Lösungsbeschreibung

Sophos NDR

Transparenz bis tief ins Netzwerk

Sophos Network Detection and Response ist sowohl für Sophos MDR als auch für Sophos XDR erhältlich. Die Lösung erkennt tief im Netzwerk schädliche Netzwerkaktivitäten, die Endpoints und Firewalls nicht sehen können. Sophos NDR analysiert den Datenverkehr kontinuierlich auf verdächtige Muster – u.a. auf ungewöhnliche Aktivitäten, die von unbekannten oder nicht verwalteten Geräten ausgehen, nicht autorisierte Assets, neue Zero-Day-C2-Server und unerwartete Datenbewegungen.

Anwendungsfälle

1 | MEHR TRANSPARENZ

Gewünschtes Ergebnis: Wichtige Einblicke in Netzwerkaktivitäten erhalten, die von anderen Produkten nicht erkannt werden

Lösung: Sophos NDR überwacht in Zusammenarbeit mit Ihren verwalteten Endpoints und Firewalls Netzwerkaktivitäten und erkennt verdächtige und schädliche Muster, die Ihre Endpoints und Firewalls nicht sehen können. Sophos NDR erkennt ungewöhnliche Datenverkehrsflüsse von nicht verwalteten Systemen und IoT-Geräten, nicht autorisierte Assets, interne Bedrohungen, bisher unbekannte Zero-Day-Angriffe und ungewöhnliche Muster tief im Netzwerk.

2 | FRÜHZEITIGE ERKENNUNG

Gewünschtes Ergebnis: Hochwertige Analyse-Ergebnisse erhalten, um Bedrohungen schneller zu erkennen

Lösung: Sophos NDR nutzt fünf unabhängige Erkennungs-Engines, die in Echtzeit zusammenarbeiten, um verdächtigen und schädlichen Datenverkehr schnell zu erkennen. Dafür nutzen sie Technologien wie Deep Learning, Deep Packet Inspection, Analyse verschlüsselter Payloads, Domänennamen-Analyse und analytische Informationssysteme. Durch dieses Zusammenspiel erhalten Sie nur hochwertige Warnmeldungen und müssen sich nicht durch eine Flut von Fehlalarmen kämpfen.

3 | AUTOMATISCHE REAKTION

Gewünschtes Ergebnis: Aktive Angreifer und Bedrohungen automatisch stoppen, bevor sie sich ausbreiten können

Lösung: Die produktübergreifende Automatisierung zwischen Sophos NDR, Sophos XDR, Sophos MDR und Sophos Firewall ermöglicht sofortige Reaktionsmaßnahmen zum Stoppen aktiver Bedrohungen. Wenn Sophos NDR einen Indicator of Compromise, eine aktive Bedrohung oder einen Angreifer erkennt, werden die Analysten sofort benachrichtigt. So können sie direkt einen Bedrohungsfeed an die Sophos Firewall senden, um automatische Reaktionsmaßnahmen zum Isolieren des kompromittierten Hosts einzuleiten.

4 | EINFACHE VERWALTUNG

Gewünschtes Ergebnis: Weniger Zeit für die Verwaltung Ihrer Netzwerksicherheit aufwenden

Lösung: Mit Sophos Central erhalten Sie eine zentrale Cloud-Management-Plattform für all Ihre Sophos-Produkte, einschließlich NDR, XDR, Endpoints, Firewalls etc. Sie erhalten umfassende, leistungsstarke Tools, die unseren Deep Data Lake nutzen, um ein produktübergreifendes Threat Hunting durchzuführen. Damit können Sie frühzeitig Reaktionsmaßnahmen ergreifen und erhalten darüber hinaus Funktionen zur effektiven Reporting- und Auditing-Verwaltung. So benötigen Sie deutlich weniger Zeit für die Verwaltung Ihrer Netzwerksicherheit.

Identifizieren Sie ungeschützte und nicht autorisierte Assets

Enttarnen Sie ungewöhnliche Datenbewegungen und interne Bedrohungen

Erkennen Sie bislang unbekannte Zero-Day-Angriffe

Mehr erfahren und Sophos NDR testen
sophos.de/ndr

SOPHOS

2023-11-06 DS-DE (MP)