FIREEYE™

Ficha técnica

Arquitetura de nuvem e Avaliação da segurança

Aprimore as defesas cibernéticas por meio de melhores configurações e arquitetura de nuvem

Principais vantagens

- **Entender** as ameaças à arquitetura específica do seu ambiente de nuvem
- **Mitigar** falhas de configuração de arquitetura de nuvem comumente exploradas
- **Reduzir** sua superfície de ataque das técnicas de exploração comuns
- **Ganhar visibilidade** dos principais riscos de segurança relacionados às configurações existentes
- **Melhorar** o monitoramento, a visibilidade e a detecção na nuvem
- **Priorizar** as melhorias de segurança certas para o seu ambiente de nuvem

Por que contar com a FireEye Mandiant?
A FireEye Mandiant está na linha de frente da inteligência em segurança cibernética e ameaças cibernéticas desde 2004. Os responsáveis pela resposta a incidentes estão nas linhas de frente das violações mais complexas do mundo. Temos um profundo conhecimento sobre os agentes de ameaça existentes e emergentes, bem como sobre suas táticas, técnicas e procedimentos extremamente dinâmicos.

Visão geral
Para reduzir os custos e melhorar a escalabilidade, as empresas estão cada vez mais migrando seus ativos de dentro das instalações para a nuvem. Em resposta, os atacantes estão realinhando suas táticas e técnicas, incluindo engenharia social e explorando os erros de configuração para visar ambientes de nuvem.

A Arquitetura de nuvem e a Avaliação da segurança da FireEye Mandiant avalia seu atual estado de segurança e recomenda solidificar as prioridades para ativos nas plataformas de nuvem mais populares: Microsoft Azure, Amazon Web Services e Google Cloud Platform.

Esta avaliação ajuda a sua empresa a entender as ameaças e controles de segurança exclusivos do seu ambiente de nuvem específico, solidifica o ambiente contra ameaças visadas e melhora sua habilidade em detectar, investigar e responder à atividade do atacante por todas as fases do ciclo de vida do ataque.

Esses serviços foram criados para as empresas usando provedores de serviços de nuvem compatíveis com um modelo de infraestrutura como serviço (infrastructure as a service, IaaS) ou plataforma como serviço (platform as a service, PaaS). Esses modelos dependem das responsabilidades compartilhadas entre o provedor de serviços de nuvem e o cliente para a proteção contra acidentes cibernéticos. Nossa avaliação foca nas responsabilidades do cliente que fortalecerão sua postura de segurança.

Nossa abordagem

A avaliação consiste em quatro fases, durante as quais os especialistas da Mandiant mapeiam seu ambiente de nuvem existente e determinam como seu atual programa de segurança funciona para protegê-lo:

Semana 1: Revisão inicial do documento de estratégias de migração, diagramas de arquitetura, documentação de fortalecimento, políticas e padrões de gestão de acesso, padrões de logs e SOPs/playbooks, conduzindo externamente em colaboração com as partes interessadas dos clientes.

Semana 2: Workshops no local para explorar seu ambiente de nuvem, o atual modelo de segurança implementado e potenciais conceitos e controles de segurança para implementar no futuro para atender suas necessidades comerciais.

Semanas 3-4: Revisão de configuração a partir da plataforma de nuvem, para assegurar que os controles de segurança sejam implementados com eficácia, identificar possíveis fraquezas e confirmar os aprendizados dos workshops no local para identificar possíveis fraquezas que podem ser exploradas pelos atacantes.

Semana 5: Geração de relatórios que detalham recomendações técnicas práticas para fortalecer o ambiente de nuvem, aprimorar a visibilidade e a detecção e melhorar os processos para reduzir o risco de comprometimento.

MATERIAIS ENTREGUES

O relatório de pós-avaliação fornecido pela Mandiant inclui

- Um snapshot do seu atual ambiente de nuvem, detalhando os controles de arquitetura e de segurança existentes.
- Segurança para serviços de nuvem específicos alinhados com suas atuais configurações e processos operacionais.
- Recomendações práticas para melhorar a visibilidade e a detecção.
- Recomendações priorizadas e detalhadas para solidificar ainda mais sua infraestrutura de nuvem.

Resumos técnicos e executivos estão disponíveis mediante solicitação.

Principais áreas de foco para avaliação durante a análise.

Governança, risco e conformidade

- Governança e serviços de nuvem
- Políticas e padrões de nuvem
- Avaliações de risco de ameaças
- Gestão de vulnerabilidades
- Exigências de conformidade regulatória

Rede e arquitetura de segurança

- Controles de segurança e arquitetura de nuvem
- Segmentação de rede e integração no local
- Conectividade e gestão de sistema remoto
- Recuperação de desastres
- Contêineres, configurações e controles de segurança

Gerenciamento de acessos e identidades

- Infraestrutura de autenticação de nuvem, inclusive conectividade no local (p. ex., ADFS)
- Gestão de identidades
- Gestão de acesso de privilégios
- Controles de acesso com base em papéis

Proteção de dados e segredos

- Proteção de dados e prevenção de perdas
- Segurança do banco de dados
- Certificados e gestão de senhas
- Criptografia

DevOps

- Configurações de pipeline
- Implantação de sistema e de aplicação
- Ciclo de vida seguro de desenvolvimento de software
- Controles de segurança de repositório de códigos

Detecção e resposta a ameaças

- Logs de sistema, banco de dados e aplicação
- Logs e centralização de segurança
- Controles de segurança de rede e de terminais
- Processos de resposta de acidentes de nuvem

Para saber mais sobre a FireEye, visite: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

Sobre a FireEye, Inc.

A FireEye é a empresa líder em segurança orientada por inteligência. Atuando harmoniosamente como extensão expansível das operações de segurança dos clientes, a FireEye oferece uma plataforma única que mescla tecnologias de segurança inovadoras, inteligência contra ameaças em nível governamental e a consultoria mundialmente reconhecida da Mandiant®. Com essa abordagem, a FireEye elimina a complexidade e o fardo da segurança cibernética para organizações empenhadas em se preparar, prevenir e responder a ataques cibernéticos.

FIREEYE™