# REDEFINIR AS OPERAÇÕES DE SEGURANÇA COM O XDR

## Não se limite com a detecção e resposta do endpoint

**Introdução**

O objetivo de qualquer equipe de segurança é defender a infraestrutura e os dados de uma organização contra danos, acesso não autorizado e uso indevido. Os arquitetos e engenheiros de segurança geralmente adotam uma abordagem estratificada para a prevenção. Conforme os ataques se tornaram mais automatizados e complexos, essa abordagem evoluiu para incluir visibilidade estratificada na forma de produtos de detecção e resposta, como detecção e resposta de endpoint (sigla em inglês EDR), análise de tráfego de rede (sigla em inglês NTA) e gerenciamento de eventos e informações de segurança (sigla em inglês SIEM).

Essa visibilidade estratificada é obtida mediante o custo de tempo e especialização. Produtos de detecção e resposta diferentes geram alertas adicionais, exigindo um conjunto maior de habilidades para resolver e que prolonga um ciclo interminável: um fluxo interminável de eventos, mais ferramentas e informações para lidar, cada vez mais tempo até a detecção e uma equipe de segurança que beira a exaustão, tudo isso enquanto o gasto com segurança nunca parece ser suficiente. Quanto mais reagimos, mais longe ficamos.


**Figura 1:** Rede, endpoint ou nuvem

Muitas organizações como a sua se deparam com a mesma questão: como podemos deixar de reagir a alertas de entrada e adotar uma postura de defesa ativa que possa melhorar a prevenção de ameaças?

Está na hora de uma abordagem diferente, uma que beneficie toda a equipe de segurança, em vez de sobrecarregá-la, simplifique as operações e forneça os meios para detectar e responder rapidamente às ameaças mais sofisticadas em todo o ecossistema.

**Abordagem atual: resolver um problema cria outros**

As equipes de segurança trabalham arduamente para manter suas organizações seguras, mas enfrentam dificuldades em seus esforços para evitar violações de dados. Os cinco principais desafios incluem:

- Excesso de eventos
- Poucos analistas de segurança
- Ferramentas limitadíssimas
- Falta de integração
- Falta de tempo


**Figura 2:** As equipes do SOC enfrentam cinco desafios primários

Vamos explorar cada um com algum detalhe.

### *1. Excesso de eventos*

Os analistas de segurança observam eventos em demasia para lidar com eles de forma eficaz. 55% das equipes de segurança ou dos centros de operações de segurança (sigla em inglês SOCs) recebem em média mais de 10.000 eventos por dia.[1] No entanto, nem todos os eventos são iguais, a maioria precisa ser priorizada, correlacionada ou normalizada e incluída no pool de alertas. Mesmo com o SIEM para ajudar a equipe SOC vasculhar essa massa de dados, um analista de segurança ainda precisa empregar esforço manual para coletar dados, realizar análises e eliminar falsos positivos, e rapidamente, ou vai perder os alertas mais essenciais. Com muita frequência, os analistas são vítimas da "fadiga de alertas", quando filtram os alertas com base em suposições anteriores ou na grande quantidade de dados. Devido ao volume de alertas, 54% dos profissionais de segurança ignoram os alertas que deveriam ser investigados.[2]

### *2. Escassez de qualificação*

Muitas organizações estão tentando superar o aumento das cargas de trabalho contratando mais pessoas, mas existe uma escassez mundial de profissionais de segurança treinados que os analistas preveem atingir 1,8 milhões até 2022.[3] É especialmente difícil encontrar especialistas com experiência forense de rede ou endpoint, ou ambos. Como resultado, as equipes de segurança estão sobrecarregadas em termos de triagem de alertas, bem como de investigação e resposta. Elas gastam um exorbitante tempo com tarefas entediantes, como coleta de dados, análise manual e incorporação de inteligência, ou tentando incorporar a automação, o que resulta em mais pressão. Isso também serve para restringir o aprendizado e o compartilhamento, pois o conhecimento e a atividade histórica permanecem isolados e indisponíveis para outros grupos.

A combinação de muitos alertas, investigações complexas e poucos analistas leva ao erro humano e cria um efeito bola de neve downstream. Os alertas têm sua priorização revertida ou falsamente escalada devido à falta de informações, resultando em mais trabalho para os membros da equipe de investigação de incidentes, que precisam da ajuda das equipes de caça para lidar com a carga de trabalho.

### *3. Ferramentas diferentes com um foco muito limitado*

A inclusão de ferramentas é uma forma de superar outros desafios, permitindo ao mesmo tempo decisões mais rápidas e substanciadas. Mas será que o excesso de ferramentas existe mesmo? A maioria das ferramentas de segurança foi desenvolvida para abordar lacunas tecnológicas específicas sem considerar como as ferramentas devem funcionar em um ambiente operacional e, muitas vezes, elas funcionam no sentido inverso da meta da equipe de segurança de fornecer prevenção e visibilidade holísticas. Operando em silos, sem integração e ingerindo dados de apenas uma única fonte, essas ferramentas trazem valor apenas para aqueles com qualificação específica na equipe de segurança, e, ao mesmo tempo, não fornecem valor e ainda sobrecarregam outros.

Algumas ferramentas comumente usadas para aos detecção e resposta são valiosas, mas limitadas:

- O **EDR** pode reduzir o tempo de investigação para equipes experientes de resposta a incidentes, mas é limitado a dados dos endpoints nos quais você pode instalar um agente. O EDR também pode aumentar drasticamente o volume de alertas, e requer desenvolvimento personalizado para habilitar a automação básica, sobrecarregando outras partes da equipe ao mesmo tempo.
- O **NTA** exige o posicionamento adequado do sensor para evitar a perda de volumes do tráfego, raramente inclui resposta e não incorpora os dados do endpoint como um fator na detecção de anomalias ou na investigação de ameaças.
- O **UEBA** (análise de comportamento de usuários e entidades) é amplamente focado em dados de log e não fornece detalhes importantes da análise profunda da rede, sem mencionar o endpoint e a nuvem. Além disso, o UEBA tem uma alta taxa de falsos positivos, aumentando ainda mais as cargas de trabalho dos analistas.

Todas essas ferramentas ajudam na visibilidade, mas, como introduzem novos problemas, ainda exigem qualificação específica para entregar resultados acionáveis.

### *4. Síndrome da cadeira giratória para investigações*

A detecção de ataques sofisticados exige que os dados sejam correlacionados de qualquer lugar no domínio digital. Como a maioria das ferramentas que auxiliam na detecção e na resposta são baseadas em apenas uma fonte de dados, assim como o endpoint, elas perdem pistas importantes de outras fontes essenciais, fazendo com que as equipes de segurança façam o trabalho pesado na validação de ameaças. Com um típico SOC de uma grande organização usando mais de quarenta ferramentas, cada uma operando de forma independente, os analistas do SOC se encontram no modo "cadeira giratória": mudam de tela para tela, tentando reunir conclusões de informações relevantes para atenuar as ameaças reais. Se os dados fossem correlacionados, isso poderia fornecer uma visão holística do ambiente, mas exigiria normalização, data/hora/correspondência de eventos e um entendimento das técnicas investigativas em várias áreas, como a rede e os endpoints. Não é uma proposta fácil e, hoje, deve ser feita manualmente.

1. "Pesquisa: 27% dos profissionais de TI recebem mais de 1 milhão de alertas de segurança diariamente", Imperva, 28 de maio de 2018, https://www.imperva.com/blog/2018/05/27-percent-of-it-professionals-receive-more-than-1-million-security-alerts-daily/.
2. "2017: Desafios, prioridades e estratégias das operações de segurança", ESG, março de 2017, http://resources.siemplify.co/hubfs/PDF%20Downloads/ESG-Research-Insights-Report-Siemplify.pdf?hsCtaTracking=4303efc5-9f7b-4a8a--9438-263c0588b898%7C6043fb9a-2881-4940-9a0e-6239a8686b81.
3. "Estudo global sobre a força de trabalho de segurança da informação 2017", Frost & Sullivan, acessado em 8 de janeiro de 2019, https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf.

*5. O tempo é o inimigo*

Não há nada mais valioso que o tempo. Quanto mais rapidamente uma ameaça puder ser identificada, maiores serão as chances de contenção. À medida que as equipes lutam com o excesso de eventos, problemas de recursos e falta de correlação, elas correm o risco de perder alertas comuns que se tornam incidentes importantes e têm dificuldade para alocar tempo para encontrar ameaças desconhecidas. Em média, observamos mais de seis meses entre a ocorrência de uma violação de dados até quando ela é identificada pela primeira vez,[4] e esse "tempo de espera" está piorando. O tempo médio de identificação (MTTI) aumentou de 190 dias em 2017 para 197 dias em 2018, e os tempos de resposta, mensurados como tempo médio para conter (MTTC), aumentaram de 66 dias em 2017 para 69 dias em 2018.[5]

Tudo isso ocorre em um momento em que as organizações adotam o EDR, NTA e UEBA e reavaliam o SIEM enquanto gastam quase 60% dos orçamentos de TI em segurança.[6] Mesmo com essas ferramentas, os analistas gastam quantidades significativas de tempo em tarefas manuais, como gravar consultas, correlacionar alertas com dados de log e juntar informações de fontes diferentes. Com um conjunto de trabalho constante, não é de se admirar que poucas equipes de segurança tenham tempo para se concentrar em tarefas essenciais, como caçar ameaças sofisticadas, pensar mais profundamente e resolver problemas obscuros de segurança que programas inteligentes e automação não conseguem desvendar.

## O SOC merece uma abordagem melhor

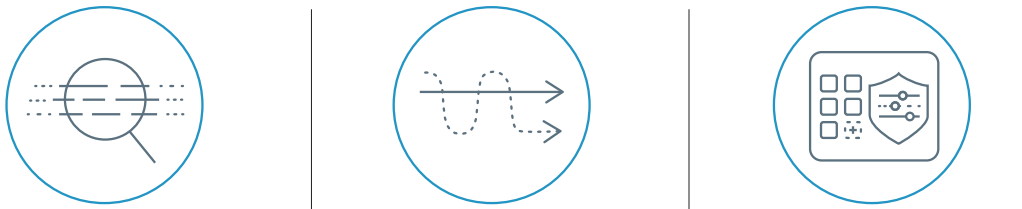
A equipe do SOC precisa de uma abordagem que resolva efetivamente os problemas mencionados anteriormente. Isso exige uma nova abordagem que possa ajudar o SOC em todos os estágios das operações (triagem de alertas, investigação de incidentes e caça a ameaças) e ajudar a concluir investigações rapidamente, independentemente do tipo da ameaça. Em termos práticos, a abordagem ideal seria:

- Rastrear as atividades em toda a sua rede, endpoints e nuvens para fins de detecção, triagem de alertas, investigação e resposta.
- Integrar com as ferramentas que geram alertas ou fornecem inteligência para apresentar informações automaticamente, tirar conclusões e até tomar providências quando possível.
- Usar análises em grande escala para correlacionar os dados de todas as fontes, permitindo a detecção automatizada ou manual de ameaças difíceis de encontrar, abrangendo várias fontes de dados, com poucos falsos positivos.
- Simplificar as investigações para auxiliar analistas menos experientes e reduzir a sobrecarga dos funcionários experientes, melhorando drasticamente o tempo em todos os estágios das operações do SOC.
- Garantir que as informações de cada investigação possam ser transformadas rapidamente em defesas, como incluir contexto em futuras investigações, reduzir o número de alertas e fechar vulnerabilidades recém-conhecidas.

Isso reduziria notavelmente o tempo médio entre detectar e responder às ameaças (tempo de espera), bem como ajudaria as equipes de segurança a não reagirem aos alertas de segurança e a defenderem a rede proativamente.

## O XDR eleva a detecção e a resposta a um outro nível

A Palo Alto Networks está introduzindo uma abordagem inovadora para as operações de segurança, aumentando a visibilidade, bem como a velocidade de detecção, investigação e resolução de ameaças. Ela se chama XDR, uma evolução na categoria de detecção e resposta. O "X" representa qualquer fonte de dados, seja rede, endpoint ou nuvem, com um foco na multiplicação da força de produtividade do SOC por meio da automação. A visibilidade total fornece um retrato holístico da atividade da organização, ao vincular os dados de várias fontes, para que não haja mais correlação manual de dados e nenhum lugar para que as ameaças se escondam. A integração extrai dados



Encontrar ameaças sigilosas mais rapidamente com análises em rede, nuvem e endpoint

Simplificar a investigação e a resposta a ameaças conhecidas e desconhecidas

Melhorar radicalmente as operações de segurança e o retorno sobre os investimentos em segurança

**Figura 3:** Três principais benefícios do XDR

4. "Custo de um estudo de violação de dados 2018", Instituto Ponemon, maio de 2018, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=55017055USEN&.
5. Ibid.
6. "Infográfico: os orçamentos de TI estão um pouco maiores; o foco dos gastos está na segurança, hardware e nuvem 2018", ZDNet, 2 de outubro de 2017, https://www.zdnet.com/article/infographic-2018-it-budgets-are-up-slightly-spending-focus-is-on-security-hardware-and-cloud.

de fontes externas, como alertas de segurança e inteligência global de ameaças, para incluir insights. A automação une dados essenciais, ao mesmo tempo que chega a conclusões para os analistas de segurança, fazendo em segundos o que normalmente levaria horas com anos de experiência. O resultado são investigações simplificadas em todas as operações de segurança, reduzindo o tempo necessário para descobrir, caçar, investigar e responder a qualquer tipo de ameaça.

O XDR inaugura uma nova era de heurística, análise e modelagem, aplicando inteligência artificial e aprendizado de máquina para detectar e interromper rapidamente as ameaças mais sofisticadas. À medida que rastreia ameaças em qualquer fonte ou local na infraestrutura de uma organização, o XDR pode automatizar a contenção, reconstruir cada etapa de um ataque para fornecer uma sequência clara dos eventos, aplicar inteligência de ameaças e preencher as lacunas para prevenção futura. Isso acelera o tempo de resolução e libera os analistas da investigação intensiva. É importante ressaltar que o XDR deve ser entregue como uma oferta completa de nuvem para garantir a facilidade da implantação.

## Benefícios da detecção e resposta do XDR

O XDR foi projetado para trabalhar para e com o SOC. Ele oferece três benefícios significativos: visibilidade ilimitada, operações simplificadas de segurança e retorno radicalmente maior sobre o investimento em segurança.

### *Visibilidade ilimitada para encontrar ameaças furtivas mais rapidamente*

O XDR descobre atividades anômalas, correlacionando o comportamento de usuários, entidades e ações em todas as fontes de dados. Ele reduz a complexidade da caça às ameaças fornecendo recursos avançados de pesquisa, atribuição qualitativa e correlação de dados. O XDR automatiza a descoberta de ameaças ativas ou pregressas usando análise de big data em todos os de endpoints, redes, nuvens e inteligência de terceiros, convergindo a descoberta de ameaças desconhecidas para um local para o SOC.

### *Simplifica as operações de segurança em triagem, investigação e resposta*

O XDR acelera e simplifica as investigações, ao visualizar a cadeia de atividades de qualquer evento para revelar automaticamente as causas raiz e fornecer detalhes forenses acionáveis para todos os analistas de segurança. Ele elimina a fadiga de alertas correlacionando os resultados da investigação com todos os alertas de segurança de qualquer tecnologia, permitindo que analistas menos experientes façam mais, mais rapidamente. O XDR responde a ameaças ativas e evita futuros ataques bem-sucedidos por meio da aplicação coordenada da segurança em toda a sua rede, nuvens e endpoints, liberando os analistas do trabalho manual e dando mais tempo para a detecção de ameaças.

### *Aumenta radicalmente o retorno sobre os investimentos em segurança*

O XDR atua como um multiplicador de forças para a equipe de analistas de segurança, agilizando os fluxos de trabalho, bem como reduzindo o tempo e a complexidade da triagem de eventos, investigação de incidentes, resposta e caça. Ele permite que as ferramentas de segurança trabalhem juntas para resolver automaticamente os problemas, usando inteligência de ameaças e dados qualitativos. O XDR fortalece a prevenção aplicando o conhecimento adquirido em cada investigação para melhorar as defesas e evitar alertas adicionais ou ameaças semelhantes, no futuro.

## Como o XDR poderia beneficiar seu SOC?

O XDR complementa sua abordagem primordialmente preventiva com uma tecnologia de detecção e resposta que ajuda a transformar suas operações de segurança de reativas em proativas. A visibilidade total de todas as fontes de dados e o foco correto no processo, da triagem de alertas à caça a ameaças, ajudarão você a melhorar drasticamente as operações de segurança.

Você será capaz de tornar a fadiga de alertas uma coisa do passado, capacitar seus analistas de segurança a filtrar falsos positivos e tomar decisões em tempo recorde, liberar seus analistas qualificados da investigação manual e correção, dar aos caçadores de ameaças a capacidade de encontrar ameaças desconhecidas e a estarem preparado para ameaças conhecidas no futuro.

Ao fornecer automação e uma visão geral da segurança, o XDR mantém a promessa de liberar todo o poder do seu SOC. Se você estiver pesquisando tecnologias de detecção e resposta, pergunte ao seu fornecedor sobre o X, porque uma visualização do seu ambiente não é mais suficiente.

3000 Tannery Way
Santa Clara, CA 95054

Principal: +1.408.753.4000
Vendas: +1.866.320.4788
Suporte: +1.866.898.9087

www.paloaltonetworks.com



redefine-security-operations-with-xdr-wp-012219