XDR: Unternehmensweite Bedrohungserkennung und -abwehr

Was Sie über die Lösungen wissen sollten, die Daten aus Datensilos zusammenführen und Sicherheitsprozesse revolutionieren

Inhalt

CORTEX XDR™ BY PALO ALTO NETWORKS

Einleitung

Der Schutz kritischer Daten ist eine Herausforderung, die Jahr für Jahr größer wird. Cloud-Computing, das Internet der Dinge und andere moderne Technologien tragen maßgeblich dazu bei, dass die Angriffsfläche von Unternehmen und die Anfälligkeit sensibler Daten für raffinierte Cyberangriffe stetig zunehmen. Hacker nutzen diese modernen Technologien, um immer größere und gefährlichere Angriffskampagnen zu starten und um dieselben Infrastrukturen immer und immer wieder anzugreifen, bis sie einmal erfolgreich sind. Das reicht leider schon aus. Zukünftige Technologien werden beide Probleme voraussichtlich noch verschärfen.

Sicherheitsteams haben verschiedene Tools, Prozesse und sogar unterschiedliche Modelle zur Besetzung von Sicherheitspositionen ausprobiert, um ihre Unternehmen vor immer neuen Angriffen zu schützen, sehen sich aber zu oft Angreifern gegenüber, die ihnen zahlenmäßig überlegen und besser ausgerüstet sind. Hinzu kommt, dass durch das ständige Aufsetzen neuer Funktionen auf vorhandene Systeme ein kompliziertes Gewirr aus schlecht integrierten Tools entstanden ist, dessen Nutzung viel Zeit, Energie und Erfahrung erfordert. Relativ unerfahrene Analysten sollen trotz ihrer mangelnden Kenntnisse und ähnlich lückenhafter Toolkits die ernstzunehmenden Benachrichtigungen in einem endlosen Strom finden – eine schier unmögliche Leistung. Angesichts der Kombination aus zu vielen Benachrichtigungen und zu wenig Kontext verlieren Sicherheitsteams die Übersicht und geraten gegenüber den Angreifern ins Hintertreffen. Dadurch wird das Unternehmen noch verwundbarer.

Auf dem Markt gibt es für dieses Problem „XDR“, eine Kategorie von Lösungen zur Bedrohungserkennung, -untersuchung und -abwehr, die die verschiedenen Bedrohungsvektoren in der Infrastruktur eines Unternehmens (d. h. Netzwerk, Endpunkte und Cloud) nicht einzeln, sondern gemeinsam betrachten. Dank dieser engeren Integration generieren XDR-Tools bessere Übersichten und Einblicke, die nicht nur menschlichen Analysten zur Verfügung gestellt, sondern auch zur Verbesserung der KI-Modelle genutzt werden, auf denen XDR-Tools basieren.

„Cyberkriminalität ist die größte Bedrohung für jedes Unternehmen weltweit.”

Quelle: Ginni Rometty, CEO, IBM

CORTEX XDR BY PALO ALTO NETWORKS

Über diesen Leitfaden

Sie brauchen dringend Informationen über XDR und ihre Bedeutung für Ihr Unternehmen? Dann sind Sie hier richtig. Im Folgenden legen wir dar, was XDR ist (und was nicht), was sie kann, für welche Einsatzszenarien sie geeignet ist und welche Auswirkungen sie auf die wichtigsten Elemente der Security Operations (SecOps) hat. Außerdem beschreiben wir Vorteile von XDR gegenüber herkömmlichen Tools für die Bedrohungserkennung und -abwehr und erläutern, auf welche Funktionen und Features Sie bei der Auswahl einer XDR-Lösung achten sollten und wie Sie Ihre Sicherheitsprozesse mit XDR straffen und verbessern können.

Die Herausforderung

Die Berichte über Datendiebstähle und raffinierte Cyberangriffe sind so zahlreich geworden, dass sie kaum noch Beachtung finden. Im Geschäftsleben ist es schon zum Klischee geworden, dass jeder Feinde hat, „ob er das weiß oder nicht“. Das macht Ihre Feinde jedoch nicht weniger gefährlich. Fakt ist, dass jede Minute, in der ein Hacker in Ihrer Infrastruktur tätig ist, unvorstellbaren Schaden verursachen kann. Als Sicherheitsexperte wissen Sie das natürlich längst und arbeiten hart daran, Angriffe so schnell wie möglich zu erkennen und zu blockieren – bevor die Angreifer sensible Daten finden und ausschleusen.

Doch angesichts der immer perfideren Angriffsmethoden und -taktiken ist das ein ungleicher Kampf. Technisch versierte Angreifer benötigen nicht einmal mehr Malware, um fremde Geräte unter ihre Kontrolle zu bringen. Stattdessen hacken sie beispielsweise autorisierte Systemdateien oder die Geräteregistrierung oder missbrauchen Utilities wie PowerShell. Diese neuen Vorgehensweisen können nur mit neuen Erkennungsmethoden aufgedeckt werden.

Tagtäglich werden knapp 4 Millionen digitale Datensätze gestohlen

Quelle: Cybersecurity Ventures

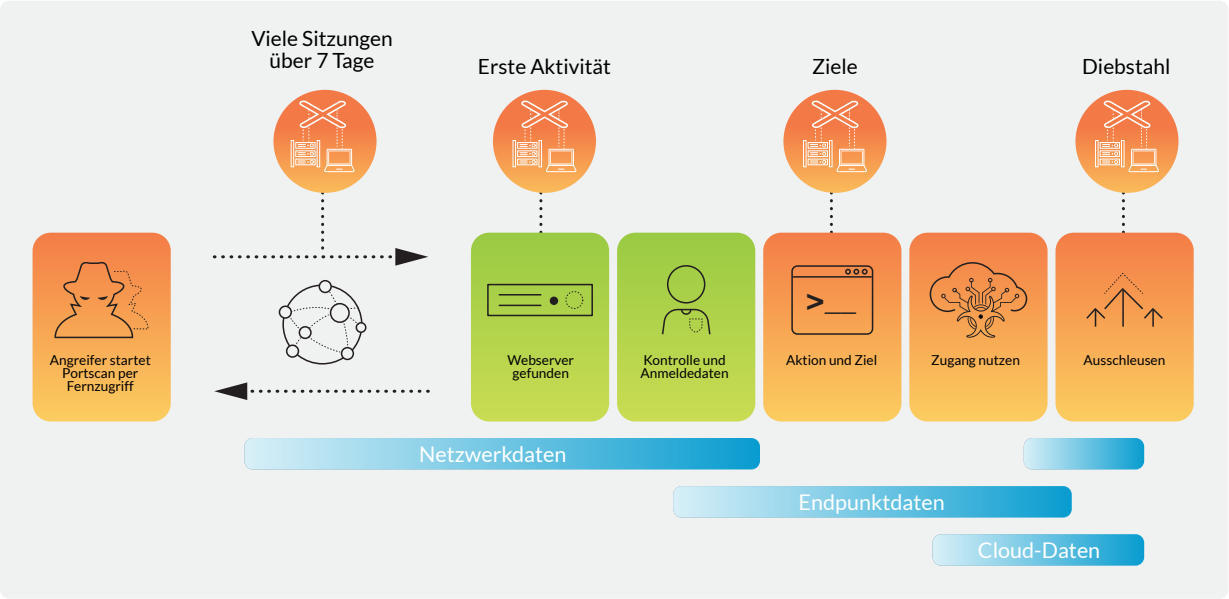

Abbildung 1: Beispiel eines mehrstufigen Angriffs

Für die Verteidiger kommt erschwerend hinzu, dass ihre Infrastrukturen durch Investitionen in neue Technologien wie Cloud und IoT ständig wachsen, weil die Datennutzung immer schneller, flexibler und innovativer werden soll. Angreifer sehen solche Investitionen als neue potenzielle Einfallstore und Chancen, fremde Infrastrukturen zu missbrauchen. Deshalb sollte Ihr Sicherheitsteam die besten verfügbaren Methoden und Tools zur Angriffsprävention anwenden und seine Fähigkeiten zur Angriffserkennung kontinuierlich ausbauen, um die sogenannte Verweildauer (die Zeit, während der ein Angreifer unbemerkt im System aktiv ist) zu verkürzen und schneller auf Angriffe zu reagieren.

Das Missverhältnis

Ob diese Ziele erreicht werden oder nicht, hängt von zwei Faktoren ab: effektiven Tools und einem Team von fähigen Sicherheitsanalysten. Leider ist dieses Gleichgewicht zwischen Technologie und Personal eher die Ausnahme als die Regel.

Erkennungs- und Präventionstechnologien generieren täglich hunderte oder sogar tausende von Benachrichtigungen – viel mehr, als ein Sicherheitsteam bearbeiten kann. Hinzu kommt, dass diese Benachrichtigungen meist aus vielen separaten Quellen stammen, sodass die Analysten sie „von Hand“ zueinander in Beziehung setzen müssen. Zur Analyse einer potenziellen Bedrohung sind in der Regel mehrere Schritte erforderlich:

1) Durchsuchung der verfügbaren Protokolldateien nach Hinweisen, die zur Rekonstruktion des Vorgangs nützlich sind.

2) Manueller Vergleich dieser Hinweise mit Bedrohungsdaten aus einer oder mehreren Quellen, um zu ermitteln, ob es sich um Indikatoren für bekannte Bedrohungen handelt.

3) Identifizierung von fehlenden Informationen und Suche nach verfügbaren Daten, die diese Lücken schließen und möglicherweise auf weitere Schritte im Angriffsverlauf hinweisen.

4) Prüfung, ob diese neuen Hinweise bereits von anderen Teammitgliedern untersucht werden, und falls ja, Koordination der Arbeit.

5) Beurteilung, ob die Meldung eskaliert werden muss, ignoriert werden kann oder ob der Analyst selbst Maßnahmen zur Schadensbehebung einleiten kann.

In 69 % der Unternehmen glauben die Befragten nicht, dass die Antiviren-Software alle Bedrohungen abwehrt.

Quelle: Ponemon Institute

Diese Schritte sind traditionell zeitaufwendig und erfordern die Nutzung mehrerer Tools. Dabei handelt es sich nur um die (auch als Triage bezeichnete) Ersteinschätzung. Infolgedessen haben Analysten meist nur Zeit, den Meldungen mit der höchsten Priorität nachzugehen. Eine beunruhigende Anzahl von Benachrichtigungen mit niedrigerer Priorität bleibt tagtäglich liegen.

Zudem haben die mit der Ersteinschätzung betrauten Sicherheitsanalysten oftmals zu wenig Kontext, um das mit einem Angriff verbundene Risiko korrekt einzuschätzen. Also eskalieren sie Benachrichtigungen im Zweifelsfall an eine höher qualifizierte Gruppe, die dann noch einmal Zeit, Arbeit und Ressourcen in sie investieren muss. Damit pflanzt die Ineffizienz sich im gesamten System fort.

Vielerorts wird versucht, APIs zur Integration von Erkennungs- und Abwehrdaten zu nutzen. Dazu werden die verschiedenen Protokolldateien meist in eine teure SIEM-Lösung eingespeist, die sie durch Parsen und Normalisieren zusammenführt. Leider geht hierbei viel wertvoller Kontext verloren. Die Mitarbeiter des Sicherheitsteams sehen also alle Protokolldateieinträge in einem Fenster, doch sie sind nicht sinnvoll miteinander verknüpft. Zu den umfassenderen Rohdaten haben die für die Ersteinschätzung verantwortlichen Analysten hingegen oft keinen Zugang.

Andere Unternehmen übertragen die Verantwortung für die Bedrohungserkennung und -abwehr ganz oder teilweise an Managed Security Services Provider (MSSP) oder die noch mehr auf die Bedrohungserkennung spezialisierten Anbieter von Managed Detection and Response (MDR). Insbesondere für Unternehmen, die sich keine eigene Sicherheitsabteilung leisten können oder wollen, kann dies eine gute Option sein. Unternehmen und Institutionen, die Wert auf umfassende Transparenz und Kontrolle legen, sollten jedoch nicht zum Outsourcing gezwungen sein, nur weil ihre vorhandenen Tools unzureichend sind. Der richtige Technologiestack ist im Übrigen auch für externe Sicherheitsanbieter wichtig. Wenn diese Ihre Infrastruktur mit veralteten Tools schützen sollen, werden auch sie mit den oben beschriebenen Ineffizienzen zu kämpfen haben.

Was wirklich gebraucht wird, sind Technologien, die die Gesamtzahl der Benachrichtigungen senken und es auch weniger erfahrenen Analysten ermöglichen, Bedrohungen zuverlässig und effizient einzuschätzen, sodass sie nur wirklich ernstzunehmende Benachrichtigungen an die höher qualifizierten Analysten weiterreichen müssen.

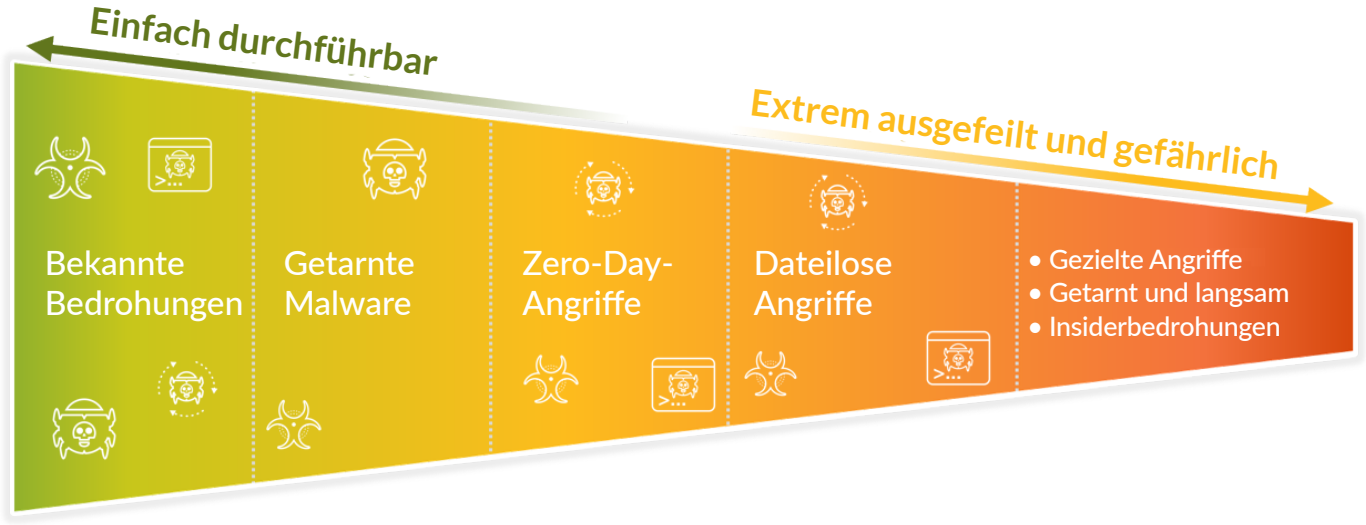

Abbildung 2: Tools für die Bedrohungserkennung und -abwehr sind für raffinierte und komplexe Angriffe ausgelegt

Technologien zur Bedrohungserkennung und -abwehr

Natürlich besteht das Ziel eines Sicherheitsteams darin, möglichst alle Angriffe zu blockieren. Fakt ist jedoch, dass es einzelnen Angreifern immer wieder gelingen wird, in fremde Infrastrukturen einzudringen und dort Schaden anzurichten. Deshalb müssen Sicherheitsteams auch auf diese Situation vorbereitet sein. Am Markt gibt es eine ganze Palette von Tools für die Protokollierung, Erkennung und Abwehr von Bedrohungen, die die erste Linie von Schutzmaßnahmen umgangen haben. Jedes dieser Tools hat seine Stärken und Schwächen und seine Daseinsberechtigung, beispielsweise zum Blockieren relativ einfacher Angriffe, bei denen bekannte dateibasierte Malware eingesetzt oder ein bestimmter Teil der Infrastruktur angegriffen wird. Die meisten haben aber nur ein enges Einsatzgebiet, und es gibt keines, das wirklich gut zur Erkennung komplexer Angriffskampagnen geeignet ist. Aus diesen Gründen setzen Sicherheitsteams hauptsächlich auf die in den folgenden Abschnitten beschriebenen Lösungen.

EDR

Definition von Gartner: ***Endpoint Detection and Response (EDR)*** *beschreibt Lösungen, die das Systemverhalten an Endpunkten aufzeichnen, mit verschiedenen Datenanalysetechniken verdächtiges Systemverhalten erkennen, Kontextinformationen bereitstellen, schädliche Aktivitäten blockieren und Behebungsvorschläge zur Wiederherstellung betroffener Systeme machen. EDR-Lösungen müssen die folgenden vier Hauptfunktionen bieten:*

- *Erkennung von Sicherheitsvorfällen*
- *Eindämmung von Vorfällen am Endpunkt*
- *Untersuchung von Sicherheitsvorfällen*
- *Empfehlungen zur Schadensbehebung*

Die IDC sagt bis 2022 ein durchschnittliches Jahreswachstum von 9,9 % bei den Ausgaben für die Sicherheit voraus.

Quelle: Worldwide Security Spending Guide, IDC

Endpoint Detection and Response (EDR) kam erstmals 2013 bei forensischen Untersuchungen zum Einsatz, bei denen sehr detaillierte Endpunkttelemetrie für das Reverse Engineering von Malware und zur Rekonstruktion des Angriffsverlaufs auf einem infiltrierten Gerät benötigt wurde.

Da EDR-Lösungen sich ausschließlich auf Endpunkte konzentrieren, können sie allein keine vollständige Bedrohungserkennung in einem Unternehmen leisten. Zudem sind sie nur mithilfe spezieller Agenten auf Geräten (IoT, BYOD, ICS sowie Switches, Router, Server usw.) und in Cloud-Ressourcen (z. B. Workloads, Cloud-Netzwerke, PaaS) in der Lage, Einblicke in den Netzwerkverkehr der Endpunkte zu bieten. Unternehmen nutzen allerdings auch viele nicht verwaltete Endpunktgeräte, die keine EDR-Agenten unterstützen und daher nicht mit EDR vor potenziellen Angreifern geschützt werden können.

SIEM

Definition von Gartner: ***Security Information and Event Management (SIEM)*** *ist eine Technologie zur Unterstützung von Bedrohungserkennung, Compliance- und Vorfallsmanagement durch die Erfassung und Analyse von Sicherheitsvorfällen und anderer Ereignisse und Kontextdaten aus verschiedensten Quellen (sowohl nahezu in Echtzeit als auch rückblickend). Zu den Kernfunktionen gehören die umfassende Protokollierung und Verwaltung von Ereignissen, Funktionalität zur Analyse protokollierter Ereignisse und anderer Daten aus unterschiedlichen Quellen sowie Bearbeitungsfunktionen wie Incident Management, Dashboards und Berichterstellung.*

Viele SecOps-Teams geben einen großen Teil ihres Budgets für SIEM-Tools aus, um die Protokolldateien von Sicherheitsgeräten (IDS/FW) und Serverumgebungen (Ereignis-Logs) zusammenzuführen. Tatsächlich wurden SIEM-Lösungen ursprünglich zur Zusammenführung von Protokolldateien für die Compliance-Berichterstellung entwickelt. Später wurde ihre Funktionalität um die Bedrohungserkennung erweitert und inzwischen werden sie in vielen Security Operations Centers (SOCs) als zentrales Repository für Benachrichtigungen genutzt.

Laut Daten von Gartner ist die Sicherheit heute der wichtigste Grund für steigende IT-Ausgaben und die Bedrohungserkennung und -abwehr ist dabei der teuerste Posten.

Quelle: Gartner

SIEM-Systeme führen die Benachrichtigungen von vielen Sicherheits- und Netzwerkgeräten zusammen und weisen auf geräteübergreifende Angriffe hin. Für anspruchsvollere Anwendungsszenarien sind SIEM-Lösungen allerdings eher ungeeignet, da sie auf festen, einprogrammierten Regeln basieren. Nutzt ein findiger Angreifer ein neues Muster, wird dies von einem SIEM-System wahrscheinlich nicht erkannt. Zudem enthalten die Protokolldateieinträge, die bei SIEM-Analysen genutzt werden, nur wenig Kontext zur Überprüfung der Meldungen, da dieser bei der Normalisierung verloren geht. Daher müssen in der Regel weitere Systeme herangezogen werden, um festzustellen, ob ein Gerät wirklich infiltriert wurde bzw. ob Daten ausgeschleust wurden oder werden.

NTA und UEBA

Definitionen von Gartner:

Network Traffic Analysis (NTA) *analysiert den Datenverkehr in Unternehmensnetzwerken anhand einer Kombination aus maschinellem Lernen, intelligenter Analyse und regelbasierter Erkennung verdächtiger Aktivitäten. NTA-Tools analysieren fortlaufend Roh- bzw. Flow-Daten (beispielsweise NetFlow) und erstellen Modelle des normalen Netzwerkverhaltens. Wenn das NTA-Tool ein von diesem Modell abweichendes Traffic-Muster erkennt, generiert es eine Benachrichtigung. Zusätzlich zur Überwachung des ein-/ausgehenden Traffics am Perimeter können NTA-Lösungen auch die interne Kommunikation überwachen, indem sie die Datenflüsse an strategisch platzierten Sensoren analysieren.*

User and Entity Behavior Analytics (UEBA) *nutzt verschiedene einfache Analysemethoden (z. B. Regeln zur Untersuchung von Signaturen, Mustervergleiche und einfache Statistiken) und anspruchsvolle Analyseverfahren (wie überwachtes und unüberwachtes maschinelles Lernen), um Profile von Nutzern und Objekten zu erstellen und Abweichungen von deren normalem Verhalten zu erkennen. Anbieter von UEBA-Lösungen nutzen Analysepakete zur Auswertung des Verhaltens von Anwendern und Objekten (Hosts, Anwendungen, Netzwerkverkehr und Datenspeichern), um potenzielle Vorfälle zu erkennen.*

Schließlich wurde eine neue Kategorie von Sicherheitsanalysetools entwickelt, um die Herausforderungen zu bewältigen, mit denen SIEM-Systeme bei der Erkennung unbekannter Angriffe konfrontiert sind. Zu dieser neuen Kategorie gehören NTA und UEBA. Diese Tools erfassen Telemetriedaten und nutzen maschinelles Lernen, um aufgrund dieser Daten ein Modell des Normalzustands zu erstellen. Von diesem Modell abweichendes Verhalten wird als potenzieller Hinweis auf verdächtiges Verhalten betrachtet. Mit diesen Technologien können auch bisher unbekannte Angriffe anhand ungewöhnlicher Traffic-Muster entdeckt werden.

Auch diesen Tools sind jedoch Grenzen gesetzt. Netzwerkbasierte Produkte sind auf das Netzwerk beschränkt und können keine lokalen Ereignisse überwachen oder verfolgen wie beispielsweise auf Endpunkten erfasste Informationen. NTA geht außerdem nicht sehr tief: Während EDR einzelne Endpunkte sehr gründlich beobachtet, analysiert die NTA zwar großflächig, aber nur oberflächlich. UEBA-Tools sind bei ihrer Suche nach Sicherheitsbedrohungen auf Netzwerken und Endpunkten auf die Protokolldateien anderer Produkte angewiesen. Die UEBA analysiert die gemeldeten Bedrohungen und weist den einzelnen Anwendern Risikoeinschätzungen zu. Wenn die Drittprodukte jedoch bei der Erkennung versagen oder einen Teil der Infrastruktur nicht überwachen, wird die UEBA unwirksam.

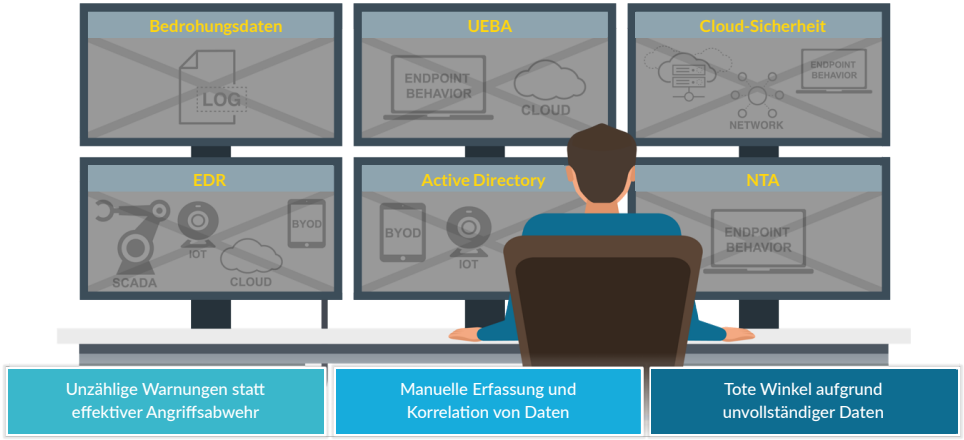

Abbildung 3: Disparate Tools erschweren die Untersuchung und die Reaktion

Fazit

Aufgrund der Komplexität moderner Angriffe müssen Daten aus verschiedenen Quellen analysiert werden, um verdächtige Aktivitäten zu erkennen und zu validieren. Die Nutzung mehrerer Punktlösungen lässt möglicherweise tote Winkel entstehen und ist zudem teuer und zeitaufwendig für die Sicherheitsanalysten, die ständig zwischen den verschiedenen Anwendungen hin- und herschalten müssen, um einen Angriff nachzuvollziehen. 451 Research hat ermittelt, dass 76 % der Sicherheitsteams mindestens ein Viertel der erkannten Angriffe durch manuelle Bedrohungssuche finden, was darauf hinweist, dass die genutzten Erkennungstechnologien und -prozesse unzureichend sind. Das bedeutet, dass Sicherheitsteams Bedrohungen leicht übersehen können, wenn sie keinen vollständigen Überblick über alle Komponenten in ihrer Infrastruktur haben.

Gegen den Fachkräftemangel

Selbst mit den neuen, besseren und umfassenderen Tools für die Bedrohungserkennung sind qualifizierte Fachleute für die Ersteinschätzung von Benachrichtigungen – und potenziellen Vorfällen – erforderlich. Leider gibt es jedoch nicht genug dieser Sicherheitsexperten, was für die betroffenen Unternehmen im Kampf gegen Angreifer ein erheblicher Nachteil ist.

Kriminelle nutzen inzwischen hochgradig automatisierte Angriffe, um Schwachstellen zu finden und sich Zugang zu fremden Systemen zu verschaffen. Dadurch werden die Auswirkungen des Fachkräftemangels noch verschärft, denn die Angreifer können ihre automatisierten Toolkits schneller und kostengünstiger skalieren als Unternehmen neue, qualifizierte Mitarbeiter finden und einarbeiten können. Deshalb sollten Sie nach Tools Ausschau halten, die auch Ihre weniger erfahrenen Mitarbeiter leistungsfähiger und effizienter machen, indem sie monotone Aufgaben automatisieren, Untersuchungen vereinfachen und Ihre Analysten beim Ausbauen ihrer Fähigkeiten unterstützen.

Laut ESG Research herrscht in 66 % der Unternehmen die Ansicht, dass die Bedrohungserkennung und -abwehr darunter leidet, dass mehrere separate Tools verwendet werden.

Quelle: ESG

Zusammenfassung: Die meisten Unternehmen erhalten tausende Benachrichtigungen aus vielen verschiedenen Überwachungslösungen, aber das dadurch entstehende „Rauschen" ist kontraproduktiv. Für eine bessere Bedrohungserkennung sind nicht mehr, sondern bessere – also aussagekräftigere und praxistaugliche – Meldungen gefragt. Eine Erkennung und Validierung verdächtiger Aktivitäten in Ihren Systemen erreichen Sie durch eine Integration nicht nur aller verwendeten Erkennungstechnologien, sondern auch intelligenter Analysen von Endpunkt-, Netzwerk- und Cloud-Daten.

Mit taktischen Erkennungs- und Abwehrlösungen lassen komplexe Angriffe sich nicht aufdecken. Unternehmen werden weiterhin gehackt und Daten werden gestohlen. Es ist also dringend erforderlich, die Fähigkeiten der verfügbaren Sicherheitsexperten so effektiv und effizient wie möglich zu nutzen.

In den USA gibt es derzeit über 300.000 offene Stellen im Bereich Cybersicherheit und diese Zahl wird in den nächsten Jahren voraussichtlich noch erheblich steigen.

Quelle: Cyberseek

CORTEX XDR BY PALO ALTO NETWORKS

Was ist XDR?

XDR ist eine neue Kategorie, die den Bedarf an umfassenderer und intelligenterer Erkennung und Abwehr decken soll. Das „X“ steht dabei für jede beliebige Datenquelle, da die isolierte Betrachtung einzelner Komponenten der Infrastruktur erwiesenermaßen weder effektiv noch effizient ist. XDR setzt maschinelles Lernen und dynamische Analysen ein, um die Funktionalität und die Ergebnisse zu bieten, die von SIEM, UEBA, NTA und EDR bekannt sind.

Das „X“ steht für jede beliebige Datenquelle.

Wenn XDR die Zukunft der Bedrohungserkennung und Abwehr werden soll, muss sie den Herausforderungen gerecht werden, mit denen SecOps-Teams Tag für Tag konfrontiert sind. Definieren wir also die Anforderungen an die XDR gemäß den weiter oben beschriebenen Herausforderungen.

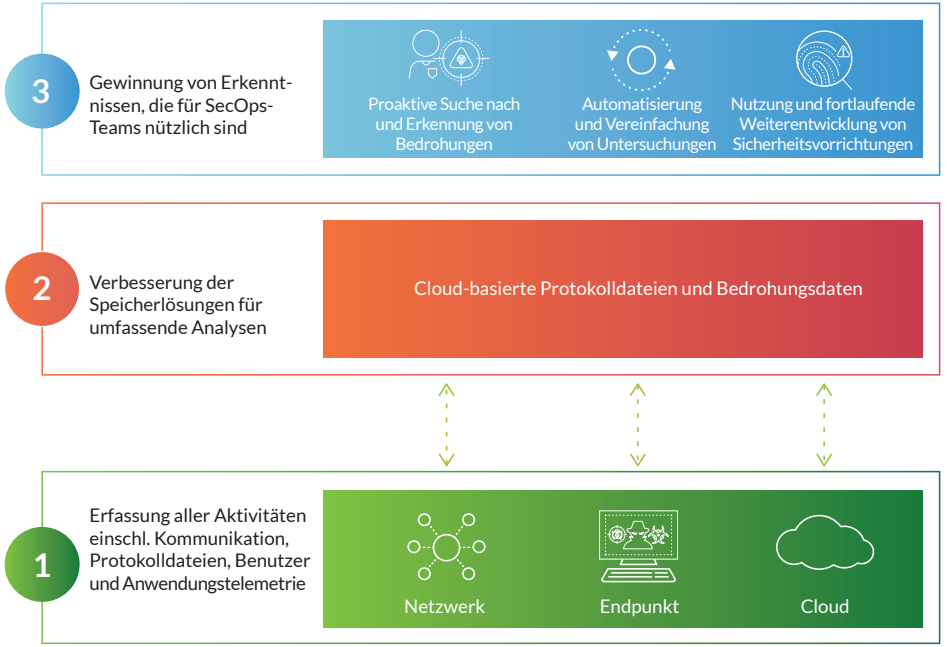

Abbildung 4: XDR verknüpft die traditionell isolierten Bereiche Erkennung und Abwehr

CORTEX XDR BY PALO ALTO NETWORKS

Anforderung 1: Schnellere Erkennung getarnter Bedrohungen durch Analysen, die Netzwerke, Clouds und Endpunkte einschließen

Der erste Schritt der Bedrohungserkennung und -abwehr ist – logischerweise – die Erkennung. Wenn Sie eine Bedrohung nicht erkennen, können Sie sie nicht untersuchen und erst recht nicht stoppen. Angreifer nutzen Clouds und KI für komplexe mehrstufige Kampagnen, mit denen sie sich im Zielsystem festsetzen und kritische Daten sowie geistiges Eigentum stehlen. Deshalb muss eine praxistaugliche XDR-Lösung die folgenden Eigenschaften aufweisen.

Umfassende Transparenz und Verständnis des Kontexts

Punktlösungen generieren Datensilos. Das ist heute nicht mehr akzeptabel. Sie können Angreifer nur wirksam bekämpfen, wenn Sie sich in Ihrer eigenen Infrastruktur mindestens genauso wendig umschauen können wie diese. XDR muss Transparenz und Erkennungsfunktionen für Ihre gesamte IT-Umgebung bieten und dabei telemetrisch Daten von Ihren Endpunkten, aus Ihren Netzwerken und aus Ihren Clouds erfassen. Zudem muss sie die Daten aus den verschiedenen Quellen zusammenführen, Beziehungen zwischen den beschriebenen Ereignissen erkennen und anhand des Kontexts ermitteln können, ob ein bestimmtes Verhalten verdächtig ist.

Datenaufbewahrung

Manche Angreifer sind sehr geduldig. Sie wissen, dass sie weniger auffallen, wenn sie langsam vorgehen und dass es sich lohnt, die Aufbewahrungszeiträume der Erkennungstechnologien auszusitzen, die im Zielsystem implementiert sind. XDR sollte ihnen das so schwer wie möglich machen. Ihre Erkennungssysteme müssen Daten aus dem Netzwerk, den Endpunkten und der Cloud in einem einzigen Repository erfassen, zusammenführen, analysieren und dort mindestens 30 Tage lang aufbewahren.

88 % der Hacker sind sich sicher, ein Ziel in weniger als 12 Stunden infiltrieren zu können.

Quelle: Nuix (über NBC)

Analyse der internen und externen Datenströme

Herkömmliche Erkennungstechnologien konzentrieren sich hauptsächlich auf externe Bedrohungen und übersehen dadurch eine ganze Gruppe potenzieller Gegner. Die Erkennung darf sich nicht auf Angriffe von außerhalb des Perimeters beschränken. Sie muss auch **interne Nutzerkreise profilieren und analysieren**, um ungewöhnliches und potenziell schädliches Verhalten zu erkennen, dass auf einen Missbrauch von Anmeldedaten hindeutet.

Integrierte Bedrohungsdaten

Sie müssen auch auf noch **unbekannte Angriffe** vorbereitet sein. Um im Kampf gegen Cyberkriminelle bessere Chancen zu haben, sollten Sie sich über neue Angriffsmethoden auf dem Laufenden halten, die bei anderen Unternehmen beobachtet wurden. Dann können Sie sich bei der Erkennung auf Bedrohungsdaten aus einem globalen Netzwerk von Anwendern stützen. Sobald ein Unternehmen in Ihrer erweiterten Netzwerk-Community einen Angriff identifiziert, können Sie die Erkenntnisse aus diesem ersten Angriffsversuch anwenden, um ähnliche Versuche in Ihrer eigenen Infrastruktur zu erkennen.

Anpassbare Bedrohungserkennung

Der Schutz jedes Unternehmens wirft spezifische Herausforderungen auf, die unter anderem von den genutzten Systemen, der Benutzerzusammensetzung und den potenziellen Angreifern abhängen. Deshalb müssen Erkennungssysteme flexibel an die Anforderungen der Umgebung anpassbar sein, in der sie eingesetzt werden. Das bedeutet unter anderem, dass sie sowohl vordefinierte als auch benutzerdefinierte Erkennungsmethoden unterstützen müssen.

Bedrohungserkennung auf der Basis des maschinellen Lernens

Zur Erkennung von Angriffen, bei denen keine herkömmliche Malware genutzt, sondern autorisierte Systemdateien gehackt, Skripting-Umgebungen missbraucht oder die Systemregistrierung unterwandert werden, müssen alle erfassten Telemetriedaten **mit modernsten Analysetechniken untersucht werden**. Für diesen Ansatz sind überwachtes und teilüberwachtes maschinelles Lernen erforderlich.

Nur 38 % der SecOps-Teams sind der Meinung, dass sie auf einen raffinierten Cyberangriff vorbereitet sind.

Quelle: Cybint

CORTEX XDR BY PALO ALTO NETWORKS

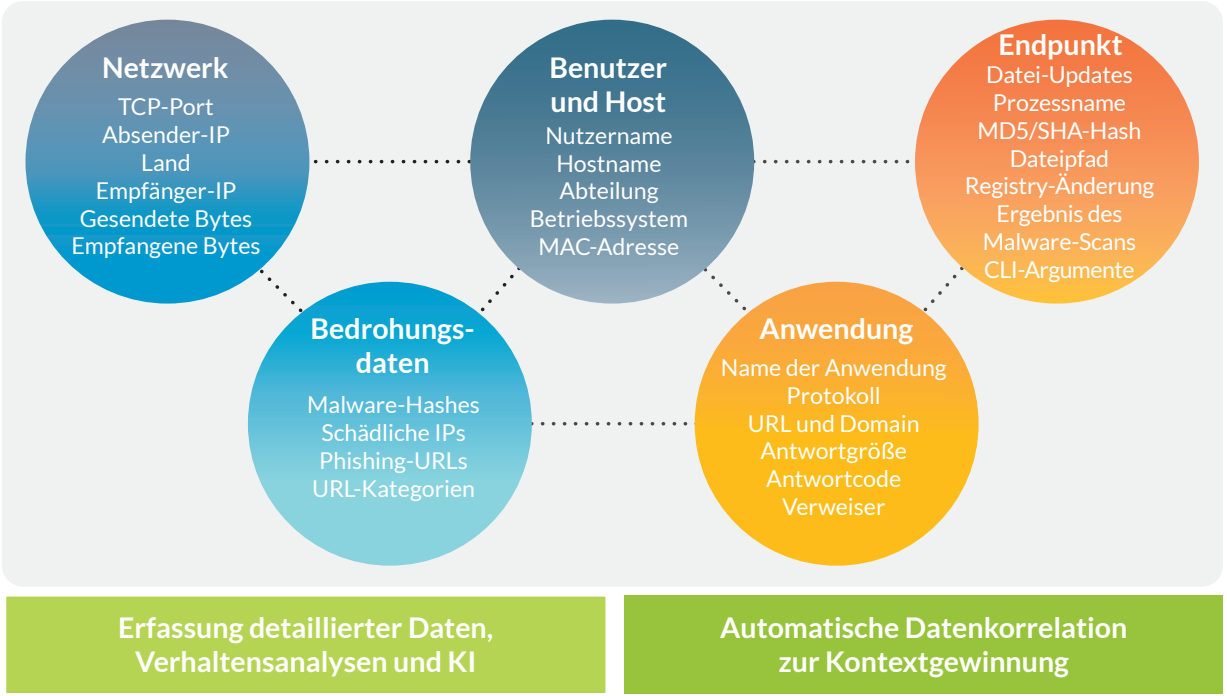

Abbildung 5: XDR führt detaillierte Daten zusammen und gleicht sie ab

Anforderung 2: Einfachere Untersuchung und Abwehr bekannter und neuer Bedrohungen

Nun, da Sie die potenziellen Bedrohungen in Ihren Systemen kennen, müssen Sie diese rasch sichten und untersuchen können. Herkömmliche Erkennungs- und Abwehrsysteme können dies nicht schnell und effektiv genug, besonders bei Angriffen, von denen mehrere Infrastrukturbereiche betroffen sind. XDR-Lösungen können die Situation erheblich verbessern. In den folgenden Abschnitten wird dies näher erläutert.

Korrelation und Gruppierung von zusammengehörigen Benachrichtigungen und Telemetriedaten

Wenn Sie eine Benachrichtigung erhalten, arbeitet Ihr Angreifer bereits emsig an der Umsetzung seiner Ziele. Gehen Sie also davon aus, dass jede Sekunde zählt. Sie müssen sich so schnell wie möglich einen Überblick über den Angriff, seine Ursachen und die möglichen Auswirkungen verschaffen. Dazu muss Ihr XDR-Tool zunächst zusammengehörige Meldungen zusammenfassen und effektiv denjenigen Ereignissen Priorität geben, auf die am dringendsten reagiert werden muss. Außerdem muss das Tool in der Lage sein, den **Angriffsverlauf** unter Verwendung von Protokolldateieinträgen für das Netzwerk, die Endpunkte und die Cloud zu rekonstruieren. Durch die grafische Darstellung der Ereignisse in der richtigen Reihenfolge können der Ausgangspunkt des Angriffs ermittelt und der mögliche Schaden und die Ausbreitung eingeschätzt werden.

Eine einzige Benutzeroberfläche für den Zugriff auf alles

Zur effektiven Untersuchung von Benachrichtigungen benötigen Ihre Analysten eine **effiziente Arbeitsumgebung**, in der sie mit einem Klick zwischen den Daten aus verschiedenen Quellen hin- und herschalten können. Sie sollten keine Zeit mit dem Wechsel zwischen zwei oder mehr verschiedenen Tools verschwenden müssen.

CORTEX XDR™ BY PALO ALTO NETWORKS

Manuelle und automatisierte Bedrohungssuche

In immer mehr Unternehmen suchen die SecOps-Teams proaktiv nach möglichen Angreifern, wobei die Analysten Angriffshypothesen entwickeln und in den Systemen nach entsprechenden Aktivitäten Ausschau halten. Dazu benötigen sie **leistungsstarke Suchfunktionen** zur Überprüfung ihrer Hypothesen und **integrierte Bedrohungsdaten** zur Suche nach schädlichen Aktivitäten, die bei anderen Mitgliedern der erweiterten Netzwerk-Community beobachtet wurden. Diese Bedrohungsdaten sollten so integriert und automatisiert sein, dass sie ohne zeitraubende manuelle Arbeit genutzt werden können. Analysten sollten beispielsweise nicht dutzende Feeds in parallelen Browserfenstern durchforsten müssen, um zu prüfen, ob eine verdächtige IP-Adresse bereits anderswo als „schädlich“ klassifiziert wurde.

Funktionen für die Orchestrierung

Nachdem ein Angriff entdeckt und untersucht wurde, ist der nächste Schritt eine effiziente und effektive Abwehr. Ihr System muss in der Lage sein, die Reaktionen auf eine aktive Bedrohung zu koordinieren („Orchestrierung“) und zukünftige ähnliche Angriffe auf Ihr Netzwerk, Ihre Endpunkte und Ihre Cloud-Umgebungen zu vereiteln. Dazu müssen die verschiedenen Abwehrtechnologien miteinander kommunizieren, entweder nativ oder über APIs. So muss beispielsweise ein Angriff, der im Netzwerk blockiert wird, zu einer automatischen Aktualisierung der Richtlinien an den Endpunkten führen. Außerdem müssen Ihre Analysten direkt vom XDR-Bildschirm aus aktiv eingreifen können.

Anforderung 3: Rentablere Nutzung aktueller und zukünftiger Sicherheitsinvestitionen

Eine XDR-Lösung sollte die Rendite aus Ihren Sicherheitsinvestitionen erheblich steigern, indem sie die Effizienz Ihres SecOps-Teams verbessert, sodass aufgrund des Fachkräftemangels unbesetzte Stellen weniger ins Gewicht fallen. Zudem sollte sie Ihre vorhandenen Tools besser miteinander verknüpfen und die Angriffsprävention mittelfristig durch eine skalierbare Infrastruktur und den Einsatz von KI stärken. Um all dies zu erreichen, benötigt Ihre perfekte XDR-Lösung die folgenden Eigenschaften.

Sicherheitsorchestrierung

Orchestrierung ist nicht nur, wie beschrieben, wichtig für die Vereinfachung der Bedrohungsabwehr, sondern erlaubt auch die Maximierung der Rendite aus Ihren Investitionen in Sicherheitstechnologien. In den allermeisten Unternehmen wurden bereits Sicherheitsmaßnahmen implementiert, die zur Reaktion auf aktive Bedrohungen genutzt werden können. Der Erfolg eines Erkennungs- und Abwehrsystems hängt wesentlich davon ab, wie gut **die Investitionen in die vorhandenen Maßnahmen** genutzt werden, um eine einheitliche Reaktion im gesamten Unternehmen zu gewährleisten.

Nutzung externer Daten

Die vorhandenen Sicherheitstoolkits von Unternehmen sind in der Regel heterogen. Je besser eine XDR-Lösung die Daten aus jedem dieser Tools erfassen und nutzen kann, desto umfassender kann sie die Infrastruktur schützen. Die besten XDR-Lösungen zeichnen sich dadurch aus, dass sie die Daten aus den anderen Tools in Ihrer IT-Umgebung importieren, um sie voll auszunutzen und anzuwenden.

Skalierbare Speicher- und Rechenkapazität

Angesichts des Erfindungsreichtums moderner Hacker sollten Sie Ihre Telemetriedaten, die Hinweise auf langsam ausgeführte, hartnäckige Angriffe enthalten könnten, nicht löschen müssen. Besser ist es, ausreichend **Speicherkapazitäten für forensische Daten** mehrerer Monate oder sogar Jahre sowie genügend **Rechenleistung** zu deren effektiver Analyse zur Verfügung zu haben. Cloud-basierte Plattformen bieten diese unbegrenzten Kapazitäten.

Ständige Verbesserung

Die Erkennung raffinierter Hackerangriffe erfordert künstliche Intelligenz oder maschinelles Lernen sowie Automatisierung, um die Fertigkeiten hoch qualifizierter Sicherheitsanalysten nicht auf manuelle Kleinarbeit zu verschwenden. XDR-Lösungen sollten aus Erfahrungen lernen, zukünftige Risiken minimieren und die Prävention kontinuierlich stärken, indem sie die bei der Erkennung, Untersuchung und Abwehr von Bedrohungen gewonnenen Erkenntnisse weiternutzen.

Berichte und Dashboards

Sicherheitsteams müssen ihr Sicherheitskonzept und die dazugehörigen Kennzahlen durchschauen und kommunizieren können. XDR-Lösungen müssen also nicht nur die Sicherheitsergebnisse verbessern, sondern das Sicherheitsniveau auch in Berichten und auf Dashboards darstellen können.

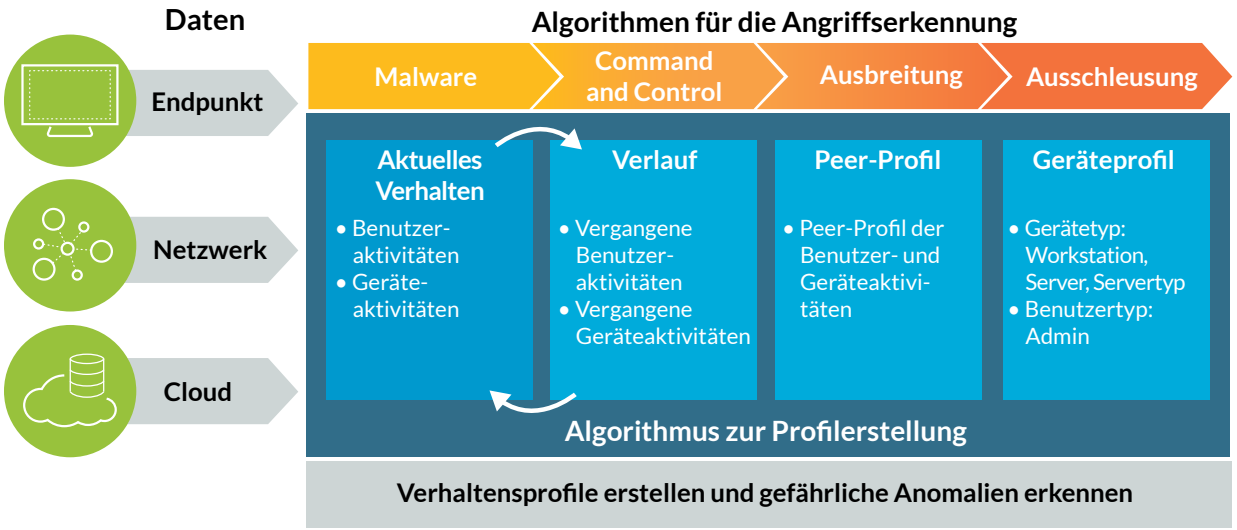

Abbildung 6: Gezielte Erkennung umgebungsspezifischer Bedrohungen mit KI

XDR ist eine neue Herangehensweise an die Erkennung und Abwehr von Bedrohungen, die sich durch eine umfassende Beobachtung Ihrer IT-Umgebung einschließlich Netzwerk, Endpunkten und Cloud auszeichnet. Dank modernster Analyseverfahren und integrierter Bedrohungsdaten haben SecOps-Teams sowohl bei der Angriffsabwehr als auch bei der proaktiven Suche nach Bedrohungen Zugriff auf alle Informationen, die sie zum Identifizieren und Vereiteln schädlicher Aktivitäten benötigen.

Abbildung 7: XDR passt sich kontinuierlich an und verbessert den Schutz

Anwendungsbereiche der XDR

Einige der wichtigsten Aufgaben fallen überall an, unabhängig von der Größe des Sicherheitsteams. Traditionell werden diese Aufgaben auf mehrere „Ebenen“ von Analysten mit steigender Erfahrung verteilt. Die typischen Verantwortungsbereiche der verschiedenen Ebenen sind:

Ebene 1: Triage (Sichten und Priorisieren)

Auf dieser arbeitsintensivsten Ebene sind in der Regel die weniger erfahrenen Analysten tätig. Ihre Hauptaufgabe ist die Durchsuchung von Protokolldateien nach verdächtigen Aktivitäten. Wenn sie das Gefühl haben, dass etwas genauer untersucht werden sollte, stellen sie so viele Informationen wie möglich zusammen und eskalieren den Vorfall auf Ebene 2.

Ebene 2: Untersuchung

Die Analysten auf dieser Ebene untersuchen die verdächtige Aktivität näher und stellen fest, wie weit sie schon in die Infrastruktur eindringen konnte. Dann koordinieren sie die Behebung des Problems. Für diese Tätigkeit ist oft eine höhere Qualifikation oder längere Erfahrung erforderlich.

Ebene 3: Proaktive Bedrohungssuche

Hier sitzen die erfahrensten Analysten. Sie unterstützen die Analysten der Ebene 2 bei komplexen Aktivitäten zur Bedrohungsabwehr und forschen ansonsten in forensischen Daten und Telemetriedaten nach Bedrohungen, die von der Erkennungssoftware möglicherweise nicht als verdächtig erkannt wurden. In einem typischen Unternehmen ist der Zeitaufwand für die Tätigkeiten auf Ebene 1 und 2 so groß, dass nur ein Bruchteil der verfügbaren Arbeitszeit für die proaktive Bedrohungssuche bleibt.

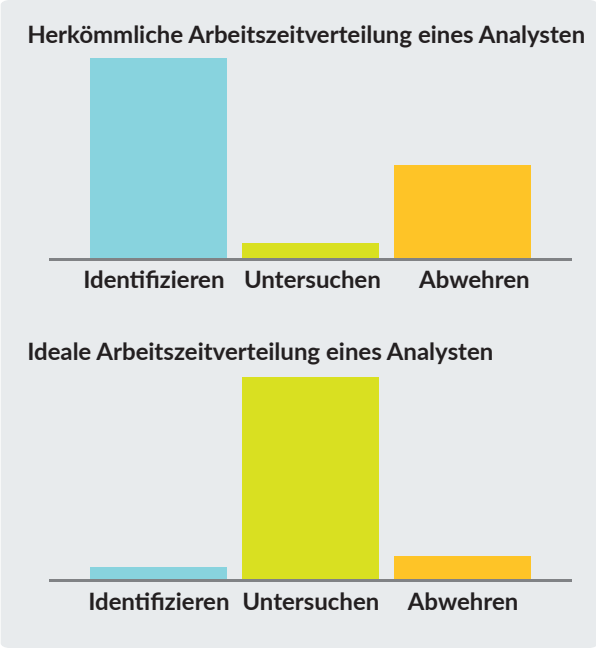

Abbildung 8: Im konventionellen SOC-Modell werden die Arbeitszeit und die Fähigkeiten der Analysten nicht optimal eingesetzt

Dieses Modell ist zwar weit verbreitet, aber es ist alles andere als ideal. Erstens fällt es den meisten Menschen schwer, den ganzen Tag lang Protokolldateien zu lesen. Sie leiden früher oder später unter Alarmmüdigkeit und übersehen einzelne Bedrohungen, die zwischen den vielen irrelevanten Meldungen der zahlreichen Sensoren verborgen sind, die in einem typischen SOC eingehen. Analysten, die dies tagtäglich tun müssen, werden sich bald nach einer anspruchsvolleren Tätigkeit umsehen. (Möglicherweise haben sie auch innovative Ideen, die sie nur nicht umsetzen können, weil ihnen die Fachkenntnisse fehlen, die für die veralteten Untersuchungsmethoden erforderlich sind.) Zweitens bleibt bei diesem Ansatz viel zu wenig Zeit für die proaktive Bedrohungssuche und die Verbesserung der Abläufe, weil das Personal die meiste Zeit mit Erkennung und Abwehr verbringt.

Sehen wir uns nun näher an, wie die oben definierte XDR bei der Arbeit auf diesen Ebenen eingesetzt werden kann, um das herkömmliche Modell zu verbessern. Wir gehen dabei nach den Hauptfunktionen vor: Erkennung, Triage, Untersuchung und Abwehr sowie proaktive Bedrohungssuche.

Erkennung

Eine effektive Vermeidung von Datenlecks ist nur möglich, wenn Sie verdächtige Aktivitäten in Ihrer IT-Umgebung zuverlässig erkennen. XDR macht sich mithilfe des maschinellen Lernens rasch mit den individuellen Eigenschaften Ihres Unternehmens vertraut und kann so bald wesentlich effektiver zwischen einem Angriff und harmloser Aktivität unterscheiden als menschliche Analysten oder statische Korrelationsregeln. Zudem werden durch diese maschinellen Lernverfahren auch anspruchsvolle Analysen, die Erstellung von Profilen und eine verhaltensbasierte Bedrohungserkennung möglich. Die Erkennung krimineller Aktivitäten wie beispielsweise gezielter Angriffe, bösartiger Insider und anderer Auffälligkeiten wird dadurch verbessert.

Gezielte Angriffe

Beim Ausspionieren von Zielumgebungen und der Suche nach lohnenden Zielen versuchen die meisten Angreifer, sich als legitime Benutzer zu tarnen. Doch wenn Sie Ihre Sicherheitsdaten aus Netzwerk- und Cloud-Umgebungen sowie von Endpunkten in die leistungsstarken Analysefunktionen einer XDR-Lösung einspeisen, sehen Sie ungewöhnliche Aktivitäten, wenn Angreifer sich Zugang zu Ihren Geräten verschaffen, sich in Ihrem Netzwerk ausbreiten oder nach Kundendaten und geistigem Eigentum suchen oder diese ausschleusen.

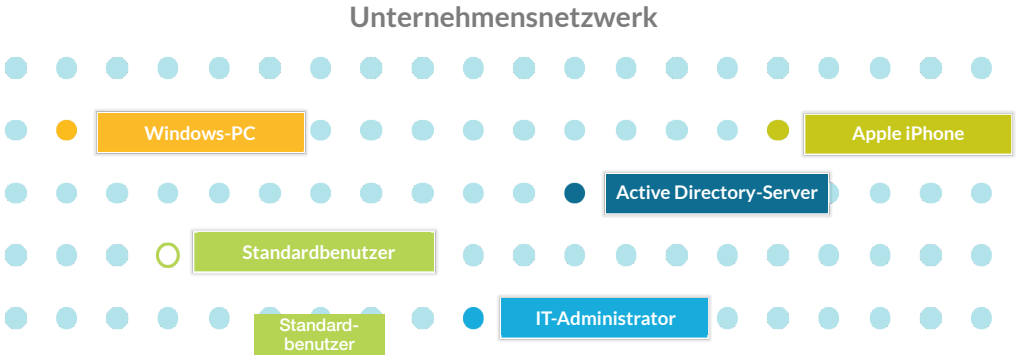

Abbildung 9: Verhaltensanalyse erkennt Anomalien auf Benutzer-, Anwendungs- und Geräteebene

Angriffe durch Mitarbeiter

Mitunter missbrauchen Insider ihre autorisierten Anmeldedaten, um unerkannt erhebliche Mengen von Unternehmensdaten zu stehlen. XDR begegnet dieser Herausforderung, indem es auf Änderungen im Nutzerverhalten und damit verbundene Aktivitäten in der Infrastruktur hinweist, wodurch sich mögliche Spionage und verdächtige Bewegungen im Netzwerk erkennen lassen, die von Insidern ausgehen.

Unbeabsichtigte Fehler

Auch ehrliche Mitarbeiter können ein Unternehmen unbeabsichtigt unnötigen Risiken aussetzen. Mit einer XDR-Lösung können alle Benutzeraktivitäten verfolgt werden, um riskantes Verhalten und die (absichtliche oder versehentliche) Verletzung von Sicherheitsrichtlinien zu erkennen und die Einhaltung von Best Practices durchzusetzen.

Infizierte Endpunkte

Häufig nutzen Angreifer Malware, um sich Zugang zu den Endpunkten eines Zielnetzwerks zu verschaffen und sich von dort aus im Netzwerk auszubreiten. XDR führt Daten aus dem Netzwerk und von den Endpunkten zusammen, um von der Norm abweichenden Datenverkehr zu identifizieren, der auf Malware oder andere schädliche Aktivitäten hindeutet. Anhand dieser Sicherheitsdaten kann auch die ganze Infrastruktur untersucht werden, um zu erkennen, wie weit die Angreifer bereits vorgedrungen sind.

Da XDR Benachrichtigungen zu Vorfällen gruppiert und die einem Vorfall zugeordneten Aktivitäten mit Tags versieht, um sie in ihren Kontext zu setzen, können auch weniger erfahrene Analysten einen potenziellen Angriff erkennen und überprüfen. Das ist insbesondere angesichts des oben erwähnten Fachkräftemangels sehr nützlich. Außerdem werden die gewonnenen Erkenntnisse so in einem Format festgehalten, das für das gesamte Team nutzbar ist.

Wenn beispielsweise ein Eindringling einen neuen Wert zum Autorun-Registrierungsschlüssel hinzufügt, kann eine XDR-Lösung automatisch einen Tag erzeugen, der dem Analysten anzeigt, dass die Aktion „Ausführbare Datei zur Ausführung nach dem Booten festgelegt“ mit der Angriffsart „Persistenz“ stattgefunden hat. Dazu kommt eine detaillierte Beschreibung wie „Der Prozess fügte einen neuen Schlüssel im Autorun-Ordner der Windows-Registrierung ein. Dadurch wird beim Systemstart eine ausführbare Datei oder ein Skript ausgeführt. Überprüfen Sie, um welche Datei es sich handelt und warum sie ausgeführt werden soll.“

Durch die Zusammenführung von Daten aus dem Netzwerk, aus der Cloud und von Endpunkten mit Algorithmen für die Angriffserkennung und ein kontinuierliches Lernen sowohl aus internen Reaktionen als auch aus externen Bedrohungsdaten identifiziert eine XDR-Lösung aktive Angriffe mit konkurrenzloser Präzision.

Überblick

Vorteile von XDR für die Erkennung

Mit XDR können Sicherheitsteams:

- Muster in den Aktivitäten im Netzwerk, an den Endpunkten und in der Cloud erkennen, die auf verdächtige Aktivitäten internen oder externen Ursprungs hindeuten.
- Große Mengen von Sicherheitsdaten mit modernsten Verfahren analysieren, um anormales Verhalten zu erkennen, ohne zusätzliche Fehlalarme zu generieren.
- Die Leistung des gesamten Sicherheitsteams verbessern, indem externe Bedrohungsdaten und die bei der Reaktion auf frühere Angriffe gewonnenen Erkenntnisse so aufbereitet werden, dass auch weniger erfahrene Analysten sie nutzen können.

CORTEX XDR™ BY PALO ALTO NETWORKS

Sichtung und Priorisierung von Benachrichtigungen

Wie bereits erwähnt, gehört es zu den größten Herausforderungen für Sicherheitsteams, dass ihre teilweise unerfahrenen Analysten mehr Sicherheitsvorfälle früher erkennen müssten, um die Verweildauer der Angreifer zu verkürzen. Je besser die Mitarbeiter der Ebene 1 diese Aufgabe erledigen, desto mehr Benachrichtigungen können gesichtet werden und desto mehr Angriffe werden erkannt. Noch besser wäre der Einsatz von mehr Automatisierung im Sichtungsprozess, damit die Analysten der Ebene 1 echte Sicherheitsbedrohungen zuverlässiger identifizieren können und nur diese eskalieren müssen.

Da XDR-Lösungen Daten aus dem Netzwerk, von den Endpunkten und aus der Cloud zusammenführen, können sie den Ausgangsort eines Angriffs automatisch identifizieren und die Überprüfung und Untersuchung damit erheblich beschleunigen. So erkennt XDR beispielsweise nicht nur, welche Datei auf welchem Endpunkt ausgeführt wurde, um einen Netzwerkangriff zu starten, sondern auch, von welcher Anwendung diese Datei gestartet wurde. XDR rekonstruiert den Ablauf der Ereignisse, die zu dem Angriff geführt haben, und stellt relevante integrierte Bedrohungsdaten zur Verfügung. All das hilft den Analysten, den Ausgangsort des Angriffs, die genaue Art der Bedrohung und die notwendigen Gegenmaßnahmen zu bestimmen.

So läuft die Sichtung und Priorisierung von Benachrichtigungen mit XDR ab:

(1) Einschätzung: Zunächst beurteilt die XDR-Lösung extern (von SIEM- und anderen Tools) und intern generierte Benachrichtigungen (aufgrund von Regeln und anderen Indikatoren), um potenziell verdächtiges Verhalten zu identifizieren.

(2) Priorisierung: Das XDR-Tool gruppiert diese Benachrichtigungen dann automatisch zu Vorfällen und weist diesen Vorfällen Prioritätswerte zu, damit Analysten sich sofort auf die gefährlichsten Bedrohungen konzentrieren können. Die Analysten können auf jeden Vorfall klicken, um eine vollständige Liste der Benachrichtigungen, Geräte, relevanten Bedrohungsdaten und Kontextinformationen zu sehen und sich ein umfassendes Bild zu machen.

Die Produktnutzungsdaten von Palo Alto Networks zeigen, dass für einen Sicherheitsvorfall durchschnittlich 50 Benachrichtigungen generiert werden. Durch das Gruppieren zusammengehöriger Ereignisse zu Vorfällen kann XDR die Anzahl der Benachrichtigungen, die Analysten sichten müssen, um 98 % reduzieren.

CORTEX XDR BY PALO ALTO NETWORKS

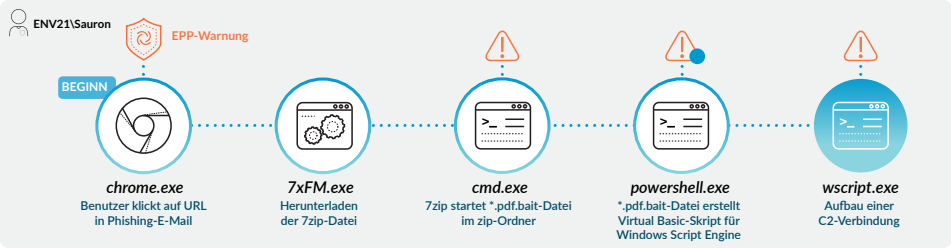

Abbildung 10: Visualisierung eines Angriffsverlaufs mit XDR

(3) Analyse: Innerhalb eines Vorfalls können Analysten auf einzelne Benachrichtigungen klicken, um den zeitlichen Verlauf visuell darzustellen und aus verschiedenen Telemetriequellen alles Relevante für eine schnellere und bessere Analyse zusammenzutragen.

(4) Anreicherung: Der Angriffsverlauf wird dann mit Kontextinformationen angereichert, einschließlich einer schrittweisen Darstellung der Ereignisse, die zum Generieren der Benachrichtigung geführt haben, des Angriffsbeginns bzw. Ausgangspunktes, anderer betroffener Endpunkte, Netzwerk- und Cloud-Geräte und der Glaubwürdigkeit aller forensischen Artefakte.

Überblick

Vorteile von XDR im Triage-Prozess

Mit XDR können Analysten:

- Mehr Ereignisse pro Tag zurückverfolgen, nicht nur diejenigen, die von SIEM-Systemen oder anderen Tools zur Verwaltung von Benachrichtigungen priorisiert werden
- Die Gefahr, wichtige Benachrichtigungen zu übersehen, erheblich senken
- Fehlalarme schneller als solche erkennen und damit die Produktivität und Effektivität der nachfolgenden Schritte verbessern
- Neue Verhaltens-Trigger anwenden, um den Triage-Prozess zu beschleunigen und die Sicherheit kontinuierlich zu stärken

(5) Überprüfung: Die Anreicherung, Analyse, Einschätzung und Priorisierung erfolgen automatisch, bevor der Mitarbeiter die Benachrichtigung zur weiteren Untersuchung erhält. XDR nutzt alle vorhergehenden Benachrichtigungen als Kontext für den Zeitstrahl der aktuellen Benachrichtigungen, um die Prioritätenzuweisung zu verbessern und den Zeitaufwand für die Überprüfung zu reduzieren.

Da die meisten SecOps-Teams täglich Tausende oder sogar Millionen von Benachrichtigungen erhalten, sind ein automatisierter Triage-Prozess und die Bereitstellung von umfassenden Kontextinformationen die einzige praxistaugliche Art, mit diesem Volumen an Meldungen umzugehen. Mit XDR können Sicherheitsteams ihre Zeit und Energie dort investieren, wo sie am meisten nützt: bei der Reaktion auf die gefährlichsten Angriffe.

Automatisierung und Vereinfachung der Untersuchung und Abwehr

Wenn eine Benachrichtigung als berechtigt eingestuft wird und Priorität erhält, muss sich eine genauere Untersuchung anschließen. Analysten benötigen Kontextinformationen, um den Angriff richtig einzuordnen und angemessene Gegenmaßnahmen einzuleiten. Dazu gehören Informationen über den Benutzer und den Endpunkt (den beteiligten Prozess usw.), Bedrohungsdaten (z. B. ob es sich um bekannte Malware handelt) und Netzwerkdaten. Anhand dieser Daten sollte es möglich sein, den Ausgangspunkt des Angriffs zu ermitteln und den Angriffsverlauf zu rekonstruieren. Wenn die Analysten diese Informationen erst manuell zusammensuchen müssen, vergeht wertvolle Zeit, während der das Risiko steigt. Die Automatisierung der XDR beschleunigt sowohl die Untersuchung von Benachrichtigungen als auch die proaktive Bedrohungssuche, weil sie den Analysten ein klares Bild der Bedrohungen und ihrer Ursachen vermittelt, die Verlässlichkeit der Anhaltspunkte prüft und die Identität der Angreifer ermittelt.

Zu Beginn führen XDR-Tools alle Telemetriedaten von Endpunkten, aus dem Netzwerk und der Cloud in einem Pool von Sicherheitsdaten wie beispielsweise einem „Data Lake“ zusammen. Benachrichtigungen aus verschiedenen Erkennungs-Tools werden zueinander in Beziehung gesetzt und zeitsparend zu einer deutlich kleineren Anzahl von Vorfällen zusammengefasst, die dann durch Angaben zum betroffenen Benutzer, der Anwendung und dem Gerät angereichert werden. Zudem macht XDR langwierige forensische Untersuchungen überflüssig, indem es Endpunkte durchsucht, um zu ermitteln, von welchem Prozess oder welcher ausführbaren Datei ein Angriff ausging.

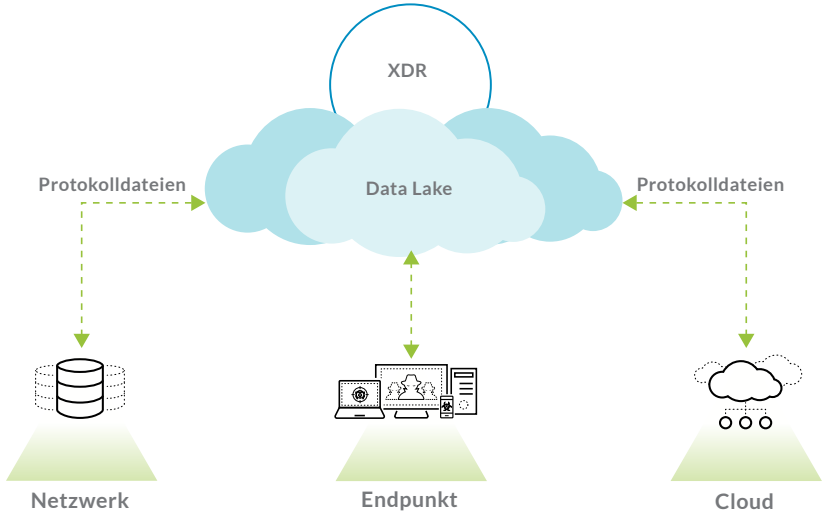

Abbildung 11: XDR-Tools führen Daten von verschiedenen Sensoren in einem Cloud-basierten Data Lake zusammen

Zur weiteren Untersuchung des Vorfalls überprüft eine XDR-Lösung dann, ob der Endpunktprozess bösartig ist. Dazu zieht sie Bedrohungsdaten aus integrierten Quellen oder verlinkten Services heran. Die Arbeit der Sicherheitsanalysten ist erheblich einfacher, weil alle benötigten Informationen auf einer Konsole zur Verfügung stehen.

XDR-Tools können die Erkenntnisse aus der Untersuchung von Vorfällen und der proaktiven Bedrohungssuche auch nutzen, um Sicherheitsmaßnahmen so anzupassen, dass einmal gefundene Bedrohungen automatisch abgewehrt werden, falls sie erneut auftreten. Dieses „unterstützte Lernen" ermöglicht eine zeitnahe Erkennung von Angriffen auf der Grundlage bekannter Sachverhalte.

Dadurch stehen den für die Reaktion auf Vorfälle verantwortlichen Mitarbeitern Dutzende von Methoden zur Verfügung, mit denen sie infizierte Systeme gezielt per Fernzugriff säubern können, ohne den Betrieb unterbrechen zu müssen. Dadurch werden sie wesentlich effizienter, benötigen weniger Schulungen, entlasten die höher qualifizierten Mitarbeiter und reagieren schneller auf Vorfälle.

Überblick

Vorteile von XDR für die Untersuchung

Mit XDR können Incident-Response-Experten:

- Bedrohungsdaten und Verhaltensanalysen nutzen, um getarnte Bedrohungen schneller aufzudecken
- Telemetriedaten aus Netzwerken, Endpunkten und der Cloud mit leistungsstarken Suchfunktionen durchsuchen, um die Untersuchung und Behebung von Vorfällen zu vereinfachen und zu beschleunigen

CORTEX XDR BY PALO ALTO NETWORKS

Proaktive Bedrohungssuche

XDR-Lösungen sind äußerst nützlich für die Bedrohungssuche, da sie sowohl automatisierte als auch spontan gestartete infrastrukturweite Suchen nach verdächtigen Aktivitäten unterstützen. Die zuständigen Mitarbeiter können komplexe Abfragen durchführen und erhalten sofort extrem präzise Antworten. Im Folgenden finden Sie einige Beispiele für Varianten der Bedrohungssuche, die durch XDR-Funktionen unterstützt werden.

Gezielte Bedrohungssuche

Dies ist die am häufigsten vorkommende Art der Bedrohungssuche. Das SecOps-Team hat von einer aktuellen Bedrohung erfahren und will nun wissen, ob diese auch in der eigenen Umgebung präsent ist. Der Auslöser für eine solche Suche kann zum Beispiel eine in einer Bedrohungsdatenbank gefundene Beschreibung, ein kürzlich bekannt gewordener Gefahrenindikator (Indicator of Compromise, IOC), ein Tipp aus einer anderen Abteilung oder einfach nur ein Verdacht sein. Wie kompliziert die Suche ist, hängt zu einem großen Teil davon ab, wie detailliert diese Informationen sind. XDR-Lösungen können schnell belastbare Suchergebnisse liefern, weil sie Zugang zu integrierten Datenquellen haben, die mit mehreren Anbietern von Bedrohungsdaten verlinkt sind. Zudem unterstützen sie auch den manuellen Import von Artefakten und IOCs aus unterschiedlichen Quellen.

Ungezielte Bedrohungssuche

Fast genauso häufig suchen Fachleute auch ohne spezifische Anhaltspunkte nach Bedrohungen. Dabei stützen sie sich auf ihre eigenen Kenntnisse der Funktionsweise von Computern und Netzwerken sowie des normalen Verhaltens ihrer Anwendungen, Benutzer und Daten, um davon abweichende (und somit potenziell verdächtige) Verhaltensweisen zu finden. Für diese „fortgeschrittene“ Bedrohungssuche sind meist die erfahrensten Teammitglieder verantwortlich, die mit Techniken wie Carving oder besonders anspruchsvollen Analysefunktionen vertraut sind. Eine XDR-Lösung enthält integrierte Funktionen, mit denen auch deutlich weniger erfahrene Teammitglieder diese Methoden nutzen können, ohne Skripte oder zusätzliche Tools einsetzen oder spezielle Abfragesprachen erlernen zu müssen.

CORTEX XDR™ BY PALO ALTO NETWORKS

Ergebnisbasierte Bedrohungssuche

Bei der ergebnisbasierten Bedrohungssuche werden ältere Benachrichtigungen, die zur Isolation von Ressourcen geführt haben, abgeschlossene Untersuchungen oder andere abgewehrte Bedrohungen analysiert, um neuere oder modifizierte Varianten derselben Bedrohung schneller zu finden. Eine hochwertige XDR-Lösung kann dies automatisch und fortlaufend direkt in den Arbeitsablauf bei Sicherheitsvorfällen integrieren. Die Erkenntnisse aus den Untersuchungen gewährleisten dann, dass wiederholte Angriffe generell erfolglos bleiben.

Compliance-basierte Bedrohungssuche

Mit dieser Art der Bedrohungssuche soll überprüft werden, ob unternehmensinterne und branchenübliche Richtlinien sowie gesetzliche Vorgaben hinsichtlich der Datensicherheit eingehalten werden. Dazu wird routinemäßig nach nichtkonformem Verhalten gesucht, beispielsweise nach sensiblen Daten, die in nicht dafür autorisierten Systemen gespeichert sind, oder nach Hinweisen darauf, dass Administratoren ihre Zugriffsprivilegien ausweiten oder an andere weitergeben. Eine XDR-Lösung kann so konfiguriert werden, dass sie kontinuierlich nach derartigen Aktivitäten Ausschau hält und Benachrichtigungen generiert, damit sie zeitnah erkannt und unterbunden werden können.

Auf maschinelles Lernen gestützte Bedrohungssuche

Bei dieser Art der Bedrohungssuche erstellen maschinelle Lernverfahren ein Modell des für eine Umgebung typischen Verhaltens. Diese sogenannte „Baseline“ kann dann genutzt werden, um zu beurteilen, ob ein bestimmtes beobachtetes Verhalten für die Umgebung normal ist oder nicht. Mittels umfassender Analysen lernen XDR-Lösungen auf diese Weise, von der „Baseline“ abweichende Vorgänge zu erkennen. Mithilfe dieser

Überblick

Vorteile von XDR für die Bedrohungssuche

Mit XDR können Bedrohungssucher:

- Daten aus dem Netzwerk, aus der Cloud und von den Endpunkten für Suchen und Analysen nutzen
- Automatisierte Funktionen für die Durchsuchung aller Aktivitäten im Netzwerk, in der Cloud und auf Endpunkten einsetzen
- Mit hochgradig konfigurierbaren Suchfunktionen und maschinellen Assistenten in der Bedrohungsbibliothek nach IOCs und BIOCs suchen, die auf interne oder externe Bedrohungen hindeuten
- Bei Angriffen entstehende Schäden durch die Verknüpfung der verschiedenen Sicherheitsmaßnahmen begrenzen und beheben

CORTEX XDR™ BY PALO ALTO NETWORKS

sogenannten verhaltensbasierten Gefahrenindikatoren (behavioral indicators of compromise, BIOCs) können viele gut getarnte Angreiferaktivitäten erkannt werden, die Analysten höchstwahrscheinlich nicht aufgefallen wären. Die maschinellen Lernmodelle lassen sich kontinuierlich optimieren. Diese Form der Bedrohungssuche bringt dem Analystenteam die größte Zeitersparnis und ist für die Verbesserung des Sicherheitsniveaus unverzichtbar.

Zusammenfassung

Unternehmen müssen ihre Technologien und Prozesse für die Erkennung und Abwehr von Cyberangriffen grundlegend ändern. Erstens sind herkömmliche Punktlösungen zu begrenzt in ihrer Funktionalität und zudem weder flexibel noch skalierbar genug, um mit den Angreifern von heute Schritt zu halten. Zweitens sind in den meisten SecOps-Teams effizientere und effektivere Arbeitsweisen erforderlich, um den in der Sicherheitsbranche herschenden Fachkräftemangel auszugleichen. Mit XDR können Sie beide Herausforderungen bewältigen, denn dieser neue Ansatz bietet nicht nur Transparenz über Endpunkte, Netzwerke und Cloud-Umgebungen hinweg, sondern auch auf maschinellem Lernen basierte Analyseverfahren und integrierte Gegenmaßnahmen, die die Bedrohungssuche, -erkennung, -untersuchung und -abwehr entscheidend verbessern.

Checkliste für XDR-Ausschreibungen

Um eine Infrastruktur effizient und effektiv vor den heutigen komplexen Angriffen zu schützen, muss XDR zahlreiche gängige EDR-Funktionen abdecken und zudem mit wichtigen anderen Tools für die Prävention, Erkennung und Abwehr zusammenarbeiten, die über die gesamte Infrastruktur verteilt sein können. Die folgende Checkliste enthält neun Anforderungskategorien zur Beurteilung und zum Vergleich verschiedener Plattformen.

Wir empfehlen, dass Sie diese Checkliste als Ausgangspunkt betrachten und an die spezifische Situation in Ihrem Unternehmen bzw. Ihrer Institution anpassen, bevor Sie sie zur Auswahl des Anbieters nutzen, der Ihre Anforderungen am besten erfüllt.

Sie können die Checkliste auch als Kalkulationstabelle herunterladen und sofort damit arbeiten: go.paloaltonetworks.com/xdrrfp.

1. Anforderungen in puncto AV

- ☐ PML-basierte Bedrohungsprävention
- ☐ Verhaltensbasierte Bedrohungsprävention
- ☐ Prävention bekannter Exploit-Techniken
- ☐ Signaturbasierte Bedrohungsprävention
- ☐ Echtzeit-Aktualisierung von Urteilen durch den Anbieter
- ☐ Integration in Cloud-basierten Malware-Analyseservice
- ☐ Transparente Updates der Threat Detection Engine
- ☐ Sicherheitsprofile und Ausnahmen
- ☐ Spontane und geplante Scans von Endpunkten

- ☐ Schutz vor Malware, Ransomware und dateilosen Angriffen
- ☐ Ein einziger, schlanker Agent für den Endpunktschutz und für die Bedrohungserkennung und -abwehr

2. Anforderungen in puncto Datentransparenz und Protokollierung

Benutzerdaten

- ☐ Domain-Name und definierter Name
- ☐ E-Mail-Adresse
- ☐ Abteilung
- ☐ Telefonnummer

Geräteinformationen

- ☐ MAC-Adresse
- ☐ Host-Name des Geräts
- ☐ Domain-Name
- ☐ Definierter Name des Hosts
- ☐ Abteilung
- ☐ Betriebssystem
- ☐ Betriebssystemversion
- ☐ Name der Firewall, falls zutreffend
- ☐ Andere von der Firewall-Konfiguration verwendete Namen, falls zutreffend

Prozessinformationen

- ☐ Prozess-Timestamp
- ☐ Pfad und Name
- ☐ Prozess-ID
- ☐ Geladene Module
- ☐ Hashwerte wie MD5 und SHA-256
- ☐ Befehlszeilenargumente
- ☐ Signaturstatus

Dateiinformationen für Vorgänge wie das Erstellen, Schreiben, Lesen, Öffnen, Umbenennen oder Löschen von Dateien

- ☐ Timestamp
- ☐ Pfad und Name
- ☐ Vorheriger Dateiname und Pfadname bei Umbenennungen
- ☐ Hashwerte wie MD5 und SHA-256
- ☐ Nutzername

Netzwerkaktivität einschließlich ein- und ausgehende Verbindungen sowie fehlgeschlagene Verbindungsversuche

- ☐ Timestamp
- ☐ Empfänger- und Absender-IP und -Port
- ☐ Anzahl gesendeter und empfangener Bytes

- ☐ Protokoll
- ☐ Beteiligtes Land
- ☐ Proxy-Informationen
- ☐ Benutzer
- ☐ Integration mit Next-Generation Firewalls für vollständige Layer-7-Transparenz einschließlich Anwendungsname
- ☐ Verbindungsdauer
- ☐ Daten von der Transaktionsebene und zusätzliche Informationen über die wichtigsten Protokolle wie DNS, HTTP, DHCP, RPC, ARP und ICMP

Aktivitäten in der Registrierung wie Erstellen, Ändern, Löschen und Umbenennen von Schlüsseln

- ☐ Timestamp
- ☐ Name des Schlüssels
- ☐ Wert und Typ
- ☐ Vorheriger Schlüsselname bei Umbenennungen

Systemereignisse

- ☐ Änderungen des Benutzerstatus (wie Login oder Logout)
- ☐ Änderungen des Host-Status
- ☐ Änderungen des Agenten-Status

Sicherheits-Benachrichtigungen

- ☐ Protokolldateien für das URL Filtering

CORTEX XDR™ BY PALO ALTO NETWORKS

- ☐ Protokolldateien von Firewalls
- ☐ Protokolldateien von Endpunkten

Benutzer-Kontextdaten

- ☐ Angemeldeter Benutzer
- ☐ Typischer Benutzer eines Geräts
- ☐ Ersteller des Prozesses, der die Kommunikation begonnen hat
- ☐ Benutzergruppe und Abteilung aus Verzeichnisdiensten

3. Anforderungen in puncto Dauer und Umfang der Datenspeicherung

- ☐ Übersicht über die Ausbreitung im Netzwerk und in anderen Teilen der Infrastruktur
- ☐ Erkennung und Abwehr von Bedrohungen sowohl an verwalteten als auch nicht verwalteten Endpunkten
- ☐ Erkennung und Abwehr von Bedrohungen, bei denen Remote-Nutzer involviert sind (als Urheber oder Betroffene)
- ☐ Erkennung und Abwehr von Bedrohungen, bei denen Cloud-Nutzer involviert sind (als Urheber oder Betroffene)
- ☐ Mindestens 30 Tage Datenspeicherung
- ☐ Ein Jahr Speicherung der Audit-Logs von Verwaltungs- und Untersuchungsaktivitäten

4. Anforderungen in puncto Untersuchungen

- ☐ Automatisierte Ursachenanalyse für jede Benachrichtigung, einschließlich Netzwerkbenachrichtigungen, wenn Endpunktdaten zur Verfügung stehen

- ☐ Funktion zur Anzeige der Folge von Ereignissen, die zu einer Benachrichtigung geführt haben
- ☐ Funktion zur Anzeige aller Aktionen und Benachrichtigungen auf einem Zeitstrahl
- ☐ Funktion zur Suche nach Gefahrenindikatoren (IOCs) und bestimmten Endpunktaktivitäten
- ☐ Funktion zur Durchsuchung von Online- und Offline-Hosts
- ☐ Einfacher Wechsel zwischen Ansichten am Analysten-Arbeitsplatz
- ☐ Nuancierte Filterung und Sortierung von Abfrageergebnissen
- ☐ Anzeige, ob ein Ereignis von einem Endpunkt-Agenten, einer Firewall oder einer anderen präventiven Technologie blockiert wurde
- ☐ Automatisierte Verknüpfung sicherheitsrelevanter Benachrichtigungen aus verschiedenen Quellen, beispielsweise von Firewalls und Endpunkten
- ☐ Unterdrückung nichtssagender Meldungen, Entfernung irrelevanter Binärdateien und DLLs aus der Verlaufskette
- ☐ Kontextinformationen zu Taktiken, Techniken und Prozessen bekannter Angreifer für SOC-Analysten, Unterstützung für die Verwendung der gewonnenen Erkenntnisse in zukünftigen Untersuchungen

5. Anforderungen in puncto Incident Management

- ☐ Automatisierte Gruppierung zusammengehöriger Benachrichtigungen aus verschiedenen Quellen zu einem einzigen Vorfall
- ☐ Funktion zum Extrahieren wichtiger Artefakte aus Benachrichtigungen zum Abgleich mit Bedrohungsdaten
- ☐ Funktion zum Herausfiltern der für einen Vorfall relevanten Elemente für eine übersichtlichere Darstellung

- ☐ Funktion zur Zuweisung von Vorfällen an Teammitglieder
- ☐ Funktion zur Benachrichtigung der Teammitglieder bei der Zuweisung eines Vorfalls
- ☐ Funktion zum Einfügen von Kommentaren
- ☐ Funktion(en) für die Verwaltung des gesamten Lebenszyklus eines Vorfalls (neu, in Untersuchung, geschlossen, behoben usw.)
- ☐ Funktion(en) zur Aufspaltung und Zusammenführung von Vorfällen
- ☐ Funktion zum Weiterleiten von Vorfallsdaten an externe Fallmanager

6. Anforderungen in puncto Bedrohungsdaten

- ☐ Fähigkeit zur Nutzung von IOC-Regeln, um eine Benachrichtigung zu generieren, wenn ein als schädlich bekanntes Objekt auf einem Endpunkt gefunden wird
- ☐ Automatische Durchsuchung historischer Daten und Generieren der entsprechenden Benachrichtigungen, wenn neue IOCs in das System eingespeist werden
- ☐ Integration mit einem oder mehreren Bedrohungsdaten-Service(s) für Bedrohungsdaten-Tags und zusätzlichen Kontext für wichtige Artefakte
- ☐ Fähigkeit zur Ausführung beliebiger Skripte per Fernzugriff

7. Anforderungen in puncto Reaktion

- ☐ Remote-Terminal-Funktionen
- ☐ Remote-Terminal mit grafischer Benutzeroberfläche (und nicht nur einer Befehlszeilenschnittstelle)
- ☐ Möglichkeit zur Ausführung von CMD-, PowerShell- und Python-Befehlen
- ☐ Möglichkeit zur Ausführung benutzerdefinierter Skripte

CORTEX XDR™ BY PALO ALTO NETWORKS

- ☐ Isolierung von Endpunkten per Fernzugriff
- ☐ Löschen von Dateien per Fernzugriff
- ☐ Automatisches und manuelles Erfassen oder Abrufen von Dateien und Objekten, die in Quarantäne sind
- ☐ Unterbrechen oder Beenden von Prozessen per Fernzugriff
- ☐ Funktion zur Anzeige laufender Prozesse
- ☐ File-Manager mit Funktionen zum Anzeigen, Herunterladen, Umbenennen oder Verschieben von Dateien
- ☐ Task-Manager mit grafischer Benutzeroberfläche

8. Anforderungen in puncto Erkennung, Integration und Automatisierung

- ☐ Verhaltensanalysen zur Erstellung von Benutzer- und Endpunktprofilen und zur Erkennung von Anomalien, die auf Angriffe hindeuten
- ☐ Funktionen für überwachtes und nicht überwachtes maschinelles Lernen
- ☐ Vordefinierte und benutzerdefinierbare Regeln für die verhaltensbasierte Bedrohungserkennung
- ☐ Benutzerdefinierte Regeln für die rückblickende Bedrohungserkennung
- ☐ Integration von SIEM-Lösungen (Security Information and Event Management)
- ☐ Zugriff auf Crowdsourcing-Bedrohungsdaten aus Cloud-basierten Malware-Analyse-Services; Verteilung dieser Daten auf Firewalls, Endpunkt-Agenten und Erkennungs- und Abwehrservices
- ☐ Integration einer SOAR-Lösung (Security Orchestration, Automation and Response) zur Vorfallsanalyse
- ☐ Fähigkeit zur Erkennung von Ausspähaktivitäten und Seitwärtsbewegungen

9. Anforderungen in puncto Systemsupport und Ressourcen

- ☐ Modularer Produktaufbau und Skalierbarkeit
- ☐ Cloud-basierte Implementierung
- ☐ Vollständige Protokollierung aller Aktivitäten im System
- ☐ Möglichst niedrige Anzahl erforderlicher Agenten
- ☐ Durchschnittliche CPU-Belastung unter 3 %, wenn alle Services aktiviert sind
- ☐ Installationsgröße der Agenten unter 50 MB
- ☐ Aktualisierung der Agenten per „Push“ von der Management-Konsole aus
- ☐ Lauffähigkeit auf und Schutz für alle macOS- und Mac OS X-Versionen der letzten fünf Jahre
- ☐ Unterstützung für Android
- ☐ Unterstützung aller wichtigen Linux-Distributionen
- ☐ Unterstützung aller neueren Windows-Versionen einschließlich Windows Server
- ☐ Mehrfaktor-Authentifizierung für das Management
- ☐ Unterstützung für nicht persistente VDI
- ☐ Unterstützung temporärer Sitzungen für Maschinen, die wiederholt auf Snapshots (oder Images) zurückgesetzt werden, auf denen kein Agent installiert ist

10. Anforderungen in puncto Managed Services (optional)

Wenn Ihr SecOps-Team sich für komplettes Outsourcing oder ein Hybrid-Modell entscheidet, können Sie auch die folgende Checkliste für die Bewertung verwalteter Sicherheitsservices nutzen:

- ☐ Überwachung und Verfügbarkeit rund um die Uhr, 365 Tage im Jahr

CORTEX XDR™ BY PALO ALTO NETWORKS

- □ Funktionen zum Importieren, Priorisieren und Sichten von Benachrichtigungen aller Anbieter
- □ Identifikation und Validierung kritischer Bedrohungen innerhalb höchstens einer Stunde
- □ Überblick über alle Datenquellen wie Endgeräte, Netzwerkpakete und-sitzungen sowie Cloud-Pakete, -Sitzungen und -Konfigurationen
- □ Monitoring nicht verwalteter Geräte, Erkennung von anormalem Verhalten auf diesen Geräten
- □ Monitoring und Erkennung von anormalem Benutzerverhalten
- □ Kontinuierliche proaktive Bedrohungssuche auf verwalteten und nicht verwalteten Geräten
- □ Feineinstellung von Tools für individuelle Kundenumgebungen (einschließlich kundenspezifischer Regeln und Ausnahmen)
- □ Möglichkeiten zur Kontaktaufnahme mit Spezialisten per E-Mail, Telefon oder Messenger (z. B. Slack)
- □ Portal oder mobile App für Transparenz, Kommunikation und Reaktion
- □ Zugriff auf Tools durch den Kunden

Oval Tower, De Entrée 99-197
1101 HE Amsterdam
Niederlande

Telefon: +31 20 888 1883

www.paloaltonetworks.de

Detection-and-Response-ebook-111219-de

Technisch versierte Hacker können auch die besten Verteidigungssysteme unterwandern und geschäftskritische Daten manipulieren oder stehlen – oftmals mit verheerenden Folgen für den Ruf eines Unternehmens. Die meisten Unternehmen haben bereits Tools implementiert, die Angriffe blockieren, bei denen die erste Verteidigungslinie schon überwunden wurde. Diese überwachen und schützen jedoch meist nur einen winzigen Teil der IT-Infrastruktur. Diese Tools sind nicht intelligent oder integriert genug, um die verschiedenen zu einem Angriff gehörigen Ereignisse miteinander in Beziehung zu setzen. Stattdessen generieren sie Benachrichtigungen für alles, was entfernt verdächtig wirkt – hunderte oder sogar tausende pro Tag. Sicherheitsanalysten müssen dann viel Zeit damit verbringen, die wirklich wichtigen Benachrichtigungen aus dieser Flut herauszufischen. Wenn ihnen eine echte Bedrohung durch die Maschen geht, bleibt sie oft monatelang unbemerkt.

Diese Vorgehensweise ist schlicht nicht mehr gut genug.

Doch es gibt inzwischen eine ganze Kategorie besserer Tools für die Bedrohungserkennung und Abwehr: XDR. Diese Tools verknüpfen Daten aus Netzwerken, Cloud-Umgebungen und von Endpunkten in einem robusten Data Lake miteinander. Zudem nutzen sie modernste, auf maschinellem Lernen basierte Analysen und stellen den Analysten Kontextinformationen bereit, sodass sie Vorfälle schneller und einfacher untersuchen können. In diesem E-Book erfahren Sie mehr über:

- die Herausforderungen, mit denen herkömmliche Tools für die Bedrohungserkennung und abwehr ihre Nutzer konfrontieren
- taktische Anwendungsbereiche für die Verbesserung der Sicherheitsprozesse mit XDR
- die Definition von und die wichtigsten Anforderungen an XDR-Lösungen