INCAS
MEMBER OF THINK ABOUT IT

SOPHOS

– Information –

KOSTENLOSE INTEGRATIONEN

von Drittanbietern bei Sophos

Unser Partner Sophos stellt die Third-Party-Integrationen für Sophos XDR und MDR ab sofort *kostenfrei* bereit. Die zuvor lizenzpflichtigen Integration Packs sind nun Bestandteil aller XDR- und MDR-Subscriptions – sowohl für Neu- als auch Bestandskunden. Unternehmen profitieren so von einer deutlich erweiterten Sichtbarkeit über ihre gesamte IT-Landschaft.

Was sind Third-Party-Integrationen für XDR und MDR?

Drittanbieter-Integrationen – häufig auch Connectoren genannt – erweitern Sophos XDR und MDR um Telemetrie aus externen Systemen. Sie binden Datenquellen, wie beispielsweise Microsoft 365, Firewalls, Cloud-Plattformen oder Identity- und Productivity-Dienste, direkt in Sophos Central ein.

Die Informationen fließen in den Sophos Data Lake, um dort für Analysen, Abfragen und automatisierte Korrelationen genutzt zu werden. Gerade in heterogenen Umgebungen entsteht so ein vollständigeres Lagebild, ohne dass zusätzliche Tools oder Middleware notwendig sind. Für Administratoren und das Sophos SOC bedeutet das eine deutlich umfassendere Sicht auf sicherheitsrelevante Ereignisse, da Endpoint-, Server- und Netzwerkdaten sich mit den Logs anderer Hersteller verknüpfen lassen.

XDR-Abfragen werden präziser und das MDR-SOC bekommt mehr Kontext für die Incident-Analyse. So können sowohl die Erkennungsqualität als auch die Reaktionsgeschwindigkeit gesteigert werden.

Was bedeutet die Neuerung für Kunden?

Für Unternehmen steigt mit der kostenlosen Intergration der Connectoren die Qualität der Erkennung deutlich. Verdächtige Aktivitäten lassen sich besser korrelieren, weil Daten aus Firewalls, Cloud-Diensten, Productivity-Tools und Identity-Systemen einheitlich ausgewertet werden. XDR- und MDR-Umgebungen erhalten unmittelbar mehr Kontext und eine umfassendere Sichtbarkeit, ohne dass zusätzliche Module lizenziert oder nachträglich eingeplant werden müssen. Für XDR-Kunden bedeutet die Neuerung vor allem mehr Flexibilität und eine höhere Datenqualität in Abfragen und Reportings. So wird Ihr SOC Teams best-möglich unterstützt und in die Lage versetzt, kurzfristig auf Bedrohungen zu reagieren und umfassende Entscheidungen treffen zu können.

Vorteile im Überblicke

- Nahtlose Einbindung ohne zusätzliche Kosten
- Qualität der Erkennung und Geschwindigkeit steigt
- Einheitliche Auswertungen, bessere Korrelation
- höhere Datenqualität in Abfragen und Reportigns

Beispielintegrationen

- M365-Integration ab 199 €*
- Veeam Integration ab 199 €*

*Kosten der Integrationen hängen von verschiedensten Faktoren ab und müssen nach Anfrage und Bedarf kalkuliert werden.

Die INCAS unterstützt Sie bei der Anbindung von XDR-Connectoren

Die Anbindung externer Systeme an Sophos XDR oder MDR erfordert Erfahrung mit API-Zugriffen, Log-Formaten und Berechtigungsmodellen. Gerade bei Firewalls anderer Hersteller, Cloud-Plattformen oder Identity-Diensten empfiehlt es sich, Connectoren sauber zu planen und strukturiert einzurichten. Wir als *Sophos Platinum Partner* übernehmen und unterstützen Sie gerne bei:

- der Auswahl sinnvoller Datenquellen für XDR/MDR
- der technischen Einrichtung der jeweiligen Connectoren
- der Optimierung von Log-Volumen, Berechtigungen und Data-Lake-Qualität
- der Validierung der eingehenden Telemetrie und Tests im Produktivbetrieb
- Best Practices für Hybrid- und Multi-Cloud-Umgebungen

Wir stellen Ihnen ein SOC Team und die Ressourcen bereit, damit Sie sich bestmöglich aufstellen können.

SOPHOS PLATINUM PARTNER

Kontaktieren Sie unseren Experten:

Yannick Marx
Product Owner | Security

E: marx@incas.de
T: +49 2151 6201051

www.incas.com

INCAS GmbH · Medienstraße 8 · 47807 Krefeld