MANDIANT®

FICHA TÉCNICA

Plataforma de Validação de Segurança

Conheça a sua real postura de segurança

DESTAQUES

- **Priorize ameaças que são importantes** com base em inteligência de ameaças cibernéticas relevantes e oportunas
- **Avalie a eficácia das ferramentas de segurança atuais** contra ataques de adversários reais
- **Descubra falhas e sobreposições não detectadas** em sua infraestrutura de segurança
- **Meça o tempo da equipe** para detectar e responder
- **Identifique as melhores oportunidades** para otimização
- **Quantifique a melhoria** nas defesas no decorrer do tempo
- **Racionalize com evidências o valor** de investimentos para executivos
- **Simplifique comunicações** sobre o estado da postura de segurança em toda a empresa

No atual ambiente de ameaças cada vez mais dinâmico, CISOs e suas equipes têm o desafio de manter os ativos corporativos seguros. Espera-se que eles saibam, e provem, o valor de seus investimentos em cibersegurança e a eficácia das defesas cibernéticas contra ataques atuais e futuros.

Testes de penetração, criação de red teams e simulações de ataques e violações não são suficientes—eles não oferecem a prova quantificável que CISOs e líderes de negócios exigem para entender a exposição ao risco e sua prontidão cibernética. Sem evidências baseadas em dados de desempenho, os times de segurança ficam impedidos de otimizar defesas com sucesso e afirmar sua postura de segurança com confiança.

O Mandiant Security Validation, um elemento essencial da tecnologia de validação de controles liderados por inteligência da Mandiant, fornece as evidências necessárias. O Security Validation é uma plataforma de gestão e avaliação de risco de cibersegurança que permite que as equipes garantam que seus ativos essenciais estejam sempre protegidos.

Melhor Eficácia de Controles

O Mandiant Security Validation conta com os dados globais de resposta a incidentes e inteligência de ameaças da Mandiant, dados de ameaças e de visibilidade exclusivos e incomparáveis que representam o que os atacantes estão fazendo neste momento. Essa combinação de tecnologia de validação de segurança e inteligência de ameaças da Mandiant arma as equipes de segurança com uma estratégia de validação baseada no conhecimento de quem e o que tem probabilidade de atacar a organização.

A tecnologia de validação de segurança liderada por inteligência da Mandiant começa priorizando ameaças críticas e relevantes e depois avalia e captura, com segurança, evidências discretas e quantificadas da eficácia de sua arquitetura de segurança geral contra ataques adversários reais. Os resultados destacam ataques individuais específicos e até mesmo áreas inteiras na extensa cadeia de destruição que derrotam ou burlam suas tecnologias de segurança. Você pode usar esses insights para determinar onde e como otimizar seus controles, trabalhar com dados específicos de desempenho e fornecedores conforme necessário e, por fim, transformar todo o seu programa.

Com o Mandiant Security Validation, é possível quantificar rapidamente e provar a eficácia do seu programa de segurança contra os mais recentes adversários sofisticados no mundo todo. Essa tecnologia pode ser usada em arquiteturas on-premises, na nuvem e híbridas.

Quantificar suas melhorias de eficácia possibilita provar o valor dos seus investimentos em segurança em relação à tolerância de risco da empresa para a liderança da organização.

Com o Mandiant Security Validation, o processo é automatizado e contínuo, permitindo focar em defender seus negócios mais estrategicamente enquanto a plataforma monitora e mede atentamente a eficácia de segurança geral.

Ganhe Confiança na Sua Postura de Segurança
Os especialistas de validação de segurança da Mandiant trabalham com você para configurar rapidamente a plataforma, conectando atores, uma fonte de alertas e quaisquer controles específicos para profundidade adicional. Por meio da facilidade de integração, você pode visualizar o desempenho de suas tecnologias de defesa quando comportamentos de ataque forem executados com segurança.

Uma vez configurada, é possível selecionar testes discretos ou sequências de testes pré-configuradas da vasta biblioteca da Mandiant de ataques reais, desde técnicas, táticas e procedimentos de adversários até vários tipos de malware. À medida que esses testes são executados com segurança, você pode validar imediata e continuamente que controles específicos estão funcionando corretamente. Os painéis são preenchidos em tempo real para mostrar a você os índices de detecção, alerta, não detecção e prevenção enquanto os testes são executados.

A plataforma também valida se os eventos estão em conformidade com a data e a hora que foram gerados e se são corretamente interpretados; além disso, se as regras de correlação e os modelos de ameaças forem definidos, os eventos geram alertas apropriados.

Relatórios estão disponíveis para visualização e exportação, resumindo a eficácia geral da segurança no decorrer do tempo. Por meio de validação contínua e constante, você obtém a prova necessária para conquistar e manter a confiança em seu programa, não apenas para si mesmo, mas também para os seus executivos e o Conselho de Administração.

Detalhes da Plataforma
A plataforma expansível, personalizável e aberta da Mandiant oferece descoberta de controles automatizados e uma arquitetura que permite o uso de binários de ataques reais para testar seguramente os controles de segurança. Ela inclui seis componentes principais.

Diretor
O Diretor é o painel central de gestão de todos os seus ambientes. Ele está disponível tanto no modelo SaaS quanto no modelo on-premises (como appliance virtual ou via instalador).

Atores
Os Atores executam testes seguros em ambientes de produção para validar a eficácia da Rede, dos endpoints Windows, MacOS e Linux, dos controles de segurança na Nuvem e no Email e garante que a infraestrutura esteja configurada corretamente.

Integrações
Integrações avançadas, prontas para uso, com tecnologias defensivas e infraestrutura de segurança podem realizar a validação de controles mais profundos.

Biblioteca de Ataques
A biblioteca de conteúdo representa milhares de ataques em cada etapa do ciclo de vida do adversário, incluindo a extensa cadeia de destruição e baseados em comportamentos de ataques adversários atuais e emergentes e TTPs informadas pela inteligência de violações, adversários e ameaças globais da Mandiant.

Frameworks
Os ataques são alinhados com as estruturas MITRE™ ATT&CK e NIST para vincular facilmente a eficácia aos seus programas de avaliação de segurança. A validação de segurança da Mandiant é única porque seu conteúdo fornece insights sobre quais táticas de estrutura de ataque são relevantes para uma organização e pode ser usado para executar validações contra táticas MITRE ATT&CK para garantir testes abrangentes e relevantes e resultados precisos.

Painéis e Relatórios
Exibição gráfica em tempo real com resultados de testes executados em seu ambiente e relatórios de melhorias na eficácia no decorrer do tempo contendo dados quantitativos reais que podem ser usados para informar seus executivos (Fig. 1).

Figura 1. O painel ajuda a validar os controles de segurança em todo o ciclo de vida do ataque para identificar áreas de risco.

Metodologia de Validação Liderada por Inteligência

O Mandiant Security Validation executa a validação, a otimização e o monitoramento contínuos de controles de segurança com detecção automatizada de mudanças no ambiente. Esse processo de validação contínuo é conduzido por meio de uma tecnologia liderada por inteligência em cinco etapas (Fig 2.)

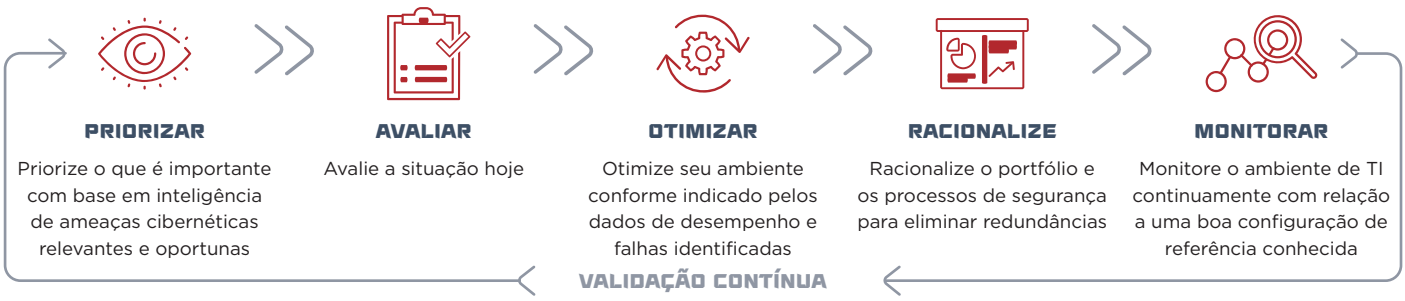

Figura 2. Metodologia de validação liderada por inteligência em cinco etapas da Mandiant.

Recursos Avançados

- **Módulo de Segurança dos Atores de Ameaças (*Threat Actor Assurance Module*, TAAM):** torna acionável a inteligência de ameaças para que seja possível testar o desempenho dos controles em relação a atores de ameaças reais, especialmente aqueles mais prováveis de atingir uma organização. O TAAM integra-se a feeds de inteligência de terceiros líderes do setor (Fig. 3).
- **Análise Automatizada de Mudanças no Ambiente (*Advanced Environmental Drift Analysis*, AEDA):** ativação de monitoramento contínuo da infraestrutura de TI para promover a validação contínua contra regressões defensivas para garantir a integridade da infraestrutura de segurança de uma organização.
- **Atividades Protegidas - Endpoint:** valida a eficácia de controles de endpoint executando com segurança malware, ransomware e outros ataques destrutivos para permitir a proteção proativa contra as ameaças mais recentes e emergentes.
- **Atividades Protegidas - Email:** testa os controles oferecidos nas plataformas de segurança de e-mail.

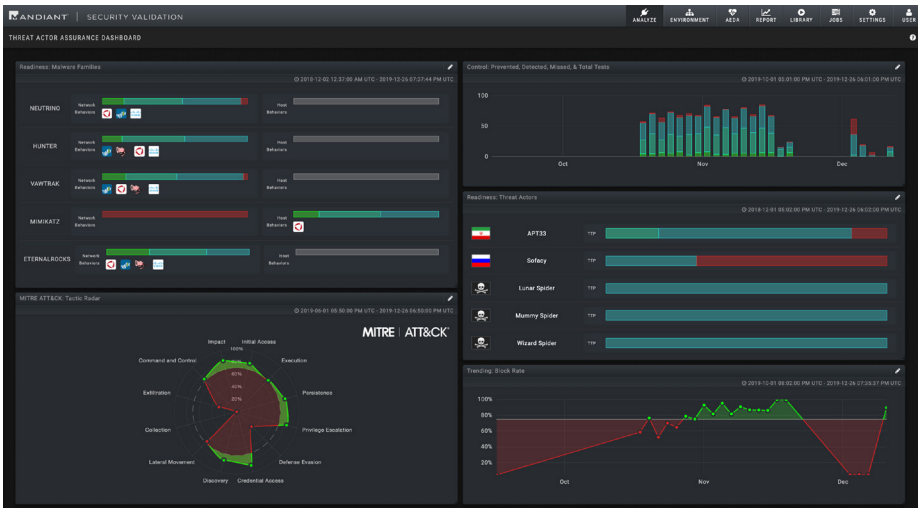

Figura 3. Módulo de Segurança dos Atores de Ameaças (TAAM).

O portfólio de validação de segurança da Mandiant inclui várias opções de implantação:

- **Modelo Gerenciado e de Propriedade do Cliente:** baseado na nuvem (SaaS) ou implantado como appliance virtual on-premises.
- **Modelos Cogerenciados e Totalmente Gerenciados:** com base nos resultados de negócios desejados pelo cliente, as equipes da Mandiant criam programas de validação para atender casos de uso específicos, fornecendo continuamente relatórios detalhados a partes interessadas do cliente.
- **Validação Sob Demanda:** permite que os clientes comprem um único caso de uso para uma avaliação específica de sua capacidade de bloquear/prevenir um autor de ameaça ou ataque predefinido e obter recomendações sobre futura investigação necessária para melhorar as defesas ou reduzir a exposição ao risco.

Validação de Segurança Informada por Inteligência de Ameaças da Mandiant

Nos últimos 15 anos, através de investigações, consultoria de incidentes e exercícios Red Team em todo o mundo, a Mandiant criou e aperfeiçoou um portfólio exclusivo de threat intelligence que é constantemente atualizado com dados de novas evidências, experiência humana e tradecraft analítico exclusivo. A Mandiant agora domina o campo de inteligência de ameaças cibernéticas por meio do seguinte conjunto equilibrado de fontes:

- **Inteligência de violações** coletada através das interações de resposta a incidentes da consultoria da Mandiant
- **Inteligência de adversários** obtida por pesquisadores da Mandiant
- **Inteligência de máquina** dos produtos de segurança da FireEye
- **Inteligência operacional** derivada dos serviços gerenciados de defesa da Mandiant

Para saber mais sobre a Mandiant Solutions, 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 a Mandiant Solutions
A Mandiant Solutions reúne a inteligência de ameaças líder mundial e expertise de linha de frente com validação de segurança contínua para equipar as organizações com as ferramentas necessárias para aumentar a eficácia da segurança e reduzir o risco de negócios.

MANDIANT®