FIREEYE™

FICHA TÉCNICA

ThreatSpace

Practique su capacidad de respuesta a amenazas del mundo real, sin exponerse a consecuencias reales.

VENTAJAS

- **Identificar las brechas y las oportunidades de mejora:** Investigar incidentes complejos, del mundo real para identificar brechas en la capacitación, los procesos, procedimientos y planes de comunicación.
- **Aprender de los expertos de respuesta a incidentes:** Trabajar estrechamente con experimentados responsables de la respuesta a incidentes de Mandiant que aprovechan años de experiencia en investigación basada en inteligencia de amenazas para evaluar y brindar sugerencias y asesoramiento en tiempo real.
- **Investigar incidentes de seguridad clave:** Haga que los equipos de respuesta e inteligencia de amenazas estén familiarizados con los escenarios de ataques más recientes y los TTP más relevantes del atacante con respecto a su organización, como se aprendió de las investigaciones de amenazas persistentes avanzadas (*Advanced Persistent Threat*, APT) de Mandiant.
- **Obtenga experiencia mediante distintos escenarios de ataques y perpetradores:** Evalúe y mejore la capacidad de los equipos de información y respuesta a incidentes a medida que responden a diversos escenarios de ataque y perpetradores.
- **Investigue y analice las amenazas identificadas:** Obtenga más información para investigar los TTP de los atacantes e identificar los indicadores de riesgo a partir de artefactos basados en host y artefactos basados en la red.

ThreatSpace es un servicio basado en tecnología que permite que su organización evalúe y desarrolle la capacidad que tiene su equipo de seguridad de responder a las amenazas del mundo real en un entorno libre de consecuencias. Mediante la utilización de un entorno virtualizado que simula una infraestructura de TI típica como segmentos de redes, estaciones de trabajo, servidores y aplicaciones, los equipos utilizan ThreatSpace para evaluar su capacidad técnica, los procesos y procedimientos a medida que investigan escenarios de ataques simulados.

Los escenarios, que se basan en la vasta experiencia de respuesta aincidentes de Mandiant para responder a miles de vulneraciones, incluyen las tácticas, técnicas y procedimientos (TTP) más recientes de los adversarios y y comprueban la capacidad de una organización para detectar, delimitar el alcance y neutralizar un ataque específico. Durante todo el proceso los expertos de respuesta a incidentes de Mandiant brindan sugerencias y orientación en tiempo real a fin de ayudar a mejorar la capacidad de su equipo de seguridad de responder a los ciberataques.

Nuestro método que se enfoca en el análisis y es independiente de la tecnología comprueba la capacidad que su equipo de seguridad tiene para identificar y priorizar los sistemas y artefactos forenses que se analizarán, entre ellos:

- **Sistemas, redes, cuentas de usuario y aplicaciones afectados**
- **Software malicioso y vulnerabilidades aprovechadas**
- **Acceso a y/o robo de información**

Los escenarios de ThreatSpace abarcan todas las fases del ciclo de vida de un ataque específico.

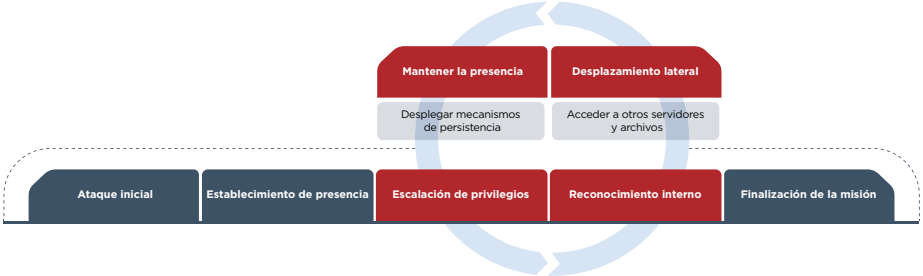

Figura 1. Ciclo de vida de ataque.

Prestación del servicio
Preparación remota

Identifique los escenarios

Revise las metas, expectativas y la logística

Analice los procesos y procedimientos de respuesta ante incidentes

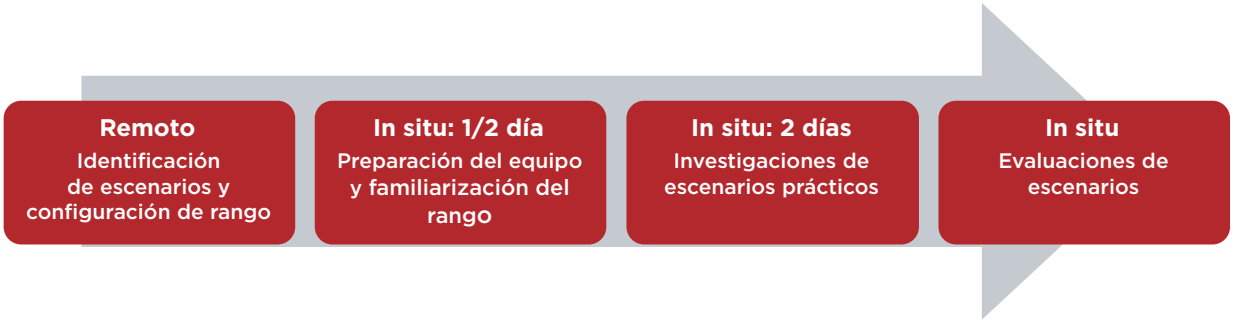

Figura 2. Flujo de trabajo para la preparación remota y prestación del servicio In situ

Escenarios in situ

- Medio día de capacitación y familiarización del rango.
- Dos días de investigaciones prácticas de un ataque simulado que progresa a través de las fases del ciclo de vida del ataque. Durante todo el escenario, los responsables de la respuesta a incidentes de Mandiant proporcionan sugerencias y orientación a los responsables de la respuesta a incidentes y a los analistas de ciberamenazas.
- Evaluaciones para revisar los logros y las fortalezas del equipo, además de detectar las brechas en la capacitación, los procesos y procedimientos, con recomendaciones de mejora.

Resultados

Después del contrato, recibirá un informe que identifica las fortalezas que se observaron y las mejoras que se recomiendan con respecto a las capacidades de respuesta a incidentes de su organización.

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 ante los ataques cibernéticos, además de prevenirlos.