XDR VERSUS SIEM

ISSO É XDR

O QUE É ISSO?

XDR é um novo acrônimo e significa Extended Detection and Response. É considerada a evolução das soluções existentes de detecção e resposta a ameaças.

POR QUE DEVERIA ME IMPORTAR?

Ele aplica medidas proativas ao fornece visibilidade de dados em componentes de endpoint, rede e sistema em combinação com análises e automação.

É ASSIM QUE FUNCIONA

Ao coletar e analisar dados de várias fontes, as soluções XDR são capazes de validar melhor os alertas, reduzindo assim os falsos positivos e aumentando a confiabilidade. Isso ajuda a reduzir o tempo que você pode perder com alertas imprecisos.

PARA QUEM É ISSO?

O XDR ajuda as equipes de segurança a lidar com incidentes centralizando, normalizando e correlacionando dados de segurança de várias fontes.

QUANDO É QUE FAZ SENTIDO?

Se seus objetivos são aumentar a precisão da detecção, correlacionando a intensidade da ameaça e os sinais em várias soluções de segurança, e maior eficiência e produtividade das operações de segurança, então o XDR é para você.

ESSA É A DIFERENÇA

FATO 1

XDR é um sistema que fornece proteção coordenada em tempo real, com um foco profundo na resposta a incidentes.

FATO 2

O SIEM coleta dados e oferece uma visão de todo o ambiente para detectar, investigar e responder adequadamente.

Créditos

Este pôster foi criado por Patrick em colaboração com André Ruschel.

Saiba mais sobre a solução XDR e SIEM da Microsoft em aka.ms/SIEMandXDR

AFRAIT

ISSO É SIEM

O QUE É ISSO?

SIEM é outro acrônimo e significa informações de segurança e gerenciamento de eventos para ajudá-lo a obter percepções de seu ambiente.

POR QUE DEVERIA ME IMPORTAR?

O principal objetivo dos SIEM é coletar e agregar dados, como logs de diferentes ferramentas e aplicativos para atividade, visibilidade e investigação de incidentes.

É ASSIM QUE FUNCIONA

Em sua essência, o SIEM é um agregador de dados, pesquisa e sistema de relatórios. O SIEM reúne imensas quantidades de dados de todo o ambiente de rede, consolida e torna esses dados acessíveis para humanos.

PARA QUEM É ISSO?

O SIEM ajuda a equipe de TI a identificar, revisar e responder às violações de segurança com mais rapidez e facilidade, pois oferece mais insights de diferentes fontes.

QUANDO É QUE FAZ SENTIDO?

Se o seu objetivo é registrar e gerenciar os registros de logs, então as informações de segurança e o gerenciamento de eventos são para você. Outro caso de uso é ajudar no que diz respeito à conformidade com regulamentos como HIPAA, GDPR e LGPD.