MANDIANT®

E-BOOK

CONSIDERAÇÕES PARA EVOLUIR PARA A SEGURANÇA BASEADA EM INTELIGÊNCIA

Introdução

O cenário atual dos ataques é aparentemente ilimitado.

Os cibercriminosos estão ativando campanhas em todos os países do mundo, usando uma infinidade de técnicas de ataque. Para reduzir com sucesso o risco cibernético, as equipes de segurança precisam saber mais sobre os atacantes específicos que visam sua organização, incluindo quem eles são, as regiões e setores que visam, quando foram avistados, sua motivação e as táticas, técnicas e procedimentos que adotam. Esta é a promessa da inteligência contra ameaças cibernéticas (CTI).

Quando as equipes conhecem os atacantes que visam sua organização e como operam, os programas para mitigar os riscos podem ser desenvolvidos de forma proativa, gerando investimentos em ferramentas para proteger com eficácia seus negócios.

Este e-book discute o que as equipes devem considerar à medida que desenvolvem seu programa de segurança para uma capacidade baseada em inteligência, ajuda a avaliar o valor de uma postura mais proativa e fornece um framework para implementação que incorpora:

- As fases de transformação para uma abordagem de segurança baseada em inteligência
- Como avaliar e identificar os principais componentes necessários para a transformação
- Os componentes básicos da capacidade CTI
- Os componentes avançados da capacidade CTI

> Para reduzir com sucesso o risco cibernético, as equipes de segurança precisam saber mais sobre os atacantes específicos que visam sua organização

Os Desafios da Segurança Baseada em Conformidade

Algumas organizações contam com segurança baseada em conformidade para gerenciar seus riscos cibernéticos. Essa abordagem, com seu método estereotipado ou de uso geral, não leva em consideração as muitas complexidades e os pontos de diferenciação entre as organizações e os setores em que operam. Ao usar a segurança baseada em conformidade, as organizações provavelmente acabarão com:

- **Uma estratégia de coleta de dados sem foco:** A organização não é capaz de coletar informações relevantes porque não conhece seus atacantes.
- **Nenhuma missão definida ou declaração de missão:** Sem um propósito, a equipe não pode ser eficaz.
- **Sem compreensão das necessidades comerciais:** Não são capazes de identificar ferramentas e estratégias úteis para a proteção adequada.
- **Sem requisitos analíticos:** A organização não está ciente do que ou quem deve rastrear.

Como resultado, as equipes de segurança acabarão com uma postura de segurança reativa, sem saber quais ameaças priorizar, sem foco nos negócios e dificultando a quantificação do programa de segurança e seu valor.

O Valor de uma Estratégia de Segurança Baseada em Inteligência

A cibersegurança baseada em inteligência transforma uma postura de segurança reativa em proativa, permitindo que as equipes de segurança aumentem a conscientização sobre as ameaças e reduzam os impactos das violações. As decisões são baseadas em análises profundas, comprovações e insights técnicos. Eles incluem previsões de especialistas e a gestão eficaz das expectativas das partes interessadas.

A segurança baseada em inteligência agrega valor ao:

Refinar a estratégia de cibersegurança

- Identificar as ameaças mais relevantes e impactantes que visam uma organização, não apenas no dia a dia, mas também durante os períodos de mudança, como fusões e aquisições ou expansão dos negócios
- Influenciando o investimento alinhando o risco do negócio com o programa de segurança de uma organização
- Alinhar recursos contra as ameaças mais prováveis e as capacidades do ator

Aumentar a eficiência operacional

- Fornecer avisos antecipados e permitir respostas automatizadas às ameaças mais importantes
- Apoiar o ciclo de vida de gerenciamento de patches e capacitar equipes para corrigir vulnerabilidades que representam o maior risco para uma organização
- Permitir que as equipes procurem proativamente por atacantes que visem sua organização e identifiquem suas intenções, técnicas e ferramentas para ajudar a melhorar as defesas de segurança

Agilizar a capacidade de resposta

- Fornecer os detalhes e a inteligência por trás de um incidente de segurança
- Ajudar as equipes a priorizar suas respostas aos alertas

Esses atributos são comuns em ambientes verdadeiramente baseados em inteligência. Em organizações em que um programa CTI amadureceu, uma abordagem baseada em inteligência também pode ajudar a estabelecer um programa sustentável, atendendo às demandas de negócios e quantificando o retorno sobre os investimentos em segurança.

As Fases de Transformação de Segurança Baseada em Inteligência

A transformação em qualquer negócio geralmente exige uma abordagem em fases, para garantir que as mudanças atendam às necessidades da organização e sejam implementadas metodicamente. Os especialistas da Mandiant recomendam quatro fases para transformar um negócio em uma operação de segurança baseada em inteligência, incluindo uma avaliação das capacidades atuais, identificando requisitos de negócios, implementando sistemas e operacionalizando sistemas.

Fase 1. Avaliação
Compreender as ameaças atuais que sua organização enfrenta: quem são os principais interessados e como a inteligência de ameaças pode apoiá-los ao longo do tempo. Examinar os gaps da CTI e suas soluções e identificar como a CTI poderia beneficiar a equipe de cibersegurança de forma mais ampla.

Fase 2. Projeto
Durante a fase de projeto, criar recomendações para um programa de CTI alinhado aos processos organizacionais e ao ciclo de vida do processo de CTI. Documentar os pontos finais de integração para toda a equipe de defesa cibernética e criar fluxos de trabalho de comunicação específicos da organização.

Fase 3. Aprimoramento
Desenvolver habilidades e experiência em sua equipe de CTI, que podem ser especialmente úteis quando não existir um histórico de inteligência cibernética tradicional. Esta fase não apenas fortalece os recursos da equipe, mas também promove o consumo, a aplicação e os benefícios da inteligência contra ameaças para as partes interessadas em toda a organização.

Fase 4. Operacionalização
Alinhar a estratégia de CTI com processos e procedimentos. Implantar o programa em estágios tornará a implementação gerenciável e as oportunidades de melhorias podem ser registradas após a revisão de cada estágio.

Um Framework para a Segurança Baseada em Inteligência

A introdução de um programa CTI pode ser uma tarefa complexa. A adoção de um framework garante a implementação de bases sólidas, sobre as quais uma organização pode introduzir a tecnologia e os processos para dar suporte às suas necessidades à medida que amadurecem. Com muitos anos de experiência trabalhando na linha de frente da resposta a incidentes, os especialistas da Mandiant desenvolveram um framework confiável e comprovado para guiar uma organização em sua jornada.

Blocos de Construção de um Framework para Segurança Baseada em Inteligência

Estabelecendo Princípios

Perfil Organizacional de Ameaças

- Ambiente de Negócios e Conhecimento Operacional
- Ameaças, Vulnerabilidades e Exposição

Análise das Partes Interessadas

- Funções do Consumidor
- Necessidades de CTI (formato desejado/conteúdo de frequência)
- Casos de Uso de Consumo

Requisitos de Inteligência

- Critérios, Categorização e Priorização
- Fonte e Métodos
- Objetivo e Ações Esperadas

Práticas de Implementação

Gerenciamento do Ciclo de Vida da CTI

- Coleta e Processamento
- Habilidade/ Experiência do Analista
- Framework Analítico
- Padrões de Produção

Integração de Tecnologia

- DICA
- CMS
- Integração com SIEM
- Big Data
- Suporte a Conjuntos de Ferramentas Analíticas

Realizando Capacidades

Operações de CTI

- Suporte Analítico/ Tático para Operações de Segurança
- Compartilhamento de Informações COI
- Análise de Tendências e Previsões de Ameaças
- Detecção Proativa de Ameaças
- Comunicações Repetíveis e Eficazes Contra Ameaças
- Suporte à Decisão Estratégica

Maturidade

Blocos de Construção de um Framework para Segurança Baseada em Inteligência (cont.)

Estabelecendo Princípios

Os blocos de construção no primeiro estágio devem criar uma organização de inteligência cibernética duradoura que possa determinar:

- As ameaças que uma organização está enfrentando, incluindo ameaças a serem priorizadas
- Partes interessadas que precisarão e usarão inteligência contra ameaças na empresa
- Requisitos de inteligência que atenderão melhor às partes interessadas

Os elementos fundamentais são essenciais para um programa de CTI bem-sucedido. Negligenciar os blocos básicos pode complicar o alinhamento dos recursos de inteligência com as necessidades do negócio quando as organizações devem se concentrar nos blocos avançados à medida que amadurecem.

Práticas de Implementação

Este estágio se concentra na criação dos processos necessários para apoiar o uso da CTI em toda a organização e inclui:

- Treinamento dos analistas que estarão executando o programa de capacitação em CTI
- Determinação da estratégia de aquisição de dados
- Implementação das ferramentas e tecnologias corretas.

Realizando Capacidades

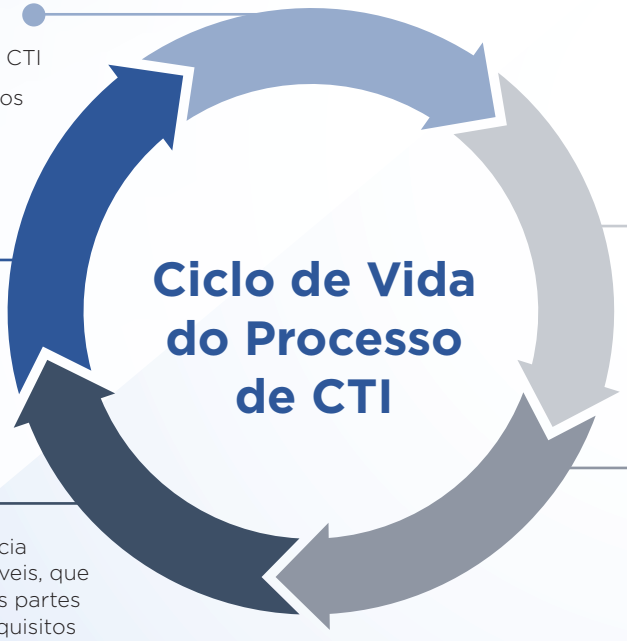
O estágio final concretiza o recurso da CTI, implementando um fluxo de trabalho diário dos processos identificados no estágio dois. Isso permite que uma equipe de inteligência contra ameaças mude de uma postura reativa para uma proativa na detecção de ameaças.

> Negligenciar os blocos básicos pode complicar o alinhamento dos recursos de inteligência às necessidades de negócios

O Ciclo de Vida da Inteligência

Quando um recurso baseado em inteligência tiver sido operacionalizado, as equipes podem adotar um ciclo de vida do processo de CTI para guiá-los através do fluxo contínuo de planejamento, coleta de dados, análise, produção e revisão da inteligência de ameaças e os meios pelos quais ela é reunida e aplicada em todo o negócio.

Usar um processo de CTI organizado garante práticas estruturadas e consistentes em toda a organização. Para colher todos os benefícios comerciais e do gerenciamento de risco dessa abordagem, o ciclo de vida do processo de CTI e os principais componentes do programa devem ser tratados no nível executivo.



Planejamento e Requisitos

- Definir as principais diretivas da CTI
- Identificar e priorizar os requisitos de inteligência
- Gerenciar continuamente a execução

Coletas e Processamento

- Decifrar a estratégia de aquisição de dados para cumprir os requisitos
- Normalizar, eliminar a duplicação e enriquecer os dados brutos em formulários consumíveis

Análise

- Avaliar, analisar e interpretar as informações processadas em relação aos requisitos
- Avaliar os gaps da coleta

Produção

- Produzir produtos de inteligência oportunos, relevantes e acionáveis, que se alinhem às necessidades das partes interessadas e atendam aos requisitos
- Deficiências de documentos

Disseminação e Feedback

- Entregar produtos de inteligência acabados para as partes interessadas, com frequências e métodos definidos
- Obter e analisar o feedback das partes interessadas

Suporte por Meio do Desenvolvimento de Capacidade de Inteligência (ICD)

A Mandiant Threat Intelligence passou a última década ajudando organizações de vários setores a adotar e integrar a CTI de maneira eficaz em suas operações de segurança.

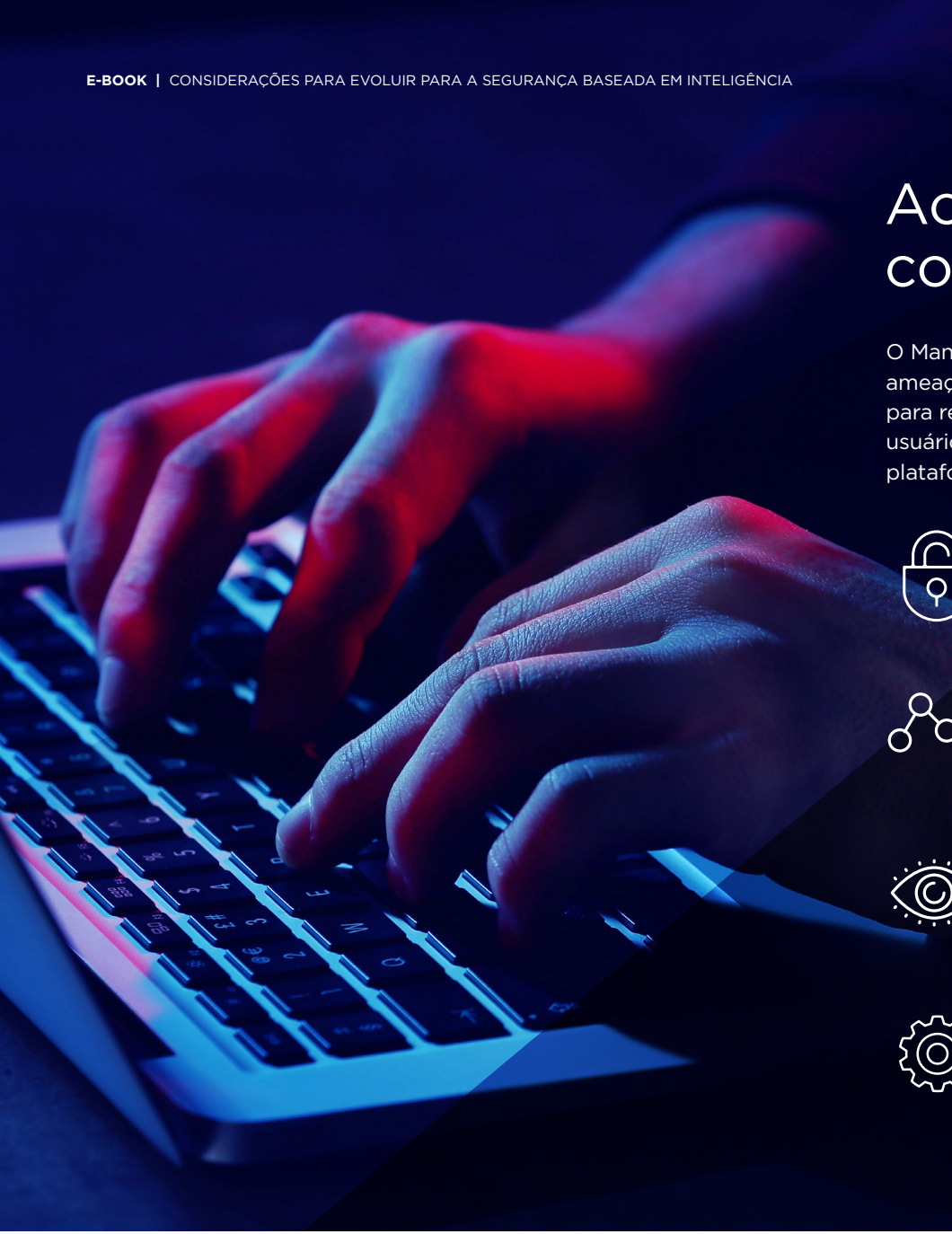
Essas experiências ajudaram a FireEye a criar e refinar um conjunto de serviços projetados para construir sistematicamente as melhores práticas para o consumo, a análise e a aplicação prática da CTI.

Os serviços ICD da Mandiant Threat Intelligence variam de compromissos com um requisito específico a implementações de programas de inteligência em larga escala que ajudam as equipes de segurança a:

- Encontrar a linha de base dos recursos de inteligência existentes e planejar melhorias
- Determinar o risco cibernético que sua organização enfrenta, a inteligência necessária para combatê-lo e quem o utilizará
- Mapear seus casos de uso estratégico, operacionais e táticos para a aplicação da inteligência
- Fornecer workshops para melhorar os recursos de CTI e usar a CTI de maneira mais eficaz nas suas atividades diárias

Sejam combinados ou entregues separadamente, os serviços de ICD oferecem suporte ao desenvolvimento e manutenção de um programa abrangente de inteligência de ameaças.

> Um conjunto de serviços projetados para construir sistematicamente as melhores práticas para o consumo, a análise e a aplicação prática da CTI



Acesse uma CTI incomparável com o Mandiant Advantage

O Mandiant Advantage fornece às organizações de todos os tamanhos insights de ameaças atualizados, relevantes e fáceis de consumir, acelerando a tomada de decisões para reduzir o risco e melhorar a postura de segurança de uma organização. Os usuários acessam uma inteligência contra ameaças que vai além dos recursos das plataformas SaaS de código aberto atuais com insights derivados de:

Inteligência de Violação
Nos últimos 15 anos, a Mandiant construiu uma reputação como principal responsável pela resposta a incidentes do setor, participando de mais de 800 reuniões de resposta a incidentes anualmente.

Inteligência Operacional
A equipe da Mandiant Managed Defense realiza serviços de detecção e resposta para mais de 300 clientes de quatro centros internacionais de operações de ameaças cibernéticas, ingerindo +99 milhões de eventos e validando +21 milhões de alertas.

Inteligência Adversária
A Inteligência de Ameaças da Mandiant utiliza mais de 200 analistas e pesquisadores de inteligência localizados em 23 países, que coletam até um milhão de amostras de malware por dia em mais de 70 fontes diferentes.

Inteligência de Máquina
Os especialistas da Mandiant aproveitam as vantagens das tecnologias FireEye, que têm aproximadamente quatro milhões de imagens guest virtuais implantadas globalmente em 102 países, gerando dezenas de milhões de detonações de sandbox por hora, confirmando de 50 mil a 70 mil eventos nocivos por hora.

Conclusão

A cibersegurança baseada em inteligência é transformadora para uma organização. Uma equipe de segurança proativa, operando com inteligência atualizada, está mais bem equipada para proteger sua organização contra ameaças porque está perfeitamente ciente das ameaças específicas que enfrentam.

As organizações precisam de um framework comprovado para que possam seguir e desenvolver um programa de CTI sustentável e bem-sucedido. Em última análise, suas equipes usarão vários feeds de dados, briefings, investigações e recomendações de priorização para tomar decisões estratégicas de segurança e negócios diariamente. Mas primeiro eles precisam estabelecer uma base sólida que garanta que qualquer investimento em novos recursos de inteligência esteja alinhado com suas necessidades organizacionais. Com o tempo, um compromisso com a evolução contínua da segurança, combinado com um esforço consciente para incorporar a CTI à estratégia de negócios, levará a uma prática de cibersegurança madura e baseada em inteligência.

Para saber mais sobre como melhorar sua postura de segurança, acesse: **www.fireeye.com/intel.**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6500/877.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®