paloalto NETWORKS | CORTEX XSIAM®

Kaufleitfaden für XSIAM:
So rüsten Sie Ihr SOC für das KI-Zeitalter

INHALT

DAS FEHLENDE BINDEGLIED:
PROAKTIVE PRÄVENTION IM MODERNEN SOC

In der extrem dynamischen Cyber-Sicherheitslandschaft von heute werden Organisationen mit ganz neuen Herausforderungen konfrontiert. Cyber-Kriminelle von heute sind versierter als je zuvor und nutzen KI und andere moderne Techniken, um herkömmliche Sicherheitsmaßnahmen zu umgehen. Den Sicherheitsprofis unter Ihnen ist zweifelsohne bewusst, wie sehr sich die Anforderungen eines modernen Security Operations Center (SOC) verändert haben. Da die durchschnittliche Zeit vom Beginn eines Angriffs bis zum Erreichen der Angriffsziele im letzten Jahr von 24 auf wenige Stunden geschrumpft ist1 und regulatorische Vorgaben immer strikter werden, reichen konventionelle Tools und Methoden zur Bedrohungserkennung und -abwehr einfach nicht mehr aus.

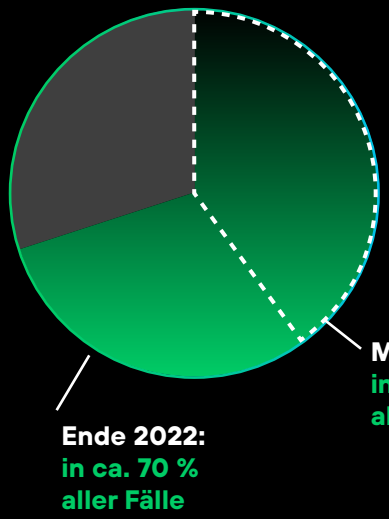
Im Anschluss an einen Sicherheitsvorfall ist Ihr Sicherheitsteam normalerweise in der Lage, den Angriffsverlauf zu rekonstruieren und festzustellen, wie die Akteure in Ihre Umgebung eingedrungen sind, welche Systeme betroffen waren und welche Daten ausgeschleust wurden. Da stellt sich natürlich die folgende Frage: Wenn die erforderlichen Informationen vorhanden sind, um einen Angriff im Nachhinein nachzuvollziehen, warum kann man Angriffe nicht rechtzeitig stoppen? Genau um diese Diskrepanz zwischen einer nachträglichen Analyse und proaktiver Prävention geht es bei den neuen Anforderungen an moderne SOCs.

Traditionelle Security-Information-and-Event-Management(SIEM)-Lösungen, die einst ein Grundpfeiler vieler SecOps-Ansätze waren, können nicht mehr mithalten. Zu den gängigen Problemen von heute zählen komplexe Konfigurationen, zeitaufwendige Integrationen, kostspielige Investitionen in Technologie für die Bedrohungserkennung und eine unüberschaubare Flut von Alarmen.

Mehrfacherpressungstaktiken gewinnen weiter an Bedeutung

Ransomwareangriffe haben sich in den letzten Jahren stark weiterentwickelt und Mehrfacherpressungen kommen immer häufiger vor.

Datendiebstahl bei Ransomwareangriffen:[2]



75 % mehr

Datendiebstähle im Rahmen von Ransomwareangriffen (über einen Zeitraum von 18 Monaten)

1. *Globaler Incident-Response-Bericht 2025 von Unit 42*, Palo Alto Networks, 25. Februar 2025.
2. *Ransomware- und Erpressungsbericht von Unit 42 2023*, Palo Alto Networks, Unit 42, 28. September 2025.

Die Folgen sind überforderte Sicherheitsteams und eine bedrohungsanfällige Umgebung. Voneinander isolierte Sicherheitstools führen zu ineffizienten Arbeitsabläufen, einer erhöhten kognitiven Belastung für Analysten und dazu, dass kritische Bedrohungen leicht übersehen werden. Die fehlende Integration zwischen proaktiven Sicherheitsfunktionen (wie dem Schwachstellenmanagement) und reaktiven Tools behindert zudem die Bedrohungserkennung in Echtzeit und verzögert die Reaktion auf Vorfälle, wodurch Ihre Organisation Risiken ausgesetzt wird.

Ausschließlich auf statische Korrelationsregeln und umfangreiches Detection Engineering zu setzen, macht es angesichts der schieren Datenmenge sehr schwierig, bedeutsame Beziehungen zwischen Sicherheitsereignissen in der gesamten Umgebung zu erkennen. Auch das schwächt Ihre Bedrohungsabwehr. In diesem Szenario sind Alarme oft unzusammenhängende Datenpunkte mit einem Übermaß an False Positives, die das SOC-Team manuell abgleichen muss. Die fehlenden Zusammenhänge innerhalb dieses Prozesses beeinträchtigen die Effektivität der Sicherheitsinfrastruktur. Es wird deutlich, dass fortschrittlichere und anpassungsfähigere Methoden zur Bedrohungserkennung erforderlich sind.

Messbare Vorteile: der wahre ROI der SOC-Transformation

Eine von Palo Alto Networks bei Forrester® Consulting in Auftrag gegebene Total Economic Impact™-Studie hat die Auswirkungen des Umstiegs auf Cortex XSIAM® untersucht und deutliche Belege für geschäftskritische Vorteile gefunden:[3]

257 % | $5,6 Mio. | <6 Monate

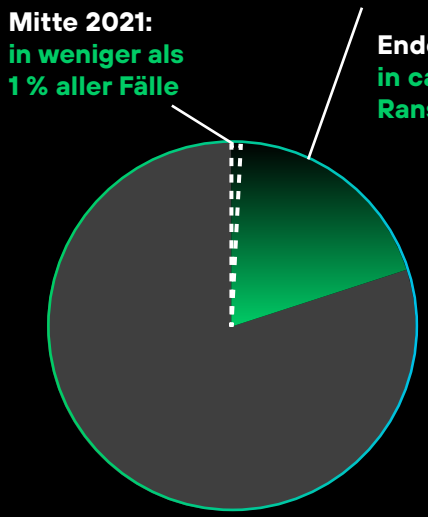
3-Jahres-ROI | Nettobarwert | Amortisationszeit

85 % | 70 % | $3,1 Mio.

Senkung der MTTR | Weniger Vorfälle mit SOC-Untersuchungen | Einsparungen durch Toolkonsolidierung

Mehrfacherpressungstaktiken gewinnen weiter an Bedeutung (Forts.)

Belästigung als Erpressungstaktik:[4]



1.900 % mehr

Belästigung durch Ransomwaregruppen (im selben Zeitraum)

Diese Statistiken verdeutlichen, wie sehr sich Ransomwarestrategien verändert haben und dass Angreifer zunehmend auf mehrgleisige Taktiken setzen, um ihre Opfer zu erpressen. Die drastische Zunahme an Datendiebstahls- und Belästigungsmethoden unterstreicht die neuartige Komplexität und Ernsthaftigkeit moderner Ransomwareangriffe.

- **Verschlüsselung:** Opfer zahlen, um wieder Zugriff zu erlangen
- **Datendiebstahl:** Hacker drohen mit der Veröffentlichung der gestohlenen Daten
- **DDoS:** DDoS-Angriffe legen die öffentlichen Websites lahm
- **Belästigung:** Kunden, Geschäftspartner und Medien werden kontaktiert

3. *The Total Economic Impact™ of Palo Alto Networks Cortex XSIAM*, Forrester Consulting, 13. Oktober 2025.
4. Ransomware- und Erpressungsbericht 2023, *Palo Alto Networks, Unit 42.*

DIE TRANSFORMATION IM SICHERHEITSBETRIEB

Ausgangspunkt der SOC-Transformation mit Palo Alto Networks ist der Cortex® Extended Data Lake (XDL) – ein erweiterbares, KI-fähiges Fundament für moderne SecOps-Plattformen. Das bedeutet zum einen, dass Cortex XDL alle Sicherheitsdaten aus sämtlichen Quellen zusammenführt, normalisiert und um wichtige Kontextinformationen anreichert. Zum anderen fungiert die Lösung als zentrale Datenquelle für Ihr SOC.

So schaffen Sie die erforderliche Datengrundlage für die Implementierung von Cortex XSIAM, eine einheitliche Plattform für die Konsolidierung der folgenden kritischen Sicherheitsfunktionen in Ihrem Unternehmen:

- Sicherheits-, Informations- und Ereignismanagement (SIEM)
- Bedrohungserkennung und -abwehr an Endpunkten (EDR)
- Erweiterte Bedrohungserkennung und -abwehr (XDR)
- Sicherheitsorchestrierung, Automatisierung und Reaktion (SOAR)
- Angriffsflächenmanagement (ASM)
- Analyse des Anwender- und Objektverhaltens (UEBA)
- Identitätsbezogene Bedrohungserkennung und -abwehr (ITDR)
- Bedrohungserkennung und -abwehr in der Cloud (CDR)
- Management von Threat Intelligence (TIM)
- Threat-Intelligence-Plattform (TIP)

> XSIAM gibt uns mehr Transparenz und ermöglicht schnellere Untersuchungen. Die nahtlose Datenintegration und automatische Einrichtung sind revolutionär.
>
> – Mike Dembek
>
> Network Architect, Boyne Resorts

Abbildung 1: XSIAM Command Center

Cortex XSIAM transformiert den Sicherheitsbetrieb durch das Zusammenführen von Daten, KI-gestützten Abwehrmaßnahmen und Automatisierung – alles auf einer Plattform. Im XSIAM Command Center erscheint eine Auflistung diverser Datenquellen, die unter anderem Endpunkte, Netzwerke, Systeme für das Identitätsmanagement sowie Cloud-Umgebungen und Anwendungen umfasst. Zugleich erhalten Sie einen detaillierten Überblick über Status und Volumen der Dateneinspeisung.

Mitarbeiter müssen nicht mehr zwischen verschiedenen Tools wechseln, komplexe Abläufe werden vereinfacht und Ihr Team kann effizienter arbeiten. An die Stelle mehrerer Konsolen und Dashboards mit zahlreichen Integrationsproblemen tritt eine einheitliche Plattform, die speziell für die Anforderungen moderner SOCs konzipiert ist. So können Sie den gesamten Sicherheitsbetrieb von zentraler Stelle aus verwalten.

Vor diesem Hintergrund zeigen aktuelle Forschungsergebnisse, dass Organisationen durch den Umstieg auf Cortex XSIAM messbare Vorteile erzielen. Beispielsweise hat eine unlängst von Forrester Consulting veröffentlichte Total Economic Impact™-Studie erwiesen, dass ein für die untersuchten Kunden repräsentatives Modellunternehmen nach drei Jahren **die Anzahl der an Level-1-SOC-Analysten überstellten Warnmeldungen um 85 % reduzieren** und dadurch über **$930.000** an Kosten für Level-1-SOC-Prozesse einsparen konnte. Zugleich waren nach drei Jahren sowohl ein **70-prozentiger Rückgang der Vorfälle mit anschließenden SecOps-Untersuchungen** als auch eine **Senkung der mittleren Behebungsdauer um 85 %** feststellbar. Dadurch wurde ein geschätzter Mehrwert von über **$1,2 Mio.** realisiert.[5]

Außerdem straffen die agentische KI und die leistungsstarken Automatisierungsfunktionen von XSIAM alle bei akuten Sicherheitsvorfällen eingeleiteten Reaktionsprozesse. Die Plattform automatisiert die Integration, Analyse und Ersteinstufung von Daten und erspart Ihren Analysten damit einen erheblichen Teil des manuellen Aufwands. Ihr Team kann sich nun auf das Wesentliche konzentrieren, nämlich die Bearbeitung von Vorfällen mit hoher Priorität, die menschliche Expertise erfordern.

Die sofort einsatzbereiten KI-Modelle von XSIAM 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. Durch die Gruppierung von Alarmen und die KI-gestützte Vorfallsbewertung kann XSIAM nicht sicher beurteilbare Ereignisse zu zuverlässig klassifizierbaren Vorfällen zusammenfassen. Bei dieser Priorisierung wird das Gesamtrisiko berücksichtigt, sodass Ihr Sicherheitsteam seine Aufgaben effizienter erledigen kann.

Darüber hinaus liefert die kontinuierliche Erfassung, Verknüpfung und Normalisierung von Rohdaten auf der XSIAM-Plattform weit mehr Informationen als reine Alarme. Ihre SOC-Teams können daher schneller und einfacher Untersuchungen starten sowie entsprechend schneller und effektiver Bedrohungen erkennen und beheben.

Auf diese Weise bringt die Einführung von XSIAM entscheidende Vorteile und Impulse für die Produktivität und die Expertise Ihrer Analysten. Der KI-gestützte Ansatz der Plattform hilft Ihrem Team, Unwichtiges zu ignorieren und sich auf kritische Bedrohungen zu konzentrieren. So beugt XSIAM der Warnungsmüdigkeit vor. Das Ergebnis: Anstatt ihre Zeit mit Routineaufgaben wie der Sichtung von Alarmen zu verbringen, können sich Ihre Analysten auf die Erweiterung ihrer Kompetenzen, die detaillierte Untersuchung von Vorfällen und die proaktive Suche nach Bedrohungen konzentrieren.

Darüber hinaus beschleunigen die Automatisierungsfunktionen von XSIAM die Vorfallsbehebung. Hierfür sind im Cortex Marketplace Hunderte bewährter Content Packs sowie native MCP-Server und nützliche Supportangebote verfügbar, sodass Sie Ihre Sicherheitsinfrastruktur auf einfache Weise vernetzen, wichtige Erkenntnisse integrieren und Reaktionsprozesse unternehmensweit koordinieren können. Dank der eingebetteten Automatisierungsfunktionen sparen 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.

Sie können Automatisierungsfunktionen flexibel hinzufügen und an Ihre Anforderungen anpassen. Die bereitgestellten Playbooks können on-demand, zu festgelegten Zeitpunkten oder bei Eingang bestimmter Warnmeldungen ausgeführt werden, was die schnelle Reaktion auf akute Vorfälle erleichtert und bestehende Risiken minimiert.

Abgesehen davon stellt Ihnen Cortex Agentic Assistant für den Ernstfall ein Team aus KI-Agenten zur Seite, das Sie bei Ihren Untersuchungsprozessen unterstützt und für sämtliche Sicherheitsherausforderungen gewappnet ist. Da die entsprechenden Agenten in XSIAM eingebettet sind, ist die Plattform in der Lage, Cortex AgentiX™ zur Gestaltung und Ausführung komplexer Workflows zu nutzen – und auf diese Weise mühsame manuelle Prozesse durch blitzschnelle, auf Expertenwissen basierende Maßnahmen abzulösen. Dabei erhält Ihr Team schrittweise Anleitungen und kompetente Unterstützung durch kontextbewusste Agenten mit integrierten Kontrollen, was das Tempo und die Präzision Ihrer Reaktionsprozesse deutlich steigert und Ihrem Unternehmen starken Schutz bietet.

All dies und mehr ist möglich mit Cortex AgentiX und seinen personabasierten KI-Agenten, die Ihr Team ohne personelle Aufstockung um praxisbewährte Expertise erweitern. Damit eröffnet sich modernisierungswilligen Unternehmen der Zugang zu den Produkten eines Trainingsdatensatzes, der auf einem Jahrzehnt Erfahrung im Bereich Sicherheitsautomatisierung, globaler Threat Intelligence und 1,2 Milliarden Playbook-Ausführungsprozessen basiert. Zugleich können Analysten Prompts in natürlicher Sprache nutzen, um implementierte Agenten zur ebenso raschen wie zielsicheren Planung und Ausführung komplexer mehrstufiger Aufgaben zu veranlassen.

5. Forrester Consulting, *The Total Economic Impact™*.

SO ERMITTELN SIE, OB CORTEX XSIAM DIE RICHTIGE LÖSUNG FÜR IHRE ORGANISATION IST

Wenn Sie abwägen, ob Cortex XSIAM die richtige Lösung für Ihre Organisation ist, sollten Sie verschiedene Aspekte berücksichtigen. Führen Sie zunächst eine Bewertung Ihrer vorhandenen Sicherheitstools durch und schenken Sie dabei der Komplexität besondere Beachtung. Falls in Ihrer Organisation eine unkontrollierte Ausbreitung von Tools und fehlende Koordination zwischen Arbeitsabläufen für proaktive und reaktive Sicherheitsfunktionen eine Herausforderung sind, dann würden Sie wahrscheinlich von dem konsolidierten Ansatz, den XSIAM bietet, profitieren. Bedenken Sie, wie viel Zeit Ihr Team mit dem Wechsel zwischen verschiedenen Tools und dem manuellen Abgleich von Daten verbringt. Als einheitliche Plattform kann XSIAM diesen Aufwand erheblich reduzieren und die Effizienz steigern.

Bewerten Sie dann den Umfang und die Vielfalt der Daten in Ihrer Organisation. Zu den Stärken von XSIAM gehören die Verarbeitung und die Analyse großer Datenmengen, weshalb die Lösung besonders gut für Organisationen mit komplexen, datenintensiven Umgebungen geeignet ist. Wenn Ihre Daten auf On-Premises- und Cloud-Umgebungen verteilt sind und Sie Schwierigkeiten haben, sich einen Überblick über Ihr Sicherheitsniveau zu verschaffen, kann XSIAM mit seiner Fähigkeit, Daten aus zahlreichen Quellen einzuspeisen und zu analysieren, Ihnen das Leben sehr viel einfacher machen.

In Organisationen mit Cloud- oder Hybridinfrastrukturen ermöglicht die cloudnative Architektur von XSIAM umfassende Einblicke in On-Premises- und Cloud-Assets und erleichtert so den Sicherheitsbetrieb. Viele Organisationen haben damit zu kämpfen, dass ihre vorhandenen Sicherheitstools nicht in der Lage sind, die für Cloud-Umgebungen erforderliche Transparenz und Schutzmechanismen zu bieten. XSIAM weitet Ihre SOC-Funktionen in die Cloud aus und vereinheitlicht den Sicherheitsbetrieb über Ihre gesamte Infrastruktur hinweg.

Ein dritter wichtiger Faktor sind die Complianceanforderungen. Die zuverlässigen Berichtsfunktionen und umfassenden Datenanalysen von XSIAM können Sie dabei unterstützen, die Vielfalt an regulatorischen Vorgaben effektiver zu erfüllen. Machen Sie sich bewusst, wie viel Zeit Ihr Team momentan für Complianceberichte aufwendet und wie XSIAM diese Prozesse straffen könnte.

Dank des KI-gestützten Ansatzes bietet XSIAM eine bessere Bedrohungserkennung als herkömmliche SIEM- und andere Sicherheitsplattformen. Die Konsolidierung von Tools und die gesteigerte Effizienz werden Ihnen aller Voraussicht nach gleich zwei Vorteile bieten: den Abbau betrieblicher Komplexität und erhebliche Kosteneinsparungen. Bei der Analyse des ROI sollten Sie nicht nur die direkten Kosten berücksichtigen, sondern auch die Zeitersparnis für Ihre Analysten und das verbesserte Sicherheitsniveau. Bedenken Sie, wie die automatisierten Funktionen für die Ersteinschätzung und die Einleitung von Abwehrmaßnahmen von XSIAM Ihrem Team eine wesentlich schnellere Erkennung und Eindämmung von Bedrohungen ermöglichen könnten.

Dass diese Vorteile vielerorts bereits Realität sind und über kurz oder lang in messbaren Mehrwerten münden, beweist eine kürzlich veröffentlichte Total Economic Impact™-Studie von Forrester Consulting. Hier zeigte sich, dass Organisationen nach dem Umstieg **einen Drei-Jahres-ROI von 257 %** erzielten und dabei von einer **Amortisationszeit von unter sechs Monaten** profitierten. Den entscheidenden Unterschied machen dabei die deutlich gestrafften Prozesse, die im Interview unter anderem durch einen VP für den Bereich globale Sicherheit hervorgehoben wurden: „Der mittlere Zeitaufwand für die Bedrohungserkennung und -abwehr hat sich um 80 % verringert. Wo früher vier Stunden für die Erkennung und zwei Stunden für die Eindämmung erforderlich waren, sind jetzt nur noch 40–50 Minuten nötig."[6]

> Cortex XSIAM hat unseren Sicherheitsbetrieb auf eine Art und Weise revolutioniert, wie dies mit unserem früheren SIEM-System einfach nicht möglich war. Dank XSIAM sind unsere Abläufe bei der Bedrohungserkennung, -untersuchung und -abwehr nun automatisiert und orchestriert, wodurch wir enorme Produktivitätssteigerungen erzielen und unser Sicherheitsniveau erheblich verbessern konnten.
>
> – Prasanna Siriwardena
>
> Chief Information Officer, LOLC Holdings PLC

6. Forrester Consulting, *The Total Economic Impact™*.

Vorteile von XSIAM gegenüber einer SIEM-Lösung

Zeitersparnis: Herkömmliches SIEM und XSIAM im Vergleich

SIEM XSIAM

Dynamische Bedrohungserkennung

Kontinuierliche Prozesse schaffen neue Alarme, die sich flexibel an die Bedrohungslandschaft anpassen.

100
Std./Woche eingespart

Die Entwicklungsprozesse bei der Bedrohungserkennung werden größtenteils vom XSIAM-Team übernommen.

Alarmanpassung

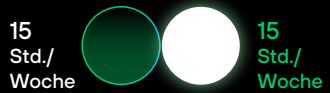
Kontinuierliche Prozesse verbessern die Qualität der Alarme basierend auf der Zuverlässigkeit früherer Alarme.

72
Std./Woche eingespart

Auslagerung der Feineinstellung der Endpunktalarme an das XSIAM-Forschungsteam.

Wartung des Systems

Protokollanalyse, Patchen des Servers usw.



Keine Veränderung

Analysen

Es werden fortschrittliche Alarme unter Berücksichtigung komplexer Statistiken und ML-Prozesse erstellt.

SIEM

[Funktionsmangel]
Dies erfordert ein Add-on-Paket und ein BYOML-Modell. Die Normalisierung ist schwierig.

XSIAM

[Neue Funktion]
XSIAM nutzt Statistiken und ML für die automatisierte Festlegung des Normalverhaltens und die Anomalieerkennung.

Zeitersparnis insgesamt:
4,5 VZÄ
weniger Arbeitsaufwand

Abbildung 2: Zeitersparnis mit XSIAM im Vergleich zu einem herkömmlichen SIEM-System

Bevor Sie XSIAM implementieren, sollten Sie überprüfen, ob Ihre Organisation auf die Einführung KI-gestützter SecOps-Prozesse vorbereitet ist. Bewerten Sie die aktuellen Kompetenzen und Abläufe Ihres Teams und schaffen Sie das Fundament für eine neue Art des Sicherheitsbetriebs.

XSIAM kann SecOps-Abläufe erheblich verbessern, aber das erfordert möglicherweise eine Anpassung der Arbeitsweise Ihres Teams. Bedenken Sie, dass die Umstellung auf eine neue, KI-gestützte Plattform ein gewisses Maß an Einarbeitung und Änderungsmanagement mit sich bringt.

ZUKUNFTSSICHERE SECOPS

Cortex XSIAM spielt eine entscheidende Rolle bei der Umsetzung moderner Sicherheitsstrategien wie Zero Trust, Secure Access Service Edge (SASE) und Security Service Edge (SSE). Die umfassende Transparenz und die fortschrittlichen Analysefunktionen der Plattform sind die perfekte Ergänzung dieser Ansätze, um Ihren Sicherheitsbetrieb für die Zukunft aufzustellen. Bei der Umstellung auf eine Zero-Trust-Architektur bietet XSIAM detaillierte Einblicke in das Verhalten von Benutzern und Objekten, die Ihnen die Implementierung und Aufrechterhaltung eines belastbaren Zero-Trust-Modells erleichtern.

Des Weiteren vereint die Plattform reaktive Incident-Response-Maßnahmen mit einem proaktiven Management des Sicherheitsniveaus. Durch die Bereitstellung der folgenden Funktionen deckt sie die beiden wichtigsten Risikobereiche für Unternehmen ab:

- **Cortex Exposure Management:** Eliminiert mit KI-gestützter Priorisierung und automatisierten Behebungsmaßnahmen in unternehmensinternen Cloud-Umgebungen 99 % der irrelevanten Meldungen zur Angriffsfläche. Dieser disruptive Ansatz konzentriert sich auf die Schwachstellen, für die es aktiv genutzte Exploits und keine ausgleichenden Kontrollen gibt, sodass Sie den 0,01 % der gefährlichsten Bedrohungen die höchste Priorität einräumen können.
- **Cortex Email Analytics:** Stoppt ausgefeilte Phishingversuche und E-Mail-basierte Angriffe mit einer Kombination aus LLM-basierten Analysen und branchenführender Bedrohungserkennung und -abwehr. Dies ist ein entscheidender Vorteil, da ein Großteil der Kommunikation weiterhin per E-Mail erfolgt und die Anzahl der Benutzer dieser Technologie Prognosen zufolge im Jahr 2030 bei fünf Milliarden liegen wird.[7] Zudem zählt dieser Kanal nach wie vor zu den wichtigsten Zielen der Kriminellen. Cortex Email Analytics schafft hier Abhilfe, indem es schädliche E-Mails automatisch entfernt, kompromittierte Benutzerkonten deaktiviert und betroffene Endpunkte in Echtzeit isoliert.

Die Skalierbarkeit von XSIAM stellt sicher, dass auch steigende Datenmengen verarbeitet werden können und neue Arten von Gefahren zuverlässig erkannt werden, wenn Ihre Organisation wächst und sich die Bedrohungslandschaft weiterentwickelt. Die KI-Modelle und Detektoren von XSIAM werden kontinuierlich aktualisiert, um stets die neueste Threat Intelligence und modernste Erkennungsfunktionen zur Verfügung zu stellen. So sind Sie jederzeit vor neuen Bedrohungen geschützt, ohne dass Ihr Team die Sicherheitstools manuell aktualisieren und neu konfigurieren muss.

XSIAM lernt auch aus den manuellen Aktionen der Analysten und macht Vorschläge zu Prozessen, die in Zukunft automatisch erledigt werden könnten. Damit verbessert sich nicht nur die Fähigkeit der Plattform, Vorfälle automatisch zu beheben, sondern auch die Effizienz und Genauigkeit. So wird das Sicherheitsniveau Ihrer Organisation Tag für Tag gestärkt.

Parallel dazu nutzt XSIAM ausgereifte, auf Sicherheitsanwendungen zugeschnittene ML-Datenmodelle, um große Datenmengen aus verschiedenen Quellen zusammenzuführen und automatisch zu normalisieren und dadurch letztlich die Bedrohungserkennung zu stärken. Grundlage dieser Modelle sind verhaltensbezogene Trainingsdaten, die aus Zehntausenden Umgebungen stammen und für Lernprozesse rund um die trennscharfe Unterscheidung zwischen Anomalien und schädlichen Aktivitäten herangezogen werden. So lassen sich False Positives minimieren und die Erkennungs- und Abwehrfunktionen verbessern, sodass Angriffe verhindert werden, bevor Schäden entstehen.

Darüber hinaus können Sie dank des BYOML-Features (Bring-your-own-ML) von XSIAM eigene ML-Tools in die Plattform integrieren. Dies ermöglicht die ML-gestützte Bedrohungssuche unter Nutzung der in XSIAM zusammengeführten und normalisierten Daten – für eine noch effektivere Bedrohungserkennung und -abwehr.

Finanzielle Vorteile der Konsolidierung

Basierend auf der von Forrester Consulting erstellten Studie *The Total Economic Impact™ of Palo Alto Networks Cortex XSIAM*:[8]

$3,1 Mio.
Einsparungen durch die Ablösung von mehr als 20 alten Tools (über drei Jahre)

$2,2 Mio.
Mehrwert durch ein um 60 % verbessertes Sicherheitsniveau

$5,6 Mio.
Nettobarwert über drei Jahre

In Anbetracht all dieser Vorteile steht außer Zweifel, dass Sie durch den Umstieg auf XSIAM nicht nur die Sicherheitsherausforderungen von heute meistern, sondern Ihr Unternehmen auch für die Anforderungen von morgen wappnen. Ein zukunftsgerichteter Ansatz wie dieser gibt Ihnen die Gewissheit, dass Ihre Organisation in der sich ständig weiterentwickelnden Bedrohungslandschaft langfristig geschützt ist. Zudem sorgen Sie mit dem anpassungsfähigen, KI-gestützten Ansatz von XSIAM dafür, dass sich Ihre IT-Infrastruktur flexibel und effektiv an neue Bedrohungen anpassen lässt und Ihr Team im Ernstfall schnell reagieren kann.

Kurz: XSIAM versetzt Ihr SOC in die Lage, das Sicherheitsniveau Ihrer Organisation jeden Tag ein wenig zu heben.

Ein besonders wichtiger Aspekt von XSIAM ist, dass sich die Lösung mittels KI und ML kontinuierlich verbessert. Anhand neuer Daten und Informationen zu Angriffstechniken optimiert sie fortlaufend ihre Erkennungs- und Abwehrfunktionen. So passen sich Ihre SecOps-Abläufe ganz ohne manuelle Eingriffe an neue Bedrohungen und Muster an und werden im Laufe der Zeit immer effektiver.

7. *E-Mail-Statistiken für den Zeitraum 2025-2030*, cloudHQ, 24. April 2025.
8. Forrester Consulting, *The Total Economic Impact™*.

STRATEGIEN ZUR VERBESSERUNG IHRER SOC-KENNZAHLEN

Mit seinem revolutionären Ansatz verbessert Cortex XSIAM nicht nur Kennzahlen wie MTTD (Mean Time to Detect) und MTTR (Mean Time to Respond), sondern auch den Sicherheitsbetrieb insgesamt. Innovative KI- und ML-Funktionen unterstützen XSIAM bei der Automatisierung der aufwendigen Integration und Analyse von Daten und ermöglichen Ihrem Team, Bedrohungen nahezu in Echtzeit zu erkennen. So können Ihre Sicherheitsprofis potenzielle Sicherheitsverstöße schneller denn je aufdecken und Angreifer stoppen, bevor sie schweren Schaden anrichten.

Doch die erfolgreiche Aufdeckung eines Angriffs ist lediglich der Auftakt zu einer umfassenden Untersuchung. Der automatisierungsorientierte Ansatz von XSIAM reduziert stundenlange manuelle Analyseprozesse auf wenige Minuten und beschleunigt so die Incident-Response-Maßnahmen.

Anstatt ihre kostbare Zeit mit manueller Ersteinschätzung oder der Korrelierung von Daten aus unterschiedlichen Quellen zu vergeuden, können sich Ihre Analysten dank der KI-gestützten Vorfallsbewertung und intelligenten Alarmgruppierung nun auf wirklich wichtige Aufgaben konzentrieren.

Und da die Plattform einen einheitlichen Ansatz für reaktive und proaktive Sicherheitsmaßnahmen unterstützt, können Ihre Teams nicht nur schneller auf Vorfälle reagieren, sondern sie in vielen Fällen sogar von vornherein vermeiden. Abgesehen davon ist XSIAM durch die direkte Integration von Exposure Management und Email Analytics in die SOC-Plattform in der Lage, zwei der meistgenutzten Angriffsvektoren mit denselben konsolidierten Daten, KI-Modellen und Automatisierungsfunktionen abzudecken.

Somit kann Ihr Team automatisierte Playbooks und die von Cortex AgentiX bereitgestellten Agenten nutzen, um schnell und entschieden gegen Bedrohungen vorzugehen und die MTTR drastisch zu senken. Ein vielleicht noch größerer Vorteil ist, dass XSIAM kontinuierlich dazulernt und sich an Ihre Umgebung anpasst, wodurch sich Ihr Sicherheitsniveau stetig verbessert. Die innovativen KI-Modelle der Plattform entwickeln sich in Reaktion auf neue Bedrohungen weiter, damit Sie sicher sein können, dass Sie Angreifern immer einen Schritt voraus bleiben.

Dadurch verbessern Sie nicht nur in kürzester Zeit die MTTD und MTTR, sondern sichern Ihre Infrastruktur auch in Bezug auf zukünftige Herausforderungen ab. Mit Cortex XSIAM navigieren Sie zuverlässig in der komplexen Cyber-Sicherheitslandschaft, da Sie wissen, dass sich Ihre geschäftskritischen SOC-Kennzahlen ständig verbessern und Ihre wertvollsten Assets geschützt sind.

Neue Forschungsarbeiten belegen diese Vorteile mit Zahlen und Fakten. Beispielsweise ist die Anzahl der vierteljährlich bei einem spezialisierten Einzelhändler eingehenden Alarme nach Angaben des Leiters der Abteilung SecOps **von 25.000 auf 4.500 zurückgegangen**. Zugleich dokumentiert eine auf Kundeninterviews basierende Studie, dass ein repräsentatives Unternehmen für die Bereitstellung von XSIAM **drei Vollzeitbeschäftigte über einen Zeitraum von drei Monaten** benötigt, während sich der **personelle Aufwand für die laufende Wartung und Pflege auf eine halbe Vollzeitstelle beschränkt**.[9]

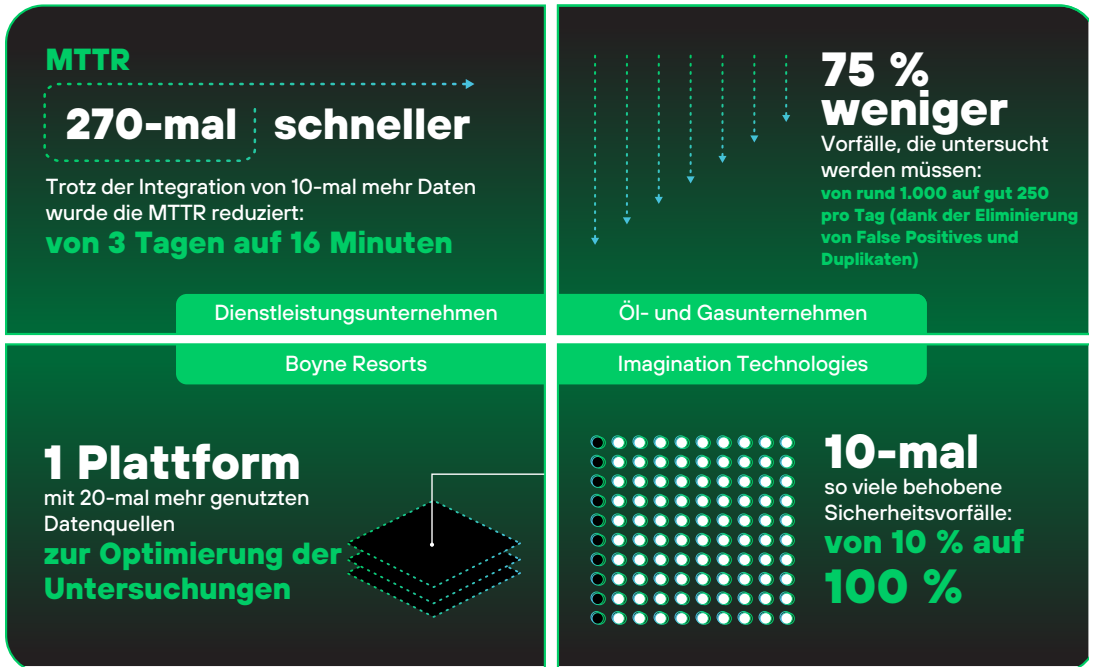


Abbildung 3: Kundenbeispiele für messbare Verbesserungen mit XSIAM

> Wir betrachten XSIAM – und die Integration zahlreicher Funktionen in eine zentrale, einheitliche Plattform – als nächsten Schritt für das SOC der kommenden Generation. Von XSIAM erhoffen wir uns ein höheres Maß an Automatisierung und eine stärkere Unterstützung für unser Cyber-Sicherheitsteam.
>
> – Rob Jillson
>
> Head of Cybersecurity, Resolution Life Australasia

9. Forrester Consulting, *The Total Economic Impact™*.

IST CORTEX XSIAM DIE RICHTIGE LÖSUNG FÜR IHRE ORGANISATION?

1. Aktuelle Herausforderungen im SOC

- ☐ Haben Sie bei Ihrem derzeitigen SIEM-System mit komplexen Konfigurationen zu kämpfen?
- ☐ Müssen Sie zeitaufwendige Integrationen zwischen Sicherheitstools einrichten?
- ☐ Ist Ihr Team mit einer Unmenge an Alarmen konfrontiert?
- ☐ Verursachen isolierte Sicherheitstools Ineffizienzen?
- ☐ Fehlt die Verbindung zwischen Ihren proaktiven Sicherheitsfunktionen und den reaktiven Incident-Response-Maßnahmen?

2. Bedrohungserkennung und -abwehr

- ☐ Sind Sie maßgeblich auf statische Korrelationsregeln angewiesen?
- ☐ Muss Ihre Echtzeiterkennung optimiert werden?
- ☐ Verursachen fehlende Integrationsoptionen Verzögerungen bei der Incident Response?
- ☐ Ist der Anteil der False Positives zu hoch?

3. Datenmanagement

- ☐ Verarbeiten Sie große Mengen unterschiedlicher Sicherheitsdaten?
- ☐ Gibt es in Ihrer Organisation eine Mischung aus On-Premises- und Cloud-Daten?
- ☐ Benötigen Sie bessere Funktionen für die Normalisierung und Korrelierung von Daten?

4. KI- und Automatisierungsanforderungen

- ☐ Haben Sie die Absicht, KI zur Verbesserung der Bedrohungserkennung zu nutzen?
- ☐ Beabsichtigen Sie, Routineaufgaben im Sicherheitsbereich zu automatisieren?
- ☐ Hat die Reduzierung des manuellen Aufwands bei der Vorfallseinschätzung Priorität?
- ☐ Benötigen Sie eine KI-gestützte Priorisierung von Schwachstellen, um der vielen Alarme Herr zu werden?

5. Anforderungen an eine einheitliche Plattform

- ☐ Müssen Sie mehrere Sicherheitsfunktionen konsolidieren (SIEM, EDR, XDR, SOAR, Schwachstellenmanagement und andere)?
- ☐ Suchen Sie nach einer zentralen Plattform für die Verwaltung aller SecOps-Abläufe?
- ☐ Möchten Sie proaktive und reaktive Sicherheit miteinander verbinden?

6. Cloud- und Hybridumgebungen

- ☐ Nutzen Sie Cloud- oder Hybridumgebungen?
- ☐ Benötigen Sie mehr Transparenz in Bezug auf Ihre On-Premises- und Cloud-Assets?

7. Compliance und Berichterstellung

- ☐ Wünschen Sie sich bessere Funktionen für Complianceberichte?
- ☐ Benötigen Sie umfassendere Datenanalysen für regulatorische Zwecke?

8. Skalierbarkeit

- ☐ Müssen Sie größere Datenmengen verarbeiten, weil Ihre Organisation wächst?
- ☐ Benötigen Sie eine Lösung, die sich an neue Bedrohungen anpassen kann?

9. Erweiterte Analysen

- ☐ Haben Sie Interesse an KI-gestützten Vorfallsbewertungen und Alarmgruppierungen?
- ☐ Ist Ihr Abgleich von Ereignissen aus verschiedenen Datenquellen verbesserungswürdig?
- ☐ Möchten Sie KI zur Priorisierung der gefährlichsten Schwachstellen nutzen?

10. Bereitschaft Ihres Teams

- ☐ Ist Ihr Team bereit, auf KI-gestützte SecOps-Prozesse umzustellen?
- ☐ Sind Sie bereit, in Schulungen für eine neue, moderne Plattform zu investieren?

11. Absicherung für die Zukunft

- ☐ Planen Sie, auf Zero-Trust-, SASE- oder SSE-basierte Sicherheitsmodelle umzusteigen?
- ☐ Benötigen Sie eine Lösung, die sich mittels KI und ML selbst optimiert?

12. Kundenspezifische ML-Integrationen

- ☐ Möchten Sie Ihre eigenen ML-Tools integrieren?

13. E-Mail- und Sicherheitslückenmanagement

- ☐ Benötigen Sie stärkeren Schutz vor raffinierten, E-Mail-basierten Bedrohungen?
- ☐ Haben Sie Probleme mit der zeitnahen Behebung und Priorisierung von Sicherheitslücken?
- ☐ Würden Sie von einer automatischen Beseitigung kritischer Schwachstellen profitieren?

Wenn Sie einen Großteil der Fragen mit „**Ja**“ beantwortet haben (insbesondere bei Aspekten, die sich auf die konkreten Sicherheitsherausforderungen und -ziele Ihrer Organisation beziehen), dann ist Cortex XSIAM wahrscheinlich die passende Lösung für Ihr SOC.

Verlieren Sie keine Zeit!

Entdecken Sie, wie Cortex XSIAM Abläufe vereinfacht, Bedrohungen umgebungsweit abwehrt, proaktive und reaktive Sicherheit vereint und die Vorfallsbehebung beschleunigt – heute und in Zukunft.

Nehmen Sie Kontakt mit uns auf →

Über Cortex XSIAM

Cortex XSIAM ist eine KI-gestützte SecOps-Plattform für moderne SOCs, die mithilfe von KI 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.

Cortex XSIAM vereint erstklassige SecOps-Funktionen für EDR, XDR, SOAR, ASM, UEBA, TIP und SIEM. Alle Sicherheitsdaten werden bei XSIAM an einer zentralen Stelle zusammengefasst. Darüber hinaus kommen eigens für Sicherheitsaspekte konzipierte Datenmodelle für das maschinelle Lernen zum Einsatz. Mit XSIAM lassen sich Datenintegration, Analysen und Abwehrmaßnahmen automatisieren, sodass sich die Analysten wieder auf die tatsächlich relevanten Vorfälle konzentrieren können. Weitere Informationen über Cortex XSIAM finden Sie unter www.paloaltonetworks.de/cortex/cortex-xsiam.

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

cortex_ebook_cortex-xsiam-buyers-guide_102125