LERNEN LEICHT GEMACHT

Palo Alto Networks Sonderausgabe

# XDR

für dummies®

Was ist XDR und was nicht?

Angriffsketten mit XDR durchbrechen

Anwendungsfälle für XDR

Präsentiert von

CORTEX XDR BY PALO ALTO NETWORKS

Lawrence Miller

## Über Palo Alto Networks

Palo Alto Networks ist ein weltweit führender Anbieter von Cybersicherheitslösungen und gestaltet mit Technologien, welche die Arbeitsweise von Menschen und Unternehmen verändern, eine cloudzentrierte Zukunft. Wir möchten bevorzugter Cybersicherheitspartner werden und zum Schutz unserer digitalen Lebensweise beitragen. Mit unseren kontinuierlichen Innovationen, die sich die neuesten bahnbrechenden Entwicklungen in den Bereichen künstliche Intelligenz, Analytik, Automatisierung und Orchestrierung zunutze machen, meistern wir die größten Sicherheitsherausforderungen der Welt. Durch die Bereitstellung einer integrierten Plattform und die Unterstützung eines wachsenden Partnernetzwerks sind wir führend beim Schutz zehntausender Unternehmen über Clouds, Netzwerke und Mobilgeräte hinweg. Unsere Vision ist eine Welt, in der jeder neue Tag sicherer ist als der letzte. Für weitere Informationen besuchen Sie www.paloaltonetworks.com.

# XDR

Palo Alto Networks Sonderausgabe

**Lawrence Miller**

für dummies®

# XDR Für Dummies®, Palo Alto Networks Sonderausgabe

Veröffentlicht von
**John Wiley & Sons, Inc.**
111 River St., Hoboken, NJ 07030-5774
www.wiley.com



ISBN 978-1-119-87897-1 (pbk); ISBN 978-1-119-87898-8 (ebk)

## Danksagung des Verlags

Die folgenden Personen haben dabei geholfen, dieses Buch auf den Markt zu bringen:

**Project Editor:** Elizabeth Kuball
**Acquisitions Editor:** Ashley Coffey
**Editorial Manager:** Rev Mengle
**Business Development Representative:** Cynthia Tweed
**Production Editor:** Mohammed Zafar

# Einführung

Der Schutz kritischer Daten ist eine Herausforderung, die Jahr für Jahr größer wird. Die schnelle Übernahme von Trends wie Cloud Computing, Internet der Dinge und die digitale Transformation erhöhen maßgeblich das Risiko für sensible Unternehmensdaten. Bedrohungsakteure machen sich viele dieser modernen Technologietrends zunutze, um immer größere und raffiniertere Angriffskampagnen zu starten.

Sicherheitsteams nutzen bereitgestellte Tools, implementierte Prozesse und eigene Mitarbeiter, um ihre Unternehmen vor immer neuen Bedrohungen zu schützen. Doch die Angreifer sind ihnen nicht nur zahlenmäßig überlegen, sondern auch besser ausgerüstet. Durch das ständige Aufsetzen neuer Funktionen auf bestehende Systeme entsteht ein wahres Durcheinander aus schlecht integrierten Tools, deren Nutzung viel Zeit, Energie und Fachwissen erfordert. Statische Prozesse, die sich nicht an sich schnell ändernde Trends und Umgebungen wie die Cloud und Remote-Arbeit anpassen lassen, werden rasch unflexibel und ineffektiv. Sicherheitsanalysten haben dann die fast unmögliche Aufgabe, eine nicht enden wollende Flut von Sicherheitswarnungen zu selektieren, auch wenn sie oft nur über mangelnde Kenntnisse verfügen und unzureichende Tools verwenden müssen. Die Kombination aus zu vielen Warnmeldungen und zu wenig Kontext führt dazu, dass Sicherheitsteams den Überblick und die Kontrolle verlieren. Dadurch wird das Unternehmen letztendlich noch verwundbarer.

Um dieses komplexe Problem zu lösen, wurde Extended Detection and Response (XDR) entwickelt. XDR ist eine Kategorie von Lösungen zur Erkennung, Untersuchung und Abwehr von Bedrohungen, die die verschiedenen Bedrohungsvektoren in der Infrastruktur eines Unternehmens – d. h. Netzwerk, Endpunkt, Cloud und Identität – nicht als einzelnen Aspekt, sondern als Ganzes behandeln. Dank der direkten Integration in die Architektur des Unternehmens liefern XDR-Tools bessere Einblicke in Bedrohungen und geben Empfehlungen aus, die die Arbeitsweise von Sicherheitsteams optimieren.

## Über dieses Buch

*XDR Für Dummies* enthält nützliche Informationen über diese Kategorie von Sicherheitslösungen und ihre Bedeutung für Ihr Unternehmen. Dieses Buch besteht aus fünf Kapiteln, die sich mit den folgenden Themen befassen:

- dem aktuellen Stand der Bedrohungserkennung und -abwehr, einschließlich Einschränkungen und Herausforderungen (Kapitel 1)
- Was ist XDR und was nicht? (Kapitel 2)
- Wie durchbricht XDR den Angriffslebenszyklus, um Angriffe zu stoppen? (Kapitel 3)
- diverse Anwendungsfälle für XDR (Kapitel 4)
- unverzichtbare Funktionen und Merkmale einer XDR-Lösung (Kapitel 5)

Jedes Kapitel ist in sich geschlossen. Sie können deshalb einfach zu einem Thema springen, das Ihr Interesse weckt. Lesen Sie das Buch, wie es Ihnen am liebsten ist (verkehrt herum oder rückwärts würden wir allerdings nicht empfehlen).

# Leichtfertige Annahmen

Einem Zitat zufolge haben die meisten unserer Annahmen ihre Nutzlosigkeit überlebt. Ich erlaube mir trotzdem, einige Annahmen zu treffen:

Ich gehe davon aus, dass Sie für ein Unternehmen arbeiten, das nach einem besseren Weg sucht, um die Effektivität seiner Sicherheitsstrategie zu verbessern, insbesondere seine Bedrohungserkennung und -abwehr. Vielleicht sind Sie eine IT-Führungskraft, z. B. Chief Information Security Officer (CISO), Chief Information Officer (CIO), Chief Technology Officer (CTO), VP oder Director of Security. Womöglich sind Sie auch ein Netzwerk- oder Sicherheitsarchitekt oder -techniker. Dieses Buch ist daher in erster Linie für technische Leser mit allgemeinen Kenntnissen über moderne Sicherheitskonzepte und -technologien vorgesehen.

Wenn Sie sich in einer dieser Beschreibungen wiedererkennen, dann ist dieses Buch genau richtig für Sie. Wenn keine dieser Annahmen auf Sie zutrifft, lesen Sie trotzdem weiter – XDR ist eine Technologie, die man kennen muss. Ihr Team wird es Ihnen danken, wenn Sie ein Experte für XDR werden!

# In diesem Buch verwendete Symbole

In diesem Buch verwende ich gelegentlich besondere Symbole, um Ihre Aufmerksamkeit auf wichtige Informationen zu lenken. Sie werden auf die folgenden Hinweise stoßen:

WICHTIG

Dieses Symbol macht auf wichtige Informationen aufmerksam, die Sie Ihrem nichtflüchtigen Speicher bzw. Ihrem Kopf zusätzlich zu all den Jubiläen und Geburtstagen anvertrauen sollten!

TECHNISCHES

Wenn Sie in Zukunft mit Fachbegriffen und -wissen prahlen möchten, sind Sie hier an der richtigen Stelle! Dieses Symbol erläutert den Jargon hinter dem Jargon und signalisiert, dass hier näher auf technische Details eingegangen wird.

TIPP

Tipps sind meist unerwartet, aber wertvoll. Ich hoffe jedenfalls, dass die in diesem Buch enthaltenen Tipps nützlich für Sie sein werden.

WARNUNG

Dieses Symbol macht auf Dinge aufmerksam, vor denen Sie Ihre Mutter schon immer gewarnt hat. Trotzdem sollten Sie diese Warnungen beherzigen, denn sie helfen Ihnen dabei, kostspielige und frustrierende Fehler zu vermeiden.

## Zusätzliche Informationen

In diesem kurzen Buch können wir natürlich nur eine Auswahl der wichtigsten Themen behandeln. Wenn Sie nach der Lektüre unbedingt noch mehr erfahren wollen, besuchen Sie bitte `www.paloaltonetworks.com/cortex/cortex-xdr`.

**IN DIESEM KAPITEL**

- **Warum ein besseres Sicherheitskonzept benötigt wird**
- **Verständnis der Einschränkungen herkömmlicher Tools zur Bedrohungserkennung und -abwehr**
- **Ermüdungserscheinungen durch die Alarmflut und Fachkräftemangel im IT-Sicherheitsbereich**

# Kapitel 1
# Der aktuelle Stand der Bedrohungserkennung und -abwehr

In diesem Kapitel werde ich erklären, warum moderne Cyberbedrohungen heute mehr Schaden anrichten können als je zuvor, und weshalb herkömmliche Ansätze zur Prävention, Erkennung und Abwehr von Bedrohungen nicht mehr ausreichen. Außerdem werden wir uns ansehen, wie Ermüdungserscheinungen durch Alarmflut und der im Cybersicherheitsbereich herrschende Fachkräftemangel zu größeren Risiken für Ihr Unternehmen führen.

## Übersicht über die moderne Bedrohungslandschaft

Datenschutzverletzungen und Ransomware-Angriffe traten in letzter Zeit so häufig auf, dass sie neben dem Wetter, Sport und Verkehr eigentlich ihre eigene Nachrichtenrubrik verdienen. Die Tatsache, dass Berichte über Sicherheitsvorfälle so zahlreich geworden sind, macht sie jedoch nicht weniger gefährlich. Jede Minute, in der ein aktiver Bedrohungsakteur in Ihrer Umgebung sein Unwesen treibt, kann enorme Schäden verursachen.

WARNUNG

Nach Angaben des Ponemon Institute stiegen die durchschnittlichen Kosten einer Datenpanne zwischen 2020 und 2021 um 10 Prozent auf 4,24 Millionen US-Dollar an. Dies war der größte jährliche Zuwachs in den vergangenen sieben Jahren.

Natürlich sind Sie sich dessen längst bewusst und bemühen sich, Bedrohungen so schnell wie möglich zu erkennen und abzuwehren, bevor es zu Datenverlusten kommt. Doch angesichts der immer perfider werdenden Taktiken, Techniken und Verfahren der Bedrohungsakteure ist das ein harter Kampf. Angreifer sind heute in der Lage, eine Umgebung nahezu beliebig zu kompromittieren, ohne herkömmliche Methoden wie dateibasierte Malware einzusetzen. Stattdessen hacken sie zum Beispiel autorisierte Systemdateien, unterwandern die Geräteregistrierung oder missbrauchen Dienstprogramme wie PowerShell. Diese neuartigen, besser getarnten Methoden erfordern neue Strategien und Taktiken, die über die übliche Bedrohungsabwehr hinausgehen.

WICHTIG

benötigen Unternehmen effektive Tools und ein Team fähiger Sicherheitsanalysten. Leider ist eine ausgewogene Kombination aus Technologie und qualifizierten Experten für die meisten Unternehmen eher die Ausnahme als die Regel.

## Einschränkungen herkömmlicher Technologien und Ansätze

Auch wenn sich Ihr Sicherheitsteam nach Kräften bemüht, möglichst alle gegen Ihr Unternehmen gerichteten Angriffe zu verhindern, müssen Sie sich auf die unvermeidliche Tatsache einstellen, dass keine Umgebung vollkommen sicher ist. Irgendwann wird es einem Angreifer gelingen, sich Zugang zu Ihrer Umgebung zu verschaffen.

Auf dem Markt gibt es unzählige Tools für die Protokollierung, Erkennung und Abwehr von Bedrohungen, die Sicherheitsteams beim Aufspüren von Bedrohungen helfen können. Jedes dieser Tools hat seine eigenen Stärken und Schwächen und kann einen wirksamen Schutz vor Angriffen bieten – etwa gegen bekannte dateibasierte Malware oder bei Angriffen, bei denen nur ein Teil der Infrastruktur ausgeschaltet werden soll. Die meisten dieser Tools sind jedoch für einen ganz bestimmten Zweck gedacht und es gibt keines, das wirklich gut mit komplexen Bedrohungen umgehen kann.

WARNUNG

Laut ESG Research herrscht in 66 Prozent der Unternehmen die Ansicht, dass die Bedrohungserkennung und -abwehr darunter leidet, wenn mehrere unabhängige Punktlösungen verwendet werden.

In den folgenden Abschnitten werde ich näher auf einige der gebräuchlichsten Tools zur Protokollierung, Erkennung und Abwehr von Bedrohungen eingehen, die von Sicherheitsteams verwendet werden. Außerdem werde ich ihnen die damit verbundenen Herausforderungen und Einschränkungen vorstellen.

## Endpoint Detection and Response

*Endpoint Detection and Response* (EDR) ist eine Kategorie von Tools, die zur Erkennung und Untersuchung von Bedrohungen auf Endpunkten eingesetzt werden. EDR-Tools bieten in der Regel Funktionen zur Erkennung, Analyse, Untersuchung und Reaktion auf Bedrohungen.

EDR kam erstmals 2013 bei forensischen Untersuchungen zum Einsatz, bei denen sehr detaillierte Endpunkt-Telemetrie für das Reverse Engineering von Malware und zur Rekonstruktion des Angriffsverlaufs auf einem kompromittierten Gerät benötigt wurde.

EDR-Tools überwachen von Endpunkt-Agenten generierte Ereignisse, um verdächtige Aktivitäten aufzuspüren. Die von EDR-Tools erstellten Warnmeldungen helfen Securityanalysten bei der Identifizierung, Untersuchung und Behebung von Sicherheitsvorfällen. EDR-Tools erfassen auch Telemetriedaten über verdächtige Aktivitäten und können die Daten mit weiteren kontextbezogenen Informationen von korrelierten Ereignissen anreichern. Durch diese Funktionen trägt EDR maßgeblich zur Verkürzung der Reaktionszeiten von Incident-Response-Teams bei.

Da sich EDR-Lösungen jedoch ausschließlich auf Endpunkte konzentrieren, können sie allein keine Bedrohungserkennung für Großunternehmen bieten. Zudem können sie nur mithilfe spezieller Agenten auf vernetzten und Netzwerkgeräten – Router, Switches, Server, IoT-Geräte (Internet of Things), Bring Your Own Device (BYOD), Industrial Control System (ICS) – und in Cloud-Ressourcen, z. B. Workloads, Cloud-Netzwerken und Platform-as-a-Service (PaaS)-Angeboten, Einblicke in den Netzwerkverkehr von Geräten bieten.

## Endpoint Protection Platform

Eine *Endpoint Protection Platform* (EPP) ist ein Software-Agent, der auf Endpunkten installiert wird, um dateibasierte Malware-Angriffe zu verhindern und bösartige Aktivitäten zu erkennen. EPP ist eine Weiterentwicklung herkömmlicher hostbasierter Antiviren- und Anti-Malware-Lösungen und gilt gemeinhin als die erste Verteidigungslinie am Endpunkt.

Die Erkennungsmöglichkeiten von EPP-Lösungen variieren. Die meisten verwenden eine Kombination aus Erkennungs- und Abwehrmethoden, darunter:

- statische Indicators of Compromise (IOCs, also signaturbasierte Erkennung)

- *Allowlisting* (Zulassen) oder *Blocklisting* (Sperren) von Anwendungen, URLs, Ports und Adressen
- Verhaltensanalyse und maschinelles Lernen
- Sandboxing zum Entpacken (oder Testen) mutmaßlicher Bedrohungen, z. B. ausführbarer Dateien

Eine EPP-Lösung sollte über die Cloud verwaltet werden, damit Aktivitätsdaten kontinuierlich überwacht und erfasst werden können. Gleichzeitig sollte sie die Möglichkeit bieten, aus der Ferne Maßnahmen zu ergreifen, unabhängig davon, ob der Endpunkt im Unternehmensnetz oder per Fernzugriff verwendet wird. EPP-Lösungen stützen sich auf Cloud-Daten. Der Endpunkt-Agent muss also keine lokale Datenbank mit allen bekannten IOCs unterhalten, sondern kann einfach eine Cloud-Ressource abfragen, um aktuelle Informationen zu Objekten zu finden, die er nicht klassifizieren kann. Zudem kann er verfügbare Bedrohungsdaten in Echtzeit nutzen.

EPP dient lediglich der Prävention oder Kontrolle und ist daher nicht auf die Erkennung oder Erfassung von Informationen zur Verteidigung gegen moderne Angriffe ausgerichtet. Die meisten EPP-Plattformen verfügen zudem nicht über die zur Untersuchung von Vorfällen erforderlichen Funktionen und reichen daher nicht aus, um moderne Angriffe zu stoppen.

## Security Information and Event Management

*Security Information and Event Management* – kurz SIEM-Tools bzw. -Software – ermöglichen die Erfassung, Korrelation und Analyse von Sicherheitsvorfällen nahezu in Echtzeit. Sie stellen Benachrichtigungen über Alarme bereit, die von verschiedenen Netzwerkgeräten und -anwendungen generiert werden.

Viele Unternehmen geben einen großen Teil ihres Sicherheitsbudgets für SIEM-Tools aus, um Protokolle von verschiedenen Sicherheitstools und Serverumgebungen zusammenzutragen. Tatsächlich wurden SIEM-Lösungen ursprünglich als Protokollsammler für die Compliance-Berichterstellung entwickelt. Im Laufe der Zeit wurden sie auch zur Bedrohungserkennung eingesetzt und inzwischen verwenden viele Security Operations Center (SOC) ein SIEM-Tool als zentrales Repository für Benachrichtigungen.

SIEM-Lösungen zentralisieren Warnmeldungen und aggregieren Protokolldaten durch Parsen und Normalisieren. Sicherheitsteams können zwar alle Protokolldaten an einem einzigen Ort sehen, doch diese Daten werden in der Regel nicht in einer aussagekräftigen Form zusammengestellt. Zudem können die mit der Auswertung der Daten beauftragten

Analysten oft nicht die Tools verwenden, welche die zur Validierung von Warnmeldungen erforderlichen umfassenden Quelldaten enthalten. SIEM-Tools fehlt es an der für wichtige Informationsquellen wie Endpunkt- und Netzwerkdaten erforderlichen Analysetiefe. Außerdem gestaltet sich deren Bereitstellung, Konfiguration und Wartung oft schwierig, was zum Teil daran liegt, dass sie nicht vorkonfiguriert sind.

### Network Detection and Response und User and Entity Behavior Analytics

*Network Detection and Response* (NDR) und *User and Entity Behavior Analytics* (UEBA) sind Begriffe, die sich auf eine neuere Kategorie von Sicherheitsanalysetools beziehen. Sie wurden zur Bewältigung der Herausforderungen entwickelt, mit denen SIEM-Systeme bei der Erkennung unbekannter Angriffe konfrontiert sind. Diese Tools machen sich maschinelle Lernverfahren zunutze, um auf der Grundlage der erfassten Telemetriedaten eine Baseline zu erstellen und dann nach davon abweichenden atypischen Vorgängen zu suchen, die auf bösartiges Verhalten hindeuten könnten. Da diese Technologien Muster für ungewöhnlichen Datenverkehr erkennen können, ermöglichen sie es Unternehmen, bisher unbekannte Angriffe zu identifizieren.

Aber auch diesen Tools sind Grenzen gesetzt. Netzwerkbasierte Produkte sind auf das Netzwerk beschränkt und können keine lokalen Ereignisse überwachen oder verfolgen, z. B. auf Endpunkten erfasste Prozessinformationen. NDR Tools arbeiten außerdem nicht sehr tiefgehend. Während EDR sehr gründliche Untersuchungen anstellt, arbeitet NDR zwar großflächig, aber nur oberflächlich.

WICHTIG

Aufgrund der Komplexität moderner Angriffe müssen Daten aus verschiedenen Quellen analysiert werden, um verdächtige Aktivitäten zu erkennen und zu validieren. Die Nutzung mehrerer eindimensionaler Tools kann für Sicherheitsteams hohe Kosten verursachen und möglicherweise zu toten Winkeln führen. Und für Sicherheitsanalysten, die ständig von Konsole zu Konsole wechseln müssen, kann dies einen hohen manuellen Aufwand erfordern.

## Zu viele Warnmeldungen, zu wenig Zeit und Personal

Erkennungs- und Präventionstools erzeugen täglich Tausende von Warnmeldungen – weit mehr, als ein Sicherheitsteam effektiv bewältigen kann. Hinzu kommt, dass diese Warnmeldungen meist aus vielen voneinander getrennten Quellen stammen. Sicherheitsanalysten haben dann die Aufgabe, sie mühsam zueinander in Beziehung zu setzen (siehe Abbildung 1-1).

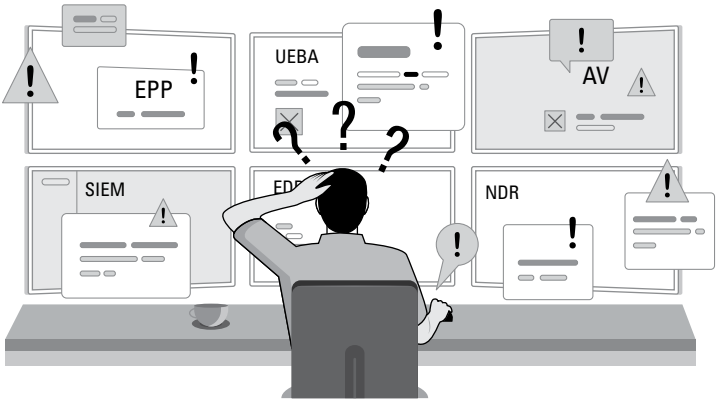


**ABBILDUNG 1-1:** Isolierte Tools erschweren die Untersuchung und Behebung von Sicherheitsvorfällen.

Zur Analyse einer potenziellen Bedrohung sind in der Regel mehrere Schritte erforderlich:

1. Durchsuchung der verfügbaren Protokolldaten nach Hinweisen, die zur Rekonstruktion des Vorgangs verwendet werden können
2. Manueller Vergleich dieser Hinweise mit Bedrohungsdaten aus unterschiedlichen Quellen, um zu ermitteln, ob die Indikatoren als schädlich bekannt sind
3. Suche nach verbundenen Ereignissen mithilfe von IOCs, um zu bestimmen, ob der Alarm Teil eines größeren Angriffs ist
4. Sammeln von Informationen über den Vorfall, einschließlich der Systeme, Hosts, Assets, Ressourcen, IP-Adressen und Dateien, die mit jedem Alarm verbunden sind
5. Erstellung eines Zeitplans und Identifizierung der Grundursache eines Alarms
6. Prüfung, ob diese neuen Hinweise bereits von anderen Teammitgliedern untersucht werden, und Koordination der Maßnahmen
7. Beurteilung, ob Warnmeldungen zu eskalieren, zu ignorieren oder schnell zu beheben und blockieren sind

Alle diese Schritte sind zeitaufwendig und erfordern in herkömmlichen SOCs die Nutzung mehrerer Tools – und das allein für die Triage. Infolgedessen haben Analysten meist nur Zeit, um sich um Warnmeldungen mit „höchster Priorität“ zu kümmern. Eine beunruhigende Anzahl von Meldungen mit „niedrigerer Priorität“ bleibt tagtäglich unbearbeitet. Und ohne den richtigen Kontext, um die Priorität einer Warnmeldung als „hoch“ oder „niedrig“ einzustufen, übersieht das SOC möglicherweise, was wirklich wichtig ist, und/oder verfolgt weniger kritische Probleme.

## WELCHE AUFGABE HAT EIN SOC-TEAM?

Große wie kleine Security-Operations-Teams übernehmen wichtige Funktionen. In vielen SecOps- und SOC-Teams werden diese Funktionen normalerweise entsprechend den Erfahrungsstufen der Analysten unterteilt. Die typischen Verantwortungsbereiche der verschiedenen Stufen sind:

- **Stufe 1 – Triage:** Diese Stufe ist für Sicherheitsanalysten besonders arbeitsintensiv. Analysten der ersten Stufe sind in der Regel weniger erfahren. Ihre Hauptaufgabe ist die Überwachung von Ereignisprotokollen auf verdächtige Aktivitäten. Wenn sie das Gefühl haben, dass etwas genauer untersucht werden sollte, tragen sie möglichst viele Kontextinformationen aus diversen Quellen zusammen und erstellen einen Schadensbericht, der den Benutzer, den Host, die IP-Adresse und alle zugehörigen IOCs enthält. Danach wird der Vorfall zur Stufe 2 eskaliert.
- **Stufe 2 – Untersuchung:** Die Analysten der zweiten Stufe untersuchen die verdächtige Aktivität näher. Sie bestimmen die Art der Bedrohung und ermitteln, wie weit sie schon in die Infrastruktur eindringen konnte. Dazu gehört auch die Erstellung eines Zeitplans, um den Verlauf der Ereignisse zu verstehen, sie zu korrelieren und die Ursache herauszufinden. Sie müssen weitere Untersuchungen durchführen, um zu verstehen, wie weit der Angriff bereits fortgeschritten ist. Dann koordinieren sie die Maßnahmen zur Behebung des Problems. Für diese Tätigkeit ist oft eine höhere Qualifikation oder mehr Erfahrung mit Analysen erforderlich.
- **Stufe 3+ – Bedrohungssuche:** Hier kommen die erfahrensten Analysten zum Zug. Sie unterstützen komplexe Maßnahmen zur Bedrohungsabwehr und suchen in der verbleibenden Zeit in forensischen Daten und Telemetriedaten nach Bedrohungen, die von der Erkennungssoftware möglicherweise nicht als verdächtig erkannt wurden (auch genannt: "Threat Hunting"). In einem typischen Unternehmen ist der Ressourcenaufwand für Analysen auf Stufe 1 und 2 so groß, dass nur ein Bruchteil der verfügbaren Arbeitszeit für die proaktive Bedrohungssuche bleibt.

Dieses Modell ist zwar weit verbreitet, aber alles andere als ideal. Den meisten Menschen fällt es schwer, den ganzen Tag lang Protokolle zu überprüfen. Sie leiden früher oder später unter Ermüdungserscheinungen durch die Alarmflut und übersehen dann Bedrohungen, die zwischen den vielen irrelevanten Meldungen („Rauschen") der zahlreichen Sensoren in einem SOC verborgen sind. Viele Analysten lassen sich nur schwer bei der Stange halten, weil sie viel lieber einen sinnvollen Beitrag zu den Untersuchungen leisten würden (und vielleicht auch neue und innovative Ideen haben, die sie nicht umsetzen können, weil ihnen die Fachkenntnisse fehlen, die für die veralteten Untersuchungsmethoden erforderlich sind). Bei diesem Ansatz kommen die Bedrohungssuche und die Verbesserung von Prozessen zu kurz, weil das Personal die meiste Zeit mit der Erkennung und Eindämmung verbringt.

Zudem haben die mit der Triage betrauten Sicherheitsanalysten oftmals zu wenig Kontext, um das echte Risiko eines Angriffs auf das Unternehmen korrekt einzuschätzen. Daher eskalieren sie Meldungen im Zweifelsfall an eine höher qualifizierte Gruppe, die dann noch einmal Zeit, Arbeit und Ressourcen investieren muss, was zu Ineffizienzen auf allen Ebenen führt.


Die meisten Unternehmen erhalten Tausende von Warnmeldungen von vielen unterschiedlichen Überwachungslösungen, doch das dadurch entstehende „Rauschen" ist kontraproduktiv. Für eine bessere Bedrohungserkennung sind nicht *mehr* Meldungen erforderlich, sondern *bessere* und aussagekräftigere. Eine effektive Erkennung verdächtiger Aktivitäten in Ihrer Umgebung erfordert nicht nur die Integration aller verwendeten Erkennungstechnologien, sondern auch intelligentere Analysen von Endpunkt-, Netzwerk- und Cloud-Daten.

Selbst mit besseren und umfassenderen Tools zur Erkennung von Bedrohungen erfordert der Umgang mit Warnmeldungen – und möglichen Vorfällen – eine weitere Validierung und Triage durch qualifizierte Mitarbeiter. Leider gibt es nicht genügend dieser Sicherheitsexperten und dieser erhebliche Fachkräftemangel beeinträchtigt die Fähigkeit von Unternehmen, mit Angreifern Schritt zu halten (siehe Abbildung 1-2).

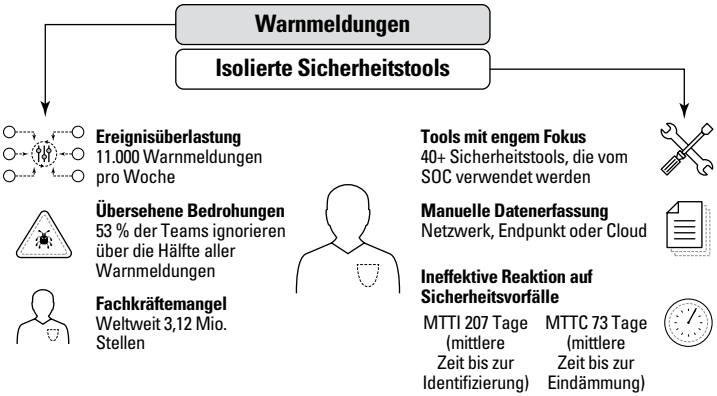


**ABBILDUNG 1-2:** Die vielen Herausforderungen eines Sicherheitsanalysten

Bedrohungsakteure nutzen inzwischen hochgradig automatisierte Tools, um Schwachstellen zu finden und sich Zugang zu Ihrer Umgebung zu verschaffen. Dadurch werden die Auswirkungen des Fachkräftemangels noch verschärft, denn die Angreifer skalieren ihre

automatisierten Toolkits schneller und kostengünstiger als Unternehmen qualifizierte Mitarbeiter finden und einarbeiten können. Deshalb sollten Sie nach Tools Ausschau halten, die Folgendes können:

- Ihre weniger erfahrenen Mitarbeiter leistungsfähiger und effizienter machen
- die Erkennung komplexer Bedrohungen automatisieren
- Untersuchungen vereinfachen
- Analysten beim Ausbau ihrer Fähigkeiten unterstützen

TIPP

Das International Information Systems Security Certification Consortium, kurz ISC², berichtet in seiner *Cybersecurity Workforce Study 2020*, dass weltweit 3,12 Millionen qualifizierte Cybersicherheitsexperten benötigt werden. Laut Cyberseek gibt es heute in den Vereinigten Staaten über 300.000 offene Stellen im Bereich Cybersicherheit – eine Zahl, die in den kommenden Jahren voraussichtlich noch erheblich steigen wird.

Viele Unternehmen entscheiden sich dafür, ihre Erkennungs- und Reaktionsfunktionen ganz oder teilweise an MSSP- (Managed Security Service Provider) oder MDR-Anbieter (Managed Detection and Response) auszulagern. Die Auslagerung dieser Funktionen ist verbreitet (und gilt in vielen Fällen als Best Practice), besonders für Teams mit kleineren Sicherheitsbudgets oder Unternehmen, die weder den Wunsch noch die nötigen Ressourcen haben, um ihre Sicherheitsfunktionen selbst zu verwalten. Unternehmen, die eine umfassende Transparenz und Kontrolle anstreben, sollten jedoch nicht zur Auslagerung ihrer Sicherheit gezwungen sein, nur weil ihre Tools unzureichend sind. Es ist auch erwähnenswert, dass die Technologie-Basis für ein ausgelagertes Sicherheitsteam ebenso wichtig ist. Anbieter, die veraltete Tools verwenden, haben mit denselben Ineffizienzen zu kämpfen, die auch interne Sicherheitsteams plagen.

Was wirklich benötigt wird, sind Technologien, die die Gesamtzahl der Warnmeldungen reduzieren und weniger erfahrenen Analysten die Möglichkeit geben, Bedrohungen effizient und souverän selbst zu bewerten. Dadurch wird sichergestellt, dass nur zuverlässige Warnmeldungen an erfahrenere Analysten weitergeleitet werden.

**IN DIESEM KAPITEL**

- **Zuverlässige Bedrohungsabwehr reduziert das „Rauschen"**
- **Durchgängige Transparenz für Ihre gesamte Umgebung**
- **Reduzierung von manuellen Untersuchungen zur Beschleunigung und Verbesserung der Reaktion auf Vorfälle**
- **Maximale Rendite für Ihre Sicherheitsinvestitionen**

# Kapitel 2
# Was ist XDR?

Extended Detection and Response (XDR) ist ein neuer Ansatz zur Bedrohungserkennung und -abwehr. Der Begriff *XDR* wurde 2018 von Nir Zuk, Chief Technology Officer (CTO) und Mitbegründer von Palo Alto Networks, geprägt. XDR wurde mit dem Ziel entwickelt, Angriffe effizienter zu stoppen, die Techniken und Taktiken von Angriffen zu erkennen, die nicht verhindert werden können, und SOC-Teams bei der Reaktion auf Bedrohungen zu helfen, die untersucht werden müssen.

Laut Forrester Research optimiert XDR „die Erkennung, Untersuchung, Behebung und Abwehr von Bedrohungen in Echtzeit. XDR vereint sicherheitsrelevante Endpunkterkennungsfunktionen mit Telemetrie von Sicherheits- und Business-Tools wie Network Analysis and Visibility (NAV), E-Mail-Sicherheits-, Identitäts- und Zugriffsmanagement, Cloud-Sicherheit und vielen mehr in einer Lösung."

Das *X* in XDR steht für *extended* (erweitert), stellt aber im Grunde jede beliebige Datenquelle dar, da es weder effizient noch effektiv ist, einzelne Komponenten einer Umgebung isoliert zu betrachten. XDR ermöglicht einen proaktiven Ansatz zur Bedrohungserkennung und -abwehr, der Transparenz über mehrere Netzwerke, Clouds und Endpunkte hinweg bietet und gleichzeitig Analyse- und Automatisierungsfunktionen einsetzt, um die immer perfider werdenden Bedrohungen von heute zu bekämpfen.

In diesem Kapitel werden wir uns genauer ansehen, was XDR ist und welche wesentlichen Anforderungen eine XDR-Lösung erfüllen muss.

# Gewährleistung einer zuverlässigen Bedrohungsabwehr

Die Grundlage von XDR ist eine absolut zuverlässige Bedrohungsabwehr. Eine XDR-Lösung sollte über 99 Prozent aller echten Bedrohungen abwehren, die automatisch in Echtzeit oder nahezu in Echtzeit blockiert werden können; und das ohne manuelle Überprüfung. Mit einer erstklassigen Prävention kann sich Ihr Team auf die Erkennung und Abwehr besonders perfider und verdeckter Angriffe konzentrieren, anstatt Zeit mit der Untersuchung jeder potenziellen Bedrohung zu verschwenden, die das Abwehrsystem überwunden hat.

Zur Bekämpfung von Endpunktbedrohungen benötigen Sie eine robuste Lösung mit integriertem Antivirenschutz der nächsten Generation (NGAV), der jede Phase eines Angriffs erkennen und vereiteln kann – vom ersten Exploit und der Malware-Installation bis hin zu den illegalen Aktivitäten, die von Bedrohungsakteuren mit Malware ausgeführt werden. Jede Verteidigungsebene muss intelligent genug sein, um die Umgehungstechniken von Bedrohungsakteuren zu erkennen und sich kontinuierlich anpassen, um die neuesten Bedrohungen aufzuhalten.

TIPP

Achten Sie bei einer XDR-Lösung auf die folgenden NGAV-Funktionen:

- auf maschinellem Lernen (ML) basierende lokale Analyse und Bedrohungsabwehr
- verhaltensbasierte Bedrohungsabwehr für die dynamische Analyse laufender Prozesse
- Exploit-Prävention nach Exploit-Methode
- Schutz vor bekannten Bedrohungen auf der Grundlage von Bedrohungsdaten, wie Datei-Hashes
- automatische Integration in einen cloudbasierten Malware-Präventionsservice mit Analyseberichten und Unterstützung von Dateien mit einer Mindestgröße von 100 MB
- Zero-Delay-Signaturen für sofortige Schutzmaßnahmen und das schnelle Teilen von Bedrohungsdaten
- Reverse-Shell-Schutzfunktion
- transparente Updates der Bedrohungserkennungs-Engine
- Sicherheitsprofile und Ausnahmen
- spontane und geplante Scans von Endpunkten
- Schutz vor Malware, Ransomware und dateilosen Angriffen

- ein einziger einfacher Agent für Endpunktschutz, -erkennung und -reaktion

Ihre XDR-Lösung sollte auch Ihre Angriffsfläche reduzieren und sensible Daten mit Endpunktschutz-Funktionen absichern, darunter:

- Host-Firewall
- Festplattenverschlüsselung
- USB-Gerätekontrolle (Universal Serial Bus)
- anpassbare Präventionsregeln

Ihre XDR-Lösung sollte außerdem mit einem Netzwerksicherheits-Client für Endgeräte kompatibel sein, damit sie sicheren Fernzugriff, Bedrohungsabwehr und URL-Filterung (Uniform Resource Locator) bieten kann.

## Vollständige Transparenz und Bedrohungserkennung

Transparenz und Bedrohungserkennung sind für die Bedrohungsabwehr von entscheidender Bedeutung. Wenn Sie eine Bedrohung nicht *sehen* können, sind Sie nicht in der Lage, sie zu identifizieren, zu untersuchen oder gar aufzuhalten. Bedrohungsakteure machen sich die Cloud und maschinelles Lernen zunutze, um große und mehrstufige Angriffe durchzuführen, damit sie längerfristig wertvolle Daten ausschleusen und geistiges Eigentum ausschlachten können. XDR muss daher über robuste Transparenz- und Erkennungsfunktionen wie die folgenden verfügen:

- **Umfassende Transparenz und Verständnis des Kontexts:** Voneinander isolierte Punktlösungen führen zu Datensilos und sind daher nicht effektiv. Sie werden sich kaum wirksam vor Angriffen schützen können, wenn Sie in Ihrer eigenen Umgebung nicht mindestens ebenso agil sind wie die Bedrohungsakteure. Eine XDR-Lösung muss über Transparenz- und Erkennungsfunktionen für Ihre gesamte Umgebung verfügen und Telemetriedaten von Ihren Endpunkten, Netzwerken und Cloud-Umgebungen integrieren. Außerdem muss sie in der Lage sein, diese Datenquellen zu korrelieren, damit Sie nachvollziehen können, wie einzelne Ereignisse miteinander verknüpft sind und wann ein bestimmtes Verhalten in einem bestimmten Kontext verdächtig ist oder auch nicht (siehe Abbildung 2-1).

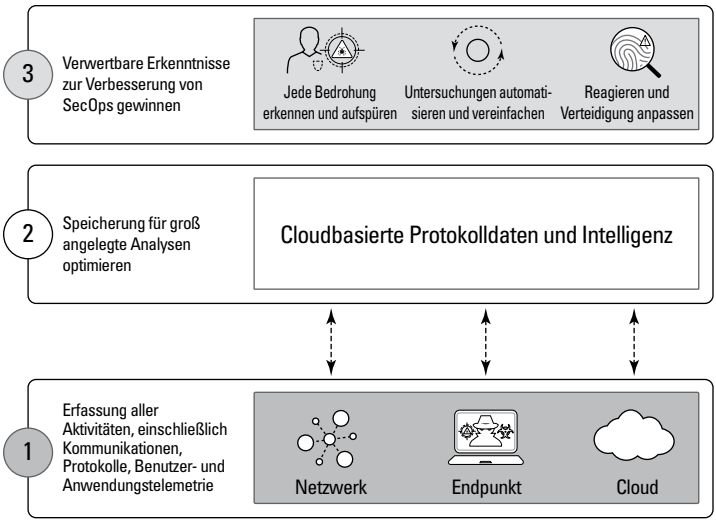


**ABBILDUNG 2-1:** XDR bricht typische Silos bei der Bedrohungserkennung und -abwehr auf.

- **Datenaufbewahrung:** Angreifer sind geduldig und hartnäckig. Sie wissen, dass sie weniger auffallen, wenn sie langsam vorgehen und dass es sich lohnt, die Protokollaufbewahrungszeiträume 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, korrelieren und analysieren, das eine Aufbewahrungsfrist von mindestens 30 Tagen bietet.
- **Analyse des internen und externen Datenverkehrs:** Herkömmliche Erkennungstechnologien konzentrieren sich hauptsächlich auf externe Angreifer und Bedrohungen und übersehen dadurch andere potenzielle Bedrohungsakteure. Tools zur Bedrohungserkennung dürfen sich nicht auf Angriffe von außerhalb des Netzwerkperimeters beschränken. Sie müssen auch Profile von internen Bedrohungen erstellen und diese analysieren, um ungewöhnliches und potenziell schädliches Verhalten zu erkennen, das auf einen Missbrauch von Anmeldedaten hindeutet.
- **Integrierte Bedrohungsdaten:** Sie müssen 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 Unternehmensnetzwerk stützen. Sobald ein Unternehmen in Ihrem erweiterten Netzwerk 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 stellt spezifische Herausforderungen dar, die unter anderem von bestimmten Systemen, unterschiedlichen Benutzergruppen und den diversen Bedrohungsakteuren abhängen. Deshalb müssen Erkennungssysteme flexibel an die jeweiligen Anforderungen Ihrer Umgebung anpassbar sein. Das bedeutet unter anderem, dass eine XDR-Lösung sowohl vordefinierte als auch benutzerdefinierte Erkennungsmethoden unterstützen muss.
- **ML-basierte Bedrohungserkennung:** Zur Erkennung von unüblichen Malware-Angriffen, bei denen beispielsweise autorisierte Systemdateien kompromittiert, Scripting-Umgebungen missbraucht oder die Registry angegriffen werden, muss Erkennungstechnologie erweiterte Analysetechniken nutzen, um die erfasste Telemetrie auszuwerten. Für diesen Ansatz sind überwachtes und teilüberwachtes maschinelles Lernen erforderlich.

TIPP

Halten Sie nach einer XDR-Lösung Ausschau, die die folgenden Hauptanforderungen an die Transparenz und Bedrohungserkennung erfüllt:

- Verhaltensanalysen zur Erstellung von Verhaltensprofilen und zur Erkennung von Anomalien, die auf einen Angriff hindeuten, durch Analyse des Netzwerkverkehrs und der Endpunkt- und Benutzerereignisse im Zeitverlauf
- überwachte und nicht überwachte ML-Funktionen
- vordefinierte und benutzerdefinierbare verhaltensbasierte Erkennungsregeln
- benutzerdefinierte Regeln für die nachträgliche Bedrohungserkennung
- granulare Alarmausschlüsse für die optionale Anpassung von Endpunkt-, Netzwerk-, Cloud- oder Drittanbieterwarnungen
- gemeinsame Nutzung von Bedrohungsdaten, um auf Crowdsourcing basierende Bedrohungsdaten aus cloudbasierten Malware-Analyseservices an Firewalls, Endpunktagenten sowie Erkennungs- und Abwehrservices zu verteilen
- Möglichkeit, Bedrohungsdaten-Feeds von Drittanbietern in den Formaten JSON (JavaScript Object Notation) und CSV (Comma-Separated Values) zu nutzen

- Erkennung von Angriffstechniken über den gesamten Angriffslebenszyklus hinweg, einschließlich Entdeckung, Lateral Movement, Command and Control sowie Exfiltration
- nachgewiesene Fähigkeit zur Erkennung von Angreifertaktiken und -techniken durch MITRE ATT&CK-Evaluierungen (Adversarial Tactics, Techniques & Common Knowledge)
- Kennzeichnung von MITRE ATT&CK-Taktiken und -Techniken in Warnmeldungen und Erkennungsregeln
- Asset-Management mit Erkennung von nicht autorisierten Geräten
- Bewertung von Schwachstellen
- Hostbestand mit detaillierten Benutzer-, System- und Anwendungsinformationen

## Automatisierung von Untersuchungen und Abwehrmaßnahmen

Wenn Sie vor potenziellen Bedrohungen in Ihrer Umgebung gewarnt werden, müssen Sie in der Lage sein, diese Bedrohungen schnell einzustufen und zu untersuchen. Hier versagen herkömmliche Systeme zur Bedrohungserkennung und -abwehr oft, wenn sich ein Angriff insbesondere gegen mehrere Bereiche einer Umgebung richtet. XDR-Lösungen können diesen Prozess erheblich verbessern, da sie über die folgenden Untersuchungs- und Abwehrfunktionen verfügen:

- **Korrelation und Gruppierung von zusammengehörigen Warnmeldungen und Telemetriedaten:** Bei Angriffen auf Ihr Unternehmen zählt jede Sekunde. Ihr Angreifer arbeitet bereits intensiv an der Umsetzung seiner Ziele in Ihrer Umgebung, wenn Sie eine Bedrohungswarnung erhalten. Sie müssen sich so schnell wie möglich einen Überblick über den Angriff und seine gesamte Kausalitätskette verschaffen. Dazu muss Ihr XDR-Tool zunächst ähnliche Meldungen zusammenfassen und effektiv die Ereignisse priorisieren, auf die am dringendsten reagiert werden muss, um unnötiges Rauschen zu reduzieren. Außerdem muss das XDR-Tool in der Lage sein, den Angriffsverlauf durch das Zusammenfügen von Aktivitätsprotokollen aus Ihren Netzwerk-, Endpunkt- und Cloud-Umgebungen zu rekonstruieren. Durch die Visualisierung von Aktivitäten und Sequenzierung von Ereignissen können Sie die Ursache des Angriffs ermitteln und den möglichen Schaden und Umfang einschätzen (siehe Abbildung 2-2).

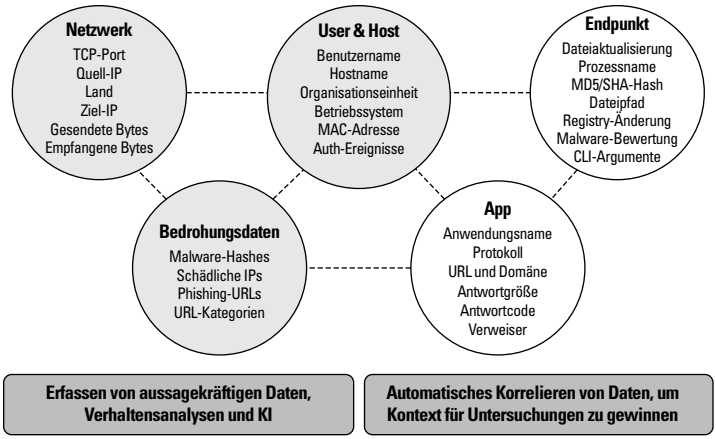


**ABBILDUNG 2-2:** XDR korreliert und verknüpft aussagekräftige Daten.

- **Schnelle Untersuchung von Vorfällen mit sofortigem Zugriff auf alle forensischen Artefakte, Ereignisse und Bedrohungsdaten an einem Ort:** Schnelle Ermittlung von Angreiferaktivitäten durch Überprüfung wichtiger Artefakte wie Ereignisprotokolle, Registrierungsschlüssel, Browserverlauf usw. Mit modernen Open-Source-Tools sind Sicherheitsteams gezwungen, Beweise von den unterschiedlichsten Agenten und Skripten zusammenzutragen. Agenten, die nur für eine Aufgabe eingesetzt werden – Forensik, Endpunktschutz, Bedrohungserkennung und -abwehr – können die Leistung beeinträchtigen und die Komplexität erhöhen. Um einen Vorfall aufzuklären, müssen Sie den Eintrittspunkt des Angreifers finden, um seine Spuren verfolgen zu können – auch wenn er versucht hat, sie zu verwischen.
- **Konsolidierte Benutzeroberflächen, die schnelle Ansichtswechsel erlauben:** Zur Untersuchung von Warnmeldungen benötigen Ihre Analysten eine optimierte 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 mehreren verschiedenen Tools verschwenden müssen.
- **Manuelle und automatische Bedrohungssuche:** In immer mehr Unternehmen suchen SecOps-Teams proaktiv nach aktiven Angreifern, wobei die Analysten Angriffshypothesen entwickeln und in den Systemen nach entsprechenden Aktivitäten Ausschau halten. Für die erfolgreiche Bedrohungssuche sind leistungsstarke Suchfunktionen erforderlich, um Belege für die Hypothesen zu finden, sowie integrierte Bedrohungsdaten, um nach schädlichen Aktivitäten zu

suchen, die bereits im erweiterten Netzwerk beobachtet wurden. Diese Bedrohungsdaten sollten so integriert und automatisiert sein, dass sofort klar ist, ob eine Bedrohung schon erkannt wurde. Somit müssen Analysten keine unzähligen manuellen Aufgaben erledigen und beispielsweise 30 verschiedene Browserregisterkarten öffnen, um zahlreiche Bedrohungsdaten-Feeds nach einer bekanntermaßen schädlichen IP-Adresse zu durchforsten.

- **Orchestrierung von Behebungsmaßnahmen:** Nachdem ein Angriff entdeckt und untersucht wurde, ist der nächste Schritt eine effiziente und effektive Abwehr. Ihr System muss in der Lage sein, die koordinierte Reaktionen auf aktive Bedrohungen zu orchestrieren und zukünftige Angriffe auf Ihre Netzwerk-, Endpunkt- und Cloud-Umgebungen zu vereiteln. Dazu müssen die verschiedenen Abwehrtechnologien miteinander kommunizieren, entweder nativ oder über APIs (Application Programming Interfaces). So muss beispielsweise ein Angriff, der im Netzwerk blockiert wird, zu einer automatischen Aktualisierung der Richtlinien auf den Endpunkten führen. Außerdem müssen Analysten direkt über die XDR-Schnittstelle Abwehrmaßnahmen ergreifen können.

TIPP

Achten Sie bei einer XDR-Lösung auf die folgenden Untersuchungs- und Abwehrfunktionen:

- automatisierte Ursachenanalyse für jede Warnmeldung, einschließlich Netzwerk-Warnmeldungen, wenn Endpunktdaten zur Verfügung stehen
- Visualisierung der Ereignisketten, die zu einer Warnmeldung geführt haben
- Anzeige aller Aktionen und Warnmeldungen auf einer Zeitleiste zu Analysezwecken
- Abfrage von Indicators of Compromise (IOC) und Endpunktverhaltensweisen, von Online- und Offline-Hosts, Netzwerkverkehrsprotokollen von Firewalls und Authentifizierungsprotokollen von Identitätsverwaltungsanbietern
- erweiterte Abfragesprache mit Unterstützung für Wildcards, reguläre Ausdrücke, JSON, Datenaggregation, Feld- und Wertmanipulation, Zusammenführung von Daten aus unterschiedlichen Quellen und Datenvisualisierung
- einfacher Wechsel zwischen verschiedenen Ansichten für Analysten, granulare Filterung und Sortierung von Abfrageergebnissen
- automatische Zusammenfassung relevanter IP- oder Hash-Informationen, Bedrohungsdaten, Ereignissen und zugehöriger Vorfälle in

einer einzigen Ansicht, um Untersuchungen zu vereinfachen und den Zugang zu bösartigen IP-Adressen oder Domänen zu blockieren

- Anzeige, ob ein Ereignis von einem Endpunktagenten, einer Firewall oder einer anderen Präventionstechnologie blockiert wurde; Möglichkeit, laufende Prozesse per Fernzugriff anzuzeigen, zu unterbrechen, zu beenden oder Binärdateien herunterzuladen
- automatisierte Verknüpfung sicherheitsrelevanter Warnmeldungen aus verschiedenen Quellen, zum Beispiel von Firewalls und Endpunkten
- Unterdrückung von Rauschen und Entfernung irrelevanter Binärdateien und DLLs (Dynamic-Link-Libraries) aus der Ereigniskette
- Kontextinformationen zu Taktiken, Techniken und Verfahren von Angreifern für SOC-Analysten, um die gewonnenen Erkenntnisse für zukünftige Untersuchungen zu nutzen
- Integration in SOAR- (Security Orchestration, Automation and Response) und SIEM-Lösungen (Security Information and Event Management)
- Ereignisbewertung zur Einstufung und Priorisierung von risikoreichen Vorfällen, damit sich Analysten schnell auf die gefährlichsten Bedrohungen konzentrieren können; Erstellung von Ereignisbewertungen auf der Grundlage von Alarmattributen, einschließlich der Benutzer oder Hosts in einer Warnmeldung
- Quarantäne schädlicher Dateien und deren Entfernung aus ihren Arbeitsverzeichnissen
- schnelles Auffinden und Löschen von Dateien im Unternehmen mit Search and Destroy zur Indizierung von Endpunktdateien
- direkter Zugriff auf Endpunkte mit Live-Terminal, um Python-, PowerShell- oder Systembefehle oder Skripte auszuführen, aktive Prozesse zu überprüfen und zu verwalten sowie Dateien anzuzeigen, zu löschen, zu verschieben oder herunterzuladen

## Erhöhung der Sicherheitswirkung

XDR sollte Ihre Rendite aus Ihren Sicherheitsinvestitionen erheblich steigern. Das bedeutet, dass die Effizienz und Effektivität Ihres SecOps-Teams verbessert werden muss, um den Fachkräftemangel zu verhindern oder zu überwinden. Zudem sollten Ihre vorhandenen Tools besser integriert und die Angriffsprävention laufend durch eine skalierbare Infrastruktur und den Einsatz von künstlicher Intelligenz (KI) gestärkt werden. Um all dies zu erreichen, benötigt Ihre XDR-Lösung die folgenden Funktionen:

- **Orchestrierung von Sicherheitsmaßnahmen:** Orchestrierung ist nicht nur für die Vereinfachung der Bedrohungsabwehr wichtig, sondern erlaubt auch die Maximierung der Rendite aus Ihren Investitionen in Sicherheitstechnologien. In fast allen Unternehmen wurden bereits Sicherheitslösungen implementiert, die zur Reaktion auf aktive Bedrohungen genutzt werden können. Der Erfolg eines Systems zur Bedrohungserkennung und -abwehr hängt wesentlich davon ab, wie gut die Investitionen in die vorhandenen Maßnahmen genutzt werden, um eine konsistente Reaktion im gesamten Unternehmen zu gewährleisten.
- **Erfassung externer Daten:** Jedes Unternehmen verfügt heute über unterschiedliche, voneinander isolierte Sicherheitstools. Je besser eine XDR-Lösung die Daten aus jedem dieser Tools erfassen und nutzen kann, desto umfangreicher ist der bereitgestellte Schutz. Die besten XDR-Lösungen zeichnen sich durch eine hohe Flexibilität aus, um Daten aus anderen Tools in Ihre Umgebung zu importieren, sie voll auszunutzen und die Effektivität zu maximieren.
- **Skalierbare Speicher- und Rechenkapazität:** Angesichts der Hartnäckigkeit von modernen Bedrohungsakteuren sollten Sie keine Telemetriedaten löschen, die Hinweise auf bedächtig ausgeführte Low-and-Slow-Angriffe enthalten könnten, die mehrere Monate oder sogar Jahre dauern. Außerdem benötigen Sie eine bestimmte Analyseleistung, um all diese Telemetriedaten effektiv nutzen zu können. Cloudbasierte XDR-Plattformen bieten eine nahezu unbegrenzte Zugänglichkeit und Skalierbarkeit.
- **Ständige Verbesserungen:** Die Erkennung von immer raffinierteren Hackerangriffen erfordert neben künstlicher Intelligenz oder maschinellem Lernen auch Automatisierung und Orchestrierung. So kann manuelle Kleinarbeit reduziert und Sicherheitsanalysten die Möglichkeit gegeben werden, effektiver und effizienter zu arbeiten. XDR-Lösungen sollten aus Erfahrung lernen, zukünftige Risiken minimieren und die Prävention kontinuierlich stärken, indem sie die bei der Erkennung, Untersuchung und Abwehr von Bedrohungen gewonnenen Erkenntnisse anwenden.
- **Berichte und Dashboards:** Sicherheitsteams müssen den Sicherheitsstatus und die betrieblichen Kennzahlen des Unternehmens verstehen und kommunizieren können. XDR-Lösungen sollten also nicht nur die sicherheitsrelevanten Ergebnisse verbessern, sondern das Sicherheitsniveau auch in intuitiven und anpassbaren Berichten und Dashboards darstellen können.

## Echt oder nicht? Was zeichnet eine wahre XDR-Lösung aus?

XDR findet in der Branche bei Analysten, Sicherheitsanbietern und Endbenutzern insgesamt immer größeren Anklang. Aber wie bei allen anderen Sicherheitslösungen gibt es davon verschiedene Varianten. Da es sich jedoch bei einigen XDR-Varianten lediglich um eine Umbenennung von Endpoint Detection and Response (EDR) handelt, verfügen die Lösungen mancher Anbieter nicht unbedingt über dieselben Funktionen. Es lohnt sich also, genau hinzusehen.

Wie kann man zwischen den auf dem Markt verfügbaren Angeboten unterscheiden? Einem führenden Branchenanalysten zufolge „haben nur wenige Anbieter ein echtes XDR-Produkt in ihrem Sortiment". Wie erkennt man, ob es sich bei einer Lösung um ein echtes XDR-Produkt handelt oder der jeweilige Anbieter lediglich ein „Trittbrettfahrer" ist? Die folgende Liste mit Spezifikationen ist zwar nicht erschöpfend, sie kann Ihnen jedoch dabei helfen, brauchbare Lösungen von den Fakes zu unterscheiden.

**Eine echte XDR-Lösung:**

- sollte in der Lage sein, Daten aus allen Datenquellen (einschließlich Datenquellen von Drittanbietern) zu erfassen, zu normalisieren und zu verarbeiten;
- sollte die Verknüpfung von Daten ermöglichen und sie nicht nur korrelieren;
- ist cloudnativ und kann im Wesentlichen unbegrenzt skaliert werden;
- liefert datenübergreifende Analysen durch die Kombination von Netzwerk-, Endpunkt-, Identitäts- und Cloud-Daten;
- wendet eine intelligente, erweiterte Logik an, um den gesamten Verlauf eines Vorfalls in einer einzigen Ansicht zu zeigen;
- sorgt für die automatische Zuordnung von Beweisen und Artefakten zum MITRE ATT&CK-Framework;
- bietet eine integrierte Funktion zur Durchführung detaillierter forensischer Analysen;
- wird von erstklassigen Teams im Bereich Sicherheitsforschung und Sicherheitsservices unterstützt.

**Folgt die Lösung einem Ansatz, bei dem die Prävention im Vordergrund steht?**

XDR steht für „Extended Detection and Response" (erweiterte Erkennung und Reaktion). Die Stärke dieser Lösung besteht in ihrer Fähigkeit, auf

*(continued)*

*(continued)*

einer tiefen Integrationsebene mit Geräten zusammenzuarbeiten, die Bedrohungen und Angriffe blockieren, unterbrechen und eindämmen können, bevor ein Schaden entsteht. Die wichtigsten dieser Geräte sind Netzwerkfirewalls und Endpunkte der nächsten Generation, da das Netzwerk die vollständige Aufzeichnung der Kommunikation und Endpunkte darstellt und zeigt, wie Benutzer mit allen Anwendungen und Daten interagieren.

**Stützt sich die Lösung bei der Bedrohungserkennung nur auf den Endpunkt?**

Kann die Lösung auch zwischen nicht verwalteten Geräten Angriffe auf der Grundlage von Identitäts-, Cloud- und Netzwerkdaten erkennen? Einige „XDR"-Anbieter behaupten, dass sie Netzwerkdaten erkennen. Damit meinen sie aber in Wirklichkeit den von Endpunktagenten erfassten Netzwerkdatenverkehr.

Mit einer echten XDR-Lösung können alle Daten mit Bedrohungsaktivitäten korreliert und mit MITRE ATT&CK-TTPs gekennzeichnet werden, um ein detaillierteres Bild von den Angreifertaktiken zu erhalten.

**Verfügt die Lösung über native Untersuchungs- und Abwehrfunktionen?**

Eine echte XDR-Lösung:

- nutzt Sicherheitsanalysen, um Empfehlungen zur Bedrohungsabwehr zu automatisieren;
- ermöglicht native Abwehrmaßnahmen auf dem Endpunkt;
- kann, aber muss nicht zur Bedrohungsabwehr in andere Tools wie SOAR integriert werden;
- ermöglicht die Bedrohungsabwehr an Durchsetzungspunkten von Endpunktnetzwerk- und Cloud-Umgebungen und nicht nur am Endpunkt;
- bietet native Unterstützung für die spontane Durchsuchung aller Datenquellen von Drittanbietern mit Untersuchungs- und Suchmethoden, die für Analysten optimiert wurden;
- optimiert die Triage und Untersuchungen, indem alle zugehörigen schädlichen Artefakte, Hosts, Benutzer und korrelierten Alarme angezeigt und dem MITRE ATT&CK-Framework zugeordnet werden;
- kann intelligente Empfehlungen für gezielte Abwehrmaßnahmen auf der Grundlage des MITRE ATT&CK-Frameworks bereitstellen.

IN DIESEM KAPITEL

- Eine Betrachtung des Angriffslebenszyklus
- Untersuchung eines Beispiels für einen mehrstufigen Angriff

# Kapitel 3
# XDR durchbricht den Angriffslebenszyklus

Bedrohungsakteure haben mittlerweile von direkten Angriffen auf geschäftskritische Server oder Ressourcen (Schock-and-Awe-Technik) auf einen langfristigen, mehrstufigen Prozess umgestellt, der Exploits, Malware sowie getarnte und verdeckte Bedrohungen in einem koordinierten Netzwerkangriff miteinander kombiniert („unauffällig und langsam“).

In diesem Kapitel werden wir uns den Angriffslebenszyklus genauer ansehen und zeigen, wie Extended Detection and Response (XDR) Ihnen dabei helfen kann, diesen Lebenszyklus zu durchbrechen, um Angriffe auf Ihre Umgebung zu verhindern. Wir beginnen mit einer allgemeinen Beschreibung der typischen Angriffsphasen. Viele Sicherheitsteams verwenden heute das MITRE ATT&CK-Framework (Adversarial Tactics, Techniques and Common Knowledge), um Bedrohungen in den verschiedenen Phasen eines Angriffs zu verfolgen. Eine echte XDR-Lösung sollte in der Lage sein, jeden Schritt eines Angreifers zu erkennen und den MITRE ATT&CK-Taktiken und -Techniken zuzuordnen, um Untersuchungen zu vereinfachen.

## Der Angriffslebenszyklus

Der Lebenszyklus eines Angriffs veranschaulicht die Ereignisfolge bzw. die einzelnen Schritte, die ein Angreifer durchführt, um ein Netzwerk zu infiltrieren und wertvolle Daten auszuschleusen oder zu stehlen. Dazu gehören die Ausnutzung einer Schwachstelle, die Installation von Malware, Command and Control, Lateral Movement und die Exfiltration (siehe Abbildung 3-1).

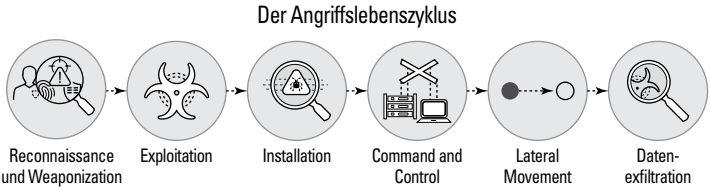


**ABBILDUNG 3-1:** Für einen erfolgreichen Angriff sind mehrere Schritte erforderlich.

TIPP

Wenn Sie bestimmte Schritte im Angriffslebenszyklus frühzeitiger erkennen können, haben Sie die Möglichkeit, Angreifer an der Ausführung späterer Angriffsphasen zu hindern. In den folgenden Abschnitten werden wir den Angriffslebenszyklus näher betrachten und erläutern, wie Ihnen eine XDR-Lösung dabei helfen kann, diesen Zyklus zu durchbrechen.

## Reconnaissance

Bedrohungsakteure planen ihre Angriffe minutiös. Sie recherchieren, ermitteln und wählen Ziele aus, wobei sie oft öffentlich zugängliche Informationen aus Social-Media-Profilen von Mitarbeitern oder von Unternehmenswebsites verwenden, die für Social-Engineering- und Phishing-Methoden nützlich sein können. Angreifer verwenden die unterschiedlichsten Tools, um nach Schwachstellen in Netzwerken, Services und Anwendungen zu suchen, z. B. Netzwerkanalysatoren, Scanner für die Suche nach Sicherheitslücken in Netzwerken und Webanwendungen, Passwortknacker und Portscanner.

XDR durchbricht den Angriffslebenszyklus in der Reconnaissance-Phase durch die kontinuierliche Überwachung und Inspektion des Netzwerkdatenverkehrs, um nicht autorisierte Port- und Schwachstellenscans, Host-Sweeps und andere verdächtige Aktivitäten zu erkennen und zu verhindern.

## Weaponization

Als Nächstes entscheiden Angreifer, mit welchen Methoden sie den anvisierten Endpunkt kompromittieren wollen. Sie können zum Beispiel schädlichen Code in scheinbar harmlose Dateien wie Microsoft Word-Dokumente oder E-Mail-Nachrichten einbetten. Bei sehr gezielten Angriffen können Angreifer die Dateien auch auf die Interessen einer bestimmten Person im Zielunternehmen abstimmen. Als Nächstes versuchen die Angreifer, die manipulierte Nutzlast an einen Zielendpunkt zu übermitteln, z. B. per E-Mail, Sofortnachricht, Drive-by-Download (wobei der Webbrowser eines Endbenutzers auf eine Webseite umgeleitet wird, die automatisch im Hintergrund Malware auf den Endpunkt herunterlädt) oder Freigabe einer infizierten Datei.

Es ist schwierig, den Angriffslebenszyklus in dieser Phase zu durchbrechen, da sie in der Regel im Netzwerk des Angreifers stattfindet.

Die Analyse der Artefakte (von Malware und Weaponizer) kann jedoch wichtige Bedrohungsdaten liefern, um einen wirksamen Zero-Day-Schutz gegen Angriffsversuche zu ermöglichen. XDR bietet Einblicke in den gesamten Netzwerkverkehr, um bösartige oder riskante Websites, Anwendungen und IP-Adressen effektiv zu blockieren und das Eindringen bekannter und unbekannter Malware und Exploits zu verhindern.

## Exploitation

Nachdem ein Schadprogramm in ein Zielendpunkt eingeschleust wurde, muss es aktiviert werden. Ein Endbenutzer kann unwissentlich einen Exploit auslösen, indem er beispielsweise auf einen bösartigen Link klickt oder einen infizierten Anhang in einer E-Mail öffnet. Ein Angreifer kann auch aus der Ferne einen Exploit für eine bekannte Schwachstelle des Servers im Zielnetzwerk auslösen.

Um den Angriffslebenszyklus in dieser Phase zu durchbrechen, sind die folgenden XDR-Funktionen erforderlich:

- Schwachstellen- und Patch-Management
- Malware-Erkennung und -Prävention
- Nutzung von Bedrohungsdaten (einschließlich bekannter und unbekannter Bedrohungen)
- Blockieren riskanter, nicht autorisierter oder nicht benötigter Anwendungen und Services
- Protokollierung und Überwachung aller Netzwerk-, Endpunkt- und Cloud-Aktivitäten

TECHNISCHES

Ein effektiver XDR-Agent verhindert bekannte, nicht gepatchte und Zero-Day-Schwachstellen, indem er Exploitation-Techniken blockiert, die Angreifer zur Manipulation von Anwendungen nutzen. Es gibt zwar Tausende von Exploits, doch Angreifer setzen normalerweise nur auf wenige Exploitation-Techniken, die sich nur selten ändern. Eine XDR-Lösung kann diese abwehren und verhindert Ausnutzungsversuche, bevor Endpunkte kompromittiert werden (siehe Abbildung 3-2).

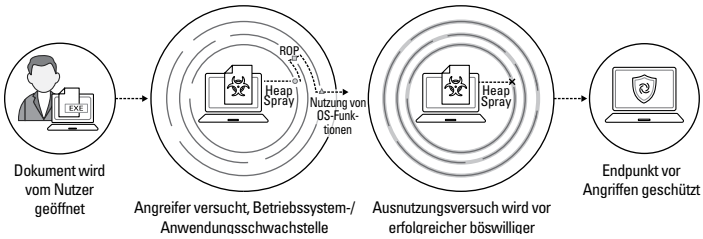


**ABBILDUNG 3-2:** Eine fortschrittliche XDR-Lösung konzentriert sich auf Methoden und Verhaltensweisen und nicht auf die Exploits selbst.

## Installation

Als Nächstes erweitert ein Angreifer seine Zugriffsberechtigungen auf dem kompromittierten Endpunkt (z. B., indem er den Zugriff auf Remote-Shells herstellt und Rootkits oder andere Malware installiert). Mit Zugriff auf Remote-Shells hat der Angreifer die Kontrolle über den Endpunkt und kann im privilegierten Modus über eine Befehlszeilenschnittstelle (CLI) Befehle ausführen, als säße er selbst vor dem Endgerät. Der Angreifer bewegt sich dann lateral durch das Netzwerk des Angriffsziels, führt Angriffscode aus, identifiziert andere sich anbietende Ziele und kompromittiert weitere Endpunkte, um sich dort längerfristig einzunisten.

Zur Unterbrechung des Angriffslebenszyklus ist es in dieser Phase entscheidend, die Installation auf dem Endpunkt zu verhindern und die laterale Bewegung der Angreifer im Netzwerk einzuschränken. Zur Verhinderung der Installation nutzen XDR-Lösungen EDR- (Endpoint Detection and Response) und EPP-Technologien (Endpoint Protection Platform). Die XDR-Lösung überwacht und prüft auch den gesamten Datenverkehr zwischen Zonen oder Segmenten in einem Zero-Trust-Modell und bietet eine granulare Kontrolle der Anwendungen, die in der Umgebung zugelassen sind.

## Command and Control

Bedrohungsakteure richten über das Internet verschlüsselte Kommunikationskanäle ein, die den Datenverkehr zurück zu ihren Command-and-Control-Servern führen. Dies gibt ihnen die Möglichkeit, ihre Angriffsziele und -methoden zu ändern, wenn im Netzwerk des Opfers weitere Angriffsziele erkannt werden. Außerdem können sie neue Sicherheitsmaßnahmen umgehen, die das Unternehmen nach der Entdeckung der Angriffsartefakte einsetzt. Kommunikation ist für einen Angriff unerlässlich, denn nur so kann der Angreifer den Angriff aus der Ferne steuern und seine Angriffsziele umsetzen. Der Command-and-Control-Datenverkehr muss stabil und unauffällig sein, damit der Angriff erfolgreich ist.

Um den Angriffslebenszyklus in dieser Phase zu durchbrechen, sind folgende Maßnahmen erforderlich:

- Untersuchung des gesamten Netzwerkverkehrs (einschließlich verschlüsselter Kommunikation)
- Blockierung des ausgehenden Command-and-Control-Kommunikationsdatenverkehrs mithilfe von Signaturen (zusammen mit Uploads von Dateien und Datenmustern), die Command and Control entgegenwirken

- Blockierung der gesamten ausgehenden Kommunikationsdatenverkehrs zu bekannten bösartigen URLs (Uniform Resource Locators) und IP-Adressen
- Abwehr neuartiger Angriffsmethoden, bei denen Portumgehungsmethoden zum Einsatz kommen
- Verhinderung der Verwendung von Anonymisierern und Proxys im Netzwerk
- Überwachung des Domain Name Systems (DNS) auf bösartige Domänen und Einsatz von Abwehrmaßnahmen wie DNS-Sinkholing oder DNS-Cache-Poisoning
- Umleitung des schädlichen ausgehenden Kommunikationsdatenverkehrs zu Honeypots, um gefährdete Endpunkte zu identifizieren oder zu blockieren und den Angriffsdatenverkehr zu analysieren

### Lateral Movement und Exfiltration

Angreifer verfolgen oft mehrere unterschiedliche Ziele, darunter Datendiebstahl, die Zerstörung oder Veränderung kritischer Systeme, Netzwerke und Daten sowie DoS-Angriffe (Denial of Service). Diese letzte Phase des Angriffslebenszyklus kann von Angreifern auch genutzt werden, um die frühen Phasen des Angriffs gegen ein anderes Ziel zu richten. Ein Angreifer kann zum Beispiel das Extranet eines Unternehmens kompromittieren, um einen Geschäftspartner anzugreifen, der das Hauptziel ist. Diese Art von Angriffen auf die Lieferkette sorgte 2020 mit dem SolarWinds-Angriff für Schlagzeilen.

Um den Angriffslebenszyklus in dieser Phase zu durchbrechen, sind XDR-Tools erforderlich, die die Datenexfiltration und andere böswillige oder unbefugte Handlungen automatisch erkennen und verhindern können.

## Ein Beispiel für einen Angriff

Um alle Schritte des Angriffslebenszyklus und ihre Rolle bei einem Angriff zu veranschaulichen, wollen wir uns nun einen hypothetischen Angriff genauer ansehen. In Abbildung 3-3 unternimmt ein Bedrohungsakteur die folgenden Schritte, um ein Ziel anzugreifen:

1. Exploitation.

   Der Angreifer nutzt Fehler auf dem Webserver aus, um die Kontrolle über den Server zu übernehmen.

2. Installation.

   Der Angreifer nutzt die Kontrolle über den Server, um Mimikatz zu installieren und Zugang zu den Admin-Anmeldedaten zu erhalten.

3. Command and Control.

   Der Angreifer installiert zusätzliche Malware und Fernzugriffstools, um sich dauerhaft einzunisten und einen Command-and-Control-Kommunikationsdatenverkehr herzustellen.

4. Lateral Movement.

   Der Angreifer bewegt sich lateral durch das Netzwerk, kompromittiert mehrere Endpunkte und greift auf Private- und Public-Cloud-Anwendungen zu.

5. Zugriff und Exfiltration.

   Der Angreifer sieht sich die Konfigurationsdateien auf dem Server an, findet den Speicherort der Backend-Datenbank, fragt die Datenbank ab und speichert die Ergebnisse in einer lokalen Datei. Die erfassten Daten werden auf einen „autorisierten" oder „sanktionierten" Cloud-Speicher hochgeladen. Anschließend löscht der Angreifer die Datei mit den Daten aus der Datenbank, leert die lokalen Protokolle und beendet die Sitzung.

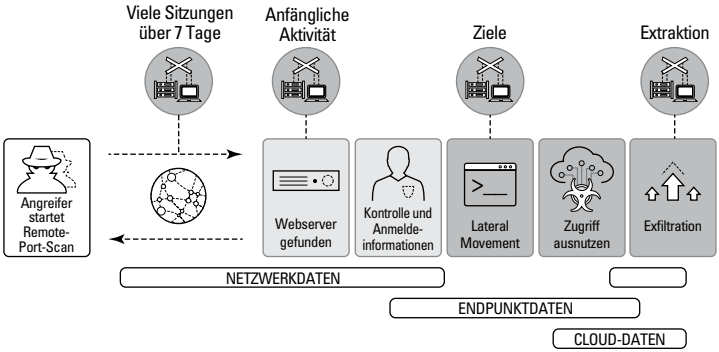


**ABBILDUNG 3-3:** Eine XDR-Lösung kann diese fortschrittlichen, mehrstufigen Angriffe auf einzigartige Weise stoppen, da sie Daten aus jeder Quelle sammelt und Angriffstaktiken erkennen und stoppen kann, die anderen Tools entgehen.

Eine XDR-Plattform erfasst und analysiert mehrere Arten von Daten, um die Methoden der Angreifer während des gesamten Angriffslebenszyklus zu erkennen und abzuwehren.

IN DIESEM KAPITEL

- Erkennung von Bedrohungsaktivitäten mit XDR
- Verwaltung und Validierung von Warnmeldungen
- Beschleunigung von Untersuchungen und Abwehrmaßnahmen
- Proaktive Bedrohungssuche

# Kapitel 4
# Anwendungsfälle für XDR

In diesem Kapitel werden wir uns die häufigsten Anwendungsfälle für XDR ansehen, mit denen Ihr Unternehmen seine Erkennungs- und Reaktionsfähigkeiten verbessern kann, einschließlich Erkennung, Alarmtriage und -validierung, Automatisierung von Untersuchungen und Abwehrmaßnahmen sowie proaktive Bedrohungssuche.

## Erkennung

Um Cyberangriffe erfolgreich abzuwehren, müssen Sie in der Lage sein, Angriffe in jeder Phase des Angriffslebenszyklus zu erkennen. Extended Detection and Response (XDR) nutzt maschinelles Lernen, um die besonderen Merkmale Ihres Unternehmens zu ermitteln und zwischen Angriffsaktivitäten und normalen Aktivitäten zu unterscheiden, was in diesem Maße mit manueller Analyse oder statischen Korrelationsregeln nicht möglich ist. Maschinelles Lernen dient als Grundlage für erweiterte Analysen, die Erstellung von Profilen und eine verhaltensbasierte Bedrohungserkennung. Aufgrund dieser umfassenden Erkennungsfunktionen sind Unternehmen mit einer XDR-Lösung besser in der Lage, kriminelle Aktivitäten wie gezielte Angriffe oder böswillige Insider zu erkennen.

### Gezielte Angriffe

Die meisten Angreifer versuchen, in jeder Phase des Angriffslebenszyklus ihre eigenen Aktivitäten neben den legitimen zu tarnen. Da XDR in der Lage ist, Daten aus jeder beliebigen Quelle für die Bedrohungserkennung zu erfassen und automatisch wichtige Sicherheitsdaten für erweiterte datenübergreifende Analysen miteinander zu verknüpfen, können auch die am besten getarnten Angriffe schnell erkannt werden. Mithilfe von Analysen können Sie ein Profil des Benutzerverhaltens erstellen, um abweichendes Verhalten zu erkennen, z. B. wenn ein

Angreifer versucht, Geräte zu kompromittieren und sich lateral durch das Netzwerk zu bewegen, um nach vertraulichen Daten zu suchen und diese auszuschleusen.

## Böswillige Insider

Mitunter missbrauchen Insider ihre autorisierten Anmeldedaten, um unerkannt Unternehmensdaten zu stehlen. XDR-Technologie begegnet dieser Bedrohung, indem sie nach Änderungen in Nutzerverhaltensweisen und -aktivitäten sucht (siehe Abbildung 4-1). XDR-Lösungen können Analysen rationalisieren, indem sie eine umfassende Ansicht jedes Benutzers mit einer klaren Risikobewertung präsentieren.

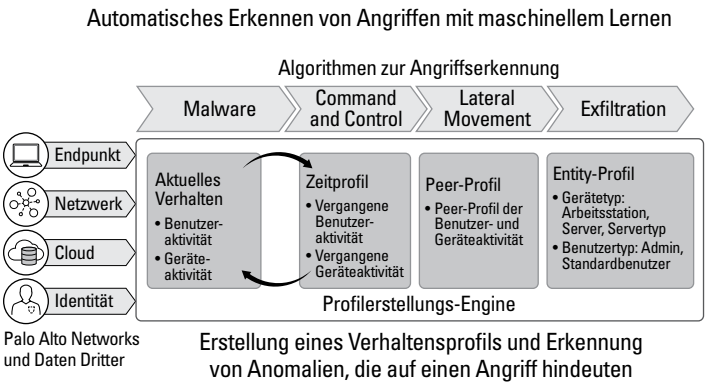


**ABBILDUNG 4-1:** Durch Verhaltensanalysen werden Anomalien auf Benutzer-, Anwendungs- und Geräteebene erkannt.

## Unbeabsichtigte Risiken

Auch ehrliche Mitarbeiter können ein Unternehmen durch den Missbrauch von Zugriffsberechtigungen ungewollt einem unnötigen Risiko aussetzen. Mit einer XDR-Lösung können Unternehmen Best Practices für Sicherheit befolgen, indem sie Benutzeraktivitäten überwachen und riskantes Verhalten identifizieren. So können sie erkennen, wenn Mitarbeiter Sicherheitsrichtlinien (absichtlich oder versehentlich) verletzen.

## Kompromittierte Endpunkte

Häufig nutzen Angreifer Malware, um sich Zugang zu einem Zielnetzwerk zu verschaffen, indem sie einen Endpunkt kompromittieren und sich von dort aus lateral im Netzwerk auszubreiten. XDR führt Sicherheitsdaten aus mehreren Netzwerken und Endpunkten zusammen, um von der Norm abweichenden Datenverkehr zu identifizieren, der durch Malware oder andere schädliche Aktivitäten generiert wird. Anhand dieser Sicherheitsdaten kann auch die ganze Infrastruktur untersucht werden, um das Ausmaß eines Angriffs zu ermitteln.

Wenn beispielsweise ein Bedrohungsakteur einen neuen Wert zum Autorun-Registrierungsschlüssel hinzufügt, kann eine XDR-Lösung den neuen Autorun-Wert erkennen und eine Warnung mit einer klaren

Beschreibung der verdächtigen Aktivität erzeugen, die dank MITRE ATT&CK-Taktiken und -Techniken umfassenden Kontext beinhaltet. Die XDR-Lösung kann nicht nur bestimmen, welcher Prozess den Autorun-Wert hinzugefügt hat, sondern auch die Abfolge der Ereignisse, die zu der Aktualisierung geführt haben. Auf diese Weise kann der Verlauf des Angriffs vollständig abgebildet werden.

WICHTIG

XDR-Technologie erkennt aktive Angriffe mit beispielloser Präzision und ermöglicht Sicherheitsteams Folgendes:

- bösartige Aktivitäten in internen und externen Ressourcen zu erkennen, indem Muster bei Aktivitäten im Netzwerk, an Endpunkten und in der Cloud erkannt werden
- große Mengen an Sicherheitsdaten mit modernsten Verfahren analysieren, um abweichende Verhaltensmuster zu erkennen, ohne zusätzliche Fehlalarme zu generieren
- die Leistung des gesamten Sicherheitsteams zu verbessern, indem interne Reaktionsmaßnahmen und externe Bedrohungsdaten genutzt werden, um aus früheren Angriffen zu lernen und die daraus gewonnenen Erkenntnisse weniger erfahrenen Analysten zugänglich zu machen

## Triage und Untersuchung

XDR vereinfacht die Triage und Analyse von Warnmeldungen, da die Lösung die Bedrohungsursache ermittelt und dadurch den Untersuchungsprozess deutlich beschleunigt. Wenn nur Endpunktdaten verfügbar sind, wird die Bedrohungsursache für den Endpunkt angezeigt. Wenn sowohl Netzwerk- als auch Endpunktdaten vorliegen, kann die XDR-Plattform Netzwerkaktivitäten automatisch mit Endpunktereignissen in Verbindung bringen. So erkennt XDR beispielsweise nicht nur, welche ausführbare Datei auf einem Endpunkt die Warnmeldung ausgelöst hat, sondern auch, von welcher Anwendung diese gestartet wurde.

In Kapitel 1 haben wir gesehen, welche Herausforderungen der Fachkräftemangel im Cybersicherheitsbereich mit sich bringen kann. Dank XDR sind auch weniger erfahrene Analysten in der Lage, potenzielle Angriffe zu erkennen und zu validieren. Denn sie können Warnmeldungen zu Vorfällen gruppieren und Aktivitäten oder Aktionen innerhalb dieser Vorfälle zu Tags zusammenfassen, die mehr Kontext liefern. Durch diese Flexibilität wird sichergestellt, dass Erkenntnisse festgehalten und vom gesamten Team genutzt werden können.

XDR-Technologie rekonstruiert den Ablauf der Ereignisse, die zur Warnmeldung geführt haben, und stellt integrierte Bedrohungsdaten zur Verfügung. All das hilft den Analysten, die Grundursache der Warnmeldung, die genaue Art der Bedrohung und die notwendigen Gegenmaßnahmen zu bestimmen.

So hilft XDR bei der Vereinfachung der Analyse und Untersuchung von Vorfällen:

1. Bewertung.

   Zunächst beurteilt die XDR-Lösung extern (z. B. von Sicherheitstools von Drittanbietern) und intern generierte Warnmeldungen (aufgrund von Regeln und anderen Indikatoren), um potenziell verdächtiges Verhalten zu identifizieren.

2. Priorisierung.

   Das XDR-Tool gruppiert diese Warnmeldungen dann automatisch in Vorfälle und weist jedem Vorfall eine Prioritätsstufe zu, damit sich Analysten auf die Fälle konzentrieren können, welche die größte Bedrohung darstellen. Analysten können auf jeden Vorfall klicken, um eine vollständige Liste der Warnmeldungen, Geräte, relevanten Bedrohungsdaten und Kontextinformationen zu sehen und sich ein umfassendes Bild zu machen.

3. Analyse.

   XDR visualisiert die Angriffskette (siehe Abbildung 4-2), trägt aus verschiedenen Telemetriequellen alle für den Vorfall relevanten Informationen zusammen und stellt zusätzlichen Kontext und Kausalzusammenhänge für eine schnellere und bessere Analyse zur Verfügung. Die Angriffskette zeigt die Schritte, die ein Angreifer unternommen hat, und deckt die Abfolge der Prozesse auf, die zum letzten Angriffsschritt geführt haben. Dabei stellt sie nicht nur die zugehörigen Warnmeldungen einschließlich einer EPP-Warnung für den XDR-Agenten dar, sondern ermittelt auch die Grundursache.

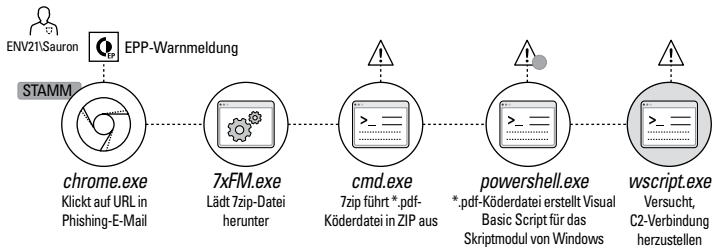


**ABBILDUNG 4-2:** Beispiel für eine mit XDR-Technologie visualisierte Angriffskette

4. Anreicherung.

   Die Angriffskette wird dann mit weiteren Kontextinformationen angereichert, die Folgendes beinhaltet: eine schrittweise Darstellung der Ereignisse, die zur Ausgabe der Warnmeldung geführt haben; ihre Grundursache, andere betroffene Endpunkte, Netzwerk- und Cloud-Geräte und Angaben zur Zuverlässigkeit aller forensischen Artefakte.

Da täglich Tausende von Warnmeldungen eingehen, hilft nur ein automatisierter Triageprozess und die Bereitstellung von umfassenden Kontextinformationen Analysten dabei, dieses Volumen an Meldungen zu handhaben. Mit XDR können Sicherheitsteams ihre Zeit und Energie dort investieren, wo sie am meisten nützt: bei der Reaktion auf die gefährlichsten Angriffe, die den größten Schaden anrichten könnten.

WICHTIG

Mit XDR können Analysten:

- durch Vorfallmanagement, intelligente Gruppierung von Warnmeldungen und Untersuchungskontext den Rückstand bei der Bearbeitung von Warnmeldungen besser verringern;
- die Wahrscheinlichkeit drastisch reduzieren, dass ein Angriff nicht bemerkt wird;
- Alarme analysieren, um die Bedrohungserkennung zu verbessern und sicherzustellen, dass die nachgelagerte Produktivität und die Abwehrmaßnahmen nicht beeinträchtigt werden;
- neue verhaltensbasierte Auslöser anwenden, um die Triagezeiten zu verkürzen und Erkennungsregeln optional in Präventionsregeln umzuwandeln (Closed-Loop-Prävention).

## Automatisierte und vereinfachte Untersuchungen und Abwehrmaßnahmen

Nachdem eine Warnmeldung als berechtigt eingestuft und priorisiert wurde, ist eine genauere Untersuchung angezeigt. Die Automatisierung von XDR-Technologie beschleunigt die Untersuchung von Warnmeldungen und Bedrohungssuchkampagnen. Sie eliminiert zeitaufwendige manuelle Aufgaben, indem sie ein klares Bild der Bedrohung liefert, eine Ursachenanalyse durchführt, die Zuverlässigkeit der Anhaltspunkte prüft und die Identität der Angreifer ermittelt.

XDR-Tools aggregieren zunächst alle Telemetriedaten in einem Repository für Sicherheitsdaten, wie beispielsweise einem Data Lake (siehe Abbildung 4-3). Um die Untersuchungszeit zu verkürzen, kann die XDR-Lösung Warnmeldungen von unterschiedlichen Erkennungstools korrelieren und zu einer kleineren Anzahl genauer Vorfälle zusammenfassen, die einer Aktion bedürfen. Diese enthalten Informationen über den Benutzer, die Anwendung und das Gerät. XDR-Technologie kann zudem forensische Untersuchungen unterstützen, indem sie Endpunkte abfragt und ermittelt, von welchem Prozess oder welcher ausführbaren Datei ein Angriff ausging.

Zur weiteren Untersuchung des Vorfalls überprüft die XDR-Lösung, ob der Endpunktprozess schädlich ist. Sie nutzt die Integration in Bedrohungsdatenquellen und -services, um den Prozess zu analysieren. Die

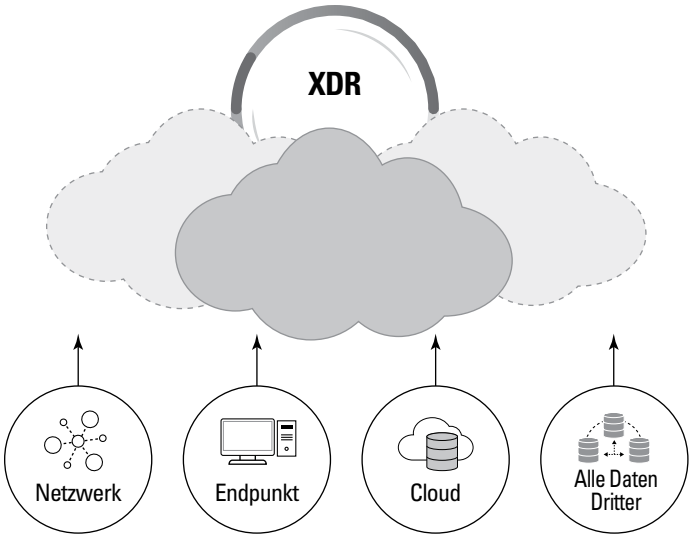


**ABBILDUNG 4-3:** XDR-Tools verknüpfen Daten von unterschiedlichen Sensoren in einem cloudbasierten Datenrepository.

Arbeit der Sicherheitsanalysten ist mit einer XDR-Lösung erheblich einfacher, da 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, sodass einmal gefundene Bedrohungen beim erneuten Auftreten automatisch abgewehrt werden. Dieses „unterstützte Lernen" ermöglicht eine frühzeitige Erkennung von Angriffen auf der Grundlage bekannter Ereignisse in der jeweiligen Umgebung.

Nach der Validierung stehen den Vorfallverantwortlichen Dutzende Remoteantwort- und Behebungsmethoden zur Verfügung, um unter anderem Angriffe zu stoppen, Folgeangriffe zu verhindern und beschädigte oder gelöschte Dateien wiederherzustellen. Zu den Reaktionsmöglichkeiten gehören das Isolieren von Endpunkten, das Blockieren, Löschen oder Quarantänisieren von Dateien, das Zurücksetzen von Dateien und der Registry auf einen bereinigten Zustand, der direkte Zugriff auf Endpunkte und das Ausführen von Skripten. Die Mitglieder des Sicherheitsteams werden wesentlich effizienter, benötigen weniger Schulungen, entlasten die höher qualifizierten Mitarbeiter und beheben Vorfälle schneller.

WICHTIG

Mit XDR können Incident-Response-Experten:

- Bedrohungsdaten und Verhaltensanalysen nutzen, um getarnte Bedrohungen schneller aufzudecken;
- Telemetriedaten aus Netzwerken, von Endpunkten und der Cloud mithilfe leistungsstarker Funktionen durchsuchen, um die Untersuchung und Behebung von Vorfällen zu vereinfachen und zu beschleunigen.

## Bedrohungssuche

XDR-Lösungen verbessern Ihre Bedrohungssuche, da sie sowohl automatisierte als auch spontane Suchen nach verdächtigen Aktivitäten in Ihrer Umgebung unterstützen. Die zuständigen Mitarbeiter können komplexe Abfragen durchführen und sofort die benötigten Antworten erhalten. Im Folgenden finden Sie einige Beispielmethoden für die Bedrohungssuche, die durch XDR-Technologie unterstützt werden:

- **Informationsbasierte Bedrohungssuche:** Dies ist die häufigste Art der Bedrohungssuche, bei der ein Threat Hunter Hinweise auf eine aktuelle Bedrohung erhalten hat, bevor er sich danach auf die Suche begibt. Bei diesen kann es sich zum Beispiel um eine Information aus einer Bedrohungsdatenbank, einen kürzlich bekannt gewordenen Indicator of Compromise (IOC), einen Tipp von jemandem aus dem Unternehmen oder einfach nur um einen Verdacht handeln. Wie kompliziert die Suche wird, hängt davon ab, wie detailliert diese Informationen sind. XDR-Lösungen greifen auf integrierte Datenquellen zu, die mit mehreren Anbietern von Bedrohungsdaten verlinkt sind. Sie können manuell Artefakte oder IOCs unterschiedlicher Standards importieren und so schnelle und zuverlässige Suchergebnisse liefern.
- **Indizienlose Bedrohungssuche:** Fast genauso häufig suchen Fachleute auch ohne spezifische Anhaltspunkte nach Bedrohungen. Dabei stützen sie sich auf ihre eigenen fundierten Kenntnisse darüber, wie Benutzer Computer, Anwendungen, Daten oder Netzwerke nutzen sollten, und ermitteln auf dieser Basis davon abweichende oder anormale Verwendungen. Für diese fortgeschrittene Bedrohungssuche sind meist die erfahrensten Teammitglieder zuständig, die Techniken wie File Carving und Analysen einsetzen, um Ergebnisse zu erzielen. Eine XDR-Lösung vereinfacht diesen Prozess, da fortschrittliche Funktionen in ihre Schnittstelle integriert sind. So können auch weniger erfahrene Threat Hunters diese Techniken nutzen, ohne Skripte oder zusätzliche Tools einsetzen oder neue Abfragesprachen erlernen zu müssen.
- **Ergebnisbasierte Bedrohungssuche:** Bei diesem Ansatz betrachtet der Hunter ältere Warnmeldungen, die zur Quarantäne geführt

haben, abgeschlossene Untersuchungen oder andere abgewehrte Bedrohungen, um Varianten derselben Bedrohung, potenzielle neue Bedrohungen oder offene Angriffsvektoren zu finden. Eine hochwertige XDR-Lösung kann die ergebnisbasierte Bedrohungssuche automatisch und kontinuierlich direkt in den Workflow für Sicherheitswarnungen und die Bearbeitung von Vorfällen integrieren. Die Erkenntnisse aus den einzelnen Untersuchungen werden dann angewendet, um sicherzustellen, dass Sie von wiederholten Angriffen verschont bleiben.

- **Compliance-basierte Bedrohungssuche:** Mit dieser Art der Bedrohungssuche soll sichergestellt werden, dass unternehmensinterne, branchenübliche und gesetzliche Vorgaben hinsichtlich der Datensicherheit eingehalten werden. Dazu werden routinemäßige Suchen auf nichtkonformes Verhalten durchgeführt, etwa nach vertraulichen Daten, die auf nicht autorisierten Systemen gespeichert sind, oder nach Hinweisen darauf, dass Administratoren Zugriffsprivilegien ausweiten. Eine XDR-Lösung kann so konfiguriert werden, dass sie Sicherheitsanalysten kontinuierlich auf derartige Aktivitäten aufmerksam macht, damit sie zeitnah untersucht und unterbunden werden können.
- **ML-basierte Bedrohungssuche:** ML-basierte Systeme erstellen eine Baseline für das typische Verhalten eines Unternehmens, um nachvollziehen zu können, was normal ist und was nicht. XDR-Lösungen nutzen maschinelles Lernen, um Verhaltensmuster zu überwachen und Abweichungen von der Baseline zu identifizieren. Mithilfe dieser Behavioral Indicators of Compromise (BIOCs) können viele gut getarnte Angriffe erkannt werden, die Analysten eventuell nicht manuell identifizieren können. Sie werden im Laufe der Zeit kontinuierlich optimiert, um das ML-Modell zu verbessern. Diese Form der Bedrohungssuche bringt dem Analystenteam die größte Zeitersparnis und ist für die Verbesserung des Sicherheitsniveaus unverzichtbar.

WICHTIG

Mit XDR können Threat Hunters:

- Daten aus dem Netzwerk, von den Endpunkten und aus der Cloud für Suchen und Analysen nutzen;
- Automatisierung für die Untersuchung aller Aktivitäten im Netzwerk, auf den Endpunkten und in der Cloud verwenden;
- mit hochgradig konfigurierbaren Suchfunktionen und maschinellen Assistenten in Ihrer Bedrohungsbibliothek nach IOCs und BIOCs suchen, die auf interne oder externe Bedrohungen hindeuten;
- Angriffe durch die Integration verschiedener Sicherheitsmaßnahmen beheben.

**IN DIESEM KAPITEL**

- **Gewährleistung einer robusten Bedrohungsabwehr und vollständiger Transparenz**
- **Vereinfachung von Untersuchungen durch Analysen, maschinelles Lernen, koordinierte Abwehrmaßnahmen und Orchestrierungsfunktionen**
- **Maximierung der Flexibilität durch eine komplette Schutzlösung**
- **Validierung durch Dritte, innovative Roadmaps und Gesamtwert**

Kapitel **5**

# Zehn entscheidende Funktionen und Merkmale einer XDR-Lösung

Mit Extended Detection and Response (XDR) können Unternehmen Cyberangriffe erfolgreich verhindern und ihre Sicherheitsprozesse durch einen proaktiven Ansatz zur Erkennung und Abwehr von Bedrohungen vereinfachen und stärken. XDR-Technologie wehrt moderne Angriffe ab, indem sie Daten aus den verschiedensten Quellen erfasst und analysiert. Die Lösung vereint Funktionen zur Prävention, Erkennung, Untersuchung und Abwehr von Bedrohungen und sorgt für beispiellose Sicherheit und betriebliche Effizienz.

In diesem Kapitel werden wir zehn wichtige Funktionen und Merkmale einer XDR-Lösung für Ihr Unternehmen betrachten. Außerdem werden wir erläutern, wie Cortex XDR, die erste Extended-Detection-and-Response-Plattform der Branche, diese wesentlichen Funktionen bereitstellt.

# Erstklassiger Schutz vor Endpunktbedrohungen

Der Schutz Ihres Unternehmens beginnt mit einem erstklassigen Schutz vor Endpunktbedrohungen, um bekannte und unbekannte Malware, Ransomware, dateilose Angriffe und Exploits abzuwehren.

WICHTIG

Cortex XDR bietet mittels eines einzelnen in der Cloud verwalteten Agenten alle Funktionen, die Sie für die Prävention, Erkennung und Reaktion auf Bedrohungen benötigen. Die Lösung schützt Ihre Endpunkte durch branchenführende, auf künstlicher Intelligenz (KI) basierende Analysen und verhaltensbasierte Sicherheitsmaßnahmen (siehe Abbildung 5-1).

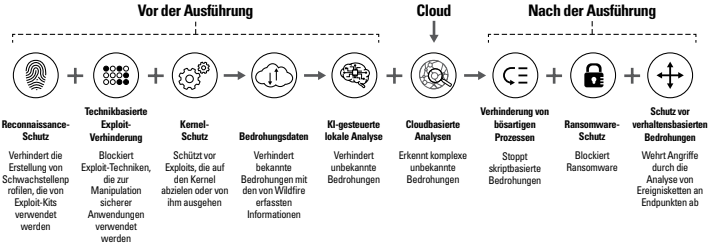


**ABBILDUNG 5-1:** Cortex XDR bietet umfassenden Schutz vor Endpunktbedrohungen.

Halten Sie nach Antivirenschutz der nächsten Generation Ausschau, der Folgendes bietet:

- Schutz vor Malware, Ransomware und dateilosen Angriffen
- cloudbasierte globale Bedrohungsdaten in Echtzeit
- lokale Analysen durch maschinelles Lernen
- verhaltensbasierte Bedrohungsabwehr
- granularer Schutz von untergeordneten Prozessen
- früh greifende und methodenbasierte Schutzmaßnahmen zur Verhinderung von Exploits
- Schutz vor Kernel-Exploits
- Schutz gegen Diebstahl von Anmeldeinformationen

## Flexible Suite mit Endpunktschutzfunktionen

Sie benötigen eine einfache Methode, um Endpunktrisiken zu identifizieren und zu priorisieren, Ihre Angriffsfläche zu reduzieren und Datenverluste zu verhindern. Achten Sie auf die folgenden Endpunktschutzfunktionen:

- **Schwachstellenbewertung:** Nutzen Sie Schwachstellenbewertung, Anwendungstransparenz über verwaltete und nicht verwaltete Endpunkte und vieles mehr, um einen unternehmensweiten Überblick über Ihre digitalen Ressourcen zu erhalten.
- **Hostbasierte Firewall:** Mit der Managementkonsole von Cortex XDR kann der ein- und ausgehende Kommunikationsdatenverkehr auf Ihren Endpunkten zentral verwaltet werden.
- **Festplattenverschlüsselung:** Cortex XDR ermöglicht die Anwendung von Verschlüsselungs- oder Entschlüsselungsrichtlinien auf Ihren Endpunkten und die Anzeige von Listen aller verschlüsselten Laufwerke.
- **Gerätesteuerung:** Cortex XDR bietet Funktionen zur Überwachung und granularen Steuerung des USB-Zugriffs (Universal Serial Bus) zum Schutz Ihrer Endgeräte.

## Transparente Einblicke in alle Datenquellen

Um das Risiko eines erfolgreichen Angriffs zu verringern, benötigen Sie einen ganzheitlichen Ansatz für die Bedrohungserkennung und -abwehr, der Schwachpunkte beseitigt, die Genauigkeit erhöht und die Untersuchungen in allen Umgebungen, einschließlich Netzwerk, Cloud und Endpunkt, rationalisiert.

TIPP

Cortex XDR ist die branchenweit erste XDR-Plattform, die Endpunkt-, Netzwerk- und Cloud-Daten nativ integriert, um komplexe Angriffe abzuwehren. Cortex XDR bietet sämtliche NDR- (Network Detection and Response), EDR- (Endpoint Detection and Response), EPP- (Endpoint Protection Platform), CDR- (Cloud Detection and Response) und UEBA-Funktionen (User and Entity Behavior Analytics) wie in Abbildung 5-2 dargestellt.

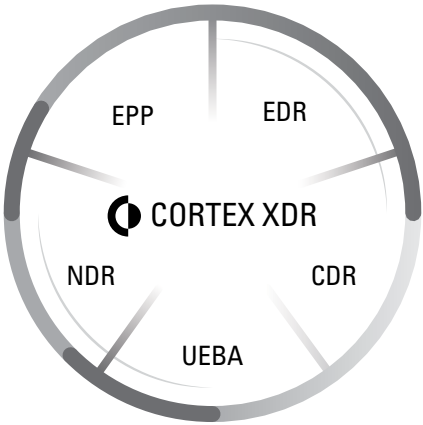


**ABBILDUNG 5-2:** Cortex XDR erfasst und analysiert aussagekräftige Daten und bietet die Funktionen, die traditionell von EPP-, EDR-, NDR-, CDR- und UEBA-Tools bereitgestellt werden.

# Vereinfachte Untersuchungen

Die isolierten Sicherheitstools von heute generieren unzählige Warnmeldungen mit begrenztem Kontext. Laut dem Bericht *Cost of a Data Breach* des Ponemon Institute aus dem Jahr 2020 dauert es im Durchschnitt 280 Tage, bis eine Sicherheitsverletzung erkannt und eingedämmt wird. Um die Reaktionszeiten zu verkürzen, müssen Sicherheitstools ein vollständiges Bild von Vorfällen mit aussagekräftigen Details liefern.

TIPP

Cortex XDR vereinfacht Untersuchungen durch die automatische Aufdeckung der Grundursachen, Ereignisfolgen und Bedrohungsdatendetails in Warnmeldungen. Die Lösung verkürzt die Untersuchungszeit um 88 Prozent, indem sie die Ursache und den umfassenden Kontext von Netzwerk-, Endpunkt- und Cloud-Warnmeldungen aufdeckt. Zudem reduziert sie die Anzahl der Warnmeldungen durch intelligente Gruppierung und Deduplizierung um 98 Prozent.

# Analytik und maschinelles Lernen

Bedrohungsakteure nutzen Cloud- und ML-Technologien, um die Reichweite und Effektivität ihrer Angriffe zu erhöhen. Sie benötigen daher umfassende Machine-Learning- und Analysetechniken, um den sich schnell entwickelnden Bedrohungen einen Schritt voraus zu sein und ausgeklügelte Angriffe abzuwehren.

WICHTIG

Cortex XDR bietet Folgendes:

- KI-gesteuerte lokale Analysen zur Abwehr von Malware
- Verhaltensanalysen zur Erkennung von Eindringversuchen und aktiven Angriffen
- globale Analysen zur Verbesserung der Erkennungsgenauigkeit und -reichweite

## Koordinierte Bedrohungsabwehr

Nachdem Sie Bedrohungen in Ihrer Umgebung erkannt haben, müssen Sie diese schnell eindämmen können. Ihr Team benötigt integrierte und flexible Abwehrmöglichkeiten, um Angriffe schnell und effektiv zu stoppen, bevor sie weiteren Schaden anrichten können. Eine XDR-Lösung muss Ihr Team in die Lage versetzen, die Ausbreitung von Malware aus der Ferne zu verhindern, den Netzwerkdatenverkehr von und zu Geräten einzuschränken und die Bedrohungsabwehrlisten, z. B. zu bösartigen Domänen, durch die enge Integration in Durchsetzungspunkten zu aktualisieren.

TIPP

Mit Cortex XDR kann Ihr Sicherheitsteam Bedrohungen im Netzwerk, auf Endpunkten und in der Cloud sofort über eine einzige Konsole beseitigen.

## Automatisierung von Sicherheitsaufgaben

Manuelle Aufgaben und Prozesse verlangsamen die Reaktion auf Sicherheitsvorfälle und erhöhen die Kosten für Sicherheitsmaßnahmen. XDR-Lösungen können Bedrohungen schnell eindämmen, indem sie eine Reihe von Abwehrmaßnahmen nativ auf dem Endpunkt und an anderen wichtigen Durchsetzungspunkten durchführen. Fortschrittliche SOCs benötigen eventuell Prozesse, die Entscheidungslogik und Workflow-Orchestrierung beinhalten, die durch Playbooks gesteuert werden, und diverse Maßnahmen für zahlreiche Sicherheits- und IT-Tools verschiedener Anbieter umfassen. Eine vollständige Sicherheitsautomatisierungs- und Orchestrierungslösung, die Orchestrierungslogik bietet und über umfangreiche Partnerintegrationen sowie vorgefertigte Inhalte und Playbooks verfügt, kann diese Anforderungen erfüllen. Halten Sie daher nach einer XDR-Lösung Ausschau, die eng in eine branchenführende SOAR-Plattform integriert ist.

WICHTIG

Cortex XDR lässt sich nahtlos in Cortex XSOAR integrieren und ermöglicht die umfassende Verwaltung von Bedrohungsdaten. Die Lösung bietet über 750 Partnerintegrationen und 680 Inhaltspakete, damit Sie das Niveau Ihrer Sicherheitsabläufe anheben können.

## Unabhängige Prüfung und Validierung

Für die Auswahl einer XDR-Lösung sollten Sie immer Tests von Drittanbietern, Analystenmeinungen und Kundenbewertungen prüfen, um eine unabhängige und objektive Perspektive zu erhalten.

TIPP

Cortex XDR hat hervorragende Testergebnisse erzielt. Die Lösung wurde in Runde 3 der MITRE ATT&CK-Evaluierung als die beste Kombination für Bedrohungserkennung und -schutz eingestuft und erhielt beim EPR-Test (Endpoint Prevention and Response) von AV-Comparatives die Bewertung „Strategic Leader". Cortex XDR wird von Kunden und Prüfern gleichermaßen gelobt. Sie können sich also darauf verlassen, dass Ihre Endpunkte und Daten optimal geschützt werden.

## Schnelles Innovationstempo

Um mit agilen Angreifern schritthalten zu können, sollten Sie nach Anbietern Ausschau halten, die die Funktionen ihrer Produkte kontinuierlich verbessern oder erweitern.

TIPP

Die Art und Weise, wie SecOps-Teams mit komplexen modernen Bedrohungen umgehen und ihre Effizienz steigern, wird von Cortex XDR kontinuierlich neu definiert. XDR löst das Problem der Systemintegration für die Erfassung, Integration und Analyse von Daten und verbindet dies mit der Fähigkeit, hochgradig optimierte und automatisierte Workflows in Gang zu setzen. Auf diese Weise hilft XDR dabei, die Herausforderungen bei der Erkennung, Untersuchung und Abwehr von Bedrohungen skalierbar und auf konsolidierte Weise zu bewältigen.

## Konkurrenzlose Anlagenrendite

Bei der Auswahl eines wichtigen Bestandteils Ihrer Sicherheitsinfrastruktur sollten Sie sicherstellen, dass die Anschaffung einen echten Mehrwert bietet, der sich gegenüber Ihren Stakeholdern leicht nachweisen lässt.

WICHTIG

Cortex XDR senkt die Gesamtbetriebskosten im Vergleich zu herkömmlichen Tools um durchschnittlich 44 Prozent durch die:

- Nutzung vorhandener Sicherheitstools als Sensoren für die Bedrohungserkennung und -abwehr
- Eliminierung von Protokollservern vor Ort durch Cloud-Bereitstellung
- Vereinfachung von Abläufen durch Verknüpfung von Daten, Gruppierung von Warnmeldungen und Ursachenanalysen

CORTEX® XDR™

# Getestet. Geprüft. Bewährt.

## Kampferprobt in der SolarWinds Attacke

100% Prävention und 97% Erkennung und Visibilität in der MITRE ATT&CK Evaluation Runde 3

MITRE ENGENUITY

Führend bei The Forrester Wave Endpoint Security As A Service, Q2 2021

FORRESTER® WAVE LEADER 2021 Endpoint Security Software As A Service

## Lernen Sie mehr über die industrieweit erste XDR-Plattform

**Cortex XDR:**
http://go.paloaltonetworks.com/xdrpdpde

**Essential Guide to MITRE Round 3:**
http://go.paloaltonetworks.com/mitrewileyde

**Forrester ESS Wave:**
http://go.paloaltonetworks.com/esswileyde

**Kontaktieren Sie uns heute:**
0800-7239771

paloalto® NETWORKS

# Effektiviere Sicherheitsabläufe mit Extended Detection and Response (XDR)

Sicherheitsteams werden mit einer Vielzahl von Bedrohungen konfrontiert – von Ransomware über dateilose Angriffe bis hin zu Datenschutzverletzungen. Das größte Problem für die meisten Sicherheitsanalysten sind jedoch nicht die vielen Angriffe, die Schlagzeilen machen; es sind die sich wiederholenden Aufgaben, die sie jeden Tag erledigen müssen, während sie Ereignisse priorisieren und versuchen, zahllose alte Warnmeldungen abzuarbeiten. Extended Detection and Response (XDR) ist ein neuer Ansatz zur Erkennung, Untersuchung und Abwehr von Bedrohungen, bei dem Daten aus beliebigen Quellen integriert und analysiert werden.

## Im Buch ...

- Einschränkungen herkömmlicher Ansätze erkennen
- Fachkräftemangel im Bereich Cybersicherheit beheben
- zuverlässige Bedrohungsabwehr sicherstellen
- vollständige Transparenz erzielen
- Bedrohungserkennung und -abwehr automatisieren
- Effektivität von Sicherheitsmaßnahmen verbessern
- Netzwerk-, Endpunkt- und Cloud-Ressourcen schützen

paloalto NETWORKS

**Lawrence Miller** ist seit über 25 Jahren in verschiedenen Branchen im Bereich Informationstechnologie tätig. Er ist Mitautor des Buches *CISSP Für Dummies* und hat über 200 weitere *Für-Dummies*-Bücher zu zahlreichen technischen und sicherheitsbezogenen Themen verfasst.

**Besuchen Sie Dummies.com®**
**um sich Videos und schrittweise Bildanleitungen anzusehen oder Produkte zu kaufen!**

**ISBN: 978-1-119-87897-1**



für dummies®

# WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.