Cortex – für proaktive, lückenlose Sicherheit im SecOps-Bereich

Security Operations Center (SOCs) gibt es seit rund 15 Jahren, doch erst in den letzten fünf Jahren hat sich ihre kritische Rolle herauskristallisiert. SOC-Teams sind dafür verantwortlich, Cyberattacken zu verhindern und einheitliche Security Operations- (SecOps-)Prozesse umzusetzen. Das ist keine leichte Aufgabe – erst recht nicht, wenn Teams unter fehlendem Fachpersonal leiden, Budgeteinschränkungen in Kauf nehmen müssen und mit einer Flut an komplexen Branchenlösungen konfrontiert sind.

Angriffe nehmen in ihrer Anzahl zu, werden immer komplexer und verursachen zunehmend höhere Kosten. Das liegt nicht zuletzt am rasanten Anstieg von Ransomwaretechniken. Leider bleiben Cyberattacken oft viel zu lange unbemerkt, das heißt die Angreifer haben ausreichend Zeit, sich im Netzwerk auszubreiten, während sich die Einleitung von Untersuchungs-, Eindämmungs- und Schadensbehebungsmaßnahmen stark verzögert. Die Ursachen für ineffiziente Betriebsabläufe unterscheiden sich natürlich von Unternehmen zu Unternehmen, doch es gibt einige gemeinsame Nenner:

- Fehlende Transparenz in Bezug auf Geräte, Anwendungen, Netzwerke und Systeme
- Keine Bestandsliste der zu schützenden Assets
- Mangelndes Verständnis der anzuwendenden Tools und der Integrationsmöglichkeiten für die vorhandene Infrastruktur

Um mit den weltweiten Bedrohungen Schritt zu halten, setzen immer mehr Sicherheitsteams auf End-to-End-Lösungen, die über die Cloud bereitgestellt werden. Damit erzielen Unternehmen eine straffere Kontrolle der SecOps-Abläufe, erhalten einen ganzheitlichen Überblick über das Sicherheitsniveau und profitieren von leistungsstarken, integrierten Tools für die Identifizierung von Assets, die Einschätzung von Schwachstellen, die Bedrohungserkennung, die Einbindung von Threat Intelligence und automatisierte Abwehrmaßnahmen.

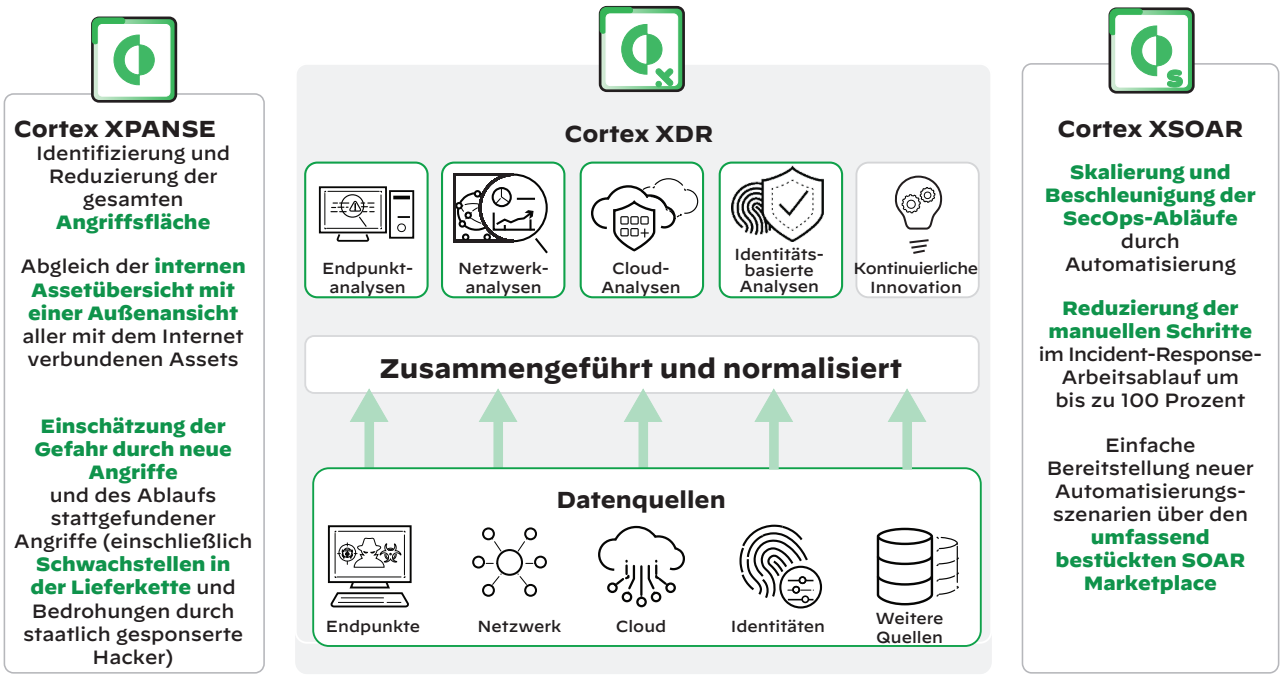

Abbildung 1: Umfassende Automatisierung der SecOps-Arbeitsabläufe

Cortex Xpanse: Erkennung und Problembehebung für mit dem Internet verbundene Assets

Durch die Zunahme an Cloud-Computing und mobiler Arbeit verschieben sich die Grenzen der Angriffsfläche ständig weiter und der Schutz aller Assets wird immer komplizierter. Zudem geben die jüngsten Scanningtechnologien Hackern die Möglichkeit, das gesamte Internet schnell auf Angriffsvektoren zu durchsuchen und ungenutzte, unautorisierte oder falsch konfigurierte Assets für Cyberattacken zu missbrauchen. Die Bereitstellung einer ASM-(Attack Surface Management-)Lösung ermöglicht die kontinuierliche Bewertung der eigenen Angriffsfläche.

Cortex® Xpanse™ bietet eine vollständige und genaue Bestandsliste mit allen über das Internet erreichbaren Cloud-Assets und Fehlkonfigurationen eines Unternehmens. Dadurch kann dieses seine externe Angriffsfläche kontinuierlich inventarisieren, einschätzen und reduzieren, Lieferantenrisiken bewerten sowie die Sicherheitslage in neu übernommenen beurteilen.

Identifizierung der Angriffsfläche: Lassen Sie automatische Bestandsaufnahmen aller mit dem Internet verbundenen Assets durchführen, um bislang unbekannte Risiken aufzudecken.

Schutz vor Ransomware: Finden Sie ungeschützte Möglichkeiten für den Fernzugriff, bevor dies Angreifern gelingt.

Governance der Infrastruktur: Überwachen Sie die Sicherheit in föderierten Umgebungen.

Cloud-Sicherheit: Eliminieren Sie Cloud-Wildwuchs und setzen Sie Cloud-Richtlinien zentral durch.

Sorgfaltspflicht in Bezug auf Dritte: Identifizieren Sie Risiken, die durch die Beziehungen mit Lieferanten und übernommenen Unternehmen entstehen.

Cortex XSOAR: Sicherheitsorchestrierung, -automatisierung und -reaktion (SOAR) plus Threat Intelligence Management

Das Herzstück einer SOAR-Lösung sind die Funktionen zur Priorisierung und Definition effizienter Arbeitsabläufe für Sicherheitsereignisse, die nur wenige oder gar keine manuellen Eingriffe erfordern. Ein überzeugendes SOAR-Produkt steigert die Effizienz durch Prozessautomatisierung und die vereinfachte Untersuchung von Cybervorfällen – alles über eine zentrale Plattform.

Cortex XSOAR ermöglicht das lückenlose Lifecycle Management aller Sicherheitsprozesse, sodass Unternehmen ihre SecOps-Abläufe straffen und den Zeitaufwand für die Untersuchung und Reaktion auf Bedrohungen reduzieren können. Mit Cortex XSOAR können Sicherheitsteams jeder Größe ihre Incident-Response-Prozesse für alle Arten von SecOps-Arbeitsabläufen orchestrieren, automatisieren und beschleunigen, nicht zuletzt unter Nutzung der zahlreichen Integrationen verschiedener Anbieter und der mehr als 725 vorkonfigurierten Content-Packs, die im XSOAR Marketplace zur Verfügung stehen.

Zudem haben Benutzer Zugang zu einer zentralen Bibliothek mit Threat Intelligence von diversen Quellen – darunter taktischen (maschinenlesbaren) und strategischen (berichtsbasierten) Daten – und der Option, Vorfällen automatisch Bedrohungsinformationen zuzuordnen sowie Threat Intelligence durch Automatisierung zu operationalisieren.

Automatisierung und Orchestrierung

Schnelle, umfassende Reaktion auf Sicherheitsvorfälle:

- Hunderte von Produktintegrationen
- Tausende von Sicherheitsmaßnahmen
- Intuitiver, visueller Playbook-Editor

Zusammenarbeit in Echtzeit

Verbesserung der Untersuchungsqualität durch Teamarbeit:

- Ein eigenes virtuelles Krisenzentrum für jeden Sicherheitsvorfall
- ChatOps und Sicherheitsmaßnahmen in Echtzeit
- Automatische Dokumentation von Playbooks und Aktionen der Analysten

Fallmanagement

Standardisierte Prozesse für alle Produkte, Teams und Einsatzbereiche:

- Echtzeit-ChatOps (in Fallmanagementtools integriert)
- Maßgeschneiderte Ansichten für jede Art von Vorfall
- Individuell anpassbare Dashboards und Berichte

Threat Intelligence Management

Volle Kontrolle über Ihre Threat-Intelligence-Feeds:

- Automatisierung von täglichen Routineaufgaben beim Management von Gefahrenindikatoren
- Sofortiger ROI durch vorhandene Threat-Intelligence-Feeds
- Mehr Vertrauen in Entscheidungen über Incident-Response-Maßnahmen

Cortex XDR: Bedrohungsprävention, -erkennung und -abwehr am Endpunkt, Verhaltensanalysen sowie Managed Detection and Response (MDR)

Cortex XDR ist deshalb eine sinnvolle Alternative zu SIEM-Lösungen, weil die Erkennung, Untersuchung und Abwehr von Bedrohungen, aber auch das Threat Hunting direkt an den Endpunkten ansetzt und weil XDR-Lösungen für Cloud-Umgebungen skalierbar sind und damit im Trend der Zeit liegen. Wichtig ist, dass alle Bedrohungen schon am Endpunkt abgewehrt werden. Cortex XDR unterstützt diesen Ansatz mit vorfallorientierten Erkennungs- und Abwehrfunktionen, die auf der automatischen Erfassung forensischer Informationen, der Gruppierung zugehöriger Alarme, Verlaufs- und Ursachenanalysen anhand von Alarmen zur Beschleunigung der Klassifizierung und Untersuchung durch Nachwuchskräfte oder erfahrene Analysten basieren.

Mit den folgenden Funktionen ermöglicht Cortex XDR die Angriffsabwehr am Endpunkt mit erstklassigem EDR für Windows® und Linux:

- Regelmäßig aktualisierte, KI-gestützte Tools für lokale Analysen und ML-basierte Verhaltensanalysen
- Zahlreiche Funktionen für den Endpunktschutz wie Sicherheitsmaßnahmen auf Geräteebene, Host-firewalls und Festplattenverschlüsselung
- Eine Vielzahl von Schutzmodulen für die Abwehr von Exploits (vor und nach der Ausführung von Dateien)

Cortex XDR bietet eine tiefere Integration von Drittlösungen, bessere Analysen und schnellere Abwehrmechanismen. All diese Merkmale sind unverzichtbar, wenn man bedenkt, dass Unternehmen bei der Reaktion auf einen Sicherheitsvorfall im Durchschnitt bis zu 45 Sicherheitstools koordinieren müssen.[1]

Mit Cortex XDR können Sicherheitsteams tote Winkel ausleuchten, Untersuchungen beschleunigen und die Sicherheit stärken. Dank der Möglichkeit, den Angriffsverlauf in einer kritischen Phase (zum Beispiel der Ausführung von Schadcode) zu unterbrechen und so größere Schäden durch eine laterale Ausbreitung zu verhindern, können Cyberattacken endlich „im Keim erstickt werden“.

Analysetools zur Erkennung komplexer Angriffe: KI, Verhaltensanalysen und benutzerdefinierte Erkennungsregeln sorgen für eine zuverlässige Bedrohungserkennung.

Vorfalluntersuchung statt Alarmüberflutung: Die bahnbrechende, konsolidierte Incident-Engine fasst Alarme zu Vorfällen zusammen.

Achtmal schnellere Untersuchungen: Eine umfassende Darstellung des Angriffsverlaufs, einschließlich Ursachenanalyse, beschleunigt die Prüfung akuter Bedrohungen.

Angriffsabwehr ohne Leistungseinbußen: Ein ressourcenschonender Agent sorgt für einen äußerst effektiven Endpunktschutz.

Maximaler ROI: Die Nutzung vorhandener Infrastrukturen zur Erfassung und Kontrolle von Sicherheitsdaten senkt Kosten um 44 Prozent.

1. 2020 *Cyber Resilient Organization Report*, Ponemon Institute, 30. Juni 2020, https://www.ibm.com/account/reg/us-en/signup?formid=urx-45839.

Alleine stark, gemeinsam stärker

Unser Cortex-Portfolio deckt alle Phasen der Sicherheitsimplementierung ab.

Mit Cortex Xpanse verschaffen Sie sich einen umfassenden und aktuellen Überblick über Ihre Angriffsfläche und alle Risiken. Dabei erkennen Sie nicht nur potenzielle Schwachstellen, sondern sehen auch auf einen Blick, welche Assets durch Cortex XDR geschützt sind – und welche nicht. Xpanse kann mithilfe von Daten aus Cortex XDR zudem wichtige Informationen über die Sicherheit der Umgebungen Ihrer mobilen Mitarbeiter bereitstellen.

Neue Risiken und Bedrohungen werden also von Cortex Xpanse und Cortex XDR erkannt, während Cortex XSOAR die manuellen Schritte reduziert, die erforderlich sind, um diese Risiken zu minimieren und auf Bedrohungen zu reagieren. Sie können mit Cortex XSOAR zum Beispiel festlegen, dass neu erkannte Assets und Schwachstellen automatisch den verantwortlichen Mitarbeitern gemeldet werden, sodass nur die Personen eine Benachrichtigung erhalten, die entsprechende Schritte einleiten müssen.

Cortex ist das branchenweit umfassendste Sicherheitsportfolio mit End-to-End-Lösungen, die es Unternehmen ermöglichen, sich proaktiv zu schützen statt reaktiv zu handeln: vom Angriffsflächenmanagement (für einen lückenlosen Überblick über Assets und Risiken) über erstklassige Präventions-, Erkennungs- und Abwehrtools für den Endpunktschutz bis hin zu leistungsstarken Automatisierungsfunktionen zur Reduzierung des manuellen Aufwands. Unternehmen, deren Sicherheitsansatz auf einem derartigen Produktportfolio basiert, profitieren von flächendeckendem Schutz und unterbrechungsfreiem Risikomanagement.

Weitere Informationen zu den branchenführenden Funktionen der Cortex-Produktsuite für Bedrohungsprävention und -erkennung, das Management der Angriffsfläche und die Sicherheitsautomatisierung erhalten Sie in unseren Whitepapern:

Building a Virtual SOC Platform with Cortex

Schon heute das SOC von morgen planen

Details finden Sie auf unseren Produktseiten:

Cortex Xpanse

Cortex XSOAR

Cortex XDR

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_b_holistic-ecosystem-security-operations_031522-de