Managed Threat Detection

Ergänzen Sie Ihren vorhandenen Endpoint-Schutz von einem anderen Anbieter mit 24/7 Monitoring und Detection als Fully-Managed-Service

Kompatibel mit anderen Endpoint-Lösungen

Nur wenige Unternehmen haben intern die richtigen Tools, Mitarbeiter und Prozesse, um ihr Sicherheitsprogramm effizient rund um die Uhr zu verwalten. Viele verlassen sich voll und ganz auf ihren automatischen Endpoint-Schutz. Aber was passiert, wenn es Angreifern gelingt, diesen Schutz zu umgehen? Wird die Kompromottierung bemerkt und rechtzeitig reagiert?

Sophos Managed Threat Detection überwacht Umgebungen rund um die Uhr und erkennt Bedrohungen 24/7. So werden auch verdächtige Aktivitäten aufgedeckt, die Ihr Endpoint-Schutz übersehen hat. Der Service ist mit Endpoint-Protection-Produkten von anderen Anbietern kompatibel. Unternehmen können also weiterhin ihren gewohnten Endpoint-Schutz nutzen und erhalten parallel dazu ein Monitoring durch Sophos-Bedrohungsexperten.

Benachrichtigt Sie bei erkannten Bedrohungen

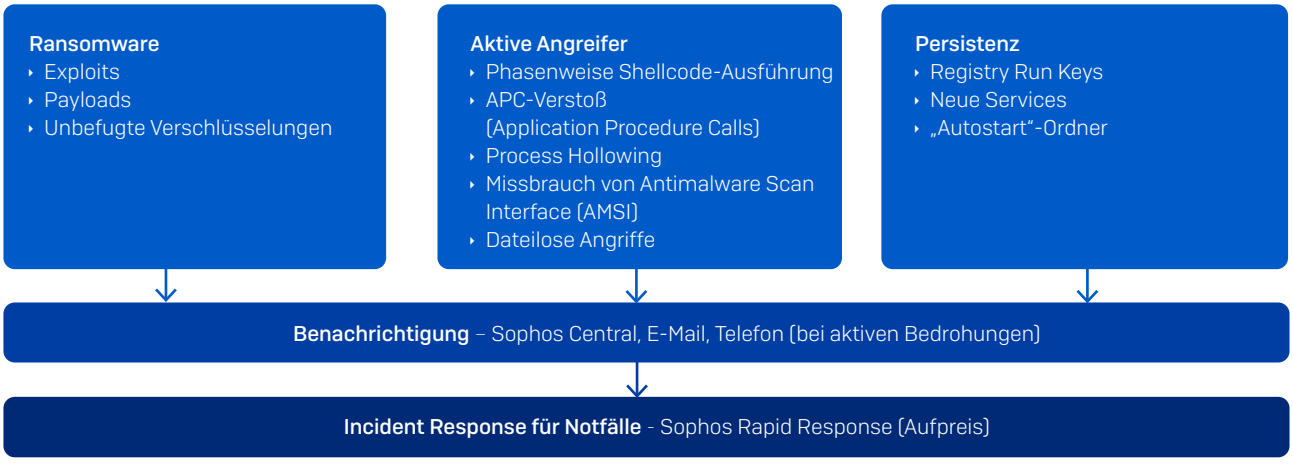
Managed Threat Detection ist in der Reaktions-Option „Benachrichtigung" erhältlich. Kunden erhalten Warnmeldungen, wenn es schwerwiegenden Bedrohungen gelingt, ihre Endpoint-Protection-Lösung zu umgehen. Zu solchen Bedrohungen zählen auch verschiedenste Aktivitäten, die oft im Vorfeld von Ransomware-Angriffen beobachtet werden.

Beispiele:

- Phasenweise ausgeführter Shellcode, der häufig in CobaltStrike Beacon oder Metasploit Meterpreter zu finden ist
- Neue geplante Aufgabe, die $PS ausführt, einschließlich Aktivitäten an Orten, die üblicherweise zur Persistenz von Malware und Hackern verwendet werden (z. B. Registry Runkeys, Dienste, Windows-Systemstart-Elemente)
- Ransomware und Aktivitäten, die andere Schutzprodukte evtl. übersehen

Highlights

- 24/7 Monitoring und Erkennung verdächtiger Aktivitäten
- Kompatibel mit Endpoint-Protection-Produkten anderer Anbieter
- Reaktions-Option „Benachrichtigung"
- Analysten-Validierung aller schwerwiegenden Erkennungen
- Benachrichtigungen mit Empfehlungen für Korrekturmaßnahmen
- Für zusätzliche Incident-Response-Maßnahmen steht Sophos Rapid Response zur Verfügung



SOPHOS

Status-Updates und blitzschnelle Reaktion

Eine klare Kommunikation ist für SecOps-Programme essenziell. Unser „Managed Threat Detection"-Team liefert kontinuierlich wichtige Informationen, u. a. wöchentliche und monatliche Reports, Benachrichtigungen per E-Mail und ein Dashboard mit Infos in Sophos Central.

Kunden erhalten E-Mail-Benachrichtigungen mit Status-Updates zum vorliegenden Fall. Hierzu zählen auch Meldungen, wenn Maßnahmen erforderlich sind und sobald Fälle abgeschlossen wurden. Alle Fälle werden von einem Analysten validiert. Die Benachrichtigungen enthalten eine Fall-Kurzfassung, eine Liste der betroffenen Geräte sowie Empfehlungen für Korrekturmaßnahmen.

Außerdem senden wir Kunden aktuelle Branchennachrichten, in denen die neuesten Erkenntnisse zur Bedrohung, die von Sophos getroffenen Gegenmaßnahmen und die Schutzmöglichkeiten für Kunden erläutert werden.

Wenn wir aktive Bedrohungen in einer Umgebung erkennen, kontaktieren unsere Sophos-Experten den betroffenen Kunden telefonisch. Dadurch wird sichergestellt, dass kritische Informationen sofort weitergegeben werden. Kunden können ihre Kontaktinformationen und Präferenzen für Managed Threat Detection jederzeit in ihrem Sophos Central Dashboard aktualisieren. Das Dashboard bietet außerdem eine Zusammenfassung aller relevanten Managed-Threat-Detection-Aktivitäten, sodass Kunden jederzeit und überall die aktuellsten Informationen erhalten.

Speziell für Kunden, die von Bedrohungen betroffen sind, bieten wir einen weiteren Service: Sophos Rapid Response. Sophos Rapid Response liefert blitzschnelle Soforthilfe beim Erkennen und Beseitigen aktiver Bedrohungen. Unsere „Rapid Response"-Experten können sofort auf Telemetrie- und andere Daten unseres MTR-Teams zugreifen – ein entscheidender Geschwindigkeitsvorteil für Sophos-Kunden.

	Managed Threat Response (MTR) Standard	Managed Threat Response (MTR) Advanced	Managed Threat Detection
Kompatibel mit Endpoint-Schutz anderer Anbieter	✗	✗	✓
24/7 Monitoring	✓	✓	✓
Angriffserkennung	✓	✓	✓
Reports, Dashboard	✓	✓	✓
Bedrohungsbenachrichtigung	✓	✓	✓
Sophos Firewall MTR Connector	✗	✓	✓
Sophos Cloud Optix MTR Connector	✗	✓	✗
Unterstützung mehrerer Betriebssysteme	✓	✓	✗ (nur Win10/2012r2+)
Indizienloses Threat Hunting durch Analysten	✗	✓	✗
Sophos Endpoint Health Check	✓	✓	✗
Schutz in Echtzeit	✓	✓	✗
Eindämmung und Beseitigung	✓	✓	✗
Kommunikation per Telefon	✗ (nur bei aktiven Bedrohungen)	✓	✗ (nur bei aktiven Bedrohungen)

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

21-07-13 DS-DE (MP)