Ein praktischer Leitfaden zur Umsetzung von Zero Trust im SOC

Ein Überblick über kritische Assets und kontinuierliche Überwachung bringen Ihre Zero-Trust-Strategie voran

paloalto NETWORKS | CORTEX BY PALO ALTO NETWORKS

Inhalt

Einleitung

SOC-Teams, also die unternehmensinternen Fachabteilungen für Sicherheitsprozesse oder Security Operations Center, haben aus historischen Gründen vorrangig den Netzwerkrand, den sogenannten Perimeter, im Blick. Doch ein solcher Ansatz funktioniert nicht mehr. Der Schutz, den die eingesetzten Sicherheitsinfrastrukturen und -systeme bieten, muss über den Netzwerkperimeter hinausgehen. Es müssen auch Public-/Private-Cloud-Umgebungen und alle angebundenen Geräte und Endpunkte erreicht werden. Nur so können laufende Aktivitäten und das Benutzerverhalten geprüft werden, um Cybervorfälle und Datenlecks zu verhindern. Eingebettete Systeme, IoT-Geräte und eine (nahezu) allgegenwärtige WLAN-Abdeckung bedeuten, dass Unternehmen mittlerweile großflächig angreifbar sind. Dementsprechend müssen sie ihre Definition von Vertrauenswürdigkeit den modernen Technologielandschaften anpassen.

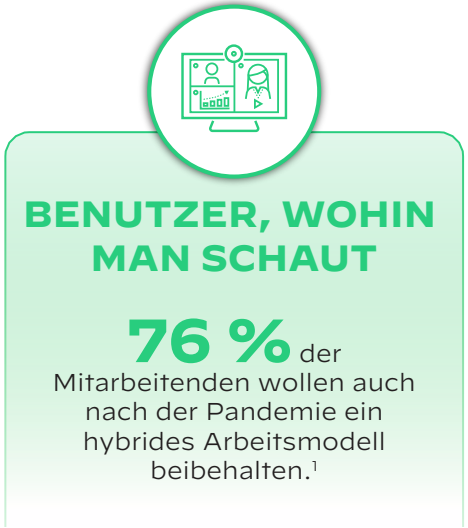
Folgende Faktoren vergrößern die Angriffsfläche zusätzlich: ein der Pandemie geschuldeter plötzlicher Übergang zu mobiler Arbeit oder hybriden Arbeitsmodellen, die Verlagerung von Anwendungen und Daten in die Cloud und an andere Standorte sowie der ungebrochene Zuwachs an vernetzten „Smart"-Geräten.

Das Konzept von Zero Trust gibt es schon länger. Es stammt vom Forrester-Analysten John Kindervag, der damit den Umgang mit Bedrohungen beschrieb, denen mit herkömmlichen Sicherheitsmaßnahmen nicht beizukommen ist. Gemäß diesem neuen Modell musste man davon ausgehen, eine bisher „vertrauenswürdige" Infrastruktur sei möglicherweise infiltriert und potenziell gefährlich. Diese Einstellung änderte die Herangehensweise an IT-Sicherheit von Grund auf.

Grob gesagt basiert ein Zero-Trust-Modell auf der strikten, ständigen Prüfung und Validierung aller Personen, Geräte oder Institutionen, die versuchen, auf Netzwerkressourcen zuzugreifen. Das vorrangige Ziel ist es, Manipulationen von Daten, Anwendungen und geschäftskritischen Systemen durch Angriffe und Exploits zu verhindern.

Alle Zero-Trust-Prinzipien sollen dabei helfen, die Bedrohungsrisiken zu verringern und den nicht autorisierten Zugriff zu verhindern. Sie wurden speziell entwickelt, um die Sicherheit kritischer Anwendungen und sensibler Daten in Unternehmen zu gewährleisten, und lassen sich ganz einfach in jede Sicherheitsstrategie integrieren. Zu den Prinzipien gehören unter anderem:

- **Multifaktor-Authentifizierung (MFA)**: Dabei müssen sich Einzelpersonen mit mehreren Sicherheitsverfahren authentifizieren. In der Regel handelt es sich um eine Kombination aus etwas, das man kennt (zum Beispiel ein Passwort oder eine PIN), etwas, das man besitzt (wie einen Handsender oder einen Ausweis), und physischen Merkmalen wie biometrischen Daten, der Stimme (bei der Spracherkennung) oder einem Fingerabdruck.



1. *The State of Hybrid Workforce Security*, Palo Alto Networks, 25. August 2021

- **Least-Privilege-Richtlinie**: Mit dieser Richtlinie erhalten Endbenutzer nur minimale Zugriffsrechte, d. h. nur jene, die sie für ihre Arbeit benötigen. Dadurch wird die Anzahl der Pfade reduziert, über die Angreifer in eine Infrastruktur eindringen, Malware ein- oder Daten ausschleusen können.
- **Mikrosegmentierung**: Das Netzwerk wird in separate Segmente bzw. in Rechenzentren oder Cloud-Umgebungen in „sichere Zonen“ mit eigenen Anmeldedaten unterteilt, um die Benutzer, Geräte und sogar Workloads zu isolieren. Dadurch wird Eindringlingen zudem die Ausbreitung in internen Netzwerken erschwert.

Was ist Zero Trust? Ein strategischer Cybersicherheitsansatz, der beim Zugriff auf Unternehmensressourcen völlig auf implizites Vertrauen verzichtet und jede Phase digitaler Interaktionen kontinuierlich prüft und verifiziert.

Für Zero Trust müssen zunächst die Identitäten der Benutzer verifiziert und validiert werden.

- Jedes Element Ihrer Sicherheitsarchitektur muss einzelne Benutzer blockieren oder zulassen können.
- An jedem Zugangspunkt in Ihrer Sicherheitsarchitektur muss sich die Identität eines Benutzers verifizieren lassen.

Zero Trust für Anwendungen verfolgt einen sehr ähnlichen Ansatz.

- Wir müssen die Identitäten der Benutzer, die auf geschützte Anwendungen zugreifen möchten, auf den Prüfstand stellen.
- Darüber hinaus muss sich der Zugang zwischen Anwendungen und Workloads sowie die betreffende Transaktion validieren lassen, damit sichergestellt ist, dass der Content dieser Anwendungen – egal, ob sie sich in der Private Cloud, Public Cloud oder anderswo befinden – nicht schädlich ist.

Genauso strikt muss die Infrastruktur geschützt sein. Validieren Sie daher die Identität der Benutzer, die sich mit der Infrastruktur verbinden möchten.

- IoT-Geräte sind oft nicht mit nativen Sicherheitsfunktionen ausgestattet und stellen daher ein erhebliches Sicherheitsrisiko dar, das sich durch Identitätsprüfungen aber beherrschen lässt.
- Sie müssen alle mit dem Internet verbundenen Assets und alle Änderungen an vorhandenen Assets kontinuierlich erkennen und überwachen, um alle Risiken und Schwachstellen im Blick zu behalten.
- Der Zugriff und Transaktionen müssen ebenfalls auf diese Weise gesichert werden.
- Gewähren Sie nur Least-Privilege-Zugriff, segmentieren Sie die Umgebung und überwachen Sie die Transaktionen in nativen und Drittanbieterinfrastrukturen.
- Prüfen Sie sämtliche Inhalte in der Infrastruktur auf schädliche Aktivitäten und Datendiebstahl.

	Identität	Gerät/Workload	Zugriff	Transaktion
Zero Trust für Benutzer	Validiert Benutzer mithilfe einer starken Authentifizierung	Verifiziert die Integrität des Benutzergeräts	Setzt das Least-Privilege-Prinzip beim Benutzerzugriff auf Daten und Anwendungen durch	Prüft sämtliche Inhalte auf schädliche Aktivitäten und Datendiebstahl
Zero Trust für Anwendungen	Validiert Entwickler, DevOps-Mitarbeiter und Administratoren mithilfe einer starken Authentifizierung	Verifiziert die Integrität der Workloads	Setzt das Least-Privilege-Prinzip beim Zugriff von Workloads auf andere Workloads durch	Prüft sämtliche Inhalte auf schädliche Aktivitäten und Datendiebstahl
Zero Trust für die Infrastruktur	Validiert alle Benutzer mit Zugriff auf die Infrastruktur	Identifiziert alle Geräte, einschließlich IoT-Geräten	Segmentierung für Least-Privilege-Zugriffsrechte in nativen und Drittanbieterinfrastrukturen	Prüft sämtliche Inhalte in der Infrastruktur auf schädliche Aktivitäten und Datendiebstahl

Abbildung 1: Ein Zero-Trust-Unternehmen erfordert einen umfassenden Ansatz, der Benutzer, Anwendungen und Infrastrukturen einschließt.

ANWENDUNGEN, WOHIN MAN SCHAUT

80 % der Unternehmen haben eine hybride Cloud-Strategie[2] und ein typisches Unternehmen nutzt im Schnitt 110 SaaS-Apps.[3]

Ein ganzheitlicher Zero-Trust-Ansatz und die Rolle des SOC

Zero Trust ist ein fortlaufender Prozess, der kontinuierlich an neue geschäftliche Anforderungen des Unternehmens und den zugehörigen technologischen Wandel angepasst werden muss – insbesondere im Zuge von Initiativen zur digitalen Transformation. Dementsprechend liegt jeder Zero-Trust-Strategie eine Kernaufgabe zugrunde: die Bedrohungslandschaft ständig im Blick zu behalten. Zudem sollten Sie gleich mehrere Sicherheitstools zur Überwachung Ihrer gesamten Infrastruktur nutzen. Deshalb ist das SOC entscheidend für eine effektive, immer auf dem Prüfstand stehende Zero-Trust-Sicherheit.

Wichtige Aufgabengebiete des SOC:

- Kontinuierliche Überprüfung von Zero-Trust-Richtlinien
- Erkennen von Lücken in der Zero-Trust-Strategie
- Eindämmung der Folgen eines Angriffs durch automatisierte Maßnahmenerzwingung
- Beschleunigte Untersuchung durch automatisch erfasste Bedrohungsdaten
- Kontinuierliche Erkennung kritischer Assets

Ein Beispiel wäre ein Unternehmen, das MFA einführt, um Benutzer zweifelsfrei identifizieren zu können und ihnen Zugriff auf Anwendungen zu ermöglichen. Das SecOps-Team analysiert Benutzeraktivitäten mit maschinellem Lernen, Verhaltensanalysen und personengebundenen Informationen, um Insiderbedrohungen aufzuspüren und böswilligen Benutzern durch das Deaktivieren ihrer Konten das Handwerk zu legen. Doch eine ausgereifte Zero-Trust-Strategie zur Absicherung von Benutzern, Anwendungen und Workloads ist noch nicht alles. Unternehmen benötigen trotzdem ein SOC, um Bedrohungen zu erkennen und abzuwehren, Prozesse zu automatisieren und Risiken zu mindern.

Als Erstes sollten Unternehmen ermitteln, wie umfangreich Zero Trust im Benutzerstamm, unter Anwendungen und in der Infrastruktur umgesetzt werden muss. Das SOC ist optimal aufgestellt, um ein breites Spektrum an sicherheitsbezogenen Daten zu verarbeiten, kontinuierliche Überwachung zu leisten sowie Zero-Trust-Kontrollmaßnahmen – Validierung und Verifizierung – umzusetzen.

Die Transformation des SOC – unverzichtbar für modernes Zero Trust

Für die erfolgreiche Umsetzung einer Zero-Trust-Strategie müssen SOC-Teams niedrige Schwellenwerte für Erkennungsalarme ansetzen. Dies führt unweigerlich zu einem Anstieg der Alarmmeldungen. Multipliziert mit den durchschnittlich mindestens 30 Tools in einem SOC

2. *2021 State of the Cloud Report*, Flexera, März 2021.
3. „Average number of SaaS apps used by organizations worldwide 2015-2020“, Statista, 16. Februar 2022.

wird klar, welche Flut an irrelevanten Meldungen und Fehlalarmen auf die Dashboards der Analysten zukommt.

Denn ein Tool ist zwar in der Lage, Alarme auszugeben, doch um festzustellen, ob es sich um legitime Warnungen oder False Positives handelt, sind Analysten nötig. Dementsprechend müssen SOC-Analysten für die Untersuchung und Validierung eines *einzigen* Alarms mitunter enorm viel Zeit aufwenden, was in keinem Verhältnis zum Ergebnis steht. Dabei können auch noch mehr Tools – oft nicht vernetzt – zum Einsatz kommen, um genügend Informationen zu sammeln, bis endlich klar wird, ob ein Alarm weitergeleitet werden muss.

Was fehlt, sind aussagekräftige Kontextinformationen zur Feststellung des Problems. Und so geht noch mehr Zeit damit verloren, relevante Daten zu suchen und in Protokollen zu recherchieren, um hoffentlich Alarme zuordnen zu können, die eventuell gar nichts miteinander zu tun haben. Wenn all das zusammenkommt – isoliert betrachtete verdächtige Aktivitäten, die unkontrollierte Ausbreitung von Tools und Personallücken im Sicherheitsbereich –, dann brauchen Unternehmen dringend eine bessere Perspektive für die Verteidigung und Absicherung ihrer kritischen Infrastrukturen.

Moderne Cyberbedrohungen entwickeln sich zudem schneller als die zu ihrer Abwehr eingesetzten Technologien. Immer mehr Hackergruppen investieren in neue Methoden wie maschinelles Lernen, Automatisierung und künstliche

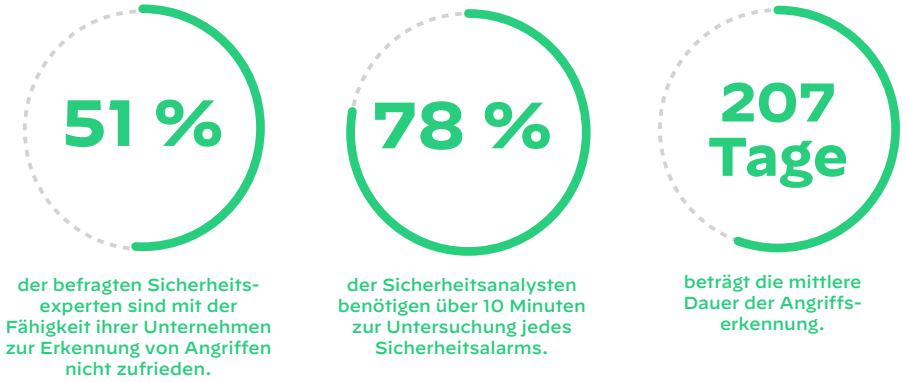


Abbildung 2: Etablierte Sicherheitsstrategien funktionieren nicht mehr.

Intelligenz. SOCs, die in erster Linie herkömmliche SIEM-Systeme (Security Information and Event Management) nutzen, verfügen dagegen nicht über ausreichend flexible und skalierbare Lösungen, die mit der digitalen Transformation, Cloud-Initiativen *und* komplexen Angriffen Schritt halten können. Herausforderungen wie False Positives, die kostenintensive Speicherung enormer Mengen an Ereignisdaten, inadäquate Untersuchungsmethoden sowie hybride und Multi-Cloud-Architekturen bzw. die wachsende Anzahl neuer Geräte und Endpunkte können Sicherheitsanalysten bei der Erkennung und Abwehr kritischer Bedrohungen überfordern.

Zu den Problemen rund um konventionelle SOC-Umgebungen gehören:

- Fehlende Transparenz und Kontextdaten
- Zunehmende Komplexität der Untersuchungsabläufe
- Alarmmüdigkeit und Personalüberlastung aufgrund der Vielzahl unspezifischer Alarmmeldungen
- Mangelnde Interoperabilität der Systeme
- Mangelnde Automatisierung und Orchestrierung
- Hindernisse bei der Erfassung, Verarbeitung und Kontextualisierung von Threat Intelligence

Die Zukunft im Blick: KI, Automatisierung und Orchestrierung nutzen

Ein Unternehmen, das Zero Trust erreichen möchte, muss zunächst eine einheitliche Sicherheitsrichtlinie aufstellen. Im ersten Schritt werden hierfür kritische Assets ermittelt und eine Zero-Trust-Architektur mit striktem Least-Privilege-Zugriff für Benutzer, Anwendungen und Infrastruktur implementiert.

Automatisierung von Arbeitsabläufen

Sicherheitsverantwortliche müssen überlegen, ob ein Tool von einem Menschen konfiguriert oder bedient werden muss. Ist für die Auslegung und Klassifizierung der Ergebnisse ein Experte erforderlich? Müssen etwaige Tests manuell durchgeführt werden? Sicherheitsverantwortliche können einfache, repetitive Aufgaben definieren, deren automatisierte Durchführung im Kontext menschlicher Entscheidungen dazu beitragen können, die Untersuchung von Vorfällen zu beschleunigen.

Die Fortschritte in den Bereichen maschinelles Lernen und künstliche Intelligenz sind vielversprechend. Dennoch ist für eine reibungslose SOC-Transformation der menschliche Input beim Wissenstransfer in alle Richtungen unverzichtbar. Mit zunehmender Reife von Automatisierungsfunktionen können und sollten Menschen für immer kleinere Abschnitte eines Arbeitsablaufs verantwortlich sein.

Fünfjahresausblick zum Thema Automatisierung

Neue SOCs können vom ersten Tag an automatisieren, wohingegen die Einführung der Automatisierung in älteren SOCs Upgrades erfordert und geplant werden muss. Als realistisches Dreijahresziel für eine etablierte Einrichtung sehen wir die Automatisierung von 50 % der SOC-Abläufe. Im fünften Jahr können ca. 75 % der Aufgaben automatisiert ablaufen. Für Tätigkeiten wie die proaktive Bedrohungssuche werden jedoch weiterhin Spezialisten benötigt.

Abläufe in den Bereichen Security Operations (SecOps) und Incident Response (IR), einschließlich der Überwachung relevanter Datenfeeds, erfordern noch zu viele manuelle Eingriffe. Deshalb kann die Investition in Lösungen für Sicherheitsorchestrierung, -automatisierung und -reaktion (SOAR) oder vergleichbare Automatisierungslösungen zur Verbesserung der Orchestrierung von Maßnahmen im gesamten Technologiestack sowie zur Beschleunigung und Skalierbarkeit der IR beitragen.

Ergänzung manueller Abläufe durch ML

Eine Schlüsselkomponente der SOC-Transformation für Zero Trust ist die Bereitstellung umfassender Funktionen für maschinelles Lernen, um die menschliche Arbeit in der IT-Sicherheit zu unterstützen und zu ergänzen. Moderne Analyseverfahren und KI können den Zeitaufwand für die Verarbeitung großer Datenmengen zur Gewinnung sicherheitsrelevanter Erkenntnisse erheblich reduzieren. Durch die automatische Erkennung von Anomalien in verschiedenen Datenquellen und das Bereitstellen von Kontextinformationen für Alarme kann maschinelles Lernen (ML) Untersuchungen beschleunigen und blinde Flecken im Unternehmen ausleuchten.

Dafür werden ML-Modelle trainiert und zur Mustererkennung innerhalb großer Datenmengen verwendet. Anschließend werden diese Verfahren getestet und verfeinert. Mit ML-Methoden werden Daten erfasst, integriert, analysiert und ausgewertet. Das spart Zeit und ermöglicht die Durchführung dieser Aufgaben ohne das sonst erforderliche Wissen einer entsprechend qualifizierten Person. Außerdem erleichtert dies dem SOC-Team die Suche nach Kontext- und forensischen Informationen in den durch mehrschichtige Sicherheitsfunktionen erfassten Daten.

Maschinelle Lernverfahren lassen sich für die folgenden übergeordneten Aufgaben einsetzen:

„Für uns sind alle Anwendungsszenarien gleich: Wir gehen immer extrem vor. Niemand hat bei uns den Fuß in der Tür, denn wir dürfen uns nicht von Vermutungen leiten lassen, wo die fragliche Person gerade ist, wer sie ist, welche Absichten sie hat und so weiter. Dasselbe gilt für Geräte und Anwendungen. Tatsächlich profitieren wir dadurch von einer viel übersichtlicheren Infrastruktur, denn wir sind nicht darauf angewiesen, für einzelne Szenarien unterschiedliche Hardware, Lösungen oder Technologien zur Absicherung von Benutzern und Anwendungen zu beschaffen.

Wir können alle Benutzer über eine einzige Architektur, ein System, eine Lösung und eine Technologie schützen – jederzeit und unabhängig davon, wo sie sich befinden und was sie vorhaben. Denn sowohl Benutzer als auch Anwendungen müssen jedes Mal wieder unsere Sicherheitsprüfung durchlaufen. ***Genau das macht ein Zero-Trust-Unternehmen aus.***“

– Nir Zuk, Mitgründer und CTO von Palo Alto Networks

- **Integration**: Nutzung von Daten für Rückschlüsse auf stattfindende Aktivitäten
- **Analyse**: Gewinnung von Erkenntnissen über den Problemraum und Erstellung von Prognosen
- **Automatisierung**: Schnellere Entscheidungsfindung bei Mitarbeitern; Anreicherung von Vorfallsdaten; automatische Maßnahmen auf Systemebene sowie Automatisierung von Arbeitsabläufen und Entscheidungsfindung

Mit Zero Trust auf Erfolgskurs – schneller dank Cortex

Mit der Bereitstellung der Cortex-Produktsuite können Sie die Transformation Ihres SOC einläuten oder vorantreiben. Cortex XDR, Cortex XSOAR und Cortex Xpanse sorgen im nahtlosen Verbund für eine nachhaltige Stärkung Ihrer Security Operations.

Im Zusammenspiel dieser Technologien erleben SOC-Teams unverzüglich allgemeine Verbesserungen:

Cortex XDR: Schützt Ihr Unternehmen dank erstklassigem Endpunktschutz und unternehmensweiter Bedrohungserkennung und -abwehr vor Gefahren – in allen Netzwerken, Clouds, Endpunkten und praktisch jeder Datenquelle. Patentierte Verhaltens- und Machine-Learning-Analysen erkennen getarnte Bedrohungen und liefern alle nötigen Informationen, um Sicherheitsvorfälle von vornherein zu verhindern.

Cortex XSOAR: Eine zentrale Plattform für SOC-Teams, in der sämtliche Vorfälle und Threat-Intelligence-Feeds gebündelt sind. Mit über 800 vorkonfigurierten Integrationen für Sicherheitstools, die von SOC-Teams sowie in Tausenden von automatisierten Skripten und Playbooks genutzt werden, ermöglicht XSOAR Ihrem SOC-Team die nötige Entschiedenheit bei der Umsetzung Ihrer Zero-Trust-Strategie. Egal, wie empfindlich die Alarmeinstellungen gewählt sind, die Warnungsflut wird Ihre Analysten nicht untergehen lassen. Ein US-amerikanischer Netzbetreiber konnte nach der Betriebsautomatisierung seines SOC durch XSOAR die Anzahl der Fälle bereits im ersten Monat der Inbetriebnahme um 30 % senken.

Cortex Xpanse: Das Tool bietet eine vollständige, genaue und aktuelle Liste mit den globalen, über das Internet erreichbaren Cloud-Assets und Fehlkonfigurationen eines Unternehmens. Dadurch kann dieses seine externe Angriffsfläche kontinuierlich überprüfen und evaluieren sowie das Bedrohungsrisiko senken, Risiken in der Lieferkette bewerten und die Sicherheitslage in verbundenen Unternehmen und Tochtergesellschaften beurteilen.

Obwohl jedes dieser Produkte durch seine besonderen Funktionen und Vorteile überzeugt, werden die Ergebnisse durch den kombinierten Einsatz exponentiell verbessert. Die umfassende Suite besteht aus drei Sicherheitsprodukten, die das Risiko und die Auswirkungen von Sicherheitsverletzungen durch ausnahmslos erstklassige Funktionen für das Erkennen, Untersuchen und Abwehren von Bedrohungen sowie das Automatisieren reduzieren.

Dank der nativen End-to-End-Integration und der optimalen Interoperabilität können SOC-Teams bestehende Sicherheitslücken durch die Synergien innerhalb des Cortex-Portfolios schließen. Die drei Produkte ergänzen einander bei der Überwachung der Bedrohungslandschaft und unterstützen robuste Funktionen zur Erkennung, Abwehr und Untersuchung von Bedrohungen:

- Cortex XDR und Cortex Xpanse ermöglichen die effektive Erkennung von Bedrohungen und Angriffsmöglichkeiten über das Internet, über Endpunkte, die Cloud und das Netzwerk, inklusive mobilen Mitarbeitern.
- Cortex XSOAR kann von Cortex XDR zur Automatisierung der Malware-Untersuchung und -Abwehr genutzt werden.
- Im Tandem reichern Cortex Xpanse und Cortex XSOAR Vorfallsdaten automatisch anhand der Assetinformationen von Xpanse an und automatisieren die Problembehebung bei neu entdeckten Assets.
- Cortex XSOAR nutzt Cortex XDR und Cortex Xpanse für die zuverlässige Bedrohungserkennung und die Ausgabe von Alarmen zum Ausführen automatisierter Incident-Response-Arbeitsabläufe.

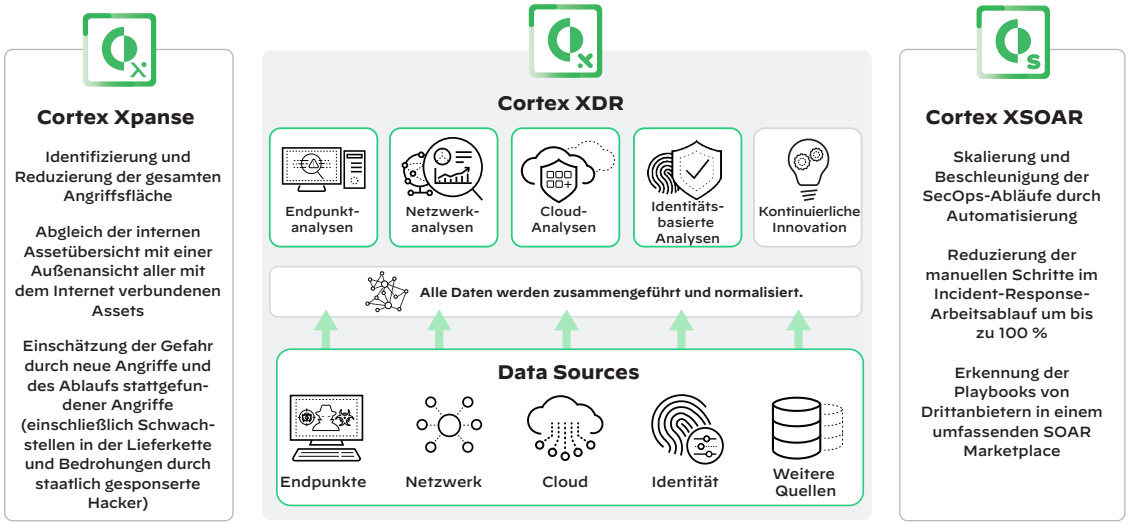


Abbildung 3: Die Cortex-Produktsuite

Was steht als Nächstes an? Zukunftssicherheit dank XSIAM

Obwohl die Produkte von Cortex die SOC-spezifischen Anforderungen an Transparenz, Schutz und Automatisierung erfüllen, sind die meisten Unternehmen immer noch abhängig von SIEM als Kernkomponente ihrer SecOps-Prozesse. Doch SIEM-Produkte hinken ihrem Versprechen effektiver und zentraler Bedrohungserkennung und -abwehr hinterher. Stattdessen zwingen sie Analysten zahllose Alarme und manuelle Prozesse auf. Sicherheitsteams benötigen jedoch eine zentrale Basisplattform, auf der mehrere Sicherheitsfunktionen automatisiert ineinandergreifen und der Einblick in unternehmensweite Sicherheitsdaten gegeben ist.

Genau dafür wurde XSIAM entwickelt, unser Tool für erweiterte Sicherheitsanalysen und die Verwaltung der Automatisierung. Es nutzt KI-gestützte Automatisierung, um die Effizienz von Sicherheitsmaßnahmen erheblich zu steigern und das manuelle SecOps-Modell auf den Kopf zu stellen. XSIAM erstellt eine intelligente Datenbasis und automatisiert einheitliche SOC-Funktionen. Dadurch beschleunigt es die Reaktionszeit, ist Bedrohungen einen Schritt voraus und rationalisiert die Arbeit der Analysten erheblich.

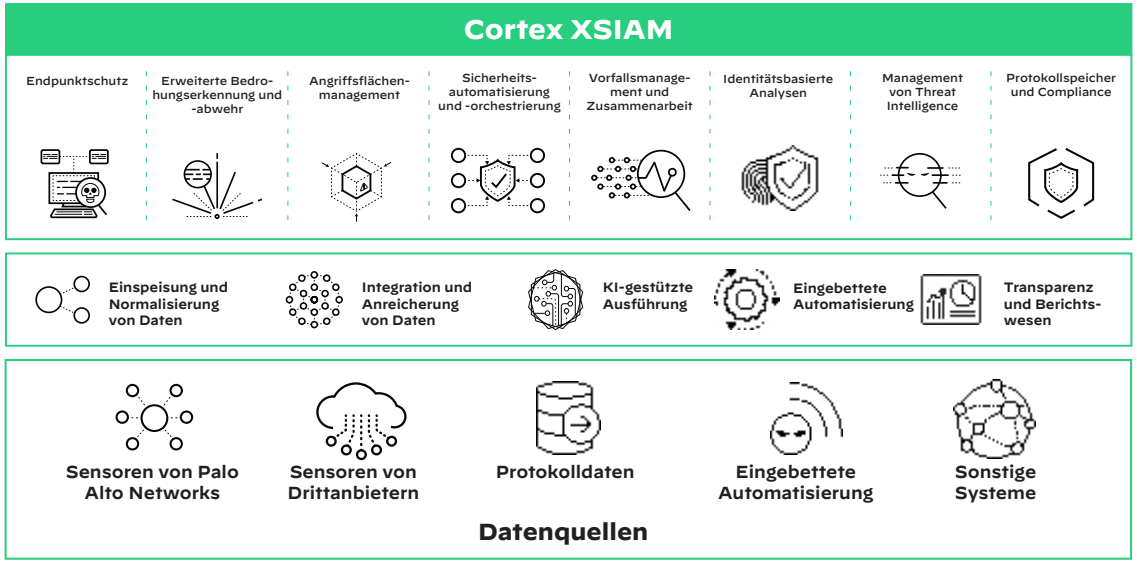


Abbildung 4: XSIAM ist die KI-gestützte Plattform für das moderne SOC.

Als konsolidierte Lösung für alle SOC-Prozesse ersetzt XSIAM Spezialprodukte und SIEM-Angebote. Es stellt ein breites Funktionsspektrum in einer umfassenden, automatisierten Lösung bereit. Die analystengesteuerte Funktionsweise der aktuell verbreiteten Sicherheitsprodukte gehört mit XSIAM und seiner intelligenten Automatisierung schon bald der Vergangenheit an. XSIAM hilft Unternehmen, Sicherheitsdaten und -tools zu konsolidieren, Prozesse zu automatisieren und Sicherheitslücken zu schließen – und all das bei deutlich besserer Schutzleistung und effizienteren Betriebsabläufen.

Unterstützt und geschützt durch Cortex

Palo Alto Networks steht für moderne und integrierte Sicherheitstools auf dem neuesten technologischen Stand. Werfen Sie einen Blick auf unsere Lösungen und sprechen Sie uns an. Wir unterstützen Sie gern dabei, Ihr Wissen zu erweitern und mit mehr Sicherheit mehr zu erreichen.

Weitere Informationen finden Sie auf unseren Produktseiten:

Cortex Xpanse

Cortex XSOAR

Cortex XDR

Cortex XSIAM

Besuchen Sie unsere Cortex-Portfolioseite.

Mehr zu Zero Trust

Bedeutende Umbrüche wie die Zunahme an hybriden Arbeitsmodellen und die ungebrochene Verlagerung von Anwendungen und Daten in die Cloud beschleunigen die digitale Transformation. Im Zuge dieser Transformation haben InfoSec-Teams die Chance, einen modernen Zero-Trust-Ansatz zu wählen, der diesen Veränderungen Rechnung trägt.

Weitere Informationen bieten wir Ihnen hier:

Lesen Sie unseren Blogbeitrag „Building the Zero Trust Enterprise: The Role of the SOC“ (Der Weg zum Zero-Trust-Unternehmen und die Rolle des SOC).

Laden Sie unser Whitepaper herunter: „So gestalten Sie das Zero-Trust-Unternehmen“.

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

cortex_ebook_practical-guide-to-adopting-zero-trust_092022