MANDIANT®

FICHA TÉCNICA

Avaliação de Comprometimento

Identifique atividades de ataque atuais ou do passado em seu ambiente

POR QUE ESCOLHER A MANDIANT SOLUTIONS?

A Mandiant Solutions tem estado na linha de frente da inteligência em segurança cibernética e de 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 sobre os agentes de ameaça existentes e emergentes, bem como sobre suas táticas, técnicas e procedimentos extremamente dinâmicos.

VANTAGENS

- Análise abrangente do seu ambiente específico focada em encontrar evidências de comprometimento atual ou passado
- Oferece uma visão dos riscos e exposições sistêmicos
- Identifica questões de integridade da segurança
- Oferece recomendações para ampliar a habilidade de sua empresa em responder com eficácia a futuros incidentes
- Flexibilidade em implementar tecnologias dentro das premissas ou hospedadas na nuvem

Em nosso atual estado de segurança cibernética, as violações de segurança são inevitáveis.

– Kevin Mandia
CEO da FireEye

A Avaliação de Comprometimento da Mandiant combina nossa ampla experiência em resposta a intrusões realizadas por agentes de ameaças avançadas, inteligência contra ameaças líder do setor e tecnologia FireEye para fornecer uma avaliação que:

- Identifique intrusões atuais e passadas dentro de sua empresa
- Avalie os riscos identificando as fraquezas na arquitetura da segurança, vulnerabilidades, uso inadequado ou violações da política e erro de configuração da segurança do sistema
- Aumente a capacidade de sua empresa em responder com eficácia a futuros incidentes

A necessidade de avaliações de comprometimento
As violações de dados de grande importância na imprensa representam apenas uma fração da atividade de intrusão realizada globalmente. Saber se sua empresa foi violada e identificar formas de reduzir os riscos é essencial para evitar que sua empresa se torne a próxima manchete por ter sofrido uma grande violação de dados.

Nossa abordagem
Combinamos nossa vasta experiência em resposta a intrusões e inteligência de ameaças líder do setor com uma pilha modular de tecnologias da FireEye para fornecer uma avaliação que atenda aos seus objetivos de negócio com velocidade, escala e eficiência. Além de identificar evidências de atividades de ataques atuais e anteriores, a avaliação oferece:

Contexto derivado da inteligência de ameaças
Fornece informações sobre a atribuição e motivação do atacante para que as organizações saibam se estão sendo alvos.

Identificação dos riscos
Identifica as fraquezas das configurações e da arquitetura de segurança, incluindo correções ou softwares de segurança não encontrados.

Facilitação de investigações futuras
Recomenda opções estratégicas que podem preparar melhor a equipe de segurança de sua empresa para responder às intrusões.

Os consultores da Mandiant utilizam as tecnologias FireEye para procurar endpoints, monitorar tráfego de rede, inspecionar e-mails e analisar logs de outros dispositivos de segurança em busca de evidências de atividade do atacante. Os consultores também usam técnicas de análise de dados sem assinatura para encontrar atividades invisíveis de atacantes. Os clientes escolhem a combinação certa de tecnologias que fazem mais sentido para seus ambientes.

- Inspeção de endpoints: os agentes FireEye Endpoint Security são utilizados para fornecer detecção em tempo real da atividade do atacante, incluindo malware e outras táticas, técnicas e procedimentos, e para investigar endpoints Windows, MacOS e Linux. Os especialistas da Mandiant oferecem a flexibilidade de implementações locais e em nuvem.
- Inspeção da rede: os sensores FireEye Network Security são implementados em locais de monitoramento estratégicos em sua empresa a fim de detectar atividades comprometedoras, como comunicação de comando e controle oriundo de malware, acesso remoto não autorizado e roubo de dados.
- Inspeção de e-mail: o monitoramento pelo FireEye Email Security é realizado on premises ou na nuvem e pode ser configurado para inspecionar de maneira passiva os e-mails recebidos e enviados. A inspeção dinâmica dos anexos permite aos especialistas da Mandiant identificar campanhas de intrusão antes de outros produtos baseados em assinatura.
- Inspeção de logs: os consultores da Mandiant utilizam diversas tecnologias para revisar logs de aplicativos e infraestrutura a fim de identificar atividades maliciosas.

INSPEÇÃO DE ENDPOINTS

- Alerta em tempo real de atividade suspeita ou maliciosa em curso
- Detecção de malware usando o mecanismo de antivírus integrado do agente FireEye
- Suporte a sistema operacional multiplataforma
  - Windows
  - MacOS
  - Linux
- Identificação de anomalias que indicariam a presença de um malware avançado

INSPEÇÃO DA REDE

- Captura de pacote completo combinada com assinaturas de detecção personalizadas
- Detecção automática e decodificação do tráfego de comando e controle do atacante

INSPEÇÃO DE E-MAIL

- Detecta ataques de phishing direcionados usados por atacantes para recuperar o acesso ao ambiente após um evento de remediação
- Utiliza o mecanismo sem assinatura Multi-Vector Virtual Execution™ (MVX) para analisar anexos de e-mail e URLs diante de uma ampla matriz mista de sistemas operacionais, aplicativos e navegadores web
- Suporte à análise de imagens dos sistemas operacionais Microsoft Windows e MacOS
- Analisa ameaças ocultas em arquivos, incluindo anexos criptografados e protegidos por senha

Para saber mais sobre as soluções da Mandiant, visite: **www.FireEye.com/mandiant**

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

Sobre as soluções Mandiant
As soluções Mandiant reúnem a inteligência de ameaças líder no mundo e conhecimento de linha de frente especializado com validação de segurança contínua para capacitar as empresas com ferramentas que aumentam a eficácia da segurança e reduzem riscos de negócios.

MANDIANT®