Resumo da solução

Sophos NDR

Visibilidade crítica profunda da sua rede

O Sophos Network Detection and Response está disponível com o Sophos MDR e o Sophos XDR para detectar atividades suspeitas no interior da sua rede, que endpoints e firewalls não conseguem ver. O Sophos NDR analisa continuamente o tráfego em busca de padrões suspeitos, como atividades incomuns que se originam em dispositivos desconhecidos ou não gerenciados, ativos patrimoniais ilegítimos, servidores de C2 de dia zero e movimentações inesperadas de dados.

Casos de uso

1 | VISIBILIDADE CRÍTICA

Resultado desejado: Obter visibilidade crítica das atividades na rede que outros produtos não conseguem ver

Solução: O NDR trabalha em conjunto com seus endpoints e firewalls gerenciados para monitorar a atividade da rede em busca de padrões de comportamento suspeito e malicioso que seus endpoints e firewalls não conseguem ver. Ele detecta fluxos anormais de tráfego de dispositivos IoT e sistemas não gerenciados, dispositivos ilegítimos, ameaças internas, ataques de dia zero nunca antes vistos e padrões incomuns nas profundezas da rede.

2 | DETECÇÃO ANTECIPADA

Resultado desejado: Cinco mecanismos independentes de detecção trabalhando em tempo real para identificar ameaças mais cedo.

Solução: O Sophos NDR inclui cinco mecanismos independentes de detecção que trabalham em conjunto em tempo real para detectar tráfego suspeito e mal-intencionado rapidamente, com tecnologias como Deep Learning, inspeção profunda de pacotes, análise de carga criptografada, análise de nome de domínio e ferramentas analíticas poderosas. Nossa análise exclusiva fornece apenas alertas de alto valor, que garantem que você não fique perdido em meio a ruído excessivo.

3 | RESPOSTA AUTOMÁTICA

Resultado desejado: Interromper ameaças e adversários ativos automaticamente antes que causem danos

Solução: A automação entre os produtos Sophos NDR, Sophos XDR, Sophos MDR e Sophos Firewall oferece resposta imediata para bloquear ameaças ativas antes que causem danos concretos. Quando o Sophos NDR identifica um indicador de comprometimento, uma ameaça ativa ou um adversário, analistas são alertados imediatamente e podem enviar um feed de ameaças ao Sophos Firewall instantaneamente para disparar uma resposta automatizada e isolar o host comprometido.

4 | GERENCIADO A PARTIR DE UM ÚNICO PAINEL

Resultado desejado: Gastar menos tempo administrando a segurança da sua rede

Solução: Com o Sophos Central, você trabalha com uma única plataforma de gerenciamento para todos os seus produtos Sophos, incluindo NDR, XDR, endpoints, firewalls e outros mais. Você tem acesso a ferramentas poderosas que utilizam a excelência de dados de nosso Data Lake na caça, gerenciamento de respostas antecipadas e registro e auditoria de ameaças entre todos os produtos. Em resumo: você gasta menos tempo administrando a segurança da sua rede.

Identifique ativos ilegítimos e desprotegidos

Desvende movimentos incomuns de dados e ameaças internas

Detecte ataques de dia zero nunca antes vistos

Saiba mais e faça uma avaliação Sophos NDR
sophos.com/ndr

2023-11-06 DS-PTBR (MP)

SOPHOS