# Vereinfachte Sicherheitsverfahren mit Cisco XDR

## Bessere Erkennung, schnellere Reaktion und gesteigerte Produktivität

Cisco XDR verändert die Art und Weise, wie Sicherheitsteams Vorfälle erkennen und darauf reagieren. Unsere Cloud-basierte Lösung vereinfacht Sicherheitsverfahren und versetzt Sicherheitsteams in die Lage, selbst besonders komplexe Bedrohungen zu erkennen, zu priorisieren und darauf zu reagieren. Da sich Cisco XDR in das umfassende Cisco Security-Portfolio und eine Reihe wichtiger Drittanbieterangebote integrieren lässt, ist die Lösung eine der umfassendsten und flexibelsten auf dem heutigen Markt.

Cisco XDR wurde von SicherheitsexpertInnen für SicherheitsexpertInnen entwickelt und hilft AnalystInnen dabei, Daten aus mehreren Quellen zu einer einheitlichen Ansicht zu aggregieren und zu korrelieren, um Untersuchungen zu optimieren, falsch-positive Meldungen zu reduzieren, Warnungen zu priorisieren und die Dauer von der Erkennung bis zur Reaktion deutlich zu verkürzen.

Integrierte Automatisierung, Orchestrierung und geführte Problembehebungsempfehlungen helfen AnalystInnen, sich wiederholende Aufgaben zu automatisieren und Bedrohungen effektiver abzuwehren. Dadurch sparen sie Zeit und Ressourcen, um sich auf andere kritische Sicherheitsaufgaben konzentrieren zu können.

Der datengesteuerte Ansatz von Cisco XDR ermöglicht es SOC-Teams, die Ereignisse mit den größten Auswirkungen zu bestimmen und Strategien für Korrekturmaßnahmen darauf zu konzentrieren, um den allgemeinen Sicherheitsstatus des Unternehmens zu stärken und die Widerstandsfähigkeit zu erhöhen.

# Vorteile

## Vereinheitlichung von Einblicken unabhängig vom Anbieter oder Vektor zur Vermeidung von Transparenzproblemen

**Erhalten Sie transparente Einblicke und identifizieren Sie Bedrohungen im gesamten Netzwerk, in der Cloud, auf Endpunkten, in E-Mails und in Anwendungen, um in Umgebungen mit verschiedenen Anbietern und Vektoren eine effektive Sicherheit zu erreichen.**

Durch die Korrelation von Daten aus mehreren unterschiedlichen Erkennungstechnologien in einer einheitlichen Ansicht ermöglicht Cisco XDR schnellere, einfachere Untersuchungen und eine optimierte Incident Response.

## Beschleunigung der Bedrohungserkennung und Reaktion für eine angemessene Priorisierung

**Korrelieren Sie Erkennungen über mehrere Telemetriequellen hinweg, um Bedrohungen nach dem größten Risiko zu priorisieren.**

Durch den Einsatz von künstlicher Intelligenz und Machine Learning ermöglicht Cisco XDR eine korrelierte Erkennung mit hoher Genauigkeit, reduziert Datenmüll und gleicht Sicherheitsrisiken effektiv mit Geschäftsrisiken ab.

## Automatisierte Reaktion mit nachweisbasierten Empfehlungen zur Minimierung von Auswirkungen

**Beheben Sie Bedrohungen zuverlässig mit Automatisierung und geführten Reaktionsempfehlungen für alle relevanten Kontrollpunkte.**

Durch die verkürzte Untersuchungszeit und die Beschleunigung von Reaktionen stoppt Cisco XDR die Aufstockung der SOC-Teams und stärkt die Widerstandsfähigkeit.

# Umfassende Bedrohungserkennung und Antwortaktionen mit datengestützten Einblicken

## Schnellere Erkennung von komplexen Bedrohungen

- Cisco XDR bietet das breiteste Spektrum an Integrationsmöglichkeiten, beispielsweise in Endpunkte, E-Mail-Lösungen, Netzwerke, Clouds und Firewalls, sowie Integrationen in ausgewählte Lösungen von Drittanbietern, was eine besonders flexible, skalierbare und effektive XDR-Strategie ermöglicht.
- Nutzen Sie die Telemetrie aus lokalen Netzwerken sowie aus Public und Private Clouds, um Bedrohungen auf verwalteten und nicht verwalteten Geräten zu erkennen und kritischen Kontext bei der Korrelation von Ereignissen zu erhalten – etwa zum Ausgangspunkt von Angriffen und ihrer Ausbreitung im Netzwerk.
- Die Talos Threat-Intelligence stärkt die Erkennungsfunktionen, sodass AnalystInnen eine beispiellose Sammlung an aussagekräftigen Informationen erhalten. Dank umfangreicherem Kontext und einem besseren Verständnis des Verhaltens von echten Bedrohungen können sie bekannte und neue Bedrohungen besser aufdecken.

## Priorisierung von Bedrohungen nach ihren Auswirkungen und schnellere Reaktionen

- Die risikobasierte Priorisierung hilft SOC-AnalystInnen, sich auf die Warnungen zu konzentrieren, welche die größte Bedrohung darstellen, um schnell und effektiv zu handeln. Dieser einzigartige Ansatz bietet eine einheitliche Ansicht der Warnungen, priorisiert nach dem vorliegenden Schweregrad.
- Reduzieren Sie die mittlere Reaktionszeit (MTTR) durch geführte Reaktionen zur Identifizierung, Eindämmung und Beseitigung von Bedrohungen bzw. zur anschließenden Wiederherstellung. Nutzen Sie zudem eingebettete Antwortaktionen, die eine konsistente und effektive Entscheidungsfindung ermöglichen.

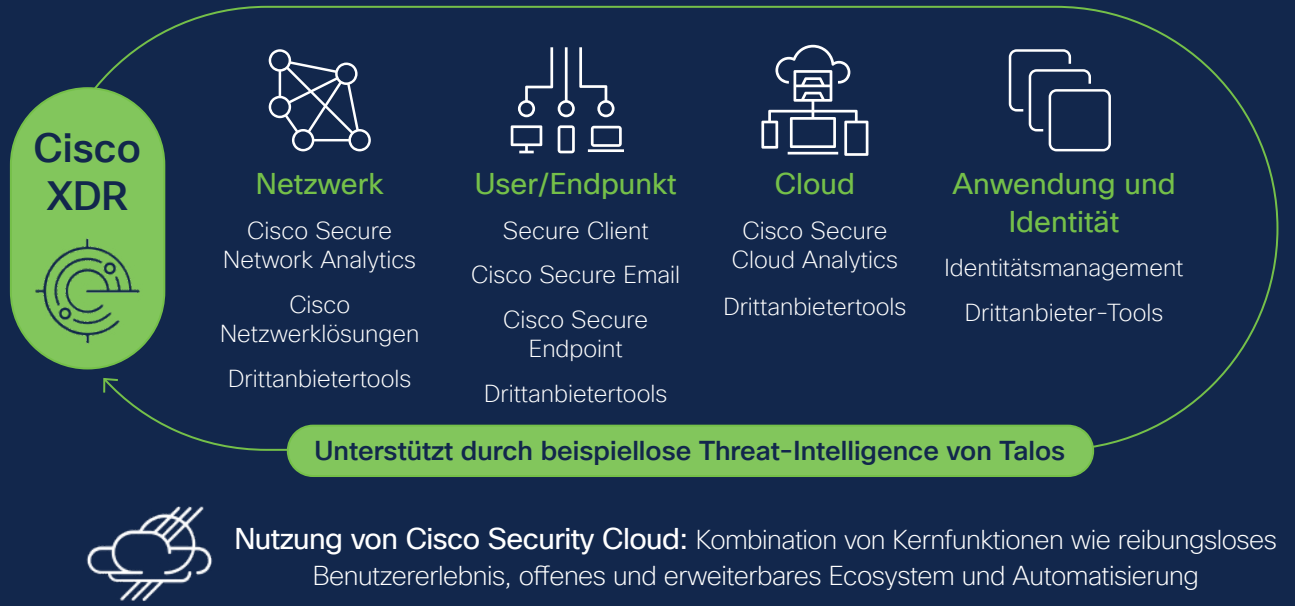
## Beschleunigung der Reaktionszeiten

- Beseitigen Sie Bedrohungen schnell mit integrierten Antwortaktionen und Orchestrierung. Mit Cisco XDR können SOC-Teams eine Reihe von vorgefertigten oder anpassbaren Arbeitsmappen zur Orchestrierung nutzen, um mit nur wenigen Klicks Bedrohungen abzuwehren und Risiken zu minimieren.
- Nutzen Sie begrenzte Ressourcen besser aus, indem Sie sich wiederholende und zeitaufwendige Aufgaben automatisieren und SOC-Teams sofort einsatzbereite Best Practices bereitstellen. Wenn Automatisierung keine Option ist, bietet Cisco XDR geführte Reaktionsvorschläge und Empfehlungen, um SOC-AnalystInnen dabei zu unterstützen, effektive Antwortaktionen durchzuführen.
- Unterstützen Sie schnell Antwortaktionen auf verschiedensten Security-Tools dank umfassenden Integrationen mit unterschiedlichen Sicherheits-kontrollpunkten, sowohl bei integrierten Cisco Lösungen als auch bei Drittanbieterlösungen. Gehen Sie die Nachverfolgung von Bedrohungen proaktiv an, indem Sie unterschiedliche Warnprotokolle untersuchen, sobald Sie Kenntnis von neuen Taktiken, Techniken und Indikatoren für Kompromittierung erhalten.

## Optimierte Untersuchungen:

- Vereinfachen und verkürzen Sie die Untersuchungszeiten mit einheitlichem Kontext und fortschrittlichen Offenlegungstechniken. Cisco XDR zeigt AnalystInnen die Informationen, die sie benötigen, um aktuelle Aufgaben zu bewältigen – und das, ohne sie mit unnötigen Daten zu überschwemmen, die Analysen unnötig erschweren. Wenn nötig, sind weitere Informationen zur Anreicherung von Untersuchungen nur einen Klick entfernt.
- SOC-AnalystInnen können Warnungen, globale Intelligence und lokalen Kontext aggregieren, um die Ursache und den gesamten Umfang der Auswirkungen nachzuvollziehen und auf alle Fälle vorbereitet zu sein.

# XDR für alle Ihre Anforderungen




**Nutzung von Cisco Security Cloud:** Kombination von Kernfunktionen wie reibungsloses Benutzererlebnis, offenes und erweiterbares Ecosystem und Automatisierung

## Erfahren Sie mehr über Cisco XDR: cisco.com/go/xdr