Cortex XSOAR

Sicherheitsorchestrierung, -automatisierung und -reaktion (SOAR) neu definiert

Viele Sicherheitsteams können nicht mit der Menge an Warnmeldungen und Routineaufgaben Schritt halten, mit denen sie Tag für Tag konfrontiert sind. In der Regel liegt das daran, dass sie nicht genug Personal haben oder dass ihre Prozesse nicht skalierbar sind. Vielerorts verschwenden Analysten Zeit, weil sie mehrere verschiedene Konsolen nutzen müssen, um Daten zu erfassen, Fehlalarme als solche zu erkennen und andere manuelle Routineaufgaben zu erledigen, die bei der Reaktion auf Sicherheitsvorfälle anfallen. Dabei bräuchten Manager im Bereich Cybersicherheit angesichts des wachsenden Fachkräftemangels eigentlich mehr Zeit für wichtige Entscheidungen und sollten nicht ständig mit diversen kleinen Baustellen beschäftigt sein.

Ein Pionier unserer Branche

Cortex™ XSOAR steigert die Effizienz von Security Operations Centern (SOC) mit einer unglaublich umfassenden Plattform für die Unternehmenssicherheit. Cortex XSOAR vereint Fallmanagement, Automatisierung, Zusammenarbeit in Echtzeit und natives Bedrohungsdatenmanagement in der branchenweit ersten erweiterten SOAR-Lösung (Sicherheitsorchestrierung, -automatisierung und -reaktion). Teams können Warnmeldungen aus allen Quellen verwalten, ihre Prozesse mit Ablaufskripten standardisieren, auf Bedrohungsdaten reagieren und die Reaktion auf beliebige sicherheitsrelevante Szenarien automatisieren. Dadurch kann die Reaktionszeit um bis zu 90 % verkürzt und die Anzahl der Warnmeldungen, mit denen die Analysten sich befassen müssen, um bis zu 95 % reduziert werden.

Kommerzielle Vorteile

- Skalierung und Standardisierung der Incident-Response-Prozesse
- Beschleunigung der Vorfallsbehebung und Steigerung der Effizienz des SOC
- Verbesserung der Produktivität der Analysten und des Erfahrungsgewinns im Team
- Direkte Rendite aus bereits getätigten Investitionen in Bedrohungsdaten

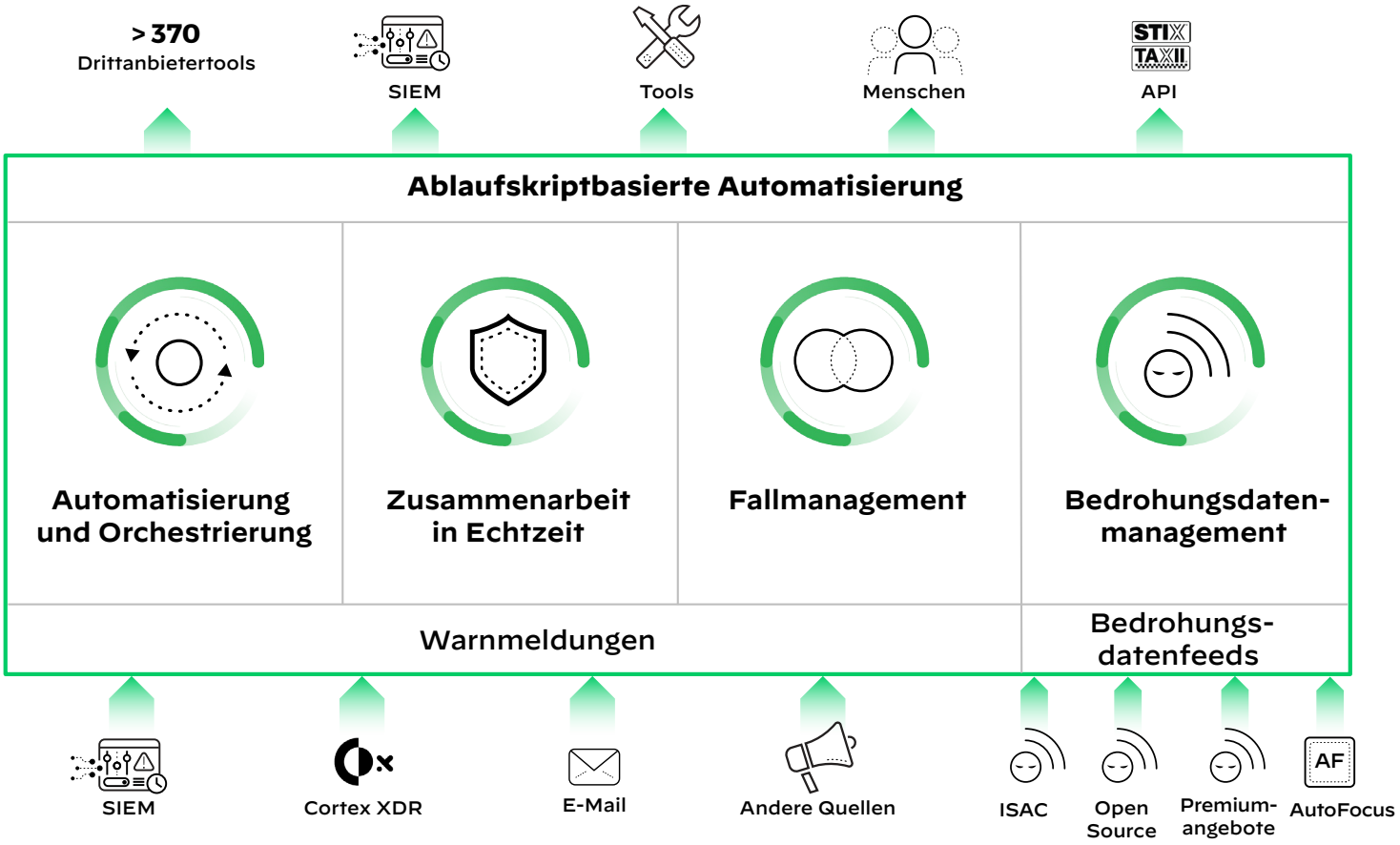

Abbildung 1: Ein- und Ausgaben von Cortex XSOAR

Tabelle 1: Standardisierung und Automatisierung der Prozesse für beliebige Sicherheitsszenarien	
Skalierbare, konsistente Reaktion auf Vorfälle	Hunderte sofort einsatzbereite Ablaufskripte decken ein breites Spektrum an Szenarien ab (Phishing, Anreicherung von Gefahrenindikatoren, Schwachstellenmanagement, Cloud-Sicherheit usw.) und beschleunigen die Bereitstellung. Ein funktionsreiches SDK ermöglicht die Entwicklung eigener Integrationen.
Modulare, anpassbare Ablaufskripte	Ein visueller Editor für Ablaufskripte bietet Tausende ausführbarer Aktionen an, die per Drag-and-Drop kombiniert werden können, um Prozesse aller Art zu automatisieren, von der Reaktion auf einfache Szenarien bis hin zu komplexen, nutzerspezifischen Workflows. Die so entstandenen Abläufe können auch ineinander verschachtelt und in anderen Ablaufskripten wiederverwendet werden. Sie können Ihre Ablaufskripte schnell und einfach ändern, testen und als YAML-Dateien mit anderen teilen.
Automatisierung und menschliche Reaktion im Gleichgewicht	Sie können manuelle Genehmigungsschritte in Ihre Ablaufskripte einfügen, um die automatisierten Prozesse unter Kontrolle zu behalten.
Orchestrierung über den ganzen Produktstack hinweg	Zur Anreicherung der Informationen über und zur Reaktion auf Vorfälle stehen über 370 Integrationen zur Verfügung, darunter Tools für die Anreicherung, Bedrohungsdaten-feeds, SIEMs, Firewalls, EDRs, Sandboxes, forensische Tools, Messaging-Systeme u. a. m.

Sicherheitsorchestrierung

Cortex XSOAR ermöglicht Sicherheitsprofis ein effizientes Arbeiten, sowohl im routinemäßigen Sicherheitsbetrieb als auch bei der Reaktion auf Vorfälle. Erreicht wird dies durch das Straffen der Sicherheitsprozesse, die Verknüpfung nicht miteinander kompatibler Sicherheitstools und das richtige Gleichgewicht zwischen maschinengestützter Sicherheitsautomatisierung und menschlichen Eingriffen.

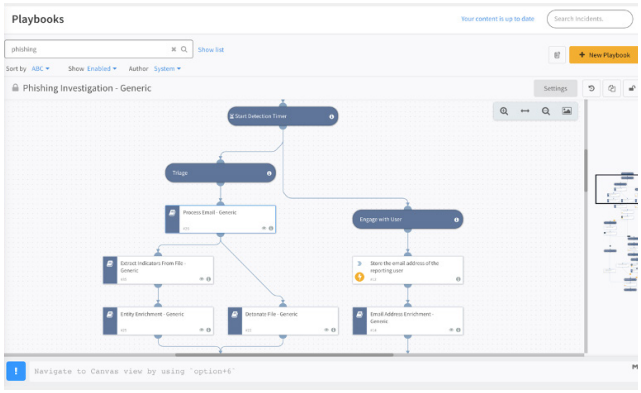

Abbildung 2: Ablaufskript für ein Phishingszenario in Cortex XSOAR

Tabelle 2: Anpassung an beliebige Warnmeldungen mit sicherheitsorientiertem Fallmanagement	
Anpassbare Ansichten für verschiedene Arten von Vorfällen	Vorfallsansichten, -layouts und -verläufe sind vollständig konfigurierbar, einschließlich spezifischer Zugriffsrechte für verschiedene Sicherheitsverantwortlichkeiten oder -rollen.
Abgleich von Gefahren-indikatoren und Vorfällen	Ein zentrales Gefahrenindikatoren-Repository unterstützt die vorfallübergreifende Suche nach und den Abgleich von Gefahrenindikatoren in verschiedenen Quellen und damit die Erkennung von Trends und Mustern.
Flexible, an die Anforderungen Ihres Unternehmens anpass-bare Berichte	Widgetgestützte Dashboards und Berichte bieten einen konkurrenzlosen Überblick über Ihre Kennzahlen.
Vorfallsüberwachung per Fernzugriff	Über die Mobilgeräte-App von Cortex XSOAR haben Sie Ihre Dashboards, Aufgabenlisten und Vorfälle auch unterwegs im Blick.
Automatisierte Ticketerstellung	Sofort einsatzbereite Integrationen mit Fallmanagementplattformen wie ServiceNow, Jira, Zendesk, Remedy und Slack unterstützen die vollständige Automatisierung der Ticketerstellung.

Fallmanagement

Wenn menschliche Eingriffe erforderlich sind, sollte die automatisierte Reaktion auf Vorfälle mit der Untersuchung komplexer Szenarien in Echtzeit kombiniert werden. Cortex XSOAR beschleunigt die Reaktion auf Vorfälle durch das Zusammenführen der Warnmeldungen, Vorfälle und Gefahrenindikatoren aus beliebigen Quellen auf einer einzigen Plattform, wo blitzschnelle Suchen, Anfragen und Untersuchungen durchgeführt werden können.

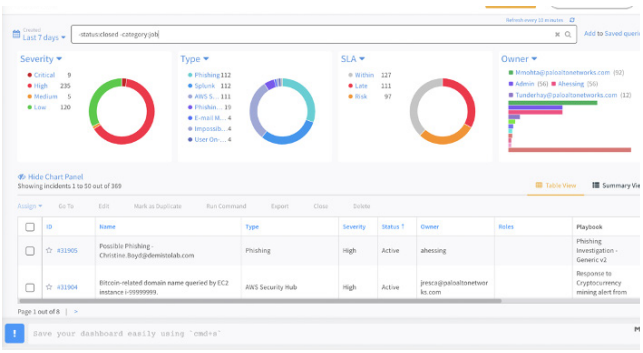

Abbildung 3: Anpassbare Vorfallsansichten

Tabelle 3: Steigerung der Effizienz des Sicherheitsbetriebs durch Zusammenarbeit in Echtzeit	
Untersuchung und Zusammenarbeit in Echtzeit	Für jeden Vorfall gibt es ein virtuelles Krisenzentrum mit integrierten ChatOps und einer Befehlszeilenschnittstelle (CLI). Dort können Analysten nicht nur in Echtzeit zusammenarbeiten, sondern auch direkt Sicherheitsaktivitäten einleiten.
Unterstützung für maschinelles Lernen	Ein ML-gestützter virtueller Assistent lernt aus den auf der Plattform durchgeführten Aktivitäten und gibt Empfehlungen zur Zuweisung von Vorfällen an Analysten und zu geeigneten Befehlen und Aktionen.
Kontinuierliches Lernen	Alle bei Untersuchungen durchgeführten Aktivitäten werden automatisch dokumentiert, damit Analysten aus ihnen lernen können.
Rationelle, automatisierte Berichterstellung	Flexible, widgetgestützte Dashboards und Berichte sind vollständig an die Anforderungen individueller Unternehmen anpassbar und machen die manuelle Berichterstellung überflüssig.

Bedrohungsdatenmanagement

Mit nativem Bedrohungsdatenmanagement, einheitlicher Konsolidierung, Bewertung und Weiterleitung von Bedrohungsdaten und ablaufskriptbasierter Automatisierung verfolgt Cortex XSOAR einen neuen Ansatz.

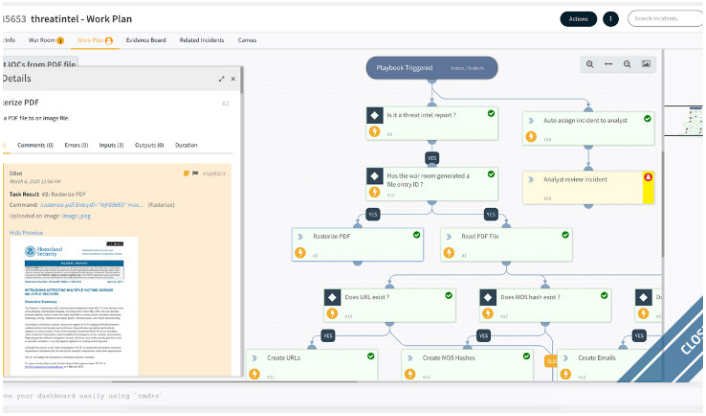

Abbildung 4: Bedrohungsdatenbasierte, automatisierte Ablaufskripte

Tabelle 4: Schnelle, souveräne Umsetzung von Bedrohungsdaten	
Automatisierte Konsolidierung von Bedrohungsdatenfeeds aus verschiedenen Quellen	Manuelle Arbeitsschritte können mit Ablaufskripten automatisiert werden, die pro Tag Millionen von Gefahrenindikatoren aus Dutzenden unterstützter Quellen aggregieren und parsen, Duplikate entfernen und die Ergebnisse verwalten.
Granulare Bewertung und Verwaltung der Indikatoren	Mit ablaufskriptbasiertem Lebenszyklusmanagement und transparenten Bewertungen, die leicht angepasst und erweitert werden können, bekommen Sicherheitsteams ihre Bedrohungsdaten in den Griff.
Vorbildliche betriebliche Effizienz	Der Abgleich von Bedrohungsdaten aus externen Quellen mit internen Vorfällen fördert die Zusammenarbeit und trägt zur Aufdeckung kritischer Bedrohungen, zur Priorisierung der wichtigsten Warnmeldungen und zur fundierten Auswahl der besten Gegenmaßnahmen bei.
Zuverlässige native Bedrohungsdaten	Integrierte, äußerst zuverlässige und kontextspezifische Bedrohungsdaten von Palo Alto Networks AutoFocus™ beschleunigen die Untersuchungen.
Automatisierte Ablaufskripte mit erweiterbaren Integrationen	Über 370 Produkte anderer Anbieter können von unternehmensspezifischen, auf bewährten SOAR-Funktionen basierten Ablaufskripten aus aufgerufen werden, um Bedrohungen automatisch zu blockieren.

Breites Anwendungsspektrum

Cortex XSOAR stellt eine offene, erweiterbare Plattform bereit, die für ein breites Spektrum von Anwendungsszenarien geeignet ist, darunter sogar Prozesse, die normalerweise nicht in den Verantwortungsbereich eines SOCs oder Sicherheitsteams fallen. Zu den gängigsten Anwendungsbereichen gehören das Blockieren von Phishingangriffen, routinemäßige Sicherheitsprozesse, die Bearbeitung sicherheitsrelevanter Warnmeldungen, die Orchestrierung der Cloud-Sicherheit, das Schwachstellenmanagement und die proaktive Suche nach Bedrohungen.

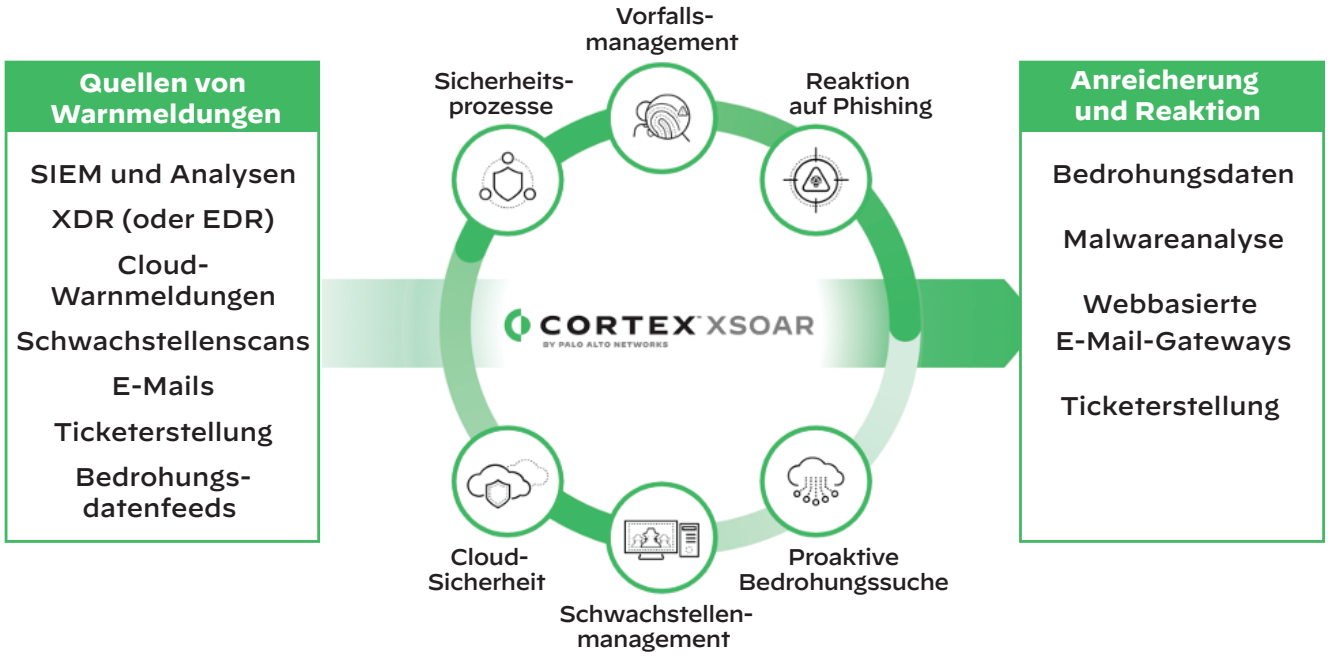

Abbildung 5 : Einspeisung von Warnmeldungen in Cortex XSOAR

Breites Spektrum von Integrationen

Cortex XSOAR enthält ein Spektrum an sofort einsatzbereiten Schnittstellen für Sicherheits- und andere Tools, die von Sicherheitsteams genutzt werden, das sowohl in seiner Breite als auch in der Tiefe der Integration seinesgleichen sucht. Alle zwei Wochen werden neue Integrationen hinzugefügt, damit unsere Kunden möglichst viele Tools schnell und nahtlos einsetzen können.

Die Vorteile der Interoperabilität

- Sie können Ihre Plattform und Lösungen anbieten,
- eine strategische Partnerschaft mit Palo Alto Networks aufbauen,
- von Co-Marketing-Aktivitäten und Lead-Generierung profitieren und
- Ihre Marke in der Sicherheitsbranche bekannt machen.

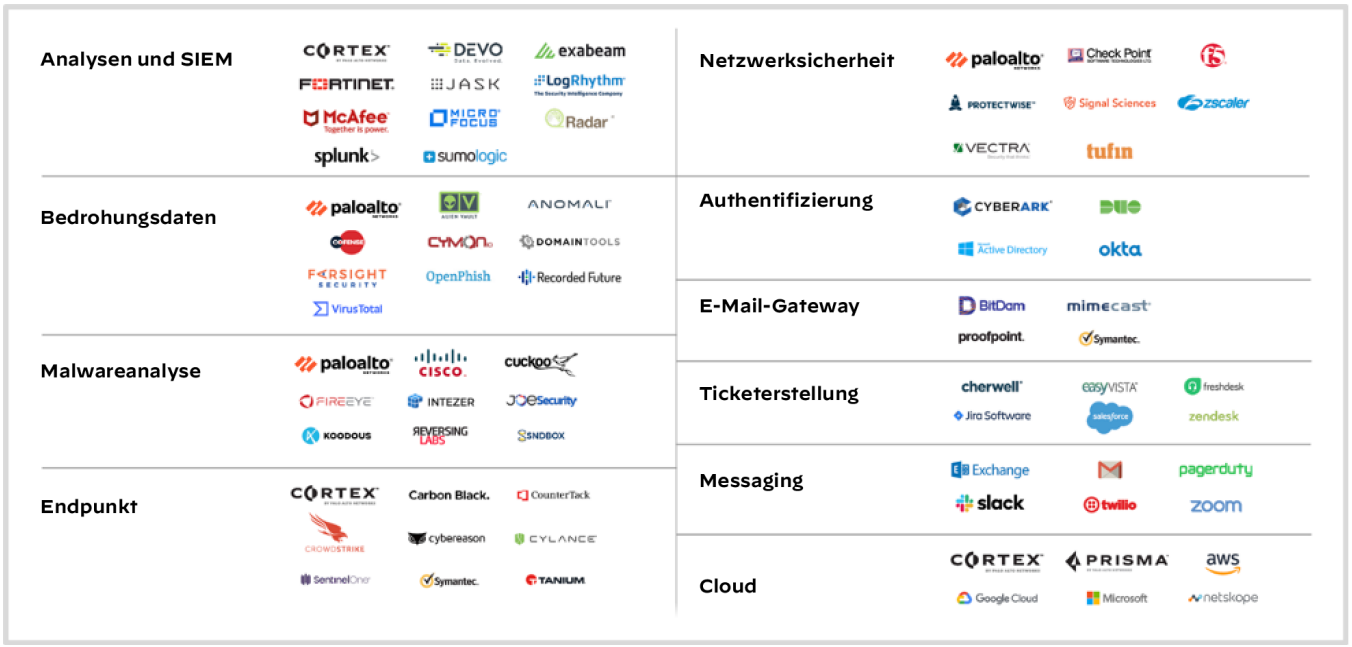

Abbildung 6: Einige unserer über 370 sofort einsatzbereiten Integrationen

Für MSSPs konzipiert

Dank seiner skalierbaren Architektur und Unterstützung für die Datensegmentierung ist Cortex XSOAR vollständig mandantenfähig und daher hervorragend für Anbieter gemanagter Sicherheitsdienste (MSSPs) geeignet. MSSPs können ihre Managed Services auf Cortex XSOAR aufbauen, um ihren Kunden erstklassige Angebote zu unterbreiten und die Produktivität ihrer internen Teams zu steigern.

Tabelle 5: Ein Fabric, das Ihre Sicherheitsinfrastruktur und Ihre Teams zusammenhält

Sicherheit und Datenschutz	Eine strenge Trennung zwischen Master und Mandanten, die Ausführung jedes Mandanten in einem eigenen Prozess zur Ausführungsisolierung und die Netzwerkisolierung mit einer Engine (Proxy) für die Netzwerksegmentierung ohne Änderungen an der Firewall sorgen für eine zuverlässige Datenisolierung zwischen den Mandanten.
Rollenbasierte Transparenz und Überwachung	Vom MSSP-Masterkonto aus können die Ablaufskripte, Berichte, Automatisierung und andere Einstellungen für alle Mandanten aktualisiert werden. Die Zugriffsrechte jedes Kunden können auf seine eigene Umgebung beschränkt werden. Die Integration von Drittanbietertools ist auf der Master- oder der Mandantenebene möglich.
Stärkeres Kundenvertrauen und agilere Reaktion	Im Bedarfsfall können Sie in einem virtuellen Krisenstab in Echtzeit mit Ihren Kunden gemeinsam Untersuchungen durchführen. Sie und Ihre Kunden profitieren jederzeit von der schnellen Bereitstellung neuer und der bedarfsgerechten Skalierung vorhandener Umgebungen.
Flexible Bereitstellung	Sie können Cloud-Services, MSSP-Systeme und die Systeme beim Kunden miteinander verknüpfen.

Branchenführender Kundensupport

Unser Kundenerfolgsteam konzentriert sich voll darauf, Ihnen zu helfen, den größtmöglichen Mehrwert aus Ihren Investitionen in Cortex XSOAR zu ziehen und Ihnen Vertrauen in die Sicherheit Ihres Geschäftsbetriebs zu vermitteln.

Standard Success ist in jedem Abonnement von Cortex XSOAR enthalten, um Ihnen den Einstieg zu erleichtern. Dieser Plan umfasst Zugang zu Materialien für das Selbststudium und zu webbasierten Supporttools.

Premium Success ist der Plan, den wir unseren Kunden empfehlen. Er enthält das gesamte Angebot von Standard Success und eine Anleitung für den Einstieg, personalisierte Workshops, Telefonsupport rund um die Uhr und Zugang zu einem Kundenerfolgsteam, das individuell auf Sie eingeht und Ihnen hilft, die größtmögliche Rendite aus Ihrer Investition zu erzielen.

		Standard	Premium
	Auf einen Blick	Selbsthilfe	Optimierte Erfahrung
Hilfe beim Einstieg	Beginn der Customer Journey	●	●
	Hilfe beim Einstieg		●
	Unterstützung bei der Definition des ersten Anwendungsszenarios		●
Technischer Support	Zugang zur Support-Community	●	●
	Zugang zum Support-Portal	●	●
	Telefonsupport		24/7
	Privater Slack-DFIR-Kanal		●
Weiterbildung Schulungen	Zugang zu Online-Dokumentation	●	●
	Zugang zu Online-Schulungen	●	●
	Personalisierter Workshop		●
Optimierte Erfahrung	Jährliche Zustandsprüfung	●	●
	Personalisierte Erfolgspläne		●
	Regelmäßige Betriebsprüfung		●
	Priorisierte Integrationsentwicklung		●

Abbildung 7: Die wichtigsten Aspekte von Standard und Premium Success

Flexible Bereitstellung

Cortex XSOAR kann On-Premises, in einer privaten Cloud oder als vollständig gehostete Lösung bereitgestellt werden. Wir bieten die Plattform in mehreren Stufen an, um verschiedenen Anforderungen gerecht zu werden.

Tabelle 6: Servicestufen von Cortex XSOAR

Cortex XSOAR	Cortex XSOAR Community Edition
Unbegrenzte Automatisierung	166 Automatisierungsbefehle pro Tag
Unbegrenztes Verlaufsprotokoll	Verlaufsprotokoll für die letzten 30 Tage
Unbegrenzte Bedrohungsdatenfeeds	5 aktive Feeds mit 100 Indikatoren/Feed
Native Bedrohungsdaten aus AutoFocus	Native Bedrohungsdaten aus AutoFocus nicht inbegriffen
Enterprise Reports (komplettes Paket)	Berichte über abgeschlossene Vorfälle
Kundensupport rund um die Uhr	Slack DFIR Community
Mandantenfähig	Ein Mandant

Systemanforderungen: On-Premises

Tabelle 7: Cortex XSOAR Server		
Komponente	**Minimum**	**Empfohlen**
CPU	8 CPU-Kerne	16 CPU-Kerne
Arbeitsspeicher	16 GB RAM	32 GB RAM
Festplattenspeicher	500 GB SSD	1 TB SSD mit mindestens 3 K dediziertem IPOS
Physische oder virtuelle Server	Linux OS: Ubuntu 14.04, 16.04, 18.04, 18.10; RHEL 7.x; Oracle Linux 7.x; Amazon Linux 2; Fedora; Centos 7.x	

Tabelle 8: Cortex XSOAR Engine		
Komponente	**Minimum**	**Empfohlen**
CPU	8 CPU-Kerne	16 CPU-Kerne
Arbeitsspeicher	16 GB RAM	32 GB RAM
Festplattenspeicher	500 GB SSD	1 TB SSD mit mindestens 3 K dediziertem IPOS
Betriebssystem	macOS, Windows, Linux	

Cortex XSOAR Community Edition

Nutzen Sie die kostenlose Community Edition, um Cortex XSOAR auszuprobieren. In dieser Version ist eine 30 Tage lang gültige Enterprise-Lizenz enthalten, damit Sie alle Funktionen auf Herz und Nieren testen können.

Registrieren Sie sich für die kostenlose Community Edition.

paloalto NETWORKS

Oval Tower, De Entrée 99-197
1101 HE Amsterdam
Niederlande

Telefon: +31 20 888 1883

www.paloaltonetworks.de

cortex-xdr-032720-de