

SIEM vs. SOAR vs. XDR



SIEM

Agrega os dados de registro gerados por aplicações, dispositivos endpoint e de rede. Suporte para big data (macrodados) e análise de eventos em tempo real

Suporta plugins de machine learning (ou aprendizado de máquina) e de análise comportamental para criar uma base de dados sobre o comportamento do usuário e do dispositivo

Depende fortemente dos produtos de segurança em silos, o que pode levar a alertas baseados em informações incompletas ou mal relacionadas

Possui resposta e visualização limitadas diante de incidentes. Coleta dados de eventos, mas requer esforço manual

Grande volume de alertas pode sobrecarregar as equipes de segurança. Exige ferramentas complementares para melhorar a qualidade dos alertas e automatizar respostas

SOAR

Visa melhorar a qualidade dos dados, simplificar a identificação de incidentes críticos e automatizar as ações de resposta a eventos e gatilhos

Tem como objetivo principal acelerar o processo de remediação e só repassar as ameaças quando a intervenção humana for necessária

Depende fortemente dos produtos de segurança em silos, o que pode levar a alertas baseados em informações incompletas ou mal relacionadas

Manter uma boa visibilidade em toda a rede se torna difícil à medida que a infraestrutura de TI continua a se modernizar e expandir

Utiliza dados de múltiplas fontes, o que requer integração com outras ferramentas de segurança, além de exigir diferentes níveis de alerta e ações personalizados

XDR

Centraliza e normaliza dados de todas as fontes conectadas, incluindo usuários, redes, ou qualquer outro local onde os dados e aplicações residam.

Tem como objetivo principal correlacionar todos os dados e alertas de segurança para possibilitar a detecção centralizada de incidentes e ameaças

Integra uma série de ferramentas de investigação, análise comportamental e capacidades de remediação automatizada em uma única plataforma

Forte foco na detecção avançada de ameaças e soluções sob medida, facilita o monitoramento de toda a superfície de ataque

Não possui as capacidades de gerenciamento, retenção e observância oferecidas pelo SIEM, portanto, precisa ser capaz de se integrar com os controles de segurança existentes

PONTOS IMPORTANTES A SEREM CONSIDERADOS

Quer as organizações optem por implantar um conjunto de sistemas ou uma plataforma unificada, elas precisarão de ferramentas de gerenciamento e retenção de logs e uma capacidade automatizada de detecção e resposta à ameaças para manter os sistemas e dados seguros e em conformidade. Os sistemas escolhidos também precisarão fornecer integração, além de possibilitar ajustes para detectar e responder aos incidentes de segurança de forma eficaz e eficiente.