Überwachung des Netzwerkverkehrs zur schnelleren Erkennung verdächtiger Aktivitäten

Wenn ein Angreifer in Ihrer Umgebung ist, zählt jede Sekunde. Doch allzu oft werden Verteidiger durch begrenzte Sichtbarkeit und Erkenntnisse ausgebremst. Und das wird noch komplizierter, wenn die Sicherheitstools nicht gut zusammenarbeiten.

Die umfangreichsten Daten sind die Grundlage für die präziseste Erkennungsstrategie

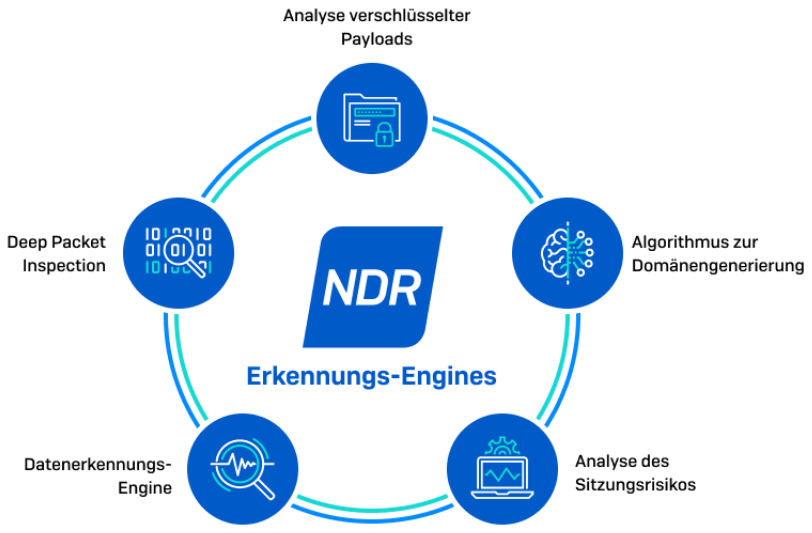
Unternehmen können von einem ganzheitlichen Ansatz zur Erkennung von und Reaktion auf Bedrohungen sowie von schnelleren Möglichkeiten zur Korrelation der ständig wachsenden Datenmenge und -vielfalt profitieren. Je größer die Transparenz und der Kontext, desto präziser ist die Untersuchung von Bedrohungsaktivitäten. Das heißt, wenn Sicherheitstelemetrie zusammengeführt werden kann, ergibt sich ein genaueres Bild des gesamten Angriffspfades.

Als Add-on zu Sophos MDR überwacht die virtuelle Appliance Sophos Network Detection and Response (NDR) den Netzwerkverkehr, um verdächtige Netzwerkströme zu identifizieren. Die Erkennungen werden an den Sophos Data Lake gesendet, ausgewertet und mit einer entsprechenden Risikobewertung versehen, so dass das Sophos Threat Response Team die Fälle untersuchen und überprüfen kann. NDR-Erkennungen können eine Untersuchung interner Host-Verbindungen zu Netzwerkservern auslösen und können auch dazu verwendet werden, die Suche nach Endpoint-Aktivitäten anzureichern, um festzustellen, welche Geräte miteinander kommunizieren.

Ihre Sicherheit braucht Tools, die gut zusammenarbeiten

Sophos NDR ist eine native Sophos MDR-Integration. Es lässt sich problemlos verbinden, erzeugt kein übermäßiges Rauschen oder unpassende Risiko-Scores und benötigt keine Zeit für die Erstellung einer Baseline wie andere Lösungen. In der folgenden Tabelle werden die Funktionen der Detection Engines von Sophos NDR Detection Engines beschrieben.

Sophos NDR wird als virtuelle Appliance bereitgestellt. Nach dem Einsatz authentifiziert sich die Appliance an der Sophos Central Management Console und beginnt mit der Datenübertragung. Der NDR-Status und Erkennungen sind in Sophos Central einsehbar.



SOPHOS

Lösung

Security & Identity

Produkt

Network Detection Response

Funktionen:

Fügen Sie Netzwerkerkennungen zu Sophos MDR hinzu, um verdächtige Netzwerkflüsse zu überwachen, auf die Endpoint-Software nicht zugreifen kann.

Ermöglicht die Untersuchung von Bedrohungen und die Suche nach internen Hostverbindungen zu Netzwerkdiensten und anderen Netzwerkverbindungen

Erkennung von Malware im verschlüsselten Datenverkehr, wo sie oft verborgen bleibt

Einfaches Anzeigen des NDR-Sensorstatus und der Erkennungen in Sophos Zentrale

Sophos NDR Detection Engines und Anwendungsfälle

Detection Engines	Beschreibung
Verschlüsselte Nutzdatenanalyse (EPA)	Erkennung von Zero-Day Command-and-Control (C2)-Servern und neuen Varianten von Malware-Familien auf der Grundlage von Mustern in Bezug auf Sitzungsgröße, -richtung und Intervallzeiten.
Bereichserzeugungsalgorithmen (DGA)	Identifiziert das Vorhandensein einer dynamischen Domain-Generierungstechnologie, die von Malware verwendet wird, um eine Erkennung zu vermeiden.
Deep Packet Inspection (DPI)	Überwacht sowohl verschlüsselten als auch unverschlüsselten Datenverkehr mithilfe bekannter IoCs, um Bedrohungsakteure und TTPs schnell zu identifizieren.
Sitzungsrisiko-Analyse (SRA)	Leistungsstarke Logik-Engine, die Regeln verwendet, die bei einer Vielzahl von sitzungsbasierten Risikofaktoren Alarm schlagen.
Geräteerkennungsmodul (DDE)	Erweiterbare Abfrage-Engine, die ein Deep-Learning-Vorhersagemodell verwendet, um verschlüsselten Datenverkehr auf Muster in nicht zusammenhängenden Netzwerkströmen zu analysieren.

Erkennen Sie verdächtiges Verhalten Über Ihre Endpunkte hinaus

Sophos NDR verwendet unabhängige Threat Detection Engines, um verdächtiges und abnormales Verhalten im Netzwerkverkehr zu erkennen wie:

- Verbindungen von einem unbekannten Gerät
- Daten, die während einer Fernsitzung hochgeladen werden
- Vermehrte Verwendung von proprietären Dateien
- Von Malware-Familien erzeugte Netzwerksitzungen

Mit der Fähigkeit, potenziell schädliche Verhaltensweisen zu erkennen, Sophos NDR identifiziert:

Ungeschützte Geräte - Sophos NDR identifiziert legitime Geräte, die nicht geschützt wurden und die als Einstiegspunkte für Cyberattacken genutzt werden könnten.

Rogue Assets - Sophos NDR überwacht nicht nur den Datenverkehr zu ungeschützten Geräten, sondern identifiziert auch nicht autorisierte Geräte, die über das Netzwerk kommunizieren.

IoT- und OT-Sensoren - Internet of Things (IoT)- und Operational Technology (OT)-Geräte stellen eine Herausforderung für die Bedrohungsüberwachung dar, da viele dieser Geräte keinen Endpoint Protection Agent unterstützen. Sophos NDR überwacht Daten von IoT- und OT-Geräten, um Angreiferaktivitäten zu erkennen.

Zero-Day-Attacken - Sophos NDR verfügt über ein patentiertes Verfahren zur Erkennung von Zero-Day-C2-Servern, die von Angreifern verwendet werden, basierend auf Mustern, die in der Größe und Richtung von Sitzungspaketen sowie in den Interarrival-Zeiten gefunden werden

Insider-Bedrohungen - Sophos NDR bietet Einblick in Netzwerkverkehrsströme und die Datenexfiltration, die für Eingeweihte zunächst "normal" erscheinen.

SOPHOS

Lösung

Security & Identity

Produkt

Network Detection Response

Funktionen:

Fügen Sie Netzwerkerkennungen zu Sophos MDR hinzu, um verdächtige Netzwerkflüsse zu überwachen, auf die Endpoint-Software nicht zugreifen kann.

Ermöglicht die Untersuchung von Bedrohungen und die Suche nach internen Hostverbindungen zu Netzwerkdiensten und anderen Netzwerkverbindungen

Erkennung von Malware im verschlüsselten Datenverkehr, wo sie oft verborgen bleibt

Einfaches Anzeigen des NDR-Sensorstatus und der Erkennungen in Sophos Zentrale