Sophos Managed Detection and Response

Threat Response aus Expertenhand

Sophos Managed Detection and Response (MDR) bietet 24/7 Managed Detection and Response mit Threat Hunting durch ein Expertenteam, als Fully-Managed-Service.

Cybersecurity als Service – rund um die Uhr

Den meisten Unternehmen fehlen die internen Tools, Fachkräfte und Prozesse, um Cyberbedrohungen effektiv abzuwehren und ihr Sicherheitsprogramm effizient zu verwalten. Sophos MDR bietet Threat Detection and Response 24/7/365. Wir sind rund um die Uhr aktiv und machen hochkomplexe Bedrohungen unschädlich.

Die MDR-Bedrohungsexperten übernehmen folgende Aufgaben:

- Proaktives Aufspüren und Prüfen von potenziellen Bedrohungen und Vorfällen
- Nutzen aller vorliegenden Informationen, um Ausmaß und Schwere von Bedrohungen zu bestimmen
- Liefern von Details zu Kontext und potenziellen Auswirkungen einer 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 MDR basiert auf Sophos XDR und vereint leistungsstarkes Machine Learning mit Expertenanalysen. So erhalten Kunden optimale Unterstützung bei der Bedrohungssuche und -erkennung, der eingehenden Analyse von Warnmeldungen und der gezielten Beseitigung von Bedrohungen. Diese leistungsstarke Kombination aus bewährter Sophos Endpoint Protection, intelligenter XDR und hochqualifizierten Sicherheitsexperten ermöglicht dank maschinengestützter Technologie eine besonders schnelle menschliche Reaktion.

Umfassende Transparenz und Kontrolle

Mit Sophos MDR steuern Sie, wie und wann potenzielle Vorfälle eskaliert werden, welche Reaktionsmaßnahmen getroffen werden und wer in die Kommunikation mit einbezogen wird. Sophos MDR bietet drei Reaktions-Optionen, d. h. Sie können flexibel auswählen, wie Sie bei Vorfällen mit unserem MDR-Team zusammenarbeiten möchten.

Benachrichtigung: Wir informieren Sie in allen Einzelheiten über potenzielle Vorfälle und helfen Ihnen dabei, diese zu priorisieren und entsprechend zu reagieren.

Zusammenarbeit: Wir arbeiten mit Ihrem internen Team oder Ihren externen Ansprechpartnern zusammen, um Reaktionsmaßnahmen einzuleiten.

Autorisierung: Wir dämmen den Vorfall ein, beseitigen alle Spuren und informieren Sie über die von uns getroffenen Maßnahmen.

Highlights

- Modernste Managed Detection and Response mit aktiver Bekämpfung von Bedrohungen als Fully-Managed-Service
- 24/7/365 aktives Expertenteam, das Bedrohungen remote eindämmt und unschädlich macht
- Sie kontrollieren, welche Maßnahmen das MDR-Team für Sie ergreift und wie auf Vorfälle reagiert wird
- Zugriff auf erstklassige Machine-Learning-Technologie und ein hochqualifiziertes Expertenteam
- Sie können zwischen zwei Servicestufen wählen (Standard und Advanced) und erhalten so das für Sie optimale Service-Paket

SOPHOS

Die Servicestufen von Sophos MDR

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

Sophos MDR: Standard

24/7 indizienbasierte Bedrohungssuche

Bestätigte schädliche Artefakte oder Aktivitäten (starke Signale) werden automatisch blockiert oder beendet. So können unsere Bedrohungsexperten indizienbasierte Threat Hunts durchführen, bei denen kausale und angrenzende Ereignisse (schwache Signale) untersucht und analysiert werden, um neue „Indicators of Attack (IoA)" und „Indicators of Compromise (IoC)" zu enttarnen.

Security Health Check

Unsere proaktiven Untersuchungen halten Sie über Ihre Betriebsbedingungen und Konfigurationen auf dem Laufenden. Wir geben Ihnen auch Empfehlungen, wie Sie bei Sophos XDR und anderen Sophos-Central-Produkten die optimale Leistung sicherstellen.

Aktivitätsreports

Wir fassen die Fallaktivitäten zusammen, damit Sie wissen, welche Bedrohungen wir gefunden haben und welche Reaktionsmaßnahmen innerhalb verschiedener Reporting-Zeiträume ergriffen wurden.

Angriffserkennung

Anhand modernster Analyseverfahren unterscheiden wir legitimes Verhalten von cyberkriminellen Taktiken, Techniken und Prozessen (TTPs).

Sophos MDR: Advanced – alle Funktionen der „Standard"-Version, plus:

24/7 indizienlose Bedrohungssuche

Anhand von Data Science und Threat Intelligence sind wir in der Lage, Cyberangriffe vorauszusagen und IOAs zu identifizieren.

Optimierte Telemetriedaten

Um ein vollständiges Bild Ihres Sicherheitsstatus zu erhalten, ergänzen wir unsere Bedrohungsanalysen mit Telemetriedaten von Sophos Central über die Endpoint-Ebene hinaus.

Proaktive Verbesserung des Sicherheitsstatus

Wir geben Ihnen konkrete Empfehlungen zur Verbesserung Ihres Sicherheitsstatus.

Dedizierter Ansprechpartner

Sie erhalten einen dedizierten Ansprechpartner, der mit Ihrem internen Team und externen Partnern zusammenarbeitet, sobald wir einen Vorfall identifiziert haben. Dieser betreut Sie, bis der Vorfall behoben ist.

Direkter Telefon-Support

Ihr Team kann unser Security Operations Center (SOC) direkt telefonisch kontaktieren. Unser MDR-Team ist 24/7/365 erreichbar und wird von Support-Teams unterstützt, die weltweit auf 26 Standorte verteilt sind.

Asset-Erkennung

Wir geben Ihnen detaillierte Informationen zu Ihren verwalteten und nicht verwalteten Ressourcen und dazu, wie Sie diese schützen können.

Onboarding Plus Package für MDR-Kunden

Unser Onboarding Plus Package ist ein remote geführter Onboarding-Service für Kunden, die Sophos MDR gekauft haben. Dieser Service umfasst einen dedizierten Ansprechpartner aus dem „Sophos Professional Services"-Team. Ihr Ansprechpartner unterstützt bei Onboarding und Planung, bei Bereitstellung und Training und führt einen Health Check durch, um sicherzustellen, dass Sie den größten Nutzen aus unseren Best-Practice-Empfehlungen ziehen. Onboarding Plus umfasst:

Tag 1 – Implementierung – Planung und Durchführung:

- Projektstart
- Konfiguration von Sophos Central
- Überprüfung der Funktionen von Sophos Central
- Aufbau und Test des Bereitstellungsprozesses
- Unternehmensweite Bereitstellung von Sophos Central

Tag 30 – XDR-Training

- Schulung, in der Sie lernen, wie ein Security Operations Center (SOC) zu denken und zu handeln
- Suche nach IOCs
- Erstellen von Abfragen für zukünftige Analysen

Tag 90 – XDR-Training

- Überprüfen Ihrer aktuellen Sicherheitsrichtlinien und ggf. Aktualisierung
- Bestimmen, mit welchen Funktionen Ihr Cyberschutz ggf. weiter verbessert werden kann
- Erhalt schriftlicher Dokumentation mit Empfehlungen von unserem Health Check

Bei Fragen wenden Sie sich bitte an unser Professional Services Team.

Europa: ProfessionalServicesEmea@Sophos.com

Weitere Informationen unter

sophos.de/mdr

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

22-08-01 DS-DE (DD)

SOPHOS