FICHA TÉCNICA

MANDIANT®
A FireEye® Company

# Desenvolvimento de centros de defesa cibernética

## Construa seu próprio programa de operações de segurança resiliente

### VANTAGENS

- **Melhore sua postura de defesa:** identifique e feche lacunas em seus recursos de monitoramento e respostas de segurança para proteger-se contra ameaças avançadas.
- **Crie um consenso sobre os aprimoramentos de segurança:** melhore a comunicação e a colaboração interna por meio do compartilhamento de conhecimentos e priorizações de aperfeiçoamentos.
- **Reduza o impacto dos incidentes de segurança:** melhore seus recursos de detecção e resposta para minimizar os riscos cibernéticos.
- **Priorize orçamentos e recursos:** aloque gastos e recursos de segurança para fortalecer a sua postura defensiva e melhorar a resposta de modo geral.

### O diferencial da 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 estiveram nas linhas de frente das violações mais complexas do mundo. Temos um profundo conhecimento de agentes de ameaça existentes e emergentes, bem como de suas táticas, técnicas e procedimentos, sempre em constante mudança.

### Visão geral

O serviço de desenvolvimento de centros de defesa cibernética ajuda as organizações na construção de um programa eficaz de operações de segurança que minimize o risco operacional e reduza o impacto das violações de segurança. Oferecemos um modelo de segurança desenvolvido especificamente de acordo com seus objetivos estratégicos e fazemos recomendações respaldadas por nossa experiência prática. Nossos consultores trabalham em estreita colaboração com sua organização para alinhar seu programa de segurança e viabilizar uma estratégia Adaptive Defense.

### Nossa abordagem

Os especialistas da Mandiant têm profundo conhecimento das táticas, técnicas e procedimentos usados pelos agentes de ameaças avançadas. Colaboraremos com sua organização para criar e implementar recursos e processos fundamentais em seu programa.

Para detectar e responder efetivamente aos ataques, um programa de resposta a incidentes precisa de processos e procedimentos eficazes, com as equipes, tecnologias e métricas apropriadas que avaliem a eficácia do programa. Com base na nossa experiência na resposta a incidentes de segurança críticos, os especialistas da Mandiant desenvolveram uma estrutura de trabalho com seis capacidades fundamentais que são a base de um programa de segurança resiliente. A estrutura de trabalho aborda:

- **Governança:** a sua estrutura organizacional está de acordo com a missão e as metas corporativas gerais?
- **Comunicações:** você tem processos implementados para promover um compartilhamento de informações eficaz entre entidades internas e externas?
- **Visibilidade:** existem tecnologias e processos implementados para gerar conscientização quanto às atividades que estão ocorrendo nos seus sistemas e redes?
- **Inteligência:** a sua inteligência sobre ameaças informa e aprimora o planejamento da segurança, o gerenciamento de vulnerabilidades e as atividades de resposta a incidentes?

FireEye®

- **Parâmetros de avaliação:** os seus parâmetros de avaliação da resposta a incidentes estão de acordo com as metas e os objetivos corporativos gerais, ao mesmo tempo em que promovem o aperfeiçoamento contínuo dentro da organização de segurança?
- **Resposta:** há tecnologias e processos estabelecidos que a equipe de segurança possa utilizar para identificar, categorizar, investigar e corrigir eventos de segurança adversos?

Durante nosso envolvimento, colaboraremos com sua organização para criar e implementar um programa com recursos e tecnologias fundamentais. Também podemos auxiliar no monitoramento de segurança de curto prazo até que sua equipe esteja estabelecida e preparada para assumir o controle.

**Tabela 1.** Fases do desenvolvimento de centros de defesa cibernética.

| Estágio | Objetivo | Tarefas |
|---|---|---|
| **Fundação** | Estabelecer uma base a partir da qual responder efetivamente aos incidentes e aplicar recursos de maneira eficiente. | • Definir uma matriz de escalação e um fluxo de trabalho de resposta a incidentes<br>• Criar planos de gerenciamento de programa e estratégico<br>• Desenvolver parâmetros de avaliação do desempenho e planos de geração de relatórios |
| **Integração** | Incorporar novos processos, procedimentos e tecnologia no seu ambiente operacional. | • Desenvolver e realizar treinamento<br>• Estabelecer contratos de nível de serviço operacionais<br>• Distribuir e configurar a tecnologia |
| **Operações** | Executar com base nos processos operacionais e analíticos e proporcionar capacidades de monitoramento. | • Proporcionar uma capacidade de monitoramento inicial<br>• Amadurecer continuamente os processos operacionais e analíticos<br>• Transferir responsabilidades para a equipe de segurança ou providenciar um aumento de pessoal |

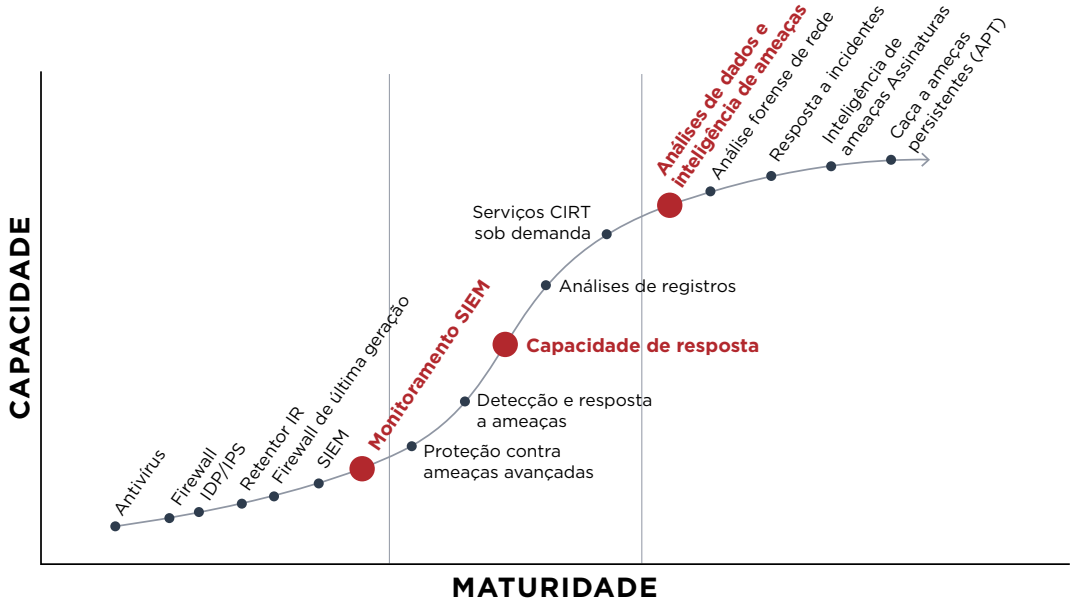


**Figura 1.** Modelo de desenvolvimento de programas de defesa cibernética.

Com base em nossa estrutura de trabalho de seis capacidades fundamentais, o serviço de desenvolvimento de centros de defesa cibernética possibilita que a organização migre de uma metodologia de resposta a incidentes reativos para um programa preditivo, orientado por uma missão e plenamente alinhado com os negócios.

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 sobre ameaças em nível de país 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. A FireEye tem mais de 6.600 clientes em 67 países, incluindo mais de 45 por cento das empresas da Forbes Global 2000.

FireEye®