Sophos XDR

Intercept X Advanced with XDR, Intercept X Advanced for Server with XDR

Intercept X kombiniert leistungsstarke Extended Detection and Response (XDR) mit einzigartiger Endpoint Protection. Nutzen Sie die Funktionen entweder zum Threat Hunting, um aktive Angreifer zu erkennen, oder aber in IT Operations, um sicherzustellen, dass Sicherheitsvorgaben durchgesetzt werden. Bei Problemen können Sie per Remote-Zugriff gezielte Maßnahmen ergreifen. Gehen Sie über die Endpoint-Ebene hinaus und nutzen Sie umfangreiche Daten, u. a. auch von Servern, Firewalls und E-Mails.

Antworten für IT Operations und Threat Hunting

Erhalten Sie schnell Antworten auf geschäftskritische Fragen. Sowohl IT-Administratoren als auch Cybersecurity-Experten können tägliche IT-Operations- und Threat-Hunting-Aufgaben so viel effizienter erledigen und erhalten entscheidenden Mehrwert.

Der beste Schutz als Basis

Intercept X stoppt Sicherheitsverstöße, bevor sie überhaupt beginnen können. Durch dieses automatische Stoppen von Vorfällen sind Sie besser geschützt und sparen viel Zeit. Dazu erhalten Sie detaillierte Bedrohungsdaten mit allen nötigen Informationen für schnelle, gezielte Gegenmaßnahmen.

Detaillierte Infos, schnelle Reaktion

Wenn Sie etwas Verdächtiges entdecken, das genauer untersucht werden sollte, können Sie vom Sophos Data Lake direkt zu aktuellen Detail-Informationen und bis zu 90 Tage zurückliegenden Daten über das betroffene Gerät wechseln. Sollte tatsächlich ein Problem vorliegen, können Sie remote auf das Gerät zugreifen und Maßnahmen ergreifen, z. B. die Deinstallation einer Anwendung und Neustart.

Produktübergreifende Transparenz

Sophos XDR geht über die Endpoint- und Server-Ebene hinaus und ermöglicht der Sophos Firewall, Sophos Email und anderen Datenquellen*, wichtige Daten an den Sophos Data Lake zu senden. So erhalten Sie einen umfassenden Überblick über die Umgebung Ihres Unternehmens.

Informationen, selbst wenn das Gerät offline ist

Der Sophos Data Lake, eine zentrale Komponente von XDR, ist ein Cloud-Daten-Repository. Hier lassen sich wichtige Daten von Ihren Endpoints, Servern, Firewalls und E-Mails speichern und abrufen und Geräteinformationen auswerten, selbst wenn das betroffene Geräte offline ist.

In Sekundenschnelle einsatzbereit

Wählen Sie aus einer Library vorformulierter SQL-Abfragen und stellen Sie IT- und Sicherheitsfragen. Auf Wunsch können Sie diese Abfragen auch anpassen oder selbst formulieren. Auch in der Sophos Community werden regelmäßig Abfragen veröffentlicht.

Highlights

- Beantwortung geschäftskritischer IT-Operations- und Threat-Hunting-Fragen
- Entwickelt für IT-Administratoren und Sicherheitsanalysten
- Remote-Bereinigung von Geräten
- Ganzheitlicher Überblick über die IT-Umgebung Ihres Unternehmens und bei Bedarf einfacher Zugriff auf Detail-Informationen
- Einbindung von Endpoint-, Server-, Firewall-, E-Mail- und anderen Datenquellen*
- Sofort einsatzbereite, individuell anpassbare SQL-Abfragen
- Verfügbar für Windows, MacOS* und Linux

** Cloud Optix und Sophos Mobile in Kürze verfügbar*

** XDR-Funktionen in Kürze für macOS verfügbar*

SOPHOS

Use Cases

IT Operations

- Warum läuft ein System langsam?
- Welche Geräte haben bekannte Schwachstellen, unbekannte Dienste oder nicht autorisierte Browser-Erweiterungen?
- Werden Programme ausgeführt, die entfernt werden sollten?
- Nicht verwaltete, Gast- und IoT-Geräte erkennen
- Warum ist die Netzwerkverbindung des Büros langsam? Welche Anwendung ist dafür verantwortlich?
- Für die letzten 30 Tage auf verloren gegangenen oder zerstörten Geräten Verlaufsdaten auf ungewöhnliche Aktivitäten prüfen

Threat Hunting

- Welche Prozesse versuchen, eine Netzwerkverbindung über Nicht-Standardports herzustellen?
- Prozesse anzeigen, die kürzlich Dateien oder Registry-Schlüssel geändert haben
- Erkannte Indicators of Compromise auflisten, die dem MITRE ATT&CK Framework zugeordnet werden
- Analyse auf 30 Tage ausweiten, ohne dass das betroffene Gerät wieder online gehen muss
- Analyse verdächtiger Hosts mithilfe von ATP- und IPS-Erkennungen der Firewall
- E-Mail-Header-Informationen, SHAs und andere IoCs vergleichen, um Datenverkehr zu einer schädlichen Domäne zu identifizieren

Das ist enthalten:

	Extended Detection and Response (XDR)
Produktübergreifende Datenquellen	✓
Produktübergreifende Abfragen	✓
Endpoint- und Server-Abfragen	✓
Sophos Data Lake	✓
Dauer der Datenspeicherung im Data Lake	30 Tage
Dauer der Datenspeicherung auf Festplatte	✓
SQL-Abfragen-Library	✓
Intercept-X-Schutzfunktionen	✓

Detaillierte Infos zur Lizenzierung finden Sie in den License Guides zu Intercept X und Intercept X for Server.

Jetzt kostenfrei testen

Kostenlose 30-Tage-Testversion unter
www.sophos.de/intercept-x

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

21-07-08 DS-DE (PS)

SOPHOS