RESUMO DA SOLUÇÃO

Sophos ITDR

Identity Threat Detection and Response

O Sophos Identity Threat Detection and Response (ITDR) identifica e relata ameaças que burlam os controles de segurança de identidade tradicionais. Totalmente integrado ao Sophos Extended Detection and Response (XDR) e ao Sophos Managed Detection and Response (MDR), o Sophos ITDR ajuda você a melhorar a postura de segurança da sua organização, monitorar continuamente o seu ambiente em busca de erros de configuração de identidade e riscos, e oferecer inteligência de dark web sobre credenciais comprometidas.

Casos de uso

1 | PROTEGER CONTRA AMEAÇAS DE IDENTIDADE

Resultado desejado: Neutralizar ataques baseados em identidade antes que possam impactar os seus negócios.

Solução: 90% das organizações enfrentaram uma violação de identidade no último ano.[1] O Sophos ITDR permite identificar proativamente ameaças sofisticadas e proteger-se contra 100% das técnicas de acesso a credenciais MITRE ATT&CK[2] no início da cadeia de ataque e responder com velocidade e precisão. Os analistas experientes do Sophos MDR podem investigar atividades de alto risco e adotar medidas imediatas por você, incluindo desabilitar um usuário, forçar a redefinição de senha, bloquear uma conta, revogar sessões e mais.

2 | DIMINUIR SUA SUPERFÍCIE DE ATAQUE DE IDENTIDADE

Resultado desejado: Identificar e corrigir erros de configuração e lacunas de segurança baseadas em identidade.

Solução: 95% dos ambientes do Microsoft Entra ID apresentam um erro crítico de configuração.[3] Se não verificado, os criminosos cibernéticos podem utilizar essas exposições para escalonar privilégios e realizar ataques baseados em identidade. O Sophos ITDR faz a varredura do seu ambiente Entra ID continuamente para identificar rapidamente erros de configuração e lacunas de segurança e oferecer recomendações para correção.

3 | DESCOBRIR CREDENCIAIS VAZADAS OU ROUBADAS

Resultado desejado: Minimizar o risco do uso de credenciais expostas para realizar um ataque.

Solução: A identidade continua a ser uma vetor de acesso para ransomwares, e a Sophos tem observado que o número de credenciais roubadas postas à venda em um dos maiores marketplaces da dark web mais que dobrou só no último ano.[4] O Sophos ITDR monitora a dark web e os bancos de dados de violações e o alerta quando ocorre a exposição de credenciais para diminuir o risco de serem usadas em ataques futuros.

4 | IDENTIFICAR COMPORTAMENTOS ARRISCADOS DE USUÁRIOS

Resultado desejado: Entender e resolver o comportamento de usuários de alto risco para proteger o seu negócio.

Solução: Ao monitorar padrões de login incomuns e atividades anormais do usuário, você pode reduzir significativamente os riscos à sua segurança cibernética e proteger os seus valiosos recursos. O Sophos ITDR identifica comportamentos de risco que agentes mal-intencionados poderiam explorar, ou que poderiam indicar que as credenciais de um usuário foram comprometidas, e oferecer detalhes dos usuários da sua organização que estiverem envolvidos em recentes alertas de segurança da Sophos.

Selo 2025 Gartner® Peer Insights™ "Customers' Choice" em Detecção e Resposta Estendidas.

Líder nos Relatórios G2 Overall Grid® em MDR e XDR de acordo com avaliações e classificações de clientes.

Excelente desempenho nas avaliações MITRE ATT&CK® em Serviços Gerenciados e Produtos para Enterprise.

Saiba mais:
sophos.com/ITDR

[1] Estudo de 2024, Identity Defined Security Alliance (IDSA). | [2] Baseado nos recursos de detecção da Sophos mapeados à estrutura MITRE ATT&CK.
[3] Dados reunidos de milhares de engajamentos de resposta a incidentes conduzidos pela Sophos. | [4] Dados do Sophos X-Ops Counter Threat Unit (CTU). Junho de 2024 – Junho de 2025.

Gartner, Gartner Peer Insights 'Voice of the Customer': Extended Detection and Response, Peer Contributors, 23 de maio de 2025. O conteúdo do Gartner Peer Insights consiste em opiniões de usuários finais individuais baseadas em suas próprias experiências e não deve ser interpretado como uma declaração de fato nem como representação da visão da Gartner ou de suas afiliadas. A Gartner não endossa fornecedores, produtos ou serviços representados neste conteúdo nem estabelece qualquer garantia, expressa ou implícita, em respeito a este conteúdo, sua precisão ou completude, incluindo garantias de comercialização ou de um propósito de uso específico. A GARTNER é uma marca registrada e marca de serviço da Gartner, Inc. e/ou de suas afiliadas nos EUA e internacionalmente, e a PEER INSIGHTS é uma marca registrada da Gartner, Inc. e/ou de suas afiliadas utilizada aqui com permissão. Todos os direitos reservados.

2025-09-16 SB-PTBR (MP)