Sophos Network Detection and Response

Erkennt verdächtiges Verhalten überall – nicht nur auf Endpoints

Was ist Sophos NDR?

Sophos Network Detection and Response (NDR) nutzt Machine Learning (ML), erweiterte Analysen und regelbasierte Abgleichtechniken, um den Netzwerkverkehr zu überwachen und verdächtige Aktivitäten zu erkennen.

Beim gemeinsamen Einsatz mit Sophos MDR und in Kombination mit anderen Sicherheitstelemetrien liefert NDR ein genaueres Bild des gesamten Angriffspfads und ermöglicht so eine schnellere, umfassende Reaktion auf Cyberbedrohungen.

Verhaltensweisen im Netzwerkverkehr

Sophos NDR überwacht den Netzwerkverkehr auf folgende Verhaltensweisen:

- Verbindungen von unbekannten Geräten
- Während einer Remote-Sitzung hochgeladene Daten
- Verstärkte Nutzung von Dateien mit proprietären Daten
- Von Malware-Familien generierte Netzwerksitzungen

Verhaltensweisen verknüpfen Risiken und Bedrohungen

Versierte Angreifer bleiben unerkannt, müssen sich jedoch im Netzwerk fortbewegen, um einen Cyberangriff durchzuführen. Sophos NDR erkennt:

- Ungeschützte Geräte – erkennt legitime Geräte, die nicht geschützt sind und als Eintrittspunkte missbraucht werden könnten
- IoT- und OT-Sensoren – überwacht Datenbewegungen von und zu ungeschützten IoT/OT-Geräten
- Rogue Assets – ermittelt nicht autorisierte, potenziell schädliche Geräte, die über das Netzwerk kommunizieren
- Zero-Day-Angriffe – erkennt Command-and-Control-(C2)-Versuche von Servern auf Basis von Mustern in Sitzungspaketen
- Interne Bedrohungen – gibt Einblick in den Netzwerkverkehr und „normale" Datenbewegungen innerhalb eines Unternehmens/einer Einrichtung

Fragen an potenzielle NDR-Kunden

- Befinden sich in Ihrer Umgebung derzeit Geräte ohne Endpoint-Schutz, z. B. Geräte in einem Labor, POS-Terminals oder IOT-Geräte?
- Überwachen Sie den Netzwerkverkehr hinter Ihrer Firewall?
- Wie überwachen Sie das Verhalten interner Benutzer?
- Wie überwachen Sie „normale" Datenbewegungen?
- Führen Sie regelmäßig eine Bestandsaufnahme der Assets in Ihrem Netzwerk durch?
- Können Sie neue oder nicht autorisierte Systeme in Ihrem Netzwerk erkennen?
- Haben Sie Einblick in den verschlüsselten Datenverkehr in Ihrem Netzwerk?

Was unterscheidet Sophos NDR von anderen NDR-Lösungen?

Sophos NDR ist eine virtuelle Appliance, die eine Verbindung zur TAP/SPAN-Erfassung herstellt und Netzwerkflüsse analysiert. Sophos NDR bietet:

- 5 unabhängige Echtzeit-Erkennungs-Engines
- Machine-Learning-Technologie, die Malware in verschlüsseltem Datenverkehr erkennt
- Domain Generation Algorithm(DGA)-Erkennung ohne Threat Intelligence
- Risikoanalysen zum Erkennen ungewöhnlicher Datenverkehrsmuster, die analysiert werden sollten
- Warnmeldungen, die im Rahmen von Sophos MDR mit anderen Sicherheits-Telemetriedaten korreliert werden

Als native Sophos MDR-Integration lässt sich Sophos NDR problemlos und störungsfrei einbinden – ohne langwierige Einrichtung oder abweichende Risikobewertungen.

Der Preis für Sophos NDR basiert auf der Gesamtzahl der Benutzer und Server in einem Unternehmen/einer Einrichtung. Die Software für die virtuelle Appliance ist in der Lizenz enthalten.

22-11-17 DA-DE (DD)

SOPHOS