de leitura e reduzir a carga no banco de dados principal.

rearquiteta

Veja 7 Rs.

objetivo de ponto de recuperação (RPO).

O máximo período de tempo aceitável desde o último ponto de recuperação de dados. Isso determina o que é considerado uma perda aceitável de dados entre o último ponto de recuperação e a interrupção do serviço.

objetivo de tempo de recuperação (RTO)

O máximo atraso aceitável entre a interrupção e a restauração do serviço.

refatorar

Veja 7 Rs.

Região

Uma coleção de AWS recursos em uma área geográfica. Cada um Região da AWS é isolado e independente dos outros para fornecer tolerância a falhas, estabilidade e resiliência. Para obter mais informações, consulte Especificar o que Regiões da AWS sua conta pode usar.

regressão

Uma técnica de ML que prevê um valor numérico. Por exemplo, para resolver o problema de “Por qual preço esta casa será vendida?” um modelo de ML pode usar um modelo de regressão linear para prever o preço de venda de uma casa com base em fatos conhecidos sobre a casa (por exemplo, a metragem quadrada).

redefinir a hospedagem

Veja 7 Rs.

versão

Em um processo de implantação, o ato de promover mudanças em um ambiente de produção.

realocar

Veja 7 Rs.

redefinir a plataforma

Veja 7 Rs.

recomprar

Veja 7 Rs.

resiliência

A capacidade de um aplicativo de resistir ou se recuperar de interrupções. Alta disponibilidade e recuperação de desastres são considerações comuns ao planejar a resiliência no. Nuvem AWS Para obter mais informações, consulte Nuvem AWS Resiliência.

política baseada em recurso

Uma política associada a um recurso, como um bucket do Amazon S3, um endpoint ou uma chave de criptografia. Esse tipo de política especifica quais entidades principais têm acesso permitido, ações válidas e quaisquer outras condições que devem ser atendidas.

matriz responsável, accountable, consultada, informada (RACI)

Uma matriz que define as funções e responsabilidades de todas as partes envolvidas nas atividades de migração e nas operações de nuvem. O nome da matriz é derivado dos tipos de responsabilidade definidos na matriz: responsável (R), responsabilizável (A), consultado (C) e informado (I). O tipo de suporte (S) é opcional. Se você incluir suporte, a matriz será chamada de matriz RASCI e, se excluir, será chamada de matriz RACI.

controle responsivo

Um controle de segurança desenvolvido para conduzir a remediação de eventos adversos ou desvios em relação à linha de base de segurança. Para obter mais informações, consulte Controles responsivos em Como implementar controles de segurança na AWS.

reter

Veja 7 Rs.

aposentar-se

Veja 7 Rs.

rotação

O processo de atualizar periodicamente um segredo para dificultar o acesso das credenciais por um invasor.

controle de acesso por linha e coluna (RCAC)

O uso de expressões SQL básicas e flexíveis que tenham regras de acesso definidas. O RCAC consiste em permissões de linha e máscaras de coluna.

RPO

Veja o objetivo do ponto de recuperação.

RTO

Veja o objetivo do tempo de recuperação.

runbook

Um conjunto de procedimentos manuais ou automatizados necessários para realizar uma tarefa específica. Eles são normalmente criados para agilizar operações ou procedimentos repetitivos com altas taxas de erro.

S

SAML 2.0

Um padrão aberto que muitos provedores de identidade (IdPs) usam. Esse recurso permite o login único federado (SSO), para que os usuários possam fazer login AWS Management Console ou chamar as operações da AWS API sem que você precise criar um usuário no IAM para todos em sua organização. Para obter mais informações sobre a federação baseada em SAML 2.0, consulte Sobre a federação baseada em SAML 2.0 na documentação do IAM.

SCADA

Veja controle de supervisão e aquisição de dados.

SCP

Veja a política de controle de serviços.

secret

Em AWS Secrets Manager, informações confidenciais ou restritas, como uma senha ou credenciais de usuário, que você armazena de forma criptografada. Ele consiste no valor secreto e em seus metadados. O valor secreto pode ser binário, uma única string ou várias strings. Para obter mais informações, consulte O que há em um segredo do Secrets Manager? na documentação do Secrets Manager.

controle de segurança

Uma barreira de proteção técnica ou administrativa que impede, detecta ou reduz a capacidade de uma ameaça explorar uma vulnerabilidade de segurança. Existem quatro tipos principais de controles de segurança: preventivos, detectivos, responsivos e proativos.

fortalecimento da segurança

O processo de reduzir a superfície de ataque para torná-la mais resistente a ataques. Isso pode incluir ações como remover recursos que não são mais necessários, implementar a prática recomendada de segurança de conceder privilégios mínimos ou desativar recursos desnecessários em arquivos de configuração.

sistema de gerenciamento de eventos e informações de segurança (SIEM)

Ferramentas e serviços que combinam sistemas de gerenciamento de informações de segurança (SIM) e gerenciamento de eventos de segurança (SEM). Um sistema SIEM coleta, monitora e analisa dados de servidores, redes, dispositivos e outras fontes para detectar ameaças e violações de segurança e gerar alertas.

automação de resposta de segurança

Uma ação predefinida e programada projetada para responder ou remediar automaticamente um evento de segurança. Essas automações servem como controles de segurança responsivos ou detectivos que ajudam você a implementar as melhores práticas AWS de segurança. Exemplos de ações de resposta automatizada incluem a modificação de um grupo de segurança da VPC, a correção de uma instância do Amazon EC2 ou a rotação de credenciais.

Criptografia do lado do servidor

Criptografia dos dados em seu destino, por Serviço da AWS quem os recebe.

política de controle de serviços (SCP)

Uma política que fornece controle centralizado sobre as permissões de todas as contas em uma organização no AWS Organizations. As SCPs definem barreiras de proteção ou estabelecem limites para as ações que um administrador pode delegar a usuários ou perfis. É possível usar SCPs como listas de permissão ou de negação para especificar quais serviços ou ações são permitidos ou proibidos. Para obter mais informações, consulte Políticas de controle de serviço na AWS Organizations documentação.

service endpoint (endpoint de serviço)

O URL do ponto de entrada para um Serviço da AWS. Você pode usar o endpoint para se conectar programaticamente ao serviço de destino. Para obter mais informações, consulte Endpoints do Serviço da AWS na Referência geral da AWS.

acordo de serviço (SLA)

Um acordo que esclarece o que uma equipe de TI promete fornecer aos clientes, como tempo de atividade e performance do serviço.

indicador de nível de serviço (SLI)

Uma medida de um aspecto de desempenho de um serviço, como taxa de erro, disponibilidade ou taxa de transferência.

objetivo de nível de serviço (SLO)

Uma métrica alvo que representa a integridade de um serviço, conforme medida por um indicador de nível de serviço.

modelo de responsabilidade compartilhada

Um modelo que descreve a responsabilidade com a qual você compartilha AWS pela segurança e conformidade na nuvem. AWS é responsável pela segurança da nuvem, enquanto você é responsável pela segurança na nuvem. Para obter mais informações, consulte o Modelo de responsabilidade compartilhada.

SIEM

Veja informações de segurança e sistema de gerenciamento de eventos.

ponto único de falha (SPOF)

Uma falha em um único componente crítico de um aplicativo que pode interromper o sistema.

SLA

Veja o contrato de nível de serviço.

ESGUIO

Veja o indicador de nível de serviço.

SLO

Veja o objetivo do nível de serviço.

split-and-seed modelo

Um padrão para escalar e acelerar projetos de modernização. À medida que novos recursos e lançamentos de produtos são definidos, a equipe principal se divide para criar novas equipes

de produtos. Isso ajuda a escalar os recursos e os serviços da sua organização, melhora a produtividade do desenvolvedor e possibilita inovações rápidas. Para obter mais informações, consulte Abordagem em fases para modernizar aplicativos no. Nuvem AWS

CUSPE

Veja um único ponto de falha.

esquema de estrelas

Uma estrutura organizacional de banco de dados que usa uma grande tabela de fatos para armazenar dados transacionais ou medidos e usa uma ou mais tabelas dimensionais menores para armazenar atributos de dados. Essa estrutura foi projetada para uso em um data warehouse ou para fins de inteligência comercial.

padrão strangler fig

Uma abordagem à modernização de sistemas monolíticos que consiste em reescrever e substituir incrementalmente a funcionalidade do sistema até que o sistema herdado possa ser desativado. Esse padrão usa a analogia de uma videira que cresce e se torna uma árvore estabelecida e, eventualmente, supera e substitui sua hospedeira. O padrão foi apresentado por Martin Fowler como forma de gerenciar riscos ao reescrever sistemas monolíticos. Para ver um exemplo de como aplicar esse padrão, consulte Modernizar incrementalmente os serviços Web herdados do Microsoft ASP.NET (ASMX) usando contêineres e o Amazon API Gateway.

sub-rede

Um intervalo de endereços IP na VPC. Cada sub-rede fica alocada em uma única zona de disponibilidade.

controle de supervisão e aquisição de dados (SCADA)

Na manufatura, um sistema que usa hardware e software para monitorar ativos físicos e operações de produção.

symmetric encryption (criptografia simétrica)

Um algoritmo de criptografia que usa a mesma chave para criptografar e descriptografar dados.

testes sintéticos

Testar um sistema de forma que simule as interações do usuário para detectar possíveis problemas ou monitorar o desempenho. Você pode usar o Amazon CloudWatch Synthetics para criar esses testes.

T

tags

Pares de valores-chave que atuam como metadados para organizar seus recursos. AWS As tags podem ajudar você a gerenciar, identificar, organizar, pesquisar e filtrar recursos. Para obter mais informações, consulte Marcar seus recursos do AWS.

variável-alvo

O valor que você está tentando prever no ML supervisionado. Ela também é conhecida como variável de resultado. Por exemplo, em uma configuração de fabricação, a variável-alvo pode ser um defeito do produto.

lista de tarefas

Uma ferramenta usada para monitorar o progresso por meio de um runbook. Uma lista de tarefas contém uma visão geral do runbook e uma lista de tarefas gerais a serem concluídas. Para cada tarefa geral, ela inclui o tempo estimado necessário, o proprietário e o progresso.

ambiente de teste

Veja o ambiente.

treinamento

O processo de fornecer dados para que seu modelo de ML aprenda. Os dados de treinamento devem conter a resposta correta. O algoritmo de aprendizado descobre padrões nos dados de treinamento que mapeiam os atributos dos dados de entrada no destino (a resposta que você deseja prever). Ele gera um modelo de ML que captura esses padrões. Você pode usar o modelo de ML para obter previsões de novos dados cujo destino você não conhece.

gateway de trânsito

Um hub de trânsito de rede que pode ser usado para interconectar as VPCs e as redes on-premises. Para obter mais informações, consulte O que é um gateway de trânsito na AWS Transit Gateway documentação.

fluxo de trabalho baseado em troncos

Uma abordagem na qual os desenvolvedores criam e testam recursos localmente em uma ramificação de recursos e, em seguida, mesclam essas alterações na ramificação principal. A

ramificação principal é então criada para os ambientes de desenvolvimento, pré-produção e produção, sequencialmente.

Acesso confiável

Conceder permissões a um serviço que você especifica para realizar tarefas em sua organização AWS Organizations e em suas contas em seu nome. O serviço confiável cria um perfil vinculado ao serviço em cada conta, quando esse perfil é necessário, para realizar tarefas de gerenciamento para você. Para obter mais informações, consulte Usando AWS Organizations com outros AWS serviços na AWS Organizations documentação.

tuning (ajustar)

Alterar aspectos do processo de treinamento para melhorar a precisão do modelo de ML. Por exemplo, você pode treinar o modelo de ML gerando um conjunto de rótulos, adicionando rótulos e repetindo essas etapas várias vezes em configurações diferentes para otimizar o modelo.

equipe de duas pizzas

Uma pequena DevOps equipe que você pode alimentar com duas pizzas. Uma equipe de duas pizzas garante a melhor oportunidade possível de colaboração no desenvolvimento de software.

U

incerteza

Um conceito que se refere a informações imprecisas, incompletas ou desconhecidas que podem minar a confiabilidade dos modelos preditivos de ML. Há dois tipos de incertezas: a incerteza epistêmica é causada por dados limitados e incompletos, enquanto a incerteza aleatória é causada pelo ruído e pela aleatoriedade inerentes aos dados. Para obter mais informações, consulte o guia Como quantificar a incerteza em sistemas de aprendizado profundo.

tarefas indiferenciadas

Também conhecido como trabalho pesado, trabalho necessário para criar e operar um aplicativo, mas que não fornece valor direto ao usuário final nem oferece vantagem competitiva. Exemplos de tarefas indiferenciadas incluem aquisição, manutenção e planejamento de capacidade.

ambientes superiores

Veja o ambiente.

V

aspiração

Uma operação de manutenção de banco de dados que envolve limpeza após atualizações incrementais para recuperar armazenamento e melhorar a performance.

controle de versões

Processos e ferramentas que rastreiam mudanças, como alterações no código-fonte em um repositório.

emparelhamento de VPC

Uma conexão entre duas VPCs que permite rotear tráfego usando endereços IP privados. Para ter mais informações, consulte O que é emparelhamento de VPC? na documentação da Amazon VPC.

Vulnerabilidade

Uma falha de software ou hardware que compromete a segurança do sistema.

W

cache quente

Um cache de buffer que contém dados atuais e relevantes que são acessados com frequência. A instância do banco de dados pode ler do cache do buffer, o que é mais rápido do que ler da memória principal ou do disco.

dados mornos

Dados acessados raramente. Ao consultar esse tipo de dados, consultas moderadamente lentas geralmente são aceitáveis.

função de janela

Uma função SQL que executa um cálculo em um grupo de linhas que se relacionam de alguma forma com o registro atual. As funções de janela são úteis para processar tarefas, como calcular uma média móvel ou acessar o valor das linhas com base na posição relativa da linha atual.

workload

Uma coleção de códigos e recursos que geram valor empresarial, como uma aplicação voltada para o cliente ou um processo de back-end.

workstreams

Grupos funcionais em um projeto de migração que são responsáveis por um conjunto específico de tarefas. Cada workstream é independente, mas oferece suporte aos outros workstreams do projeto. Por exemplo, o workstream de portfólio é responsável por priorizar aplicações, planejar ondas e coletar metadados de migração. O workstream de portfólio entrega esses ativos ao workstream de migração, que então migra os servidores e as aplicações.

MINHOCA

Veja escrever uma vez, ler muitas.

WQF

Consulte o AWS Workload Qualification Framework.

escreva uma vez, leia muitas (WORM)

Um modelo de armazenamento que grava dados uma única vez e evita que os dados sejam excluídos ou modificados. Os usuários autorizados podem ler os dados quantas vezes forem necessárias, mas não podem alterá-los. Essa infraestrutura de armazenamento de dados é considerada imutável.

Z

exploração de dia zero

Um ataque, geralmente malware, que tira proveito de uma vulnerabilidade de dia zero.

vulnerabilidade de dia zero

Uma falha ou vulnerabilidade não mitigada em um sistema de produção. Os agentes de ameaças podem usar esse tipo de vulnerabilidade para atacar o sistema. Os desenvolvedores frequentemente ficam cientes da vulnerabilidade como resultado do ataque.

aplicação zumbi

Uma aplicação que tem um uso médio de CPU e memória inferior a 5%. Em um projeto de migração, é comum retirar essas aplicações.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.