CISCO
SECURE

XDR: Kaufleitfaden

So navigieren Sie wie ein Profi durch den aufstrebenden Markt für Extended Detection and Response

CISCO The bridge to possible

cisco SECURE

Was ist Extended Detection and Response (XDR)?

Warum braucht die Welt noch ein neues Sicherheitskonzept?

Selbst die souveränsten und finanziell am besten ausgestatteten Sicherheitsteams wissen, dass sie einem überwältigenden Druck von außen ausgesetzt sind. Die jüngste Verlagerung hin zu Remote- und/oder hybrider Arbeit hat die Komplexität noch erhöht. Die Angriffsfläche wird immer größer. Es gibt unzählige Warnungen. Sicherheitstools sind miteinander inkompatibel. Bei so viel Reibung zwischen Mensch und Technik ist es kein Wunder, dass die Wirksamkeit der Sicherheit stagniert und die durchschnittliche Verweildauer von Bedrohungen immer noch bei 280 Tagen liegt[1].

Diese neue Normalität verlangt nach Security Resilience – der Fähigkeit, die Integrität jedes Aspekts des Unternehmens zu schützen, damit es unvorhersehbaren Bedrohungen oder Veränderungen standhalten und aus diesen lernen kann. Security Resilience erfordert mehr als das, was in der Vergangenheit möglich war.

Die wichtigsten Gründe für XDR:

1. Weniger irrelevante Warnungen
2. Kürzere Zeit bis zur Erkennung
3. Mehr Transparenz über alle Tools hinweg
4. Besserer Bedrohungskontext

Was genau ist also XDR und warum ist es wichtig?

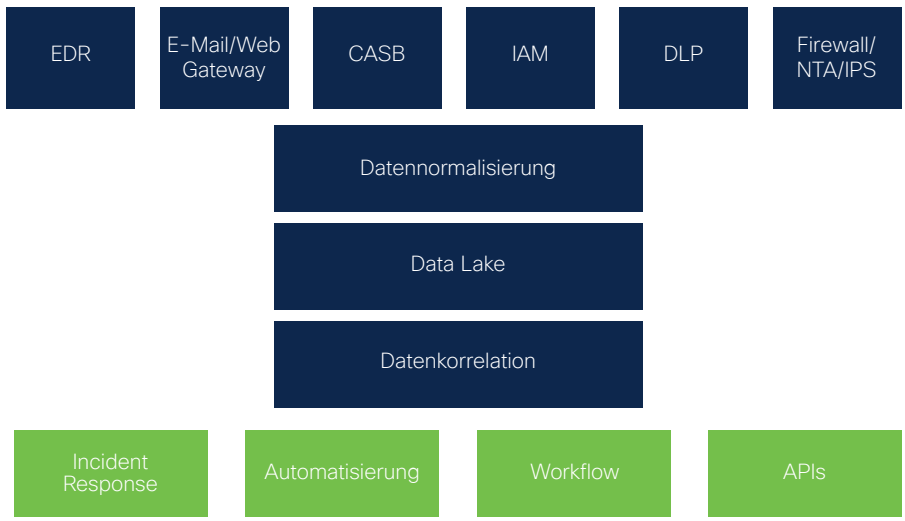
Während die Integration in native Sicherheitslösungen in XDR äußerst vorteilhaft ist, ist es auch wichtig, dass eine XDR-Plattform vorhandene Drittanbieter-Technologie nutzt und einfach damit verbunden werden kann, um einen besseren ROI und einen umfassenderen Kontext für alle Datenquellen zu bieten. Dies ist ein bedeutender Paradigmenwechsel gegenüber den bisherigen Strategien, bei denen der Großteil der Erkennung und Reaktion innerhalb einzelner Produktsilos und Teams erfolgt. Die Einheitlichkeit, die XDR bietet, wirkt sich auf mehrere Schlüsselbereiche für jedes Sicherheitsteam aus:

Erstens liefert es bei nur geringem bzw. keinerlei Konfigurationsaufwand schnellen Mehrwert für Teams. Wenn die Teams bereits ein SIEM oder SOAR eingerichtet haben, bauen die XDR-Plattformen auf diesen Vorteilen auf.

Zweitens löst es das Problem zu vieler Warnungen, das so viele Teams plagt – denn die Plattform aggregiert und korreliert alle unterschiedlichen Ereignisse, die durch dieselbe Sicherheitsverletzung verursacht werden, zu Vorfällen.

Drittens bietet es sofort einsatzbereite Automatisierungs- und Orchestrierungselemente, mit denen Teams tägliche Routineaufgaben beseitigen können.

XDR – Konzept und Architektur



1. Forschungsergebnisse des Ponemon Institute im IBM Cost of a Data Breach Report 2020

cisco SECURE

5 Schlüsselelemente einer effektiven XDR-Umsetzung

1 Koordinierte Telemetrie in Ihrer gesamten Umgebung

Für XDR werden umfassende Transparenz und Einblicke benötigt. Zum jetzigen Zeitpunkt positionieren die Anbieter ihre bestehenden Produkte als Schlüsselkomponenten von XDR. Echte XDR muss jedoch nicht nur Daten, sondern auch Telemetrie aus den verschiedensten Sicherheitskontrollkategorien und Datenbeständen sowie von Threat-Intelligence-Anbietern zusammenführen, um die Wahrscheinlichkeit bösartiger Absichten zu ermitteln. Mit XDR können Unternehmen die Lücken schließen und eine umfassende Abwehr im gesamten Ecosystem mit einer offenen, integrierten Plattform über den Campus, das Rechenzentrum, die Cloud und den Cloud-Edge hinweg erzielen. Mit dem umfangreichen Kontext aus jeder dieser integrierten Lösungen in XDR können Sie Schwachstellen finden und schneller beheben.

Wichtigste Funktionen	Diese Fragen sollten Sie stellen
Vollständige Einblicke in die Umgebung	Wie bietet Ihre Lösung mehr als nur Netzwerktransparenz?
Verwertbare Telemetrie	Verwenden Sie einen Data Lake, um Einblicke zu erhalten, oder andere Tools, die aussagekräftige Telemetriedaten liefern?
Zuverlässige Datenquellen	Wie stellt Ihre Lösung sicher, dass ich einen Überblick über alle Endpunkte, Geräte und den ein- und ausgehenden Netzwerk-Traffic erhalte?

2 Erkennungsfunktionen vorhandener Systeme nutzen, unabhängig vom Anbieter

Während Gartner in seiner XDR-Definition proprietäre Komponenten erwähnt, ist es für eine XDR-Lösung entscheidend, dass sie mit einem offenen Plattformansatz konzipiert ist und sich leicht mit Technologien von Drittanbietern verbinden lässt. Jede Komponente in Ihrem Sicherheits-Stack verfügt über einzigartige Erkennungselemente – IoC-Erkennung, Machine Learning, Verhaltensanalytik usw. –, die gemeinsam noch leistungsfähiger werden. Schwache Hinweise aus Silos werden in ihrer Gesamtheit zu starken Hinweisen. Die Zusammenarbeit bei der Erkennung ist ein entscheidender Faktor für XDR. Stellen Sie also sicher, dass die von Ihnen gewählte Plattform mit Ihrem gesamten Stack zusammenarbeitet.

Wichtigste Funktionen	Diese Fragen sollten Sie stellen
Nutzung vorhandener Lösungen	Wie viele meiner bestehenden Investitionen kann ich bei Ihrem XDR-Ansatz weiternutzen?
Unabhängigkeit von Anbietern	Inwiefern unterscheiden sich Ihre Erkennungstechnologien von anderen auf dem Markt?
Nutzung von Drittanbieter-Analytik	Welche Ihrer Lösungen lassen sich direkt miteinander integrieren?

3 Einheitlicher Kontext aus zuverlässigen Quellen, der schnelle und präzise Reaktionen ermöglicht

Durch die Zusammenführung der Einblicke in Netzwerk, Endpunkte und E-Mails (um nur einige zu nennen) erhalten Sie ein genaueres Verständnis davon, was passiert ist, wie es sich entwickelt hat und welche Schritte unternommen werden müssen, um die Bedrohung zu beseitigen. Effektives XDR erfordert native Reaktions- und Problembehebungsfunktionen, z. B. die Isolierung eines Hosts oder das Löschen schädlicher E-Mails aus allen Posteingängen. Im Idealfall sind diese Aktionen mit nur einem oder zwei Klicks möglich. XDR sollte auch die Erstellung benutzerdefinierter Reaktionsmaßnahmen erleichtern, damit Teams die Sicherheit im Laufe der Zeit weiterentwickeln können.

Wichtigste Funktionen	Diese Fragen sollten Sie stellen
Kontextgesteuerte Intelligence	Kann ich Ihre XDR verwenden, um die Auswirkungen einer Bedrohung und das Ausmaß des Verstoßes zu verstehen und mit einem einzigen Mausklick über eine zentrale Schnittstelle Maßnahmen zu ergreifen?
Mehrere Informationsquellen	Welche Art von Threat-Intelligence fließen in Ihre Erkennung ein und woher stammt diese?
Beschleunigte MTTD	Wie validieren Sie die Datenquellen, die Sie in Ihrer Lösung verwenden?

4 Kontinuierliche Automatisierung und Orchestrierung bei Problemen auf Maschinenebene

Komplizierte, manuelle und veraltete Workflows setzen Ihr Unternehmen Bedrohungen und menschlichen Fehlern aus. Die richtige XDR-Plattform verfügt über leistungsstarke Orchestrierungs- und Automatisierungsfunktionen und macht sich wiederholende Sicherheitsaufgaben einfacher und effizienter, ohne dass Sie dazu eine lange Lernkurve durchlaufen müssen. Durch die Automatisierung kritischer Workflows kann das Team schneller auf Warnungen reagieren, sodass mehr Zeit und Energie für kritische Aufgaben wie die Nachverfolgung von Bedrohungen bleibt.

Wichtigste Funktionen	Diese Fragen sollten Sie stellen
Mehr Automatisierung	Behindern API-Änderungen der Anbieter Ihre Automatisierungsskripte in Drittanbieterintegrationen?
„Security Noise“ durchdringen	Wie können Sie mich bei der Orchestrierung und Automatisierung von Workflows in meinen vorhandenen Lösungen unterstützen?
Grenzen menschlicher Wahrnehmung überwinden	Wie unterstützt Ihre Lösung das Monitoring der Datenströme von und zu Cloud-basierten Workloads?

5 Eine einzige Untersuchungsperspektive zur Vereinfachung von Isolierung und Problembehebung

XDR sollte in einem Incident-Response-Team die essenziellen Tools ergänzen, da es Einblicke in zusätzliche Telemetriedaten über den Endpunkt hinaus bietet. Sie benötigen nur eine einzige Konsole für direkte Abhilfemaßnahmen, Zugriff auf Threat-Intelligence und Tools, um eine einheitliche Ansicht einer Warnung zu erhalten. Wenn XDR das Threat-Hunting durch Modelle wie MITRE ATT&CK optimiert, haben auch unerfahrenere MitarbeiterInnen Zugang zum hypothesengestützten Threat-Hunting und können vorausschauender agieren.

Wichtigste Funktionen	Diese Fragen sollten Sie stellen
Beschleunigte MTTR	Wo unterstützt und/oder beschleunigt Ihre Lösung die Problembehebung?
Umfassenderes Threat-Hunting	Wie hilft Ihre Lösung meinem Team beim Threat-Hunting?

Der Schritt in die Zukunft mit XDR

Wir empfehlen die Zusammenarbeit mit XDR-Stakeholdern, um die für Sie geeignete XDR-Strategie zu ermitteln. Stellen Sie sicher, dass potenzielle Anbieter Automatisierung und Integration priorisieren.

Beginnen Sie mit diesen Fragen, aber stellen Sie sicher, dass Sie die verschiedenen Funktionen und Anforderungen Ihres aktuellen Stacks verstehen, damit Sie messbare Ergebnisse erzielen und den ROI verbessern können.

1. Deckt Ihr XDR-Angebot Erkennung und Reaktion im Netzwerk sowie andere Sicherheitsebenen wie E-Mail, Cloud und Firewall ab?
2. Wie können Sie mir helfen, bessere und fundiertere Sicherheitsmaßnahmen zu ergreifen?
3. Wie hilft mir Ihre XDR-Lösung bei der Automatisierung von Blockierungen oder Problembehebung?
4. Welche Ihrer Lösungen lassen sich direkt miteinander integrieren?
5. Wie lässt sich Ihr XDR-Ansatz mit anderen Sicherheitsinitiativen wie SASE oder Zero Trust verknüpfen?

cisco SECURE

XDR und Security Resilience

Heutzutage gibt es überall Unsicherheiten – vom Betrieb über die Finanzen bis hin zur Lieferkette. Unternehmen investieren in ihre Widerstandsfähigkeit gegen unvorhergesehene Ereignisse, um diese besser zu überstehen und gestärkt daraus hervorzugehen. Diese Investitionen liefern jedoch nur in Kombination mit einer Investition in Security Resilience die gewünschten Ergebnisse.

Es gibt fünf Dimensionen der Security Resilience:

1. Nutzen Sie die Milliarden von Impulsen in Ihrem gesamten Ecosystem
2. Schaffen Sie eine gemeinsame Informationsgrundlage, um Vorhersagen für die Zukunft zu treffen
3. Priorisieren Sie Warnungen mit risikobasierter Kontextanalyse
4. Schließen Sie Lücken im Ecosystem durch Integrationen
5. Stärken Sie die Sicherheit durch Orchestrierung und Automatisierung

Die richtige XDR-Plattform erfüllt jede dieser Dimensionen. Cisco ist führend bei der Bereitstellung von XDR mit einheitlichem Kontext, korrelierter Erkennung und beschleunigter Reaktion.

Unsere Sicherheitsplattform SecureX ist bereits in alle Sicherheitsprodukte von Cisco integriert und lässt sich mithilfe offener APIs leicht in die Lösungen in Ihrer Umgebung integrieren. Diese einheitliche Erkennungs- und Reaktionsschicht korreliert Telemetriedaten von allen Kontrollpunkten in einer einzigen Untersuchungsperspektive und erleichtert das Priorisieren und Ergreifen von Maßnahmen. Darüber hinaus können Sie mit der integrierten Orchestrierung Reaktionen automatisieren und Routineaufgaben entlasten, um Teams für proaktivere Aufgaben wie die Nachverfolgung von Bedrohungen zu entlasten.

Treten Sie nicht mehr auf der Stelle – es ist Zeit für mehr Geschwindigkeit.

Wenn Sie mehr über den XDR-Ansatz von Cisco erfahren möchten, wenden Sie sich an unser Sales Team.

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

Hauptgeschäftsstelle Asien/Pazifik
Cisco Systems (USA), Pte. Ltd.
Singapur

Hauptgeschäftsstelle Europa
Cisco Systems International BV Amsterdam,
Niederlande

cisco SECURE

Tabelle zur XDR-Anbietervalidierung

Verwenden Sie diese Tabelle und die zuvor in diesem Dokument aufgeführten Fragen, um sich auf Gespräche mit XDR-Anbietern vorzubereiten. Wählen Sie 8–10 Fragen aus, die für Ihre Umgebung am relevantesten sind, und fügen Sie sie unten ein.

Fragen/Anmerkungen	Überzeugende Antworten
Frage:	
Anmerkungen:	
Frage:	
Anmerkungen:	
Frage:	
Anmerkungen:	
Frage:	
Anmerkungen:	
Frage:	
Anmerkungen:	
Frage:	
Anmerkungen:	
Frage:	
Anmerkungen:	
Frage:	
Anmerkungen:	
Frage:	
Anmerkungen:	
Frage:	
Anmerkungen:	


CISCO
SECURE