block

CrowdStrike *vs* SentinelOne

Instalação e manutenção

SentinelOne

Ao ser instalado, o agente do SentinelOne exige uma reinicialização dos sistemas, o que prejudica em especial sistemas com altos requisitos de recursos e cargas de trabalho pesadas. Ele também é difícil de instalar, precisa de ajuste e configuração manuais e exige exclusões para lidar com problemas de interoperabilidade de software e controle de qualidade.

CrowdStrike

Gerenciar e manter a plataforma da CrowdStrike é muito mais fácil, com uma economia de cerca de 70% em termos de horas de manutenção. O agente Falcon é leve e pode ser instalado em minutos em milhares de usuários, sem exigir nenhuma reinicialização nem ajustes manuais.

Atualizações

SentinelOne

As atualizações do agente da SentinelOne são manuais e reconhecidas por falharem frequentemente. Todos os dispositivos, de computadores remotos a servidores críticos, precisam ser atualizados de forma cuidadosa para incorporar novas funcionalidades e proteção contra ataques emergentes.

CrowdStrike

As atualizações de sistema da CrowdStrike são automáticas para todos os dispositivos. Assim, a CrowdStrike oferece proteção contínua com uma operação muito mais simplificada, liberando tempo da equipe.

Qualidade dos alertas e inteligência de ameaças

SentinelOne:

O SentinelOne tem um número alto de falsos positivos, em parte por sua dependência excessiva de recursos autônomos, sem uma inteligência integrada contra ameaças. Na prática, os clientes perdem tempo tendo que analisar alertas de baixa qualidade.

CrowdStrike:

Por sua vez, a CrowdStrike conta com uma central de inteligência de ameaças e uma opção de serviço 100% gerenciado para detectar e responder a ameaças. A plataforma monitora mais de 200 adversários conhecidos e publica 200 mil novos Indicadores de Comprometimento (IOC) por dia.

Capacidade de detecção

SentinelOne

A SentinelOne sofre para detectar ataques sofisticados, como ataques do tipo fileless e ataques que não exigem execução de código malicioso. Seu mecanismo de detecção também está sujeito a falsos positivos.

CrowdStrike

Detecção abrangente e assertiva. Visibilidade e detecção superiores em dispositivos móveis, on-premises e na nuvem para descobrir e caçar ameaças avançadas sem sobrecarregar a equipe com falsos positivos.

Análises e telemetria

SentinelOne

A automação e a IA são aplicadas principalmente no nível do sensor, como no antivírus tradicional, e não em todo o ecossistema. Isso compromete a implementação de um verdadeiro XDR, já que há uma incapacidade de correlacionar automaticamente as detecções entre fontes de dados na nuvem.

CrowdStrike

IA e automação em todo o ecossistema, permitindo detecções de agentes locais, detecções comportamentais na nuvem e indicadores provenientes da caça a ameaças. A CrowdStrike processa trilhões de eventos de telemetria por semana e publica 200 mil novos IOCs diariamente.

Inteligência de Ameaças

SentinelOne

A inteligência de ameaças da SentinelOne funciona principalmente com base em feeds de terceiros, que entregam um valor inferior. Comparativamente, ela entrega uma fração dos IOCs, não proporciona atribuição de adversário nem descoberta tática, e não conta com sandbox para malware integrada.

CrowdStrike

Inteligência de ameaças global, aproveitando o poder do big data e da IA, bem como da experiência humana. Assim, as equipes recebem o máximo de contexto. Com essa inteligência, a CrowdStrike alavanca a publicação de IOCs, a atribuição de adversários e sua sandbox para filtragem e bloqueio de malware.

XDR

SentinelOne

XDR Parcial. O antivírus de última geração mascarado como XDR oferece enriquecimento e contextualização automatizados apenas para alertas gerados pelo SentinelOne. Ao contrário do verdadeiro XDR, o SentinelOne não pode criar alertas com base em sinais de baixa fidelidade de telemetria de terceiros.

CrowdStrike

Solução completa de XDR. Desenvolvida com base em EDR líder de mercado, com informações nativas sobre ameaças, SOAR e proteção de identidade. Também conta com uma aliança com soluções líderes de TI e de segurança (a CrowdXDR Alliance) para agir nos principais domínios de rede, nuvem, identidade e e-mail.

MDR (serviço gerenciado)

SentinelOne

MDR limitado. Os analistas do SentinelOne MDR exigem a detecção de ameaças antes de se envolverem, e a resposta é limitada à orientação de como remediar. A caça gerenciada a ameaças requer um SKU separado.

CrowdStrike

MDR com tudo incluído e pronto para uso. Inclui remediação de ciclo completo e não requer recursos adicionais de pessoal. Vale destacar que a CrowdStrike teve a maior cobertura de detecção de todos os participantes na avaliação 2022 MITRE ATT&CK para serviços gerenciados.

oblock.com.br

AGENDE UM FREE TRIAL

Veja na prática por que a CrowdStrike é líder de mercado em proteção de endpoints.

+55 (11) 2626-3401

contato@oblock.com.br

Curitiba, Brasil