XDR: Kaufleitfaden

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

Inhalt

Was ist Extended Detection and Response (XDR)?

Warum braucht die Welt noch ein neues Sicherheitskonzept?

In der heutigen hybriden, vielschichtigen IT-Landschaft mit mehreren Anbietern ist Komplexität die größte Herausforderung. Sicherheitsteams müssen ein sich ständig erweiterndes Ecosystem schützen und den Betrieb über Dutzende von Tools mit inkonsistenter Integration ausführen. IoT und hybride Arbeit haben zu einer erweiterten Angriffsfläche geführt. Phishing, Malware und Ransomware verdoppeln und verdreifachen sich sogar von Jahr zu Jahr.Gleichzeitig sind Unternehmen stärker vernetzt als je zuvor. Eine Sicherheitsverletzung bei einem Unternehmen kann sich auf Lieferanten, Partner, Kunden und sogar ganze Wirtschaftssektoren auswirken.

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.

Was ist die Lösung?

Da Bedrohungen immer raffinierter werden, reicht das alte Erkennungs- und Reaktionsmodell, das auf in sich geschlossenen Punktsicherheitslösungen basiert, nicht aus. Hier kommt XDR ins Spiel. Extended Detection and Response (XDR) ist ein einheitliches Tool zur Erkennung und Reaktion auf Sicherheitsvorfälle. XDR-Lösungen erfassen und korrelieren automatisch Telemetriedaten mehrerer Sicherheitstools, wenden Analysen an, um schädliche Aktivitäten zu erkennen, und reagieren dann auf Bedrohungen und beseitigen diese. Effektive XDR-Lösungen sind umfassend und korrelieren Daten über alle Vektoren hinweg – E-Mails, Endpunkte, Server, Cloud-Workloads und Netzwerke. Sie ermöglichen Transparenz und Kontext in Ihrer gesamten Umgebung, selbst bei den komplexesten Bedrohungen.

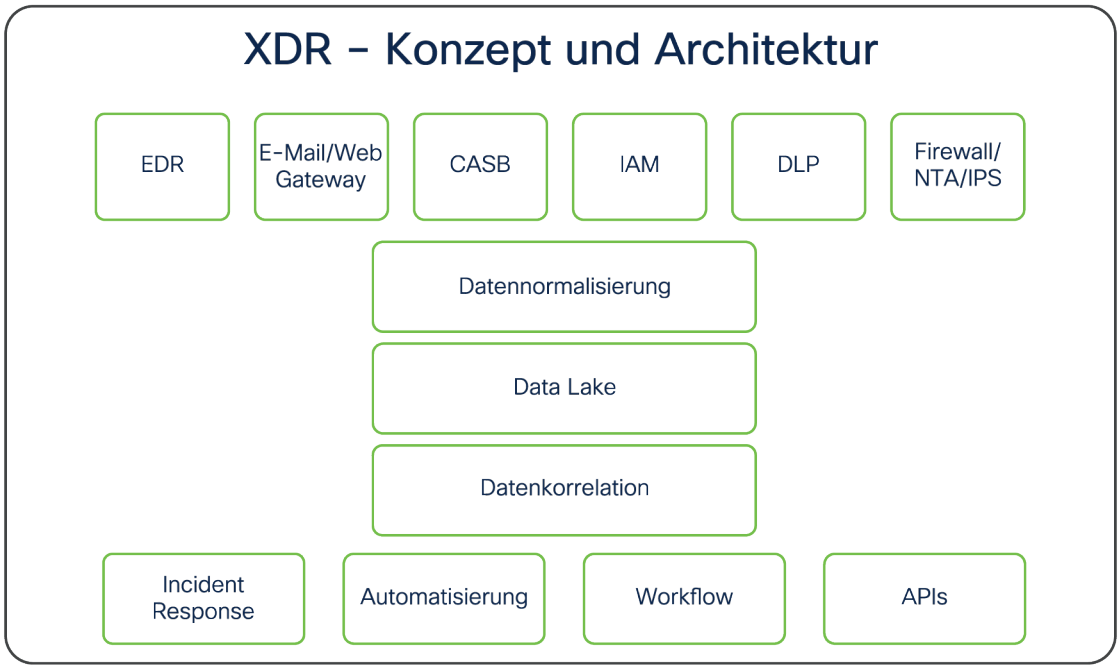
Warum XDR?

Erstens: Teams können mithilfe von Ereigniskorrelation und Multi-Vendor-Erkennung im Netzwerk, in der Cloud, auf Endpunkten, in E-Mails und mehr selbst die komplexesten Bedrohungen erkennen.

Zweitens: Die Überlastung durch zu viele Warnhinweise wird verringert, da Teams Bedrohungen abhängig von den Auswirkungen priorisieren können.

Drittens: Die Automatisierung von Arbeitsabläufen steigert die Produktivität, sodass Teams SOC-Ressourcen effizienter nutzen können.

Viertens: Unternehmen können Security Resilience aufbauen, indem sie Sicherheitslücken schließen und die nächsten Schritte anhand von aussagekräftigen Informationen vorhersehen können.



5 Schlüsselelemente einer effektiven XDR-Umsetzung

1. Bietet priorisierte und aussagekräftige Telemetrie, wo immer Sie sie benötigen

Können Sie die Vielzahl von Warnungen zu vorselektierten Bedrohungen effizient durchsuchen?

Umfassende Transparenz und umfassende Einblicke sind für XDR grundlegend. Viele komplexe Bedrohungen greifen nicht nur den Endpunkt oder das Netzwerk allein an – sie greifen über eine Vielzahl von Vektoren an, darunter E-Mails, Endpunkte, Netzwerke, Identitätsmanagement, Sandboxing und Firewalls. Daher benötigen Sie eine XDR-Lösung mit einem breiten Spektrum an Telemetriedaten und Datenqualität, die Ihre XDR-Ergebnisse unterstützen und einen ganzheitlichen und umfassenden Überblick über die Vorgänge in Ihrer Umgebung bieten. Aber es geht nicht nur darum, Einblicke zu gewinnen. Dem Management von Vorfällen kommt eine ebenso wichtige Rolle zu. Damit XDR die versprochene Wirkung entfalten kann, müssen diese Einblicke priorisiert werden. Mit XDR-Lösungen, die eine risikobasierte Priorisierung bieten (die Priorisierung von Vorfällen nach dem größten materiellen Risiko), können Sie schneller auf die wesentlichen Dinge reagieren. Sie sollten auch Empfehlungen für die nächsten Schritte geben, damit Sie fundierte Entscheidungen über die beste Vorgehensweise treffen können.

Wichtigste Funktionen und Merkmale	Entsprechende Produktbereiche
• Effektivität und Genauigkeit zur Minimierung von Störungen durch falsch-positive Meldungen • Aggregieren und Korrelieren von Warnungen in der gesamten Umgebung	Endpoint Detection and Response (EDR)
• Kontinuierliches Echtzeit-Monitoring von Netzwerken	Network Detection and Response (NDR)
• Fortschrittliche Analysen, die priorisierte Warnungen mit Kontext generieren, wenn unbekannte Malware und andere komplexe Netzwerkangriffe erkannt werden	Extended Detection and Response (XDR)
• Kontinuierliches Echtzeit-Monitoring von E-Mail-Bedrohungen und automatische Priorisierung von Korrekturmaßnahmen	E-Mail-Sicherheit

Fragen an Anbieter

- Wie bietet mir Ihre Lösung Transparenz in allen meinen Umgebungen (Endpunkte, Geräte, Netzwerk)?
- Wie liefert Ihre Lösung Einblicke? Bietet Ihre Lösung priorisierte Telemetrie?
- Wie priorisiert Ihre Lösung Bedrohungen basierend auf geschäftlichen Auswirkungen und Risiken?
- Welche Art von Threat-Intelligence fließt in Ihre Erkennung ein? Woher stammt diese Intelligence?
- Wie validieren Sie die Datenquellen, die Sie in Ihrer Lösung verwenden?
- Wie geht dieses Produkt mit komplexen Bedrohungen wie Wannacry, NotPetya und Turla um?

2. Ermöglicht eine einheitliche Erkennung, unabhängig von Vektor oder Anbieter

Können Ihre Sicherheitsinvestitionen mit Ihrer XDR-Lösung als koordinierte Einheit zusammenarbeiten?

Da Bedrohungen immer raffinierter werden und sich über eine Vielzahl von Angriffsvektoren erstrecken, ist die konsistente Erkennung in Ihrer gesamten Umgebung wichtiger denn je. Sicherheitsteams werden heutzutage mit einem außerordentlichen Grad an Komplexität konfrontiert – sowohl in ihrer Sicherheitsumgebung als auch in einem Ecosystem aus globalen Lieferketten, Angreifern und Verteidigern. XDR-Lösungen können Ihnen dabei helfen, indem sie Erkennungen basierend auf Schweregrad und Auswirkungen aggregieren, korrelieren und priorisieren. Dazu muss Ihr Security-Stack jedoch gut zusammen funktionieren. Durch die Auswahl einer offenen, erweiterbaren XDR-Lösung mit einem Cloud-First-Ansatz profitieren Sie von einer einheitlichen Erkennung und Ereigniskorrelation in Ihrer gesamten Umgebung und müssen die Komplexität nicht noch zusätzlich erhöhen. Jede Komponente in Ihrem Security-Stack verfügt über einzigartige Erkennungselemente (Netzwerke, E-Mails, Firewalls usw.), die gemeinsam noch leistungsfähiger werden. Es ist wichtig zu beachten, dass XDR alle sechs Telemetriequellen umfassen sollte – darunter Endpunkte, Netzwerke, Firewalls, E-Mails, Identität und DNS –, um einen umfassenden Überblick über potenzielle Bedrohungen zu bieten. Ihre XDR-Lösung sollte sich problemlos in Ihren gesamten Security-Stack mit nativer Backend-zu-Frontend-Integration integrieren lassen, damit die Abdeckung konsistent bleibt, selbst wenn Anbieter Änderungen am Portfolio vornehmen oder Sie den Anbieter wechseln. Zur Optimierung der Funktionen zur Bedrohungserkennung Ihres Security-Stacks lohnt es sich, XDR-Lösungen zu erkunden, die wertvollen lokalen Kontext bereitstellen und präzise Threat-Intelligence-Beurteilungen liefern, auf die Sie sich verlassen können.

Wichtigste Funktionen und Merkmale	Entsprechende Produktbereiche
• Erkennen und Blockieren von ungewöhnlichem Programmverhalten von Endpunkten, einschließlich Exploit-basierter Memory-Injection-Angriffe • Bestimmen von Indicators of Compromise (IoCs) mit MITRE ATT&CK-Zuordnungen • Monitoring der Dateireputation zur Erkennung und Isolierung von Bedrohungen am Eintrittspunkt • Identifizieren von Schwachstellen im Betriebssystem Ihrer Umgebung, sodass Admins die Korrekturmaßnahmen basierend auf Risiken priorisieren und die Angriffsfläche reduzieren können	Endpoint Detection and Response (EDR), Schwachstellenmanagement
• Profitieren mit fortschrittlichen Analysen von der schnellen Erkennung von unbekannter Malware, Insider-Bedrohungen wie Datenexfiltration, Richtlinienverstößen und anderen komplexen Bedrohungen • Erkennen von Netzwerkangriffen in Echtzeit mit hochgradig zuverlässigen Warnungen	Extended Detection and Response (XDR), Network Detection and Response (NDR)
• Erkennen und Blockieren unerwünschter E-Mails mit Reputationsfiltern • Identifizieren von und Schutz vor auf Täuschung basierenden E-Mail-Angriffen wie Social Engineering und Identitätsbetrug	E-Mail-Sicherheit

Fragen an Anbieter

- Wie viele meiner bestehenden Investitionen kann Ihre XDR-Plattform nutzen?
- Ist Ihre XDR-Plattform mit meinen Lösungen kompatibel, unabhängig vom Anbieter?
- Lassen sich Ihre Lösungen direkt miteinander integrieren?
- Wie heben sich Ihre Erkennungstechnologien von anderen auf dem Markt ab?
- Welche Art von Bedrohungen erkennt Ihre Lösung? Ordnet sie Warnungen dem MITRE ATT&CK-Framework zu?

3. Unterstützt eine schnelle und präzise Reaktion auf Bedrohungen

Wie schnell können Sie nach der Identifizierung sicher auf Bedrohungen reagieren?

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. Im Idealfall sollten Sie in der Lage sein, die Auswirkungen und den Umfang der Bedrohung von einem Standort aus anzuzeigen und mit nur einem oder zwei Klicks Maßnahmen zu ergreifen. Effektives XDR erfordert native Reaktions- und Problembehebungsfunktionen, z. B. die Isolierung eines Hosts oder das Löschen schädlicher E-Mails aus allen Posteingängen. XDR sollte zudem mit Möglichkeiten zur Automatisierung die Erstellung benutzerdefinierter Reaktionsmaßnahmen erleichtern, damit Teams die Sicherheit im Laufe der Zeit weiterentwickeln können.

Wichtigste Funktionen und Merkmale	Entsprechende Produktbereiche
• Schnelle Reaktion auf Bedrohungen für kompromittierte Endpunkte	Endpoint Detection and Response (EDR)
• Identifizieren und Isolieren der Ursache eines Netzwerkproblems oder -vorfalls innerhalb von Sekunden	Extended Detection and Response (XDR), Network Detection and Response (NDR)
• Schnelles Blockieren schädlicher Websites mit Echtzeit-Click-Time-Analysen	E-Mail-Sicherheit

Fragen an Anbieter

- Welche Antwortaktionen bietet das Produkt?
- Können Korrekturmaßnahmen auf dem Endpunkt mit einer XDR-Lösung an einem Standort durchgeführt und auf andere skaliert werden?
- Wie lässt sich das Produkt in vorhandene Sicherheitstools integrieren, die eine Reaktion ermöglichen?
- Wie beschleunigt Ihre Lösung Korrekturmaßnahmen?
- Von der Bedrohungswarnung bis zu Korrekturmaßnahmen: Wie lange dauert die Reaktionszeit (z. B. bei einem Phishing-Angriff)?

4. Bietet einen zentralen investigativen Standpunkt für ein optimiertes Benutzererlebnis

Werden Ihre Bedrohungserkennung, Ihre Reaktion auf Bedrohungen und Ihre Korrekturmaßnahmen über eine zentrale Schnittstelle gemanagt?

Bei der Bewertung von XDR-Lösungen ist es wichtig, die Erfahrung von SicherheitsanalystInnen zu berücksichtigen. SecOps-Teams haben genug zu managen, sie müssen nicht noch durch Dutzende von Tools und eine Vielzahl von Konsolen ausgebremst werden. Aus diesem Grund empfehlen wir XDR-Lösungen, mit denen AnalystInnen Bedrohungen schneller und effektiver erkennen und darauf reagieren können, indem sie eine einheitliche Ansicht von Sicherheitsdaten über mehrere Sicherheitstools und Datenquellen hinweg bereitstellen. Dadurch können Workflows optimiert und der Zeit- und Arbeitsaufwand für die Untersuchung und Behebung von Sicherheitsvorfällen reduziert werden. XDR-Lösungen sollten ein Dashboard für den gesamten Lebenszyklus bereitstellen, das alle Bedrohungsvektoren und Access Points abdeckt. XDR sollte das Threat-Hunting durch Modelle wie MITRE ATT&CK optimieren, die auch unerfahreneren MitarbeiterInnen Zugang zum hypothesengestützten Threat-Hunting bieten, sodass vorausschauender agiert werden kann. Ein weiterer zu berücksichtigender Faktor ist der Einfluss des Designs auf die Erfahrung der AnalystInnen. Es sollte die Produktivität steigern, die Entscheidungszeit im Zusammenhang mit den wichtigsten Funktionen der Erkennung, Untersuchung und Reaktion verkürzen und es AnfängerInnen und Fortgeschrittenen im Bereich Analysen ermöglichen, innerhalb von Sicherheitsverfahren erweiterte Aufgaben durchzuführen. Hierzu wird besserer Kontext für Warnungen mit fortschrittlicher Offenlegung geboten, damit der Umfang und der Schweregrad einer potenziellen Bedrohung schnell bestimmt werden kann.

Wichtigste Funktionen und Merkmale	Entsprechende Produktbereiche
• Stellt ein Dashboard für den gesamten Lebenszyklus bereit, das alle Bedrohungsvektoren und Access Points abdeckt • Bietet ein einheitliches Toolset, das sich über Ihre ITOps, SecOps und NetOps erstreckt • Zugriff und Management von Daten, Analysen und Automatisierung von einem zentralen Standort aus	Extended Detection and Response (XDR)

Fragen an Anbieter

- Wie hilft Ihre Lösung meinem Team beim Threat-Hunting?
- Wie lässt sich die Lösung in vorhandene Sicherheitstechnologien wie SOAR- und SIEM-Lösungen integrieren?
- Kann ich Ihre XDR verwenden, um die Auswirkungen einer Bedrohung sowie das Ausmaß des Verstoßes zu verstehen und mit einem einzigen Mausklick über eine zentrale Schnittstelle Maßnahmen zu ergreifen?
- Bietet Ihre Lösung Unterstützung für rollenbasierte Sicherheit, indem der gesamte System-/Subsystemzugriff oder Teile davon auf autorisierte Gruppen und einzelne User beschränkt wird?
- Können Sie die Telemetriedaten aus meiner gesamten vorhandenen Sicherheitstechnologie zentralisieren und analysieren?
- Optimiert Ihre Lösung die Incident-Response-Workflows, um den Untersuchungszeitraum insgesamt zu verkürzen?

5. Bietet Möglichkeiten zur Steigerung der Produktivität und zur Stärkung des Sicherheitsstatus

Erhöhen Ihre XDR-Lösungen die Effizienz bei der Bedrohungserkennung und -reaktion, und sind sie mit weniger Aufwand verbunden?

Automatisierung und Orchestrierung sind beim Aufbau der Security Resilience Ihres Unternehmens entscheidend. Ihre SicherheitsmitarbeiterInnen haben wichtige Aufgaben zu erledigen. Wenn sie mit einer Sicherheitsbedrohung konfrontiert sind, müssen sie nicht durch komplizierte, manuelle und sich wiederholende Workflows verschwendet werden. XDR-Lösungen, welche die Produktivität durch die Automatisierung kritischer Workflows steigern – z. B. die Erkennung und Korrelation einer Warnung, Priorisierung und schnelle Reaktion –, entlasten Ihre Teams über den gesamten Lebenszyklus hinweg. Eine effektive XDR-Lösung sollte die durchschnittliche Reaktionszeit verkürzen, indem sie eine Untersuchung ermöglicht, die klare Entscheidungen und Maßnahmen enthält, damit AnalystInnen gemäß ihren Richtlinien und Verfahren automatisiert und konsistent reagieren können. Das bedeutet, dass Ihre SecOps-Teams ihre Zeit und Energie in strategischere und proaktive Sicherheitsaufgaben investieren können, um den Sicherheitsstatus Ihres Unternehmens weiter zu stärken.

Wichtigste Funktionen und Merkmale	Entsprechende Produktbereiche
• Automatisches Threat-Hunting für Endpunkte, einschließlich Bedrohungen mit geringer Prävalenz • Admins das Schreiben und Scannen nach benutzerdefinierten Indicators of Compromise (IoCs) ermöglichen	Endpoint Detection and Response (EDR)
• Vorausschauende Eindämmung von Netzwerkbedrohungen durch verhaltensanalytische Einblicke	Extended Detection and Response (XDR), Network Detection and Response (NDR)
• Automatische Priorisierung von Korrekturmaßnahmen bei E-Mail-Bedrohungen	E-Mail-Sicherheit

Fragen an Anbieter

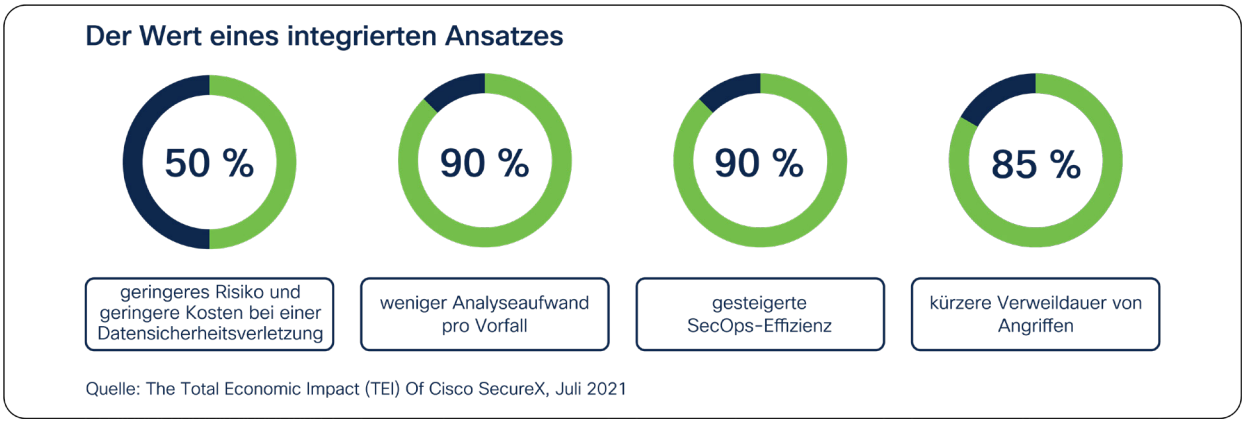
- Behindern API-Änderungen der Anbieter Ihre Automatisierungsskripte in Drittanbieterintegrationen?
- Wie unterstützt Ihre Lösung das Monitoring der Datenströme von und zu Cloud-basierten Workloads?
- Muss ich mit der XDR-Lösung die Umgebung ändern oder neue Technologien bereitstellen?
- Bietet Ihre XDR-Lösung vorgefertigte und sofort einsatzbereite Integrationen mit Sicherheitstechnologie von Drittanbietern?
- Verkürzt die XDR-Lösung die Zeit, die AnalystInnen für die Untersuchung und Behebung eines Vorfalls benötigen?
- Kann Ihre XDR-Lösung Ihr Richtlinienmanagement verbessern und so für mehr Widerstandsfähigkeit sorgen?

Cisco XDR

XDR ist eine wichtige Komponente der Security Resilience

Heutzutage ist Unsicherheit die Regel. Als Reaktion darauf investieren Unternehmen in allen Geschäftsbereichen in Widerstandsfähigkeit – von der Finanzierung bis hin zu Lieferketten. Doch diese werden ohne Investitionen in die Security Resilience nicht ausreichen. Dabei handelt es sich um die Fähigkeit, das eigene Unternehmen vor Bedrohungen und Störungen zu schützen und souverän auf Veränderungen zu reagieren, damit es noch gestärkter daraus hervorgeht.

XDR ist eine wichtige Komponente für die Security Resilience Ihres Unternehmens. Wenn Sie XDR richtig umsetzen, wird Ihr Sicherheitsstatus verbessert, indem Ihre Sicherheitsteams dabei unterstützt werden, Bedrohungen nach Auswirkungen zu priorisieren, Bedrohungen früher zu erkennen und die Reaktion zu beschleunigen. Automatisierungs- und Orchestrierungsfunktionen erleichtern diesen Prozess und entlasten Sicherheitsteams, damit diese sich auf das Wesentliche konzentrieren können.



Vereinfachte Sicherheitsverfahren mit Cisco XDR

Cisco ist führend im Bereich XDR und bietet das umfassendste Sicherheitsportfolio auf dem Markt. Wir bei Cisco haben proaktiv in die Schaffung des umfassendsten Sicherheitsportfolios auf dem Markt investiert, um die Sicherheitsanforderungen der Zukunft vorherzusehen und die Komponenten so zu integrieren, dass effektive Sicherheit für alle Teams, unabhängig vom Anbieter oder Vektor, einfach und zugänglich gemacht wird. Wir wissen, dass der Aufbau eines XDR-Ansatzes ein Prozess ist. Und wir möchten, dass Ihre Teams aus dem Teufelskreis der Patchwork-Abdeckung in einer Branche voller Punktlösungen ausbrechen können. Mit Cisco XDR möchten wir den kürzesten Weg von der Erkennung bis zur Reaktion mit der geringsten Reibung ermitteln.

Cisco XDR wurde von SOC-ExpertInnen für SOC-ExpertInnen entwickelt und vereinfacht Sicherheitsverfahren, damit SicherheitsanalystInnen proaktiv und gegenüber den komplexesten Bedrohungen widerstandsfähig bleiben. Unsere Lösung ist offen, erweiterbar und basiert auf dem Cloud-First-Ansatz, sodass Sie vorhandene Sicherheitsinvestitionen nutzen und in Ihrer gesamten Umgebung von einer einheitlichen Sicherheitserkennung profitieren.

Wir bei Cisco nehmen den Schutz von Kundenressourcen ernst, da wir auch Kunden unserer Kunden sind. Wir möchten mit Ihnen auf Ihrer Journey hin zu Security Resilience über die Cisco Security Cloud zusammenarbeiten – einer offenen Sicherheitsplattform, über die Sie Ihr gesamtes Ecosystem schützen können, unabhängig davon, was als Nächstes kommt. Erleben Sie die Vorteile umfassender Sicherheit.

Sind Sie bereit, heute schon die Sicherheitsverfahren von morgen zu entwickeln?

Cisco XDR entdecken

Wichtigste XDR-Elemente und -Funktionen

Nutzen Sie diese Tabelle (Seiten 10–11) als Kurzanleitung bei Gesprächen mit XDR-Anbietern.

Schlüsselelement	Wichtigste Funktionen	Entsprechende Cisco Produkte
Bietet priorisierte und aussagekräftige Telemetrie, wo immer Sie sie benötigen	• Integrierte, vollständig verwaltbare Endpoint Detection and Response (EDR), proaktives Threat-Hunting • Integriertes risikobasiertes Schwachstellenmanagement, das eine schnelle Identifizierung von Schwachstellen, Risikobewertung, Priorisierung und Problembehebung ermöglicht	Cisco Secure Endpoint
	• Kontinuierliche Analyse der Cloud-Aktivität • Fortschrittliche Analysen, einschließlich verhaltensbasierter Modellierung und Machine-Learning-Algorithmen • Überblick über Ihre Sicherheitsinfrastruktur für einheitliche Transparenz und aggregierte, aussagekräftige Informationen	Cisco XDR
	• Erweiterte Outbreak-Filter mit Echtzeit-Click-Time-Analysen	Cisco Secure Email
Ermöglicht eine einheitliche Erkennung, unabhängig von Vektor oder Anbieter	• Laufzeiterkennung und Blockierung von ungewöhnlichem Programmverhalten • Erweiterte Betriebssystemabfragen auf dem Endpunkt in Echtzeit • Integriertes Threat-Hunting, das dem MITRE ATT&CK-Framework zugeordnet ist	Cisco Secure Endpoint
	• Erkennen von Echtzeit-Angriffen in der Cloud mit High-Fidelity-Warnungen, die mit Kontextinformationen (z. B. User, Gerät, Standort, Zeitstempel und Anwendung) angereichert sind • Erkennen und Isolieren von Bedrohungen mit bestätigten Erkennungen • Erkennen nicht autorisierter Entitäten mit NDR und Automatisieren der Quarantäne mit Endpunkten • Erkennen interner Hosts, die mit einem externen Host kommunizieren • Ein umfassender Prüfpfad für alle Cloud-Transaktionen ermöglicht effektivere forensische Untersuchungen • Integrierte Integrationen in andere XDR-Lösungen im Portfolio • In Lösungen von Drittanbietern integrierte, vorkonfigurierte oder benutzerdefinierte Integrationen für eine vernetzte Back-End-Architektur und ein konsistentes Front-End-Erlebnis • Integrierte Integrationen in andere Technologien für die Cloud, Endpunkte, Netzwerke und Anwendungen (einschließlich anderer Technologien von Drittanbietern)	Cisco Secure Network Analytics und Cisco XDR
	• URL-bezogener Spam-Schutz und Kontrolle, leistungsstarke Virenprüfung, Outbreak-Filter und Reputationsprüfung für Domänenfunktionen • Erkennung gefälschter E-Mails zum Schutz vor BEC-Angriffen auf Führungskräfte • Automatisierte Malware-Analyse und Sandboxing	Cisco Secure Email

Schlüsselelement	Wichtigste Funktionen	Entsprechende Cisco Produkte
Unterstützt eine schnelle und präzise Reaktion auf Bedrohungen	• Zugriff auf durchgängigen Schutz mit Threat-Intelligence und gebündelte Einblicke aus dedizierten globalen Security Operations Centers (SOCs) für einen breiten Kundenstamm	Alle Cisco Secure-Produkte
	• Kontinuierliches Monitoring aller Endpunktaktivitäten mit Laufzeiterkennung und Blockierung ungewöhnlichen Verhaltens	Cisco Secure Endpoint
	• dentifizieren und Isolieren von Bedrohungen im verschlüsselten Datenverkehr, ohne Datenschutz und Datenintegrität zu gefährden • Auslösen von „Response“-Workflows von einem Standort aus • Reaktion auf Bedrohungen, die über APIs kontextbezogenes Bewusstsein aus Datenquellen für Sicherheitsprodukte sowie globale Threat-Intelligence von Talos® und Quellen von Drittanbietern aggregiert • Erstellen von Fallbüchern zur Untersuchung forensischer Vorfälle	Cisco XDR
	• Dauerhafter Schutz vor URL-basierten Bedrohungen durch die Echtzeit-Analyse von potenziell schädlichen Links • Kontinuierliche Nutzung von Echtzeit-Monitoring, Analysen und Threat-Intelligence von Talos® zur Identifizierung bisher unbekannter Bedrohungen oder plötzlicher Veränderungen	Cisco Secure Email
Bietet einen zentralen investigativen Standpunkt für ein optimiertes Benutzererlebnis	• Sammeln und Korrelieren globaler Informationen in einer einzigen Ansicht für eine schnellere Bedrohungsuntersuchung • Erstellen benutzerdefinierter Antwortaktionen zur Verkürzung der Reaktionszeit • Automatisieren der Anreicherung aus mehreren Datenquellen, kombiniert mit Threat-Intelligence	Cisco XDR
Bietet Möglichkeiten zur Steigerung der Produktivität und zur Stärkung des Sicherheitsstatus	• Automatische Identifizierung und Bedrohungsanalyse von ausführbaren Dateien mit geringer Prävalenz • Möglichkeit, benutzerdefinierte IoCs zu schreiben, um die gesamte Endpunktbereitstellung nach Kompromittierungsindikatoren zu scannen	Cisco Secure Endpoint
	• Verhaltensmodellierung, mehrschichtiges Machine Learning und globale Threat-Intelligence • Automatische Klassifizierung neuer Geräterollen nach dem Hinzufügen zum Netzwerk • Integration in eine XDR-Lösung zur Automatisierung aller Bedrohungsvektoren und Access Points	Cisco Secure Network Analytics und Cisco XDR
	• Automatische Auslösung dynamischer Reputationsanalysen und Bereitstellung von Transparenz darüber, wo E-Mail-Malware ihren Ursprung hatte, welche Systeme betroffen waren und was die Malware bewirkt • Ergreifen von Maßnahmen basierend auf Einblicken für Korrekturmaßnahmen sowohl für eingehende als auch für ausgehende E-Mails	Cisco Secure Email
	• Automatisieren von Routineaufgaben mit vorgefertigten Workflows, die für gängige Anwendungsfälle ausgelegt sind • Gemeinsame Nutzung von Leitfäden für SecOps-Teams • Automatisierte Vorselektion und Priorisierung von Warnungen aus anderen Sicherheitsportfolio-Lösungen	Cisco XDR

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 C07-3236254-03 04/23