kaspersky BRING ON THE FUTURE

# XDR vs. SIEM vs. SOAR

## O excesso de acrônimos te deixa confuso? Vamos descobrir o que está acontecendo por trás destas letrinhas...


## Introdução

SIEM, SOAR, MDR, EDR, EPP, XDR... você está se sentindo confuso e perdido em uma selva de acrônimos de cibersegurança? Nós te entedemos - por este motivo preparamos e fornecemos este guia para tratar das diferenças entre os três acrônimos principais: SIEM, SOAR e XDR. Qual é a história por trás destes acrônimos? Por que a indústria desenvolveu estes termos confusos e sobrepostos? Eles têm algum significado distinto ou são apenas truques de marketing? Quais são as similaridades e diferenças? Eles complementam um ao outro, ou são concorrentes?

Venha, junte-se a nós nesta busca! Vamos pegar nossos machados de conhecimento, passar pela floresta de acrônimos e nomenclaturas, e chegar em uma clareira aberta de entendimento!

## SIEM

Informações de segurança e gerenciamento de evento (SIEM) é um conjunto de ferramentas e serviços que combina o gerenciamento de eventos de segurança (SEM), e o gerenciamento de informações de segurança (SIM) em uma única plataforma. O SIEM coleta, agrega, analisa e armazena dados de registro na infraestrutura de TI para diversos casos de uso, incluindo governança, conformidade e correspondência de correlação baseada em regras para atividades suspeitas.

## Como o SIEM funciona?

Os primeiros serviços SIEM foram desenvolvidos em 2005, com o objetivo original de agregar e armazenar logs e eventos de toda a infraestrutura de TI de uma organização - para fins de relatórios de conformidade. O SIEM executa correlações neste conjunto de dados, procurando por quaisquer padrões ou eventos que possam indicar comportamento suspeito, e gera um alerta para o centro de operações de segurança (SOC). Os analista de segurança logo viram a possibilidade de usar estes alertas não somente para os propósitos de conformidade e governança, mas para identificar mais proativamente, e assim parar o progresso de qualquer atividade maliciosa no ecossistema.

## Limitações do SIEM

O problema era que os serviços SIEM não foram desenvolvidos para o propósito específico de detectar e responder aos incidentes. Isso tornou um pouco difícil trabalhar com eles, por diversos motivos:

- Excesso de alertas - o enorme conjunto de dados fornecido pelo SIEM tem que ser filtrado, processado e analisado manualmente, o que não é conveniente para analistas de segurança que ao mesmo tempo tentam evitar ataques em um cenário de ameaças acelerado.

- Nenhum contexto - para tratar de ataques novos, complexos e sofisticados, os analistas de segurança precisam de um quadro contextualizado e coerente do ambiente da organização, ao invés dos fluxos de dados desconexos fornecidos pelo SIEM.

- Muito passivo - bloquear processos suspeitos, colocar arquivos em quarentena e outras capacidades de resposta não estão dentro deste espectro; ele é basicamente uma ferramenta passiva e analítica.

Os profissionais de segurança tentaram resolver estes problemas ao colocar ferramentas adicionais em cima do SIEM, ou desenvolver novas gerações com machine learning e plugins de análise comportamentais. Mas a demanda por uma ferramenta que forneça alertas de melhor qualidade, agilize e automatize processos de segurança permaneceu.

# SOAR

As ferramentas de Orquestração de Segurança e Resposta Automatizada (SOAR) surgiram em 2015 para resolver algumas das falhas mencionadas acima do sistema SIEM. As plataformas SOAR fazem o processamento de dados originados de uma variedade de fontes na infraestrutura, incluindo sistemas de gerenciamento e plataformas de inteligência de ameaça, e fornecem análise de prioridade. As equipes de segurança podem então configurar respostas automatizadas em vários estágios e soluções cruzadas para ameaças recebidas, usando a integração da plataforma SOAR de um ecossistema de ferramentas de segurança conectados à API.

# Como o SOAR funciona?

Desta vez, o nome é realmente bastante útil! Veja aqui o porquê:
Ferramentas SOAR Automatizam. Embora mais conhecidas por suas capacidades de automatizar processos de resposta a incidentes, estas ferramentas podem de fato automatizar uma variedade de fluxos de trabalho, incluindo a verificação de vulnerabilidade, análise de registro, gerenciamento de acesso de usuário, triagem de ameaças e mais.

Elas fazem isso usando "roteiros" - conjuntos de regras pré-configuradas acionadas por eventos específicos, que informam ao sistema quais etapas devem ser tomadas a seguir em um fluxo de trabalho específico. A maioria das soluções SOAR vêm com centenas de roteiros prontos para uso, cobrindo a maioria das tarefas comuns enfrentadas por equipes SOAR. As equipes podem então configurar seus próprios roteiros para automatizar outros processos repetitivos particulares que elas possam ter.

E então, elas fazem a Orquestração. A automação se refere a execução conduzida por máquina de tarefas individuais dentro de um único fluxo de trabalho, e a orquestração se refere a coordenação de múltiplas ferramentas e processos diferentes em um fluxo de trabalho maior, colocando todos os dados relevantes ema um única plataforma para obter informações consolidadas e acionáveis.

# O relacionamento entre SIEM e SOAR

Normalmente, um SIEM é usado em conjunto com ferramentas SOAR em algo como um relacionamento assistente-gerente: o SIEM coleta todos os registros, os correlaciona para encontrar alertas, e serve esta informação ao SOAR, que pode então liderar as ações de resposta.

# Limitações do SOAR

Tudo parece ser ótimo, correto? A questão é que manter uma plataforma SOAR bem configurada que se integra com as ferramentas de parceiros, requer um esforço contínuo de uma equipe SOC altamente especializada e madura - um recurso que muitas organizações não têm neste momento, dada a atual lacuna de habilidades em segurança cibernética.

Sem essa manutenção qualificada e vigilante, os analistas SOAR podem acabar com muitos alertas de baixa prioridade, falsos positivos e um conjunto de dados geralmente incoerentes como resultado de todas estas diversas ferramentas isoladas que alimentam a plataforma - exatamente o que eles tentam evitar.

# XDR

O XDR é uma solução de segurança local ou baseada na nuvem, que vem sob duas amplas categorias: nativa e híbrida. XDR nativa é um conjunto unificado de ferramentas de um único fornecedor, enquanto a XDR híbrida integra outras soluções de terceiros em seu ecossistema. O termo "XDR" foi primeiramente usado em 2018, com o "X" para "eXtended" (estendido em português): o XDR se "eXtende" além das ferramentas de detecção de endpoint, resposta e proteção (EDR e EPP) ao coletar e correlacionar dados de múltiplas camadas de segurança, incluindo e-mail, nuvem e rede, para assim fornecer proteção completa em toda a infraestrutura de TI.

Portanto, é uma plataforma única que coordena uma variedade de ferramentas, e utiliza machine learning e automação para ajudar as equipes de segurança a proteger todo o ecossistema de segurança... parece um pouco similar ao SOAR, não é mesmo? Mas há algumas diferenças fundamentais. Vamos examinar...

# XDR vs. SOAR: Qual é a diferença?

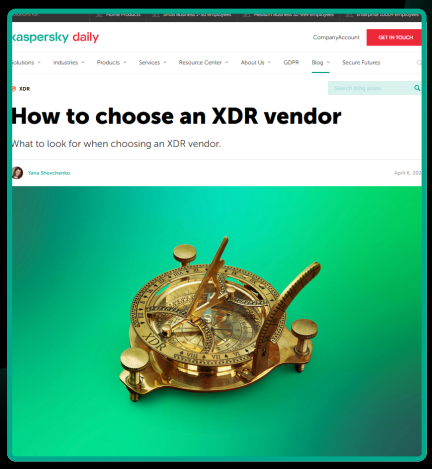
1. As soluções XDR estão ancoradas nos dados e otimização de endpoints - isto significa que a detecção e reposta de incidente é um recurso de design central, oferecendo recursos avançados de análise que as ferramentas SOAR normalmente não possuem. As ferramentas XDR são mestres em detectar ameaças desconhecidas e de dia zero, tirando vantagem de uma poderosa inteligência artificial, algoritmos de machine learning e inteligência de ameaças para proteger uma organização além de seus limites. De outro lado, as ferramentas SOAR oferecem uma variedade muito mais ampla de casos de uso, uma vez que elas podem orquestrar e automatizar quaisquer processos na infraestrutura - não apenas respostas a incidentes.

2. O XDR pode ser considerado como um tipo de SOAR leve - uma interface racionalizada que oferece com um clique, repostas automatizadas para ameaças e alertas recebidos. Isso pode ser muito mais conveniente para uma organização que não tem os recursos para manter a complexidade de uma plataforma SOAR bem configurada.

3. O XDR permite a integração entre produtos - seja em uma pilha de ferramentas de um único fornecedor, ou em produtos de terceiros, o XDR tem excelência em interoperabilidade racional. As ferramentas SOAR geralmente enfrentam dificuldades ao tentar integrar todas as ferramentas diferentes e isoladas em sua pilha; o XDR separa estas diferenças para uma resposta eficiente e completa contra as ameaças.

## Como escolher um fornecedor de XDR?

Muitos fornecedores de segurança cibernética entraram na onda do XDR com suas próprias soluções. Como você pode saber se está recebendo um produto de boa qualidade? Confira nosso guia completo: https://www.kaspersky.com/blog/choosing-xdr-vendor/44063/



# E então, o XDR substituirá o SIEM e o SOAR?

Nós da área de cibersegurança ainda não avaliamos este caso, já que o XDR é um tecnologia relativamente nova que está sendo continuamente desenvolvida. No momento, a maioria dos especialistas recomendam uma abordagem integrada, já que cada solução oferece vantagens que complementam as outras.

- SIEM - o SIEM tem casos de uso fora da detecção de ameaça, tal como gerenciamento de registro, conformidade, e análise de dados não relacionados à ameaça.
- SOAR - a grande personalização dos roteiros SOAR é útil para orquestrar e automatizar processos na infraestrutura das organizações.
- XDR — quando se trata de detectar e responder às ameaças, a análise avançada de uma solução XDR oferece proteção avançada melhor do que qualquer outra.

Procurando por uma solução adaptável, comprovada e testada para seus especialistas? O Kaspersky Expert Security, XDR com base em uma solução EDR nativa na nuvem, fornece para a sua organização visibilidade e funcionalidade aprimoradas para toda a detecção com base em IA e lógica de reposta automática em todos os endpoints e redes, facilitando uma ampla gama de cenários automatizados de resposta a incidentes. A tecnologia avançada incorporada na plataforma para a detecção e análise é complementada pela inteligência de ameaça líder mundial. A arquitetura do Kaspersky XDR fornece o gerenciamento centralizado em um único console na Web. Para saber mais, visite go.kaspersky.com/expert.

**www.kaspersky.com.br**

© 2022 AO Kaspersky Lab.
As marcas registradas e de serviço são de domínio de seus respectivos proprietários.