Cortex XSIAM

KI-gestützte SecOps-Plattform

Cortex® XSIAM™ (Extended Security Intelligence and Automation Management) ist die KI-gestützte SecOps-Plattform für das moderne Security Operations Center (SOC). Die Lösung nutzt die Vorteile von künstlicher Intelligenz (KI) und Automatisierung, um die Effizienz von Sicherheitsmaßnahmen sowie Betriebsprozesse im SecOps-Bereich radikal zu verbessern. Reduzieren Sie Ihr Risiko und die betriebliche Komplexität, indem Sie mehrere Produkte in einer einzigen Plattform zusammenführen, die speziell für Security Operations entwickelt wurde.

Die Bedingungen in den SOCs haben sich verändert

Die Anforderungen von SOCs haben sich gewandelt. Organisationen sehen sich mit einem höheren Zeitaufwand für die Erkennung und Behebung von Sicherheitsvorfällen konfrontiert. In Kombination mit den jüngsten gesetzlichen Vorschriften zur Meldung von Sicherheitsverstößen und angesichts der Tatsache, dass Cyberkriminelle für die Ausführung von End-to-end-Angriffen nur wenige Stunden benötigen, stellt dies ein erhebliches Risiko für Organisationen dar.

Nach jedem Verstoß untersucht das Sicherheitsteam den Vorfall erfolgreich und ermittelt die Methoden der Kompromittierung, die betroffenen Systeme und die gestohlenen Daten. Somit stellt sich folgende Frage: Wenn Sie über die entsprechenden Informationen verfügen, um sich nach einem Vorfall ein umfassendes Bild zu machen, warum ergreifen Sie dann nicht proaktive Maßnahmen, um solche Vorfälle zu verhindern oder zu stoppen, bevor sie auftreten?

Die Antwort auf diese Frage liegt in den drei wichtigsten Herausforderungen, denen sich SOCs heute stellen müssen:

1. Isolierte Tools und Daten

Wenn für die Erledigung einer Aufgabe zu viele Tools zum Einsatz kommen, ist dies nicht immer hilfreich. Voneinander isolierte Cybersicherheitstools führen zu ineffizienten Arbeitsabläufen, da zwischen verschiedenen Produkten und Konsolen gewechselt werden muss. Dadurch steigt die kognitive Belastung und Bedrohungen können übersehen werden. Die fehlende Integration behindert zudem die Bedrohungserkennung in Echtzeit und verzögert die Reaktion auf Vorfälle. Gleichzeitig ist der Betrieb mehrerer Tools ressourcenintensiv und kann die betriebliche Komplexität erhöhen. Die meisten Organisationen verfügen über riesige Mengen an Sicherheits- und Anwendungsdaten. Es sind jedoch zu viele und sie befinden sich an unterschiedlichen Orten. Netzwerkdaten werden in der Firewall gespeichert, Endpunktdaten in Tools für die Bedrohungserkennung und Abwehr am Endpunkt (Endpoint Detection and Response, EDR), Authentifizierungsdaten in einem separaten Protokoll und andere wichtige Informationen verlassen möglicherweise nie die anwendungsspezifischen Protokolle. Schlimmer noch: Etwa die Hälfte der Organisationen, mit denen wir in Kontakt stehen, gibt an, dass sie ihre Cloud-Prozesse nicht über das SOC abwickeln. Die Datenbestände sind also weit verteilt.

2. Unzureichende Bedrohungsabwehr

Ausschließlich auf statische Korrelationsregeln und umfangreiches Detection Engineering zu setzen, stellt angesichts der schieren Datenmenge eine große Herausforderung dar, wenn es darum geht, bedeutsame Beziehungen zwischen Sicherheitsereignissen in der gesamten Umgebung zu erkennen. In diesem Szenario sind Alarme unzusammenhängende Datenpunkte, die das SOC-Team manuell abgleichen muss. Leider führt dieser Ansatz oft zu einer unzuverlässigen Bedrohungserkennung mit vielen False Positives. Die fehlenden Zusammenhänge innerhalb dieses Prozesses beeinträchtigen die Effektivität der Sicherheitsinfrastruktur. Es wird deutlich, dass fortschrittlichere und anpassungsfähigere Methoden zur Bedrohungserkennung erforderlich sind, um False Positives zu vermeiden und die allgemeine Sicherheitslage zu verbessern.

3. Überwiegend manuelle Maßnahmen

Aufgrund riesiger Mengen unzusammenhängender Daten und uneinheitlicher Tools müssen SOCs eine überwältigende Anzahl von Alarmen untersuchen und beheben. Die Priorisierung dieser Alarme ist eine Herausforderung für SOC-Analysten. Zudem müssen sie häufig Ereignisse aus verschiedenen Datenquellen und Tools manuell abgleichen, um herauszufinden, womit sie es zu tun haben. Oftmals untersuchen Analysten mehrere verschiedene Alarme, ohne zu wissen, dass diese in Verbindung mit einem einzigen Vorfall stehen. Dies führt zu Redundanz und manueller Arbeit, wodurch sich die durchschnittliche Zeit zur Erkennung und Behebung von Sicherheitsvorfällen verlängert.

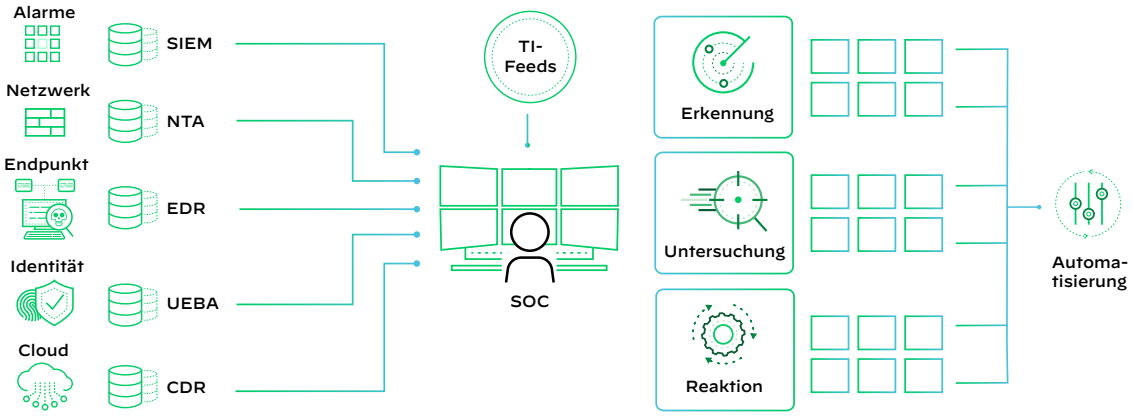

Abbildung 1: Security Operations in verschiedenen Silos

Die Lösung: SecOps muss neu durchdacht und modernisiert werden

Moderne SOCs benötigen eine neue Architektur – eine umfassende und automatisierte Integration, Analyse und Auswertung von Daten. Dabei ist eine konvergente Plattform unerlässlich, um Prozesse zu straffen und die Effizienz zu steigern. Das Reduzieren der betrieblichen Komplexität ist in der heutigen schnelllebigen digitalen Landschaft von entscheidender Bedeutung. Durch die Integration verschiedener Systeme und Tools in eine zentrale Lösung können Unternehmen Silos beseitigen und sich einen einheitlichen Überblick über ihre Abläufe verschaffen.

Darüber hinaus hat eine umfassende Bedrohungsabwehr für Organisationen höchste Priorität. Mithilfe KI-gestützter Funktionen können Unternehmen potenzielle Risiken proaktiv erkennen und abwehren und so die Sicherheit ihrer Daten und Systeme gewährleisten.

Ein automatisierungsbasierter Ansatz beschleunigt zudem die Behebung von Vorfällen und reduziert den manuellen Aufwand und die Reaktionszeiten. Dank Automatisierung können Unternehmen Probleme schnell beheben, Ausfallzeiten minimieren und ihre betriebliche Gesamtleistung optimieren.

Abbildung 2: Ein transformiertes SOC

Cortex XSIAM

Cortex® XSIAM™ ist eine KI-gestützte SecOps-Plattform für moderne SOCs, die mithilfe von KI und Automatisierungsfunktionen SecOps-Prozesse vereinfacht, Bedrohungen umgebungsweit abwehrt und die Vorfallsbehebung beschleunigt. Reduzieren Sie Ihr Risiko und die betriebliche Komplexität, indem Sie mehrere Produkte in einer einzigen kohärenten Plattform zusammenführen, die speziell für Security Operations entwickelt wurde.

Mit Cortex XSIAM meistern Sie SOC-bezogene Herausforderungen heute und in Zukunft. Durch die Konsolidierung von Daten und Tools in einer einzigen KI-basierten Plattform können SOCs ihre Security Operations vereinfachen, Bedrohungen umfassend abwehren und die Effizienz ihrer Sicherheitsmaßnahmen erheblich beschleunigen.

Cortex XSIAM wurde entwickelt, um drei grundlegende Ziele zu erreichen und im SOC das scheinbar Unmögliche möglich zu machen:

1. Einfachere SecOps dank einer zentralen Plattform

Die Integration verschiedener SOC-Lösungen wie XDR, SOAR, ASM und SIEM in eine zentrale Plattform vereinfacht den SecOps-Betrieb enorm. Die Teams müssen nicht mehr zwischen zahlreichen Tools wechseln und können daher ihre Arbeitsabläufe deutlich straffen. Die Plattform unterstützt diverse Lösungen, sodass mehrere Datenquellen ohne großen Aufwand und ohne Infrastrukturänderungen integriert werden können. Dadurch können SOC-Teams mehr sicherheitsrelevante Daten einbinden und aussagekräftigere Analysen durchführen. Darüber hinaus liefert die kontinuierliche Erfassung, Verknüpfung und Normalisierung von Rohdaten weit mehr Informationen als reine Alarme. SOC-Teams können daher schneller und einfacher Untersuchungen starten und entsprechend schneller und effektiver Bedrohungen erkennen und beheben.

2. Umfassende Bedrohungsabwehr mithilfe KI-gestützter Funktionen

Sofort einsatzbereite KI-Modelle übertreffen herkömmliche Methoden bei Weitem, da sie Ereignisse aus verschiedenen Datenquellen abgleichen und einen umfassenden Überblick über Vorfälle und Risiken an einer zentralen Stelle bieten. So können Organisationen ihre Erkennungs-, Analyse- und Abwehrfunktionen verbessern. Durch die Gruppierung von Alarmen und die KI-gestützte Vorfallsbewertung kann Cortex XSIAM nicht sicher beurteilbare Ereignisse zu zuverlässig klassifizierbaren Vorfällen zusammenfassen. Bei dieser Priorisierung wird das Gesamtrisiko berücksichtigt, sodass Sicherheitsteams ihre Aufgaben effizienter erledigen können.

3. Schnellere Vorfallsbehebung mit einem automatisierungsorientierten Ansatz

Im Cortex Marketplace sind Hunderte bewährter Content-Packs verfügbar, mit denen SOC-Teams ihre Prozesse und Interaktionen für das gesamte Sicherheitsprogramm optimieren können. Dank der eingebetteten Automatisierungsfunktionen sparen die Teams Zeit und Aufwand, da damit Aufgaben, die bisher manuell bewältigt werden mussten, automatisch erledigt werden können, wie beispielsweise die Reaktion auf Vorfälle, das Risikomanagement und der Schutz der Angriffsfläche. Außerdem können Benutzer Automatisierungsfunktionen flexibel hinzufügen und an ihre Anforderungen anpassen. Die Plattform umfasst zudem Playbooks für bestimmte Alarme, die automatisch gestartet werden, sodass Sicherheitsaufgaben sofort erledigt und Risiken behoben werden, ohne dass sich Analysten darum kümmern müssen. XSIAM lernt auch aus den manuellen Aktionen der Analysten und macht Vorschläge zu Prozessen, die in Zukunft automatisch erledigt werden könnten. Das kontinuierliche Lernen trägt dazu bei, dass die Plattform automatisch Vorfälle beheben und ihre Effizienz und Genauigkeit im Laufe der Zeit weiter verbessern kann.

Ein neues SecOps-Design, das folgende Vorteile bietet:

- **Liefert** eine neue SOC-Architektur mit einem automatisierungsorientierten Ansatz
- **Kombiniert** branchenführende SOC-Funktionen für eine bessere Analystenerfahrung
- **Konsolidiert** mehrere Produkte auf einer zentralen Plattform
- **Erweitert** das SOC auf die Cloud für umfassende Transparenz
- **Steigert** die Produktivität der Analysten, da sie sich auf die tatsächlich relevanten Vorfälle konzentrieren können

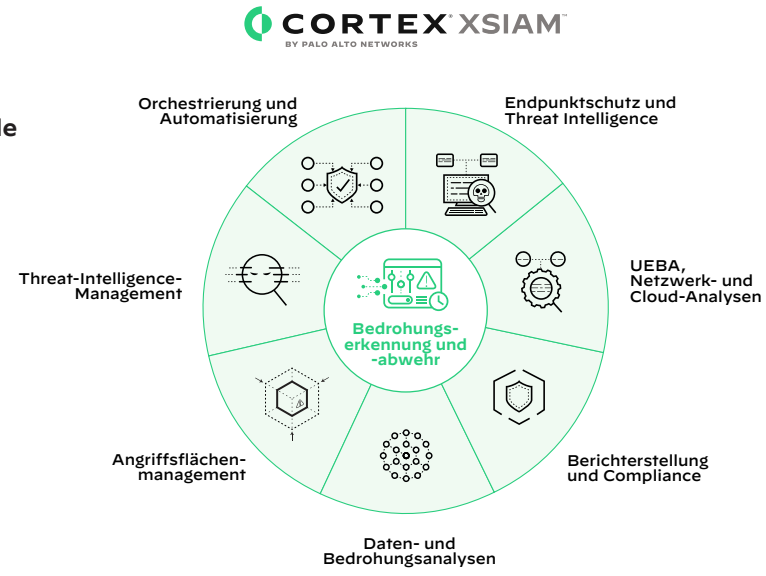

Abbildung 3: Cortex XSIAM

Wichtige integrierte Funktionen

Cortex XSIAM vereint diese unverzichtbaren Funktionen verschiedener SOC-Produkte in einer einzigen Plattform:

Security Information and Event Management (SIEM)

Bietet Protokollmanagement, Korrelation und Alarme, Berichte zu Compliancezwecken* und andere gängige SIEM-Funktionen.

Threat-Intelligence-Plattform (TIP)*

Umfasst sämtliche TIP-Funktionen, um die Feeds von Palo Alto Networks und Drittanbietern zu verwalten und automatisch mit Alarmen und Vorfällen abzugleichen.

Extended Detection and Response (XDR)

Importiert Telemetriedaten von Endpunkten, Cloud-Umgebungen, Netzwerken und Drittanbietern für eine automatisierte Bedrohungserkennung und -abwehr.

Bedrohungserkennung und -abwehr an Endpunkten (EDR)

Umfasst ein Backend-System mit Endpunktagent und Cloud-Analysen, das die Bedrohungsabwehr am Endpunkt, automatisierte Abwehrmaßnahmen und detaillierte Telemetriedaten unterstützt, die bei allen Untersuchungen nützlich sind.

Angriffsflächenmanagement (ASM)*

Bietet mithilfe eingebetteter ASM-Funktionen einen umfassenden Überblick über die vorhandenen Assets, einschließlich interner Endpunkte, und weist auf identifizierte Sicherheitslücken in Assets mit Internetanbindung hin.

Identity Threat Detection and Response (ITDR)*

Kombiniert UEBA-Funktionen mit modernen Bedrohungsmodellen zum Identitätsbetrug, um Gefahren wie Insiderbedrohungen, Datenausschleusung und die verdächtige Ausbreitung im Netzwerk zu erkennen, zu verhindern und zu beheben.

Analyse des Benutzer- und Objektverhaltens (UEBA)

Nutzt maschinelles Lernen und Verhaltensanalysen, um Profile von Benutzern und Objekten zu erstellen und auf Verhaltensweisen hinzuweisen, die auf kompromittierte Konten oder böswillige Insider schließen lassen.

Sicherheitsorchestrierung, -automatisierung und -reaktion (SOAR)

Umfasst ein zuverlässiges SOAR-Modul und einen Marketplace, um Playbooks für Cortex XSIAM zu erstellen und zu orchestrieren.

Bedrohungserkennung und -abwehr in der Cloud (CDR)

Cortex XSIAM ermöglicht mit seiner Suite von Analysefunktionen auch spezielle Analysen zur Erkennung von und Warnung vor Anomalien in Cloud-Daten, zum Beispiel Protokolldateien von Cloud-Dienstanbietern und Alarmen von Cloud-Sicherheitsprodukten.

Management, Berichterstellung und Compliance

Zentrale Managementfunktionen vereinfachen den Betrieb. Effektive Funktionen für grafische Berichte unterstützen die Erstellung von Berichten zu Compliancezwecken, Datenintegrationen, Trends bei Vorfällen, SOC-Leistungskennzahlen und anderen Anwendungsfällen.

* Über zusätzliche Lizenzen und Module erhältlich

Cortex XSIAM erzielt nachweislich die gewünschten Ergebnisse

Cortex XSIAM hat bereits die Arbeit im SOC von Palo Alto Networks enorm verbessert. Unser Hauptziel ist jedoch, innovative Lösungen bereitzustellen und Cyberbedrohungen immer einen Schritt voraus zu sein, damit sich Kunden auf unsere Technologien verlassen können. Die neuesten Kennzahlen zum Kundenerfolg beweisen, dass Cortex XSIAM auch diese Anforderungen erfüllt.

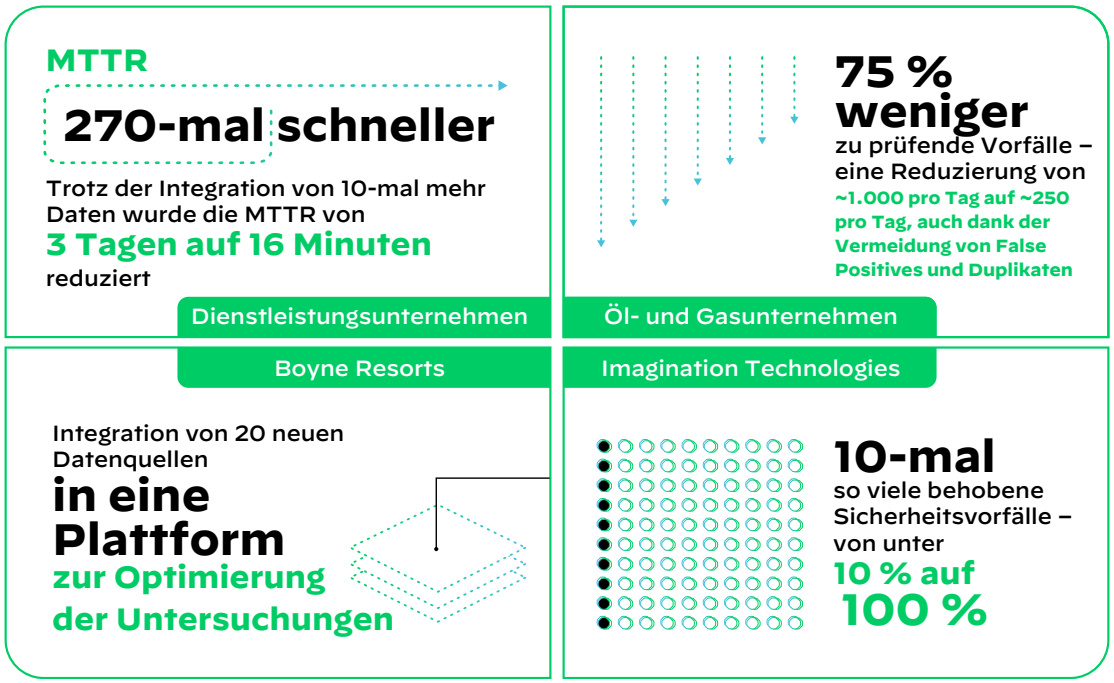

Abbildung 4: Kunden konnten mit Cortex XSIAM die Effizienz ihrer SOC-Prozesse steigern und die Transparenz verbessern.

Vorteile von Cortex XSIAM:

- Verbessert die Bedrohungserkennung und -abwehr, **sodass Angriffe verhindert werden, bevor Schäden entstehen**.
- SOCs können Daten aus mehr Quellen nutzen und trotzdem **die Reaktionszeit von mehreren Tagen auf wenige Minuten verkürzen**.
- **Ermöglicht das schnellere Beheben von Vorfällen und minimiert die Anzahl der Vorfälle**, die manuell untersucht und behoben werden müssen.
- Vereinfacht die Datenintegration und **verringert die Komplexität der Infrastruktur**.
- Bietet Unterstützung von Sicherheitsexperten mit dem notwendigen Fachwissen und entsprechenden Funktionen, um **von einer reaktiven zu einer proaktiven Sicherheitsstrategie zu wechseln**.

Unterstützung durch Experten mit Managed Services

Das Team von Unit 42® verfügt über jahrelange Erfahrung im Schutz von Unternehmen und Behörden weltweit. Dieses Know-how kommt dann auch Ihrer Umgebung zugute, die diese Experten rund um die Uhr überwachen und nach verdächtigen Aktivitäten durchsuchen. Die Unit 42-Experten haben Zugriff auf branchenführende Threat Intelligence aus mehr als zehn Jahren Malwareanalysen, die täglich um 30 Millionen neue Malware-samples und 500 Milliarden Ereignisse ergänzt werden. So sind Sie auch vor neuen Bedrohungen geschützt. Sie können die Services Managed Detection and Response (MDR) und Managed Threat Hunting (MTH) von Unit 42 ganz einfach zu Ihrer Cortex XSIAM-Subscription hinzufügen.

Managed Detection and Response-Service von Unit 42

Bei dem Managed Detection and Response-Service der Unit 42 von Palo Alto Networks (Unit 42 MDR) übernimmt ein Team aus erstklassigen Analysten, Bedrohungsfahndern und Forschern die Untersuchung und Abwehr von Angriffen, damit Ihr Team schnell reagieren und sich auf die strategisch wichtigen Aufgaben konzentrieren kann. Unit 42 MDR umfasst auch den Managed Threat Hunting-Service.

Managed Threat Hunting-Service von Unit 42

Bei dem Managed Threat Hunting-Service der Unit 42 von Palo Alto Networks (Unit 42 MTH) sucht ein Team aus erstklassigen Analysten, Bedrohungsfahndern und Forschern proaktiv nach komplexen Bedrohungen und liefert Ihnen einen detaillierten Bericht.

paloalto NETWORKS

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

Telefon: +31 20 888 1883
Vertrieb: +800 7239771
Support: +31 20 808 4600

www.paloaltonetworks.de