Sophos XDR

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

Intercept X synchronisiert als branchenweit einzige XDR-Lösung native Endpoint-, Server-, Firewall-, E-Mail-, Cloud- und O365-Sicherheit. Verschaffen Sie sich einen ganzheitlichen Überblick über Ihre Unternehmensumgebung – mit umfangreichen Datensätzen und umfassenden Analysen zur Bedrohungserkennung, -analyse und -reaktion sowohl für dedizierte SOC-Teams als auch für IT-Administratoren.

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.

Gezielte Analysen

Konzentrieren Sie sich mit einer nach Priorität geordneten Liste verdächtiger Erkennungen und anfälliger Konfigurationen auf die wichtigen Probleme. In dieser Liste finden Sie wichtige Informationen zur weitergehenden Analyse. Wählen Sie aus einer Library vorformulierter Vorlagen und stellen Sie IT-Ops- und und Threat-Hunting-Fragen. Alternativ können Sie auch Ihre eigenen Fragen formulieren.

Schnellere Analyse und Reaktion

KI-gesteuerte Analysen ermöglichen Ihnen, das Ausmaß und die Ursache eines Vorfalls schnell zu erkennen und zu bestimmen, damit Sie so schnell wie möglich reagieren können. Sehen Sie den Echtzeitstatus und bis zu 90 Tage zurückliegende Daten auf Ihren Geräten oder rufen Sie 30 Tage zurückliegende Daten im Data Lake ab.

Produktübergreifende Transparenz

Erhalten Sie maximale Transparenz über Ihr Unternehmen durch die native Datenintegration von Intercept X, Intercept X for Server, Sophos Firewall, Sophos Email, Sophos Mobile, Cloud Optix und Microsoft Office 365.

Unterstützung mehrerer Plattformen und Betriebssysteme

Überprüfen Sie Ihre lokale, Cloud- oder virtuelle Umgebung auf Bereitstellungen von Windows, macOS, Linux, Amazon Web Services, Microsoft Azure, Google Cloud Platform und Oracle Cloud Infrastructure.

Highlights

- Beantwortung geschäftskritischer IT-Operations- und Threat-Hunting-Fragen
- Liste mit nach Priorität geordneten Erkennungen und KI-gesteuerte Analysen
- Remote-Bereinigung von Geräten
- Ganzheitlicher Überblick über die IT-Umgebung Ihres Unternehmens und bei Bedarf einfacher Zugriff auf Detail-Informationen
- Native Endpoint-, Server-, Firewall-, E-Mail-, Cloud-, Mobile- und O365-Integrationen
- Library mit vorformulierten, anpassbaren Vorlagen für häufige Anwendungsfälle

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
- Nach Mobilgeräten mit fehlenden Patches oder veralteter Software suchen

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
- Benutzer mit mehreren fehlgeschlagenen Authentifizierungsversuchen erkennen

Das ist enthalten:

	Extended Detection and Response (XDR)
Produktübergreifende Datenquellen	✓
Produktübergreifende Erkennung, Analyse und Reaktion	✓
Liste mit nach Priorität geordneten Erkennungen und KI-gesteuerte Analysen	✓
Sophos Data Lake	✓
Dauer der Datenspeicherung im Data Lake	30 Tage
Statusinformationen in Echtzeit	✓
Dauer der Datenspeicherung auf Festplatte	Bis zu 90 Tage
Vorlagen-Library für Threat Hunting und IT Ops	✓
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

22-01-06 DS-DE (MP)

SOPHOS