Wie eine moderne SOAR-Plattform das Bedrohungsdaten-management erleichtert

Die digitale Transformation bringt klare geschäftliche Vorteile, aber auch neue Herausforderungen rund um die Sicherheit mit sich, da innovative Technologien sowohl die Angriffsfläche von Unternehmen als auch das Arsenal der Hacker vergrößern. Dank Cloud-Computing, Automatisierung und künstlicher Intelligenz können Angreifer die Raffinesse und den Umfang ihrer Kampagnen mit geringem Aufwand auf ein bisher ungekanntes Maß steigern. Insofern ist es nicht überraschend, dass derzeit im Durchschnitt alle 39 Sekunden ein Angriff auf einen Computer stattfindet[1] und dass laut Cybersecurity Ventures für das Jahr 2021 alle 11 Sekunden eine erfolgreiche Ransomware-Attacke auf eine Unternehmensinfrastruktur zu erwarten ist.[2]

1. „Hackers Attack Every 39 Seconds", Security Magazine, 10. Februar 2017, https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds
2. „Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021", Cybercrime Magazine, 7. Dezember 2018, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021

Das wirft die Frage auf, wie Unternehmen mit dieser rasanten Entwicklung Schritt halten können. Wie lassen sich flächendeckend effektive Sicherheitsmaßnahmen implementieren, ohne dass der Geschäftsbetrieb beeinträchtigt wird? Hier spielt das Security Operations Center (SOC) eine zentrale Rolle. Um die komplexen Bedrohungen von heute und morgen im Griff zu behalten, sollten SOC-Teams integrierte Sicherheitstechnologien einrichten, Sicherheitsprozesse straffen und ihre eigenen Fähigkeiten in den Bereichen Erkennung, Untersuchung und Abwehr kontinuierlich aktualisieren und erweitern.

Das ist jedoch leichter gesagt als getan, da viele kleine und große Sicherheitsteams überlastet sind. Infolge des Fachkräftemangels sind sie oft unterbesetzt und zudem erschweren eine Flut unzuverlässiger Warnmeldungen, voneinander isolierte Tools und ein Mangel an Kontextinformationen vielerorts die Arbeit. Deshalb müssen wir uns zunächst ein genaues Bild von den Arbeitsabläufen und den schwierigen Aufgaben der SOC-Teams machen, bevor wir effektive Lösungen und Strategien zur Bewältigung der aktuellen Herausforderungen formulieren können.

Ein guter Einstiegspunkt ist ein Blick auf die drei Arten von Spezialisten, aus denen sich die SOC-Teams größerer Unternehmen zusammensetzen: SOC-Analysten, Incident-Response-Experten und Bedrohungsanalysten.

SOC-Analysten

SOC-Analysten überprüfen Tag für Tag tausende Warnmeldungen, die von internen SIEM- und EDR-Systemen sowie hunderten weiteren Sicherheitstools ausgegeben werden. Dabei übernehmen sie nicht nur die Identifizierung und Untersuchung akuter Bedrohungen und ihrer Ursachen, sondern sind auch an der schnellen Reaktion auf Sicherheitsvorfälle beteiligt. Ihre wichtigste Waffe sind leistungsstarke Erkennungs- und Analysetools zur kontinuierlichen Überwachung des Netzwerks. Nach der Aufdeckung eines potenziellen Risikos liegt es in ihrer Verantwortung, die bei der Untersuchung dieser Gefahr gewonnenen Erkenntnisse zu dokumentieren und wichtigen Entscheidungsträgern mögliche Gegenmaßnahmen zu empfehlen.

Bei der Erledigung dieser Aufgaben sind die SOC-Analysten oft mit den folgenden Hürden konfrontiert:

- **Warnungsmüdigkeit:** Die Sicherheitsinfrastruktur eines Unternehmens erzeugt durchschnittlich über 11.000 Warnmeldungen pro Tag.[3] Die meisten Sicherheitsteams haben nicht genug Mitarbeiter, um alle zu bearbeiten.
- **Zeitmangel:** Manuelle Administrations- und Routineaufgaben nehmen zu viel Zeit in Anspruch. Zudem erhöht die mangelnde Integration der von den Analysten verwendeten Tools die Dauer sämtlicher Sicherheitsprozesse.
- **Unzureichende Kontextinformationen:** Die Untersuchung und Abwehr einer akuten Bedrohung dauert oft mehrere Tage, Da die vorhandenen Tools keinen umfassenden Überblick über die Gefahr bieten und die Analysten die benötigten Kontextinformationen selbst finden und zu einem Gesamtbild zusammensetzen müssen.

Um diese Schwierigkeiten zu überwinden, benötigen die Analysten:

- **Tools zur Automatisierung** täglich anfallender Routineaufgaben, damit sie sich auf die wirklich wichtigen Schritte konzentrieren können
- **Lösungen für die Kommunikation und Zusammenarbeit in Echtzeit** zur Koordination von Maßnahmen und zur Förderung eines reibungslosen Informationsflusses im Team
- Mit Kontextinformationen angereicherte **Bedrohungsdaten,** die Aufschluss über den Schweregrad eines Vorfalls und die potenziellen Auswirkungen geben

Abbildung 1: Herausforderungen für SOC-Analysten

Incident-Response-Experten

Incident-Response-Experten kümmern sich vor allem um die Schadensbegrenzung. Sie suchen nach Hinweisen auf Sicherheitsverletzungen und sind im Ernstfall für die Untersuchung und Eindämmung der Bedrohung zuständig. Dabei müssen sie alle Indizien und forensischen Beweise sorgfältig sichern und an die zuständigen Entscheidungsträger übermitteln. Zur Erledigung dieser Aufgaben benötigen die betreffenden Teams zum einen effektive EDR-Lösungen, mit denen infizierte Endpunkte isoliert werden können, zum anderen leistungsstarke Tools für die Firewalladministration, die die unternehmensweite Implementierung von Sicherheitsrichtlinien unterstützen und auf diese Weise die Ausbreitung von Bedrohungen auf Netzwerkebene verhindern. Darüber hinaus erfordern die Planung und Umsetzung präziser Gegenmaßnahmen die Heranziehung externer Bedrohungsdaten, die ein genaues Bild der Angreifer und ihrer Vorgehensweise zeichnen.

Infolgedessen sind Incident-Response-Experten vor allem mit den folgenden Herausforderungen konfrontiert:

- **Stockungen im Informationsfluss,** die die teamübergreifende Zusammenarbeit behindern und zu Sicherheitslücken führen
- Ineffiziente Lösungen für das **Fallmanagement**, die nicht für die Dokumentation von Sicherheitsvorfällen ausgelegt sind
- **Unnötige Verzögerungen und Risiken** durch manuelle, fehlerbehaftete Prozesse zur Zusammenführung und Bereitstellung von Bedrohungsdaten und Kontextinformationen

Um hier Abhilfe schaffen zu können, benötigen die betreffenden Teams:

- **Leistungsstarke Fallmanagementtools,** die für die Dokumentation von Sicherheitsvorfällen ausgelegt sind und sowohl den Austausch mit anderen Entscheidungsträgern als auch die Umsetzung von Präventions- und Quarantänemaßnahmen im gesamten Unternehmen unterstützen
- **Bedrohungsdaten,** die detaillierte Informationen zu den Angreifern und ihren Motiven beinhalten

Abbildung 2: Herausforderungen für Incident-Response-Experten

3. Diese Angabe stammt aus einer von Forrester Consulting im Auftrag von Palo Alto Networks durchgeführten Studie (Februar 2020).

Bedrohungsanalysten

Bedrohungsanalysten sind dafür zuständig, potenzielle Risiken zu identifizieren, bevor das Unternehmensnetzwerk infiltriert wird. Zu diesem Zweck gleichen sie Informationen aus verschiedenen externen Bedrohungsdatenfeeds mit von Experten zusammengestellten Daten ab. Laut einer aktuellen Umfrage des SANS Institute verfügen bereits 49,5 Prozent der Unternehmen über ein Bedrohungsanalyseteam oder -programm mit einem eigenen Budget und dediziertem Personal.[4] Das ist ein deutlicher Beleg für die zunehmend wichtige Rolle der Bedrohungsanalysten bei der Identifizierung von Angreifern und der Ermittlung ihrer Motive, Methoden und Prozesse. Die betreffenden Experten stellen sowohl Erkenntnisse über spezifische Angriffe als auch Informationen zur Gesamtbedrohungslage bereit, um SOC- und Incident-Response-Teams bei präventiven Maßnahmen zur Bedrohungsabwehr zu unterstützen.

Dabei stehen sie häufig vor den folgenden Hindernissen:

- **Mangelnde Kontrolle** über die Bedrohungsdatenfeeds, sodass die bereitgestellten Gefahrenindikatoren manuell angepasst und bewertet werden müssen
- **Voneinander isolierte Workflows,** die ein effektives Zusammenspiel der für die Bedrohungsabwehr und -analyse eingesetzten Teams, Tools und Prozesse verhindern
- **Schwierigkeiten bei der Operationalisierung von Bedrohungsdaten,** die oft auf manuellen Prozessen und der Zuarbeit anderer Teams basiert

Deshalb benötigen Bedrohungsanalysten:

- **Zugriff auf trennscharfe Bedrohungsindikatoren,** die die Implementierung logischer und reputationsbasierter Sicherheitsregeln auf der Grundlage geschäftlicher Anforderungen erleichtern
- **Tools für die reibungslose Zusammenarbeit** mit anderen Teams, damit aussagekräftige Kontextinformationen und aktuelle Ergebnisse ohne Zeitverlust bereitgestellt werden können
- **Leistungsstarke Dokumentationsfunktionen** zur Erstellung von Ergebnisberichten

Abbildung 3: Herausforderungen für Bedrohungsanalysten

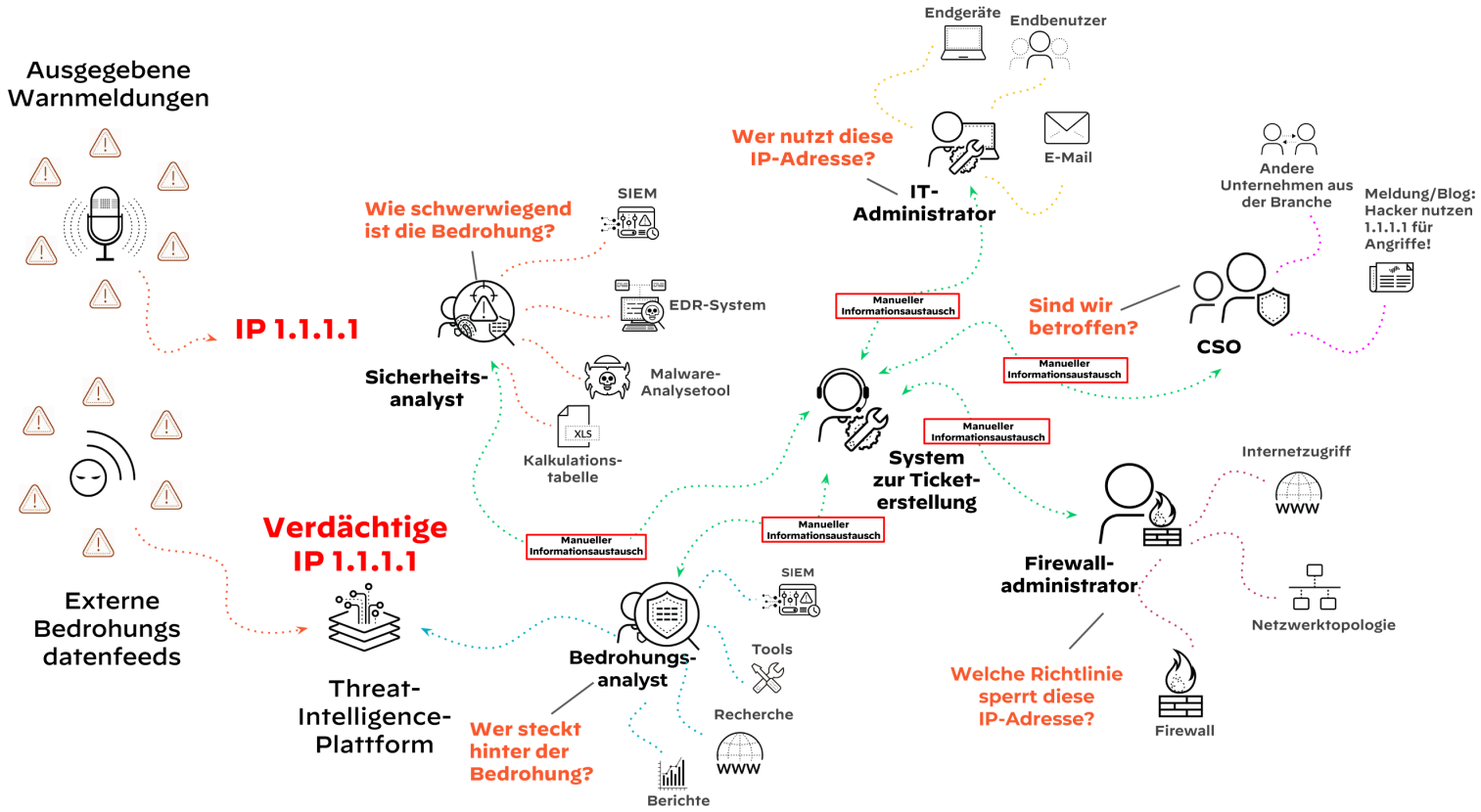

Abbildung 4: Holistischer Blick auf einen typischen Arbeitstag im SOC

4. „2020 SAN Cyber Threat Intelligence (CTI) Survey", SANS Institute, 11. Februar 2020, https:/www.sans.org/reading-room/whitepapers/threats/paper/39395.

SOAR als Retter in der Not

Die verschiedenen Spezialistenteams haben eines gemeinsam: Sie benötigen leistungsstarke, mit Bedrohungsdatenfeeds gespeiste Tools, die die Prozessautomatisierung, das Fallmanagement und die Zusammenarbeit in Echtzeit unterstützen. Zwar nutzen viele SOCs spezielle SOAR-Plattformen (Security Orchestration, Automation and Response), um Warnmeldungen aus verschiedenen Quellen zusammenzuführen, Prozesse auf der Grundlage von digitalen Leitfäden (sogenannten Playbooks) zu standardisieren und automatische Gegenmaßnahmen für verschiedene Sicherheitsvorfälle zu implementieren. Doch ist dieser Ansatz nicht zur Bewältigung der weitverbreiteten Defizite im Bereich Bedrohungsdatenmanagement geeignet.

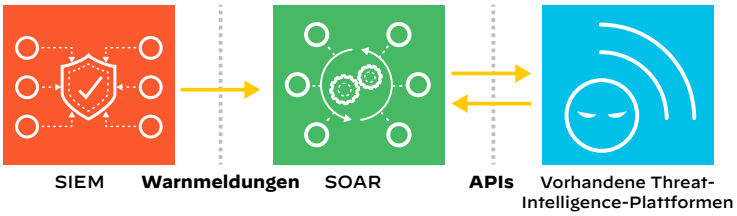

Abbildung 5: Typische Sicherheitsinfrastruktur mit voneinander isolierten SOAR- und Threat-Intelligence-Plattformen

Viele Sicherheitsteams setzen nach wie vor eigenständige Threat-Intelligence-Plattformen (TIPs) ein, um sich aus externen Quellen über Bedrohungen zu informieren. Dabei müssen sie meist feststellen, dass die TIPs hinter den Versprechungen der Anbieter zurückbleiben, weil sie die verschiedenen Feeds weder miteinander noch mit unternehmensintern erhobenen Sicherheitsdaten abgleichen und dadurch die Auswahl der für die Implementierung automatisierter Abwehrmaßnahmen am besten geeigneten Indikatoren erschweren. Branchenanalysten haben dieses Problem erkannt und regen die Zusammenführung der SOAR- und TIP-Lösungen an. Die Zeit ist also reif für einen alternativen Ansatz.

Moderne Unternehmen benötigen eine erweiterte SOAR-Plattform

Mit nativen Tools für das Bedrohungsdatenmanagement erweist sich Cortex™ XSOAR als passende Lösung für die aktuellen Herausforderungen. Die erweiterte SOAR-Plattform führt die Aggregation, Operationalisierung und Verteilung von

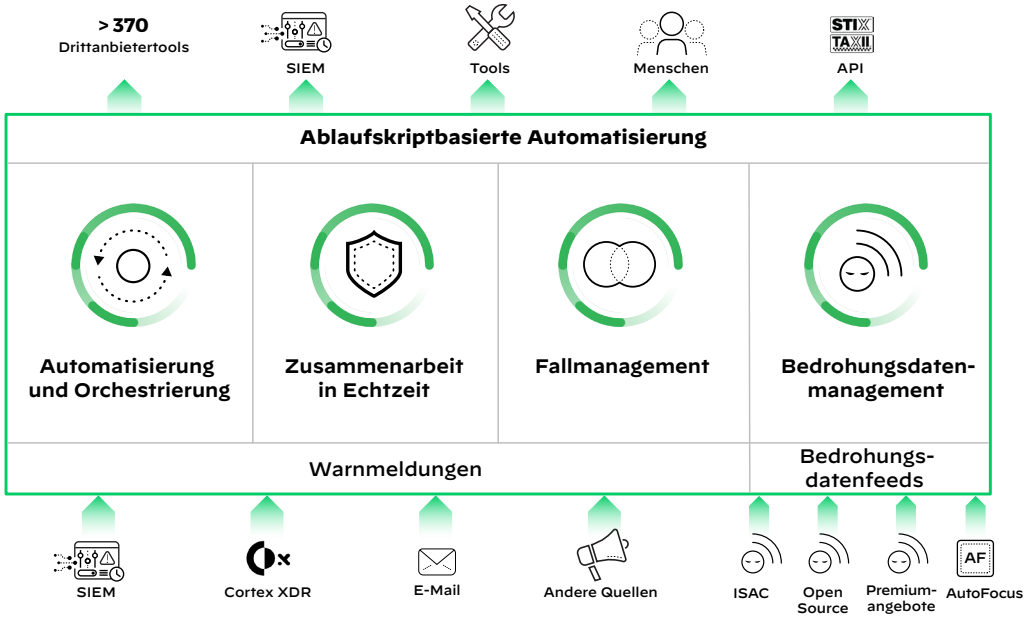

Abbildung 6: Playbook-basierte Automatisierung mit Cortex XSOAR

Bedrohungsdaten an zentraler Stelle zusammen und unterstützt außerdem die Playbook-basierte Automatisierung. Dadurch ist sichergestellt, dass Sicherheitsexperten stets über alle nötigen Informationen und Indikatoren zur präzisen, unternehmensweiten Bekämpfung kritischer Bedrohungen verfügen.

Abbildung 7: Vorteile des effektiven Managements von Bedrohungsdaten

Cortex XSOAR vereint Fallmanagement, Automatisierung, Zusammenarbeit in Echtzeit und natives Bedrohungsdatenmanagement in der branchenweit ersten erweiterten Plattform für Sicherheitsorchestrierung, -automatisierung und -reaktion.

Damit können Ihre Experten:

- **Die Zahl der manuellen Prozesse reduzieren** – mit automatisierten Aggregations-, Parsing-, Deduplizierungs-, Bewertungs- und Verwaltungsfunktionen für Millionen täglich bereitgestellter Bedrohungsindikatoren aus verschiedenen Quellen. Dadurch können stets die Indikatoren genutzt werden, die für die jeweilige Umgebung am besten geeignet sind.
- **Kritische Bedrohungen aufdecken,** Warnmeldungen priorisieren und intelligentere Entscheidungen treffen, indem sie Bedrohungsdaten aus externen Quellen mit intern erhobenen Sicherheitsdaten abgleichen. Generell ermöglichen die von Palo Alto Networks AutoFocus™ bereitgestellten Kontextinformationen schnellere und präzisere Vorfallsuntersuchungen und lassen sich in jedes Erkennungs-, Monitoring- und Sicherheitstool einspeisen.
- **Automatisierte Gegenmaßnahmen einleiten,** um akute Bedrohungen sofort unternehmensweit zu bekämpfen. Zusätzlich erleichtert wird dies durch nutzerfreundliche Mechanismen zur Weiterleitung von Bedrohungsdaten an interne Teams und vertrauenswürdige Organisationen.

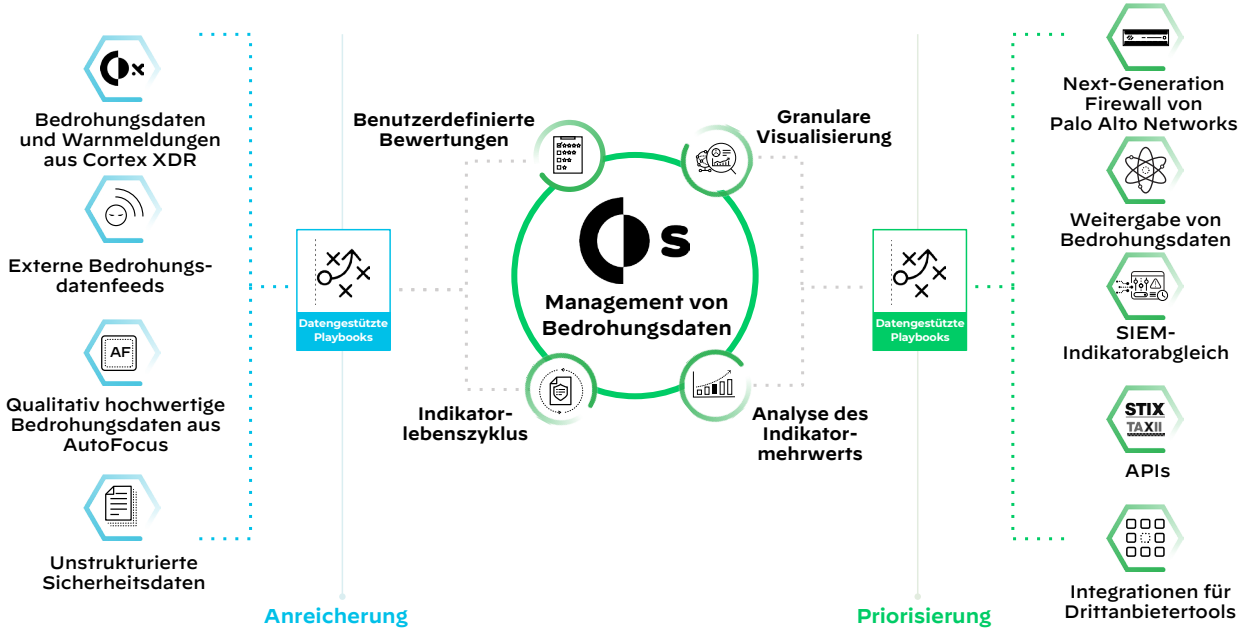

Abbildung 8: Anreicherung und Priorisierung mit einer modernen Lösung für das Bedrohungsdatenmanagement

Anwendungsfall: Die Priorisierung von Indikatoren

Moderne Unternehmen haben oft hunderte verschiedener Bedrohungsdatenfeeds abonniert, die ihren Sicherheitsanalysten tagtäglich Millionen von Bedrohungsindikatoren liefern. Allerdings erfolgt die Bereitstellung dieser Indikatoren meist ohne die Kontextinformationen, die für informierte Entscheidungen, effektive Maßnahmen und präzise Reaktionen benötigt werden. Erschwerend kommt hinzu, dass die vorhandenen Tools nicht für das enorme Datenvolumen ausgelegt sind, sodass die Analysten die Priorität der Indikatoren manuell und nach eigenem Ermessen an die Infrastruktur ihres Unternehmens anpassen müssen. Deshalb verfügt Cortex XSOAR über integrierte Funktionen für das Bedrohungsdatenmanagement, die überlasteten Analysten die Möglichkeit bieten, Indikatoren auf der Grundlage beliebiger Geschäftslogiken zu bewerten. Dank der vorkonfigurierten Integrationen für über 370 Drittanbieter können Indikatoren in Echtzeit in die Sicherheitsinfrastruktur eingespeist und zur Bedrohungsabwehr genutzt werden.

Abbildung 9: Gängige Herausforderungen bei Verwendung isolierter Tools für das Management von Bedrohungsdaten

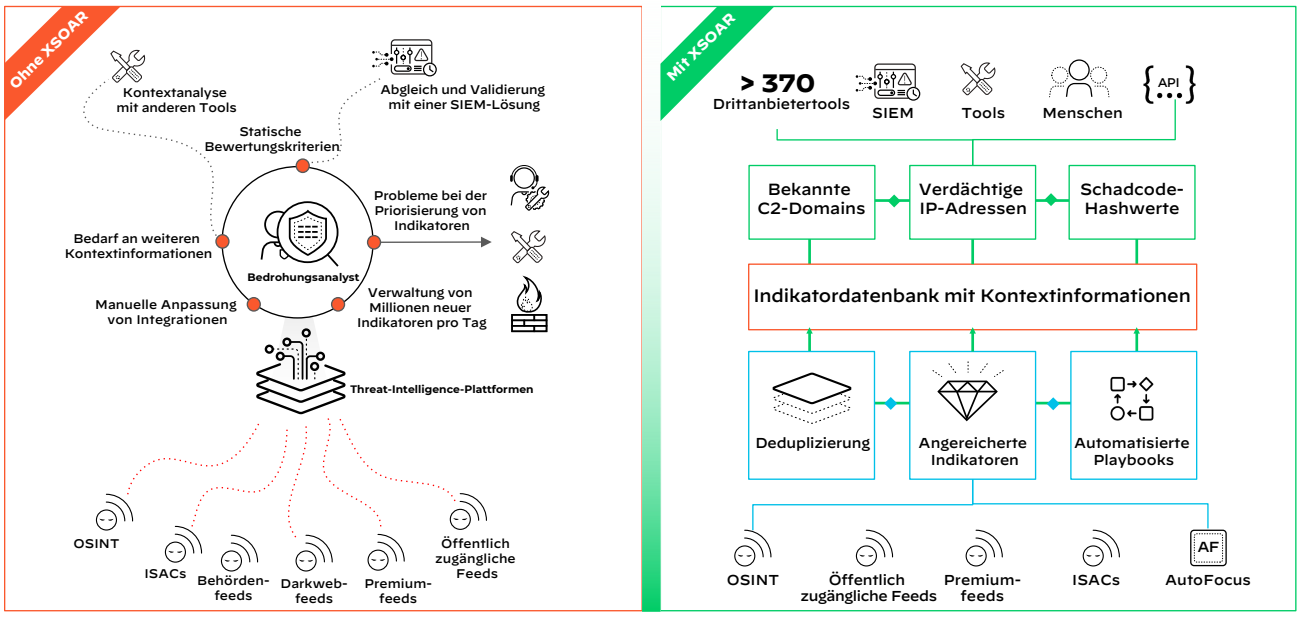

Abbildung 10: Bedrohungsdatenmanagement mit und ohne Cortex XSOAR

Abbildung 11: Vorteile von Cortex XSOAR für Ihr SOC

Die Vielseitigkeit von Cortex XSOAR

Die offene und erweiterbare Plattform Cortex XSOAR ist für ein breites Spektrum an Anwendungsszenarien ausgelegt und unterstützt sogar Prozesse außerhalb des Verantwortungsbereichs der SOC- und Incident-Response-Teams. gängigsten Anwendungsbereichen gehören das Blockieren von Phishing-angriffen, routinemäßige Sicherheitsprozesse, die Bearbeitung sicherheitsrelevanter Warnmeldungen, die Orchestrierung der Cloud-Sicherheit, das Schwachstellenmanagement und die proaktive Suche nach Bedrohungen.

Dank der in die Plattform integrierten Funktionen für das Bedrohungsdatenmanagement können Ihre Teams die strikte Trennung der datenbezogenen Abläufe von den übrigen Sicherheitsprozessen überwinden. Dadurch werden SOC-Analysten, Incident-Response-Experten und Bedrohungsanalysten in die Lage versetzt, ihre Maßnahmen zu koordinieren und die unternehmensinterne Kommunikation, Effizienz und Weitergabe gewonnener Erkenntnisse zu verbessern.

Als erste erweiterte SOAR-Plattform der Branche eröffnet Cortex XSOAR Ihrem Unternehmen in Sachen Orchestrierung, Automatisierung, Bedrohungsabwehr und Fallmanagement neue Möglichkeiten, damit Ihre Mitarbeiter heute und in Zukunft mit den Angreifern Schritt halten können.

Weitere Informationen zu diesem Produkt finden Sie auf unserer Website.

Oval Tower, De Entrée 99-197
1101 HE Amsterdam
Niederlande
+31 20 888 1883
www.paloaltonetworks.de

how-cortex-is-transforming-threat-intelligence-wp-100120-de