FIREEYE™

FICHA TÉCNICA

Exercício de Simulação

Avalie o seu plano de resposta a incidentes cibernéticos por meio de cenário simulado

VANTAGENS

- Identifique lacunas entre as respostas documentadas e esperadas em comparação com o que realmente acontece.
- Recomendações com base nas melhores práticas de resposta a incidentes da vida real.
- Avaliação rápida, eficiente e não invasiva.

"A capacidade de responder, de forma eficaz e eficiente, aos incidentes de segurança é crucial para nossos negócios. Os exercícios de simulação foram relevantes por oferecerem meios para que as equipes validassem decisões e participassem de discussões."

-CISO de uma empresa global de distribuição de tecnologia

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. Nossos analistas estão na linha de frente dos incidentes mais complexos do mundo. Temos um profundo conhecimento sobre os agentes de ameaça existentes e emergentes, bem como sobre suas táticas, técnicas e procedimentos extremamente dinâmicos.

O exercício de simulação aproveita esse conhecimento para oferecer inserções de cenários personalizadas, embasadas em experiências reais e desenvolvidas para enfrentar suas principais áreas de risco técnico e empresarial.

Visão Geral
O exercício de simulação avalia os processos, as ferramentas e a proficiência da sua organização para responder a ataques cibernéticos, tanto da perspectiva estratégica executiva quanto técnica de resposta a incidentes. Durante cada exercício, consultores da Mandiant introduzem, em um ambiente de debate, várias inserções de cenários baseadas em experiências reais para observar as ações e decisões simuladas da organização.

Abordagem
Antes de iniciar um exercício de simulação, especialistas da Mandiant desenvolvem primeiro uma compreensão do perfil de ameaças, ambiente operacional e áreas específicas preocupantes da organização do cliente. Realizamos um workshop com pessoas-chave no local e introduzimos inserções de cenários que evoluem com base no comportamento, nas técnicas e táticas do atacante, observados durante nosso trabalho de resposta a incidentes.

Durante o exercício, observamos a atuação para determinar como as ações e decisões simuladas transcorrem concomitantemente ou divergem em relação aos planos e processos documentados da organização e às melhores práticas de resposta a incidentes identificadas por especialistas da Mandiant.

O QUE VOCÊ RECEBE

Resumo Executivo [PPT]

- Uma supervisão presencial da atuação, mais especificamente:
  - Interação dos participantes com o plano de resposta a incidentes (*Incident Response Plan*, IRP), com o(s) plano(s) de comunicação e com o(s) procedimentos(s) de escalonamento
  - Lições aprendidas
  - Recomendações estratégicas

Relatório pós-ação do exercício de simulação [PDF]

- Cronologia dos eventos
  - Todas as inserções
  - Respostas dos participantes/ partes interessadas
- Análise estratégica de resposta a incidentes cibernéticos e recomendações para aperfeiçoamento relacionadas à atuação, categorizadas por:
  - Detecção
  - Resposta
  - Contenção
  - Correção

Tipos

Oferecemos dois tipos de exercício de simulação: **resposta a incidentes técnicos** e **gerenciamento de crises executivo**. De acordo com as melhores práticas, cada tipo deve ser conduzido anualmente, separadamente ou integrado a um exercício coordenado.

O tipo Resposta a Incidentes Técnicos é ideal para o gerenciamento de equipes de segurança e funcionários que pretendem testar suas capacidades do processo de resposta.

O tipo Gerenciamento de Crises Executivo é ideal para executivos em nível de diretoria que desejam testar a eficácia de suas estratégias de resposta a crises.

Após o workshop, apresentamos nossas observações à organização pessoalmente e enviamos um relatório pós-ação por escrito com um resumo passo a passo da entrada de dados no cenário e das respostas.

Comparação do tipo de serviço

Tipo de serviço	Técnico	Executivo
Objetivo	Avaliar e analisar a capacidade de resposta técnica de uma organização para detectar, responder e conter uma ameaça avançada.	Avaliar e analisar as capacidades de gerenciamento de crise de uma organização no caso de uma ameaça avançada segundo a perspectiva da equipe de executivos.
Cronologia do engajamento	• Planejamento: 1 semana fora do local • Cenário simulado: 1 a 2 dias no local • Relatório final: 1 semana	• Planejamento: 1 semana fora do local • Cenário simulado: 1 a 2 dias no local • Relatório final: 1 semana
Participantes alvo	• Equipe de Resposta a Incidentes de Segurança Cibernética (*Cyber Security Incident Response Team*, CSIRT) • Gerente de segurança • Equipe técnica (por exemplo, aqueles que trabalham com rede, servidor, e-mail)	• Diretor de Segurança da Informação (*Chief Information Security Officer*, CISO) • Executivos gerais em nível de diretoria • Relações públicas e comunicações corporativas • Assessor geral
Áreas de foco	• Quando isolar hosts em uma rede • Quando refazer um sistema • Como analistas devem acompanhar o Plano de Resposta a Incidentes definido, o plano de comunicação e a matriz de escalonamento • Quando e como engajar fornecedores terceirizados	• Quando pagar extorsão ou ameaças de ransomware • Tomada de decisão sobre o impacto de táticas de contenção • Requisitos de divulgação de violações para reguladores e principais partes interessadas • Melhores práticas de notificação do cliente • Melhores práticas de comunicação pela mídia
Método de apresentação	Cenário simulado no local	Cenário simulado no local

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

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035 EUA
1.408.321.6300/877.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 de 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 reagir a ataques cibernéticos.

FIREEYE™