Präsentiert von

Extended Detection and Response (XDR)

für dummies®

Cisco Sonderausgabe

Der Nutzen einer XDR-Plattform

Bessere Bedrohungserkennung

Geringere Komplexität für Ihr Sicherheitsteam

James Sullivan

Über Cisco Secure

Als der weltweit größte Cybersecurity-Anbieter für Unternehmen sehen wir es als unsere Pflicht an, die Branche mit Lösungen wie SASE, XDR und Zero Trust weiter anzutreiben. All das integrieren wir mit Cisco SecureX in einer Plattform, die Sicherheit über Ihre gesamte Infrastruktur hinweg so einfach wie transparent und dabei hochgradig effizient macht.

cisco.com/go/securex

Der XDR-Ansatz von Cisco basiert auf der integrierten, Cloud-nativen Plattform von SecureX. Diese offene Plattform verbindet Ihre Cisco Sicherheitsprodukte mit dem Rest Ihrer Infrastruktur, ist einfach zu verwenden, erhöht die Transparenz durch Zentralisierung und maximiert die betriebliche Effizienz, um Ihre Netzwerke, Endpunkte, Clouds und Anwendungen optimal abzusichern. Sie verkürzt die Verweildauer erheblich und reduziert die von Menschen durchzuführenden Aufgaben bei der Angriffsabwehr und der Einhaltung von Vorschriften.

- www.twitter.com/ciscosecure
- www.facebook.com/ciscosecure
- www.linkedin.com/showcase/cisco-secure/

Extended Detection and Response (XDR)

Cisco Sonderausgabe

James Sullivan

für dummies®

Extended Detection and Response (XDR) Für Dummies®, Cisco Sonderausgabe

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

ISBN 978-1-394-15622-1 (pbk); ISBN 978-1-394-15623-8 (ebk)

Danksagung des Verlags

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

Project Manager: Jennifer Bingham
Acquisitions Editor: Ashley Coffey
Editorial Manager: Rev Mengle
Content Refinement Specialist: Vivek Lakshmikanth

Einführung

Die IT-Sicherheit ist einer der sich am schnellsten verändernden Bereiche in der Tech-Branche. Ständig tauchen neue Tools, Techniken und Angriffsarten auf. Eines dieser Tools ist Extended Detection and Response (XDR). XDR-Plattformen bieten Tools zur Orchestrierung, Überwachung, Analyse, Automatisierung, Visualisierung usw. und damit einen zentralisierten Überblick über Ihre gesamte Sicherheitsinfrastruktur.

Die Sicherheitsumgebungen von Unternehmen sind so komplex geworden, dass isolierte Sicherheitsressourcen keine sinnvolle Option mehr darstellen. Es gibt immer mehr Angriffspunkte für Kriminelle und normale Geschäftsaktivitäten werden oft als böswillig interpretiert, während Sicherheitsteams versuchen, tatsächliche Bedrohungen in den Griff zu bekommen.

SIEM (Security Information and Event Management)- und SOAR (Security Orchestration Automation and Response)-Lösungen haben einige Funktionen mit XDR gemeinsam, doch es gibt auch einige wesentliche Unterschiede. SIEM-Tools sind oft nicht in der Lage, alle von ihnen erstellten Protokolle und Warnmeldungen zu organisieren und zu verarbeiten. SOAR-Lösungen wiederum verfügen nicht über die von XDR gebotenen Integrationsmöglichkeiten. Dennoch haben diese beiden Tools ihren berechtigten Platz in der Sicherheitslandschaft.

Dieses Buch erläutert, was XDR ist, in welcher Beziehung es zu anderen Sicherheitslösungen steht, wie sich XDR mit anderen Lösungen integrieren lässt und welche Herausforderungen XDR lösen soll.

Über dieses Buch

XDR ist eine Neuerscheinung im IT-Sicherheitsbereich, mit der längst noch nicht jeder vertraut ist. Deshalb gibt es dieses Buch! Die Ratgeber aus der Reihe *Für Dummies* sind leserfreundlich und enthalten leicht verdauliche Informationen, die dem Leser zur Verfügung gestellt werden, um fundierte Entscheidungen zu treffen, etwas in Gang bringen oder einfach etwas Neues zu lernen.

Es könnte auch sein, dass Sie sich nur mit einem bestimmten Aspekt von XDR befassen möchten. Das ist kein Problem! Obwohl jedes Kapitel nützliche Informationen über XDR oder IT-Sicherheit im Allgemeinen enthält, können Sie den einen oder anderen Abschnitt getrost

überspringen. Jedes Kapitel ist in sich geschlossen, sodass es nicht nötig ist, zuerst die vorherigen Abschnitte zu lesen.

Wenn Sie sich eine komprimierte Version dieses Buches wünschen, können Sie einfach zu Kapitel 6 gehen. Dort sind zehn der wichtigsten Fakten über XDR aus dem restlichen Buch zusammengefasst. Auf diese Weise können Sie sich einen Überblick über den Inhalt des Buches verschaffen oder sich schnell mit dem Thema XDR vertraut machen!

In diesem Buch verwendete Symbole

Während der Lektüre werden Sie auf einige spezielle Symbole stoßen. Wir verwenden diese Bildzeichen, um auf besondere Informationen hinzuweisen oder an die wichtigen Punkte jedes Kapitels zu erinnern. In diesem Buch finden Sie die folgenden Symbole:


ERINNERN

Dieses Symbol wird verwendet, um einen wichtigen Punkt hervorzuheben. Dabei kann es sich um konkrete Informationen zu einem Sicherheitstool oder um ein allgemeines Konzept handeln. Diese Informationen tauchen wahrscheinlich mehrmals auf.


TIPP

Dieses Symbol weist auf ein kleines Extra im Abschnitt hin. Manchmal wird ein Punkt näher erläutert oder etwas hinzugefügt, das nicht in den Hauptabschnitt gepasst hat. Tipps sind in der Regel konkret und beziehen sich nicht auf allgemeine Konzepte.

Zusätzliche Informationen

Wenn Sie nach der Lektüre noch Fragen haben oder mehr über XDR und IT-Sicherheit erfahren möchten, besuchen Sie bitte `cisco.com/go/xdr` oder `blogs.cisco.com/security`. Dort können Sie nachlesen, was die Mitarbeiter von Cisco über den Stand der IT-Sicherheit denken.

IN DIESEM KAPITEL

- So haben sich Sicherheitsbedrohungen verändert
- Moderne Sicherheitstools und -methoden
- Schlüsselelemente von XDR
- Der Ansatz von Cisco

Kapitel 1
Security Operations: Trends und Herausforderungen

Die Cybersicherheitslandschaft von heute ist besorgniserregend. Jeden Tag scheinen neue Bedrohungen – auch von Staaten ausgehend – und Bedrohungsakteure aufzutauchen, darunter Cyberspionage, Fehlkonfigurationen, Schwachstellen. Darüber hinaus gibt es so viele Anbieter und Tools auf dem Markt, dass der Versuch, das Zusammenspiel dieser Produkte zu koordinieren, nicht selten ins Chaos führt.

In diesem Kapitel werden einige der bekanntesten auf dem Markt erhältlichen Sicherheitstools vorgestellt. Sie erfahren, wie sich diese Tools voneinander unterscheiden und welche Vorteile die neue Technologie Extended Detection and Response (XDR) zu bieten hat. Doch zunächst wollen wir uns ansehen, wie sich Sicherheitsbedrohungen in den letzten Jahren entwickelt haben.

Die sich verändernde Bedrohungslandschaft

Es gibt viele Arten von Cyberangriffen, darunter Ransomware, Schwachstellen, Malware und eine Reihe anderer Sicherheitsbedrohungen, deren Anzahl so schnell zunimmt wie ihre Komplexität.

Zu den größten Bedrohungen gehören:

- **Ransomware:** Ja, es gibt sie immer noch. Bei Ransomware handelt es sich um eine Angriffsart, bei der Daten verschlüsselt werden, um Lösegeld zu erpressen. Der jüngste Angriff auf die Colonial Pipeline ist ein prominentes Beispiel für die verheerenden Folgen, die derartige Bedrohungen haben können.
- **Angriffe auf Staats- und Regierungsebene:** Dabei handelt es sich um Cyberangriffe, die von staatlichen Akteuren ausgehen. Die Angriffe auf Sony und das US-Finanzministerium haben gezeigt, dass staatlich gesponserte Angriffe weiterhin eine ernstzunehmende Bedrohung darstellen.
- **Malware und andere Viren:** Eine weitere bewährte Angriffsstrategie ist Malware. Dabei handelt es sich um Software, die darauf programmiert ist, interne Systeme zu stören oder zu schädigen. Trotz ihrer zunehmenden Komplexität können diese Bedrohungen oft durch einfache Methoden verbreitet werden. Es kommt zum Beispiel immer häufiger vor, dass Hacker „dringende" E-Mails versenden, um Benutzer zur Installation falscher Windows-Updates zu veranlassen.
- **Insider-Angriffe:** Dabei handelt es sich um Angriffe, die von Angestellten im eigenen Unternehmen ausgeführt werden. Über diese Art von Bedrohung wird nicht oft gesprochen, doch sie sollte ebenfalls sehr ernst genommen werden. Ein Unternehmen kann Bewerber vor der Einstellung noch so sorgfältig prüfen, trotzdem schlüpfen immer wieder bösartige Akteure durchs Netz. Häufige Insider-Angriffe sind das Durchsickernlassen von und Handeln mit geschützten Informationen.

Die Besorgnis über die Cybersicherheit kann für Unternehmen überwältigend sein, trotzdem ist sie der Preis, den sie für die Digitalisierung zahlen müssen. Letzten Endes geht es darum, die Kontrolle über die Ressourcen und die Infrastruktur des Unternehmens zu behalten. Jemand könnte versuchen, in Ihr Netzwerk einzudringen, Ihre Daten zu stehlen oder zu zerstören und vielleicht sogar Ihre Hardware zu kompromittieren. All das sind Risiken, auf die Sie vorbereitet sein müssen, wenn Sie die Vorteile der Arbeit in digitalen Umgebungen ausschöpfen wollen.

Sicherheitstools und -methoden

So wie die Sicherheitsbedrohungen, mit denen Unternehmen heute konfrontiert sind, haben sich auch die Sicherheitsmethoden und -tools weiterentwickelt. Für den Schutz von Kundendaten und der Integrität

von Netzwerken reicht es nicht mehr aus, eine Firewall einzurichten und dann auf das Beste zu hoffen. (Das soll allerdings nicht heißen, dass Sie keine Firewall mehr brauchen.)

Wie in der Technologiebranche üblich, werden im Bereich Sicherheitslösungen gern viele Schlagwörter, Abkürzungen und Akronyme gebraucht. In diesem Buch werden wir drei Arten von Sicherheitslösungen betrachten, die zur Verbesserung der Automatisierung und zur Erkennung von Bedrohungen verwendet werden: Security Information and Event Management (SIEM), Security Orchestration Automation and Response (SOAR) und Extended Detection and Response (XDR). Lassen Sie uns zunächst über das Siloproblem sprechen.

Isolierte Lösungen und ihre Grenzen

Es ist gängige Praxis, unterschiedliche Bereiche einer digitalen Infrastruktur voneinander zu trennen, weil dies zahlreiche Vorteile hat. Es sorgt nicht nur für Ordnung, sondern gibt Entwicklern und Administratoren auch die Möglichkeit, sich auf die Informationen zu konzentrieren, die für sie wirklich relevant sind. Oft ist dies genau die Art, wie Lösungen und Tools verwendet werden sollten. Problematisch wird es jedoch, wenn unterschiedliche Systeme über Informationen verfügen, die für die Funktion anderer von ihnen isolierter Systeme relevant sind.

Dieses Problem ist besonders bei Sicherheitslösungen zu beobachten. Bei der Endpunktsicherheit werden andere Informationen erfasst und verarbeitet als bei der Netzwerk- oder E-Mail-Sicherheit. Alle diese Systeme profitieren jedoch in hohem Maße von einer ganzheitlichen Ansicht.

ERINNERN

Seit Kurzem gibt es Innovationen und Lösungen, mit denen die Einschränkungen von isolierten Sicherheitslösungen überwunden werden können. Die beiden bekanntesten Lösungsarten der letzten fünf Jahre sind SIEM- und SOAR-Tools.

Frühe Integrationsversuche: SIEM

Security Information and Event Management (SIEM) ist eine relativ erfolgreiche und bewährte Lösung zur Verwaltung von Protokollen und Ereignissen. Im Kern hat SIEM die Aufgabe, möglichst viele Protokolldaten aus dem gesamten Unternehmen zusammenzutragen.

Viele SIEM-Lösungen können Protokolldaten von IoT-Sicherheitstools (Internet of Things), Firewall-Ereignisprotokolle und Daten aus zahlreichen anderen Quellen erfassen. Diese Lösungen tragen dazu bei, Silos aufzubrechen, da sie mit mehreren Lösungen integriert werden können und wichtige Sicherheitsinformationen an einer zentralen Stelle zusammenführen.

SIEM-Tools können Sicherheitstechniker jedoch nicht dabei helfen, schneller und effizienter auf Bedrohungen zu reagieren. Ein umfassender Überblick über die Sicherheitslandschaft des Unternehmens ist in vielerlei Hinsicht nützlich. Ebenso wichtig ist jedoch die Bedrohungsabwehr.

Frühe Versuche der Bedrohungsabwehr: SOAR

Security Orchestration, Automation and Response (SOAR) hat viele der Qualitäten, durch die sich SIEM auszeichnet, verfügt jedoch über zusätzliche Schichten, die einige der Schwächen älterer Lösungen ausgleichen. SOAR-Lösungen führen wie SIEM Daten aus unterschiedlichen Bereichen der Sicherheitsinfrastruktur an einer zentralen Stelle zusammen, worunter man die Orchestrierung versteht.

Hinzu kommen Automatisierungen, die dafür sorgen, dass die gesammelten Informationen effektiv genutzt werden können. Viele SOAR-Lösungen verfügen über Optionen zur Automatisierung unterschiedlicher Überprüfungs-, Protokoll- und Scanprozesse. Die Automatisierung kann jedoch nicht alle Aufgaben übernehmen, weshalb gelegentlich menschliches Eingreifen erforderlich ist.

Bei der Reaktionskomponente von SOAR geht es um die Organisation und Verwaltung von Reaktionsmaßnahmen auf Sicherheitsvorfälle. Diese Funktion nutzt Orchestrierungs- und Automatisierungsinformationen, um Sicherheitspersonal bei der Entscheidungsfindung und Bedrohungsabwehr zu helfen.

ERINNERN

Bei der Automatisierung mit SOAR werden nicht die Reaktionsmaßnahmen auf Sicherheitsverletzungen automatisiert, sondern einfache Analyseaufgaben, um die Arbeitsbelastung des Sicherheitspersonals zu reduzieren.

Was ist XDR?

Extended Detection and Response (XDR) wurde erst vor Kurzem in den umfangreichen Akronymwortschatz im Bereich der Unternehmenstechnologie aufgenommen. XDR übernimmt viele nützliche Funktionen von SIEM und SOAR und fügt etablierten Lösungen noch einige weitere Elemente hinzu.

Die Grundlagen von XDR

Während der Schwerpunkt bei SIEM und SOAR auf Protokollen und Analysen liegt – also auf dem, was letztendlich in die Hände des Sicherheitspersonals gelangt –, konzentrieren sich XDR-Lösungen auf die

Endpunkte selbst. Bei XDR spielt sich alles am Endpunkt ab, denn genau das ist das Angriffsziel externer Akteure.

In dieser Hinsicht hat XDR viel mit EDR (Endpoint Detection and Response) gemeinsam – doch die neue Lösung heißt nicht EDR, sondern XDR. XDR erweitert die Fähigkeiten herkömmlicher EDR-Lösungen und vertieft die Funktionen von SIEM- oder SOAR-Lösungen. So *erweitert* XDR zum Beispiel die Transparenz- und Erkennungsfunktionen einer EDR-Lösung mithilfe der Daten und Erkenntnisse der NDR-Lösung (Network Detection and Response).

Das Ziel besteht darin, dass zwischen der Protokollierung eines verdächtigen Verhaltens, dessen Erkennung als Angriff, der Erstellung eines Reaktionsplans und der Ausführung dieses Plans so wenig Zeit wie möglich vergehen sollte. Zum besseren Verständnis des Konzepts ist es hilfreich, die Bestandteile einer XDR-Lösung näher zu betrachten.

Komponenten einer XDR-Lösung

XDR ist ein relativ junges Sicherheitskonzept und unter den derzeit verfügbaren Lösungen gibt es noch einige Unterschiede. XDR-Lösungen sollten die folgenden Schlüsselfunktionen aufweisen:

- **Flexible Integration:** Der Umfang und die Art der Integration mit bestehenden Sicherheitslösungen hängen von der XDR-Lösung selbst ab. In den meisten Fällen ist es möglich, andere Sicherheitstools, insbesondere für Endpunktsicherheit, in eine XDR-Plattform zu integrieren.
- **Zentralisierte Ansicht:** Ohne eine zentralisierte Ansicht aller erfassten Informationen wäre eine XDR-Lösung nicht sehr nützlich. XDR überblickt einen Großteil der (wenn nicht die gesamte) Sicherheitsumgebung. Zur Analyse dieser Datenmengen ist eine zentrale Schnittstelle erforderlich.
- **Maschinelles Lernen:** XDR-Plattformen bieten maschinelles Lernen zur Analyse von Sicherheitsdaten. Dies trägt erheblich zur Verkürzung der Reaktionszeiten bei, da das Sicherheitspersonal vor der Behebung eines Sicherheitsproblems weniger Vorarbeit leisten muss.
- **Automatisierung:** Wie SOAR-Lösungen auch nutzt XDR Automatisierung, um SecOps-Workloads zu reduzieren. Dabei werden zwar nur einfache Aufgaben automatisiert, doch diese können viel bewirken.

Je nach Anbieter kann eine XDR-Plattform mit zusätzlichen Funktionen ausgestattet sein, doch die oben genannten Merkmale sollte die Grundlage jeder XDR-Lösung bilden.

Warum ist XDR so wichtig?

SIEM, SOAR, NDR und EDR – alle diese Lösungen sind auf ihre Weise nützlich. XDR ist eine Neuheit auf dem Markt für Sicherheitslösungen und muss daher etwas bieten, was es bisher noch nicht gegeben hat. Der wirkliche Vorteil dieser neuen Option liegt nicht nur in ihren neuen Funktionen. Entscheidend ist auch, wie diese Funktionen die Herausforderungen der aktuellen Sicherheitslandschaft direkt angehen.

Neue Sicherheitsherausforderungen

Cyberangriffe werden immer raffinierter – und das gilt nicht nur für die Angriffsmethode. Auch die Einfallstelle ändert sich zunehmend. Das Internet of Things (IoT) und die zunehmende Cloud-Nutzung haben dazu geführt, dass immer mehr Netzwerke entstehen und dass die Anzahl der mit ihnen verbundenen Endpunkte rapide zunimmt. Das wissen auch Außenstehende, die nichts Gutes im Schilde führen.

Heutzutage ist es möglich, Angriffe auf mehreren Netzwerken und Endpunkten gleichzeitig auszuführen. Es gibt breit angelegte Angriffe, die neuartige IT-Sicherheitslösungen erfordern. SIEM- und SOAR-Lösungen sind nicht für die Verarbeitung und Verwaltung dieser Art von Angriffen ausgelegt. EDR und NDR können eher mit solchen Angriffen umzugehen. Allerdings verfügen sie nicht über die nötigen Verwaltungsfunktionen, um schnell auf komplexe Bedrohungen zu reagieren.

Vielfältige Informationsquellen

Nicht nur die Angriffsformen werden immer ausgefeilter, sondern auch die IT-Umgebungen von Unternehmen. Jeden Tag kommen neue potenzielle Angriffsziele hinzu. Die Nutzung von IoT-Geräten, Cloud-Anwendungen und Datenbanken nimmt rasant zu. Besonders der Homeoffice-Trend gibt Anlass zur Besorgnis. Dieser Arbeitsstil wird immer beliebter und führt zur stetigen Zunahme von Geräten mit Zugriff auf interne Ressourcen.

Die Arbeit von zu Hause bringt unter anderem die folgenden Herausforderungen mit sich:

- Es gibt mehr Geräte, die geschützt werden müssen, und damit auch mehr Angriffsziele, die von böswilligen Außenstehenden ausgenutzt werden können.
- Die Gerätevielfalt hat zugenommen. Viele Unternehmen verlassen sich nicht mehr ausschließlich auf Arbeitscomputer. Deshalb ist eine ebenso vielfältige Palette von Sicherheitslösungen erforderlich.

» Heimnetzwerke sind selten so gut abgesichert wie Büronetzwerke. Die meisten Mitarbeiter eines Unternehmens sind keine Sicherheitsexperten und können keine durchgängig sichere Netzwerkverbindung garantieren.

So entsteht ein komplexes Ökosystem, das eine komplexe Kombination von Sicherheitslösungen erfordert. Der Wunsch, diese Sicherheitstools und Informationsquellen voneinander zu trennen, ist vor diesem Hintergrund durchaus nachvollziehbar. XDR ist deshalb so wichtig, weil es Unternehmen die Möglichkeit bietet, ungleichartige Sicherheitstools in ihrer Sicherheitsumgebung zu verwenden, ohne die Sicherheitsvorgänge zu beeinträchtigen.

Überlastetes Sicherheitspersonal

IT-Sicherheitsexperten sind hoch qualifizierte und sachkundige Fachleute, doch auch ihre Fähigkeiten haben Grenzen. Da moderne Sicherheitsökosysteme immer komplexer und umfangreicher werden, sind Sicherheitstechniker oft überlastet, was wiederum zu Fehlern bei Sicherheitsvorgängen führt.

Im richtigen Kontext sind SIEM- und SOAR-Lösungen zwar sehr nützlich, doch da sie Daten aus zahlreichen Quellen erfassen, können sie schnell eine Informationsüberflutung auslösen. Oft werden SIEM-Produkte lediglich als neue Sammelstelle für Protokolle eingesetzt, für deren Verarbeitung jedoch keine Tools zur Verfügung stehen. Die von Sicherheitstools generierten Informationen sind so zahlreich und vielfältig, dass sie ohne maschinelle Hilfe kaum noch bewältigt werden können.


TIPP

All das soll nicht heißen, dass ich SIEM grundsätzlich negativ gegenüberstehe. Diese Lösungen sind besonders für Branchen nützlich, in denen die Einhaltung von Vorschriften eine große Rolle spielt, da dort Unmengen von Protokollen benötigt werden.

Überlastetes und gestresstes Sicherheitspersonal macht Fehler, die zu Sicherheitsverstößen und zur Unzufriedenheit am Arbeitsplatz führen. In einer solchen Situation gibt es nur Verlierer! Da sich XDR auf die Endpunktsicherheit und die Automatisierung von Aufgaben konzentriert, wird die Arbeitsbelastung von Sicherheitsexperten erheblich reduziert.

Hauptziel: Verkürzung der MTTD und der MTTR

Jedes Sicherheitsteams hat ein wesentliches Ziel: die mittlere Erkennungszeit (Mean-Time-to-Detect, MTTD) und die mittlere Reaktionszeit (Mean-Time-to-Respond, MTTR) zu reduzieren. MTTD und MTTR – das sind die beiden Gründe, warum es IT-Sicherheitsteams überhaupt gibt!

Worum es dabei geht, lässt sich aus der Bezeichnung ableiten: Wie lange dauert es normalerweise, bis ein Sicherheitsproblem erkannt und behoben wird? Die Erkennungszeit erhöht sich, wenn zum Auffinden von Sicherheitsproblemen zahlreiche Warnmeldungen und Protokolle durchsucht werden müssen. Die Reaktionszeit erhöht sich, wenn keine Automatisierungs- und Analysetools vorhanden sind.

XDR ist die jüngste Lösung in der Sicherheitslandschaft, die versucht, sowohl die MTTR als auch die MTTD zu verringern. Sammlung, Analyse, Automatisierung und Zentralisierung – das alles sind wesentliche Aspekte von XDR, die dazu beitragen, die Erkennungs- und Reaktionszeiten zu verkürzen. Ist das nicht genau das, was eine Sicherheitslösung leisten sollte?

Der Ansatz von Cisco Secure

Dem XDR-Ansatz von Cisco Secure liegt eine integrierte Plattform zugrunde. Bei XDR geht es um Organisation und Kontrolle. Deshalb hat Cisco Secure die Schlüsselkomponenten einer erfolgreichen erweiterten Erkennungs- und Reaktionslösung zusammengefasst:

- **X:** Die Plattform sollte so viele Kontrollpunkte und Datenquellen wie möglich unterstützen. Eine Sicherheitslösung ist nur so gut wie die Schwachstellen, die sie abdecken kann.
- **D:** Auf maschinellem Lernen basierende Analysemethoden reduzieren die Erkennungszeit (MTTD) und helfen Sicherheitsexperten dabei, bessere Entscheidungen zu treffen.
- **R:** Durch Automatisierungsfunktionen und die Nutzung zentralisierter Sicherheitsinformationen werden kürzere Reaktionszeiten erzielt, während die Untersuchung von Sicherheitsvorfällen optimiert wird.

Die Philosophie von Cisco Secure hat noch einen weiteren wichtigen Aspekt: Jedes der oben aufgeführten Ziele von XDR ist gleichermaßen wichtig. Die Reichweite einer XDR-Plattform bringt nicht viel, wenn sie nicht über Automatisierungsfunktionen verfügt, die Sicherheitsanalysten Routineaufgaben abnehmen können. Cisco Secure will die Integration mit bestehenden Sicherheitsprodukten in Ihrer Umgebung so einfach wie möglich gestalten. XDR versucht nicht, diese Sicherheitstools zu ersetzen, sondern unterstützt sie durch den Abbau von Silos und durch die Optimierung von Sicherheitsvorgängen.

IN DIESEM KAPITEL

- Isolierte Lösungen schaffen Hindernisse
- Ungelöste Probleme in Security Operations im Unternehmen

Kapitel 2
Der aktuelle Stand der Bedrohungserkennung und -reaktion

Der aktuelle Stand der Erkennung von und Reaktion auf Bedrohungen ist dem in anderen IT-Bereichen nicht unähnlich. Es gibt so viele Tools, dass es schwierig ist, den Überblick zu behalten. Anbieter verwenden unterschiedliche Bezeichnungen für dieselben Konzepte und IT-Umgebungen sind so komplex, dass die Silobildung zur gängigen Praxis geworden ist.

Doch obwohl Sicherheitsexperten heute unzählige Tools zur Verfügung stehen, sind SecOps-Teams weiterhin mit ungelösten Problemen konfrontiert. Sie sind ständig darum bemüht, die mittlere Erkennungszeit (Mean-Time-to-Detect, MTTD) und die mittlere Reaktionszeit (Mean-Time-to-Respond, MTTR) so gering wie möglich zu halten, während ihnen Fehlalarme unnötige Arbeit aufbürden.

Bevor wir auf die bislang ungelösten Probleme eingehen, wollen wir einen Blick auf die Silobildung werfen und herausfinden, warum sie Sicherheitsteams ausbremsen.

Isolierte Lösungen schaffen Hindernisse

Die Abgrenzung von Lösungen in Silos erfolgte ursprünglich als Reaktion auf das immer größer und komplexer werdende Netz aus Ökosystemen und die Sicherheitstools, die zu seinem Schutz benötigt wurden. Durch die Aufteilung verschiedener Sicherheitsbereiche in eigene Umgebungen sollte die Komplexität reduziert und die Verwaltung vereinfacht werden.

Stattdessen heben diese Silos die Herausforderungen nur noch deutlicher hervor, mit denen Unternehmen bei der Verwaltung und dem Schutz moderner Infrastrukturen zu kämpfen haben. Immerhin sind diese Ökosysteme nicht ohne Grund so komplex! Netzwerke, Anwendungen und Datenbanken – sie alle sind Teil eines größeren Ganzen und keine unabhängigen Einzelgänger, die in der Wildnis umherwandern und von der Natur leben können.

Jeder dieser isolierten Bereiche steht vor seinen eigenen durch die Silobildung verursachten Herausforderungen. Die folgenden Beispiele sollen dies deutlich machen.

Netzwerksicherheit

Stellen Sie sich die Netzwerksicherheit wie ein Vorhängeschloss an einer Tür vor, hinter der sich alle Ihre Schätze befinden. Sie umfasst:

- Firewalls
- Eindringschutz
- Netzwerkzugriffssteuerung

Dies ist keineswegs eine erschöpfende Liste aller Netzwerksicherheitsfunktionen, doch sie enthält einige der wichtigsten Tools. Das Silo der Netzwerksicherheit enthält Informationen über die IP-Adressen, die versuchen, sich mit dem Netzwerk zu verbinden, das Volumen des Netzwerkverkehrs und die Integrität der Ports, um nur einige zu nennen.

ERINNERN

Was die Netzwerksicherheit sehen kann, verrät gleichzeitig, was sie nicht sehen kann. Eine plötzlich auftretende anhaltende Datenverkehrsspitze kann aus Sicht der Netzwerksicherheit wie ein verteilter Denial-of-Service-Angriff (DDoS) aussehen. Doch was passiert, wenn es sich um eine neue Workload handelt, die anfänglich hohe Anforderungen an interne Services stellt?

In diesem Fall muss die Netzwerksicherheit mit den Anwendungsteams Rücksprache halten – und mit allen anderen Teams, die die

Datenverkehrsspitze verursacht haben könnten. Das nimmt Zeit und zusätzliche Ressourcen in Anspruch, die der Sicherheit verloren gehen, während möglicherweise ein Angriff stattfindet. Die MTTD und die MTTR sind in diesem Fall viel länger als nötig.

Anwendungssicherheit

Bei der Anwendungssicherheit geht es um den Schutz von Anwendungen und ihrer Ressourcen, darunter Server, Datenbanken, Messaging-Systeme und andere Software-Infrastrukturen. Dieses Sicherheitssilo deckt zahlreiche Aufgaben ab, von Datenbankautorisierungen über die Überwachung der CPU-Auslastung bis hin zum Input/Output-Monitoring.

Die Anwendungssicherheit kann ähnlich wie die Netzwerksicherheit verlangsamt und beeinträchtigt werden, wenn keine vollständigen Informationen über ein ungewöhnliches Verhalten vorliegen. Sie muss mehr als nur die eigene Umgebung sehen können.

Nehmen wir eine I/O-Spitze als Beispiel. Angenommen, mitten in der Nacht tritt eine extreme Änderung der Netzwerknachfrage auf. Außerhalb der üblichen Betriebszeit werden große Datenmengen durch eine Anwendung ein- und ausgeschleust, und die Anwendungssicherheit wird alarmiert. Dies könnte ein Hinweis auf eine Datenpanne sein. Es könnte sich aber auch um einen Testlauf einer Datenmigration handeln, der von einer anderen Abteilung durchgeführt wird.

Was ist, wenn die CPU-Auslastung sprunghaft ansteigt und ungewöhnlich erscheint? Das könnte bedeuten, dass Schadsoftware auf einer virtuellen Maschine läuft oder dass eine Schwachstelle in einer Anwendung ausgenutzt wird. Es könnte sich aber auch um etwas völlig Harmloses handeln, das zum normalen Geschäftsbetrieb gehört.

In beiden Fällen schafft das Silo zusätzliche Hürden, die das Sicherheitsteam überwinden muss. Es kann nicht effizient arbeiten und muss viel Zeit mit der wiederholten Überprüfung alle Aktivitäten verbringen, um sicherzustellen, dass sie kein Risiko darstellen.

Endpunktsicherheit

Auch die Endpunktsicherheit umfasst eine Reihe von Sicherheitstools. Anti-Malware, Verhinderung von Datenverlust und die Erkennung von Bedrohungen auf Endgeräten fallen alle unter den Begriff Endpunktsicherheit. Dieser Bereich wird immer komplexer, da die Anzahl der Sicherheitstools für Endgeräte aufgrund des Homeoffice-Trends

ständig zunimmt. Da mehr Geräte auf interne Ressourcen zugreifen müssen, werden mehr Sicherheitslösungen als je zuvor benötigt.

Die Endpunktsicherheit selbst wird nicht in dem Maß durch das Sicherheitssilo beeinträchtigt wie andere Sicherheitsbereiche, doch sie verursacht Probleme für andere Teams, z. B. das Identitätsmanagement und die Netzwerksicherheit.

Identitäts- und Zugriffsmanagement

In diesem Bereich ist die Situation nicht so eindeutig. Das Wort „Sicherheit" ist nicht einmal im Namen enthalten! Eine der Hauptaufgaben des Identitäts- und Zugriffsmanagements (Identity and Access Management, IAM) ist die Verwaltung der Authentifizierung. Unter diesen Oberbegriff fallen:

- Zwei-Faktor-Authentifizierung
- Digitale Zertifikate
- Benutzernamen
- Passwörter

Die jeweiligen Authentifizierungsanforderungen bei der Anmeldung hängen von einem oder mehreren der folgenden Punkte ab: worauf der Benutzer zugreifen will, welche Branchenvorschriften gelten und welche unternehmensspezifischen Richtlinien angewandt werden.

Fehlgeschlagene Anmeldeversuche sind ein einfaches Beispiel für die hemmende Wirkung von Silos. Wiederholte fehlgeschlagene Anmeldeversuche – sei es durch die Eingabe eines falschen Passworts oder Benutzernamens (oder etwas völlig anderes) – können sowohl für Anwendungs- als auch Netzwerksicherheitsteams wie ein Angriffsversuch aussehen.

Da IAM für die Identitäten von Servicekonten verantwortlich ist, gibt es bei der Autorisierung der Ressourcennutzung Überschneidungen mit dem Bereich Anwendungssicherheit. Um die MTTD und die MTTR zu verringern, ist es besonders wichtig, die Silos zwischen Netzwerksicherheit und IAM aufzubrechen.

Ungelöste Probleme, mit denen Unternehmen zu kämpfen haben

Auch wenn sich die Unternehmenstechnologie in einem rasanten Tempo weiterentwickelt, gibt es nach wie vor zahlreiche Probleme, die Entwicklern, Administratoren, Sicherheitsexperten und Führungskräften Kopfzerbrechen bereiten. MTTD, MTTR, Fehlalarme und die ineffiziente Triage von Vorfällen sind Probleme, mit denen Unternehmen immer noch konfrontiert sind.

MTTD

Die mittlere Erkennungszeit (Mean Time to Detect, MTTD) ist ein kritisches Element der Unternehmenssicherheit. MTTD ist die Zeit, die ein Sicherheitsteam in der Regel benötigt, um eine Sicherheitsverletzung zu finden und zu bestätigen. Zur Reduzierung der MTTD reicht es nicht aus, eine Warnmeldung entgegenzunehmen und den Angriffsort zu finden.

Zur Erkennung einer Bedrohung oder eines laufenden Angriffs müssen mehrere ineinandergreifende Systeme untersucht und die Kommunikation zwischen den für diese Systeme zuständigen Teams koordiniert werden. Wenn ein Netzwerkadministrator zum Beispiel eine Aktivität bemerkt, die wie eine Datenbankinfiltration aussieht, muss die Aktivität mit den Datenbankteams abgeglichen und herausgefunden werden, ob sie legitim ist.

Die Herausforderung besteht hierbei darin, die Erkennung schnell zu koordinieren, ohne Abstriche hinsichtlich der Genauigkeit zu machen. Wenn die Gültigkeit einer Bedrohung nicht bestätigt wird, führt dies zu noch mehr Zeit- und Ressourcenverschwendung.

MTTR

Für die mittlere Reaktionszeit (Mean-Time-to-Respond, MTTR) beginnt die Uhr zu ticken, sobald ein Sicherheitsproblem erkannt und bestätigt wurde. MTTR ist das Maß für die durchschnittliche Zeit, die Sicherheitsteams benötigen, um ein Problem einzudämmen oder zu beheben. Die wichtigsten Fragen in Bezug auf MTTR sind: Was wurde kompromittiert und wie lässt sich das Problem beheben?

Die größte Herausforderung bei der Reaktion auf Bedrohungen besteht oft darin, dass das Ausmaß des Schadens nur schwer zu erkennen ist, weil die IT-Umgebung so groß ist. Dafür gibt es mehrere Gründe, und der Kontext spielt dabei eine wichtige Rolle:

- Bei einem netzwerkbasierten Angriff müssen möglicherweise IP-Adressen gefunden und mit dem Netzwerksicherheitsteam gegengeprüft werden. Doch wo befindet sich der Angreifer, wenn der Angriff bereits stattgefunden hat?
- Wenn eine Datenbank kompromittiert wurde, ist es mitunter nur schwer nachvollziehbar, auf welche Tabellen zugegriffen wurde, ob sich der Angreifer mit den erbeuteten Informationen Zugang zu anderen Teilen des Systems verschaffen kann usw.
- Der Angreifer kann an mehreren Angriffspunkten in das System eingedrungen sein.

Jedes dieser Probleme erfordert eine andere Lösung, die auf die jeweilige Situation zugeschnitten sein muss. Müssen Sie ein schnelles Software-Update durchführen oder eine gefährdete Bibliothek reparieren? Müssen Sie eine IP-Adresse oder einen Port sperren, um weitere Angriffe zu verhindern? Die Antwort kann eine Kombination aus mehreren Lösungen sein. Die Auswahl der richtigen Reaktionsmaßnahmen ist genauso wichtig wie die Entdeckung der Sicherheitsverletzung selbst.

Fehlalarme

Im Sicherheitskontext handelt es sich bei Fehlalarmen um gutartige Aktivitäten, die fälschlicherweise als Sicherheitsbedrohung identifiziert werden. Ein Datenbankadministrator hat vielleicht einen großen Datenexport gestartet und ist in die Mittagspause gegangen. In der Zwischenzeit lässt ein Mitarbeiter im Bereich Netzwerksicherheit seine Mittagspause ausfallen, weil er ein hohes Volumen an Netzwerkverkehr sieht, mit dem er nicht gerechnet hat. Und das, obwohl er sich ein besonders leckeres Sandwich ausgesucht hatte! Was für eine Verschwendung!

Fehlalarme kosten nicht nur Zeit und verursachen unnötige Störungen, sondern lassen auch echte Sicherheitsverletzungen durchs Netz schlüpfen. Mit der Alarmmüdigkeit verhält es sich wie mit dem Sprichwort „Wer einmal lügt, dem glaubt man nicht“. Angenommen, ein Anwendungssicherheitsteam erhält im Durchschnitt zehn Sicherheitswarnungen pro Tag, aber nur zwei davon sind echte Bedrohungen. Ein paar Tage lang ist das kein Problem, aber ein wochenlanges Auftreten von Fehlalarmen führt dazu, dass das Team diesen Meldungen letztendlich keine große Aufmerksamkeit mehr schenkt. Immerhin ist die Wahrscheinlichkeit groß, dass es sich nicht um eine echte Bedrohung handelt!

Fehalarme stellen also eine besonders große Herausforderung für Sicherheitsteams dar. Sie vergeuden nicht nur die wertvolle Zeit der Sicherheitsexperten, sondern können auch dazu führen, dass mehr Sicherheitsbedrohungen die Verteidigungslinie durchdringen.

Triage von Vorfällen

Die Triage von Sicherheitsvorfällen hat viele Gemeinsamkeiten mit der MTTR. Während es sich bei der MTTR um die Zeit handelt, die zur Behebung eines Problems benötigt wird, geht es bei der Triage um die Priorisierung der Maßnahmen zur Behebung eines Vorfalls.

Wie bei allen anderen in diesem Abschnitt beschriebenen Herausforderungen ist auch hier der Kontext entscheidend. Sie müssen sich über die Auswirkungen der Sicherheitslösung im Klaren sein, um negative Folgen minimieren zu können. Wenn es beispielsweise zu einer Datenbankverletzung kommt, haben Sie die Möglichkeit, die Datenbank herunterzufahren. Es kann jedoch sein, dass diese Datenbank für geschäftskritische Aktivitäten verwendet wird. Wenn das der Fall ist, gibt es vielleicht eine weniger offensichtliche, aber ebenso effektive Lösung.

Viele Sicherheitsverletzungen, wie Datenbankverletzungen, erfordern eine sofortige Reaktion. In solchen Fällen müssen Sicherheitsteams so schnell wie möglich handeln. Allerdings kann die Lösung für den falschen Kontext am Ende schlimmere Folgen haben als das Problem selbst.

Damit sind wir wieder bei der Silo-Problematik. Wenn Sicherheitsteams nur das sehen, was sich in ihren eigenen Silos befindet, können Sicherheitsmaßnahmen langsam, ineffektiv, ineffizient und letztlich störend sein.

ERINNERN

Bei der Sicherheit spielt Kontext eine entscheidende Rolle. Kontext, Kontext, Kontext!

IN DIESEM KAPITEL

- Konsolidierung der Erkennungsanalyse
- Untersuchung und Behebung von Bedrohungen
- Vorteile der Orchestrierung und Automatisierung

Kapitel 3
XDR: Integration des Sicherheits-Stacks

Ein unzusammenhängender Sicherheits-Stack kann viel Ärger verursachen. Oft fehlt Sicherheitsexperten der nötige Kontext, um Sicherheitsprobleme schnell und effizient anzugehen. Alarmmüdigkeit führt dazu, dass tatsächliche Sicherheitsprobleme unbeachtet bleiben, während das überlastete Sicherheitspersonal zu viel Zeit mit der Untersuchung von Fehlalarmen verschwendet.

XDR-Lösungen (Extended Detection and Response) bieten zahlreiche Vorteile. Der wichtigste davon ist ihre Fähigkeit, den Sicherheits-Stack zu integrieren. Analysen, Schwachstellenbehebung und automatisierte Aufgaben können optimiert werden, wenn es möglich ist, den gesamten Kontext des Sicherheits-Stacks zu verstehen und zu nutzen. In diesem Kapitel wird erläutert, wie XDR dies alles zusammenführt.

Erkennungsanalyse

Bei der Erkennungsanalyse geht es nicht nur darum, was Sie sehen, sondern auch, was Sie daraus lernen können. Security Operations (SecOps) bedeutet, Sicherheitsbedrohungen wirksam zu begegnen und gleichzeitig zu lernen, wie man in Zukunft am besten mit ähnlichen Bedrohungen umgehen kann. Dazu ist oft mehr erforderlich, als nach ähnlichen Software-Schwachstellen wie in der Vergangenheit zu suchen oder zu

überlegen, wie eine bestimmte Malware das System erneut infizieren könnte.

TIPP

Besonders hilfreich ist es, die von Angreifern verwendeten Angriffsmuster und Strategien zu erkennen. Es gibt ständig neue Bedrohungsarten und Angriffsmethoden, deshalb versucht eine gute Erkennungsanalyse, beides zu berücksichtigen.

Die Analysefähigkeiten der XDR-Plattformen beruhen auf Integration. XDR betrachtet und aggregiert unter anderem die folgenden Quellen:

- **Endpunkte:** Dazu gehören Mitarbeitergeräte wie Workstations, Laptops, Smartphones, Tablets und IoT-Geräte.
- **Netzwerke:** Dies umfasst unter anderem öffentliche und private Netzwerke und virtuelle Private Clouds.
- **Anwendungen:** Dazu gehören E-Mail-Programme und von Mitarbeitern genutzte SaaS-Lösungen (Software-as-a-Service), z. B. der Zugriff über einen Webbrowser.
- **Cloud:** Zu Cloud-Services können Cloud-Datenbanken, Managementtools und andere Services gehören.

Mit XDR können Sicherheitsteams über all diese Teile einen Überblick gewinnen und herausfinden, wie sie miteinander kommunizieren, was wohin verschoben wurde usw. Was können Sicherheitsteams dank dieser Integration sehen und wie verändert sich dadurch ihre Arbeitsweise?

Aggregierte Bedrohungsdaten und Visualisierungen

Ein wesentliches Merkmal vieler XDR-Lösungen ist eine aggregierte Ansicht aller Bedrohungsinformationen. Wie diese aussieht, ist von Plattform zu Plattform unterschiedlich. Im Kern geht es jedoch um lesbare Visualisierungen der relevanten Sicherheitsinformationen.

Da XDR vom Endpunkt bis zum Sicherheitsteam reicht, kann die Plattform den Sicherheitsexperten eine durchgängige Ansicht des Sicherheitsproblems bieten. Sie können nicht nur sehen, welchen Endpunkt (bzw. welche Endpunkte) Angreifer als Einstiegspunkt genutzt haben könnten, sondern auch die Warnmeldungen, die darauf aufmerksam gemacht haben, welche Ressourcen von dem Angriff betroffen sein könnten und viele weitere Informationen.

ERINNERN

XDR-Plattformen verarbeiten eine Fülle von Informationen und können diese auf zugängliche Weise organisieren, sodass die Aggregation von Bedrohungsdaten in diesem Kontext fast einer Überprüfung in Echtzeit gleichkommt. Deshalb sehen Sie die relevanten Sicherheitsinformationen direkt nach dem Sicherheitsvorfall.

Wie all diese Informationen dem Sicherheitspersonal angezeigt werden, hängt von der jeweiligen XDR-Plattform ab. Es gibt jedoch einige gängige Methoden zur Visualisierung von Sicherheitsinformationen:

- **Dashboards:** Viele Plattformen weisen ein Dashboard auf, in das unterschiedliche Informationsquellen integriert werden können, was die Kontrolle und Überwachung vereinfacht.
- **Bedrohungskarten:** XDR-Plattformen verfügen oft über Tools zur Visualisierung der Infrastruktur, die die Beziehungen zwischen Services oder Ressourcen sichtbar machen. Dabei kann es sich um ein Knotendiagramm, eine Karte oder eine andere Darstellung der relevanten Sicherheitsinformationen handeln.
- **Kundenspezifische Anpassung:** XDR-Plattformen bieten Benutzern oft die Möglichkeiten, selbst zu entscheiden, wie und wo all diese Ressourcen dargestellt werden sollen.

TIPP

Jedes Unternehmen stellt andere Anforderungen an seine Sicherheitslösungen. Flexibilität bei der Überwachung und Bedrohungsanalyse ist daher unerlässlich. Dashboard-Komponenten visualisieren Sicherheitsprobleme oft im Zeitverlauf, zum Beispiel in Form von Liniendiagrammen, die die Anzahl der Eindringversuche in das Netzwerk in den letzten sechs Monaten oder die Reaktionszeiten für die Erkennung und Beseitigung von Malware anzeigen.

Mithilfe der Mapping-Funktionen von XDR erhalten Sicherheitsteams eine durchgängige Sicht auf Sicherheitsverletzung - wo sie begonnen hat, in welchem Stadium sie sich befinden und welche anderen Ressourcen sie potenziell beeinträchtigen könnten. Dieser Punkt ist so wichtig, dass er seinen eigenen Abschnitt verdient!

Korrelation und Kontextualisierung

Kontext und Korrelation – und deren Transparenz - sind die (gar nicht so geheimen) Geheimwaffen von XDR. Im Bereich der IT-Sicherheit lassen sich diese beiden Begriffe folgendermaßen definieren:

- **Kontext** hilft bei der Beantwortung der Frage, warum ein Sicherheitsproblem aufgetreten ist. Im Idealfall bindet der Kontext das Sicherheitsproblem in eine Gesamtperspektive ein und zeigt die möglichen Auswirkungen eines Angriffs oder einer Lösung auf.
- **Korrelation** sollte die Frage beantworten, wo ein Sicherheitsproblem aufgetreten ist, welche Ressourcen betroffen sind und worauf sich diese kompromittierten Ressourcen auswirken können.

XDR-Plattformen konzentrieren sich auf den Endpunkt und arbeiten sich von dort aus vor. Auf diese Weise werden alle Sicherheitstools des Ökosystems sichtbar gemacht. Ohne einen klaren Überblick über das gesamte Ausmaß eines Angriffs - vom Endpunkt über das Netzwerk bis hin zu den Anwendungen – ist es schwierig, Bedrohungen einzuschätzen und zu beseitigen. IT-Sicherheitsverletzungen stellen heute vor allem aus den folgenden drei Gründen eine große Herausforderung dar:

- Die Zahl der potenziellen Angriffspunkte ist in den letzten Jahren angestiegen.
- Die Komplexität und Raffinesse der Angriffe haben zugenommen.
- Diese neuen Herausforderungen haben dazu geführt, dass Sicherheits-Stacks komplizierter geworden sind.

Visualisierung ist eine der wichtigsten Funktionen von XDR-Plattformen, die Sicherheitsteams bei der Bewältigung dieser neuen Herausforderungen unterstützen. Die XDR-Funktionen zur Darstellung von Bedrohungen (Mapping) zeigen die Zusammenhänge zwischen unterschiedlichen Systemen auf, die direkt oder indirekt an einem Angriff beteiligt sind. Wird zum Beispiel Malware entdeckt, lässt sich die Schadsoftware mithilfe einer Bedrohungskarte zu einem Endpunkt (Laptop) zurückverfolgen, auf dem ein Mitarbeiter die E-Mail eines Angreifers geöffnet hat.

Und wie sieht es mit dem Kontext aus? Angenommen, mitten in der Nacht gibt es eine große geplante I/O-Spitze: Ein einfacher Alarmauslöser liefert nicht den gesamten Kontext. Der Alarm wurde möglicherweise ausgelöst, weil die I/O-Spitze verdächtig erschien, obwohl es sich in Wirklichkeit um einen geschäftskritischen Vorgang handelte. Ein erweiterter Kontext sorgt dafür, dass Sicherheitsteams - und ihre Warnsysteme – mehr Informationen über die Ereignisse erhalten. Fehlalarme kosten Zeit und Energie und können sogar dazu führen, dass Teams aufgrund von Alarmmüdigkeit tatsächliche Bedrohungen übersehen.

Deshalb liefern Korrelations- und Kontextualisierungsfunktionen Sicherheitsteams ein ganzheitliches Bild. Die nächste Frage ist: Was kann man mit diesen Erkenntnissen tun?

Erkennung von Bedrohungen und die entsprechende Reaktion

Dank der XDR-gestützten Korrelation und Kontextualisierung lassen sich Bedrohungen einfacher erkennen. XDR reduziert nicht nur die Zeit, die zur Ermittlung des Angriffsortes und der weiterreichenden Folgen eines Angriffs benötigt wird, sondern hat auch direkte Auswirkungen darauf, wie Sicherheitsexperten mit einer Bedrohung umgehen.

Mit dem Full-Stack-Ansatz von XDR und der Möglichkeit, umfassende Sicherheitsverläufe zu erstellen, können Teams Anomalien eindeutig als solche identifizieren.

Eine Zunahme der Aktivität auf Server A, der ein Aktivitätsanstieg auf Server B folgt, könnte auf eine normale Geschäftsaktivität hindeuten. Wenn Ihre Sicherheitssysteme zusammenarbeiten, sind sie in der Lage, derartige Muster zu erkennen und diese Informationen dann auf zukünftige Angriffe anzuwenden. Was passiert, wenn Server B einen Aktivitätsanstieg verzeichnet, während auf Server A nichts passiert? Die XDR-Lösung erkennt, dass es sich um anomales Verhalten handelt, und löst eine Reaktion aus.

Durch Analysen wird auch die Formulierung von Reaktionsmaßnahmen beschleunigt. Der kompromittierte Server B wird nun erneut untersucht. Möglicherweise führt er eine Software mit einer bekannten Schwachstelle aus. Da das Sicherheitsteam diesen Server bereits als Problembereich identifiziert hat, kann es schnell nach bekannten Schwachstellen in der Software suchen und sie bei Bedarf reparieren.

Die Analyse von Bedrohungsdaten hilft Sicherheitsteams nicht nur dabei, intelligenter zu handeln, sondern auch schneller zu reagieren. Server B könnte während des Angriffs geschäftskritische Daten an Server C weiterleiten, weshalb er nicht heruntergefahren bzw. seine Verbindung nicht unterbrochen werden kann. Das Sicherheitspersonal weiß Bescheid, da es eine ganzheitliche Sicht auf die Ereignisse hat, und kann einen neuen Plan erstellen, mit dem die Unterbrechung wichtiger Geschäftsabläufe unterbunden wird.

Untersuchung und Behebung von Bedrohungen

Letztendlich spielt es keine Rolle, wie viele Bedrohungen Sie aufspüren, wenn Sie sich dann nicht effektiv um sie kümmern. Es gibt viele Ansätze zur Behebung von Bedrohungen. XDR versucht, Ihnen die Auswahl des richtigen Ansatzes und dessen Umsetzung zu erleichtern.

ERINNERN

XDR verbessert die Behebung auf zwei Arten: Die Plattform unterstützt die Mitarbeiter des Security Operations Center (SOC) und macht die Ereignisverfolgung effektiver.

SOC-Mitarbeiter sind oft überlastet, und das hat Folgen für die Sicherheit. XDR kann diese Belastung verringern, da viele notwendige Sicherheitsprozesse rationalisiert und vereinfacht werden. Auch die Nachverfolgung von Sicherheitsvorfällen wird durch XDR erheblich verbessert. Die Verfolgung des Angriffsverlaufs kann ein großartiges Werkzeug für Sicherheitsteams sein.

Unterstützung für das SOC

SOC-Mitarbeiter müssen viel Arbeit investieren und schnell reagieren können, um mit der aktuellen Bedrohungslage Schritt zu halten. Leider sind viele Sicherheitstools nicht in der Lage, die praktischen Anforderungen des SOC zu erfüllen. Ein ineffizienter Sicherheits-Stack verursacht nicht nur zusätzlichen Stress für Sicherheitsteams. Er kann auch Alarmmüdigkeit hervorrufen, die oft dazu führt, dass Bedrohungen übersehen werden.

Der größte Vorteil, den XDR dem SOC bringt, ist das zentralisierte Dashboard. Das Dashboard vieler XDR-Plattformen dient als zentrale Schnittstelle für den Zugriff auf integrierte Sicherheitsdaten aus dem gesamten Sicherheits-Stack und enthält oft Visualisierungen, Alarmverläufe und -protokolle, anpassbare Informationsfelder und weitere nützliche Elemente.

TIPP

Vielleicht machen Sie sich jetzt Sorgen, dass Alarmmüdigkeit in Dashboard-Müdigkeit umschlagen könnte. Diese Sorge ist unbegründet, da das Dashboard anpassbar ist. Sie können nur das anzeigen lassen, was Sie tatsächlich sehen wollen.

Benutzerdefinierte Analysetools reichern Sicherheitsprobleme mit Kontext an. Dadurch lassen sich Reaktionsmaßnahmen einfacher priorisieren, Fehlalarme werden reduziert und das SOC kann effizienter arbeiten.

Ein weiteres wichtiges Instrument, das XDR für das SOC bereitstellt, ist die Automatisierung der Orchestrierung. SOC-Mitarbeiter sind qualifizierte und erfahrene Sicherheitsexperten, die ihre wertvolle Zeit nicht mit Aufgaben verschwenden sollten, die automatisiert werden können.

Ein kompromittierter Endpunkt wie ein Laptop kann mit den richtigen Automatisierungsauslösern schnell aus dem Netzwerk ausgesperrt werden. Ein Mensch bräuchte für diese Aufgabe viel mehr Zeit, die anderweitig besser genutzt werden könnte. Menschliches Eingreifen sollte erst dann erforderlich sein, wenn es um schwierigere Aufgaben im Zusammenhang mit der Planung und Entscheidungsfindung geht.

ERINNERN

Bei der Automatisierung geht es nicht nur darum, Zeit zu sparen. Durch sie kann auch der gesamte Reaktionsprozess beschleunigt werden.

Verfolgung von Vorfällen

XDR bietet noch einen weiteren entscheidenden Vorteil für Sicherheitsteams: Angriffsverläufe. XDR-Plattformen verfügen über anpassbare Dashboard-Module – manchmal sogar spezielle Dashboards – zur Nachverfolgung und Protokollierung früherer Sicherheitsverletzungen. Manchmal werden Ereignisse für jedes System getrennt verfolgt, z. B. durch die separate Auflistung von Datenbankverletzungen und Netzwerkangriffen, oder nach Art des Angriffs, etwa durch Auflistung aller DDoS-Angriffe.

Die Erkennung von Angriffsmustern kann nützliche Erkenntnisse über zukünftige Angriffe liefern. Wenn eine Sicherheitsverletzung festgestellt wird und Teams ein bestimmtes Verhalten wiedererkennen – das sie vielleicht schon oft gesehen haben – ist der Umgang mit der Bedrohung wesentlich einfacher.

Durch einen Verlauf früherer Angriffe können Sicherheitsteams institutionelles Wissen über gängige Angriffsarten und -muster entwickeln. In der Historienansicht sollten Bedrohungsdaten aus internen und externen Quellen korreliert werden. Diese sollten auch entsprechende Verfallsdaten für Informationen enthalten, besonders im Fall von IPs, die leicht den Besitzer wechseln und eine wichtige Ressource auf der Blockierungsliste hinterlassen können. Mit XDR können SOC-Teams gängige Bedrohungen schneller erkennen und effizienter auf sie reagieren – dank des von den Sicherheitsteams selbst zusammengetragenen Wissens.

Um noch einmal auf das Beispiel des kompromittierten Servers B zurückzukommen: Angenommen, der Aktivitätsanstieg wird als Bedrohung erkannt. Die aus dem Angriffsverlauf gewonnenen Erkenntnisse

können Sicherheitsteams dabei helfen, die Art der Aktivität sowie frühere und aktuelle Muster zu erkennen. Dadurch wissen sie genau, um welche Art von Angriff es sich handelt, und haben eine gute Vorstellung davon, woher die Bedrohung kommt.

Diese Art von historischen Informationen erstreckt sich auch auf die Reaktionsmaßnahmen selbst. Wenn diese Art von Angriff schon einmal vorgekommen ist, dann haben sich die Sicherheitsteams auch schon einmal damit befasst. Bei der Verfolgung von Vorfällen geht es nicht nur darum, Probleme zu identifizieren: Ebenso wichtig ist es, herauszufinden, wie man in Zukunft besser mit diesen Problemen umgehen kann.


TIPP

Wenn ein Angreifer Ihnen Zitronen in Form von Malware gibt, machen Sie Limonade draus! Pressen Sie auch das letzte Quäntchen an Informationen aus dem Verlauf der Sicherheitsverletzungen heraus. Angriffe sind schlimm, während sie stattfinden, doch danach verwandeln sie sich in eine äußerst nützliche Sicherheitsressource.

Automatisierung der Orchestrierung

Durch Orchestrierung unterstützen XDR-Plattformen die Automatisierung von Aufgaben, für die Informationen aus dem gesamten Sicherheits-Stack erforderlich sein können. Dazu gehört die Integration unterschiedlicher Sicherheitstools, damit Automatisierungsaufgaben von unterschiedlichen Sicherheitsperspektiven profitieren können, sowie die Durchführung der eigentlichen Automatisierungsaufgaben.

Integration mehrerer Sicherheitstechnologien

Das System von Sicherheitstools, aus denen ein Sicherheits-Stack besteht, ist relativ kompliziert. Wenn diese Tools jedoch über XDR integriert werden, lassen sich Automatisierungsskripte und -aufträge vereinfachen. Wie bei vielen anderen Aufgaben des SOC wird auch die Automatisierung durch fehlenden Kontext behindert. Mit einer Gesamtansicht des Technologie-Stacks können Automatisierungsaufgaben komplexere, anspruchsvollere Auslöser haben, die effizienter und konsequenter auf tatsächliche Bedrohungen reagieren.

Bei einer isolierten Endpunktlösung lassen sich durch die Automatisierung möglicherweise nur einige Endpunktverletzungen abfangen. Informationen über die Netzwerksicherheit und Protokolle zur Vorfallreaktion gibt es keine. Durch Orchestrierungsfunktionen wird die Effektivität der Sicherheitsmaßnahmen im gesamten Stack erhöht.

TIPP

Die Lösung darf nicht schlimmer als das Problem sein. Vermeiden Sie benutzerdefinierte Ad-hoc-Skripte für jede neue Reaktionsmaßnahme. Sicherheitsexperten sollten nicht auch noch für die Wartung von Software zuständig sein.

Außerdem muss sich jemand auch um die Automatisierungsskripte selbst kümmern. Für Automatisierungsaufgaben in isolierten Umgebungen wird oft ein Aufpasser benötigt. Software-Updates und Änderungen von Compliance-Anforderungen oder Sicherheitstools können die normale Verwendung von Ad-hoc-Skripten beeinträchtigen.

Wenn integrierte Sicherheitstools für Automatisierungsaufgaben zur Verfügung stehen, können Sicherheitsteams mehr Informationen und eine stabilere Umgebung nutzen. Ausnahmefälle mit benutzerdefinierten Automatisierungsskripten können in eine größere Automatisierungslösung integriert werden. Das Ergebnis: weniger Aufsicht und weniger Skripte, die nachverfolgt werden müssen.

ERINNERN

Ad-hoc-Automatisierung ist nicht dasselbe wie Automatisierung!

Automatisierte Reaktionsmaßnahmen

Integration und Reichweite sind vorhanden, doch was wird durch die Automatisierung tatsächlich erreicht?

Mit XDR können Sicherheitsteams feiner abgestimmte Automatisierungsaufgaben durchführen als mit anderen Sicherheitslösungen. Der Umfang des Sicherheits-Stacks und der Angriffsverlauf sorgen dafür, dass XDR-Automatisierungsaufgaben fundierte Pläne für zukünftige Angriffe sind.

Das folgende Beispiel soll dies demonstrieren: Es wurde festgestellt, dass auf einem Endpunkt Malware ausgeführt wird. Das Sicherheitspersonal hat eine Automatisierungsaufgabe zur Reaktion auf diese Art von Bedrohung erstellt. Diese Aufgabe umfasst eine bestimmte Folge von Aktionen zur anfänglichen Bedrohungsabwehr. In diesem Fall könnte es sich dabei um die Trennung des Endpunkts vom Rest des Netzwerks und die Ausführung von Antimalware-Software auf dem infizierten Rechner handeln.

Bei einer Datenpanne kann eine komplexere Folge automatisierter Maßnahmen erforderlich sein, um angemessen auf den Vorfall zu reagieren. Einige Datenbanken können nicht einfach heruntergefahren werden, da sie möglicherweise für geschäftskritische Aufgaben benötigt werden. Stattdessen könnte es eine anhand bestimmter Kriterien automatisierte Reaktion geben, dass eine infizierte Datenbank nicht heruntergefahren werden kann und daher eine Firewall-Regel geändert wird, um die Datenübertragung von dem betroffenen Server zu stoppen.

IN DIESEM KAPITEL

- Was ist SIEM und was wird damit überwacht?
- Was ist SOAR und was wird damit erreicht?
- So interagieren SIEM und SOAR mit XDR

Kapitel 4
XDR, SIEM, SOAR: Freund oder Feind?

Ich kann nicht über Extended Detection and Response (XDR) sprechen, ohne auch auf die beiden größten Vorgänger dieser Technologie einzugehen: Security Information and Event Management (SIEM) und Security Orchestration Automation and Response (SOAR). SIEM und SOAR sind zwei der bekanntesten Sicherheitstools auf dem Markt, die sich als ganzheitliche Problemlöser präsentieren.

Sie verfolgen unterschiedliche Ansätze zur Optimierung des IT-Sicherheits-Stacks und liefern unterschiedliche Ergebnisse für den Kunden. Obwohl XDR in das Territorium von SIEM und SOAR vordringt, sind die alten Standards mit dem Neuankömmling nicht völlig unvereinbar.

SIEM

Security Information and Event Management (SIEM) ist eine Sicherheitslösung, die Daten aus der gesamten Sicherheitsinfrastruktur erfasst und so viele Protokolle und Warnmeldungen wie möglich bereitstellt. SIEM konzentriert sich auf die Erfassung roher Sicherheitsinformationen, was sowohl Vor- als auch Nachteile hat.

ERINNERN

Manchmal braucht ein Unternehmen einfach möglichst viele Protokolle. Branchen, in denen die Einhaltung von Vorschriften eine große Rolle spielt, z. B. im Gesundheits- oder Finanzwesen, benötigen oft große Mengen an Daten über ihre internen Systeme. In vielen andere Branchen ist es jedoch nicht so wichtig, über jede Auffälligkeit auf dem Sicherheitsradar informiert zu sein. In vielen Fällen handelt es sich bei diesen Auffälligkeiten nicht um Angriffe. In den folgenden Abschnitten werden einige der Funktionen von SIEM-Lösungen und ihre Bedeutung für Sicherheitsteams erläutert.

Wo wird gesucht?

Die Kurzfassung ist: SIEM-Lösungen suchen dort, wo sie suchen sollen. SIEMs sind im Laufe der Zeit immer besser darin geworden, Informationen zu sammeln und sie an einem zentralen Ort zur Analyse zusammenzufassen. Die Fähigkeiten von SIEM zur Datenerfassung hängen von den zu überwachenden Produkten und Tools ab.

SIEM ist ein bewährtes Sicherheitstool, das versucht, bisher isolierte Systeme zu integrieren, die überwacht werden müssen. SIEM-Tools überwachen zum Beispiel:

- Firewall-Ereignisse
- IoT-Geräte
- Sicherheitsgeräte
- Antivirus-Software
- Anwendungen

Ereignisprotokolle werden zur Verarbeitung und Analyse an einem zentralen Ort erfasst. Zu den jüngsten Ergänzungen im SIEM-Bereich zählen einige automatisierte Verarbeitungsfunktionen, Orchestrierungstools und andere Fähigkeiten, die bisher ausschließlich SOAR-Lösungen vorbehalten waren.

SIEM-Lösungen verwenden unterschiedliche regelbasierte Systeme, um verdächtige Aktivitäten auf den überwachten Ressourcen zu erkennen. Wenn ein Verhalten als potenzielle Sicherheitsverletzung eingestuft wird, werden Warnmeldungen an einen zentralen Zugriffspunkt gesendet, damit das Sicherheitspersonal sie überprüfen und eine Entscheidung über die weitere Vorgehensweise treffen kann.

SIEM-Tools gibt es schon seit geraumer Zeit und sie haben ihre Nützlichkeit wiederholt unter Beweis gestellt. Diese Art von Sicherheitslösung hat aber auch einige Einschränkungen. Einige neuere Lösungen

haben diese überwunden und gleichzeitig die Hauptvorteile von SIEM beibehalten.

Das Ergebnis: eingeschränkte Transparenz

SIEM ist in der Lage, die Warnmeldungen eines ganzen Sicherheits-Stacks zu verwalten. Dies kann ein sehr nützliches Werkzeug sein, überraschenderweise aber auch den Überblick des Sicherheitsteams über das gesamte Ökosystem einschränken. Alarmmüdigkeit und Fehlalarme stellen eine unnötige Belastung für das Sicherheitspersonal dar und können dazu führen, dass tatsächliche Bedrohungen übersehen werden.

Alarmmüdigkeit stellt sich oft ein, wenn ein Sicherheitssystem so viele Warnmeldungen ausgibt, dass Sicherheitsteams mit der Überprüfung der Bedrohungen überfordert sind. Für die zunehmende Anzahl von Warnmeldungen gibt es mehrere Gründe:

- Aufgrund der Isoliertheit der Systeme können Sicherheitsteams oft nicht klar erkennen, welches Verhalten tatsächlich verdächtig ist.
- Warnmeldungen haben keinen ausreichenden Kontext und sind daher ungenau.
- Das Warnsystem selbst ermöglicht keine detaillierten Kontrollen von Warnmeldungen, um sie auf spezifische Bedürfnisse abstimmen zu können.

Wenn Alarmmüdigkeit einsetzt, ignorieren Sicherheitsteams mit größerer Wahrscheinlichkeit Bedrohungen, auf die sie eigentlich reagieren müssten. Während Mitarbeiter mit irrelevanten Alarmen beschäftigt sind, werden tatsächliche Sicherheitsprobleme übersehen.

Isolierte Systeme und weit gefasste Alarmkriterien führen ebenfalls zu Fehlalarmen. Ohne den Kontext des größeren IT-Ökosystems sind Warntools oft nicht in der Lage, aktuelle Ereignisse in Systemen richtig zu interpretieren, oder sie warnen vor nicht vorhandenen Sicherheitsbedrohungen. Wenn bei einem Server am Wochenende ein Aktivitätsanstieg auftritt, kann dieses vermeintlich verdächtige Verhalten eine Warnmeldung auslösen, obwohl es sich bei der Aktivität um einen geplanten Auftrag handelt, der eigentlich außerhalb der Hauptgeschäftszeiten laufen sollte.

Fehlalarme vergeuden die Zeit von Sicherheitsteams und tragen zur Alarmmüdigkeit bei. Da kann es irgendwann passieren, dass Warnmeldungen nur eine niedrige Priorität eingeräumt wird, weil es sich dabei wahrscheinlich nicht um echte Bedrohungen handelt. Warnmeldungen

sollten immer ernst genommen werden und sie sollten Teams die Informationen liefern, die sie benötigen.

ERINNERN

Qualität geht vor Quantität. Sicherheitsteams brauchen aussagekräftige Informationen, aber nicht zu viele davon.

SOAR

SOAR-Lösungen (Security Orchestration, Automation and Response) befassen sich hinsichtlich Sicherheit eher mit Vorbereitungs- und Reaktionsmaßnahmen. Damit scheinen sie XDR-Plattformen auf den ersten Blick recht ähnlich zu sein. Der Hauptunterschied zwischen SOAR und XDR besteht in der Integration, die beeinflusst, was Sicherheitsteams in welcher Form tun können.

Was wird damit erreicht?

SOAR-Lösungen zielen darauf ab, die Orchestrierung und die Reaktion auf Sicherheitsvorfälle durch Automatisierungstools zu optimieren. SOAR – der Begriff wurde 2017 von Gartner geprägt – ist eine relativ neue Kategorie von Sicherheitstools, die Anwendern neue Möglichkeiten zur Bewältigung von Bedrohungen bieten.

Im Mittelpunkt von SOAR-Plattformen steht das „Playbook" – ein Orchestrierungstool, das von Sicherheitsteams erstellt werden kann, um eine Folge von Aktionen zur Bedrohungsabwehr zu planen. Ein Teil dieses Plans kann durch Automatisierung optimiert werden, für die zur Leistungsverbesserung oft maschinelle Lernverfahren zum Einsatz kommen.

SOAR-Lösungen können jedoch nicht eigenständig eingesetzt werden. Daher bieten sie Integrationsmöglichkeiten mit anderen Sicherheitstools wie NDR-Lösungen (Network Detection and Response). Mithilfe von Playbooks und automatisierten Funktionen kann SOAR dann auf die von den anderen Tools generierten Informationen reagieren.

Diese Plattformen sind leistungsstarke Tools zur Orchestrierung von Sicherheitsreaktionen, doch sie haben auch einige Nachteile. Obwohl sich SOAR-Plattformen mit anderen Sicherheitstools integrieren lassen, ist es oft mühsam, sie in Gang zu bringen. Darüber hinaus fehlt es ihnen an umfassenden Erkennungsfunktionen.

Das Ergebnis: eine Belastung für SecOps-Teams

SecOps-Teams (Security Operations) sind für die Sicherung von Unternehmensressourcen und -systemen verantwortlich. Unter ihre Aufsicht

fallen Netzwerke, Anwendungen sowie Kunden- und Geschäftsdaten. Bei diesen vielen Aufgaben ist es nicht leicht, den Überblick zu behalten. SecOps-Teams brauchen keine zusätzlichen Belastungen, die sie bei der Arbeit ausbremsen.

SOAR-Lösungen können häufig mit zahlreichen Sicherheitstools integriert werden, die schon in Ihrer Sicherheitsinfrastruktur vorhanden sind. Manchmal ist zusätzlicher Aufwand jedoch unvermeidlich, um eine Kompatibilität zwischen SOAR und den anderen Tools herzustellen. Viele SOAR-Tools haben einen unzureichenden API-Zugang, sodass die vollständige Integration der von Ihnen benötigten Sicherheits- bzw. Beobachtungstools schwierig, wenn nicht gar unmöglich ist.

Dies kann Workflow-Unterbrechungen und eine eingeschränkte Bedrohungserkennung zur Folge haben. Die daraus entstehenden Sicherheitslücken versucht man dann mit zusätzlichen Sicherheitstools zu schließen. Alle drei Faktoren erhöhen die Arbeitsbelastung für SecOps-Teams und beeinträchtigen ihre Effizienz. Jedes neue Tool im Sicherheits-Stack ist eine potenzielle neue Schwachstelle, eine neue Lösung, die integriert und erlernt werden muss, und eine neue Belastung für das ohnehin schon viel beschäftigte Sicherheitspersonal.

ERINNERN

SOAR ist ein leistungsfähiges Sicherheitstool, doch es kann SecOps-Teams auch unnötige Kopfschmerzen bereiten – besonders in Anbetracht der jüngsten Entwicklungen im Bereich von XDR-Plattformen und ihren Fähigkeiten.

Alles zusammenbringen

So wie SIEM und SOAR kann auch XDR nicht eigenständig arbeiten. XDR muss von anderen Sicherheitstools unterstützt werden, die ihm die benötigten Informationen liefern und seine Funktionslücken schließen. SIEM und SOAR sind kompetente Sicherheitslösungen, die sich für viele Unternehmen als äußerst nützlich erwiesen haben. XDR ist neu und vielversprechend. Das heißt jedoch nicht, dass die gängigeren Tools ausrangiert und vergessen werden sollten.

SIEM und SOAR können XDR unterstützen

XDR hat Unternehmen viel zu bieten, doch es ist keineswegs ein Allheilmittel. Eine erfolgreiche XDR-Bereitstellung muss von anderen Sicherheitstools unterstützt werden und könnte – je nach den konkreten Anforderungen eines Unternehmens – von den Stärken von SIEM- oder SOAR-Lösungen profitieren.

Da SIEM ein so leistungsstarkes Tool für die Protokollierung und Benachrichtigung ist, kann es die Analysefunktionen von XDR durch die Bereitstellung umfassender Protokolldaten unterstützen. XDR ist in der Lage, große Mengen an Sicherheitsinformationen zu verarbeiten. Eine Flut von SIEM-Protokollen sollte daher nicht zum Verlust kritischer Informationen oder zu verpassten Warnmeldungen führen. Teams, die XDR einsetzen, können SIEM-Lösungen auch zur Erfüllung ihrer Compliance-Anforderungen nutzen. Einige Unternehmen benötigen eine beträchtliche Anzahl an Protokollen zur Einhaltung von Branchenstandards, und XDR kann dafür als Analyse- und Organisationstool verwendet werden.

Die Integration von SOAR mit XDR ist allerdings eher ein Ausnahmefall. XDR-Lösungen bieten umfassende Orchestrierungs- und Automatisierungstools – und genau das ist das große Verkaufsargument für SOAR. XDR kann für seine Analysefunktionen und Tools verwendet werden, während eine ergänzende SOAR-Lösung für viele der Automatisierungs- und Orchestrierungsaufgaben eingesetzt wird. Dies ist eine Möglichkeit für jene, die das SOAR-Produkt gern in ihrer Sicherheitsumgebung weiterverwenden möchten. Ihre Sicherheitsteams möchten vielleicht die Playbook- und Automatisierungsfunktionen von SOAR beibehalten und sich die Analysen und die zentralisierte Ansicht von XDR zunutze machen, ohne die anderen Tools zu verwenden.

ERINNERN

XDR sollte nicht lediglich als Ersatz für bestehende Sicherheitslösungen betrachtet werden, sondern stattdessen als eine willkommene Bereicherung der Sicherheitslandschaft. In vielen Fällen kann XDR bestehende Tools ersetzen. Ein besonderer Vorteil dieses Produkttyps ist jedoch seine Integrationsfähigkeit: Es lässt sich leicht in bereits bestehende Sicherheitsumgebungen einfügen.

Zentralisierung von Sicherheitsinformationen

XDR lässt sich nicht zuletzt deshalb so effektiv in die bestehende Sicherheitsinfrastruktur integrieren, weil seine Hauptfunktion die Zentralisierung von Sicherheitsinformationen ist. XDR-Plattformen zentralisieren die von Sicherheitsteams benötigten Informationen mithilfe der folgenden Merkmale:

- **Anpassbares Dashboard:** XDR-Lösungen verfügen häufig über mindestens ein zentrales Dashboard mit konfigurierbaren Beobachtungsbereichen. Diese Bereiche können verschoben werden, um verschiedene Teile Ihrer Sicherheitsinfrastruktur, Warnmeldungen, den Angriffsverlauf usw. anzuzeigen.

- **Vorfallkarten:** Dabei handelt es sich um Visualisierungen von Sicherheitsvorfällen, die zeigen, welche Systeme von einem Angriff betroffen waren und welche anderen Systeme noch betroffen sein könnten. Sie sind mit epidemiologischen Karten vergleichbar, die zur Untersuchung der Ausbreitung von Krankheiten verwendet werden, und können Teams dabei helfen, einen Angriff zu seinem Ursprung zurückzuverfolgen.
- **Zugang zu unterstützenden Sicherheitstools:** Die meisten XDR-Lösungen bieten einfachen Zugang zu den anderen Sicherheitstools, die die Plattform mit Informationen versorgen. Dies wird in der Regel als Teil des zentralen Dashboards oder eines schnell zugänglichen Menüs angezeigt.

Das große Versprechen der Integrationsfähigkeit von XDR wäre nicht viel wert, wenn es keine zentralen Schnittstellen für den Zugriff auf all diese Informationen gäbe. Daher sind XDR-Anbieter sehr daran interessiert, die Benutzerfreundlichkeit und Verständlichkeit ihrer Produkte zu gewährleisten. Zentralisierte Informationen entlasten Sicherheitsteams, verkürzen die zur Bedrohungserkennung und -reaktion benötigte Zeit und geben Sicherheitsexperten die Möglichkeit, künftige Reaktionsmaßnahmen zu verbessern, anstatt sich durch Unmengen von Daten wühlen zu müssen.

Andere wichtige Technologien

Wenn Sie über die Implementierung von XDR nachdenken, sollten Sie auch diese zwei Technologien berücksichtigen: Endpoint Detection and Response (EDR) und Network Detection and Response (NDR). Diese beiden Tools können zu einer erfolgreichen XDR-Bereitstellung beitragen, da sie Sicherheitsteams dabei helfen, die Komplexität von Netzwerk- und Endpunktumgebungen zu meistern.

EDR, manchmal auch als Endpoint Threat Detection and Response oder ETDR bezeichnet, ist so etwas wie ein Verwandter oder Vorläufer von XDR. Diese Lösung führt einige der wichtigsten Funktionen von XDR-Produkten aus und konzentriert sich auf die Überwachung von Endpunkten und die Bedrohungserkennung. Die zentralisierte Ansicht und die Analysefunktionen von XDR-Plattformen sind bei EDR in der Regel nicht vorhanden. Es lohnt sich, diese Lösung im Auge zu behalten, da EDR wahrscheinlich das passende Tool ist, um Ihre zentralisierte XDR-Lösung mit den erforderlichen Endpunktsicherheitsdaten zu versorgen.

NDR ist EDR in vielerlei Hinsicht ähnlich, überwacht jedoch Netzwerkaktivitäten und -ressourcen. NDR kann bei der Erkennung von Netzwerkbedrohungen helfen und automatisierte Reaktionen durchführen – doch auch diese Lösungen verfügen oft nicht über die umfassenden Tools, die XDR zu bieten hat. Ein Tool, das speziell zur Überwachung der Netzwerksicherheit verwendet wird, hat den Vorteil, dass Sie Einblicke in Netzwerkangriffe erhalten, die immer komplexer und vielschichtiger werden. Da es oft mehrere Angriffspunkte gibt, kann ein zielgerichtetes Netzwerksicherheitstool eine Sicherheitsinfrastruktur erheblich bereichern.

ERINNERN

XDR ist keine Lösung, die Ihrem SIEM den Rang ablaufen will! Sie ist eine Plattform, die gut mit vielen bereits vorhandenen Sicherheitstools zusammenarbeitet.

IN DIESEM KAPITEL

- Die XDR-Philosophie von Cisco
- Die SecureX-Plattform

Kapitel 5
Der XDR-Ansatz von Cisco

Cisco Secure verfolgt einen einzigartigen Ansatz zur erweiterten Bedrohungserkennung und -reaktion (Extended Detection and Response, XDR), der sich auf eine Reihe patentierter Tools und maschineller Lernverfahren für die Datenanalyse sowie Automatisierungsfunktionen stützt. Dieser beschleunigt nicht nur die Reaktionszeiten, sondern ermöglicht auch einen proaktiven Umgang mit potenziellen Sicherheitsproblemen.

Der XDR-Ansatz von Cisco Secure baut auf einer integrierten Plattformlösung auf. SecureX bietet vollständige Transparenz über den gesamten Sicherheits-Stack und umfassende Integrationsmöglichkeiten mit Ihrer bestehenden Sicherheitsinfrastruktur. In diesem Kapitel erfahren Sie, wie Cisco Secure die Anforderungen an eine XDR-Plattform definiert.

Die drei Säulen einer effektiven XDR-Plattform

Cisco Secure betrachtet XDR als eine Sicherheitsplattform, die versagt, wenn eine ihrer Komponenten ihre Aufgabe nicht erfüllt. Das X in XDR steht für „extended“ (erweitert), doch erweiterte Erkennung bringt nicht viel, wenn keine leistungsfähigen Analysetools vorhanden sind, die die gewonnenen Erkenntnisse optimal nutzen können. Alle drei Hauptbestandteile einer XDR-Plattform müssen zusammenarbeiten, damit sie das große Versprechen dieses neuen IT-Sicherheitsansatzes erfüllen

können. In diesem Abschnitt werden die drei Säulen der XDR-Philosophie von Cisco Secure sowie die Konzepte erläutert, auf denen SecureX basiert.

X: Große Reichweite

Dank der größeren Reichweite von XDR können Sicherheitsteams nicht nur mehr Bedrohungen schneller erkennen, sondern auch unübersichtliche und komplexe Sicherheits-Stacks vereinfachen. XDR schafft das nicht allein, deshalb ist die Kompatibilität dieser Lösung mit bestehenden Sicherheitslösungen entscheidend, wenn ein vollständiger Überblick über alle Sicherheitsressourcen erreicht werden soll.

Cisco Secure bietet eine Reihe von Sicherheitstools, die sich problemlos in seine Plattform integrieren lassen und nach Ansicht von Cisco die Norm darstellen sollten. Jede lohnenswerte XDR-Plattform sollte über umfassende Integrationsmöglichkeiten verfügen, damit Unternehmen das Beste aus Ihren bereits vorhandenen Tools herausholen und gleichzeitig von den Vorteilen einer XDR-Plattform profitieren können.

Außerdem sollte eine XDR-Plattform Daten aus möglichst vielen Quellen zusammenführen. Jede Ressource und jeder Endpunkt mit erfassbaren Informationen ist ein potenzieller Angriffspunkt und muss überwacht werden. Eine gute XDR-Plattform sollte vollständig mit leistungsstarken NDR- (Network Detection and Response) und EDR-Systemen (Endpoint Detection and Response) kompatibel sein, um eine umfassende Transparenz aller gefährdeten Ressourcen zu gewährleisten.

D: Schnelle, leistungsstarke Analysen

Ebenso wichtig wie die Reichweite ist die Tatsache, dass XDR Sicherheitspersonal in die Lage versetzt, Angriffe als solche zu erkennen und aus ihnen zu lernen. Die XDR-Analyse umfasst zwei wesentliche Aspekte: 1) die Art und Weise, wie Informationen von vorhandenen Tools und den Machine-Learning-Tools der XDR-Lösung verarbeitet werden, und 2) wie Informationen den Sicherheitsteams präsentiert werden.

Aufgrund der Komplexität heutiger IT-Umgebungen gibt es viele Sicherheitsdaten, für die zusätzlicher Kontext erforderlich ist, um sie angemessen interpretieren und darauf reagieren zu können. Diese Datenmengen lassen sich am effizientesten mit auf maschinellem Lernen (ML) basierenden Analysetools verarbeiten. Eine gute XDR-Lösung sollte über leistungsstarke ML-Funktionen verfügen, die Sicherheitsteams effektiv unterstützen können.

ERINNERN

Die Verständlichkeit von Sicherheitsinformationen ist ebenfalls eine Grundvoraussetzung für eine erfolgreiche XDR-Lösung. Dazu gehören benutzerfreundliche Dashboards mit allen benötigten Informationen und Visualisierungstools zur besseren Analyse von Sicherheitsdaten.

Visualisierung sollte Angriffsverläufe, Nutzungsmetriken und Netzwerkaktivitäten umfassen. Darüber hinaus sollte es möglich sein, die Kontaktpunkte einer Bedrohung mit Ihren Systemen darzustellen. XDR-Analysen ermöglichen die schnelle und genaue Erkennung von Bedrohungen, damit Sicherheitsteams Probleme so schnell wie möglich beheben können.

R: Kürzerer Verweilzeit durch Automatisierung

Die Automatisierung spielt im Bereich der IT-Sicherheit schon seit einiger Zeit eine Rolle. Durch XDR-Plattformen wird sie jedoch auf ein völlig neues Niveau gehoben. Bei XDR-Plattformen kann sich die Automatisierung die anderen Stärken der Lösung zunutze machen. Automatisierungspläne sind fundiert, haben Zugriff auf die Erkenntnisse des gesamten Sicherheits-Stacks und können über ein zentrales Dashboard einfach verwaltet werden.

ERINNERN

Diese Vorteile verringern nicht nur die Arbeitsbelastung des Sicherheitspersonals, sondern können auch die Verweildauer von Bedrohungen reduzieren. Automatisierte Reaktionen können den Ball ins Rollen bringen, indem sie gefährdete Ressourcen isolieren, Server herunterfahren und andere einfache Aufgaben ausführen. Da XDR über ein zentrales Zugangsportal zu zahlreichen Services verfügt, kann nach der Erkennung einer Bedrohung durch automatisierte Abläufe verhindert werden, dass ähnliche Systeme von demselben Angriff betroffen sind.

Die SecureX-Plattform

SecureX ist eine Cloud-native integrierte Plattform, die das Portfolio von Cisco mit der Infrastruktur des Kunden verbindet und ein konsistentes Anwendererlebnis ermöglicht. Die integrierte und offene Plattform ist einfach zu verwenden, erhöht die Transparenz durch Zentralisierung und maximiert die betriebliche Effizienz, um Ihre Netzwerke, Endpunkte, Clouds und Anwendungen optimal abzusichern. Sie reduziert die Verweildauer und die von Menschen ausgeführten Aufgaben, um die Abwehr von Angriffen und die Einhaltung von Vorschriften zu unterstützen.

Integration mit neuen und bestehenden Lösungen

Ein gutes XDR-Produkt zeichnet sich dadurch aus, dass es nicht aufgrund mangelnder Integrationsfähigkeit aus bestimmten Systemen ausgesperrt werden kann. SecureX ist offen für andere Sicherheitsprodukte, die über offene und robuste RESTful-APIs verfügen. Viele dieser Produkte sind unerlässlich, um das volle Potenzial von XDR auszuschöpfen.

Zur umfassenden Behebung von Sicherheitsproblemen werden Informationen von Identitäts- und Autorisierungsservices, E-Mail-Sicherheitstools, Endpunkt- und Netzwerkerkennungslösungen und anderen Tools benötigt. Viele Ihrer bereits vorhandenen Sicherheitslösungen sind mit SecureX kompatibel.

Das Portfolio von Cisco Secure enthält viele Sicherheitslösungen, die sich problemlos mit SecureX integrieren lassen. Zwei nennenswerte Produkte sind Cisco Secure Network Analytics für Network Detection and Response (NDR) und Cisco Secure Endpoint für Endpoint Detection and Response (EDR). Leistungsstarke EDR- und NDR-Funktionen sind entscheidende Bestandteile einer erfolgreichen XDR-Plattform.

Darüber hinaus ist SecureX mit der Threat Intelligence-Gruppe Talos von Cisco integriert, die einen umfassenden Überblick über aktuelle und neue Bedrohungen bietet. Diese Sicherheitsinformationen können dann effektiv in Ihrem eigenen Sicherheitsökosystem genutzt werden, um die bereits beträchtliche Reichweite von SecureX noch weiter auszubauen.

Zentrales Dashboard

SecureX bietet ein übersichtliches Dashboard, das sich an die spezifischen Anforderungen jedes Teams anpassen lässt. Cisco hat das Dashboard in drei Bereiche unterteilt:

- eine Bildlaufliste mit Sicherheitsprodukten auf der linken Seite, über die schnell auf ein bestimmtes Tool zugegriffen werden kann
- eine große, zentralisierte Ansicht der Bedrohungsmetriken und Analysedaten in der Mitte
- ein Newsfeed, der Teams über neue Entwicklungen in der Sicherheitslandschaft auf dem Laufenden hält

ERINNERN

Das Dashboard ist einer der wichtigsten Bestandteile der XDR-Lösung, da es dem Sicherheitspersonal dabei hilft, Bedrohungen schnell zu erkennen und auf sie zu reagieren. Eine zentralisierte Ansicht eines Sicherheitsökosystems kann dazu beitragen, die Alarmmüdigkeit und

Informationsüberflutung zu verringern und die Anzahl von Fehlalarmen zu reduzieren, da Sicherheitsteams klare, präzise Informationen erhalten.

Bedrohungserkennung und -reaktion

Wenn die Funktionen zur Bedrohungserkennung und -reaktion von SecureX mit den Erkennungsfunktionen der Cisco Secure-Produkte kombiniert werden, ermöglichen sie einen mehrschichtigen Ansatz für auf maschinellem Lernen basierende Analysen. Mehrere Machine-Learning-Engines – darunter überwachte, unüberwachte, statistische und verhaltensbasierte Modelle sorgen für eine schnelle Erkennung von Bedrohungen und Ausgabe von Warnmeldungen. Diese Engines gleichen verdächtiges Verhalten mit vorhandenen sicherheitsrelevanten Erkenntnissen ab, um die Klassifizierung zu unterstützen und schnell einen Reaktionsplan in Gang zu setzen.

In einem größeren Ökosystem werden Sicherheitsinformationen mit Kontext angereichert, damit Teams Zusammenhänge zwischen betroffenen Ressourcen und Systemen erkennen können. SecureX profitiert dabei erheblich von den Telemetriedaten, die Cisco von seinem großen Kundenstamm erfasst. Cisco Secure nutzt ein globales Threat-Intelligence-Netzwerk, das Bedrohungen identifizieren und künftige Vorkommen dieser Bedrohung im gesamten Kundenstamm schnell erkennen kann. Leistungsstarke Analysen, eine zentralisierte Ansicht, umfassende Bedrohungsdaten und ein einfacher Zugriff auf Sicherheitsressourcen helfen Sicherheitsteams dabei, Reaktionszeiten zu verkürzen und fundierte Entscheidungen über Reaktionsmaßnahmen zu treffen.

Orchestrierung

SecureX enthält spezielle Orchestrierungs-Workflows für die proaktive Bedrohungssuche, das Schwachstellenmanagement und die Optimierung des Datenverkehrs. Diese Abläufe sind nicht in Stein gemeißelt. Sie können aber als Blaupause für Pläne verwendet werden, die den Anforderungen Ihres Unternehmens entsprechen.

SecureX verfügt über eine Drag-and-Drop-Oberfläche zur Erstellung individueller Workflows. Automatisierte Reaktionen, Genehmigungen und Maßnahmen können in einem Reaktionsplan zusammengestellt werden, um die Reaktionszeiten für zukünftige Sicherheitsbedrohungen zu verkürzen.

Kapitel 6
Zehn Dinge, die Sie über XDR wissen sollten

Dieses Kapitel fasst einige der wichtigsten Erkenntnisse aus diesem Buch zusammen und hebt die Merkmale hervor, auf die Sie bei XDR-Lösungen (Extended Detection and Response) und umfassenden Sicherheitsplattformen wie SecureX achten sollten.

Kürzere Erkennungs- und Reaktionszeiten

Letztendlich zielen XDR-Plattformen darauf ab, die Erkennungs- und Reaktionszeiten zu verkürzen. Mehr Daten und mehr Tools helfen Sicherheitsteams nicht unbedingt dabei, schneller zu arbeiten. Im Gegenteil: Sie stellen oft eine zusätzliche Belastung dar. XDR konzentriert sich auf die Bereitstellung verwertbarer Informationen durch ML-gestützte Analysen und ein zentrales Dashboard. Orchestrierungs- und Automatisierungsfunktionen optimieren Reaktionsprozesse, da das Sicherheitspersonal mit benutzerfreundlichen und anpassbaren Tools arbeiten kann.

Visualisierung integrierter Sicherheitsdaten

XDR erfasst eine Vielzahl von Informationen, die organisiert werden müssen, um Alarmmüdigkeit, Fehlalarme und Stress im Bereich Security Operations zu vermeiden. Zentrale Dashboards sind anpassbare Informationsdrehscheiben, mit denen Sicherheitsteams ihre Daten entsprechend den Anforderungen des Unternehmens organisieren können. Visualisierungstools wie Vorfallkarten helfen bei der Erkennung neuer Bedrohungsquellen und potenzieller Angriffspunkte.

Präzise Überwachung

Da XDR-Plattformen in der Regel maschinelles Lernen zur Analyse von Daten verwenden und sich bei der Datenerfassung auf sekundäre Sicherheitstools stützen, erhalten Sicherheitsteams einen klaren Überblick über das gesamte Ökosystem des Unternehmens. Anstatt möglichst vieler Daten werden nur wirklich verwertbare Informationen angezeigt. Das Sicherheitspersonal sieht also nur das, was es benötigt, um echte Sicherheitsprobleme zu beheben.

Kontextualisierung von Warnmeldungen und Reduzierung von Fehlalarmen

Die Features des zentralen Dashboards von XDR reichern sicherheitsrelevante Situationen mit Kontext an. Eingehende Warnmeldungen sind zuverlässiger, da das XDR-System über die relevanten Bedrohungsdaten verfügt, um zu entscheiden, welches Verhalten von der Norm abweicht und welches nicht.

Fehlalarme führen zur Verschwendung von Ressourcen. Deshalb bieten XDR-Lösungen eine umfassende Ansicht der IT-Infrastruktur, die zur Reduzierung von Fehlalarmen beiträgt.

Automatisierte Reaktionen

Automatisierungsfunktionen gibt es in der Sicherheitsbranche schon seit geraumer Zeit. Dank der großen Reichweite von XDR können die Automatisierungstools der Plattform aber noch feiner abgestimmt werden. Viele XDR-Produkte bieten Automatisierungsfunktionen, die sich auf maschinelles Lernen stützen. Diese können routinemäßige Sicherheitsaufgaben übernehmen, damit sich das Sicherheitspersonal auf anspruchsvollere Aufgaben konzentrieren kann, die menschliches Eingreifen erforderlich machen.

Eine offene Plattform

XDR ist kein Einzelkämpfer und benötigt deshalb die Unterstützung anderer spezialisierter Sicherheitstools. XDR-Plattformen bieten viele Integrationsmöglichkeiten, sowohl mit bestehenden Sicherheitstools als auch mit Produkten, die zu einem späteren Zeitpunkt hinzukommen könnten.

TIPP

Beim Aufbau einer optimalen Sicherheitsinfrastruktur sollten vor allem EDR- und NDR-Tools in Betracht gezogen werden.

Skalierbare Speicherung und Analyse von Protokollen

Aufgrund ihrer leistungsstarken Analysetools sind XDR-Plattformen in der Lage, große Mengen an Sicherheitsdaten zu verarbeiten. XDR-Lösungen sind einfach skalierbar. Ihr Unternehmen kann also wachsen und sich weiterentwickeln, ohne dass Sie sich Sorgen über Ihre Sicherheitsanalysen machen müssen.

Erfüllung von Compliance-Anforderungen

XDR kann große Mengen an Daten verarbeiten. Sie können sich also darauf verlassen, dass Compliance-Anforderungen erfüllt und Branchenvorschriften eingehalten werden.

ERINNERN

Unternehmen im Gesundheits- oder Finanzwesen benötigen besonders umfangreiche Protokollierungs- und Analysetools.

Isolierte Lösungen sind Teillösungen

Sicherheitsinfrastrukturen sind heute so umfangreich, dass die Trennung von Systemen in Silos zu einer gängigen Praxis geworden ist. Auf Unternehmensebene ist diese Trennung der IT-Infrastruktur jedoch kein ausreichender Schutz, da Angreifer ihre Angriffsstrategien ständig ausweiten und weiterentwickeln. Unvollständige Sicherheitsinformationen können zu Fehlalarmen und Alarmmüdigkeit führen, da Überwachungstools nicht über den vollständigen Kontext verdächtiger Aktivitäten verfügen.

Der menschliche Faktor ist wichtig

Das Sicherheitspersonal, das die Tools verwaltet, ist der wichtigste Teil einer erfolgreichen IT-Sicherheitsumgebung. Sicherheitsteams werden durch ineffiziente Sicherheitslösungen überlastet. Sie werden mit Fehlalarmen und unnötigen Warnmeldungen überflutet, die Alarmmüdigkeit verursachen, und durch unzureichende Tools zur Bedrohungserkennung und -reaktion ausgebremst.

CISCO
SECURE X

Wir machen es Ihnen leicht.

Die Cisco SecureX-Plattform ist eine integrierte Plattform innerhalb unseres Sicherheitsportfolios, die mit Ihrer gesamten Sicherheitsinfrastruktur verbunden ist.

Erfahren Sie wie der XOR-Plattformansatz von Cisco Ihre Sicherheitsziele verbessern kann

CISCO The bridge to possible

Eine zentralisierte Sicht auf Ihre Sicherheitsinfrastruktur!

Zu den Hauptzielen von XDR-Plattformen gehören die Verkürzung der Erkennungs- und Reaktionszeiten, die Minimierung der Alarmmüdigkeit und die Anreicherung von Warnmeldungen mit zusätzlichem Kontext. XDR stellt Bedrohungsdaten durch MT-gestützte Analysen bereit und bietet ein zentrales Dashboard, das Sie in die Lage versetzt, schneller und gezielter auf Bedrohungen zu reagieren. Orchestrierungs- und Automatisierungsfunktionen rationalisieren den Reaktionsprozess, da das Sicherheitspersonal mit benutzerfreundlichen und anpassbaren Tools arbeiten kann.

Im Buch ...

- So haben sich Sicherheitsbedrohungen weiterentwickelt
- Moderne Sicherheitstools und -techniken
- Schlüsselelemente von XDR
- Isolierte Lösungen schaffen Hindernisse
- Lösung der Probleme von Security Operations-Teams
- Konsolidierung der Erkennungsanalyse
- Untersuchung und Behebung von Bedrohungen

James Sullivan ist ein Technikautor aus Portland in Oregon (USA). Seine Arbeit befasst sich mit Cloud-Sicherheit, IoT und Cloud-Datenbanklösungen. In seiner Freizeit hört er gern Horror-Podcasts an, begeistert sich für Brettspiele und studiert die linguistischen Strukturen des Miauens seiner Katze.

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

ISBN: 978-1-394-15622-1
Nicht für den Wiederverkauf

für dummies®

WILEY END USER LICENSE AGREEMENT

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