Ein XDR-Leitfaden: Das Versprechen einfacherer Sicherheitsverfahren

Inhalt

Einleitung 3

Die Auswirkungen der Konnektivität 3

Zeit ist Geld 4

XDR verändert das Paradigma 5

Korrelieren von Daten zur übergreifenden Erkennung fortschrittlicher Bedrohungen 5

Schneller auf das reagieren, was wirklich wichtig ist 5

Optimieren der Effizienz für maximalen Mehrwert und schnellere Ergebnisse 6

Die Journey zu Security Resilience 6

Warum Cisco XDR? 7

Einleitung

Wenn Sie an ein Security Operations Center (SOC) denken, was kommt Ihnen in den Sinn? Ein Raum voller Ninjas, die Warnmeldungen bearbeiten? Oder ein großer Raum mit riesigen Karten zur Bedrohungslandschaft?

Sicherheitsverfahren gehören zweifellos zu den schwierigsten Aufgaben in der Branche. Im Laufe der Jahre hat die Bedeutung und Komplexität des SOC eines Unternehmens als Nebenprodukt der Digitalisierung und der Einführung neuer Technologien weiter zugenommen.

Ein aktueller ESG-Bericht zeigt, dass über die Hälfte aller Unternehmen mehr als 26 verschiedene kommerzielle, selbst entwickelte oder Open-Source-Tools für Sicherheitsverfahren einsetzt.[1] Die Einführung neuer Technologien sollte die Arbeit des SOC-Teams erleichtern, das ist aber häufig nicht der Fall.

Die Auswirkungen der Konnektivität

Durch hybride Arbeit und die Einführung der Cloud sind wir heute stärker vernetzt als je zuvor. Unternehmen agieren als integrierte Ökosysteme, in denen die Grenzen zwischen Konzernen, Kunden, Lieferanten und Partnern verschwimmen. Dieses neue Zeitalter der Vernetzung – auch wenn es sich positiv auf unser geschäftliches und privates Leben auswirkt – hat zu einer wachsenden Angriffsfläche und einem Anstieg raffinierter Cyberangriffe geführt.

Wir wissen, dass es verlockend ist, einfach die neueste Technologie zu kaufen, um neue Sicherheitsbedenken auszuräumen. Die Realität sieht jedoch so aus, dass ohne eine Lösung, die den Security-Stack optimiert, das Hinzufügen weiterer Tools nur noch mehr Verwirrung in einer bereits unzusammenhängenden Sicherheitsumgebung schafft. Das kann zu mehr Sicherheitslücken führen, die Sie ausbremsen, wenn das eigentliche Ziel darin besteht, die Erkennung zu beschleunigen und die Reaktion zu priorisieren.

„Um wirklich effektiv zu sein, müssen Anbieter von Cybersicherheit offen für den Austausch von Daten und Kontext sein, damit fortschrittliche Analysen über möglichst viele Vektoren hinweg die raffiniertesten Gruppen von Bedrohungsakteuren schnell erkennen und darauf reagieren können.“

AJ Shipley
VP of Product Management for Threat Detection and Response

Zeit ist Geld

Machen wir uns nichts vor: Wenn es um Sicherheit geht, ist Zeit Geld. Die Erkennung und Eindämmung einer einzelnen Sicherheitsverletzung dauert im Durchschnitt 277 Tage. Das bedeutet, dass in Ihrem Unternehmen ein Dieb fast 10 Monate lang unentdeckt herumlaufen, auf interne Anwendungen zugreifen und jeden Tag private Daten stehlen könnte – das ist inakzeptabel!

SicherheitsanalystInnen tun ihr Bestes, um täglich Tausende von Warnungen zu sortieren und zu priorisieren, in der Hoffnung, den effektivsten Ansatz für die Erkennung und Beseitigung von Bedrohungen zu finden. Aber die meisten haben Schwierigkeiten. Um diese Probleme wirklich zu lösen, müssen wir die Ursachen eines ineffektiven Sicherheitsteams aufdecken:

1. **Schlechte Integration mit bestehenden Sicherheitsinvestitionen**

   Die meisten Unternehmen verlassen sich auf Tools von mehreren Anbietern, um ihre gesamte Security-Infrastruktur aufzubauen. Das bedeutet, dass sie in der Regel mehrere eigenständige Lösungen mit wenig bis gar keiner Integration und ohne gemeinsam genutzte Telemetriedaten einsetzen. Wenn Lösungen nicht zusammenarbeiten, entsteht ein Schneeballeffekt.

   Eine fehlerhafte Integration schränkt die Menge der gemeinsam genutzten Telemetriedaten und Intelligence ein und macht es unmöglich, eine einzige, kontextreiche Ansicht zu erstellen. Wenn Sie nicht alle Bedrohungen im gesamten Unternehmen sehen können, wie können Sie dann effektiv Risiken in großem Maßstab oder überhaupt mindern?

   AJ Shipley, VP of Product Management for Threat Detection & Response bei Cisco, bringt es auf den Punkt: „Seit Jahren nutzen Cyberangreifer jeden möglichen Vorteil aus, um ihre Ziele zu erreichen. Dazu gehört auch die Unfähigkeit aufgrund fehlenden Datenaustauschs, mehrere Low-Fidelity-Signale verschiedener Anbieter effektiv zu einer hochpräzisen Erkennung zu korrelieren. Um wirklich effektiv zu sein, müssen Anbieter von Cybersicherheit bereit sein, Daten und Kontext weiterzugeben, damit fortschrittliche Analysen über möglichst viele Vektoren hinweg die raffiniertesten Gruppen von Bedrohungsakteuren schnell erkennen und darauf reagieren können.“ Security-Teams benötigen einen offenen und erweiterbaren Ansatz, damit ihre Lösungen besser zusammenarbeiten.

2. **Warnungsüberlastung**

   In der aktuellen Studie von ESG zur SOC-Modernisierung wird darauf hingewiesen, dass 37 % der IT- und SicherheitsexpertInnen zugaben, dass ihre Sicherheitsverfahren 2022 aufgrund des zunehmenden Volumens und der Komplexität von Sicherheitswarnungen schwieriger zu verwalten sind als noch vor zwei Jahren. AnalystInnen haben Schwierigkeiten damit, nicht nur die richtigen Bedrohungen zu identifizieren, sondern sie auch so zu priorisieren, dass sie die beste Strategie zur Behebung der Probleme finden, um die Auswirkungen auf ihr Unternehmen zu minimieren.

   Wenn die Analystenteams nicht über ausreichende Threat-Intelligence oder kontextbezogenes Bewusstsein verfügen, ist es fast unmöglich, Bedrohungen entsprechend den geschäftlichen Auswirkungen zu priorisieren. Das Ergebnis ist eine Flut von Warnungen, ohne dass genau unterschieden werden kann, welche Schadenshöhen diese für Ihr Unternehmen verursachen könnten, wenn sie übersehen werden. Entstehen vielleicht Schäden in Millionenhöhe oder hat es nur geringe bis gar keine Auswirkungen?

3. **Fachkräftemangel**

   Der Mangel an AnalystInnen, die über die notwendigen Fähigkeiten verfügen, um die Verantwortlichkeiten auszugleichen, verschärft die Auswirkungen von isolierten Systemen und irrelevanten Warnungen auf den Sicherheitsbetrieb noch weiter. Laut ESG stimmen 81 % der IT- und CybersicherheitsexpertInnen zu, dass ihre Sicherheitsabläufe durch den weltweiten Fachkräftemangel im Bereich Cybersicherheit beeinträchtigt wurden.[2]

Unternehmen benötigen eine Möglichkeit, ihre AnalystInnen weiterzubilden, um sicherzustellen, dass die richtigen aussagekräftigen Erkenntnisse erlangt und hervorgehoben werden, damit komplexe Bedrohungen nicht unentdeckt bleiben. Integrierte globale und lokale Threat-Intelligence hilft, diese Lücke zu schließen, indem sie den zusätzlichen Kontext bereitstellt, der erforderlich ist, um Bedrohungen für Ihr Team präzise zu kennzeichnen und zu priorisieren. Dies erhöht das Bewusstsein aller AnalystInnen dafür, welche Bedrohungen ein hohes Risiko darstellen und sofort behandelt werden sollten, um die Sicherheitseffizienz zu verbessern und Ihr Team unabhängig von seiner Erfahrung und seinem Fachwissen effektiver zu machen.

XDR verändert das Paradigma

Da Bedrohungen immer raffinierter werden, reicht das alte Erkennungs- und Reaktionsmodell, das auf eigenständigen Punktsicherheitslösungen basiert, nicht mehr aus. Heute nutzen Teams Lösungen wie SIEM und SOAR, um isolierte Umgebungen zu vereinheitlichen und Warnungen zu reduzieren, aber das Problem bleibt bestehen. Die heutigen Security-Teams benötigen eine Lösung, die Daten aus verschiedenen Quellen in zuverlässige Warnungen und Erkenntnisse umwandelt, damit sie schnell und selbstbewusst handeln können.

In den letzten Jahren hat Extended Detection and Response (XDR) an Dynamik gewonnen. Diese Technologie verspricht, die Lücke mit einem offenen und einheitlichen Ansatz zu schließen, um Bedrohungen schnell und effizient zu verhindern, zu erkennen und darauf zu reagieren.

Aber was genau ist XDR? Kurz gesagt, handelt es sich um eine Lösung, die Telemetriedaten von mehreren Security-Tools in einem zentralen Daten-Repository sammelt, die gesammelten und homogenisierten Daten analysiert, um eine Erkennung der Schädlichkeit zu ermöglichen, und die Reaktion und Behebung dieser erkannten Schädlichkeit beschleunigt. Mit effektiver XDR ist es für AnalystInnen einfacher, sich unabhängig von der Stufe auf umfassende Bedrohungserkennung, priorisierte risikobasierte Incident Response und die Verbesserung der Produktivität zu konzentrieren.

Laut der ESG-Studie geben 51 % der Fachleute an, dass die derzeit verwendeten Security-Tools Schwierigkeiten haben, fortschrittliche Bedrohungen zu erkennen und zu untersuchen.[2]

Eine risikoorientierte XDR-Lösung nutzt globale Threat-Intelligence und lokalen Kontext, um Bedrohungen schnell zu quantifizieren, zu überprüfen und zu priorisieren.

Korrelieren von Daten zur übergreifenden Erkennung fortschrittlicher Bedrohungen

Wenn Sie an alle Daten denken, die in Ihren Netzwerken, Endpunkten, E-Mails und Anwendungen vorhanden sind, gibt es viel zu schützen.

Wir wissen, dass die überwiegende Mehrheit der Unternehmen einen Security-Stack aus Produkten mehrerer Anbieter nutzt, um Bedrohungen zu untersuchen und darauf zu reagieren. Isoliert können diese Lösungen nur einen teilweisen Überblick über das bieten, was zu einem bestimmten Zeitpunkt geschieht, aber zusammengenommen werden diese Daten zu verwertbaren und nützlichen Erkenntnissen.

Schneller auf das reagieren, was wirklich wichtig ist

Jedes Unternehmen ist anders. Je nachdem, welche Systeme und Betriebsabläufe für Ihr Unternehmen am wichtigsten sind, kann eine Bedrohung, die zu lange am falschen Ort aktiv ist, den Ruf Ihrer Marke schädigen oder den finanziellen Ruin bedeuten. Erschwerend kommt hinzu, dass Analystenteams oft nicht die Zeit haben, die vielen Warnungen, die sie täglich sehen, genau zu priorisieren.

Eine risikoorientierte XDR-Lösung nutzt jedoch globale Threat-Intelligence und lokalen Kontext, um Bedrohungen schnell zu quantifizieren, zu verifizieren und entsprechend der Wahrscheinlichkeit eines Risikos zu priorisieren. Im Grunde genommen übersetzt XDR den vereinheitlichten globalen und lokalen Kontext, um das gesamte Angriffskontinuum zu visualisieren und AnalystInnen dabei zu unterstützen, sowohl die Ursache als auch den gesamten Umfang der Auswirkungen zu verstehen.

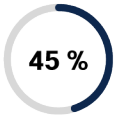
Fünf Schlüsselelemente einer effektiven XDR-Umsetzung

1. Bietet priorisierte und aussagekräftige Telemetrie, wo immer Sie sie benötigen
2. Ermöglicht eine einheitliche Erkennung, unabhängig von Vektor oder Anbieter
3. Unterstützt eine schnelle und präzise Reaktion auf Bedrohungen
4. Bietet eine zentrale Untersuchungsperspektive für ein optimiertes Benutzererlebnis
5. Bietet Möglichkeiten zur Steigerung der Produktivität und zur Stärkung des Sicherheitsstatus

Optimieren der Effizienz für maximalen Mehrwert und schnellere Ergebnisse

Abgesehen von Angreifern sind die wichtigsten Gegner der Sicherheit ein Mangel an Kontext, Fähigkeiten und Zeit. Aber mit einer einheitlichen XDR-Konsole können auch Teams mit wenig Zeit und Ressourcen die Verweildauer drastisch verkürzen.

Der XDR-Ansatz, Sicherheitsdaten an einem zentralen Ort zu aggregieren, erleichtert es Ihren Teams, die kritischsten Bedrohungen unabhängig von ihrer Erfahrung schnell und präzise zu analysieren, zu priorisieren und darauf zu reagieren. Die integrierte Orchestrierung und Automatisierung hilft Teams, sich von repetitiven Aufgaben zu entlasten und begrenzte Ressourcen dorthin zu lenken, wo sie am dringendsten benötigt werden.



Unternehmen mit einer ausgereiften XDR-Implementierung verzeichneten eine Verbesserung der Security Resilience im Vergleich zu Unternehmen ohne XDR.[3]

Die Journey zu Security Resilience

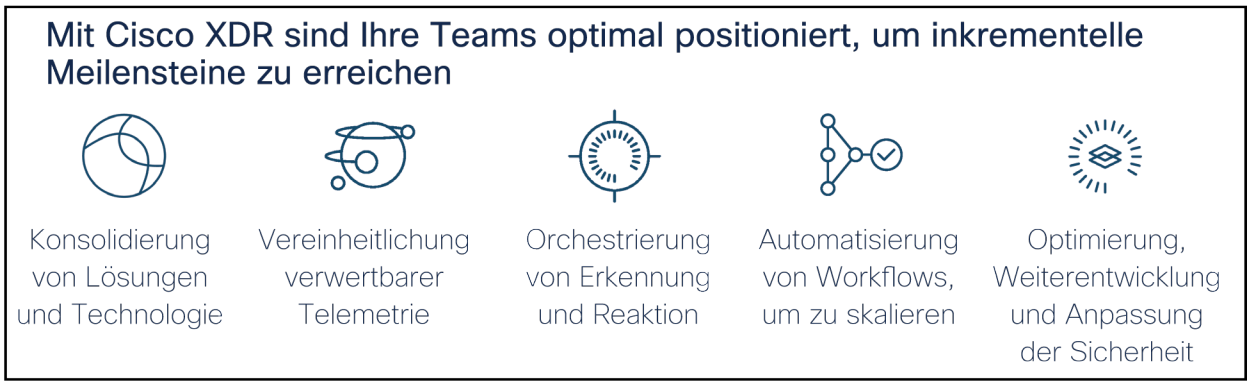
Heute ist Unsicherheit die Regel. Als Reaktion darauf investieren Unternehmen in allen Geschäftsbereichen in Widerstandsfähigkeit. Aber ohne Security Resilience ist Ihr Unternehmen möglicherweise anfällig für unvorhersehbare Bedrohungen und Veränderungen.

Als Teil einer offenen, integrierten Plattform namens Cisco Security Cloud integriert unsere XDR-Lösung Security Resilience selbst in den komplexesten hybriden Multicloud-Umgebungen. Da immer mehr Lösungen in Ihre XDR integriert sind, können Sie die Erkennung stärken und vollständigere Reaktionsmaßnahmen über alle erforderlichen Vektoren hinweg durchführen.

Warum Cisco XDR?

Bei Cisco stehen unsere Kunden im Mittelpunkt unseres Handelns. Aus diesem Grund bieten wir eine umfassende XDR-Lösung mit einer umfangreichen Bibliothek von Drittanbieter-Integrationen, darunter führende Sicherheitsanbieter, um maximale Flexibilität zu bieten.

Wir wissen auch, dass das Letzte, was Sie brauchen, mehr Komplexität ist. Deshalb haben wir eine All-in-One-Konsole für Sie entwickelt, mit der Ihre Security- und SOC-AnalystInnen Bedrohungen mit nur wenigen Klicks erkennen, untersuchen und beheben können. Unsere Lösung ist offen, erweiterbar und Cloud-first, sodass Sie Ihre bestehenden Sicherheitsinvestitionen optimieren und die Sicherheitserkennung in Ihrer gesamten Umgebung vereinheitlichen können.



[1] „ESG Complete Survey Results: SOC Modernization and the Role of XDR“, Enterprise Strategy Group (ESG), September 2022
https://www.esg-global.com/research/esg-complete-survey-results-soc-modernization-and-the-role-of-xdr

[2] „SOC Modernization and the Role of XDR“, Enterprise Strategy Group (ESG), Juni 2022
https://www.cisco.com/c/en/us/products/security/soc-modernization-xdr

[3] „Security Outcomes Report, Volume 3“, Cisco, Dezember 2022
https://www.cisco.com/c/en/us/products/security/security-outcomes-report.html

Hauptgeschäftsstelle Nord- und Südamerika
Cisco Systems, Inc.
San Jose, CA

Hauptgeschäftsstelle Asien-Pazifik-Raum
Cisco Systems (USA) Pte. Ltd.
Singapur

Hauptgeschäftsstelle Europa
Cisco Systems International BV Amsterdam,
Niederlande

Cisco verfügt über mehr als 200 Niederlassungen weltweit. Die Adressen mit Telefon- und Faxnummern finden Sie auf der Cisco Website unter **www.cisco.com/go/offices**.

Gedruckt in den USA C95-3551078-00 04/23