AWS Cloud Adoption Framework

Perspectiva de segurança

Junho de 2016

Avisos

Este documento é fornecido apenas para fins informativos. Ele relaciona as atuais ofertas de produtos e práticas da AWS a contar da data de emissão deste documento, que estão sujeitas a alterações sem aviso prévio. Os clientes são responsáveis por fazer sua própria avaliação independente das informações neste documento e de qualquer uso dos produtos ou serviços da AWS, cada um dos quais é fornecido “como está”, sem garantia de qualquer tipo, expressa ou implícita. Este documento não cria quaisquer garantias, representações, compromissos contratuais, condições ou seguros da AWS, suas afiliadas, fornecedores ou licenciadores. As responsabilidades e as obrigações da AWS com os seus clientes são controladas por contratos da AWS, e este documento não é parte, nem modifica, qualquer contrato entre a AWS e seus clientes.

Tópicos

Resumo

O Cloud Adoption Framework[1] (CAF) da Amazon Web Services (AWS) apresenta diretrizes para coordenar as diferentes partes das organizações que estão migrando para a computação em nuvem. As diretrizes do CAF são divididas em diversas áreas de enfoque relevantes para a implementação de sistemas de TI baseados em nuvem. Essas áreas de enfoque são chamadas de *perspectivas* e cada perspectiva ainda é dividida em *componentes*. Há um whitepaper para cada uma das sete perspectivas do CAF.

Este whitepaper aborda a Perspectiva de segurança, que foca nas diretrizes e nos processos de incorporação para os seus controles de segurança existentes específicos para o uso da AWS no seu ambiente.

Introdução

Na AWS, a segurança é nossa principal missão. Todos os clientes da AWS se beneficiam de um datacenter e de uma arquitetura de rede criados para satisfazer os requisitos das empresas com as maiores exigências de segurança. A AWS e seus parceiros oferecem centenas de ferramentas e recursos para ajudar você a alcançar seus objetivos de segurança em relação a visibilidade, auditabilidade, controlabilidade e agilidade. Isso significa que você pode ter a segurança de que precisa, mas sem desperdício de capital e com despesas operacionais muito menores do que em um ambiente no local.

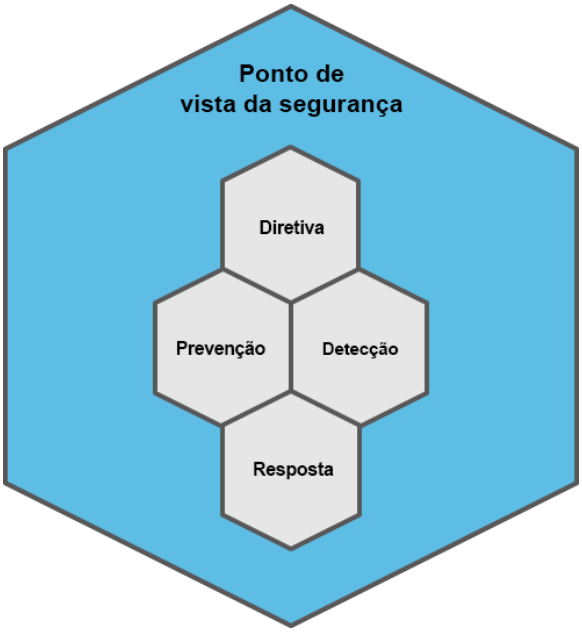

Figura 1: Perspectiva de segurança AWS CAF

O objetivo da Perspectiva de segurança é ajudar você a estruturar a seleção e a implementação de controles certos para a sua organização. Como ilustra a Figura 1, os componentes da Perspectiva de segurança organizam os princípios que ajudarão a conduzir a transformação da cultura de segurança da sua organização. Para cada componente, este whitepaper discute as medidas específicas que você pode tomar e os meios para medir o progresso:

- Os controles de **diretiva** determinam os modelos de governança, risco e conformidade em que o ambiente operará.
- Os controles de **prevenção** protegem suas cargas de trabalho e elimina ameaças e vulnerabilidades.
- Os controles de **detecção** fornecem total visibilidade e transparência sobre a operação das suas implantações na AWS.
- Os controles de **resposta** conduzem à remediação de possíveis desvios das linhas de base da sua segurança.

A segurança na nuvem é conhecida. O aumento da agilidade e a habilidade de desempenhar ações mais rapidamente, em maior escala e por um menor custo, não invalida princípios bem estabelecidos de segurança da informação.

Depois de abordar os quatro componentes da Perspectiva de segurança, este whitepaper descreve os passos que você pode tomar em sua jornada até a nuvem para garantir que o seu ambiente mantenha uma base forte de segurança:

- Defina uma **estratégia de segurança** na nuvem. Quando você iniciar sua jornada, observe os objetivos organizacionais da sua empresa, a abordagem de gerenciamento de risco e o nível de oportunidades apresentadas pela nuvem.
- Forneça um **programa de segurança** para o desenvolvimento e a implementação de recursos de segurança, privacidade, conformidade e gerenciamento de risco. O escopo pode parecer vasto inicialmente, por isso, é importante criar uma estrutura que permita que sua organização aborde a segurança na nuvem de maneira alternativa. A implementação deve permitir o desenvolvimento iterativo para que os recursos se consolidem à medida que os programas se desenvolvem. Isso permite que o componente de segurança seja um catalisador do restante dos esforços de adoção da nuvem pela organização.

- Desenvolva recursos de **operações de segurança** robustos que evoluem e se aprimoram continuamente. A jornada de segurança continua ao longo do tempo. Recomendamos que você combine o rigor operacional com a criação de novos recursos, para que a iteração constante possa promover melhorias contínuas.

Benefícios de segurança da AWS

A segurança da nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você se beneficiará de um datacenter e uma arquitetura de rede criados para atender os requisitos das organizações com as maiores exigências de segurança.

Uma vantagem da Nuvem AWS é permitir que os clientes escalonem e inovem, enquanto mantêm o ambiente seguro. Os clientes pagam apenas pelos serviços que utilizam, o que significa que você pode ter a segurança de que precisa, mas sem as despesas iniciais e com menor custo do que um ambiente no local.

Esta seção discute alguns dos benefícios de segurança da plataforma da AWS.

Criado para segurança

A infraestrutura da Nuvem AWS é operada nos datacenters da AWS e é projetada para atender os requisitos dos nossos clientes com as maiores exigências de segurança. A infraestrutura da AWS foi projetada para fornecer alta disponibilidade, estabelecendo uma forte defesa para a privacidade do cliente. Todos os dados são armazenados em datacenters da AWS altamente seguros. Os firewalls de rede criados no Amazon VPC e os recursos de firewall de aplicativos Web no AWS WAF permitem que você crie redes privadas e controle o acesso a suas instâncias e aplicativos

Quando você implanta sistemas na Nuvem AWS, a AWS ajuda compartilhando com você as responsabilidades de segurança. A AWS projeta a infraestrutura subjacente usando princípios de projeto seguros, e os clientes podem implementar sua própria arquitetura de segurança para cargas de trabalho implantadas na AWS.

Altamente automatizado

Na AWS, criamos ferramentas de segurança com propósitos específicos e as personalizamos para nosso próprio ambiente, tamanho e requisitos globais. Criar ferramentas de segurança do zero permite que a AWS automatize muitas das tarefas de rotina para as quais especialistas em segurança dedicam seu tempo. Isso significa que os especialistas em segurança da AWS podem dedicar mais tempo concentrando-se em medidas para aumentar a segurança do seu ambiente na Nuvem AWS. Os clientes também automatizam a engenharia de segurança e as funções de operações usando um amplo conjunto de APIs e ferramentas. Gerenciamento de identidade, segurança de rede e proteção de dados e recursos de monitoramento podem ser totalmente automatizados e fornecidos usando métodos populares de desenvolvimento de software que você já tenha instaurados.

Os clientes adotam uma abordagem automatizada para responder a questões de segurança. Quando você automatiza usando os serviços da AWS, em vez de ter pessoas monitorando sua posição de segurança e reagindo a um evento, seu sistema pode monitorar, examinar e iniciar uma resposta.

Altamente disponível

A AWS cria seus datacenters em várias regiões geográficas. Dentro das regiões, existem várias Zonas de disponibilidade para fornecer resiliência. A AWS projeta datacenters com excesso de largura de banda para que, caso ocorra uma importante interrupção, haja capacidade suficiente para balancear o tráfego e roteá-lo para os sites restantes, minimizando o impacto sobre nossos clientes. Os clientes também podem utilizar essa estratégia Multirregião e Multi-AZ para criar aplicativos altamente resilientes a um custo baixíssimo para replicar e fazer backup de dados de forma fácil e implantar controles de segurança globais de forma consistente em suas empresas.

Altamente credenciado

Os ambientes da AWS são auditados continuamente, com certificações de organismos de credenciamento em todo o mundo. Isso significa que os segmentos da sua conformidade já foram concluídos. Para obter informações sobre todos os padrões e regulamentos de segurança com os quais a AWS tem conformidade, visite a página da web Conformidade da Nuvem AWS[2]. Para ajudar você a atender padrões e regulamentos de segurança governamentais, industriais e corporativos, a AWS fornece relatórios de certificação que descrevem como a infraestrutura da Nuvem AWS atende aos requisitos de uma lista extensa de padrões globais de segurança. Para obter os relatórios de conformidade disponíveis, entre em contato com seu representante de conta da AWS. Os clientes herdam muitos controles operados pela AWS em seus próprios programas de conformidade e certificação, baixando o custo para manter e conduzir esforços de garantia de segurança, além de manter eles mesmos esses controles. Com uma forte base instalada, você pode otimizar a segurança das suas cargas de trabalho para obter agilidade, resiliência e escala.

O restante deste whitepaper apresenta cada componente da Perspectiva de segurança. Você pode usar esses componentes para explorar os objetivos de segurança de que precisa para ter êxito em sua jornada até a nuvem.

O componente Diretiva

O componente Diretiva da Perspectiva de segurança da AWS fornece diretrizes para o planejamento da sua abordagem de segurança à medida que você migra para a AWS. A chave para um planejamento eficaz é definir as diretrizes que você fornecerá para as pessoas que estiverem implementando e operando o seu ambiente de segurança. As informações precisam fornecer orientações suficientes para determinar os controles necessários e como eles devem ser operados. Dentre as áreas iniciais a serem consideradas estão:

- **Governança da conta** – oriente a organização a criar um processo e procedimentos para gerenciar contas da AWS. As áreas a serem definidas incluem: como inventários de contas serão coletados e mantidos, que contratos e emendas estão em vigor e quais critérios devem ser usados ao criar uma conta da AWS. Desenvolva um processo para criar contas de forma consistente, garantindo que todos as configurações iniciais sejam apropriadas e que uma propriedade clara seja estabelecida.

- **Propriedade da conta e informações de contato** – estabeleça um modelo de governança adequado das contas da AWS usadas na sua organização e planeje como as informações de contato serão mantidas para cada conta. Considere criar contas da AWS vinculadas a listas de distribuição de e-mails em vez do endereço de e-mail de uma pessoa. Isso permite que um grupo de pessoas monitore e responda às informações da AWS sobre a atividade da sua conta. Além disso, forneça resiliência quando o corpo interno de funcionários é trocado e proporcione um meio de atribuir responsabilidade pela segurança. Liste sua equipe de segurança como um ponto de segurança de contato para acelerar comunicações urgentes.
- **Estrutura de controle** – estabeleça ou aplique uma estrutura de controle padrão do setor e determine se você necessita modificações ou adições para incorporar os serviços da AWS nos níveis de segurança esperados. Desempenhe um exercício de mapeamento de conformidade para determinar como os requisitos de conformidade e os controles de segurança refletirão o uso do serviço da AWS.
- **Propriedade de dados** – revise as informações no Modelo de responsabilidade compartilhada da AWS[3] no site da AWS para determinar se devem ser feitas modificações na propriedade de dados Revise e atualize sua matriz de atribuição de responsabilidade (gráfico RACI) para incluir a propriedade de dados operando no ambiente da AWS.
- **Classificação de dados** – revise as classificações de dados atuais e determine como essas classificações serão gerenciadas no ambiente da AWS e quais controles serão adequados.
- **Gerenciamento de alterações e ativos** – determine como o gerenciamento de alterações e ativos deverá ser executado na AWS. Crie um meio de determinar os ativos existentes, para que os sistemas serão usados e como os sistemas serão gerenciados de forma segura. Isso pode ser integrado com um Configuration Management Database (CMDB – banco de dados de gerenciamento de configuração). Considere criar uma prática de nomeação e marcação que permita que a identificação e o gerenciamento ocorram no nível de segurança exigido. Você pode usar esta abordagem para definir e rastrear os metadados que permitem a identificação e o controle.

- **Localidade de dados** – revise os critérios por onde seus dados podem residir para determinar quais controles serão necessários para gerenciar a configuração e o uso dos serviços da AWS nas regiões. Os clientes da AWS escolhem as regiões da AWS onde o conteúdo será hospedado. Isso permite que os clientes com necessidades geográficas específicas estabeleçam os ambientes nos locais que escolherem. Os clientes podem replicar e fazer backup do conteúdo em mais de uma região, mas a AWS não migra conteúdo do cliente para fora da região escolhida por ele.
- **Acesso com privilégio mínimo** – estabeleça uma cultura de segurança organizacional criada sobre o princípio de privilégio mínimo e autenticação forte. Implemente protocolos para proteger o acesso a credenciais confidenciais e materiais-chave associados com cada conta da AWS. Defina as expectativas sobre como a autoridade será delegada para os engenheiros de software, a equipe de operações e outras funções de trabalho envolvidas na adoção da nuvem.
- **Manuais de operações de segurança** – defina os seus padrões de segurança para criar proteções duráveis que podem ser recomendadas pela organização ao longo do tempo. Implemente as ações durante a automação como manuais; documente intervenções human-in-the-loop (HTIL) conforme adequadas.

Considerações

- **Crie** um modelo de responsabilidade compartilhada da AWS personalizado para seu ecossistema.
- **Use** autenticação forte como parte de um esquema de proteção para todos os atores em sua conta.
- **Promova** uma cultura de propriedade de segurança para equipes de aplicativos.
- **Amplie** o modelo de classificação de dados para incluir serviços na AWS.
- **Integre** os objetivos dos desenvolvedores, das operações e da equipe de segurança com as funções de trabalho.
- **Considere** criar uma estratégia para nomear e acompanhar as contas usadas para gerenciar serviços na AWS.
- **Centralize** as listas de distribuição de telefones e e-mail para que as equipes possam ser monitoradas.

O componente Prevenção

O componente Prevenção da Perspectiva de segurança da AWS fornece diretrizes para a implementação de uma infraestrutura de segurança com a AWS e dentro da sua organização. A chave para implementar o conjunto correto de controles é permitir que suas equipes de segurança ganhem a confiança e os recursos de que precisam para criar as habilidades de automação e implantação necessárias para proteger a empresa no ambiente ágil e escalável que é a AWS.

Use o componente Diretiva para determinar os controles e as diretrizes de que você precisará e use o componente Prevenção para determinar como você operará os controles efetivamente. A AWS fornece regularmente diretrizes sobre as melhores práticas para a utilização do serviço da AWS e de padrões de implantação de carga de trabalho que podem ser usados como referências de implementação de controle. Visite o Centro de Segurança da AWS, o blog e os vídeos mais recentes sobre segurança da Conferência da AWS e da conferência re: Invent.

Considere as seguintes áreas para determinar quais mudanças (se houver) você precisa fazer nas suas atuais arquiteturas e práticas de segurança. Isso ajudará você com uma estratégia simples e planejada de adoção da AWS.

- **Identidade e acesso** – integre o uso da AWS ao ciclo de vida da força de trabalho da organização, bem como às fontes de autenticação e autorização. Crie políticas granuladas e funções associadas com usuários e grupos. Crie proteções que permitem alterações importantes somente por meio de automação e impedem alterações não desejadas ou as reverte automaticamente. Essas etapas reduzirão o acesso humano a sistemas de produção e dados.
- **Proteção da infraestrutura** – implemente uma linha de base de segurança incluindo limites de confiança, configuração e manutenção de segurança de sistemas (por exemplo, “harden and patch”) e outros pontos adequados de aplicação de política (por exemplo, security groups, AWS WAF, Amazon API Gateway) para atender as necessidades que você identificou usando o componente Diretiva.
- **Proteção de dados** – utilize as proteções adequadas para proteger dados em trânsito e em repouso. As proteções incluem controles granulados de acesso a objetos, criando e controlando as chaves de criptografia usadas para criptografar seus dados, selecionando métodos de criptografia e tokenização, validação de integridade e retenção adequada de dados.

Considerações

- **Trate** segurança como código, permitindo que você implante e valide a infraestrutura de segurança de forma a proporcionar escala e agilidade para proteger a organização.
- **Crie** proteções, padrões confidenciais e modelos de oferta e melhores práticas como código.
- **Crie** serviços de segurança que a organização pode utilizar para funções de segurança altamente repetitiva ou particularmente confidenciais.
- **Defina** atores e faça um esboço de suas experiências interagindo com os serviços da AWS.
- **Use** a ferramenta AWS Trusted Advisor para avaliar continuamente sua postura de segurança da AWS e considere fazer uma revisão bem arquitetada da AWS.
- **Estabeleça** uma linha de base minimamente viável e itere continuamente para elevar o nível das cargas de trabalho que você está protegendo.

O componente Detecção

O componente Detecção da Perspectiva de segurança AWS CAF fornece diretrizes para a obtenção de visibilidade na postura de segurança da sua organização. Diversos dados e informações podem ser reunidos usando serviços como o AWS CloudTrail, registros específicos de serviço e valores de retorno API/CLI. Incluir essas fontes de informação em uma plataforma escalável para gerenciamento e monitoramento de registros, gerenciamento de eventos, testes e inventários/auditorias dará a você a transparência e a agilidade operacional de que você precisa para sentir-se confiante na segurança das suas operações.

- **Registro e monitoramento** – a AWS fornece registro nativo assim como serviços que você pode utilizar para proporcionar maior visibilidade quase em tempo real para ocorrências no ambiente da AWS. Você pode usar essas ferramentas para integrar suas soluções de registro e monitoramento existentes. Integre profundamente a saída de registro e as fontes de monitoramento ao fluxo de trabalho da organização de TI para obter a resolução completa de atividades relacionadas a segurança.
- **Testes de segurança** – teste o ambiente da AWS para garantir que sejam atendidos os padrões de segurança definidos. Você estará melhor preparado para eventos reais executando testes para determinar se os seus sistemas responderão como esperado quando certos eventos ocorrerem. São alguns exemplos de testes de segurança: varredura de vulnerabilidades, teste de penetração e injeção de erro para verificar se os padrões estão sendo atendidos. O objetivo é determinar se seu controle responderá como esperado.
- **Inventário de ativos** – conhecer as cargas de trabalho que você implantou e o processo operacional permitirá que você monitore e garanta que o ambiente esteja operando nos níveis de governança da segurança esperados e demandados pelos padrões de segurança.
- **Detecção de alterações** – depender de uma linha de base segura de controles preventivos também requer saber quando esses controles são alterados. Implemente medidas para transitar entre configuração segura e estado atual.

Considerações

- **Determine** quais informações de registro para o seu ambiente AWS você deseja capturar, monitorar e analisar.
- **Determine** como a capacidade de negócios do centro de operações de segurança (SOC) integrará o monitoramento e o gerenciamento de segurança da AWS às práticas existentes.
- **Conduza** continuamente verificações de vulnerabilidade e testes de penetração de acordo com procedimentos da AWS para isso.

O componente Resposta

O componente Resposta da Perspectiva de segurança AWS CAF fornece diretrizes para a parte responsiva da postura de segurança da sua organização. Ao incorporar seu ambiente AWS em sua postura de segurança e preparar e simular ações que requerem resposta, você estará melhor preparado para responder aos incidentes quando ocorrerem.

Com o processo de resposta e recuperação de incidentes automatizado e a habilidade de minimizar partes da recuperação de desastres, é possível mudar o foco principal da equipe de segurança, de resposta para execução de forense e análise de causa principal. Como parte da adaptação da sua postura de segurança, algumas coisas devem ser consideradas:

- **Resposta a incidentes** – durante um incidente, conter o evento e retornar a um bom estado conhecido são elementos importantes de um plano de resposta. Por exemplo, automatizar aspectos dessas funções usando as regras do AWS Config e os scripts de resposta do AWS Lambda permite que você escalone sua resposta na velocidade da Internet. Revise os atuais processos de resposta a incidentes e determine se e como o processo de resposta e recuperação automatizado se tornará operacional e gerenciado para ativos da AWS. As funções do centro de operações de segurança devem estar fortemente integradas com as APIs da AWS para que sejam o mais responsivas possível. Isso determina a função de monitoramento e gerenciamento de segurança para a adoção da Nuvem AWS.
- **Simulações de resposta a incidentes de segurança** – ao simular eventos, você pode garantir que os controles e processos instalados reajam como esperado. Usando essa abordagem, você pode determinar se está efetivamente apto para recuperar e responder a incidentes quando ocorrem.
- **Forense** – na maioria dos casos, suas ferramentas forenses funcionarão no ambiente da AWS. As equipes forenses se beneficiarão da implantação automatizada de ferramentas em todas as regiões e da habilidade de coletar grandes volumes de dados rapidamente, com baixo atrito usando os mesmos serviços robustos e escaláveis sobre os quais são criados aplicativos críticos para a empresa, como Amazon Simple Storage Service (S3), Amazon Elastic Block Store (EBS), Amazon Kinesis, Amazon DynamoDB, Amazon Relational Database Service (RDS), Amazon RedShift e Amazon Elastic Compute Cloud (EC2).

Considerações

- **Atualize** seus processos de resposta a incidentes para que reconheçam o ambiente da AWS.
- **Utilize** os serviços na AWS para preparar forensicamente suas implantações por meio da seleção de recursos e da automação.
- **Automatize** a resposta para obter solidez e escala.
- **Use** os serviços na AWS para a coleção e a análise de dados como suporte a uma investigação.
- **Valide** sua capacidade de resposta a incidentes por meio de simulações de respostas a incidentes de segurança.

Início da jornada – definindo uma estratégia

Revise sua atual estratégia de segurança para determinar se partes da estratégia se beneficiariam das mudanças como parte de uma iniciativa de adoção da nuvem. Mapeie sua estratégia de adoção da Nuvem AWS de acordo com o nível de risco que sua empresa está disposta a aceitar, sua abordagem para alcançar objetivos regulatórios e de conformidade e suas definições do que precisa ser protegido e como será protegido. A Tabela 1 mostra um exemplo de uma estratégia de segurança que articula um conjunto de princípios que são mapeados para iniciativas e fluxos de trabalho específicos.

Princípio	Exemplos de ações
Desenvolva a infraestrutura como código.	Capacitar a equipe de segurança em código e automação; migrar para DevSecOps.
Crie proteções, não portas.	Arquitetar unidades para bom funcionamento.
Use a nuvem para proteger a nuvem.	Crie, opere e gerencie ferramentas de segurança na nuvem.
Atualize-se; mantenha-se seguro.	Consumir novos recursos de segurança; corrigi-los e substitui-los com frequência.
Reduza a dependência sobre o acesso persistente.	Estabelecer um catálogo de funções; automatizar KMI via serviço secreto.
Visibilidade total	Agregar registros e dados da AWS ao SO e a registros de aplicativos.
Perspectivas aprofundadas	Implementar um data warehouse de segurança com BI e análise.
Resposta a incidentes (IR) escalonável.	Atualizar a IR e os procedimentos operacionais padrão (SOP) forenses para obter a estrutura de responsabilidade compartilhada.
Autorrecuperação	Automatizar a correção e a restauração para um bom estado conhecido.

Tabela 1: Exemplo de estratégia de segurança

À medida que sua estratégia evolui, você desejará começar a iterar as estruturas de garantia terceirizadas e os requisitos de segurança organizacionais e a incorporar a uma estrutura de gerenciamento de riscos que guiará sua jornada à AWS. Evoluir seu mapeamento de conformidade é, muitas vezes, uma prática efetiva à medida que você entende melhor as necessidades das suas cargas de trabalho na nuvem e os recursos de segurança fornecidos pela AWS.

Outro elemento chave da sua estratégia é fazer o mapeamento usando o modelo de responsabilidade compartilhada específico para seu ecossistema. Além do relacionamento macro compartilhado com a AWS, você desejará explorar responsabilidades internas organizacionais compartilhadas, bem como as que você partilha com seus parceiros. As empresas podem dividir seu modelo de responsabilidade compartilhada em três áreas importantes: uma estrutura de controle, um modelo responsável, consultado e informado (RACI) e um registro de riscos. A estrutura de controle descreve como os aspectos de segurança da empresa devem trabalhar e quais controles serão instalados para gerenciar riscos. Você pode usar o RACI para identificar e designar uma pessoa com responsabilidade para os controles na estrutura. Por fim, use um registro de riscos para capturar controles sem propriedade adequada. Priorize riscos residuais que foram identificados, alinhando seu tratamento com novos fluxos de trabalho e iniciativas instauradas para solucioná-las.

À medida que você mapeia essas responsabilidades compartilhadas você pode esperar encontrar novas oportunidades de automatizar operações e melhorar o fluxo de trabalho entre atores críticos em sua comunidade de segurança, conformidade e gerenciamento de riscos. A Figura 2 mostra um exemplo de modelo de responsabilidade compartilhada.

Figura 2: Exemplo de modelo de responsabilidade compartilhada

Considerações

- **Crie** uma estratégia personalizada que trate da abordagem da sua organização para implementar a segurança na nuvem.
- **Promova** a automação como um tema subjacente para todas as suas estratégias.
- **Articule** claramente sua abordagem para a nuvem primeiro.
- **Promova** agilidade e flexibilidade definindo proteções.
- **Adote** a estratégia como um exercício rápido que define a abordagem da sua organização para a segurança de informações na nuvem.
- **Itere** rapidamente enquanto estabelece o que é a estratégia. Seu objetivo é ter um conjunto de princípios de orientação que levará adiante o centro dos esforços. A estratégia não é o fim em si mesma. Mova-se rapidamente e esteja disposto a adaptar-se e a evoluir.
- **Defina** princípios estratégicos que partilharão a cultura que você deseja em segurança e que informem as decisões de projeto que você tomará, em vez de uma estratégia que sugira soluções específicas.

Início da jornada – oferecendo um programa

Agora, com uma estratégia definida, é hora de colocá-la em prática e iniciar a implementação que transformará sua organização de segurança e proteger a jornada na nuvem. Enquanto você tem ampla variedade de opções e recursos, sua implementação não deve ser um esforço prolongado. Este processo de projetar e implementar como os diferentes recursos funcionarão juntos representa uma oportunidade para ganhar familiaridade rapidamente e aprender a como iterar seus projetos para melhor atender seus requisitos. Aprenda rápido com a real implementação e, então, adapte-se e evolua usando pequenas alterações enquanto aprende.

Figura 3: Épicos de segurança do AWS CAF

Para ajudar você com sua implementação, você pode usar os Épicos de segurança do CAF. (Ver Figura 3.) Os Épicos de segurança consistem em grupos de histórias de usuários (casos de uso e casos de abuso) com os quais você pode trabalhar durante sprints. Cada um desses épicos tem várias iterações que lidam com requisitos cada vez mais complexos e agregam solidez. Apesar de recomendarmos o uso de metodologias ágeis, os épicos também podem ser tratados como fluxos de trabalho em geral ou como tópicos que ajudam a priorizar e elaborar o resultado usando qualquer outra estrutura. Uma estrutura proposta consiste nos 10 seguintes épicos de segurança (Figura 4) para guiar sua implementação.

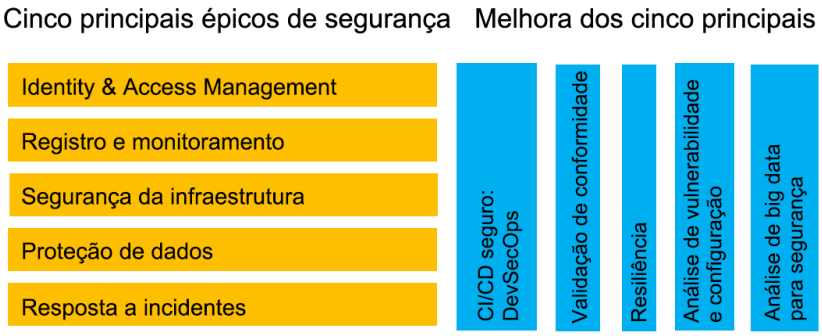

Figura 4: Os dez Épicos de segurança da AWS

Os cinco principais

Os cinco épicos a seguir constituem o controle principal e as categorias de recursos que você deve considerar desde o princípio, pois são fundamentais para iniciar sua jornada.

- **IAM** – o AWS Identity and Access Management (IAM) forma a espinha dorsal da implantação da AWS Na nuvem, você deve estabelecer uma conta e receber privilégios antes de poder provisionar ou orquestrar recursos. Histórias típicas de automação podem incluir mapeamento/concessões/ auditoria de qualificação, gerenciamento de material secreto, separação de execução de responsabilidades e de acesso com privilégio mínimo, gerenciamento de privilégios just-in-time e dependência decrescente de credenciais de longo prazo.
- **Registro e monitoramento** – os serviços da AWS fornecem uma diversidade de dados de registro para ajudá-lo a monitorar suas interações com a plataforma. O desempenho dos serviços da AWS baseados nas suas escolhas de configuração e a habilidade de incluir SO e registros de aplicativos para criar um quadro comum de referência. Histórias típicas de automação podem incluir agregação de registro, limites/alarme/alerta, enriquecimento, plataforma de pesquisa, visualização, acesso a partes interessadas e fluxo de trabalho e tíquetes para iniciar respostas organizacionais de circuito fechado.
- **Segurança da infraestrutura** – quando você trata a infraestrutura como código, a infraestrutura de segurança torna-se a primeira carga de trabalho de nível que também deve ser implantada como código. Essa abordagem dará a você a oportunidade de configurar programaticamente os serviços da AWS e implantar a infraestrutura de segurança da AWS

Parceiros do mercado ou soluções do seu próprio projeto. Histórias típicas de automação podem incluir criar modelos personalizados para configurar serviços da AWS para atender suas necessidades, implementar padrões de arquitetura de segurança e ações de operações de segurança como código, criar soluções de segurança personalizadas a partir dos serviços da AWS, usar estratégias de gerenciamento de patch como implantações azul/verde, reduzir a superfície de ataque exposta e validar a eficácia das implantações.

- **Proteção de dados** – proteger dados importantes é uma parte crítica na criação e operação de sistemas de informação, e a AWS fornece serviços e recursos dando a você opções robustas para proteger seus dados ao longo do ciclo de vida. Histórias típicas de automação podem incluir tomar decisões sobre disposição de cargas de trabalho, implementar um esquema de marcação, construir mecanismos para proteger dados em movimento como conexões VPN e TLS/SSL (incluindo AWS Certificate Manager), construir mecanismos para proteger dados em repouso por meio de criptografia nos níveis adequados da sua infraestrutura, usar a implementação/integração da AWS Key Management Service (AWS KMS), implantar o AWS CloudHSM, criar esquemas de tokenização e implantar e operar soluções de parceiro do AWS Marketplace.
- **Resposta a incidentes** – automatizar aspectos do seu processo de gerenciamento de incidentes melhora a confiabilidade e aumenta a velocidade da sua resposta e geralmente cria um ambiente mais fácil de acessar em revisões pós-ação. Histórias típicas de automação podem incluir usar a função “responders”, do AWS Lambda, que reage a alterações específicas no ambiente, orquestrar eventos de auto scaling, isolar componentes suspeitos do sistema, implantar ferramentas just-in-time de investigação e criar fluxos de trabalho e tíquetes para finalizar e aprender com uma resposta organizacional de circuito fechado.

Melhora dos principais

Estes cinco épicos representam os temas que motivarão a excelência operacional continuada por meio da disponibilidade, automação e auditoria. Você poderá integrar estes épicos criteriosamente em cada sprint. Quando é necessário foco adicional, você pode considerar tratá-los como seus próprios épicos.

- **Resiliência** – alta disponibilidade, continuidade de operações, solidez e resiliência e recuperação de desastres são razões frequentes para realizar implantações da nuvem com a AWS. Histórias típicas de automação podem incluir usar implantações Multi-AZ e Multirregião, alterar a superfície de ataque disponível, escalonar e mover a alocação de recursos para absorver ataques, proteger recursos expostos e induzir deliberadamente a falha de recursos para validar a continuidade de operações de sistema.
- **Validação de conformidade** – incorporar conformidade de ponta a ponta em seu programa de segurança impede que a conformidade seja reduzida a um exercício de caixa de seleção ou a uma sobreposição que ocorre após a implantação. Este épico fornece a plataforma que consolida e racionaliza os artefatos de conformidade gerados por meio dos outros épicos. Histórias típicas de automação podem incluir criar testes de unidade de segurança mapeados para requisitos de conformidade, projetar serviços e cargas de trabalho para dar suporte à coleta de evidências de conformidade, criar pipelines de conformidade para notificação e validação a partir de recursos comprovativos, monitorar continuamente e criar equipes de DevSecOps voltadas para ferramentas de conformidade.
- **CI/CD seguro (DevSecOps)** – ter confiança em sua cadeia de suprimento de software por meio do uso de integração contínua confiável e validada e de cadeias de ferramentas de implantação é uma forma de aprimorar práticas de operação de segurança enquanto você migra para a nuvem. Histórias típicas de automação podem incluir fortalecer e corrigir a cadeia de ferramentas, acesso com privilégio mínimo à cadeia de ferramentas, registro e monitoramento do processo de produção, visualização da integração/implantação de segurança e verificação da integridade do código.
- **Análise de configuração e vulnerabilidade** – a análise de configuração e vulnerabilidade se beneficia muito da escala, da agilidade e da automação proporcionadas pela AWS. Histórias típicas de automação podem incluir habilitar o AWS Config e criar regras do AWS Config, usar eventos do Amazon CloudWatch e do AWS Lambda para reagir à detecção de alterações, implementar o Amazon Inspector, selecionar e implantar soluções de monitoramento contínuo do AWS Marketplace, implantar verificações acionadas e incorporar ferramentas de avaliação às cadeias de ferramentas CI/CD.

- **Big data de segurança e análise preditiva** – as operações de segurança se beneficiam de serviços de big data e de soluções assim como qualquer outro aspecto da empresa. Utilizar big data permite que você tenha perspectivas mais aprofundadas de forma mais segura, portanto, aprimorando sua agilidade e habilidade para iterar em sua postura de segurança em escala. Histórias típicas de automação podem incluir criar data lakes de segurança, desenvolver pipelines de análise, criar visualização para impulsionar a tomada de decisão sobre segurança e estabelecer mecanismos de feedback para resposta autônoma.

Depois que essa estrutura é definida, um plano de implementação pode ser criado. Os recursos mudarão ao longo do tempo e as oportunidades de melhora serão continuamente identificadas. Como um lembrete, os temas ou as categorias de recursos acima podem ser tratados como épicos em uma metodologia ágil, que contém diversas histórias de usuários, incluindo casos de uso e casos de abuso. Vários sprints levarão a uma maior maturidade enquanto mantêm a flexibilidade para adaptar o ritmo ou a demanda da empresa.

Exemplos de séries de sprint

Considere organizar um conjunto de amostra de seis sprints de duas semanas (um grupo de épicos conduzidos ao longo de um trimestre), incluindo um período curto de preparação, da forma a seguir. Sua abordagem dependerá da disponibilidade de recursos, da prioridade e do nível de maturidade desejada em cada recurso à medida que você avança em direção à sua capacidade de produção minimamente viável (MVP).

- **Sprint 0** – cartografia de segurança: mapeamento de conformidade, mapeamento de políticas, revisão de modelo de ameaça inicial, definição de registro de riscos; criar uma lista de pendências de casos de uso e abuso; planejar os épicos de segurança
- **Sprint 1** – IAM; registro e monitoramento
- **Sprint 2** – IAM; registro e monitoramento; infraestrutura e proteção
- **Sprint 3** – IAM; registro e monitoramento; proteção de infraestrutura
- **Sprint 4** – IAM; registro e monitoramento; proteção de infraestrutura; proteção de dados
- **Spring 5** – proteção de dados, automação de operações de segurança, planejamento/ferramentas de resposta a incidentes; resiliência
- **Sprint 6** – automação de operações de segurança, reposta a incidentes, resiliência

Um elemento chave da validação de conformidade é incorporar a validação em cada sprint por meio de casos de teste de unidade de segurança e conformidade e passar pela promoção ao processo de produção. Quando a capacidade explícita de validação de conformidade é necessária, os sprints podem ser definidos para focar especificamente nessas histórias de usuários. Com o tempo, a iteração pode ser utilizada para alcançar a validação contínua e a implementação de autocorreção de desvios onde apropriado.

A abordagem em geral pretende definir claramente o que é uma MVP ou uma linha de base, o que mapeará o primeiro sprint em cada área. Nos estágios iniciais, o objetivo final pode ser menos definido, mas um mapa claro dos sprints iniciais é criado. Tempo, experiência e iteração permitirão refinar e ajustar o estado final para que ele seja perfeito para sua organização. Na verdade, o estágio final pode ser mudado continuamente, mas finalmente o processo leva a uma melhora contínua em um ritmo mais rápido. Esta abordagem pode ser mais eficaz e ter maior eficiência de custos do que uma abordagem inovadora baseada em cronogramas longos e despesas de capital altas.

Analisando com mais profundidade, o primeiro sprint para IAM pode consistir em definir a estrutura da conta e implementar o conjunto básico de melhores práticas. Um segundo sprint pode implementar federação. Um terceiro sprint pode expandir o gerenciamento de contas para atender várias contas e assim por diante. Histórias de usuários de IAM que podem abranger um ou mais desses sprints iniciais poderiam incluir histórias como estas:

"Como administrador de acesso, quero criar um conjunto inicial de usuários para gerenciar acesso privilegiado e relacionamentos de confiança do provedor de identidades da federação."

"Como administrador de acesso, quero mapear usuários no meu diretório corporativo existente para papéis funcionais ou conjuntos de qualificações de acesso, na plataforma AWS."

"Como administrador de acesso, quero aplicar a autenticação multifator em todas as interações com o console da AWS por meio de usuários interativos."

Neste exemplo, as histórias de usuários de registro e monitoramento podem abranger um ou mais desses sprints iniciais:

"Como analista de operações de segurança, quero receber registros no nível da plataforma para todas as regiões e contas da AWS."

"Como analista de operações de segurança, quero todos os registros no nível da plataforma fornecidos para um local compartilhado de todas as regiões e contas da AWS."

"Como analista de operações de segurança, quero receber alertas para qualquer operação que conecte as políticas do IAM a usuários, grupos ou funções."

Você pode criar recursos em paralelo ou de maneira serial e manter a flexibilidade incluindo histórias de usuários sobre recursos de segurança na lista de pendências de produtos em geral. Você também pode dividir as histórias de usuários entre uma equipe de DevOps com foco em segurança. Essas são decisões que você pode revisitar periodicamente, permitindo que você adapte seu fornecimento às necessidades da organização ao longo do tempo.

Considerações

- **Revise** sua estrutura de controle existente para determinar como os serviços da AWS serão operados para atender aos padrões de seguranças exigidos.
- **Defina** atores e faça um esboço de suas experiências interagindo com os serviços da AWS.
- **Defina** qual é o primeiro sprint e qual será o objetivo inicial de alto nível a longo prazo.
- **Estabeleça** uma linha de base minimamente viável e itere continuamente para elevar o nível das cargas de trabalho e dos dados que você está protegendo.

Início da jornada – desenvolver operações de segurança robustas

Em um ambiente onde a infraestrutura é código, a segurança também deve ser tratada como código. O componente de Operações de segurança fornece um meio de comunicar e operacionalizar os princípios fundamentais de segurança como código:

- Use a nuvem para proteger a nuvem.
- A infraestrutura de segurança deve reconhecer a nuvem.
- Exponha recursos de segurança como serviços usando a API.
- Automatize tudo, para que sua segurança e conformidade possam ser escalonadas.

Para tornar esse modelo de governança prático, as linhas da empresa se organizam como equipes de DevOps para criar e implantar a infraestrutura e o software da empresa. Você pode estender os princípios fundamentais do modelo de governança integrando segurança à sua cultura ou prática de DevOps, que é chamada, às vezes, de DevSecOps. Forme uma equipe em torno dos seguintes princípios:

- A equipe de segurança adere às culturas e aos comportamentos de DevOps.
- Os desenvolvedores contribuem abertamente para programar operações usadas a automatizadas de segurança.
- A equipe de operações de segurança está habilitada a participar de testes e automação de código de aplicativos.
- A equipe se orgulha em implantar de forma rápida e frequente. Implantar mais frequentemente, com pequenas alterações, reduz o risco operacional e mostra o progresso rápido em relação à estratégia de segurança.

Equipes de desenvolvimento integrado, segurança e operações têm três missões-chave compartilhadas.

- Fortalecer a cadeia de ferramentas de integração contínua/implantação contínua.
- Permitir e promover o desenvolvimento de softwares resilientes à medida que percorre a cadeia de ferramentas.
- Implantar toda a infraestrutura e o software de segurança por meio da cadeia de ferramentas.

Determinar as mudanças (se for o caso) para práticas de segurança atuais ajudará você a planejar uma estratégia simples de adoção da AWS.

Conclusão

À medida que você embarca em sua jornada de adoção da AWS, você poderá atualizar sua postura de segurança para incluir a parte da AWS do seu ambiente. Este whitepaper sobre a Perspectiva de segurança guia você, prescritivamente, em uma abordagem para aproveitar os benefícios que a operação na AWS tem para sua postura de segurança. Há muitas outras informações de segurança disponíveis no site da AWS, onde os recursos de segurança são descritos em detalhes e é oferecida uma orientação prescritiva mais detalhada para implementações comuns. Também há uma lista abrangente de conteúdo com foco em segurança[4] que deve ser revisado por vários membros da sua equipe de segurança enquanto você se prepara para iniciativas de adoção da AWS.

Apêndice A: Monitorando o progresso na Perspectiva de segurança AWS CAF

Você pode usar os principais capacitadores de segurança e o modelo de progresso dos épicos de segurança discutidos neste apêndice para medir o progresso e a maturidade da sua implementação da Perspectiva de segurança AWS CAF. Os capacitadores e o modelo de progresso podem ser usados para fins de planejamento de projeto, para avaliar a solidez das implementações ou simplesmente como um meio de conduzir o debate sobre o caminho a percorrer.

Principais capacitadores de segurança

Os principais capacitadores de segurança são metas que ajudam você a permanecer atualizado. Usamos um modelo de pontuação que consiste em três valores: não abordado, engajado e completo.

- Estratégia de segurança da nuvem [não abordado, engajado, completo]
- Plano de comunicação da parte interessada [não abordado, engajado, completo]
- Cartografia de segurança [não abordado, engajado, completo]
- Modelos de documento de responsabilidade compartilhada [não abordado, engajado, completo]
- Manuais de operações de segurança [não abordado, engajado, completo]
- Plano de épicos de segurança [não abordado, engajado, completo]
- Simulação de resposta a incidentes de segurança [não abordado, engajado, completo]

Modelo de progresso dos épicos de segurança

O modelo de progresso dos épicos de segurança ajuda você a avaliar seu progresso na implementação dos 10 épicos de segurança descritos neste documento. Usamos um modelo de pontuação de 0 (zero) a 3 para medir a solidez. Fornecemos exemplos dos épicos do Identity and Access Management e de registro e monitoramento para que você veja como funciona esse progresso.

5 principais épicos

0 – não abordado

1 – Abordado em arquitetura e planos

2 – implementação mínima viável

3 – Implementação da produção pronta da empresa

Épico de segurança	0	1	2	3
Identity and Access Management	Exemplo: Nenhuma relação entre identidades no local e da AWS.	Exemplo: Uma abordagem é definida para o gerenciamento de identidades do ciclo de vida da força de trabalho. A arquitetura da IAM é documentada. As funções de trabalho são mapeadas para as necessidades da política do IAM.	Exemplo: IAM implementado conforme definido na arquitetura. Políticas do IAM implementadas que são mapeadas para algumas funções de trabalho. Implementação do IAM validada.	Exemplo: Automação dos fluxos de trabalho do ciclo de vida do IAM.
Registro e monitoramento	Exemplo: Nenhuma utilização das soluções de registro e monitoramento fornecidas pela AWS.	Exemplo: Uma abordagem é definida para agregação, monitoramento e integração de registros em processos de gerenciamento de eventos de segurança.	Exemplo: O registro no nível da plataforma e no nível de serviço é ativado e centralizado.	Exemplo: Eventos com implicações de segurança são integrados profundamente ao fluxo de trabalho de segurança e aos processos e sistemas de gerenciamento de incidentes.
Segurança da infraestrutura				
Proteção de dados				
Gerenciamento de incidentes				

Melhora dos 5 principais épicos

0 – não abordado

1 – Abordado em arquitetura e planos

2 – implementação mínima viável

3 – Implementação da produção pronta da empresa

Épico de segurança	0	1	2	3
Resiliência				
DevSecOps				
Validação de conformidade				
Gerenciamento de vulnerabilidade e configuração				
Big data de segurança				

Taxonomia e termos do CAF

O Cloud Adoption Framework (CAF) é a estrutura que a AWS criou para capturar as diretrizes e as melhores práticas de engajamentos anteriores com clientes. Uma *perspectiva* do AWS CAF representa uma área de enfoque relevante à implementação de sistemas de TI baseados em nuvem nas organizações. Por exemplo, a Perspectiva de segurança fornece diretrizes e processos para avaliar e aprimorar seus controles de segurança existentes enquanto você muda para o ambiente da AWS.

Cada perspectiva do CAF é constituída de componentes e atividades. Um *componente* é uma subárea de uma perspectiva que representa um aspecto específico que requer atenção. Este whitepaper explora os componentes da Perspectiva de segurança. Uma *atividade* apresenta diretrizes mais prescritivas para criar planos práticos que a organização pode usar para migrar para a nuvem e operar soluções baseadas em nuvem de maneira contínua.

Por exemplo, *Diretiva* é um componente da Perspectiva de segurança e adaptar um modelo de responsabilidade compartilhada da AWS para seu ecossistema pode ser uma atividade dentro desse componente.

Quando combinadas, o Cloud Adoption Framework (CAF) e a Cloud Adoption Methodology (CAM) podem ser usadas como diretrizes durante sua jornada para a Nuvem AWS.

Observações

[1] https://do.awsstatic.com/whitepapers/aws_cloud_adoption_framework.pdf

[2] https://aws.amazon.com/compliance/

[3] https://aws.amazon.com/compliance/shared-responsibility-model/

[4] https://aws.amazon.com/security/security-resources/