CISCO
SECURE

Guia do comprador de XDR

Navegando como um profissional no emergente mercado de Detecção e Resposta Estendida

cisco SECURE

Compreendendo Extended Detection and Response (XDR)

Por que o mundo precisa de outra abordagem de segurança?

Até mesmo as equipes de segurança mais confiantes e bem financiadas sabem que estão enfrentando pressões externas avassaladoras. A recente mudança para o trabalho remoto e/ou híbrido adicionou novas camadas de complexidade. A superfície de ataque está em constante expansão. Existem infinitos alertas. As ferramentas de segurança são incompatíveis. Com tanto atrito entre as pessoas e a tecnologia, não é de admirar que a eficácia da segurança esteja estagnada e o tempo médio de permanência permaneça em torno de 280 dias[1].

Esse novo normal precisa de resiliência de segurança – a capacidade de proteger a integridade de todos os aspectos dos negócios para que possam resistir a ameaças ou mudanças imprevisíveis e se tornar mais fortes. E a resiliência de segurança exige mais do que o passado ofereceu.

Principais razões para explorar a XDR:

1. Diminuir a fadiga do alerta
2. Aumentar o tempo de detecção
3. Aumentar a visibilidade em todas as ferramentas
4. Obter um melhor contexto de ameaças

Então, o que exatamente é XDR e por que é importante para mim?

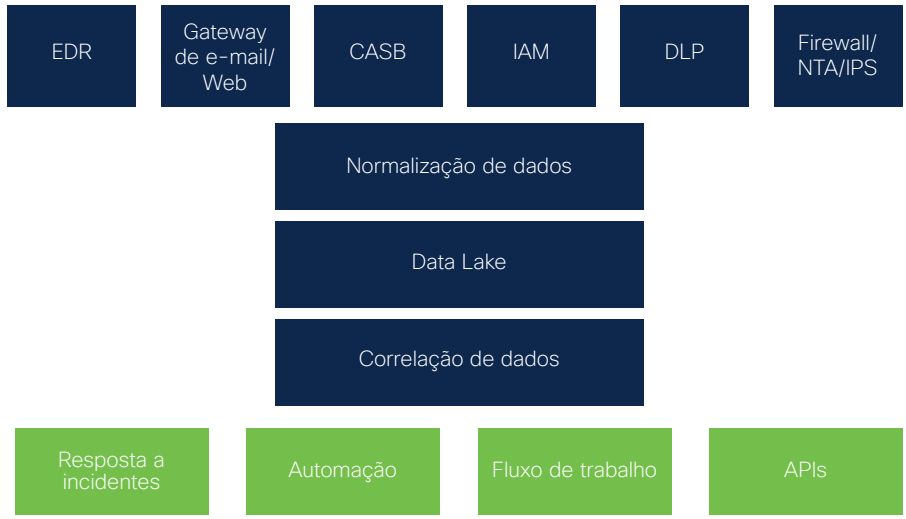
Embora a integração com soluções pontuais de segurança nativas na XDR seja extremamente benéfica, também é fundamental para uma plataforma XDR aproveitar e se conectar facilmente à tecnologia de terceiros atual, fornecendo melhor ROI e contexto mais rico para todas as fontes de dados. Essa é uma mudança de paradigma significativa em relação às estratégias atuais, em que a maior parte da detecção e da resposta é feita dentro de silos de produtos individuais e equipes. A unidade oferecida pela XDR afeta várias áreas importantes para todas as equipes de segurança:

Primeiro, ela agrega valor rápido às equipes com pouca ou nenhuma calibração. Para as equipes que já trabalharam na configuração de SIEMs ou SOAR, as plataformas XDR se baseiam nesses benefícios.

Em segundo lugar, ela resolve a fadiga de alerta que assola tantas equipes, à medida que a plataforma agrega e correlaciona todos os eventos diferentes causados pela mesma violação em incidentes.

Em terceiro lugar, ela oferece elementos de automação e orquestração prontos para uso que ajudam as equipes a eliminar tarefas rotineiras de suas atividades diárias.

Arquitetura conceitual de XDR



1. Pesquisa do PonemonInstitute apresentada no Cost of a Data Breach Report 2020 da IBM

cisco SECURE

Cinco elementos-chave de XDR que deram certo

1 Telemetria coordenada de qualquer lugar no ambiente

A amplitude de visibilidade e a profundidade de insights devem ser fundamentais para a XDR. No momento, os fornecedores estão posicionando seus produtos atuais como componentes importantes na XDR. Mas o verdadeiro XDR deve unir não apenas os dados, mas também a telemetria da mais ampla variedade de categorias de controle de segurança, repositórios de dados e fornecedores de inteligência de ameaças para determinar a probabilidade de intenção mal-intencionada. Com a XDR, as empresas podem fechar as lacunas e obter uma defesa abrangente em todo o ecossistema com uma plataforma aberta e integrada em todo o campus, data center, nuvem e borda da nuvem. Com o rico contexto extraído de cada uma dessas soluções integradas dentro da XDR, você pode encontrar vulnerabilidades e corrigi-las com mais rapidez.

Principais funções	Perguntas a serem feitas
Informações completas do ambiente	Como a solução me oferece mais do que apenas visibilidade da minha rede?
Telemetria acionável	Você está usando um data lake para fornecer informações ou algo que ofereça uma telemetria mais impactante?
Fontes de dados confiáveis	Como a solução garante que estou obtendo contexto em todos os endpoints, dispositivos e tráfego que entram e saem da minha rede?

2 Aproveite a funcionalidade de detecção de seus investimentos atuais, independentemente do fornecedor

Embora a Gartner mencione componentes proprietários na definição de XDR, é fundamental que uma solução de XDR seja desenvolvida com uma abordagem de plataforma aberta que se conecte facilmente à tecnologia de terceiros. Cada componente da pilha de segurança tem elementos de detecção exclusivos – detecção de IoC, aprendizado de máquina, análise comportamental etc. – que se tornam mais eficientes quando usados juntos. Sinais fracos de silos se tornam fortes sinais agregados. O trabalho conjunto de detecção é fundamental para o XDR, portanto, verifique se a plataforma escolhida funciona com toda a pilha.

Principais funções	Perguntas a serem feitas
Aproveite suas soluções	Quantos dos meus investimentos atuais a abordagem de XDR pode aproveitar?
Agnosticismo do fornecedor	Qual é a diferença entre as suas tecnologias de detecção e as outras existentes no mercado?
Insere análises de terceiros	Quais das suas soluções têm integrações prontas para o uso?

3 Contexto unificado de fontes confiáveis de verdade que oferecem suporte a respostas rápidas e precisas

A unificação de insights da rede, do endpoint e do e-mail (para citar alguns) fornece uma compreensão mais precisa do que aconteceu, como progrediu e quais etapas precisam ser tomadas para corrigir a ameaça. O XDR eficaz requer resposta nativa e recursos de correção, como isolar um host ou excluir um e-mail mal-intencionado de todas as caixas de entrada. Idealmente, essas ações seriam possíveis com apenas um ou dois cliques. A XDR também deve facilitar a criação de ações de resposta personalizadas para que as equipes possam desenvolver a segurança com o passar do tempo.

Principais funções	Perguntas a serem feitas
Inteligência orientada por contexto	Posso usar a XDR para entender o impacto de uma ameaça, o escopo da violação e realizar ações de um único clique em uma interface?
Várias fontes de verdade	Que tipo de inteligência de ameaças está alimentando sua detecção e de onde vem essa inteligência?
Melhore o MTTD	Como você valida as fontes de dados que você usa em sua solução?

4 Oportunidades contínuas de automação e orquestração para problemas de escala de máquina

Seguir fluxos de trabalho complicados, manuais e desatualizados expõe sua empresa a ameaças e erros humanos. A plataforma XDR certa terá recursos eficientes de orquestração e automação e tornará as tarefas de segurança repetitivas mais fáceis e mais eficientes, sem uma enorme curva de aprendizado para começar a funcionar. A automação de fluxos de trabalho essenciais ajuda a equipe a responder a alertas com mais rapidez, deixando mais tempo e energia para tarefas essenciais, como a busca de ameaças.

Principais funções	Perguntas a serem feitas
Mais automação	Para as integrações de terceiros, as alterações de API dos fornecedores interrompem os scripts de automação?
Veja através do ruído de segurança	Como você pode me ajudar a orquestrar e automatizar os fluxos de trabalho em minhas soluções atuais?
Supere as limitações de escala humana	Como sua solução oferece suporte ao monitoramento de entrada e saída de cargas de trabalho na nuvem?

5 Um único ponto de vista investigativo que simplifica o isolamento e a correção

A XDR deve expandir as ferramentas essenciais no kit de uma equipe de resposta a incidentes, fornecendo visibilidade da telemetria adicional além do endpoint. Um único console permite correção direta, acesso à inteligência de ameaças e ferramentas para fornecer uma visão unificada de um alerta. Além disso, o XDR que facilita a busca de ameaças por meio de modelos como MITER ATT e CK tornará a busca de ameaças orientada por hipóteses acessível para quem é novo no processo, além de tornar mais fácil prever o que está por vir.

Principais funções	Perguntas a serem feitas
Melhora o MTTR	Onde sua solução ajuda e/ou acelera a correção?
Permite mais busca de ameaças	Como sua solução ajuda minha equipe nos esforços de busca de ameaças?

Seguindo em frente com o XDR

Recomendamos trabalhar com as partes interessadas da XDR para determinar qual estratégia de XDR é ideal para você. Garanta que os possíveis fornecedores estejam priorizando a automação e a integração.

Comece com essas perguntas, mas certifique-se de entender as várias funções e requisitos de sua pilha atual para que você possa alcançar resultados mensuráveis e melhorar o ROI.

1. A oferta de XDR abrange detecção e resposta de rede e outras camadas de segurança, como e-mail, nuvem e firewall?
2. Como você me ajudará a tomar medidas de segurança melhores e mais fundamentadas?
3. Como a XDR me ajuda a automatizar o bloqueio ou a correção?
4. Quais das suas soluções têm integrações prontas para uso?
5. Como a abordagem de XDR se conecta a outras iniciativas de segurança, como SASE ou Zero Trust?

cisco SECURE

XDR + Resiliência em segurança

Hoje, a incerteza é uma garantia, desde as operações até as finanças e a cadeia de fornecimento. As empresas estão investindo em resiliência: a capacidade de resistir a choques imprevistos e sair mais forte. Mas esses investimentos se tornam insuficientes sem uma peça na resiliência em segurança.

As 5 dimensões da resiliência em segurança:

1. Ativa bilhões de sinais em todo o ecossistema
2. Prevê o próximo passo por meio da inteligência compartilhada
3. Prioriza alertas com análise de contexto baseada em risco
4. Elimina as lacunas em todo o ecossistema com integrações
5. Fica mais forte por meio de orquestração e automação

A plataforma XDR certa oferece em cada uma dessas dimensões. E apenas a Cisco cumpre a promessa da XDR hoje, por meio de contexto unificado, detecções correlacionadas e respostas mais rápidas.

SecureX, nossa plataforma de segurança integrada, é um benefício em todos os produtos de segurança da Cisco e se integra facilmente a soluções em seu ambiente usando APIs abertas. Essa camada unificada de detecção e resposta correlaciona a telemetria de todos os pontos de controle em um único ponto de vista investigativo e torna a priorização e a execução de ações muito mais simples. Além disso, a orquestração integrada permite automatizar respostas e transferir tarefas de rotina para liberar as equipes para tarefas mais proativas, como a busca de ameaças.

Chega de correr sem sair do lugar – é hora de avançar.

Para saber mais sobre a abordagem da Cisco para XDR, entre em contato com seu representante de vendas hoje mesmo!

Sede – Américas
Cisco Systems, Inc.
San Jose, CA

Sede – Região da Ásia Pacífico
Cisco Systems (USA), Pte. Ltd.
Cingapura

Sedes da Europa
Cisco Systems International BV Amsterdã,
Países Baixos

cisco SECURE

Planilha de validação de fornecedor XDR

Use este formato de tabela e as perguntas fornecidas anteriormente neste documento para se preparar para conversas com fornecedores de XDR. Escolha de 8 a 10 perguntas que sejam mais relevantes para o seu ambiente e copie/cole-as abaixo.

Perguntas/observações	Respostas convincentes
Pergunta:	
Observações:	
Pergunta:	
Observações:	
Pergunta:	
Observações:	
Pergunta:	
Observações:	
Pergunta:	
Observações:	
Pergunta:	
Observações:	
Pergunta:	
Observações:	
Pergunta:	
Observações:	
Pergunta:	
Observações:	
Pergunta:	
Observações:	


CISCO
SECURE