FICHA TÉCNICA

A PLATAFORMA COMPLETA DE VALIDAÇÃO DE SEGURANÇA

Validação de Controle de Segurança para Controles de Detecção

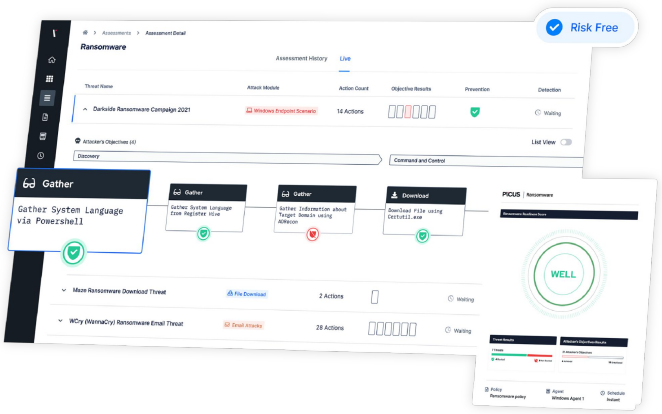
Uma defesa sólida e resiliente contra ameaças cibernéticas não só exige uma camada robusta de prevenção, como também recursos de detecção proativos. Com a **Validação de Segurança de Controle (SCV) da Picus** com **Análise de Detecção** integrada, você recebe o suporte necessário para validar o desempenho das ferramentas de SIEM e EDR da sua organização e garantir que elas sejam sempre otimizadas para identificar e responder aos ataques mais recentes.

ACELERE A DETECÇÃO E A RESPOSTA MAXIMIZANDO A EFICÁCIA DA SUA PILHA DE SEGURANÇA

Para minimizar o risco de ataques cibernéticos causarem danos e interrupções, é vital detectá-los e respondê-los o mais cedo possível.

Ao simular mais de 3.800 ameaças reais e fornecer insights práticos para otimizar seus controles para identificá-los, a Picus SCV ajuda você a ser proativo e garantir que suas defesas estejam prontas para bloquear eventos maliciosos de forma mais rápida e confiável.

Com sua abordagem automatizada e contínua à segurança validação de controle, o Picus SCV também alivia a tensão de acompanhar as ameaças 24 horas por dia, 7 dias por semana - permitindo que você se concentre em mitigar as lacunas de cobertura e visibilidade, em vez de descobrindo-os.



Valide, meça e melhore o desempenho de suas ferramentas de SIEM e EDR.

COMO A SEGURANÇA DA PICUS CONTROLA A VALIDAÇÃO COM A ANÁLISE DE DETECÇÃO AUMENTA SUAS OPERAÇÕES DE SEGURANÇA

Identifica
pontos cegos de detecção

A Picus identifica ataques que não são identificados por seus controles de prevenção e detecção, permitindo que você identifique ameaças que podem representar um risco sério se a ação de mitigação não for adotada.

Diminui
o tempo de permanência do criminoso

Assim, você pode responder a ameaças mais cedo na cadeia de disrupção, e a Picus valida que os conjuntos de regras que você usa para otimizar seus controles são eficazes e gerem alertas imediatos.

Possibilita
mitigação mais rápida de ameaças

Reduzir o tempo e o esforço necessários
para ajustar seus controles de segurança, a Picus fornece milhares de regras de detecção específicas do fornecedor e baseadas em SIGMA.

Operacionaliza
MITRE ATT&CK

A Picus mapeia os resultados da avaliação para a Estrutura Mitre ATT&CK, permitindo visualizar a cobertura de ameaças e priorizar a mitigação de lacunas.

Facilita
a caça a ameaças

Ao identificar técnicas de ataque capazes de contornar seus controles, a Picus ajuda sua caça a ameaças que podem ter usado métodos semelhantes e permanecem sem serem detectadas.

Reduz
falsos-positivos

Fornecendo regras de correlação que são testadas pela nossa equipe de Laboratórios antes do lançamento, a Picus garante que o conteúdo de detecção que você usa seja eficaz e confiável.

MELHORAR A DETECÇÃO DE AMEAÇAS EM TODAS AS REDES E ENDPOINTS

Para garantir que seus controles de detecção continuem eficazes, é essencial testá-los e ajustá-los regularmente. Com a Validação de Controle de Segurança da Picus, você recebe dados em tempo real e insights práticos necessários para obter a proteção ideal em todos os momentos.

TECNOLOGIAS COMPATÍVEIS:

Gestão de Incidentes e Eventos de Segurança (SIEM)

→ Validação de Logs

Sem os dados certos, é impossível identificar a atividade de ameaça em suas redes. Simular ameaças reais e analisar os registros de segurança capturados por seu SIEM, a Picus SCV permite que você:

- Determine se os registros de fontes relevantes estão sendo ingeridos (e em tempo hábil)
- Compreenda e priorize novas fontes de dados necessárias para resolver lacunas de registro
- Garanta que os registros contenham o nível necessário de granularidade de dados

→ Validação de Alertas

Para detectar ameaças cedo e reduzir o tempo de permanência do criminoso, também é essencial garantir que as regras de correlação de SIEM apropriadas estejam em vigor para alertar sobre os comportamentos mais recentes do adversário. Com a Picus SCV, você pode identificar rapidamente:

- Conjuntos de regras ausentes, redundantes e obsoletos
- Eventos registrados que não geram alertas
- Atrasos entre eventos de segurança e geração de alertas

OS PARCEIROS DE SIEM incluem

splunk> · Microsoft Sentinel · SIGMA · CyberRes ArcSight · Elastic Security · securonix · NETWITNESS An RSA Business · LogRhythm · CRYPTOSIM · IBM Security QRadar

Detecção e Resposta de Endpoints (EDR)
→Validação de regras de telemetria, alerta e detecção

Detectar e responder a ataques no início da cadeia de morte cibernética também depende da ampla telemetria dos endpoints. Para facilitar a detecção de ameaças que visam os dispositivos da sua organização, a Picus SCV se integra às principais soluções EDR para:

- Validar se os dados de endpoints mais relevantes estão sendo capturados e analisados
- Identificar conjuntos de regras e listas de observação ausentes, redundantes e obsoletas
- Medir o tempo entre os eventos de segurança e a geração de alertas
- Destacar comportamentos detectados não bloqueados por controles
- Localizar problemas de qualidade e desempenho que limitam a eficácia da regra

OS PARCEIROS DE EDR incluem

Microsoft Defender for Endpoint · SentinelOne · CROWDSTRIKE · vmware Carbon Black

INSIGHTS QUE VOCÊ PRECISA PARA MITIGAR RAPIDAMENTE LACUNAS

Identifique a cobertura de ameaças e as lacunas de visibilidade é uma coisa, mas fechá-las requer habilidades técnicas e experiência adicionais.

Para reduzir o tempo necessário para desenvolver, implementar e ajustar o conteúdo de detecção, a Picus SCV fornece milhares de assinaturas de prevenção e regras de detecção.*

IInclui regras específicas do fornecedor e SIGMA - todas testadas pela equipe da Picus Labs para garantir que sejam eficazes e possam ser implementadas sem um alto risco de falsos positivos.

* Os insights de mitigação para controles de detecção estão atualmente disponíveis para ataques incluídos apenas como parte do Módulo de Ataque de Endpoints da Plataforma Picus.

O QUE NOSSOS CLIENTES DIZEM

> Insights focados em ameaças e orientados para resultados fornecidos pela Plataforma Picus capacitam nossas equipes a aproveitar ao máximo nossos investimentos em segurança."
>
> Gerente Geral Adjunto
> TI e Segurança
> Indústria da Aviação

> A Plataforma Picus foi uma divisora de águas."
>
> Gerente de Produtos de Segurança de TI
> ING Bank

Gartner peerinsights™
4.9 / 5*
*average score at time of press in October 2022

Teste suas defesas contra as mais recentes ameaças

INICIAR AVALIAÇÃO GRÁTIS

CYBER SECURITY EXCELLENCE AWARDS WINNER 2022 · CYBERTECH100 2022 The World's Most Innovative CyberTech Companies for Financial Services · GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2022 · AICPA SOC 2

www.picussecurity.com

picussecurity