Schon heute das SOC von morgen planen

Fünf Schritte und vier technologische Schlüssel für neue Security Operations zur Abwehr komplexer Angriffeund zur Effizienzsteigerung im SOC

Inhalt

SOCs stehen vor ihren bislang größten Herausforderungen

Moderne Cyberbedrohungen entwickeln sich schneller als die zu ihrer Abwehr eingesetzten Technologien. Finanziell gut ausgestattete Hackergruppen investieren in neue Methoden wie maschinelles Lernen (ML), Automatisierung und künstliche Intelligenz (KI). SOCs, die in erster Linie herkömmliche SIEM-Systeme (Security Information and Event Management) einsetzen, sind nicht unbedingt darauf ausgelegt, moderne Bedrohungen zuverlässig zu erkennen. Infolgedessen können sie ML nicht effektiv für Sicherheitstechnologien einsetzen, die mit dem digitalen Wandel, mit Cloud-Initiativen und mit komplexen Angriffskampagnen Schritt halten können.

Zu den Problemen älterer SOC-Umgebungen gehören:

- Mangel an Transparenz und Kontextdaten
- Zunehmende Komplexität der Untersuchungsabläufe
- Alarmmüdigkeit und Personalüberlastung durch unspezifische Alarme
- Fehlende Interoperabilität der Systeme
- Fehlende Automatisierung und Orchestrierung
- Keine Möglichkeit zur Erfassung, Verarbeitung und Kontextualisierung von Threat Intelligence
- Das SOC ist oft nicht in die Cloud integriert

Fünf Schritte zum SOC der Zukunft

Schritt 1: Transformation des manuellen SOC-Modells

Das manuelle SOC-Modell wurde mancherorts vom Rechenzentrum in die Cloud verlagert, aber seine Kernkomponente sind nach wie vor menschliche Analysten. SOC-Analysten lesen täglich Hunderte von Alarmen und sammeln manuell Kontextinformationen, um sie auszuwerten. Diese Untersuchungen nehmen viel Zeit in Anspruch, obwohl sich die meisten Alarme als falsch herausstellen. Da die Anzahl der Meldungen zunimmt und die Daten aus immer mehr Systemen zunehmend schwieriger zu integrieren sind, scheitert dieser manuelle Ansatz. Daher empfehlen wir eine alternative, skalierbare Methode für die effiziente Arbeit im SOC. Hier bildet Automatisierung die Basis, während sich Analysten auf die Bearbeitung der gefährlichsten Vorfälle konzentrieren.

Vergleichbar mit dem Autopiloten in einem Verkehrsflugzeug werden in einem automatisierten SOC die meisten Routinealarme, Analyseaufgaben und Abwehrmaßnahmen maschinell abgearbeitet. Auf diese Weise können sich die Analysten um dringende und wichtige Vorfälle kümmern, während die SOC-Plattform automatisch für Sicherheit sorgt, aus jeder Aktivität lernt und dem Piloten am Steuer effektive Informationen und Empfehlungen liefert. Das ist unsere Vision eines autonomen SOC.

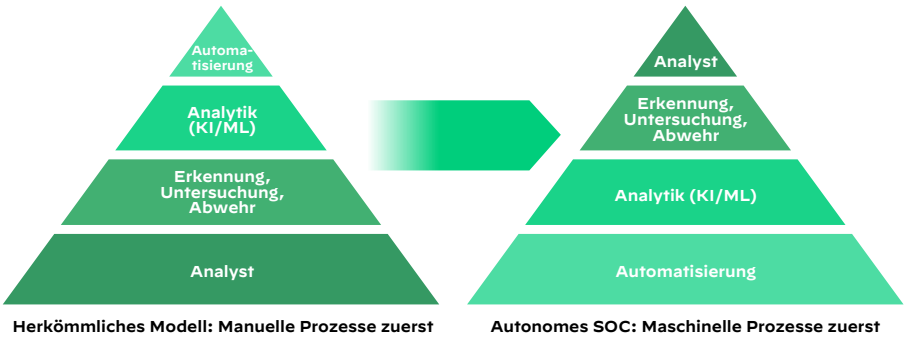

Abbildung 1: Manuelle vs. maschinelle Prozesse

Letztlich erleichtert die Kombination aus verbesserter Datenmodellierung und -integration sowie automatisierter Analyse und Erkennung die Arbeit der Sicherheitstechniker, da die Datenintegration und Bedrohungserkennung nun auch ohne eigens erstellte Korrelationsregeln funktioniert. Im Gegensatz zum traditionellen SecOps-Modell werden in einem modernen SOC bereits im ersten Schritt Data-Science-Methoden (und nicht nur menschliches Urteilsvermögen und Regeln zur Erkennung bekannter Bedrohungen) auf die riesigen eingehenden Datenmengen angewendet.

Der moderne SOC-Ansatz zur Abwehr komplexer Bedrohungen erfordert neue Architekturen, Datenprozesse und eine kontinuierliche Erweiterung des Wissens über die Bedrohungslandschaft. Dazu gehören:

- die umfassende und automatisierte Integration, Analyse und Priorisierung von Daten
- einheitliche Abläufe, die den Analysten ein produktives Arbeiten ermöglichen
- Embedded Intelligence und automatisierte Maßnahmen zur Abwehr von Angriffen mit minimalen manuellen Eingriffen

Schritt 2: Prüfung der IT-Umgebung zur Eindämmung der unkontrollierten Ausbreitung von Tools und damit verbundener Risiken

Leonardo da Vinci sagte einst: „Einfachheit ist die höchste Stufe der Vollendung." Infolge von Übernahmen, Fusionen und mangelnder Standardisierung im Bereich der IT-Sicherheit sehen sich viele Unternehmen mit einer verwirrenden Vielfalt von Tools konfrontiert. Ein Übermaß an Softwarelösungen bringt viele Probleme mit sich und die Verteilung von Ressourcen in Cloud- und On-Premises-Umgebungen hat zur Folge, dass sich Sicherheitsteams nur schwer einen vollständigen Überblick über die Angriffsfläche verschaffen können. Wie soll man die eigene Angriffsfläche kennen, wenn man kein klares Bild davon hat, welche Cloud-Lösungen eingebunden sind, welche Dienste der jeweiligen Cloud-Provider genutzt werden und welche Assets letztendlich Zugriff auf die lokale Umgebung haben?

In manchen Unternehmen beginnt der Wildwuchs an Tools mit der ersten Insellösung für ein bestimmtes Problem. Diese unkoordinierte Vorgehensweise erfordert die Verwaltung zahlreicher Agenten und führt paradoxerweise dazu, dass in den zu schützenden Netzwerken aufgrund mangelnder Interoperabilität und durch Fehlkonfigurationen neue Sicherheitslücken entstehen.

Einer der ersten Schritte zur Reduzierung der Sicherheitsrisiken durch die unkontrollierte Ausbreitung von Tools ist ein Audit der geschützten Systeme und Ressourcen.

Dabei muss möglichst genau definiert werden, was geschützt werden soll und was nicht passieren darf. Geht es um geistiges Eigentum? Personenbezogene Kundendaten? Ganz gleich ob Software oder physische Assets: Zwingende Voraussetzung für eine sinnvolle Priorisierung von Sicherheitsmaßnahmen ist eine möglichst umfassende Bestandsaufnahme aller kritischen und sensiblen Daten.

Sobald das Unternehmen ein klares Verständnis davon hat, welche Ressourcen besonders kritisch und schützenswert sind, besteht der nächste logische Schritt darin, Lösungen zu finden, die nach Möglichkeit mehrere Aufgaben erfüllen. In einer Umfrage der Enterprise Strategy Group (ESG) aus dem Jahr 2022 unter 280 IT- und Cybersicherheitsexperten aus den USA, Kanada, Europa, Mittel- und Südamerika, Afrika, Asien und Australien geben 22 % der Befragten an, dass sie den parallelen Einsatz mehrerer Insellösungen für problematisch halten, wobei 66 % der Befragten 25 oder weniger Sicherheitsprodukte einsetzen.[1] Da es heutzutage nicht mehr notwendig ist, Sensoren und die Durchsetzung von Richtlinien auf verschiedene Tools zu verteilen, ist in solchen Fällen eine Konsolidierung mehr als empfehlenswert.

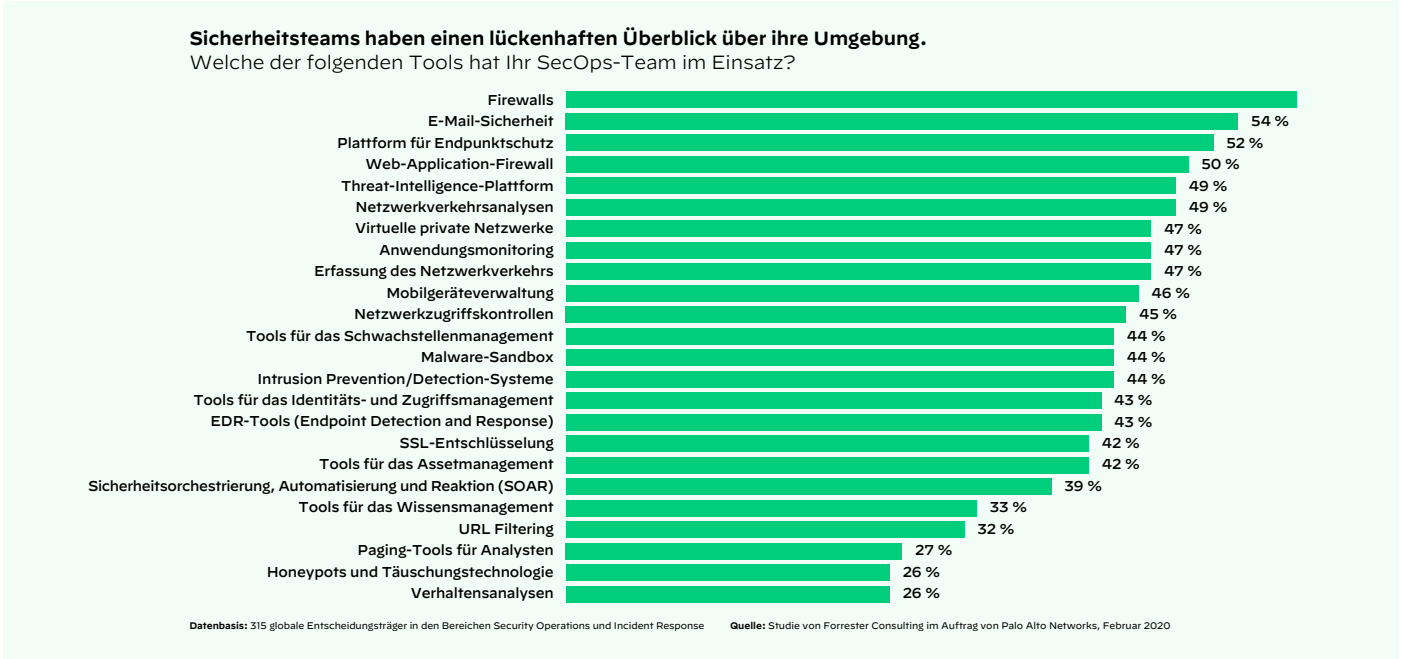

Abbildung 2: Die Tools der Sicherheitsprofis nach eigenen Angaben gegenüber ESG

1. „Cybersecurity Process and Technology Survey", ESG, Juni 2022, https://research.esg-global.com/reportaction/ESG-ISSACybersecurityProcessAndTechnologySurveyCSR/Toc.

Schritt 3: Automatisierung von Arbeitsabläufen

Sicherheitsverantwortliche müssen überlegen, ob ein Tool zwingend von einem Menschen konfiguriert oder bedient werden muss. Ist für die Interpretation und Einordnung der Ergebnisse ein Experte erforderlich? Müssen etwaige Tests manuell durchgeführt werden? Sicherheitsverantwortliche können einfache, repetitive Aufgaben definieren, deren Automatisierung im Kontext menschlicher Entscheidungen dazu beitragen kann, 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 für den Wissenstransfer in alle Richtungen unverzichtbar.

Angesichts der Vielzahl manueller Prozesse in den Bereichen Security Operations (SecOps) und Incident Response (IR), einschließlich der manuellen Überwachung von Threat Intelligence Feeds, kann die Investition in eine automatisierte SOAR-Lösung (Security Orchestration, Automation and Response) dazu beitragen, die Orchestrierung von Maßnahmen im gesamten Technologiestack sowie die Skalierbarkeit und Leistung der Bedrohungsabwehr zu verbessern.

Arbeitserleichterungen durch Automatisierung im SOC und NOC

- **Schnellere Bedrohungsabwehr**: Das Ersetzen manueller Arbeit durch automatisierte Sicherheitsprozesse ermöglicht erhebliche Zeiteinsparungen bei der Bedrohungsabwehr und verbessert zugleich die Genauigkeit und Zufriedenheit Ihrer Analysten.
- **Standardisierung und Skalierbarkeit**: Durch modulare, wiederholbare Abläufe kann die Sicherheitsautomatisierung zur Standardisierung der Datenanreicherung und Bedrohungsabwehr beitragen, wodurch die Qualität von Grund auf verbessert und die Skalierbarkeit unterstützt wird.
- **Einheitliche Sicherheitsinfrastruktur**: Eine Plattform wie Cortex XSOAR kann als Bindeglied zwischen bislang isolierten Sicherheitsprodukten dienen und die Steuerung von Incident-Response-Prozessen über eine zentrale Benutzeroberfläche ermöglichen.
- **Produktivere Analysten**: Die Automatisierung eintöniger Routineaufgaben und die Prozessstandardisierung bringen Ihren Analysten einen spürbaren Zeitgewinn, der für wichtige Entscheidungen und die Planung weiterer Sicherheitsverbesserungen genutzt werden kann.
- **Nutzung vorhandener Investitionen**: Durch die Automatisierung repetitiver Aufgaben und den Wegfall diverser Benutzeroberflächen vereinfacht die Sicherheitsorchestrierung den Einsatz mehrerer Produkte und die Abstimmung im Team, sodass aus vorhandenen Sicherheitsinvestitionen ein größerer Nutzen gezogen werden kann.
- **Optimierung der Bearbeitung von Vorfällen**: Durch die Automatisierung von Prozessen im Incident-Ticket-Management mittels Integration bekannter ITSM-Lösungen wie ServiceNow, Jira oder Remedy sowie bewährter Kommunikationstools wie Slack lässt sich die Vorfallsbearbeitung deutlich beschleunigen. Die zu bearbeitenden Vorfälle können zudem abhängig vom Typ automatisch an das jeweils zuständige Team weitergeleitet werden.
- **Höhere Netzwerksicherheit**: In der Summe bewirken die genannten Vorteile eine Verbesserung des allgemeinen Sicherheitsstatus und eine entsprechende Reduzierung der Sicherheits- und Geschäftsrisiken des Unternehmens.

Fünfjahresausblick zum Thema Automatisierung

Neue SOCs können vom ersten Tag an automatisieren, wohingegen dieser Prozess in älteren SOCs Upgrades erfordert und geplant werden muss. Ein realistisches Dreijahresziel für eine etablierte Einrichtung: 50 % der SOC-Dienste automatisieren. Im fünften Jahr können rund 75 % der Aufgaben automatisiert ablaufen. Für Tätigkeiten wie die proaktive Bedrohungssuche werden jedoch weiterhin Spezialisten benötigt.

Schritt 4: Ergänzung manueller Prozesse durch ML-Analysen

Eine Schlüsselkomponente der SOC-Transformation ist die Bereitstellung umfassender Funktionen für maschinelles Lernen, um die menschliche Arbeit im Bereich 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 die Bereitstellung von Kontextinformationen zu Alarmen können ML-Funktionen dazu beitragen, notwendige Untersuchungen zu beschleunigen und etwaige Blind Spots im Unternehmen auszuleuchten.

Dazu werden ML-Modelle trainiert und zur Mustererkennung in großen Datenmengen eingesetzt. Anschließend werden diese Verfahren getestet und verfeinert. Mit ML-Methoden können relevante Daten erfasst, integriert, analysiert und ausgewertet werden. Das spart Zeit und ermöglicht die Durchführung dieser Aufgaben ohne das sonst erforderliche Wissen einer entsprechend qualifizierten Person. Darüber hinaus erleichtert es die Suche nach Kontextinformationen und forensischen Beweisen in Daten, die durch mehrschichtige Sicherheitsfunktionen erfasst wurden.

Überwachtes maschinelles Lernen eignet sich beispielsweise zur Erstellung digitaler Fingerabdrücke von PCs, Mail- und Dateiservern oder anderen Geräten, um typische Verhaltensmuster und davon abweichende Anomalien zu erfassen und zu erkennen. Im Idealfall ermöglichen ML-Funktionen kausale Schlussfolgerungen in Bezug auf Aktivitäten in der IT-Umgebung, wobei die Software auch ohne manuelle

Eingriffe die nächsten Schritte einleiten kann. Auf diese Weise können Aktivitäten anhand des Verhaltens und der Interaktion innerhalb der verknüpften Datensätze als „böswillig“ eingestuft und gekennzeichnet werden. Diese Entscheidung wird an das gesamte Netzwerk weitergeleitet, wobei explizite Anweisungen beispielsweise die Isolierung von Daten über Agenten oder die Unterbrechung von Datenverbindungen über Firewalls anfordern können.

Im Allgemeinen eignen sich maschinelle Lernverfahren für folgende Aufgaben:

- **Integration**: Nutzung von Daten für Rückschlüsse auf laufende Aktivitäten
- **Analyse**: Gewinnung von Erkenntnissen über den Problemraum und Erstellung von Prognosen
- **Automatisierung**: Beschleunigung der menschlichen Entscheidungsfindung und Automatisierung von Maßnahmen, Prozessen und Entscheidungen auf Systemebene

Schritt 5: Verstärkung des Sicherheitsteams

Neben Sicherheitslösungen und Softwaretools ist menschliches Know-how der wichtigste Erfolgsfaktor in einem Security Operations Center. Besonders bei einfachen repetitiven Aufgaben können durch maschinelles Lernen und Automatisierung die Reaktionszeiten verkürzt, die Genauigkeit erhöht und die Effizienz der Fehlerbehebung verbessert werden. Dennoch ist und bleibt im Kontext der SOC-Transformation die Rekrutierung, Ausbildung und Bindung qualifizierter Techniker, Analysten und Systemarchitekten integraler Bestandteil jeder kohärenten Strategie. Durch den Einsatz von Automatisierungstechnologien können Unternehmen die Wirksamkeit ihrer IT-Schutzmaßnahmen optimieren.

Das US Bureau of Labor Statistics geht davon aus, dass die Zahl der Beschäftigten im Bereich Cybersecurity zwischen 2019 und 2029 um 31 % steigen wird.[2] Darüber hinaus hat das National Center for Education Statistics (NCES) festgestellt, dass die Anzahl der neuen Studiengänge mit Fokus auf Cybersicherheit in den letzten sechs Jahren um 33 % gestiegen ist, während die Anzahl der Stellenangebote in diesem Sektor um 94 % zugenommen hat.[3]

Neben der Besetzung kritischer Rollen sind Cybersecurity-Trainings besonders wichtig. Damit wird sichergestellt, dass Mitarbeiter, Auftragnehmer und bestimmte Partner für das Thema Cybersicherheit sensibilisiert werden. Beim Diebstahl von Anmeldedaten, bei Phishingangriffen und bei Social Engineering ist der Faktor Mensch entscheidend, weshalb sich die Entwicklung von Cyberkompetenzen in Ihrem Team auf lange Sicht auszahlen wird. Wie der renommierte Verschlüsselungs- und Sicherheitsexperte Bruce Schneier weiß, ist der „Mensch in der Regel das schwächste Glied in der Kette und erstaunlich oft für das Versagen von Sicherheitssystemen verantwortlich“.

Es gibt solche und solche SOCs

Palo Alto Networks folgt einem optimierten SOC-Ansatz und verzichtet bewusst auf die bekannte vierstufige Struktur, die in der Regel mit Level-1-Analysten beginnt (Monitoring, Priorisierung und Untersuchung von SIEM-Alarmen) und bis hin zu Level-4-Managern reicht (Personaleinstellung, Strategiefragen und Reporting an die Geschäftsführung). Stattdessen verfolgt das SOC-Team von Palo Alto Networks die folgende hybride Philosophie:

- 80 % des SOC-Personals verfügen über einschlägige Berufserfahrung
- Fachübergreifende Ausbildung der Mitarbeitenden in allen Disziplinen, zum Beispiel Priorisierung von Alarmen, Incident Response und proaktive Bedrohungssuche
- Angemessenes Jahresbudget zur Finanzierung von Schulungen für alle Mitarbeitenden

Dafür wurden folgende Ziele definiert:

- Flexibilität im Team hinsichtlich der Fähigkeit, zwischen Zuständigkeiten und Organisationsstufen zu wechseln
- Sicherstellung der betrieblichen Kontinuität
- Anregende Arbeitsatmosphäre, Vermeidung von Burn-out
- Förderung des kontinuierlichen Lernens
- Besserer Schutz mit weniger Personal durch kompetenten Einsatz geeigneter Technologien

2. „Occupational Outlook Handbook, Information Security Analysts“, U.S. Bureau of Labor Statistics, 9. April 2021, https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.
3. „CISO Benchmark Study“, Cisco, März 2019, https://ebooks.cisco.com/story/anticipating-unknowns/page/6/6.

ASM, SOAR und XDR: die Eckpfeiler der SOC-Transformation

Der Aufbau eines robusten und effizienten SOC beginnt mit den oben beschriebenen fünf Schritten. Die logische Fortsetzung sind die folgenden vier technologischen Schlüssel für die erfolgreiche Definition Ihrer Security-Operations-Strategie.

Schlüssel 1: Stärkung des Risikomanagements durch Kenntnis der Angriffsfläche

Solides Risikomanagement ist ein wesentlicher Bestandteil der SOC-Transformation. Die Identifizierung dessen, was vor Angriffen geschützt werden muss, ist ein logischer erster Schritt in einem Prozess, der den Rahmen für die Formulierung von mehr oder weniger komplexen Plänen und Strategien für das Risikomanagement schafft. Erst diese Eingrenzung ermöglicht die Priorisierung gefährdeter Ressourcen und die Analyse von Maßnahmen zur Minderung konkreter Risiken.

Besonders relevant für das Risikomanagement ist der Überblick über die eigene Angriffsfläche, denn was man nicht kennt, kann man auch nicht schützen.

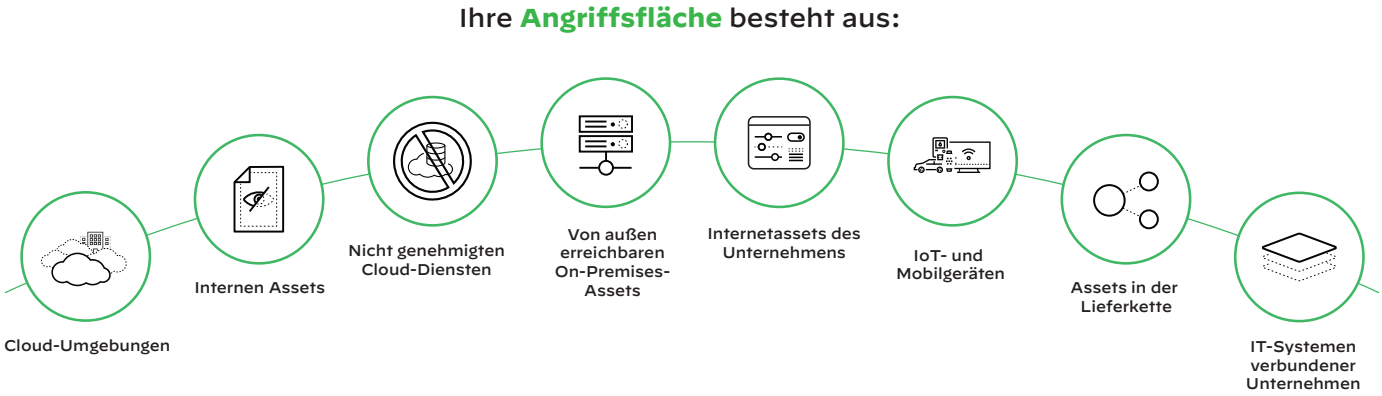

Abbildung 3: Bestandteile der Angriffsfläche

Unabhängig davon, ob Sie sich für eine ASM-Lösung (Attack Surface Management) entscheiden oder proaktiv Penetrationstests und Schwachstellenscans durchführen, müssen die produktbezogenen und operativen Anforderungen im Vorfeld geklärt werden. Dieser Anforderungskatalog umfasst in der Regel die Funktionen, Leistungsmerkmale und Bewertungskriterien zur Auswahl geeigneter Lösungen und Tools für das Angriffsflächenmanagement.

Der *Cortex Xpanse Bedrohungsbericht 2021 zur Angriffsfläche* enthält eine Zusammenfassung der wichtigsten Erkenntnisse aus der Untersuchung der im Internet exponierten Angriffsflächen einiger der weltweit größten Unternehmen. Von Januar bis März überwachte das Forschungsteam von Cortex Xpanse Scans von 50 Millionen IP-Adressen in den Netzwerken von 50 globalen Unternehmen, um zu verstehen, wie schnell Angreifer verwundbare Systeme identifizieren können.

Knapp ein Drittel der erkannten Sicherheitslücken wurde auf Probleme mit dem weit verbreiteten Remote Desktop Protocol (RDP)[4] zurückgeführt, dessen Nutzung Anfang 2020 sprunghaft anstieg, als Unternehmen diverse Cloud-Projekte vorantrieben, um das mobile Arbeiten während der COVID-19-Pandemie zu ermöglichen. Darüber hinaus wurde Folgendes festgestellt:

- **Cyberkriminelle machen keine Pause**. Im ewigen Katz-und-Maus-Spiel führen Hacker stündlich einen Scan durch, während globale Unternehmen oft mehrere Wochen zwischen einzelnen Scans verstreichen lassen.[5]
- **Cyberkriminelle stürzen sich auf neue Sicherheitslücken**. Zwischen Januar und März starteten Hacker innerhalb von 15 Minuten nach der Bekanntgabe neuer CVEs (Common Vulnerabilities and Exposures) und innerhalb der ersten fünf Minuten nach dem Sicherheitsupdate für die Zero-Day-Schwachstelle in Microsoft Exchange Server die ersten Scans.[6]

4. *Cortex Xpanse Bedrohungsbericht 2021 zur Angriffsfläche*, Palo Alto Networks, Mai 2021, https://www.paloaltonetworks.com/engage/cortex-xpanse-general/xpanse-attack-surface-threat-report-2021.
5. Ebd.
6. Ebd.

- **Sehr viele Systeme sind angreifbar**. In globalen Unternehmen treten durchschnittlich alle 12 Stunden, also zweimal täglich, neue schwerwiegende Sicherheitslücken auf. Zu den Problemen gehören unsichere Fernzugriffe (zum Beispiel über RDP, Telnet, SNMP und VNC), anfällige Datenbankserver und Zero-Day-Schwachstellen in Produkten wie Microsoft Exchange Server und in Load Balancern von F5.[7]
- **Die meisten kritischen Sicherheitsprobleme treten in der Cloud auf**. 79 % der kritischsten Schwachstellen wurden in den Cloud-Umgebungen der untersuchten Unternehmen festgestellt. Der vergleichsweise geringe Anteil von 21 % in On-Premises-Umgebungen bestätigt, dass Cloud-Dienste inhärent risikobehaftet sind.[8]

Fazit: Moderne Scanner machen es Hackern leicht, Angriffsvektoren zu finden und ungenutzte, nicht autorisierte oder falsch konfigurierte Assets für Cyberattacken zu missbrauchen. Der Einsatz einer ASM-Lösung (Attack Surface Management) ermöglicht eine kontinuierliche Bewertung der Angriffsfläche.

Schlüssel 2: SOAR – Orchestrierung aller Produkte zur Optimierung von Incident-Response-Maßnahmen

Bei SOAR denkt man meist an Lösungen zur Ausführung von Playbooks im Rahmen der Prozessautomatisierung. Eine effektive SOAR-Strategie geht jedoch über die reine Automatisierung zur Effizienzsteigerung und Reduzierung manueller Arbeitsschritte hinaus. Durch die Integration von Drittlösungen lassen sich Arbeitsabläufe orchestrieren und automatisieren, um beispielsweise folgende Ergebnisse zu erzielen:

- Priorisierung von Alarmen
- Klassifizierung von Bedrohungen
- Bedrohungsabwehr
- Auswahl und Management von Threat Intelligence
- Überwachung und Management der Compliance

Eine SOAR-Lösung für ein umfassendes Incident Management bietet vorkonfigurierte Integrationen für gängige SOC-Tools, Playbooks mit Best Practices zur Automatisierung von Arbeitsabläufen sowie integrierte Tools für das Case Management und die Echtzeitkollaboration, die eine teamübergreifende Untersuchung von Sicherheitsvorfällen ermöglichen.

Darüber hinaus unterstützt sie als zentrales Repository für interne und externe Threat Intelligence den automatisierten Abgleich von Indikatoren, Vorfällen und Analysedaten sowie die Aufbereitung strategisch relevanter Daten. Auf diese Weise können Sicherheitsanalysten und Incident-Response-Teams zusätzliche Erkenntnisse über Hackergruppen und deren Angriffsmethoden gewinnen.

SOAR-Lösungen entwickeln sich zunehmend zur Schaltzentrale des modernen SOC und haben das Potenzial, die Steuerungsfunktion für weitere Security Operations zu erfüllen. Deshalb unterstützen SOAR-Plattformen vermehrt die direkte Integration von Threat Intelligence und Schwachstellenmanagement sowie die Ausweitung der Automatisierung auf Anwendungsbereiche außerhalb des SOC. Darüber hinaus werden die Produkte führender Anbieter um technologiespezifisch vorkonfigurierte SOAR-Funktionen und Incident-Management-Features erweitert.

Fazit: Kernstück einer SOAR-Lösung sind Funktionen zur Priorisierung und Definition effizienter Arbeitsabläufe für Sicherheitsereignisse, die wenig oder keine manuellen Eingriffe erfordern. Ein überzeugendes SOAR-Produkt steigert die Effizienz durch Prozessautomatisierung und bietet gleichzeitig eine einheitliche Plattform zur Reduzierung komplexer Untersuchungen und zur Orchestrierung des gesamten Technologiestacks eines SOC.

7. *Cortex Xpanse Bedrohungsbericht 2021 zur Angriffsfläche*
8. Ebd.

Automatisierung in einem Sicherheitsunternehmen

Im SOC von Palo Alto Networks wird Cortex XSOAR eingesetzt, um das Personal von den oben beschriebenen repetitiven und zeitintensiven Aufgaben zu entlasten. Hier sehen Sie eine Aufstellung der Zeiteinsparungen durch Automatisierung im Februar 2021.

Art der Automatisierung	Anzahl	Eingesparte Analystenstunden
Aufbereitung von Artefakten	2.498	1.457
Deduplizierung	10.063	821
E-Mail-Benutzer	464	193
Neuinstallation mit Image	8	4
Passwortreset	8	4
Durchgängig automatisierte Arbeitsabläufe	57	29
Andere Aufgaben*	*	133

Repetitive und unbeliebte Aufgaben im SOC

*PhishMe-Statistiken, RSS-Feeds, Contentupdates, Bedrohungssuche und zugehörige Kennzahlen, tägliche Erstellung von Monitoring-Tickets und Lösen von Jira Tickets

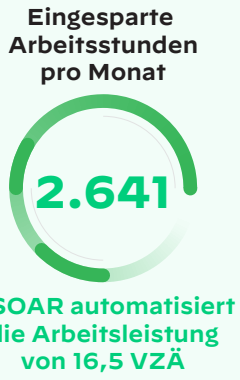

Abbildung 4: Die größten Zeiteinsparungen durch Automatisierung

Schlüssel 3: XDR – die nächste logische Entwicklungsstufe von EDR

Der Begriff XDR (Extended Detection and Response) wurde 2018 von Nir Zuk, CTO und Mitbegründer von Palo Alto Networks, geprägt. XDR wurde entwickelt, um aktive Attacken effizienter zu stoppen, unvorhersehbare Angriffe und Taktiken zu erkennen und das SOC-Team bei der Abwehr von Bedrohungen zu unterstützen, die eine Untersuchung erfordern. Die Idee ist ein nahtloser Ansatz für die Zusammenführung verschiedener Telemetriedaten aus mehreren (teils komplementären) Quellen. Dazu gehören EDR-Tools, Analysen des Netzwerkverkehrs, des Benutzer- und Systemverhaltens (UEBA) sowie Gefährdungsindikatoren (IOCs).

XDR ermöglicht eine effizientere und effektivere Abwehr von Angriffen durch die Konsolidierung isolierter Tools, die Optimierung von Prozessen und die Verbesserung der Systemtransparenz bei der Erkennung und Untersuchung von Cyberbedrohungen. Mit XDR kann das Sicherheitsteam Blind Spots ausleuchten, Untersuchungen beschleunigen und die Ergebnisse verbessern. Dank der Möglichkeit, den Angriffsverlauf in einer kritischen Phase (zum Beispiel der Ausführung von Schadcode) zu unterbrechen und so zu verhindern, dass sich Angreifer in der Umgebung festsetzen und durch die Ausbreitung im Netzwerk größeren Schaden anrichten, können Cyberangriffe endlich im Keim erstickt werden.

Für die Einführung von XDR sprechen Argumente wie die einfachere Visualisierung komplexer Angriffe entlang der Cyber Kill Chain, robuste Automatisierung, moderne Analyseverfahren und maschinelles Lernen. XDR gewinnt zunehmend an Bedeutung, da immer mehr Kunden eine nahtlosere Integration von Drittlösungen, bessere Analysen und schnellere Abwehrmechanismen fordern. Eine mögliche Erklärung für diesen Trend ist die Tatsache, dass Unternehmen im Durchschnitt bis zu 45 Sicherheitstools einsetzen und bei einem Vorfall um die 19 Tools koordinieren müssen.[9]

XDR verbindet SIEM-Funktionen wie die Integration, Normalisierung und Korrelation von Alarmen mit der von SOAR bekannten automatisierten Untersuchung und Wiederherstellung.

XDR schließt die Lücke in der Angriffserkennung und Abwehr

Vor XDR erforderte der Abgleich der Endpunkttelemetriedaten mit anderen Ereignisdaten das mühsame Durchforsten großer Datenmengen und False Positives, die sich in diversen Dashboards angesammelt hatten. Die Konsolidierung von Ereignisdaten ist zeitaufwendig und erfordert viel analytische Kompetenz bei Entscheidungen hinsichtlich der Relevanz einzelner Alarme. Das führt mitunter dazu, dass das SOC-Team viel Zeit damit verliert, irrelevante Meldungen zu überprüfen, wodurch sich die Untersuchung kritischer Alarme verzögert.

Da dies einem Kampf gegen Windmühlen gleicht und die Komplexität und Häufigkeit von Cyberangriffen zunimmt, interessieren sich immer mehr vorausschauende Unternehmen für den XDR-Ansatz und die mit dieser Sicherheitsarchitektur verbundenen Effizienzvorteile.

Endpunktschutz allein reicht nicht aus. Ebenso unverzichtbar sind detaillierte Analysen umfangreicher Cloud- und Netzwerkdaten aus einer einzigen, verbindlichen Datenquelle.

Fazit: Cortex XDR eignet sich für verschiedene Ausprägungen einer SecOps-Architektur und ermöglicht die unternehmensweite Erkennung und Abwehr von Bedrohungen einschließlich EDR- und EPP-Funktionen. Das ist besonders für Unternehmen interessant, die nicht den vollen Funktionsumfang eines SIEM-Systems benötigen. Auch im Verbund mit einer SIEM-Lösung bietet Cortex XDR EDR/EPP-Funktionen und ermöglicht die gezielte Erkennung und Abwehr von Bedrohungen.

9. *2020 Cyber Resilient Organization Report*, IBM Security, Juni 2020, https://www.ibm.com/account/reg/de-de/signup?formid=urx-45839.

Schlüssel 4: XSIAM – die KI-gestützte SOC-Plattform zur Optimierung und Beschleunigung der Bedrohungsabwehr

SIEM-Lösungen (Security Information and Event Management) wurden entwickelt, um die Verwaltung von Sicherheitsmeldungen und Ereignisprotokollen zu erleichtern. Die Erkennung und Behebung von Problemen erfolgt jedoch weitgehend manuell, und etwaige Analyse- und Automatisierungsfunktionen wurden erst im Nachhinein hinzugefügt. Im SecOps-Bereich werden seit Jahren SIEM-Systeme eingesetzt, die einen erheblichen Arbeitsaufwand verursachen und nur einen geringen Beitrag zur Verbesserung der Sicherheitslage leisten. Der Kampf gegen moderne Cyberbedrohungen erfordert ein radikales Umdenken und den verstärkten Einsatz künstlicher Intelligenz.

Mit Cortex XSIAM beschränkt sich die Aufgabe der Sicherheitsexperten auf die Feinabstimmung der KI- und Automatisierungsfunktionen für die automatische Verwaltung von Ereignisdaten. Dabei werden Alarme aus der gesamten Umgebung automatisch eingeordnet und bearbeitet.

Als konsolidierte Gesamtlösung für alle SOC-Prozesse ergänzt XSIAM Spezialprodukte und SIEM-Systeme um eine Vielzahl nützlicher Funktionen. Zu den Leistungsmerkmalen von XSIAM gehören Datenzentralisierung, intelligentes Stitching, analytische Bedrohungserkennung, Incident Management, Threat Intelligence, Automatisierung, Angriffsflächenmanagement und vieles mehr – alles verpackt in einer intuitiven Benutzeroberfläche.

Fazit: Cortex XSIAM ist eine automatisierungsorientierte Plattform für das moderne SOC. Die Lösung nutzt die Vorteile der maschinellen Intelligenz, um die Effizienz von Sicherheitsmaßnahmen im SecOps-Bereich radikal zu verbessern. Mit XSIAM können Kunden mehrere Produkte auf einer kohärenten Plattform konsolidieren, Kosten sparen und die Arbeitsweise und Produktivität ihrer Analysten optimieren.

Cortex XSIAM, Cortex XDR, Cortex XSOAR und Cortex Xpanse

Uns ist bewusst, dass sich die meisten unserer Kunden nicht unbedingt als Systemintegratoren verstehen. Sie wollen auch nicht immer wieder die gleichen manuellen Aufgaben erledigen. Der Einsatz einer Vielzahl von Insellösungen ist mit erheblichem Zeit- und Kostenaufwand verbunden. Isolierte Softwareprodukte behindern die in einem modernen SOC notwendigen Analysen durch Komplexität und Intransparenz, was sich entsprechend negativ auf die Sicherheit auswirken kann.

Auch wir können nicht mehr Zeit herzaubern, dafür aber durch Prozessoptimierung, geringere Betriebskosten und die branchenbesten Funktionen für die Integration von Drittanbietertools zum Erfolg unserer Kunden beitragen. Darüber hinaus profitieren Sicherheitsanalysten von zuverlässigen Tools für den Schutz ihrer Daten, die sie von Routineaufgaben entlasten und ihnen die Möglichkeit geben, sich auf das Wesentliche zu konzentrieren.

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

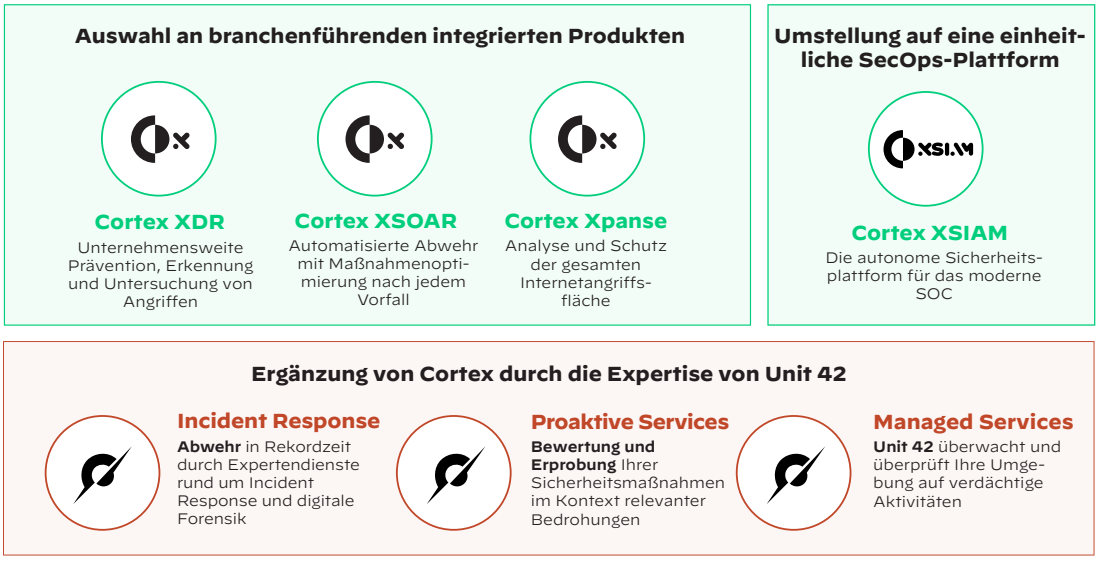

Abbildung 5: Lösungsangebot von Palo Alto Networks für den Aufbau des SOC der Zukunft

Cortex XSIAM

Cortex® XSIAM™ ist die Schaltzentrale des autonomen SOC und bietet native Funktionen für XDR, SOAR, Threat Intelligence, ASM und SIEM. Mit XSIAM (Extended Security Intelligence and Automation Management) können Kunden mehrere Produkte auf einer kohärenten Plattform konsolidieren, Kosten sparen und die Arbeitsweise und Produktivität ihrer Analysten optimieren.

Cortex XDR

Cortex XDR® ermöglicht die Abwehr von Angriffen auf Endpunkte und Hosts mit erstklassiger EDR für Windows und Linux, die vorfallsorientierte Erkennung und Abwehr von Bedrohungen durch die automatische Erfassung forensischer Daten, die Zuordnung relevanter Alarme sowie Verlaufs- und Ursachenanalysen anhand dieser Meldungen zur Beschleunigung der Klassifizierung und Untersuchung durch Nachwuchskräfte oder erfahrene Analysten.

Cortex XSOAR

Cortex® XSOAR™ ist eine zentrale Plattform für das durchgängige Lifecycle Management aller Sicherheitsprozesse. Sicherheitsteams jeder Größe profitieren von mehr als 900 vorgefertigten Content-Packs für Integrationen sowie von zuverlässigem Case Management und Kollaborationstools. Das erleichtert die Orchestrierung, Automatisierung und Beschleunigung von Incident Response und anderen Arbeitsabläufen und Sicherheitsprozessen in der gesamten IT-Umgebung. Weitere Vorteile sind das Threat Intelligence Management mit einer zentralen Bibliothek und der Möglichkeit, Threat Intelligence automatisch Vorfällen zuzuordnen und Threat Intelligence durch Automatisierung zu operationalisieren.

Cortex Xpanse

Cortex® Xpanse™ bietet eine vollständige und genaue Bestandsliste mit allen über das Internet erreichbaren Cloud-Assets und Fehlkonfigurationen. Dadurch kann das Unternehmen seine externe Angriffsfläche kontinuierlich inventarisieren, bewerten und reduzieren, risikobehaftete Kommunikation erkennen, Lieferantenrisiken beurteilen sowie die Sicherheitslage bei verbundenen Unternehmen und Tochtergesellschaften bewerten.

Durchgängige Integration und Interoperabilität

Dank der Synergien innerhalb des Cortex-Portfolios kann das SOC-Team bestehende Sicherheitslücken schließen:

- Cortex XSIAM vereint branchenführende Funktionen für EDR, XDR, SOAR, ASM, UEBA, TIP, ITDR und SIEM. XSIAM verwendet Bedrohungsmodelle und maschinelles Lernen, um die Integration, Analyse und Klassifizierung von Sicherheitsdaten zu automatisieren. Die Lösung ist in der Lage, die meisten Alarme automatisch zu verarbeiten, sodass sich Ihr Team auf die Vorfälle konzentrieren kann, bei denen tatsächlich ein manuelles Eingreifen erforderlich ist.
- Cortex XDR und Cortex Xpanse ermöglichen eine effektive Erkennung von Bedrohungen und Angriffsmöglichkeiten über das Internet, über Endpunkte, die Cloud und das Netzwerk.
- Cortex XDR und Xpanse nutzen XSOAR für umfassende Funktionen zur Orchestrierung, Automatisierung und Bedrohungsabwehr.
- Cortex XSOAR nutzt Cortex XDR und Xpanse für die zuverlässige Erkennung von Bedrohungen und die Ausgabe von Alarmen für die Orchestrierung von Arbeitsabläufen.

Cortex: neuer SecOps-Ansatz als wirksame Verteidigung gegen Cyberangriffe

Palo Alto Networks steht für kundennahe Innovation und den zuverlässigen Schutz wertvoller Ressourcen durch moderne Sicherheitstools auf dem neuesten technologischen Stand. Werfen Sie einen Blick auf unsere Lösungen und sprechen Sie uns an. Wir unterstützen Sie gerne dabei, Ihr Wissen zu erweitern und mit mehr Sicherheit mehr zu erreichen.

Weitere Informationen finden Sie auf diesen Seiten:

- Cortex Xpanse
- Cortex XSOAR
- Cortex XDR
- Cortex XSIAM
- Unit 42

Möchten Sie einen Termin für eine Demo vereinbaren? Dann füllen Sie einfach dieses Formular aus.

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