FIREEYE™

FICHA TÉCNICA

Ejercicio de simulación

Evalúe su plan de respuesta a incidentes cibernéticos a través de un escenario simulado

VENTAJAS

- Identificación de las diferencias entre las respuestas documentadas y esperadas en comparación a lo que ocurre en realidad.
- Recomendaciones basadas en las mejores prácticas de respuesta a incidentes del mundo real.
- Evaluación rápida, eficiente y no invasiva.

"Poder responder con eficiencia y eficacia ante los incidentes de seguridad es fundamental para nuestro negocio. Los ejercicios de simulación resultaron muy valiosos, ya que proporcionaron a los equipos los medios para validar decisiones y participar en debates".

-Director de Seguridad de la Información de una empresa de distribución de tecnología global

Por qué elegir FireEye Mandiant

FireEye Mandiant ha sido el líder en materia de ciberseguridad e información sobre amenazas cibernéticas desde 2004. Nuestros responsables de la respuesta a incidentes están en las primeras líneas de las vulneraciones 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.

El ejercicio de simulación se apoya en esta experiencia para proporcionar aportes a escenarios personalizados basados en experiencias del mundo real y diseñados para abordar sus áreas clave de riesgo empresarial y técnico.

Descripción general

El ejercicio de simulación evalúa los procesos, las herramientas y la capacidad de su organización a la hora de responder a ciberataques, tanto desde el punto de vista ejecutivo y estratégico como técnico de la respuesta ante incidentes. Durante cada ejercicio, los consultores de Mandiant presentan varios aportes a escenarios basados en experiencias del mundo real en un entorno de mesa redonda para observar las acciones y las decisiones simuladas de la organización.

Método

Antes de comenzar un ejercicio de simulación, los expertos de Mandiant primero desarrollan una descripción del perfil de amenazas, el entorno operativo y las áreas de preocupación específicas de la organización del cliente. Realizamos un taller in situ con las personas clave y presentamos aportes a distintos escenarios basados en el comportamiento, las técnicas y las tácticas de los atacantes que se han observado durante nuestro trabajo de respuesta a incidentes.

Durante el ejercicio, observamos el escenario simulado para determinar cómo las acciones y las decisiones simuladas cumplen o no con los planes y los procesos documentados de la organización y las mejores prácticas de respuesta a incidentes identificadas por expertos de Mandiant.

LO QUE OBTIENE

Resumen ejecutivo [PPT]

- Descripción general en persona del desarrollo del escenario simulado, concretamente:
  - Interacción de los participantes con el plan de repuesta a incidentes (*Incident Response Plan*, IRP), la planificación de las comunicaciones y los procedimientos de escalación
  - Lecciones aprendidas
  - Recomendaciones estratégicas

Informe retrospectivo del ejercicio de simulación [PDF]

- Cronología de los eventos
  - Todos los aportes
  - Respuestas de las partes interesadas/participantes
- Análisis y recomendaciones estratégicos de respuesta a incidentes cibernéticos para mejorar en relación con el escenario simulado, clasificados por:
  - Detección
  - Respuesta
  - Contención
  - Corrección

Especializaciones

Ofrecemos dos especializaciones de los ejercicios de simulación: **la respuesta ante incidentes técnicos** y **la gestión de crisis a nivel ejecutivo**. Las mejores prácticas requieren que cada especialización se realice anualmente, por separado o como parte de un ejercicio coordinado.

La especialización en la respuesta ante incidentes técnicos es ideal para la gestión del equipo de seguridad y el personal que desea comprobar su capacidad de proceso de respuesta.

La especialización en la gestión de crisis a nivel ejecutivo es ideal para ejecutivos de cuerpos directivos que desean comprobar la efectividad de sus estrategias de respuesta ante crisis.

Después del taller, informamos personalmente a la organización y presentamos un informe retrospectivo por escrito que incluye un resumen paso a paso de los aportes y respuestas del escenario.

Comparación del seguimiento del servicio

Seguimiento del servicio	Técnico	Ejecutivo
Objetivo	Evaluar y analizar la capacidad de respuesta técnica de una organización para detectar, responder y contener una amenaza avanzada.	Evaluar y analizar las capacidades de gestión de crisis de una organización en caso de una amenaza avanzada desde la perspectiva del equipo ejecutivo.
Tiempo de contrato	• Planeamiento: 1 semana fuera del sitio • Escenario simulado: 1 a 2 días in situ • Informe final: 1 semana	• Planeamiento: 1 semana fuera del sitio • Escenario simulado: 1 a 2 días in situ • Informe final: 1 semana
Perfil del participante	• Equipo de respuesta ante incidentes de ciberseguridad (*Cyber Security Incident Response Team*, CSIRT) • Gerente de seguridad • Personal técnico (como los que trabajan con redes, servidores, correos electrónicos)	• Director de seguridad de la información (*Chief Information Security Officer*, CISO) • Ejecutivos generales de los cuerpos directivos • Relaciones públicas y comunicaciones corporativas • Asesor jurídico
Áreas de enfoque	• Cuándo aislar los hosts en una red • Cuándo duplicar un sistema de nuevo • Cómo los analistas deben seguir el IRP, el plan de comunicación y la matriz de escalación definidos • Cuándo y cómo involucrar a proveedores externos	• Cuándo pagar amenazas de extorsión o rescate • Toma de decisiones sobre el impacto de las tácticas de contención • Requisitos de divulgación de vulneraciones a reguladores y partes interesadas clave • Mejores prácticas para la notificación a los clientes • Mejores prácticas para la comunicación a los medios
Método de entrega	Escenario de simulación in situ	Escenario de simulación in situ

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 de amenazas. FireEye, que funciona como una extensión escalable y flexible de las operaciones de seguridad del cliente, ofrece una plataforma integral que combina tecnologías innovadoras de seguridad, información sobre amenazas a nivel de nación-estado y los servicios de consultoría de Mandiant® de fama mundial. Gracias a este método, FireEye elimina la complejidad y la carga de la ciberseguridad para las organizaciones que desean estar preparadas y responder a los ataques cibernéticos, además de prevenirlos.