Kaspersky Next XDR Expert

Maior, melhor, mais rápido, e mais

kaspersky

Algo que irá revolucionar a indústria ou apenas uma necessidade a procura de uma solução?

Para quem serve:

A XDR é destinada a organizações com uma postura de segurança já estabelecida, que precisam de uma plataforma única que lhes forneça uma visão completa e coerente do que está acontecendo em toda a sua infraestrutura.

XDR: Detecção e Resposta Estendidas

É o acrônimo na boca de muitas pessoas, mas como qualquer tecnologia relativamente nova, nem todo mundo sabe exatamente o que é ou quais os benefícios para os seus negócios. Uma coisa é certa: a XDR envolve uma mudança estratégica da reatividade para a proatividade, porque sabemos que "esperar para ver" não funciona na cibersegurança. A aposta inteligente é que a XDR seja vista como uma estratégia, e não apenas como um produto.

Então, a XDR é apenas a última necessidade tecnológica em busca de solução ou um potencial divisor de águas? As necessidades certamente existem, desde a escassez global de especialistas, a sobrecarga de trabalho das equipes de segurança de TI em um cenário de ameaças que nunca para, até a sobrecarga de alertas, ferramentas diferentes, inteligência de ameaças fraca e superfície de ataque em expansão. A IDC afirma que o XDR será "uma força disruptiva, afetando as vendas de SIEM, EDR, SOAR, inteligência de rede e plataformas de análise de ameaças, bem como os fornecedores de inteligência de ameaças externas" [1], e a Forrester acredita que a tecnologia XDR diferenciada "substituirá a detecção e a resposta de endpoints (EDR) em curto prazo e tomará o lugar do SIEM a longo prazo" [2].

A XDR será uma força disruptiva — IDC

Mais dispositivos, mais aplicativos, mais tráfego de rede, mais dados, mais ameaças...

Pra que serve a XDR — e quais desafios ela pode resolver?

A XDR é destinada a organizações com uma postura de segurança já estabelecida, que precisam de uma plataforma única que forneça uma visão completa e coerente do que está acontecendo em toda a sua infraestrutura.

Os desafios de cibersegurança que essas organizações enfrentam são consistentes e bem estabelecidos. A ESG Research pesquisou profissionais de TI e de cibersegurança[3] em organizações com 100 ou mais funcionários, mais de 80% em empresas, em diversos cargos. Aqui estão algumas das principais descobertas:

Dificuldades para acompanhar os requisitos operacionais das tecnologias do SOC (Centro de Operações de Segurança)

O gerenciamento das operações de segurança é mais difícil agora do que em qualquer outro momento nos últimos dois anos, devido às dificuldades de acompanhar as necessidades operacionais das tecnologias SOC — escalabilidade no pipeline de dados, mecanismos de processamento de balanceamento de carga, adição de capacidade de armazenamento etc.

[1] Fonte: IDC Global Security Products Analysis: From Power Point to Power Product, Where Is XDR Right Now? 2022

[2] Fonte: Forrester, Detecção e Resposta Estendidas (XDR) — uma batalha entre o precedente e a inovação, Allie Mellen, analista sênior, 2021

[3] Fonte: Relatório da ESG Research, Modernização do SOC e a importância do XDR, 2022

A superfície de ataque em constante expansão e mudança e o cenário geral de ameaças

Mais dispositivos, mais aplicativos, mais tráfego de rede, mais dados, mais ameaças. O cenário de ameaças não para e as ciberameaças continuam e evoluir em volume e complexidade à medida que novas ferramentas se proliferam. Ao mesmo tempo, a barreira de entrada para a indústria de hackers está mais fraca do que nunca, com criminosos inexperientes comprando malwares baratos na dark web de um lado, e hackers altamente qualificados e pacientes desenvolvendo ataques complexos do outro. E não podemos esquecer das ameaças internas e de vulnerabilidades na cadeia de suprimentos.

O grande número de processos manuais necessários para gerenciar a segurança

Há mais dados de segurança a serem coletados e processados, e processá-los manualmente é ineficiente e ineficaz. Isso cria uma tempestade perfeita que afeta a escalabilidade, resulta em uma dependência excessiva do envolvimento humano direto e degrada a eficácia de lidar com todos os tipos de ameaças.

Incapacidade de desenvolver regras de detecção

Uma incapacidade de desenvolver regras de detecção, ajustar os controles de segurança e identificar e lidar com ameaças de forma rápida e eficiente, devido à falta de tempo, recursos e habilidades. As organizações nem sempre têm as habilidades ou a equipe certa para acompanhar a análise e as operações de segurança. O que nos leva diretamente ao próximo desafio...

A escassez global de habilidades em cibersegurança

Apesar da força de trabalho global em segurança cibernética atingir um recorde histórico de 4,7 milhões de profissionais, ainda há um déficit de 3,4 milhões que está longe de ser resolvido. Esse déficit está crescendo duas vezes mais rápido do que a força de trabalho, com um aumento anual de 26,2%.[4]

[4] Fonte: (ISC)², Estudo da força de trabalho de cibersegurança, 2022

As ferramentas existentes muitas vezes apresentam dificuldades

em detectar e investigar ameaças avançadas, além das habilidades especializadas necessárias para usá-las e gerenciá-las.

Ferramentas não adequadas às suas próprias finalidades

Quando as próprias ferramentas se tornam parte do problema, algo precisa ser feito. As ferramentas existentes geralmente apresentam dificuldades para detectar e investigar ameaças avançadas, além das habilidades especializadas necessárias para usá-las e gerenciá-las. A pesquisa[5] mostra que as ferramentas atuais são frequentemente ineficazes na correlação de alertas, e a equipe de segurança de TI tem dificuldades com várias ferramentas lidando com diferentes tipos de dados ao mesmo tempo. Isso acaba sendo ineficiente, incômodo, complicado e caro. Outro desafio é que as ferramentas atuais não são dimensionadas para lidar com a superfície de ataque em constante expansão, e existem grandes brechas nos recursos de detecção e resposta na nuvem.[6]

É de se admirar que o seu CISO possa estar estressado?

A boa notícia é que melhorar o SecOps é uma prioridade e é financiado — 88% das organizações vão gastar mais este ano, 66% dizem que a consolidação de ferramentas é uma prioridade, e o desenvolvimento e a implantação de aplicativos modernos aumentaram a velocidade, exigindo novas habilidades específicas.[7]

88%

das organizações vão gastar mais este ano para melhorar o SecOps

66%

afirmam que a consolidação de ferramentas é uma prioridade

O que a XDR faz

Veja como a XDR pode superar esses desafios.

A XDR detecta melhor as ameaças avançadas

Os recursos de detecção de ameaças da XDR abrangem endpoints, redes e ambientes de nuvem. Ela usa algoritmos de aprendizado de máquina e análise comportamental para identificar ameaças sofisticadas, incluindo malware, ransomware e ameaças persistentes avançadas (APTs).

Resposta e remediação automatizadas

A XDR automatiza as ações de resposta e correção, permitindo que as organizações contenham as ameaças rapidamente e minimizem os possíveis danos. Coloque em quarentena ou isole endpoints comprometidos, bloqueie atividades maliciosas e corrija vulnerabilidades, reduzindo o esforço manual e o tempo de resposta.

Integra-se com ferramentas de proteção de endpoints

A integração com o EPP é uma questão fundamental, e a XDR aproveita a telemetria avançada do endpoint e a análise comportamental para fornecer insights profundos sobre as atividades do endpoint. Ela emprega algoritmos avançados de aprendizado de máquina para identificar comportamentos suspeitos e indicadores de ataques (IOAs), facilitando a detecção antecipada de ameaças sofisticadas.

[5] Fonte: Relatório da ESG Research, Modernização do SOC e a importância do XDR, maio de 2022

[6] Fonte: Relatório da ESG Research, Modernização do SOC e a importância do XDR, 2022

[7] Fonte: Relatório da ESG Research, Modernização do SOC e a importância do XDR, maio de 2022

Onde a XDR se encaixa no ecossistema de EDR, MDR, SOAR e SIEM

A pista está no X — estendidas. A XDR amplia (estende) os recursos oferecidos pelo EDR para detectar proativamente ameaças complexas em vários níveis de infraestrutura, além de responder e combater automaticamente essas ameaças.

Uma abordagem integrada é a chave

Ao integrar várias ferramentas e aplicativos de segurança e monitorar dados em endpoints, redes, nuvens, servidores da Web, servidores de e-mail e muito mais, a XDR trabalha para melhor detectar e eliminar ameaças e, ao mesmo tempo, simplifica o gerenciamento da segurança das informações ao automatizar a interação entre produtos.

A Forrester acredita que, na maioria dos casos, a XDR não substituirá completamente as plataformas de análise de segurança, observando que "a XDR está em uma jornada e [esperamos] que, nos próximos cinco anos, as plataformas de análise de segurança e a XDR se unifiquem".

O SIEM tem casos de uso que vão além da detecção de ameaças, e a capacidade de personalização do SOAR é útil, mas quando se trata de detectar e responder a ameaças, a análise avançada da proteção aprimorada da XDR é inigualável.

Oferece visibilidade em tempo real

A XDR oferece visibilidade em tempo real da postura de segurança de sua organização. Ela coleta e analisa dados de várias fontes, como endpoints, servidores, firewalls e plataformas de nuvem, para fornecer insights abrangentes sobre ameaças contínuas e atividades suspeitas em um único console. Isso a torna verdadeiramente proativa — caça proativa a ameaças e resposta mais rápida a incidentes. Uma visão abrangente ajuda as equipes de segurança a identificar atividades suspeitas e possíveis incidentes de segurança com mais eficiência.

Contextualiza os dados e a inteligência de ameaças

Ao tirar vantagem de uma inteligência de ameaças de alta qualidade e um banco de dados abrangente de inteligência de ameaças, a XDR fornece informações contextuais altamente úteis sobre ameaças e invasores. Essa inteligência de ameaças enriquecida simplifica os alertas de investigação e o tratamento de incidentes, além de ajudar as equipes de segurança a entender suas táticas, técnicas e as motivações das ameaças, facilitando uma resposta mais eficaz a incidentes e medidas de defesa proativas.

Permite operações de segurança simplificadas

Quando devidamente integradas, as melhores soluções se encaixam sem esforço em sua infraestrutura atual para oferecer os melhores resultados da automação e proporcionar total visibilidade e conscientização, sem a necessidade de substituir soluções de segurança de terceiros já em uso. E não esqueça que ao fornecer uma visualização abrangente dos incidentes de segurança e do comportamento do usuário, a integração apoia a conformidade.

É fato que a XDR pode oferecer o que diz na embalagem: controle, estabilidade e aquela vantagem importantíssima. Mas nem todas as ofertas de XDR são iguais... Como escolher a mais adequada para você?

5 principais pontos a serem considerados ao comparar fornecedores e soluções XDR

Veja como a XDR pode superar esses desafios.

1

Há uma ligação direta entre a qualidade de uma solução XDR e a sinergia entre a EPP (plataforma de proteção de endpoint) e a EDR (detecção e resposta no endpoint) do fornecedor

Uma solução EDR para detecção avançada e resposta a ciberameaças sofisticadas no nível do endpoint é um elemento fundamental da XDR. Ao mesmo tempo, a EDR precisa de uma Plataforma de Proteção de Endpoint (EPP) robusta para filtrar automaticamente um grande número de ameaças em massa. É importante examinar cuidadosamente os recursos de proteção de endpoints e verificar se há suporte para todos os tipos de endpoints — PCs, laptops, máquinas virtuais, dispositivos móveis e vários sistemas operacionais.

2

A inteligência atualizada sobre ameaças e uma visão completa das táticas e técnicas dos criminosos cibernéticos são essenciais para combater as ciberameaças

Não é coisa de outro mundo— qualquer solução XDR de qualidade oferecerá esses dois recursos, juntamente com contexto adicional para melhorar e acelerar a investigação e a resposta a incidentes.

3

A integração com soluções de terceiros é mais sustentável e econômica

A boa integração de uma solução XDR com terceiros é outra questão absolutamente crítica, pois a interoperabilidade torna a compra um investimento mais sustentável desde o início. Uma solução XDR que ofereça inúmeras e genuínas opções de integração coletará mais fontes de dados e fornecerá um quadro mais completo do que está acontecendo em sua infraestrutura.

4

Revisões independentes, reconhecimento global e resultados de testes independentes são importantes

Quando estiver investindo em algo tão importante para a sua empresa como a cibersegurança, não deixe de lado as avaliações independentes. Solicite os resultados de testes independentes. Verifique o reconhecimento internacional de empresas como a Forrester, a IDC e outras. As soluções são implementadas globalmente? Solicite estudos de caso.

5

Seu investimento está preparado para o futuro?

A tecnologia não para de evoluir, especialmente para algo como XDR, que ainda é uma tecnologia relativamente nova, você deve descobrir qual é o roteiro do fornecedor para o desenvolvimento contínuo.

Por que a Kaspersky

A mais testada. A mais premiada. Proteção Kaspersky.

A Kaspersky é uma empresa líder global em cibersegurança que conta com um extenso histórico de experiência em segurança. Protegemos organizações em todo o mundo há mais de 25 anos e recebemos inúmeros prêmios e reconhecimentos por nossos produtos e serviços. Entre 2013 e 2022, os produtos Kaspersky:

587

conquistou 587 primeiros lugares

685

conquistou um lugar entre os três melhores

827

participaram de 62 testes e análises independentes

Em 2023, a Kaspersky foi nomeada líder no mercado de soluções XDR pela empresa líder global de pesquisa e consultoria em tecnologia ISG. O ISG define "líderes" como aqueles com uma oferta abrangente de produtos e serviços e representam força inovadora e estabilidade competitiva.

Saiba mais

Kaspersky Extended Detection and Response

Saiba mais

www.kaspersky.com.br

#kaspersky
#bringonthefuture