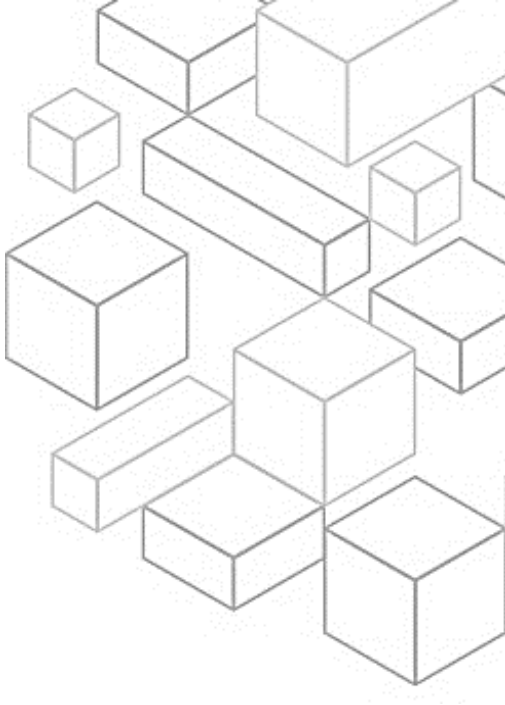


Módulo 5 - Análise detalhada do pilar de segurança

1.1 Boas-vindas!

Boas-vindas ao módulo cinco do AWS Well-Architected: Análise detalhada do pilar de segurança.

1.2 Objetivos de aprendizado

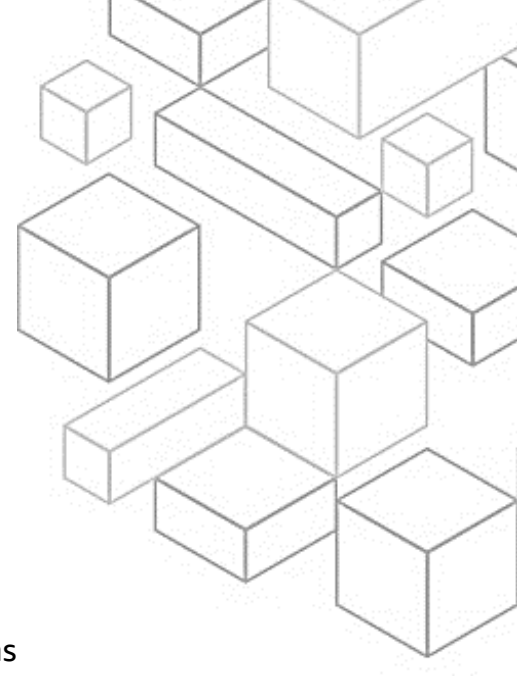
Neste módulo você terá uma visão geral do pilar de segurança do AWS Well-Architected Framework. Você também aprenderá os princípios de design e as práticas recomendadas do pilar de segurança.

1.3 Visão geral do pilar de segurança

Para começar, você terá uma visão geral do pilar de segurança.

1.4 Pilares do Well-Architected

Atualmente, há seis pilares do Well-Architected Framework: excelência operacional, segurança, confiabilidade, eficiência de desempenho, otimização de custos e sustentabilidade. Esses pilares são os fundamentos da arquitetura de suas soluções de tecnologia na nuvem. Este módulo se concentrará no pilar de segurança.



1.5 O que é o pilar de segurança?

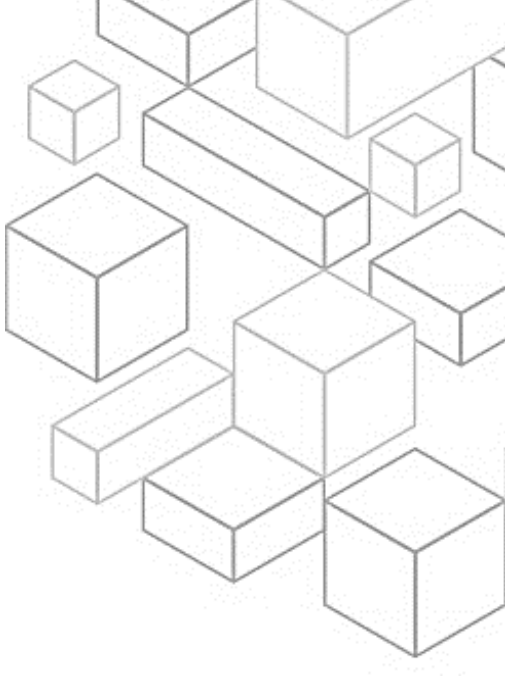
O que é o pilar de segurança? O pilar de segurança abrange a capacidade de proteger dados, sistemas e ativos na nuvem. Para operar sua carga de trabalho com segurança, você deve aplicar as práticas recomendadas abrangentes a todas as áreas de segurança.

1.6 Princípios de design de segurança

Agora que você já sabe o que é o pilar de segurança, vai se aprofundar nos princípios de design do pilar de segurança.

1.7 Segurança

Na nuvem, vários princípios podem ajudar você a fortalecer a segurança da carga de trabalho. Primeiro, implemente uma base sólida de identidade. Você pode implementar o princípio de menor privilégio e aplicar a separação de tarefas com a autorização apropriada para cada interação com os recursos da AWS. Centralize o gerenciamento de identidades e tenha como meta eliminar a dependência de credenciais estáticas de longo prazo. Segundo, ative a rastreabilidade. Você pode monitorar, alertar e fazer auditoria de ações e alterações em seu ambiente em tempo real. Integre a coleta de log e métricas com sistemas para investigar e tomar medidas automaticamente. Terceiro, aplique a segurança em todas as camadas: Aplique uma abordagem de defesa em profundidade com vários controles de segurança. Aplique controles a todas as camadas, como rede de borda, nuvem privada virtual ou VPC, balanceamento de carga, instâncias de computação, sistemas operacionais, aplicações e código. Quarto, automatize as



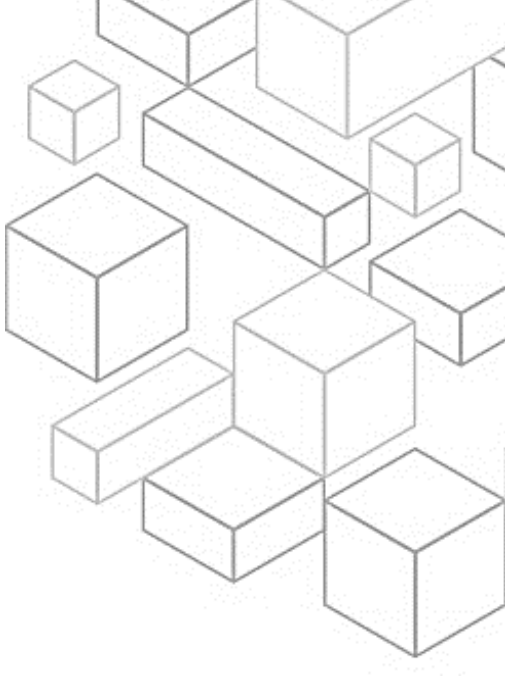
práticas de segurança. Os mecanismos automatizados de segurança baseados em software melhoram a capacidade de dimensionar com segurança de modo mais rápido e econômico. Crie arquiteturas seguras, incluindo a implantação de controles definidos e gerenciados como código em modelos com controle de versão. Quinto, proteja dados em trânsito e em repouso. Classifique seus dados em níveis de confidencialidade e use mecanismos como criptografia, tokenização e controle de acesso, conforme apropriado. Sexto, não divulgue dados. Use mecanismos e ferramentas para reduzir ou eliminar a necessidade de acesso direto ou processamento manual de dados. Isso diminui o risco de manuseio incorreto ou erro humano com dados sigilosos. Por fim, prepare-se para eventos de segurança. Prepare-se para um incidente tendo processos e uma política de investigação e gerenciamento de incidentes que estejam alinhados aos requisitos da organização. Execute simulações de resposta a incidentes e use ferramentas automatizadas para acelerar sua detecção, investigação e recuperação.

1.8 Práticas recomendadas de segurança

Agora que você entende os princípios de design de segurança, aprenderá sobre as práticas recomendadas de segurança.

1.9 Segurança

O pilar de segurança está agrupado em sete áreas de práticas recomendadas. Isso inclui fundamentos de segurança, Identity and Access Management, detecção, proteção de infraestrutura, proteção de dados, resposta a incidentes e



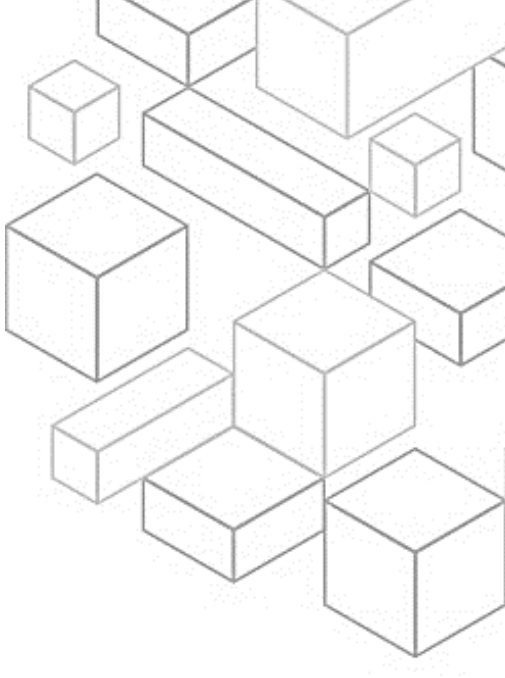
segurança de aplicações.

1.10 Fundamentos de segurança

Os fundamentos de segurança são a primeira área de práticas recomendadas de segurança.

1.11 Responsabilidade compartilhada

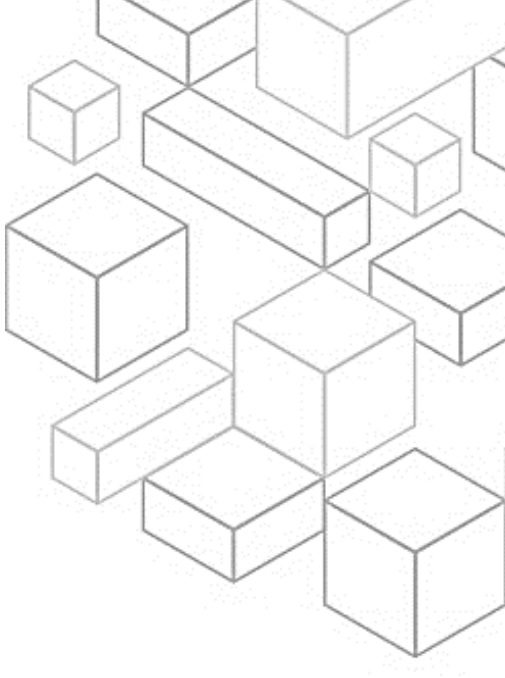
Segurança e conformidade são responsabilidades compartilhadas entre a AWS e o cliente. Esse modelo compartilhado pode auxiliar a reduzir os encargos operacionais do cliente à medida que a AWS opera, gerencia e controla os componentes do sistema operacional do host e a camada de virtualização até a segurança física das instalações em que o serviço opera. O cliente assume a responsabilidade e o gerenciamento do sistema operacional convidado (incluindo atualizações e patches de segurança) e de outros softwares de aplicações associados. O cliente também é responsável pela configuração do firewall do grupo de segurança da AWS. Os clientes devem considerar com cuidado os serviços que escolherem. As responsabilidades variam de acordo com os serviços usados, a integração desses serviços no ambiente de TI e as leis e normas aplicáveis. A natureza dessas responsabilidades compartilhadas também fornece a flexibilidade e o controle do cliente necessários para a implantação. Como mostra o gráfico, esta distinção entre responsabilidades é normalmente chamada de segurança "da" nuvem, em vez de segurança "na" nuvem. A AWS é responsável pela segurança da nuvem, protegendo a infraestrutura que executa todos os serviços oferecidos na nuvem AWS. Essa infraestrutura é composta por hardware, software, redes e instalações que executam o AWS Cloud Services. O



cliente é responsável pela segurança na nuvem. A responsabilidade dele é determinada pela seleção dos AWS Cloud Services. Isso determina a quantidade de operações de configuração que o cliente deverá executar como parte de suas responsabilidades de segurança. Por exemplo, um serviço como o Amazon Elastic Compute Cloud, ou Amazon EC2, é classificado como infraestrutura como serviço. Dessa forma, exige que o cliente execute todas as tarefas necessárias de configuração e gerenciamento de segurança. Os clientes que implantam uma instância do EC2 são responsáveis por gerenciar o sistema operacional convidado (incluindo atualizações e patches de segurança) e qualquer software ou utilitário de aplicações que instalarem nas instâncias. Eles também seriam responsáveis pela configuração do firewall fornecido pela AWS, ou grupo de segurança, em cada instância. Para serviços abstraídos, como o Amazon Simple Storage Service, ou Amazon S3, e o Amazon DynamoDB, a AWS opera a camada de infraestrutura, o sistema operacional e as plataformas. Os clientes acessam os endpoints para armazenar e recuperar dados. São responsáveis por gerenciar os dados (incluindo opções de criptografia), classificar os ativos e usar as ferramentas do AWS IAM, para aplicar as permissões apropriadas.

1.12 Separação e gerenciamento de contas da AWS

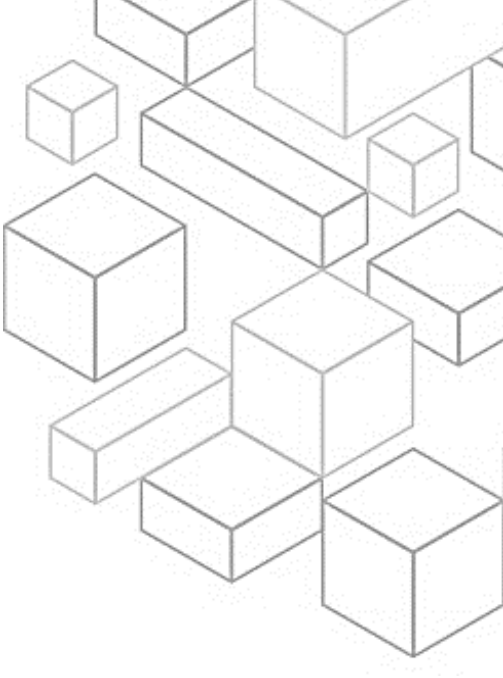
Separação e gerenciamento de contas da AWS. É uma prática recomendada organizar as cargas de trabalho em contas separadas e contas de grupo. Isso pode ser baseado na função, nos requisitos de conformidade ou em um conjunto comum de controles, em vez de espelhar a estrutura de relatórios da sua organização. Na AWS, as contas são um limite rígido. Por exemplo, a separação



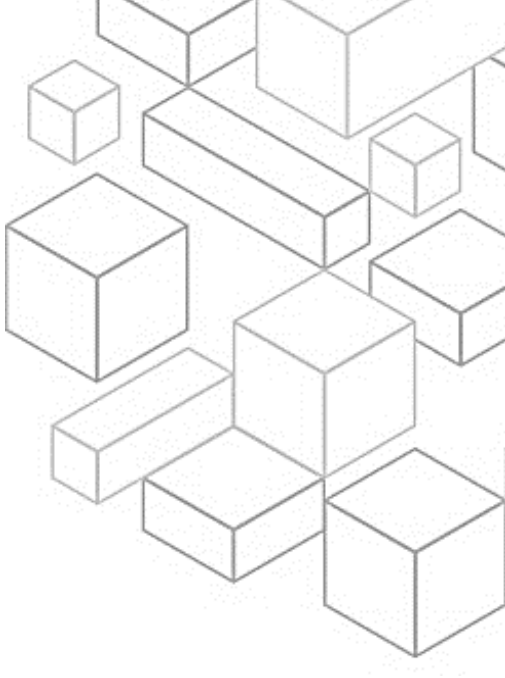
em nível de conta é altamente recomendada para isolar as cargas de trabalho de produção das cargas de trabalho de desenvolvimento e teste. Você deve gerenciar contas, definir controles e configurar serviços e recursos de forma centralizada. Para separar as cargas de trabalho usando contas, você pode estabelecer proteções comuns e isolamento entre ambientes (como produção, desenvolvimento e teste) e cargas de trabalho por meio de uma estratégia de várias contas. A separação em nível de conta é altamente recomendada porque fornece um limite de isolamento forte para segurança, faturamento e acesso. Você também deve proteger o usuário-raiz e as propriedades da conta. O usuário-raiz é o usuário mais privilegiado em uma conta AWS, com acesso administrativo total a todos os recursos da conta. Em alguns casos, ele não pode ser limitado por políticas de segurança. Você pode tomar as seguintes medidas para ajudar a reduzir o risco de exposição inadvertida de credenciais-raiz e o subsequente comprometimento do ambiente de nuvem. Desative o acesso programático ao usuário-raiz, estabeleça controles apropriados para o usuário-raiz e evite o seu uso rotineiro.

1.13 Operar suas cargas de trabalho com segurança

Para operar sua carga de trabalho com segurança, você deve aplicar as práticas recomendadas abrangentes a todas as áreas de segurança. Utilize os requisitos e processos definidos na excelência operacional em nível organizacional e de carga de trabalho e aplique-os a todas as áreas. Manter-se atualizado com as recomendações da AWS e do setor e com a inteligência sobre ameaças ajuda a desenvolver o seu modelo de ameaças e os objetivos de controle. Automatizar processos de segurança, testes e validação ajuda a dimensionar suas operações



de segurança. Considere as seguintes práticas recomendadas para operar sua carga de trabalho com segurança. Primeiro, identifique e valide os objetivos de controle. Com base nos requisitos de conformidade e nos riscos identificados no modelo de ameaças, obtenha e valide os objetivos de controle e os controles que você precisa aplicar à sua carga de trabalho. A validação contínua de objetivos de controle e controles ajudam a medir a eficácia da mitigação de riscos. Para ajudar você a definir e implementar controles adequados, reconheça os vetores de ataque mantendo-se atualizado com as ameaças de segurança mais recentes. Mantenha-se atualizado sobre as recomendações de segurança da AWS e do setor para aprimorar o procedimento de segurança de sua carga de trabalho. Automatize testes e validação de controles de segurança em pipelines. Estabeleça linhas de base e modelos seguros para mecanismos de segurança que são testados e validados como parte de sua construção, pipelines e processos. Use ferramentas e automação para testar e validar continuamente todos os controles de segurança. Identifique as ameaças e priorize as atenuações usando um modelo de ameaças. Realize a modelagem de ameaças para identificar e manter um registro atualizado de possíveis ameaças e atenuações associadas à sua carga de trabalho. Priorize ameaças e adapte mitigações de controle de segurança para prevenir, detectar e responder. Revisite-as e mantenha-as no contexto de sua carga de trabalho e do cenário de segurança em evolução. Avalie e implemente serviços e recursos de segurança da AWS e dos parceiros da AWS para ajudar você a aprimorar o procedimento de segurança de sua carga de trabalho.

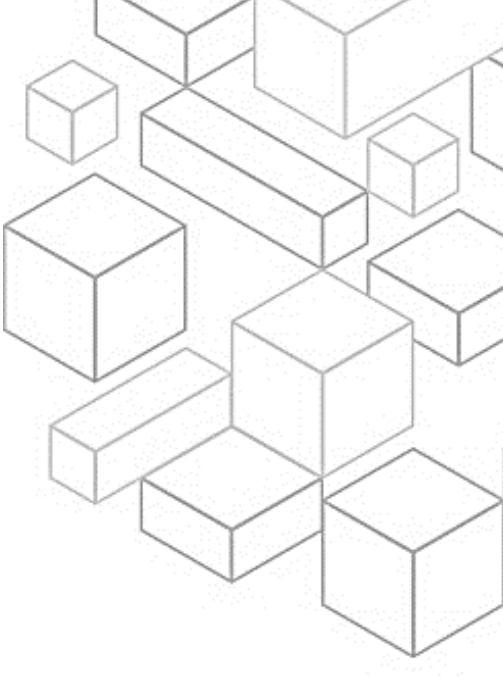


1.14 Identity and Access Management

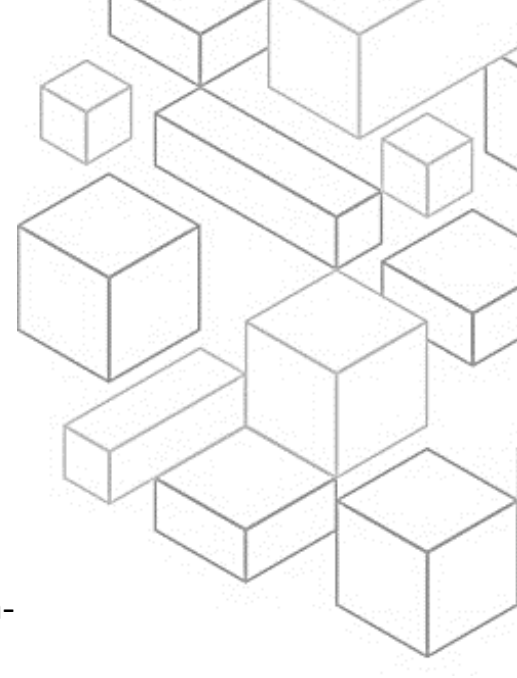
A próxima área de práticas recomendadas de segurança é o Identity and Access Management. Para usar os serviços da AWS, você deve conceder aos seus usuários e aplicações acesso aos recursos nas suas contas AWS. À medida que você executa mais cargas de trabalho na AWS, precisa de gerenciamento de identidade e permissões robustos para garantir que as pessoas certas tenham acesso aos recursos certos nas condições certas. A AWS oferece uma grande variedade de recursos para ajudar você a gerenciar suas identidades humanas e de máquina e suas permissões. As práticas recomendadas para esses recursos se enquadram em duas áreas principais: gerenciamento de identidade e gerenciamento de permissões.

1.15 Gerenciamento de identidades

Gerenciamento de identidades. Há dois tipos de identidades que você precisa gerenciar ao abordar como operar cargas de trabalho seguras da AWS. Primeiro, as identidades humanas: os administradores, desenvolvedores, operadores e consumidores das suas aplicações precisam de uma identidade para acessar seus ambientes e aplicações AWS. Elas podem ser membros da sua organização ou usuários externos com os quais você colabora. Elas interagem com seus recursos da AWS por meio de um navegador da web, uma aplicação cliente, um aplicativo móvel ou ferramentas interativas de linha de comando. Segundo, as identidades de máquina: suas aplicações de carga de trabalho, ferramentas operacionais e componentes exigem uma identidade para fazer solicitações aos serviços da AWS, como ler dados. Essas identidades incluem máquinas em execução em seu



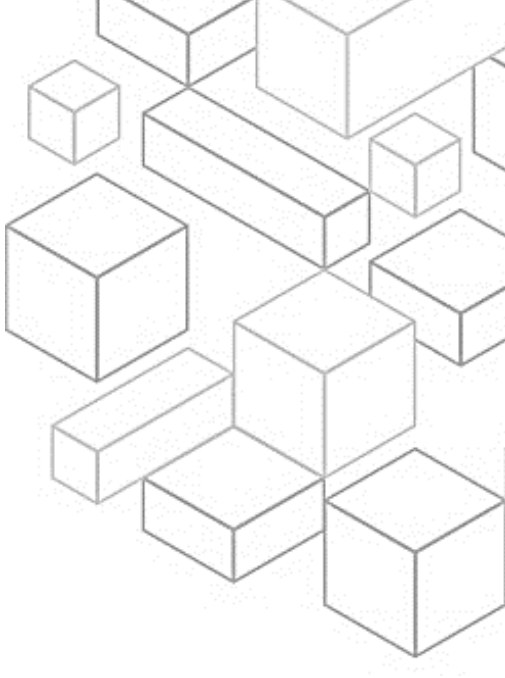
ambiente AWS, como instâncias do EC2 ou funções do AWS Lambda. Você também pode gerenciar identidades de máquinas para partes externas que precisam de acesso. Além disso, você pode ter máquinas fora da AWS que precisam de acesso ao seu ambiente AWS. Há várias práticas recomendadas para o gerenciamento de identidades, como o uso de mecanismos de login fortes. Autenticação com credenciais de login pode apresentar riscos quando não são usados mecanismos como a autenticação multifator, ou MFA. Isso é verdadeiro em situações em que as credenciais de login foram divulgadas inadvertidamente ou são facilmente adivinhadas. Os mecanismos de login podem ajudar a reduzir esses riscos, exigindo MFA e políticas de senhas fortes. É melhor usar credenciais temporárias para autenticação em vez de credenciais de longo prazo. Isso ajuda a reduzir ou eliminar riscos, como a divulgação, o compartilhamento ou o roubo inadvertido de credenciais. Você também pode armazenar e usar segredos com segurança. Uma carga de trabalho requer um recurso automatizado para comprovar a identidade em bancos de dados, recursos e serviços de terceiro. Isso é feito usando credenciais de acesso secretas, como chaves de acesso à API, senhas e tokens OAuth. O uso de um serviço criado para armazenar, gerenciar e trocar essas credenciais ajuda a reduzir a probabilidade de que elas sejam comprometidas. Para as identidades da força de trabalho, conte com um provedor de identidade que o ajude a gerenciar identidades em um local centralizado. Isso facilita o gerenciamento do acesso em várias aplicações e serviços porque você está criando, gerenciando e revogando o acesso a partir de um único local. Realize auditorias e troque as credenciais periodicamente para limitar o tempo que as credenciais podem ser usadas para acessar seus recursos.



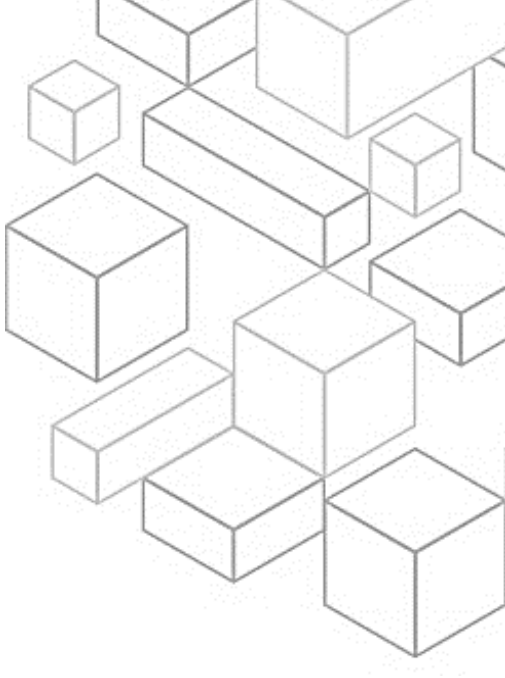
As credenciais de longo prazo criam muitos riscos, e esses riscos podem ser reduzidos com a troca regular das credenciais de longo prazo. À medida que o número de usuários que você gerencia aumenta, será necessário determinar maneiras de organizá-los para que possa gerenciá-los de forma dimensionada. Coloque os usuários com requisitos de segurança comuns em grupos definidos pelo seu provedor de identidade. Implemente mecanismos para garantir que os atributos do usuário que podem ser usados para controle de acesso, como departamento ou local, estejam corretos e atualizados. Use esses grupos e atributos para controlar o acesso em vez de usuários individuais. Isso ajuda a gerenciar o acesso de forma centralizada, alterando a associação ao grupo ou os atributos de um usuário uma vez com um conjunto de permissões. Evita-se a necessidade de atualizar muitas políticas individuais quando o acesso de um usuário precisa ser alterado.

1.16 Gerenciamento de permissões

Gerenciamento de permissões. Gerencie as permissões para controlar o acesso a identidades humanas e de máquinas que exigem acesso à AWS e às suas cargas de trabalho. As permissões controlam quem pode acessar o que e em que condições. Defina permissões para identidades humanas e de máquina específicas para conceder acesso a ações de serviço específicas em recursos específicos. Além disso, especifique as condições que devem ser verdadeiras para que o acesso seja concedido. Por exemplo, você pode permitir que os desenvolvedores criem novas funções Lambda, mas somente em uma Região específica. Ao gerenciar seus ambientes AWS dimensionados, siga as práticas recomendadas a seguir para garantir que as identidades tenham apenas o acesso



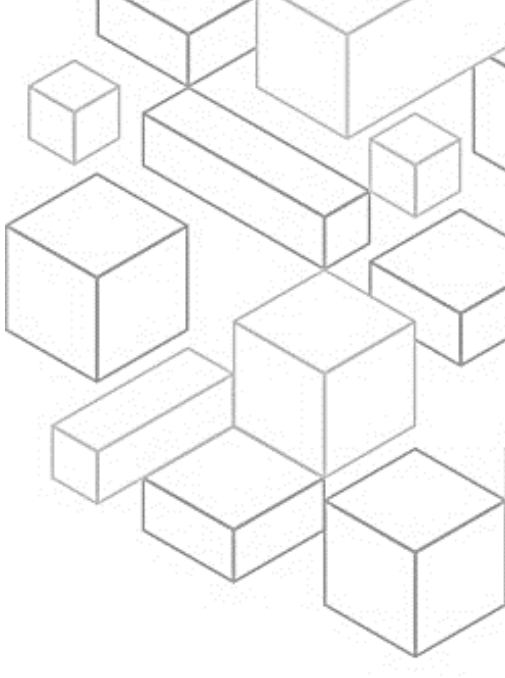
necessário e nada mais. Cada componente ou recurso de sua carga de trabalho precisa ser acessado por administradores, usuários finais ou outros componentes. Tenha uma definição clara de quem ou o que deve ter acesso a cada componente. Escolha o tipo de identidade adequado e o método de autenticação e autorização. Recomenda-se conceder apenas o acesso necessário para que as identidades realizem ações específicas em recursos específicos sob condições específicas. Use atributos de grupo e identidade para definir dinamicamente as permissões de acordo com suas dimensões, em vez de definir permissões para usuários individuais. Por exemplo, você pode permitir que um grupo de desenvolvedores tenha acesso para gerenciar apenas os recursos de seu projeto. Dessa forma, se um desenvolvedor deixar o projeto, o acesso dele será automaticamente revogado sem alterar as políticas de acesso subjacentes. Você também pode considerar um processo que dê acesso de emergência à sua carga de trabalho no caso improvável de um processo automatizado ou problema no pipeline. Isso ajudará você a contar com o acesso de menor privilégio, mas garantirá que os usuários possam obter o nível certo de acesso quando necessário. À medida que as equipes e as cargas de trabalho determinam o acesso de que precisam, remova as permissões que não são mais usadas e estabeleça processos de revisão para obter permissões de privilégio mínimo. Reduza e monitore as identidades e permissões não utilizadas. Defina barreiras de permissão para a sua organização e estabeleça controles comuns que restrinjam o acesso a todas as identidades da sua organização. Você também pode gerenciar o acesso com base no ciclo de vida. Integre os controles de acesso ao ciclo de vida do operador e da aplicação e ao seu provedor de federação centralizado. Para analisar o acesso público e entre contas, monitore



continuamente as descobertas que destacam o acesso público e entre contas. Reduza o acesso público e o acesso entre contas a apenas recursos que exigem esse tipo de acesso. Com o aumento do número de cargas de trabalho, talvez seja necessário compartilhar o acesso aos recursos nessas cargas de trabalho ou provisionar os recursos várias vezes em várias contas. Você pode ter construções para compartimentar seu ambiente, como ambientes de desenvolvimento, teste e produção. No entanto, ter construções de separação não impede você de compartilhar com segurança. Ao compartilhar componentes que se sobrepõem, é possível reduzir a sobrecarga operacional e criar uma experiência consistente sem adivinhar o que pode ter perdido ao criar o mesmo recurso várias vezes. A segurança de seu ambiente de nuvem não se limita à sua organização. Sua organização pode confiar em um terceiro para gerenciar uma parte de seus dados. O gerenciamento de permissões para o sistema gerenciado por terceiros deve seguir a prática de acesso just-in-time usando o princípio de menor privilégio com credenciais temporárias. Ao trabalhar em conjunto com um terceiro, você pode reduzir o escopo do impacto e o risco de acesso não intencional.

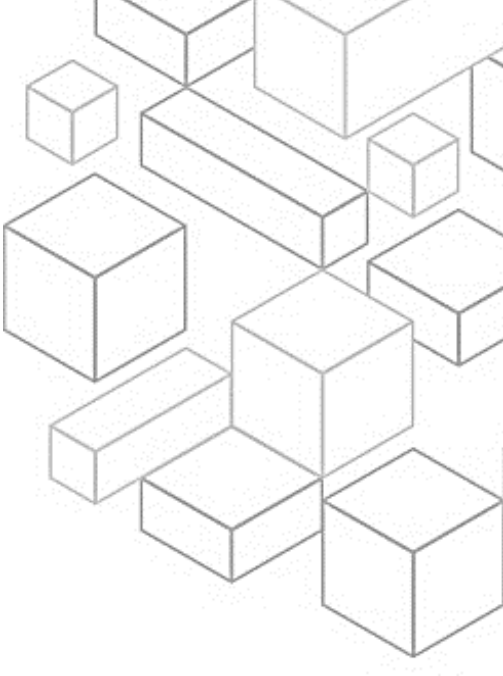
1.17 Detecção

A próxima área de práticas recomendadas de segurança é a detecção. Você pode usar controles de detecção para identificar uma ameaça ou incidente de segurança potencial. Eles são parte essencial das estruturas de governança e podem ser usados para dar suporte a um processo de qualidade, a uma obrigação legal ou de conformidade e para esforços de identificação e resposta a ameaças.



1.18 Detecção

A detecção consiste em duas partes: detecção de alterações inesperadas ou indesejadas na configuração e detecção de comportamento inesperado. A detecção ajuda você a identificar uma possível configuração incorreta da segurança, uma ameaça ou um comportamento inesperado. Trata-se de parte essencial do ciclo de vida da segurança e pode ser usada para dar suporte a um processo de qualidade, a uma obrigação legal ou de conformidade e para esforços de identificação e resposta a ameaças. Para a AWS, há várias abordagens que você pode usar ao tratar de mecanismos de detecção. Veja a seguir as práticas recomendadas de detecção. Primeiro,configure o log de serviços e aplicações. Retenha os logs de eventos de segurança de serviços e aplicações. Esse é um princípio fundamental de segurança para auditoria, investigações e casos de uso operacional. É um requisito de segurança comum orientado por governança, risco e conformidade, ou GRC, padrões, políticas e procedimentos. Depois, analise logs, descobertas e métricas de modo central. As equipes de operações de segurança dependem da coleta de logs e do uso de ferramentas de pesquisa para descobrir possíveis eventos de interesse que possam indicar atividade não autorizada ou alteração não intencional. No entanto, a simples análise dos dados coletados e o processamento manual das informações são insuficientes para acompanhar o volume de informações que flui de arquiteturas complexas. A análise e os relatórios, por si só, não facilitam a atribuição dos recursos certos para trabalhar em um evento em tempo hábil. Terceiro, automatize respostas a eventos de métrica. O uso da automação para investigar e corrigir eventos reduz o esforço e o erro humano e ajuda a dimensionar os recursos de investigação. Por meio de revisões regulares, você pode ajustar as ferramentas de automação e



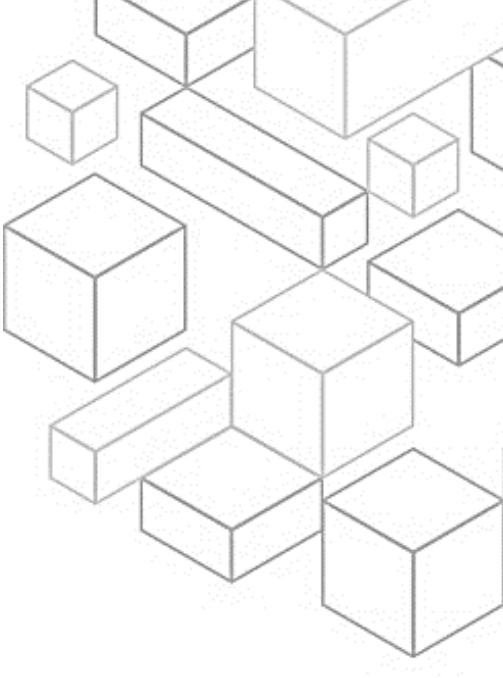
iterar continuamente. Por fim, implemente eventos de segurança acionáveis. Crie alertas que são enviados e podem ser acionados pela sua equipe. Garanta que os alertas incluam informações relevantes para que a equipe tome providências. Para cada mecanismo de detecção que tiver, você também deve ter um processo, na forma de um runbook ou playbook, para investigar.

1.19 Proteção de infraestrutura

A próxima área de práticas recomendadas de segurança é a proteção da infraestrutura. A proteção da infraestrutura abrange metodologias de controle, como defesa em profundidade, necessárias para atender às práticas recomendadas e às obrigações organizacionais ou regulatórias. O uso dessas metodologias é fundamental para o sucesso das operações contínuas na nuvem. A proteção da infraestrutura é uma parte fundamental de um programa de segurança da informação. Ela garante que os sistemas e recursos em suas cargas de trabalho sejam protegidos contra acesso não intencional, não autorizado e outras possíveis vulnerabilidades.

1.20 Proteção de redes

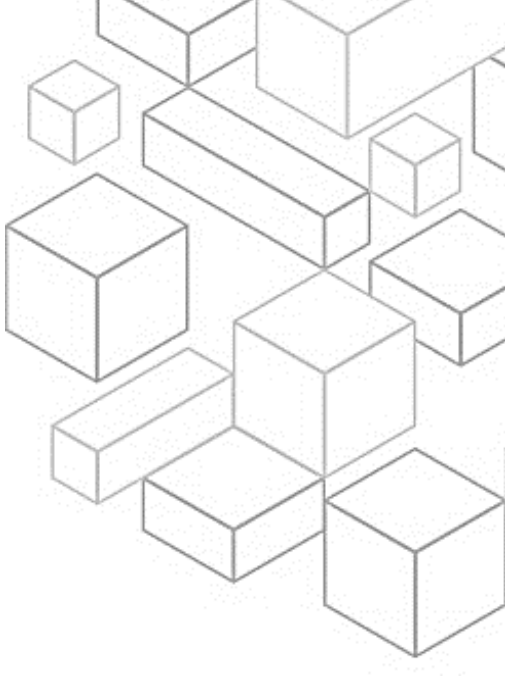
Proteção de redes. Os usuários, tanto da sua força de trabalho quanto de seus clientes, podem estar localizados em qualquer lugar. Você precisa abandonar os modelos tradicionais de confiar em qualquer pessoa e em qualquer coisa que tenha acesso à sua rede. Quando você segue o princípio de aplicar a segurança em todas as camadas, emprega uma abordagem Zero Trust. A segurança Zero



Trust é um modelo em que os componentes da aplicação ou os microsserviços são considerados distintos uns dos outros, e nenhum componente ou microsserviço confia em outro. Veja a seguir as práticas recomendadas para proteger as redes. Primeiro, crie camadas de rede. Agrupe os componentes que compartilham requisitos de confidencialidade em camadas para minimizar o escopo potencial do impacto do acesso não autorizado. Em seguida, controle o tráfego em todas as camadas. Ao arquitetar a topologia da rede, você deve examinar os requisitos de conectividade de cada componente. Terceiro, automatize os mecanismos de proteção da rede para fornecer uma rede autodefensiva com base na inteligência contra ameaças e na detecção de anomalias. Por fim, implemente inspeção e proteção. Inspecione e filtre seu tráfego em cada camada.

1.21 Proteção de computação

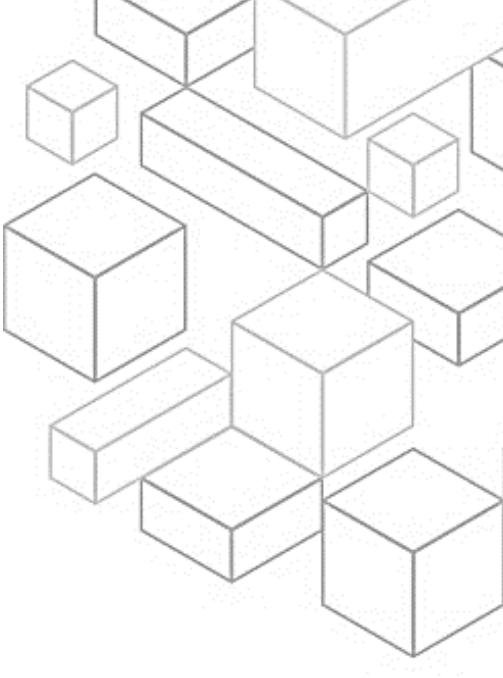
Proteção de computação. Os recursos de computação incluem instâncias EC2, contêineres, funções Lambda, serviços de banco de dados, dispositivos da Internet das Coisas e muito mais. Cada um desses tipos de recursos de computação exige abordagens diferentes para protegê-los. Porém, elas compartilham estratégias comuns que você precisa considerar: defesa em profundidade, gerenciamento de vulnerabilidades, redução da superfície de ataque, automação da configuração e da operação e execução de ações à distância. Nesta seção, você encontrará orientações gerais para proteger seus recursos de computação para os principais serviços. Para cada serviço AWS usado, é importante que você verifique as recomendações de segurança específicas na documentação do serviço. Veja a seguir as práticas recomendadas



para proteger os recursos de computação: realizar o gerenciamento de vulnerabilidades. Examine e corrija com frequência as vulnerabilidades em seu código, dependências e infraestrutura para ajudar na proteção contra novas ameaças. Reduza a superfície de ataque. Limite sua exposição a acessos indesejados tornando os sistemas operacionais mais fortes e minimizando os componentes, as bibliotecas e os serviços consumíveis externamente em uso. Implemente serviços que gerenciam recursos, como o Amazon Relational Database Service (Amazon RDS), o Lambda e o Amazon Elastic Container Service (Amazon ECS). Isso pode ajudar a reduzir suas tarefas de manutenção de segurança como parte do modelo de responsabilidade compartilhada. Automatize seus mecanismos de proteção de computação, incluindo o gerenciamento de vulnerabilidades, a redução da superfície de ataque e o gerenciamento de recursos. A automação o ajudará a investir tempo na proteção de outros aspectos de sua carga de trabalho e reduzirá o risco de erro humano. Ajude as pessoas a realizar ações à distância. A remoção da capacidade de acesso interativo reduz o risco de erro humano e o potencial de configuração ou gerenciamento manual. Implemente mecanismos como assinatura de código para validar se o software, o código e as bibliotecas usados na carga de trabalho são de fontes confiáveis e não foram adulterados.

1.22 Proteção de dados

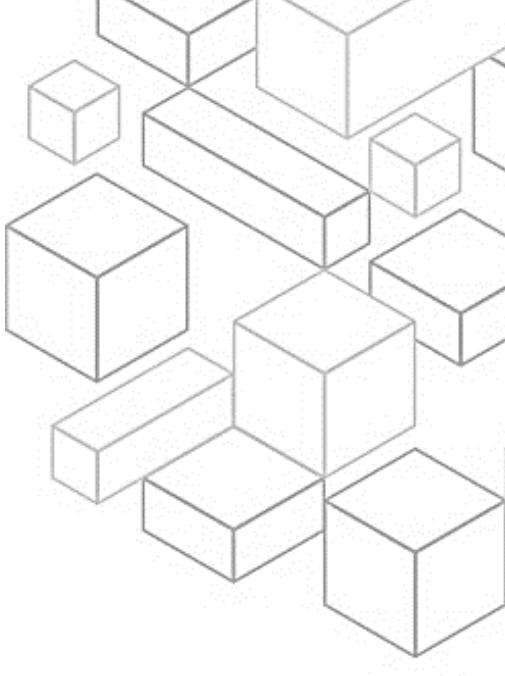
A próxima área de práticas recomendadas de segurança é a proteção de dados. Antes de arquitetar qualquer carga de trabalho, as práticas fundamentais que influenciam a segurança devem estar em vigor. Por exemplo, a classificação de dados oferece uma maneira de categorizar os dados com base em níveis de



confidencialidade. A criptografia protege os dados, tornando-os inacessíveis para quem não tem autorização. Esses métodos são importantes porque apoiam objetivos como limitar o manuseio incorreto ou ajudar a cumprir as obrigações regulatórias. Com a AWS, há várias abordagens diferentes que você pode usar ao tratar da proteção de dados. A seção a seguir descreve como usar essas abordagens.

1.23 Classificação de dados

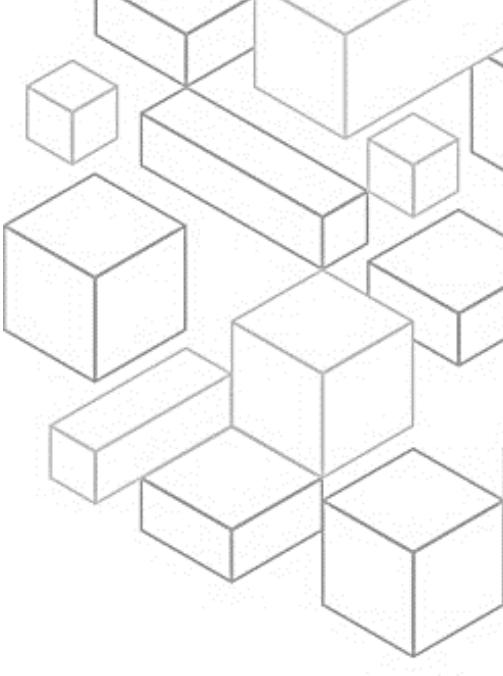
Classificação de dados. A classificação de dados oferece uma maneira de categorizar os dados organizacionais com base na criticidade e na confidencialidade. Isso pode ajudar você a determinar os controles adequados de proteção e retenção. Identifique os dados em sua carga de trabalho. É fundamental entender o tipo e a classificação dos dados que sua carga de trabalho está processando, os processos comerciais associados, onde os dados estão armazenados e quem é o proprietário dos dados. Você também deve entender sobre normas legais e de conformidade aplicáveis à sua carga de trabalho e quais controles de dados precisam ser aplicados. A identificação dos dados é a primeira etapa da jornada de classificação de dados. É importante definir os controles de proteção de dados. Você pode proteger os dados de acordo com seu nível de classificação. Automatizar a identificação e a classificação dos dados ajuda a implementar os controles corretos. O uso da automação, em vez do acesso direto de uma pessoa, reduz o risco de erro humano e exposição. Você também pode definir o gerenciamento do ciclo de vida dos dados. Sua estratégia deve ser baseada no nível de confidencialidade, juntamente com os requisitos legais e da organização. Aspectos como a duração



da retenção de dados, processos de destruição de dados, gerenciamento de acesso a dados, transformação de dados e compartilhamento de dados devem ser considerados.

1.24 Proteger dados em repouso

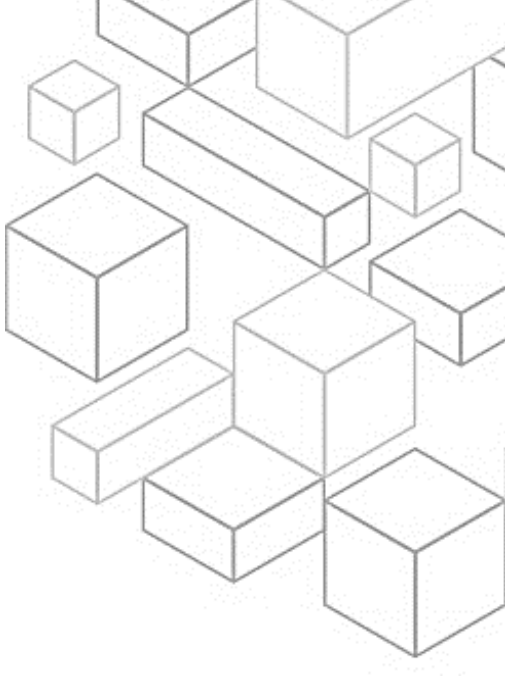
Proteger dados em repouso. Os dados em repouso representam todos os dados que persistem no armazenamento não volátil por qualquer duração em sua carga de trabalho. Isso inclui armazenamento em bloco, armazenamento de objeto, bancos de dados, arquivos, dispositivos de IoT e qualquer outra mídia de armazenamento na qual os dados são mantidos. A proteção dos seus dados em repouso reduz o risco de acesso não autorizado quando a criptografia e os controles de acesso apropriados são implementados. Considere as seguintes práticas recomendadas para proteger esses dados. Primeiro, implemente o gerenciamento seguro de chaves. Defina uma abordagem de criptografia que inclua o armazenamento, a alternância e o controle de acesso das chaves. Isso ajuda você a proteger o conteúdo contra usuários não autorizados e a exposição desnecessária a usuários autorizados. Em seguida, aplique a criptografia em repouso. Você deve impor o uso de criptografia para dados em repouso. A criptografia mantém a confidencialidade dos dados sigilosos em caso de acesso não autorizado ou divulgação acidental. Também é possível automatizar a proteção de dados em repouso usando ferramentas automatizadas para validar e aplicar controles de dados em repouso continuamente. Imponha o controle de acesso. Para ajudar a proteger seus dados em repouso, imponha o controle de acesso usando mecanismos como isolamento e versionamento e aplique o princípio de menor privilégio. Previna a concessão de acesso público aos seus dados. Por fim,use mecanismos para



distanciar as pessoas dos dados. Mantenha todos os usuários longe do acesso direto a sistemas e dados sigilosos em circunstâncias operacionais normais.

1.25 Proteger dados em trânsito

Proteger dados em trânsito. Dados em trânsito são quaisquer dados enviados de um sistema para outro. Isso inclui a comunicação entre os recursos da sua carga de trabalho e também a comunicação entre outros serviços e seus usuários finais. Ao fornecer o nível adequado de proteção para dados em trânsito, você protege a confidencialidade e a integridade dos dados de sua carga de trabalho. Considere as seguintes práticas recomendadas para proteger os dados em trânsito. Primeiro,implemente o gerenciamento seguro de chaves e certificados. Armazene chaves de criptografia e certificados de forma segura e troque-os em intervalos de tempo apropriados com controle de acesso rigoroso. Segundo, imponha criptografia em trânsito. Imponha os requisitos de criptografia definidos com base nas políticas, obrigações regulamentares e padrões da sua organização para ajudar a atender aos requisitos organizacionais, legais e de conformidade. Use apenas protocolos com criptografia ao transmitir dados sigilosos para fora de sua VPC. A criptografia ajuda a manter a confidencialidade dos dados, mesmo quando eles transitam por redes não confiáveis. Terceiro, automatize a detecção de acesso não intencional aos dados. Use ferramentas como o Amazon GuardDuty para detectar automaticamente atividades suspeitas ou tentativas de mover dados para fora dos limites definidos. Autentique as comunicações de rede. Verifique a identidade das comunicações usando protocolos que suportam autenticação, como Transport Layer Security ou IPsec.

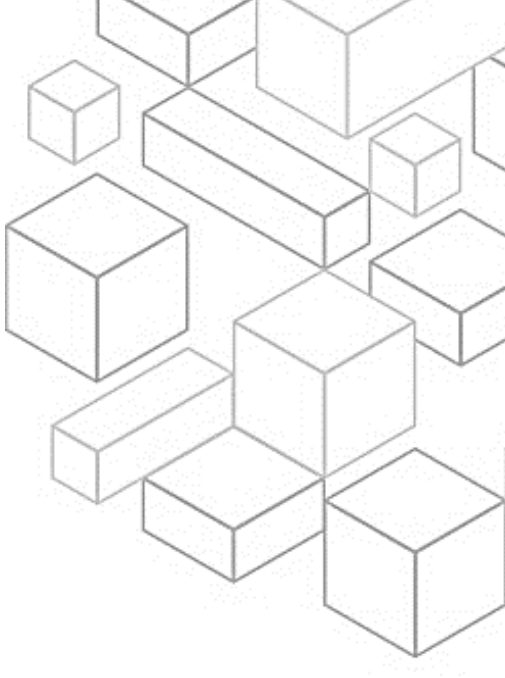


1.26 Resposta a incidentes

A próxima área de melhores práticas de segurança é a resposta a incidentes. Mesmo com controles de prevenção e detecção extremamente desenvolvidos, sua organização ainda deve implementar os processos para responder e mitigar o impacto potencial de incidentes de segurança. A arquitetura da sua carga de trabalho afeta fortemente a capacidade das suas equipes de operar com eficiência durante um incidente para isolar ou conter os sistemas e restaurar as operações para um estado bom conhecido.

1.27 Objetivos de design da resposta à nuvem

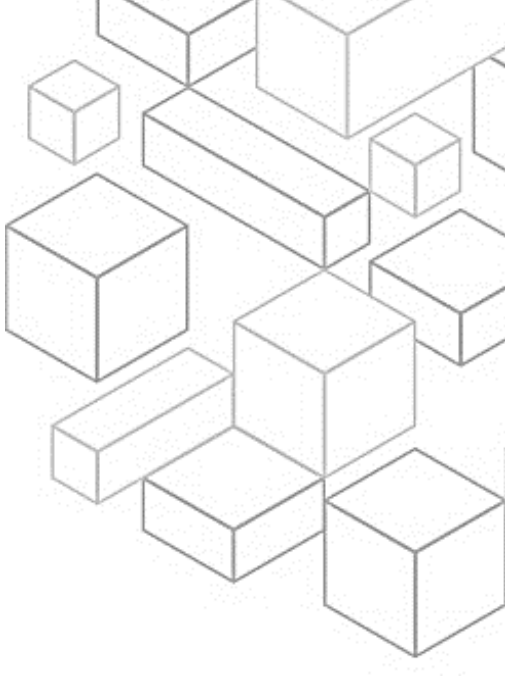
Objetivos de design da resposta à nuvem. Os processos e mecanismos gerais de resposta a incidentes, como os definidos no NIST SP 800-61 Computer Security Incident Handling Guide, são importantes. Você também deve avaliar as seguintes metas de design para ajudar a responder a incidentes de segurança em um ambiente de nuvem. Primeiro, estabeleça objetivos de resposta. Trabalhe com seus stakeholders, com a assessoria jurídica e com a liderança organizacional para determinar o objetivo de responder a um incidente. Alguns objetivos comuns incluem a contenção e a atenuação do problema, a recuperação dos recursos afetados, a preservação dos dados para análise forense e a atribuição. Em seguida, documente os planos. Crie planos para ajudar você a responder, comunicar-se durante e recuperar-se de um incidente. Responda usando a nuvem: implemente seus padrões de resposta onde o evento e os dados ocorrem. Saiba o que você tem e do que você precisa. Preserve adequadamente os logs, snapshots e outras provas, copiando-as para uma conta



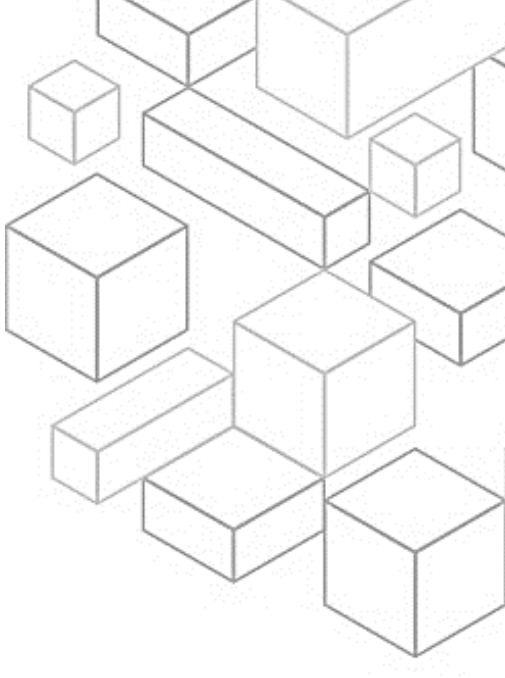
de nuvem de segurança centralizada. Use tags, metadados e mecanismos que imponham políticas de retenção. Por exemplo, você pode optar por usar o comando dd do Linux ou um equivalente do Windows para fazer uma cópia completa dos dados para fins de investigação. Use mecanismos de reimplantação. Se uma anomalia de segurança puder ser atribuída a uma configuração incorreta, a correção poderá ser tão rápida quanto remover a variação, reimplantando os recursos com a configuração adequada. Se possível, torne seus mecanismos de resposta seguros para serem executados mais de uma vez e em ambientes em um estado desconhecido. Automatize sempre que possível. Quando notar problemas ou incidentes que se repetem, crie mecanismos que façam uma triagem programática e respondam a situações comuns. Use respostas humanas para incidentes únicos, novos e sigilosos. Escolha soluções dimensionáveis. Você deve se esforçar para combinar o dimensionamento da abordagem da sua organização à computação em nuvem e reduzir o tempo entre a detecção e a resposta. Por fim, aprenda e melhore seu processo. Ao identificar lacunas em seus processos, ferramentas ou pessoas, implemente planos para corrigi-las. As simulações são métodos seguros para encontrar lacunas e aprimorar processos.

1.28 Instruir

Os processos automatizados ajudam as organizações a dedicar mais tempo às medidas para aumentar a segurança das cargas de trabalho. A resposta automatizada a incidentes também torna os seres humanos disponíveis para correlacionar eventos, praticar simulações, elaborar novos procedimentos de resposta, realizar pesquisas, desenvolver novas habilidades e testar ou criar



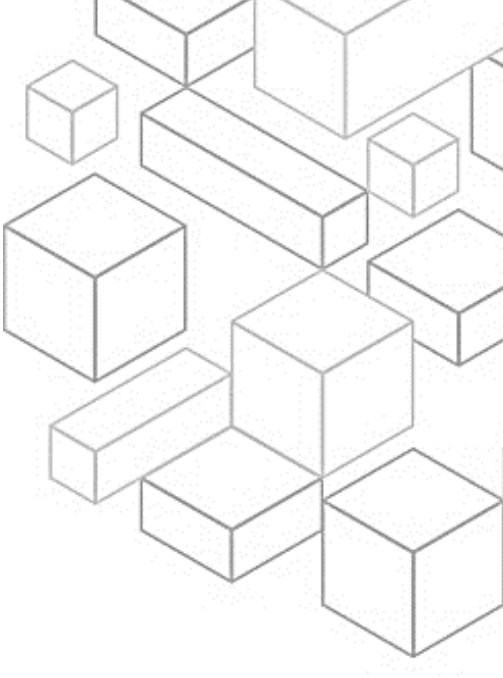
novas ferramentas. Apesar do aumento da automação, a sua equipe, os especialistas e os respondentes de uma organização de segurança ainda precisam de educação contínua. Convém analisar e incorporar as seguintes áreas ao pensar em educar suas equipes de segurança. Para iniciar, considere as habilidades de desenvolvimento. Equipar os profissionais de segurança com habilidades de programação pode ajudar a acelerar os esforços de automação da sua organização. Isso inclui não apenas garantir a educação em linguagens de programação, como Python, mas também garantir a familiaridade com o sistema de controle de origem, controle de versão e processos de CI/CD. Quando os desenvolvedores têm esse entendimento, eles podem aumentar a eficiência e reduzir os erros ao automatizar. Você também pode treinar sua equipe para que ela seja proficiente com os serviços de segurança oferecidos pela AWS. Entender como usar as ferramentas de nuvem ajuda a reduzir o tempo de resposta e a aumentar a confiança da equipe. Além disso, estabeleça uma cadência de educação sobre novos serviços e recursos para iterar continuamente seus recursos. Assim como o cenário de ameaças muda, o mesmo acontece com as ferramentas. Por fim, mantenha a conscientização das aplicações. Treine a sua equipe de resposta a incidentes sobre as especificidades das cargas de trabalho e dos ambientes de sua propriedade. Isso inclui entender quais logs são emitidos, quais informações os registros contêm, o fluxo de tráfego do aplicativo e os mecanismos de autenticação e autorização em uso. Esse é um componente essencial porque o conhecimento profundo da infraestrutura e das aplicações da sua organização oferece uma vantagem para protegê-las. A melhor maneira de aprender é a prática, por exemplo, por meio de dias de teste de resposta a incidentes. Isso ajuda os especialistas da sua equipe a



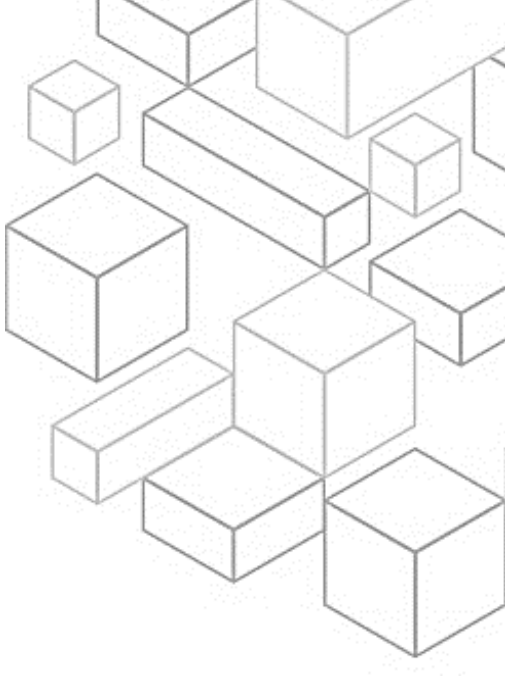
aprimorar as ferramentas e técnicas enquanto ensinam outras pessoas. Isso é abordado em mais detalhes na seção a seguir No futuro, lembre-se de manter o treinamento necessário para toda a sua organização. A conscientização sobre a segurança é uma importante linha de defesa. Todos os usuários devem ser treinados para relatar comportamentos suspeitos à sua equipe de segurança para investigação adicional.

1.29 Preparar, simular, iterar

Não deixe de considerar o acesso pré-provisionado. Durante um incidente, suas equipes de resposta a incidentes devem ter acesso a várias ferramentas e recursos de carga de trabalho envolvidos no incidente. Verifique se suas equipes têm acesso pré-provisionado adequado para realizar suas tarefas antes da ocorrência de um evento. Todas as ferramentas, acessos e planos devem ser documentados e testados para garantir que possam fornecer uma resposta em tempo hábil. Considere as seguintes práticas recomendadas. Identifique os principais funcionários e recursos externos. Busque o pessoal interno e externo, os recursos e as obrigações legais que ajudariam sua organização a responder a um incidente. Desenvolva planos de gerenciamento de incidentes. Crie planos para ajudar você a responder, comunicar-se durante e recuperar-se de um incidente. Em seguida, prepare os recursos forenses. É importante que os responsáveis pela resposta a incidentes entendam quando e como a investigação forense se encaixa no seu plano de resposta. Sua organização deve definir quais provas são coletadas e quais ferramentas são usadas no processo. Identifique e prepare os recursos de investigação forense adequados, incluindo especialistas externos, ferramentas e automação. Considere também como automatizar a



contenção e a recuperação de um incidente. Isso pode ajudar a reduzir os tempos de resposta e o impacto organizacional. Depois de criar e praticar processos e ferramentas de seus playbooks, desconstrua a lógica em uma solução baseada em código. Isso pode ser usado como uma ferramenta por muitos respondentes para automatizar a resposta e eliminar a variação ou o trabalho de adivinhação de seus respondentes. Você também pode acelerar o ciclo de vida de uma resposta. O próximo objetivo é automatizar totalmente esse código para ser invocado pelos próprios alertas ou eventos, e não por um respondente humano, para criar uma resposta orientada por eventos. Esses processos também devem adicionar automaticamente dados relevantes aos seus sistemas de segurança. Por exemplo, um incidente envolvendo tráfego de um endereço IP indesejado pode preencher automaticamente uma lista de bloqueio do AWS WAF ou um grupo de regras do AWS Network Firewall para impedir outras atividades. Para o acesso pré-provisionado, verifique se os respondentes de incidentes têm o acesso correto pré-provisionado na AWS. Isso pode ajudar a reduzir o tempo necessário para a investigação até a recuperação. Garanta também que a equipe de segurança tenha as ferramentas certas pré-implantadas na AWS para reduzir o tempo de investigação até a recuperação. Realize dias de teste, também conhecidos como simulações ou exercícios. Esses são eventos internos que oferecem uma oportunidade estruturada de praticar seus planos e procedimentos de gerenciamento de incidentes em um cenário realista. Esses eventos devem exercitar os profissionais de resposta usando as mesmas ferramentas e técnicas que seriam usadas em um cenário real. Os dias de teste podem até mesmo imitar ambientes do mundo real. Basicamente, trata-se de estar preparado e melhorar



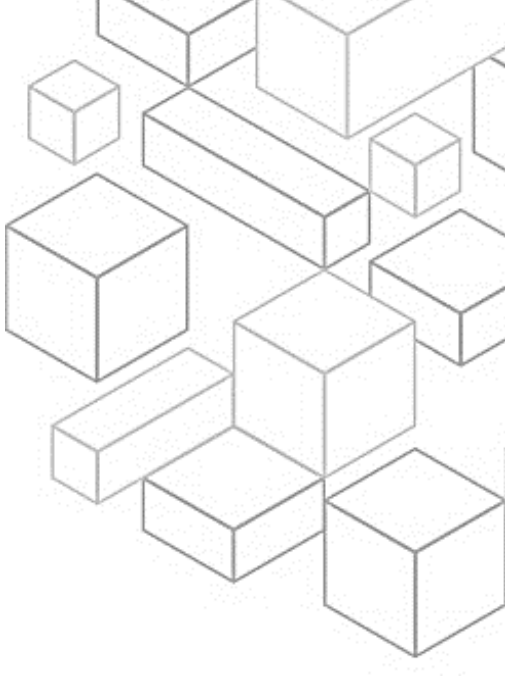
iterativamente seus recursos de resposta.

1.30 Segurança de aplicações

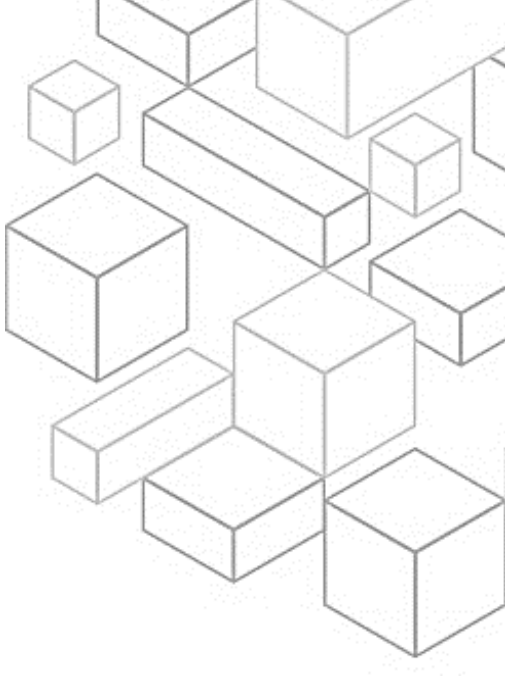
A última área de práticas recomendadas de segurança é a segurança de aplicações. A segurança é um tópico que abrange todas as áreas da tecnologia. Você já aprendeu sobre identidade, proteção de infraestrutura, proteção de dados e resposta a incidentes. A seguir, você aprenderá sobre segurança de aplicações.

1.31 Segurança de aplicações

Segurança de aplicações. O treinamento de pessoas, os testes com automação, a compreensão das dependências e a validação das propriedades de segurança de ferramentas e aplicações ajudam a reduzir a probabilidade de problemas de segurança nas cargas de trabalho de produção. É importante realizar treinamentos sobre segurança de aplicações. Ofereça treinamento aos desenvolvedores de sua organização sobre práticas comuns para o desenvolvimento e a operação seguros de aplicações. A adoção de práticas de desenvolvimento com foco na segurança ajuda a reduzir a probabilidade de problemas que só são detectados no estágio de revisão de segurança. Automatize os testes durante todo o ciclo de vida de desenvolvimento e lançamento, inclusive para propriedades de segurança durante todo o ciclo de vida de desenvolvimento e lançamento. A automação ajuda você a identificar de forma consistente e repetitiva os possíveis problemas no software antes do lançamento. Isso pode reduzir o risco de problemas de segurança no software que está sendo fornecido. Realize testes de penetração regulares em seu



software. Esse mecanismo ajuda a identificar possíveis problemas de software que não podem ser detectados por testes automatizados ou por uma revisão manual do código. Ele também pode ajudar você a entender a eficácia dos seus controles de detecção. Os testes de penetração devem tentar determinar se o software pode ser executado de maneiras inesperadas, como a exposição de dados que deveriam estar protegidos ou a concessão de permissões mais amplas do que o esperado. Realize uma análise manual do código do software que você produz. Esse processo ajuda a verificar se a pessoa que escreveu o código não é a única que está verificando a qualidade do código. Centralize serviços para pacotes e dependências. Forneça serviços centralizados para que as equipes de construtores obtenham pacotes de software e outras dependências. Isso valida os pacotes antes que eles sejam incluídos no software que você escreve e fornece uma origem de dados para análise de software. Realize implantações de software de forma programática sempre que possível. Essa abordagem reduz a probabilidade de uma implantação falhar ou de um problema inesperado ser introduzido devido a um erro humano. Avalie regularmente as propriedades de segurança das pipelines. Aplique os princípios do pilar de segurança do AWS WA aos seus pipelines, com atenção especial à separação de permissões. Avalie regularmente as propriedades de segurança de sua infraestrutura de pipeline. O gerenciamento eficaz da segurança dos pipelines ajuda você a fornecer a segurança do software que passa pelos pipelines. Por fim, crie um programa que incorpore a propriedade da segurança nas equipes de carga de trabalho. Capacite as equipes de construtores a tomar decisões de segurança sobre o software que criam. Sua equipe de segurança ainda precisa validar essas decisões durante uma revisão,



mas incorporar a propriedade da segurança nas equipes de construtores leva à criação de cargas de trabalho mais rápidas e seguras. Esse mecanismo também promove uma cultura de propriedade que afeta positivamente a operação dos sistemas que você constrói.

1.32 Pergunta 1

A resposta correta para a pergunta exibida está no slide a seguir.

1.33 Pergunta 2

A resposta correta para a pergunta exibida está no slide a seguir.

1.34 Pergunta 3

A resposta correta para a pergunta exibida está no slide a seguir.

1.35 Resumo

Neste módulo, você aprendeu sobre o pilar de segurança. Iniciamos com uma visão geral e incluímos uma discussão aprofundada sobre a proposta de valor, os princípios de design e as práticas recomendadas do pilar de segurança.

1.36 Agradecemos sua atenção

Agradecemos sua participação!