FIREEYE™

FICHA TÉCNICA

Cloud Architecture and Security Assessment

Mejorar las defensas cibernéticas a través de una mejor arquitectura y configuraciones en la nube

VENTAJAS PRINCIPALES

- **Comprender** las amenazas a su arquitectura del entorno en la nube específica
- **Mitigar** los errores de configuración comunes que se aprovechan en la arquitectura en la nube
- **Reducir** la superficie de ataque provenientes de técnicas de ataques comunes
- **Obtener visibilidad** de los riesgos de seguridad principales relacionados con la configuración existente
- **Mejorar** la supervisión, visibilidad y detección en la nube
- **Priorizar** las mejoras de seguridad correctas para el entorno en la nube

Por qué FireEye Mandiant

FireEye Mandiant ha sido el líder en cuanto a ciberseguridad e inteligencia sobre amenazas cibernéticas desde 2004. Nuestros responsables de la respuesta ante incidentes están en las primeras líneas de las brechas más complejas en todo el mundo. Tenemos una comprensión exhaustiva en lo que respecta a perpetradores existentes y emergentes, además de sus tácticas, técnicas y procedimientos que cambian rápidamente.

Descripción general

Para reducir los costos y mejorar la escalabilidad, las organizaciones están migrando cada vez más sus activos locales a la nube. En respuesta, los atacantes están reorientando sus tácticas y técnicas, incluida la ingeniería social y la explotación de errores de configuración, para atacar a los entornos de nube.

FireEye Mandiant Cloud Architecture and Security Assessment evalúa su estado actual de seguridad y recomienda reforzar las prioridades de los activos en las plataformas de nube más populares: Microsoft Azure, Amazon Web Services y Google Cloud Platform.

Esta evaluación ayuda a su organización a comprender las amenazas y los controles de seguridad exclusivos para su entorno de nube específico, fortalece el entorno frente a las amenazas específicas y mejora su capacidad de detectar, investigar y responder a la actividad del atacante en todas las fases del ciclo de vida del ataque.

Estos servicios están diseñados para organizaciones que utilizan proveedores de servicios en la nube que admiten un modelo de infraestructura como servicio (Infrastructure as a Service, IaaS) o de plataforma como servicio (Platform as a Service, PaaS). Estos modelos se basan en responsabilidades compartidas entre el proveedor de servicios en la nube y el cliente para protegerse contra incidentes cibernéticos. Nuestra evaluación se enfoca en las responsabilidades del cliente que fortalecerán su nivel de seguridad.

Nuestro método

La evaluación consta de cuatro fases, durante las cuales los expertos de Mandiant evalúan el entorno de nube existente y determinan cómo funciona su programa de seguridad actual para protegerlo:

Semana 1: Revisión inicial de documentos de estrategias de migración, diagramas de arquitectura, documentación de refuerzo, políticas y estándares de gestión de acceso, SOP/tácticas y estándares de inicio de sesión, realizados fuera del sitio en colaboración con las partes interesadas del cliente.

Semana 2: Talleres en el sitio para explorar el entorno de la nube, el modelo de seguridad actual existente, y conceptos y controles potenciales de seguridad a implementarse en el futuro con el fin de satisfacer sus necesidades comerciales.

Semanas 3 a 4: Revisión de la configuración desde la plataforma en la nube para garantizar que los controles de seguridad se implementen con eficacia, identificar las deficiencias potenciales y confirmar el aprendizaje en los talleres en el sitio de modo de identificar deficiencias potenciales que los atacantes puedan explotar.

Semana 5: Informes que detallan las recomendaciones técnicas prácticas a fin de fortalecer el entorno en la nube, mejorar la visibilidad y la detección, y mejorar los procesos para reducir el riesgo de vulneración.

RESULTADOS

El informe posterior a la evaluación proporcionado por Mandiant incluye

- Una instantánea de su entorno actual en la nube, que detalla la arquitectura y los controles de seguridad existentes.
- La seguridad de los servicios en la nube específicos que se alinean con las configuraciones y procesos operativos actuales.
- Las recomendaciones prácticas para mejorar la visibilidad y la detección.
- Las recomendaciones priorizadas y detalladas para reforzar aún más su infraestructura en la nube.

Los informes de nivel técnico y ejecutivo están disponibles a petición.

Áreas de enfoque principales de análisis durante la evaluación.

Gestión, riesgo y cumplimiento	Arquitectura y redes de seguridad	Gestión de identidad y acceso
• Gestión corporativa y servicios en la nube • Políticas y estándares en la nube • Evaluación de riesgos de amenazas • Gestión de la vulnerabilidad • Requisitos de cumplimiento de normativas	• Arquitectura en la nube y controles de seguridad • Segmentación de redes e integración en el sitio • Conectividad y gestión remota del sistema • Recuperación ante desastres • Contenedores, configuración y controles de seguridad	• Infraestructura de autenticación en la nube, incluyendo la conectividad en el sitio (p. ej.: ADFS) • Gestión de identidad • Gestión de acceso con privilegios • Controles de acceso basados en funciones
Protección de datos y secretos	**Desarrollo y operaciones**	**Detección de y respuesta ante amenazas**
• Protección y prevención de pérdidas de datos • Seguridad de la base de datos • Gestión de certificados y claves • Cifrado	• Configuración de la línea de productos • Implementación de sistemas y aplicaciones • Ciclo de vida seguro del desarrollo del software • Controles de seguridad del repositorio de código	• Sistema, base de datos y registro de aplicaciones • Inicio de sesión y centralización de seguridad • Controles de seguridad de redes y del endpoint • Procesos de respuesta ante incidentes en la nube

Para obtener más información sobre FireEye, visite: **www.FireEye.com**

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

Acerca de FireEye, Inc.

FireEye es una empresa de seguridad basada en inteligencia. FireEye, que funciona como una extensión escalable y transparente de las operaciones de seguridad del cliente, ofrece una sola plataforma que combina tecnologías innovadoras de seguridad, inteligencia sobre amenazas similar a la de una nación y los servicios de consultoría de fama mundial de Mandiant®. Gracias a este enfoque, FireEye elimina la complejidad y la carga de la seguridad cibernética para las organizaciones que desean estar preparadas y responder ante los ataques cibernéticos, además de prevenirlos.

FIREEYE™