

Validação de Segurança

Evidencie o Valor da Cibersegurança



CISOs Precisam Evidenciar a Eficácia da Segurança

O atual ambiente corporativo - atento aos riscos - está pressionando de forma sem precedentes os CISOs e suas equipes para proteger os ativos corporativos e a postura financeira e de valor da marca de suas organizações. Eles precisam provar para a liderança o valor dos investimentos em cibersegurança e sua eficácia para impedir adversários de comprometer sistemas essenciais.

Mas sem as ferramentas necessárias para validar a eficácia da segurança, quantificar o risco e apresentar competência operacional, eles dependem de scanners de vulnerabilidade, testes de penetração, red teams ou simulações de violações e ataques. Devido às limitações inerentes, essas abordagens não são suficientes para

avaliar a eficácia, nem fornecem insights relevantes e oportunos sobre ameaças específicas e de alta prioridade para a organização.

A solução é o Mandiant Security Validation, um portfólio liderado por inteligência, automatizado e contínuo, composto de módulos de desempenho exclusivos e a Mandiant Security Instrumentation Platform.¹

Quantifique e Evidencie a Eficácia do Seu Programa de Segurança

A validação de segurança feita corretamente baseia-se em uma metodologia de cinco etapas que fornece informações sobre o que é mais importante testar e como otimizar as defesas com base no conhecimento de quem e o que pode ter a organização ou o setor como alvo.

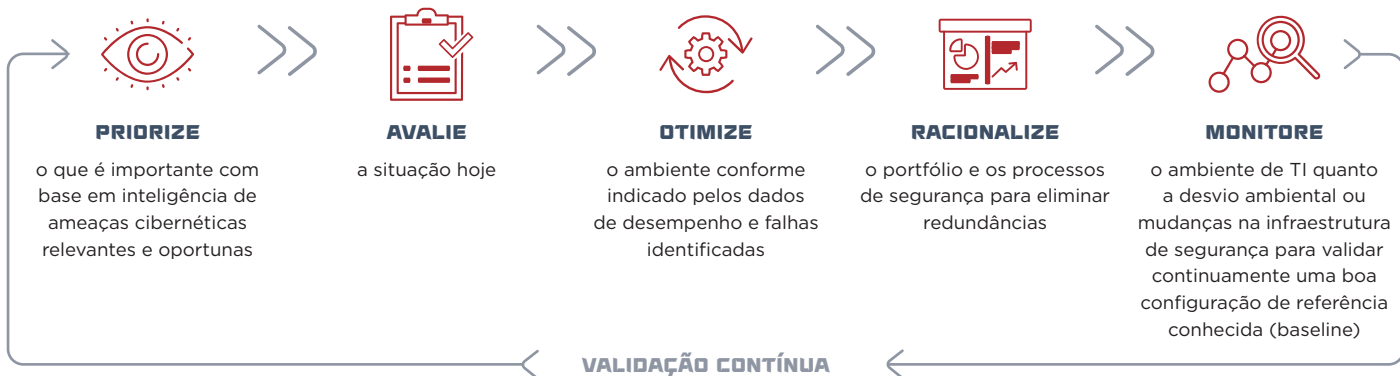


Figura 1. Metodologia de validação liderada por inteligência em cinco etapas da Mandiant.

¹ Antiga Plataforma de Instrumentação de Segurança da Verodin.

A metodologia exige a capacidade de aproveitar dados de ameaças em tempo real. O Mandiant Security Validation usa os dados de resposta a incidentes e inteligência de ameaças da Mandiant para proporcionar visibilidade incomparável do adversário que revela o que os atacantes estão fazendo neste momento. Com a validação de segurança liderada por inteligência, as equipes de segurança podem identificar ameaças de alta prioridade para a organização e criar uma estratégia de validação baseada no conhecimento de quem ou o que representa ameaça para a organização. Com a Mandiant, os líderes de segurança e suas equipes podem executar a validação contínua e completa dos controles de segurança em toda a tecnologia, processos e pessoas.

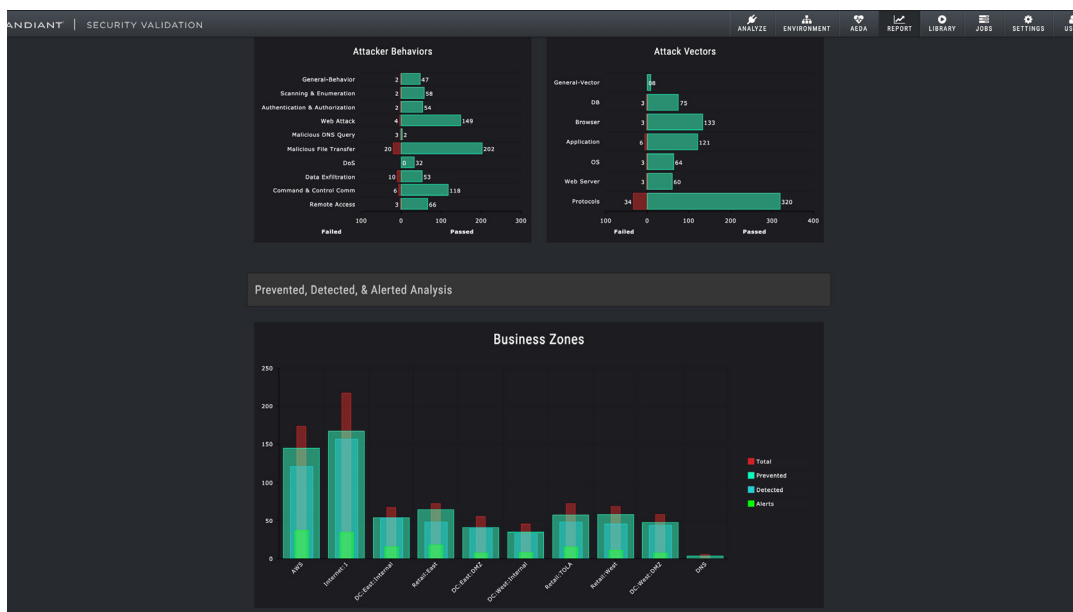
O Mandiant Security Validation usa a Security Instrumentation Platform, sua tecnologia de validação de controles, para ajudar as equipes de segurança a executar comportamentos de ataques reais contra controles de segurança para rapidamente quantificar e evidenciar a eficácia do programa de segurança e a capacidade de defesa contra os ataques de adversários mais sofisticados.

A Funcionalidade Básica do Mandiant Security Instrumentation Platform:

- Prioriza as ameaças e os controles adversários mais importantes
- Mede a eficácia dos controles de segurança em relação aos ataques adversários reais
- Executa com segurança ataques relevantes informados por dados inigualáveis de respostas a incidentes e inteligência de ameaças da Mandiant
- Descobre falhas não detectadas na infraestrutura de segurança da organização
- Identifica as melhores oportunidades para otimização
- Quantifica a melhoria nas defesas no decorrer do tempo
- Racionaliza com evidências quantificáveis o valor de investimentos para executivos

Figura 2.

A plataforma ajuda a visualizar e gerar provas de que seus controles estão protegendo ativos essenciais.



O Mandiant Security Implementation Platform apresenta funcionalidade avançada:

- **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.
- **Análise de Alteração Automatizada do Ambiente (Advanced Environmental Drift Analysis, AEDA):** ativação de monitoramento contínuo da infraestrutura de TI para promover a validação contínua com relação a regressões defensivas para assegurar a integridade da infraestrutura de segurança de uma organização.
- **Validação do Endpoint:** valida a eficácia de controles do endpoint executando com segurança malware, ransomware e outros ataques destrutivos para permitir a proteção proativa contra as ameaças mais recentes e emergentes.
- **Validação do Email:** testa os controles oferecidos nas plataformas de segurança de e-mail.

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

- **De Propriedade do Cliente:** baseado na nuvem (segurança como um serviço (Security as a Service, SaaS)) ou implantado como appliance virtual on-premises.
- **Modelos Cogereenciados 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 única de sua capacidade de bloquear ou prevenir um ator de ameaça ou ataque predefinido e obter recomendações sobre futura investigação necessária para melhorar as defesas ou reduzir a exposição ao risco.

Benefícios da Validação de Segurança Para os Negócios

Medir a Eficácia e o Retorno do Investimento (*Return on Investment, ROI*)

Ganhe dados quantificáveis que ajudam a determinar o investimento necessário para aumentar a eficácia da segurança contra tipos de ataques priorizados e quantificar o perfil de risco geral. Equipes de segurança também podem usar essas evidências para racionalizar o valor dos investimentos em segurança com a liderança executiva e o Conselho de Administração.

Fusões e Aquisições

Entenda claramente como as empresas que passam por uma fusão ou aquisição podem ter sobreposições ou falhas nos controles. Por meio da racionalização de gastos, você pode calcular o potencial de valor em dinheiro para consolidação e o nível de risco que eles podem assumir como resultado da fusão.

Contratação e Treinamento de Mão de Obra de Segurança

Veja além dos anos de experiência e avalie o potencial de aprendizagem de um profissional de segurança, o tipo de experiência que ele tem e até que ponto seus conjuntos de qualificações correspondem bem ao ambiente da organização dentro de situações do mundo real. Ao executarem com segurança ataques reais no ambiente de produção, os líderes de TI podem monitorar como candidatos potenciais respondem e reagem. Líderes de TI também podem conduzir avaliações regulares como exercícios de treinamento para ver se as equipes demonstram tempos de resposta aceitáveis e qualificações necessárias em situações de ataques do mundo real.

Proteção à Marca

Avalie de forma contínua e proativa a eficácia da segurança para reduzir o risco de uma violação ou ataque e preservar a reputação da marca e a fidelidade do cliente.

Proteção e Privacidade dos Dados

Proteja os dados do cliente e garanta a conformidade com normas regulatórias, corporativas e de terceiros.



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

©2020 FireEye, Inc. Todos os direitos reservados.
FireEye e Mandiant são marcas registradas da FireEye, Inc. Todos os outros nomes de marcas, produtos e serviços são ou podem ser marcas comerciais ou marcas de serviços de seus respectivos proprietários.
M-EXT-DS-US-EN-000317-01

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[®]