SOPHOS

Managed Threat Response (MTR)

Threat Response aus Expertenhand

Sophos Managed Threat Response (MTR) liefert 24/7 Managed Detection and Response mit aktiver Bekämpfung von Bedrohungen durch ein Expertenteam, als Fully-Managed-Service.

Highlights

- Modernste Managed Detection and Response mit aktiver Bekämpfung von Bedrohungen als Fully-Managed-Service
- Zusammenarbeit mit einem 24/7 verfügbaren Expertenteam, das Maßnahmen zur Eindämmung und Neutralisierung von Bedrohungen ergreift
- Sie entscheiden und kontrollieren, welche Maßnahmen das MTR-Team ergreift und wie auf Vorfälle reagiert wird
- Kombination aus erstklassiger Machine-Learning-Technologie und einem hochqualifizierten Expertenteam
- Sie können zwischen zwei Servicestufen wählen (Standard und Advanced) und erhalten so das für Sie optimale Service-Paket

Unsere Experten werden für Sie aktiv

Nur wenige Unternehmen haben intern die richtigen Tools, Mitarbeiter und Prozesse, um ihr Sicherheitsprogramm effizient rund um die Uhr zu verwalten und sich gleichzeitig proaktiv vor neuen Bedrohungen zu schützen. Das Sophos MTR-Team informiert nicht nur über Angriffe und verdächtiges Verhalten, sondern ergreift für Sie gezielte Maßnahmen, um selbst hochkomplexe Bedrohungen unschädlich zu machen.

Mit Sophos MTR erhalten Sie ein Team von Bedrohungsexperten, das für Sie 24/7 folgende Aufgaben übernimmt:

- Proaktives Aufspüren und Prüfen von potenziellen Bedrohungen und Vorfällen
- Nutzen aller vorliegenden Informationen, um Ausmaß und Schwere von Bedrohungen zu bestimmen
- Anwenden geeigneter Maßnahmen je nach Risiko-Bewertung der Bedrohung
- Einleiten von Maßnahmen zum Stoppen, Eindämmen und Beseitigen von Bedrohungen
- Bereitstellen konkreter Ratschläge, um die Ursache wiederholt auftretender Vorfälle zu bekämpfen

Menschliche Expertise und modernste Technologie

Sophos MTR basiert auf unserer Technologie Intercept X Advanced with EDR und vereint leistungsstarkes Machine Learning mit Expertenanalysen. So erhalten Sie eine optimale Bedrohungssuche und -erkennung, eine fundierte Analyse der Warnmeldungen sowie gezielte Maßnahmen zur schnellen und vollständigen Beseitigung von Bedrohungen. Diese leistungsstarke Kombination aus bewährter Sophos Endpoint Protection, intelligenter EDR und hochqualifizierten Sicherheitsexperten ermöglicht dank maschinengestützter Technologie eine besonders schnelle menschliche Reaktion.

Umfassende Transparenz und Kontrolle

Mit Sophos MTR behalten Sie die Entscheidungsgewalt: Sie kontrollieren, wie und wann potenzielle Vorfälle eskaliert werden, welche Maßnahmen wir ggf. einleiten sollen und wer über die einzelnen Schritte informiert wird. Sophos MTR bietet drei Reaktions-Optionen, d. h. Sie können auswählen, wie unser MTR-Team bei Vorfällen mit Ihnen interagieren soll:

Benachrichtigung: Wir benachrichtigen Sie bei einer erkannten Bedrohung und liefern Detail-Informationen, um Sie bei der Priorisierung und Reaktion zu unterstützen.

Zusammenarbeit: Wir arbeiten mit Ihrem internen Team oder Ihren externen Ansprechpartnern zusammen, um auf erkannte Bedrohungen zu reagieren.

Autorisierung: Wir kümmern uns um erforderliche Maßnahmen zur Eindämmung und Beseitigung von Bedrohungen und informieren Sie über die ergriffenen Maßnahmen.

Die Servicestufen von Sophos MTR

Wir bieten Sophos MTR in zwei Servicestufen an: Standard und Advanced. So können Unternehmen das für sie optimale Service-Angebot auswählen. Unabhängig von der gewählten Servicestufe können Unternehmen zwischen drei Reaktions-Optionen wählen (Benachrichtigung, Zusammenarbeit oder Autorisierung).

Sophos MTR: Standard

24/7 indizienbasierte Bedrohungssuche

Bestätigte schädliche Artefakte und Aktivitäten (starke Signale) werden automatisch blockiert oder beendet. So können die Bedrohungsexperten ihre Suche auf Bedrohungen konzentrieren, für die Indizien vorliegen. Bei dieser Art der Bedrohungssuche werden kausale und angrenzende Ereignisse (schwache Signale) aggregiert und analysiert, um neue „Indicators of Attack (IoA)" und „Indicators of Compromise (IoC)" zu enttarnen, die bislang nicht erkannt werden konnten.

Security Health Check

Sorgen Sie dafür, dass Ihre Sophos-Central-Produkte – allen voran Intercept X Advanced with EDR – stets mit maximaler Performance arbeiten, indem Sie proaktive Untersuchungen Ihrer Betriebsbedingungen und empfohlene Konfigurations-Verbesserungen durchführen.

Aktivitätsreports

Zusammenfassungen der Aktivitäten jedes Falls ermöglichen eine Priorisierung und Kommunikation. So weiß Ihr Team, welche Bedrohungen erkannt und welche Reaktionsmaßnahmen in den jeweiligen Reporting-Zeiträumen ergriffen wurden.

Angriffserkennung

Die meisten erfolgreichen Angriffe beruhen auf der Ausführung eines Prozesses, der für Überwachungstools seriös erscheinen kann. Mithilfe selbst entwickelter Analyseverfahren ermittelt unser Team den Unterschied zwischen seriösem Verhalten und den Taktiken, Techniken und Prozessen (TTPs) von Angreifern.

Sophos MTR: Advanced *Alle Funktionen der „Standard"-Version, plus:*

24/7 indizienlose Bedrohungssuche

Mithilfe von Data Science, Threat Intelligence und der Intuition erfahrener Bedrohungsexperten kombinieren wir verschiedene Informationen (Ihr Unternehmensprofil, hochwertige Assets und Benutzer mit hohem Risiko), um das Verhalten von Angreifern vorherzusagen und neue Angriffsindikatoren (IoA) zu identifizieren.

Optimierte Telemetriedaten

Bedrohungsanalysen werden um Telemetriedaten von anderen Sophos-Central-Produkten ergänzt, die über die Endpoint-Ebene hinaus ein Gesamtbild der Angriffsaktivitäten liefern.

Proaktive Verbesserung des Sicherheitsstatus

Verbessern Sie Ihren Sicherheitsstatus und Ihre Abwehr proaktiv: Sie erhalten von uns Hilfestellung zur Behebung von Konfigurations- und Architektur-Schwachstellen, die sich negativ auf Ihre gesamte Sicherheit auswirken.

Dedizierter Ansprechpartner

Bei Bestätigung eines Vorfalls wird Ihnen ein dedizierter Ansprechpartner zugewiesen, der direkt mit Ihren internen und externen Mitarbeitern vor Ort zusammenarbeitet, bis die aktive Bedrohung neutralisiert wurde.

Direkter Telefon-Support

Ihr Team kann unser Security Operations Center (SOC) direkt telefonisch kontaktieren. Unser MTR-Team ist 24/7 erreichbar und wird von Support-Teams unterstützt, die weltweit auf 26 Standorte verteilt sind.

Asset-Erkennung

Von Asset-Informationen über Betriebssystem-Versionen, Anwendungen und Schwachstellen bis hin zur Identifizierung verwalteter und nicht verwalteter Assets: Wir liefern Ihnen wertvolle Detail-Informationen bei der Einschätzung von Folgen, während Bedrohungssuchen und als Teil proaktiver Empfehlungen zur Verbesserung des Sicherheitsstatus.

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

2019-09-17 DS (GH)

SOPHOS