Cisco Xtended Detection & Response

"Wie die Deutsche Telekom und Cisco mit Hilfe von KI ihre Welt sicherer machen"

Tom Georg, Cisco Systems GmbH

November 2024

Die Bedrohungslage nimmt zu !

tagesschau.de

Startseite Videos & Audios Inland Ausland Investigativ Wirtschaft Wahlen

Startseite › Wirtschaft › Bitkom: Rekordschäden durch Attacken auf Konzerne

Bitkom-Untersuchung

Rekordschäden durch Attacken auf Konzerne

Stand: 06.11.2019 12:28 Uhr

Sabotage, Datendiebstahl oder Spionage: Attacken auf deutsche Unternehmen verursachen jährlich einen Schaden von mehr als 100 Milliarden Euro. Der

DEUTSCHER LEBENSMITTELHÄNDLER

Tegut-Daten nach Hackerangriff im Darknet

VON PATRICIA ANDREAE - AKTUALISIERT AM 18.05.2021 - 22:35

Netzpalaver

KI-gestützte Angriffe stellen das größte Risiko dar

Der Anbieter von Zero-Trust- und Zero-Knowledge-Lösungen zum Schutz von Anmeldedaten, privilegiertem Zugang und Remote-Verbindungen,...

26.03.2024

it-daily

Sicherheitsvorhersagen für 2024: KI-unterstützte Cyberangriffe auf dem Vormarsch - Onlineportal von IT Management

Trend Micro stellt seine Cybersicherheitsvorhersagen für das kommende Jahr vor. Darin warnt das Unternehmen vor der transformativen Rolle...

04.01.2024

BIG direkt gesund

MATERNA

adesso people. technology

Continental The Future in Motion

BKA-Lagebericht

Cybercrime nimmt weiter zu

Stand: 10.05.2021 17:16 Uhr

connect professional

Mit KI gegen KI - Security

Für Cyberkriminelle bieten fortschrittliche Algorithmen und maschinelles Lernen optimale Bedingungen, um Angriffe zu optimieren und...

13.12.2023

Zeit Online

NRW: Hackerangriff legt IT-Infrastruktur von 70 Kommunen lahm

Die IT-Systeme von zahlreichen Kommunen in NRW sind seit Montag außer Betrieb.

Digital Business Cloud

KI Cybersecurity: Wie schützt man sich vor einem KI-Hackerangriff?

KI Cybersecurity. Künstliche Intelligenz hat sich aber auch als ein unverzichtbares Werkzeug in der Abwehr von Cyberattacken etabliert. Durch...

08.03.2024

METRO

heute

Kein Publikumsverkehr in Ämtern

IT-System der Stadt Frankfurt off

19.12.2019 08:31 Uhr

Eine E-Mail mit Schadsoftware hat die Behörden in Frankfurt am Main a

thyssenkrupp

SPIEGEL ONLINE SPIEGEL+ Anmelden

LKA eingeschaltet

"Schwerwiegender IT-Sicherheitsvorfall" an der Universität Gießen

Die Uni Gießen hat alle ihre Server aus Sicherheitsgründen heruntergefahren. Die Ursache des Vorfalls ist noch unklar, aber das Landeskriminalamt sowie die Generalstaatsanwaltschaft wurden eingeschaltet.

Digital Business Cloud

Anstieg der KI-gesteuerten Attacken um 60 Prozent

Anstieg der KI-gesteuerten Attacken um 60 Prozent. Die Verteilung der weltweiten Phishing-Angriffe im Jahr 2023. (Bild: Zscaler) arrow forward Image Zoom.

Branche:	Attacken in %
Fertigung	22,90%
Bauwesen	11,70%
Unternehmensdienstleistungen	8,40%
Tech/IT	8,40%
Transportwesen	6,10%

INFOPOINT SECURITY

Cyber-Angriff auf GitHub-Verzeichnisse zeigt die Gefahr von Supply-Chain-Attacken

Der bessere Algorithmus gewinnt…

„Gute“ KI gegen „Böse“ KI

Herkömmliche Security-Ansätze können diese nicht mehr aufdecken oder abwehren…

Die Lage ist ernst: Jeden kann es treffen

Unzureichend vorbereitete und übertrieben selbstbewusste Unternehmen/Behörden

Cisco Cybersecurity Readiness Index | 2024

3 %

aller Unterne
sind bestmöglich
vorbereitet

+220

Milliarden € Schaden durch CyberCrime

Die eigene IT-Abhängigkeit steigt...

~206 **Tage** bis ein Datenleck indentifiziert ist

Höhere Sicherheitsmaßnahmen aufgrund neuer Regularien und komplexerer Bedrohungen notwendig.

KRITIS, DORA und/oder NIS2
Was muss ich tun ?

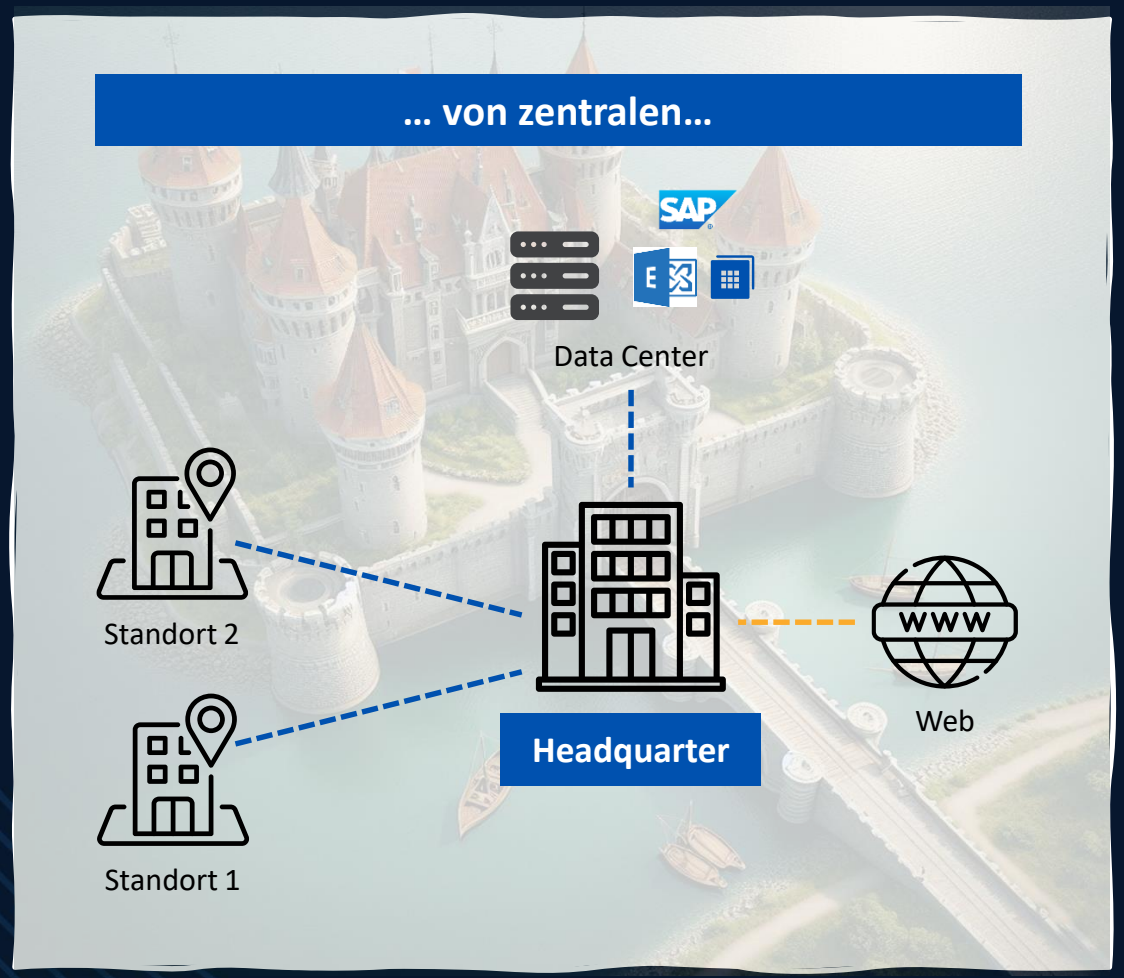
Source: Verizon 2023 Data Breach Investigations Report

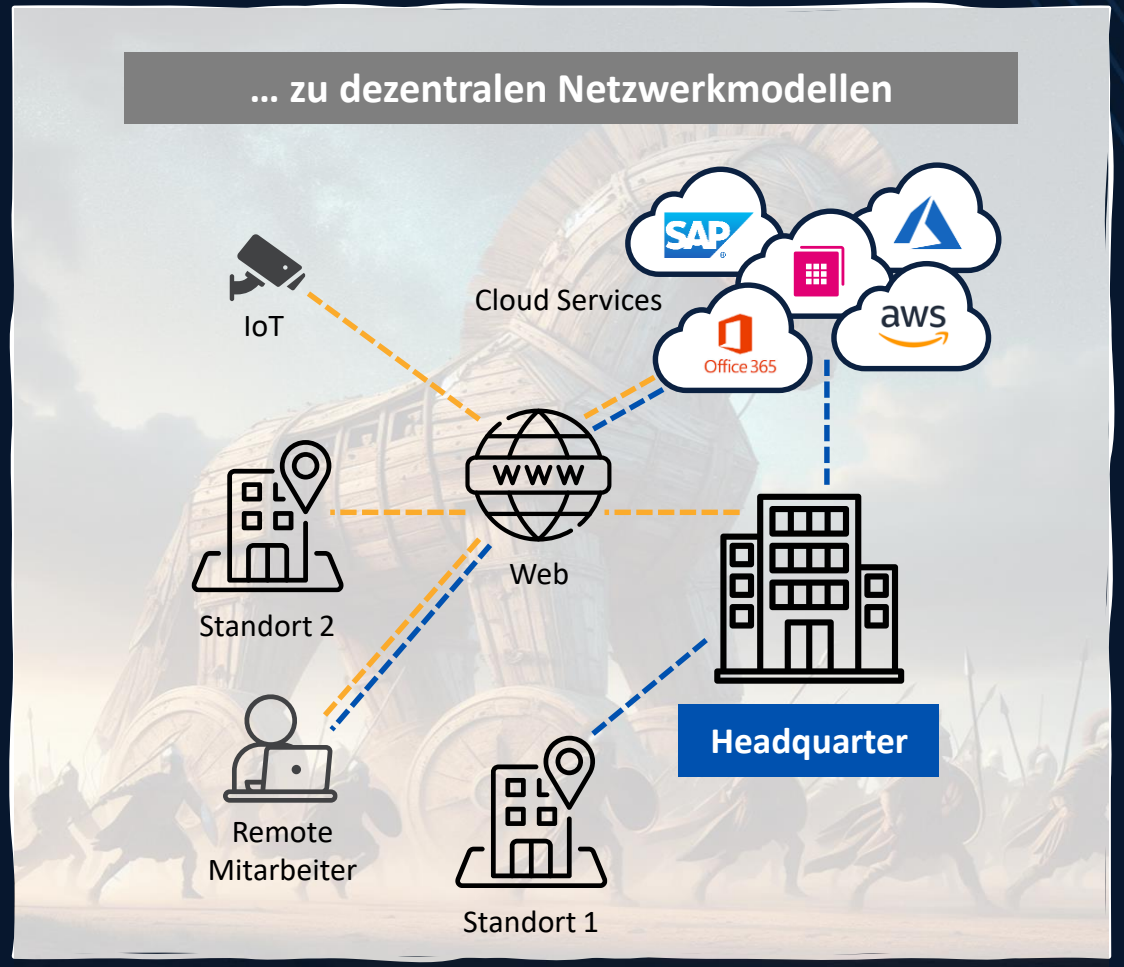
Die Folgen …

- **Finanzielle Risiken**
- **Produktionsausfälle**
- **Reputationsverlust**
- **Datenverlust**
- **Persönliche Risiken**

Was hat sich verändert ?

Das Netz hat sich verändert ...





Komplexität schafft Risiko…

…und eine massiv gewachsene Angriffsfläche

Was ist die bisherige Antwort ?!

Jede neue Bedrohung, ein neues Security Tool

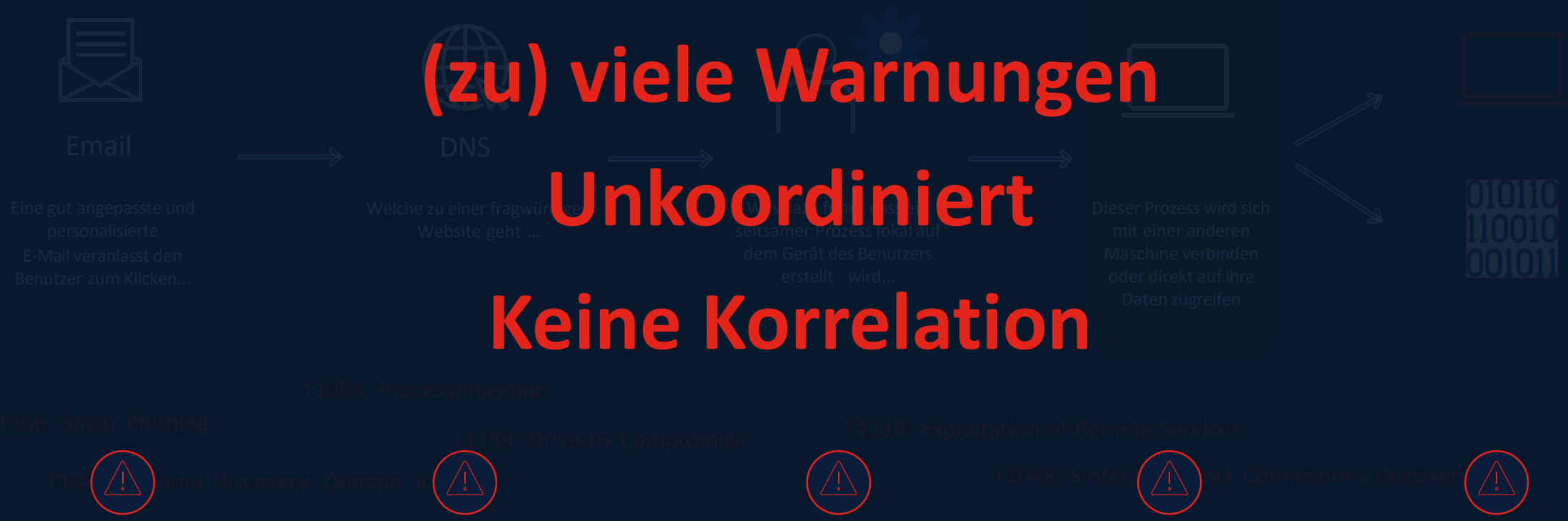
* +19 % in den letzten zwei Jahren, von 64 auf 76; Quelle: PANASEER, 2022

Würden Sie hier mitfliegen ?

Schauen wir uns mal eine Attacke an ...

Die meisten Angriffe verwenden diese Abfolge…

Ransomware Angriffsvektor Email - Isolierte Datenquellen



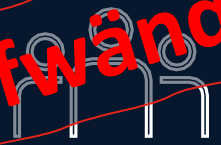
(zu) viele Warnungen

Unkoordiniert

Keine Korrelation

Was hören wir von unseren Kunden...

Aufwändig



Das Management der verschiedenen Security Tools ist über mehrere Partnerunternehmen verteilt. Ad-hoc Änderungen (z.B. Freigaben, Sperrlisten) sind so nur mit Aufwand möglich.

Komplex

Manuell

Unkoordiniert

Prozesse?

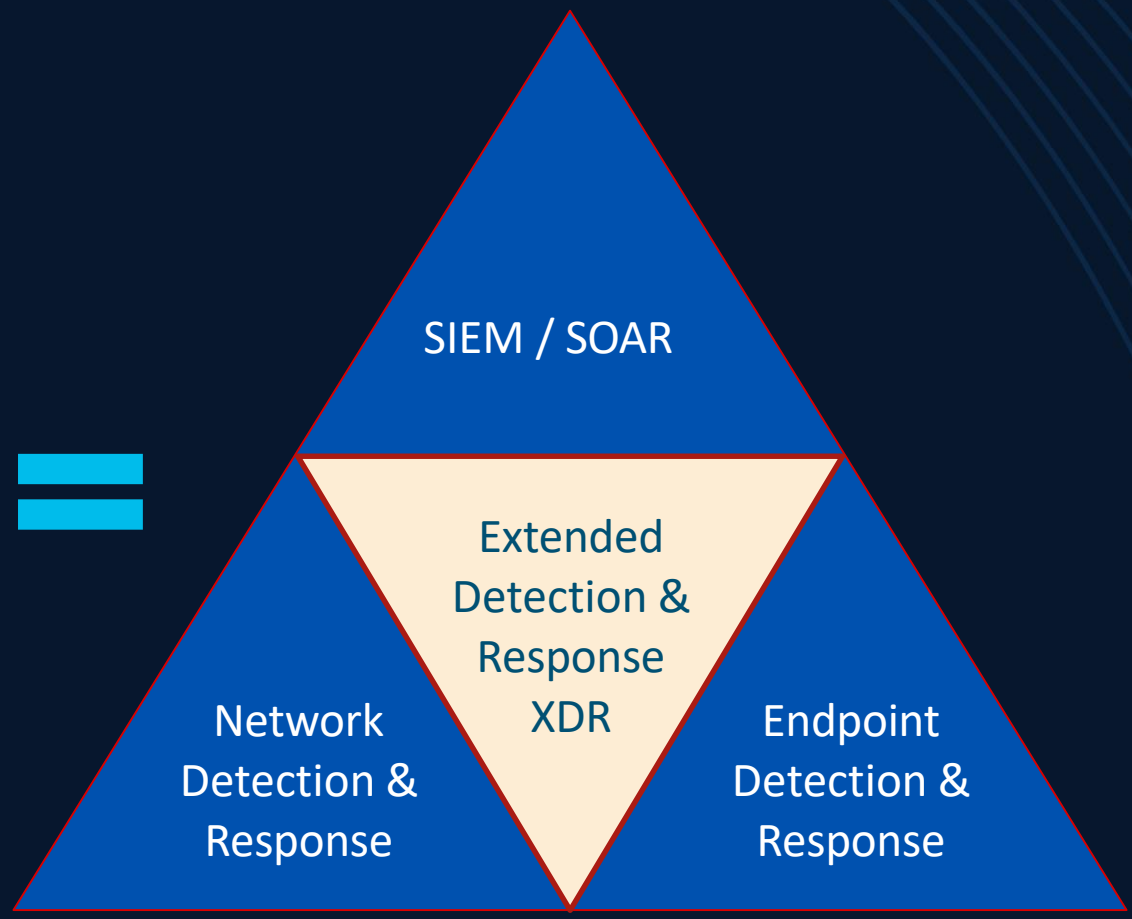
Überfordert

When something impacts your operations, how do you know what went wrong?

**** Wenn etwas Ihre Abläufe beeinträchtigt, **wie finden Sie heraus**, was schiefgelaufen ist? ****

Fragen über Fragen …

- **WER** oder **WAS** ist alles betroffen?
- **WIE** kam der Angriff in unsere IT?
- **WANN** fand das erste Eindringen statt?
- **WO** genau fand im Netzwerk eine Querbewegung statt?



Verhaltensbasierte Analyse und automatisierte Reaktion durch Cross- domain native Telemetrie-Daten und Nutzung von künstlicher Intelligenz

1, 2, 3 einfache Schritte

1
Data collection

Automatisierte Bedrohungs-erkennung

2
Actionable intelligence

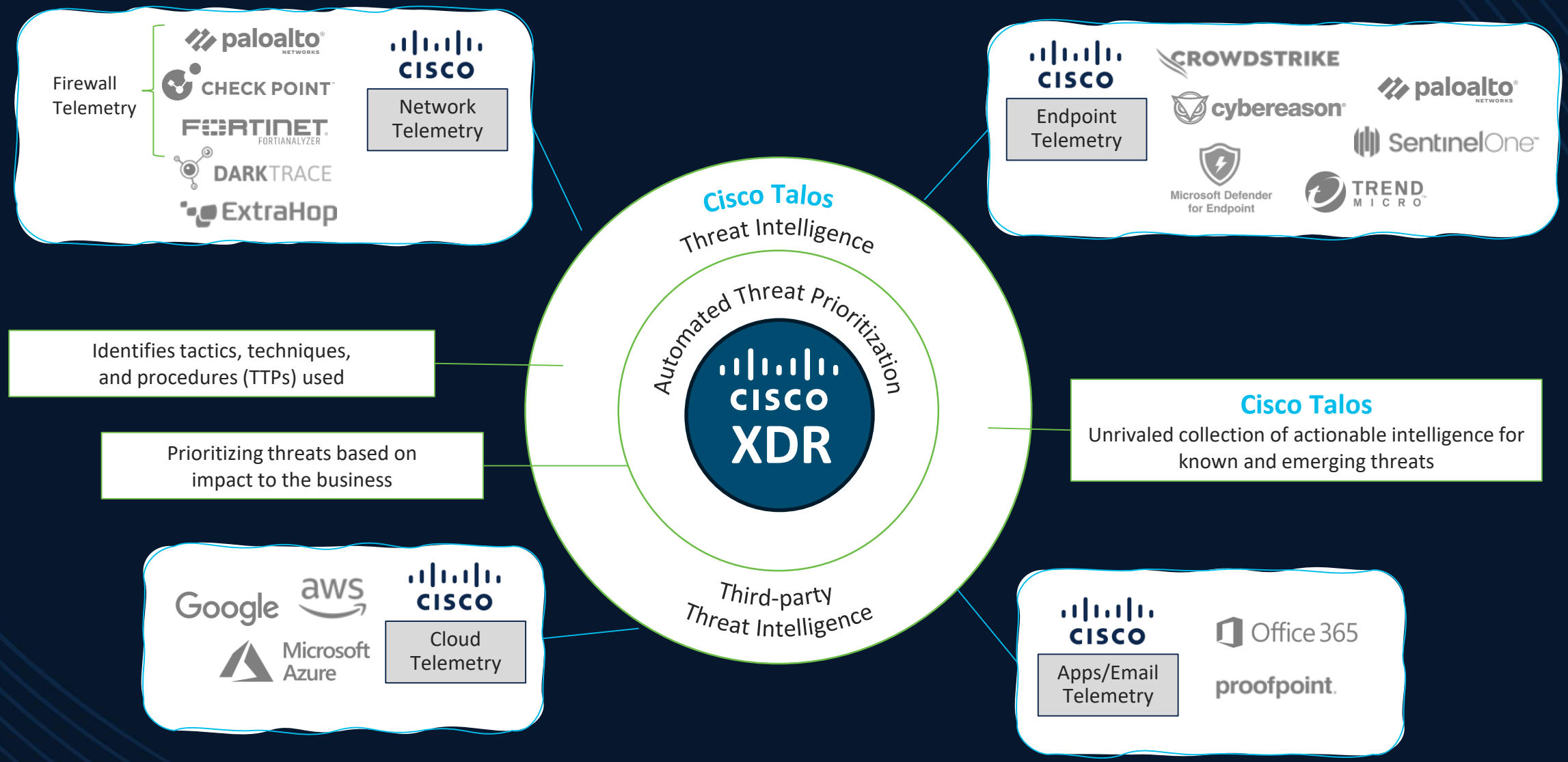
Umfassende Bedrohungs-analyse

3
Simplified security operations

Koordinierten Reaktions-maßnahmen

Wie geht das ?!

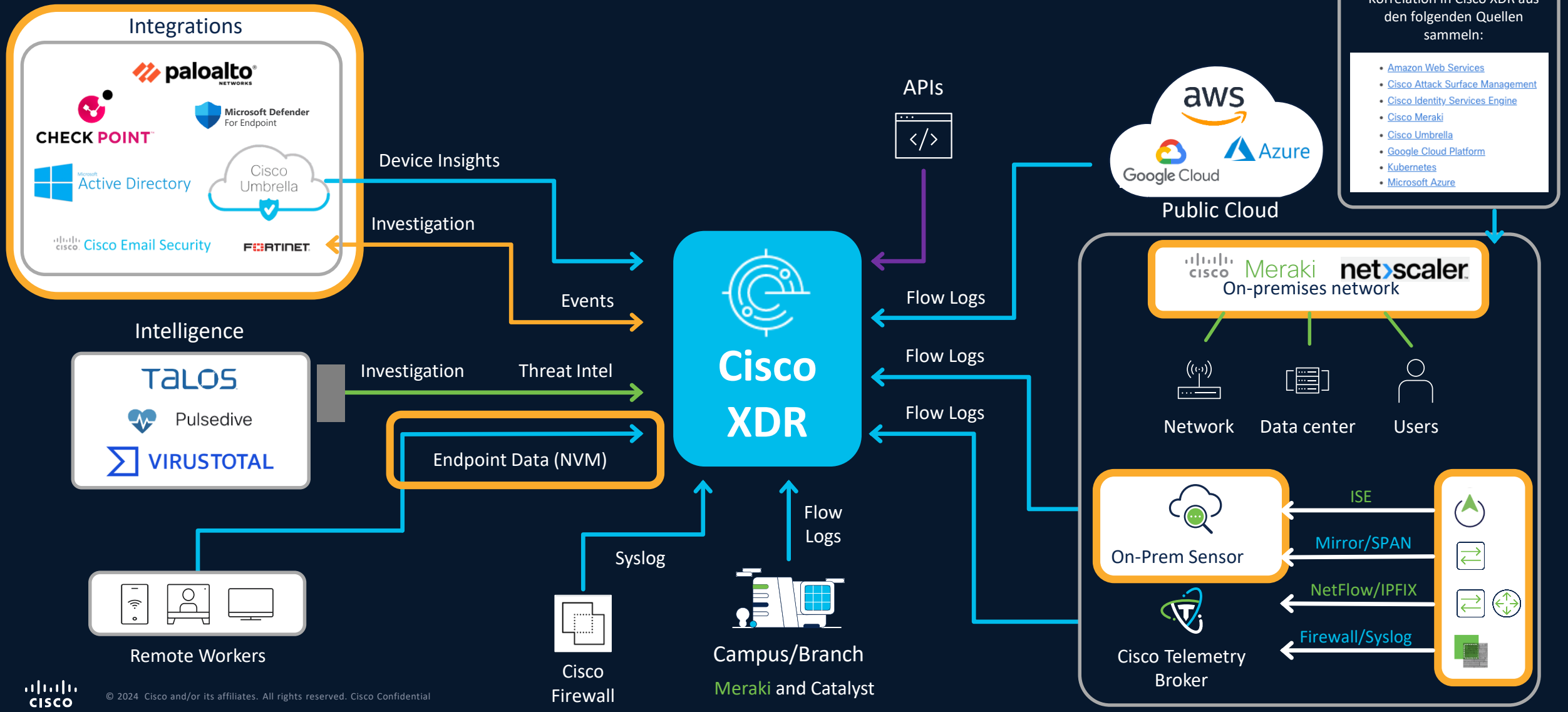
...durch Hersteller übergreifende Integration



Was wird gesammelt ?!

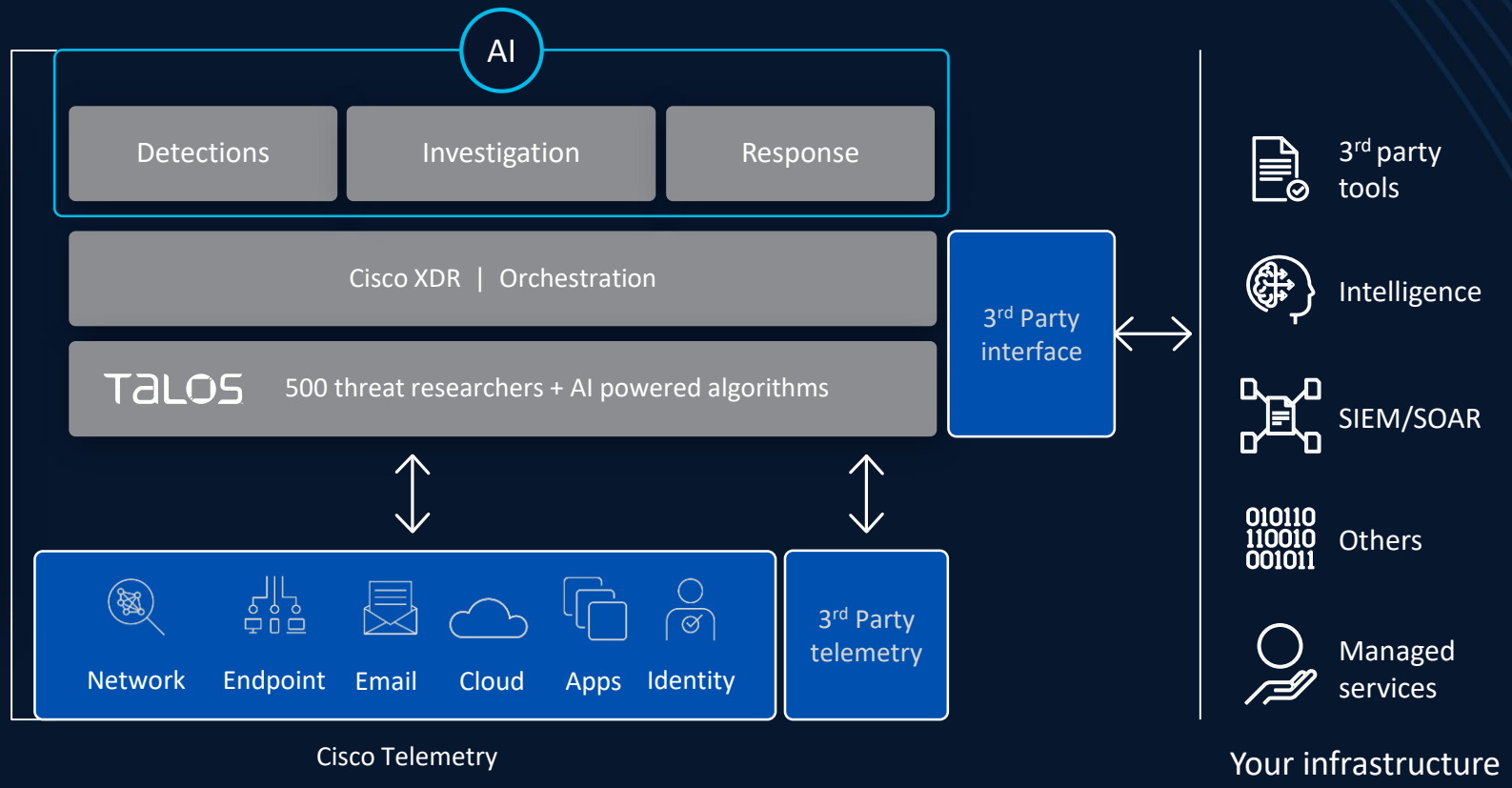
Telemetriequellen für Cisco XDR

Flexible Integration für bestehende Infrastruktur



Komplexität, simplifiziert mit XDR + KI

CISO | SOC Director | SecOps Analyst | Incident Responder



Power of data

Multi-vector detection with unmatched data across humans, machines, and services

Power of analytics

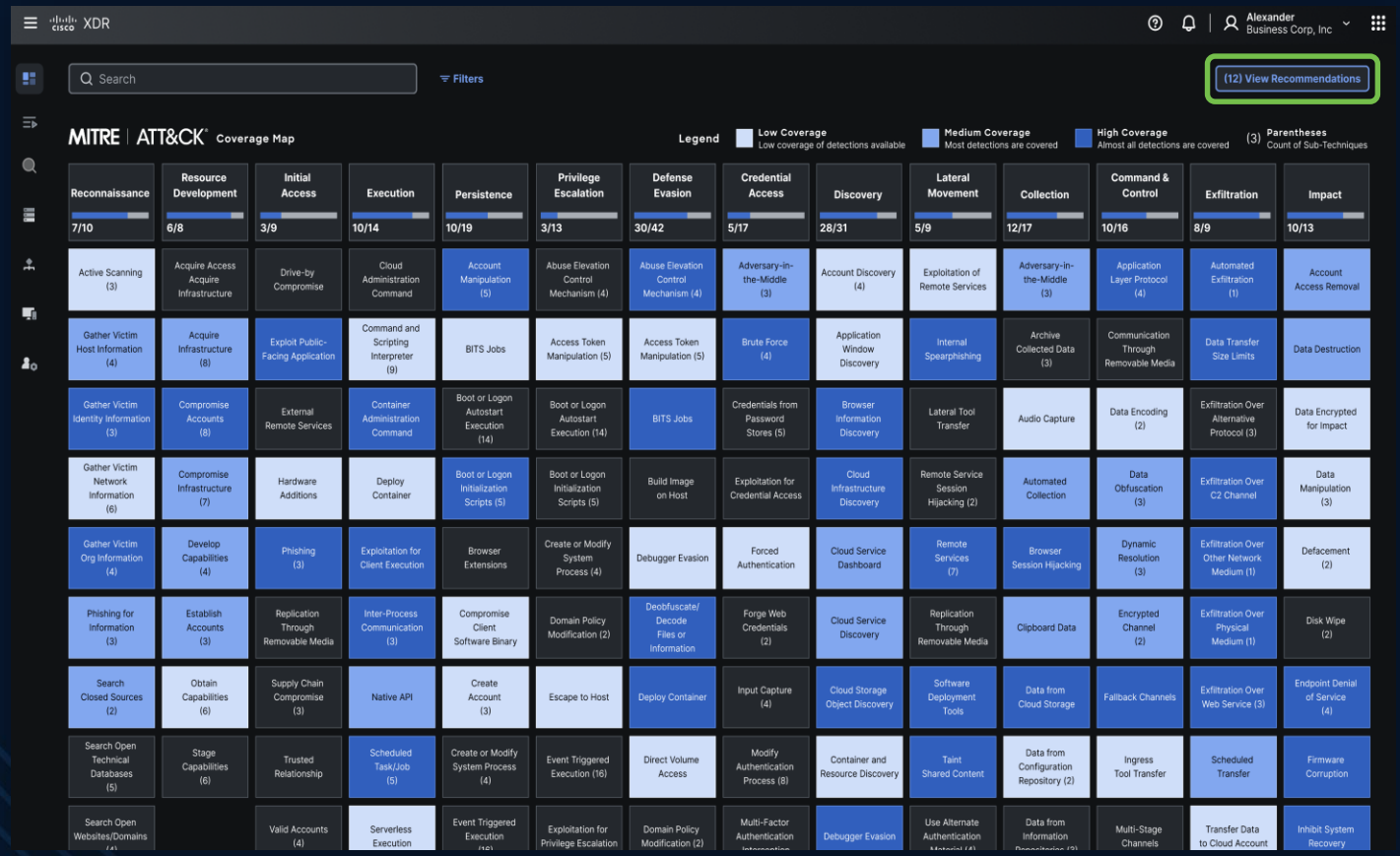
Clear prioritization with behavioral analytics and identity first platform

Power of AI

Automated playbooks and response guidance accelerated with Generative AI assistant

Was erreichen wir damit ?!

Schutz gegen Attacken, Taktiken und Techniken



"**Automatisierte Zuordnung** von MITRE ATT&CK-Gegnerverhalten zu Erkennungen"

"**Proaktive Empfehlungen** zu Tools und Telemetriearten zur Optimierung der Abdeckung"

"SOC-Analysten **identifizieren** schnell potenzielle **Anzeichen** einer Kompromittierung"

"**Volle Sichtbarkeit** auf die in einem Sicherheitsvorfall beteiligten TTPs"

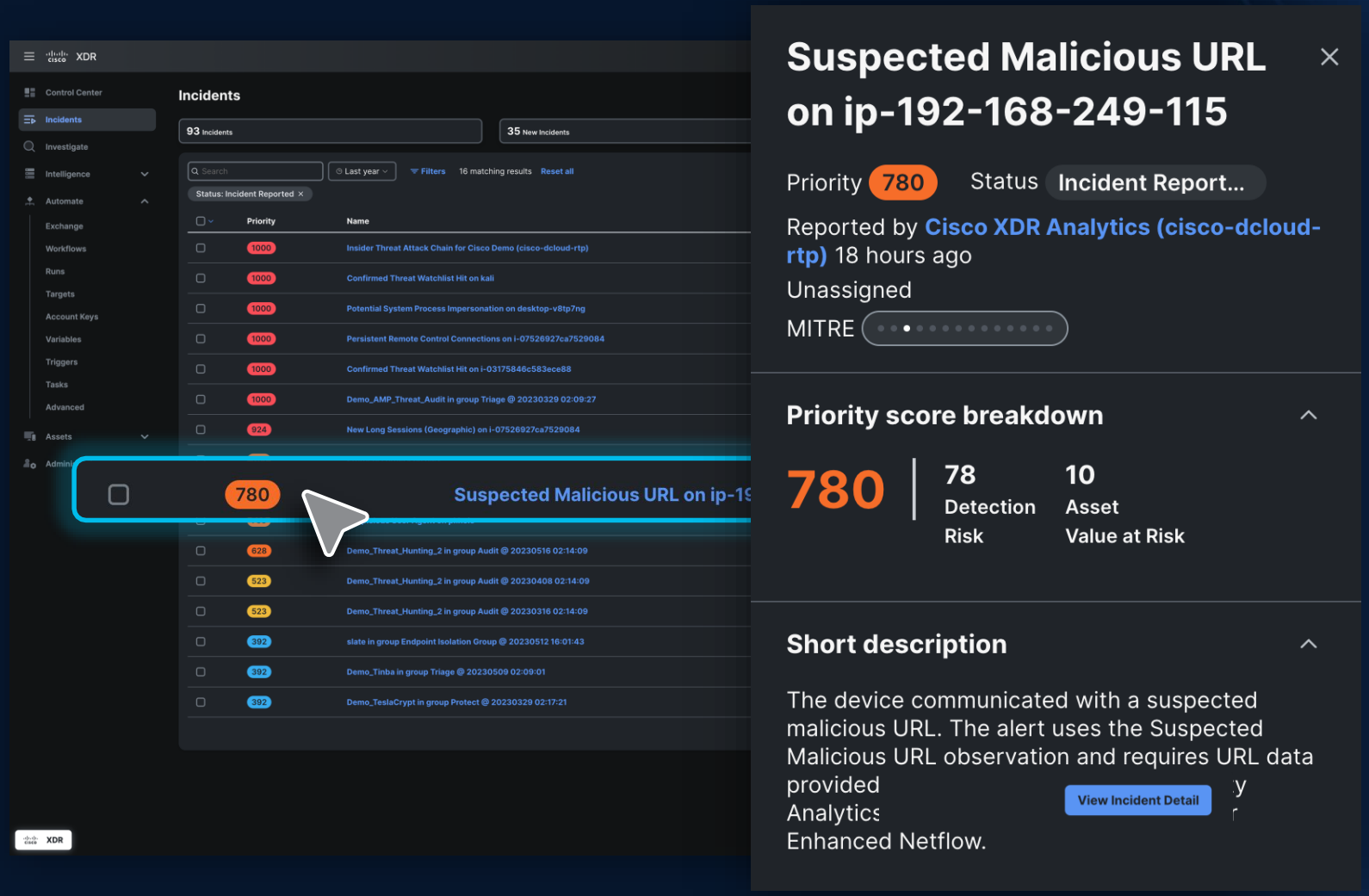
Genauigkeit und Zuverlässigkeit von Warnungen verbessern

"Risiko- und wirkungsbasierte **Priorisierungen** mit Bedrohungskorrelation liefern"

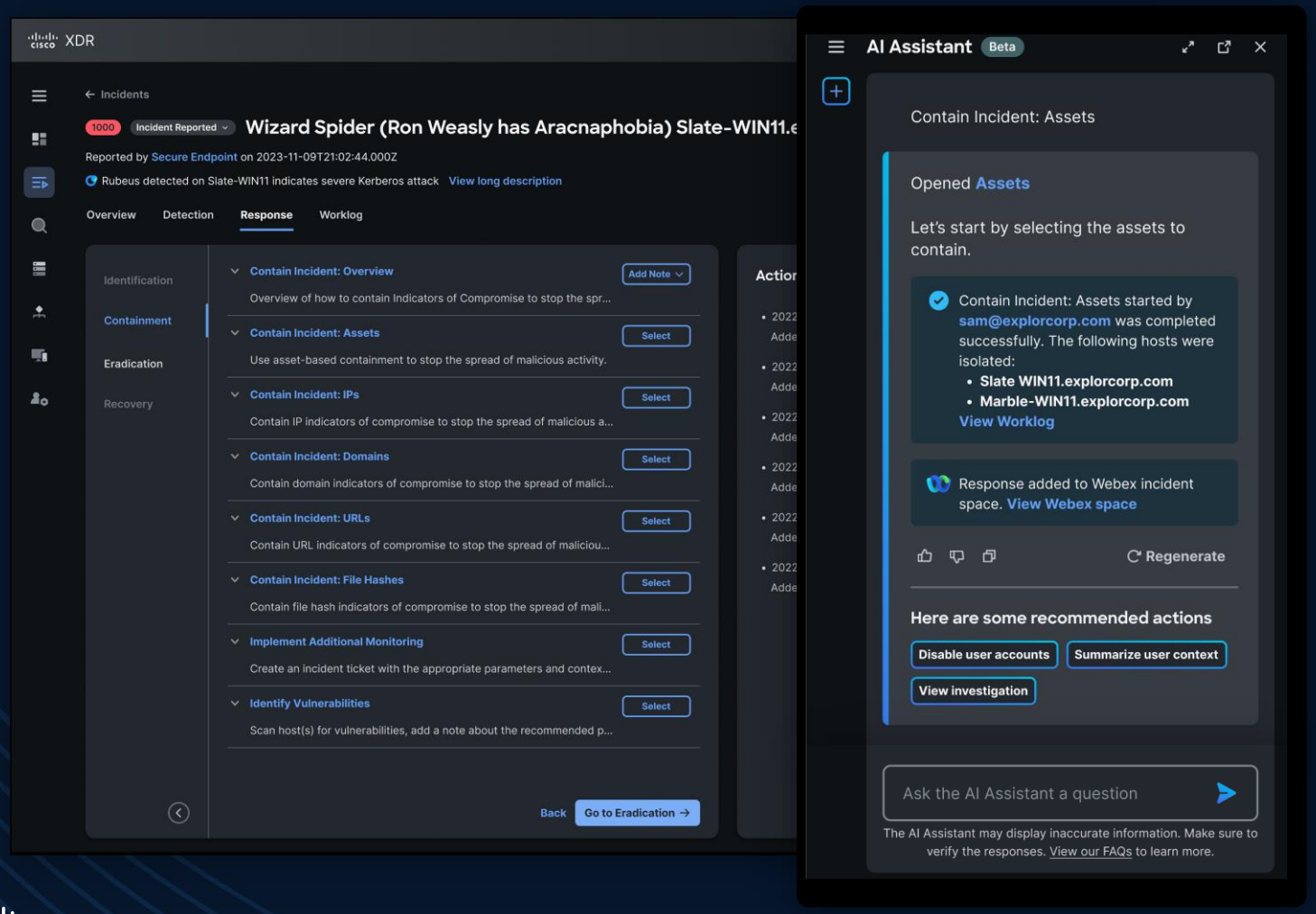
"Untersuchen, priorisieren, **reagieren** und von einer Konsole aus **wiederherstellen**"

"Jede Reaktion und Aktion mit **KI-gesteuerter Automatisierung** steuern"

Sicheres Urteil durch bereichsübergreifende Telemetrie **über Bedrohungsinformationen** erhalten



Sicherheitsteams unterstützen, menschliche Einsicht erweitern und komplexe Abläufe automatisieren



Optimierung der Wiederherstellung und Verteidigung

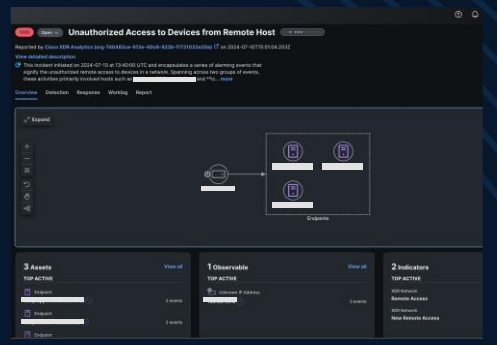
Erweiterung der **Sichtbarkeit** über alle Bereiche

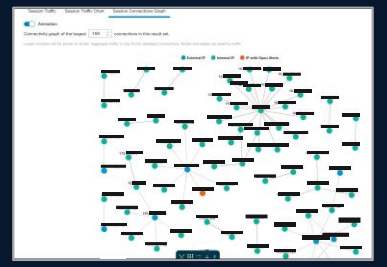
Unterstützung bei der Entscheidungsfindung verbessern

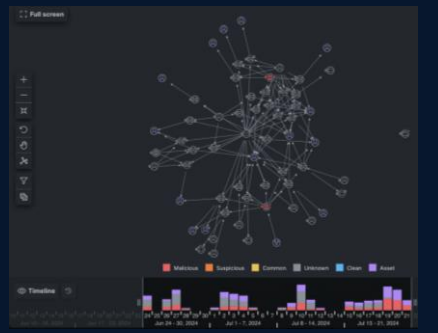
Was sagen unsere Kunden ?!

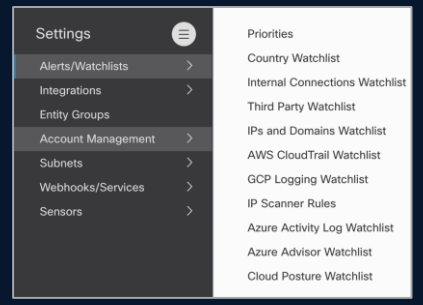
Erkenntnisse von Kunden und Teststellungen

1. **Erkennung** von „nicht authorisierten externen Zugriffen“



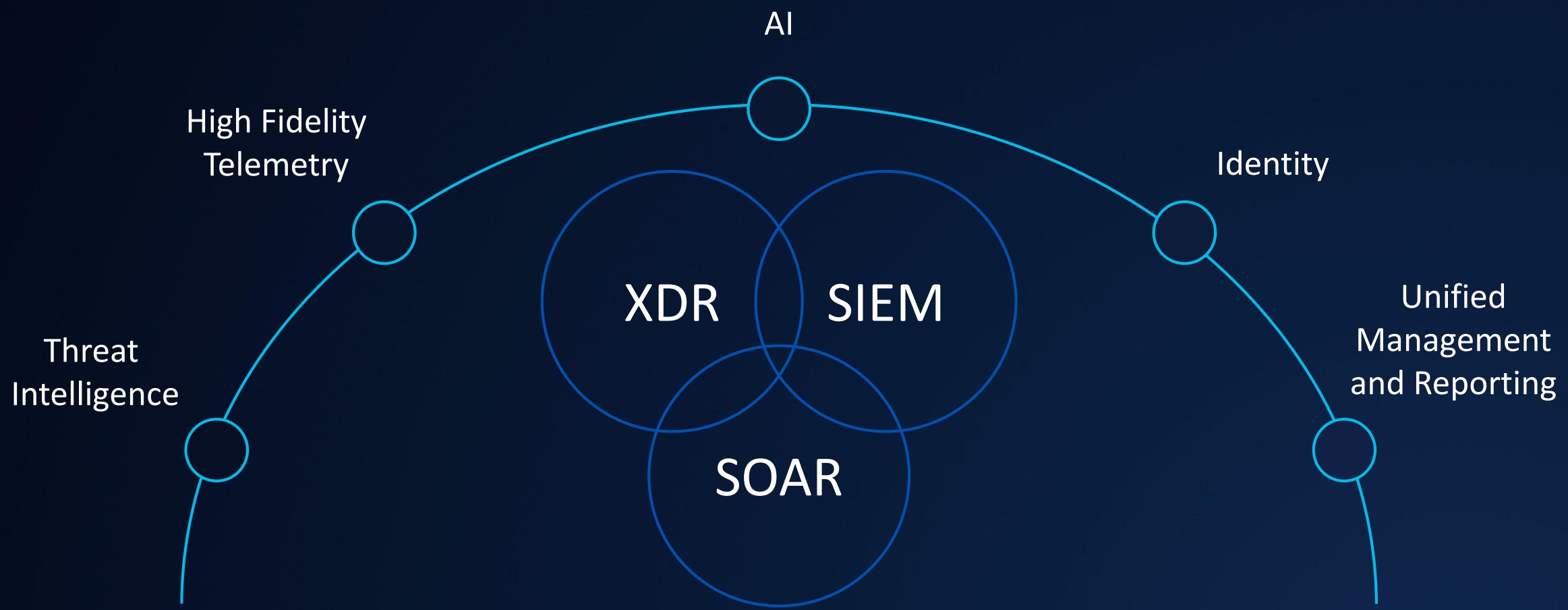






...und mit **Splunk** geht noch mehr !

Cisco + Splunk: Bereitstellung grundlegender TDIR-Elemente."



TDIR – Threat Detection, Investigation & Response

Warum nun Cisco & Telekom ?!

Unübertroffener Überblick über die gesamte Bedrohungslandschaft

Weltweit grösstes „Threat Reseach Team“ mit über 500 Personen

+800 Mrd. Sicherheitsereignisse pro Tag

~9 Mio. E-Mails blockiert pro Stunde

~2.000 neue Proben pro Minute

~2.000 blockierte Domains pro Sekunde

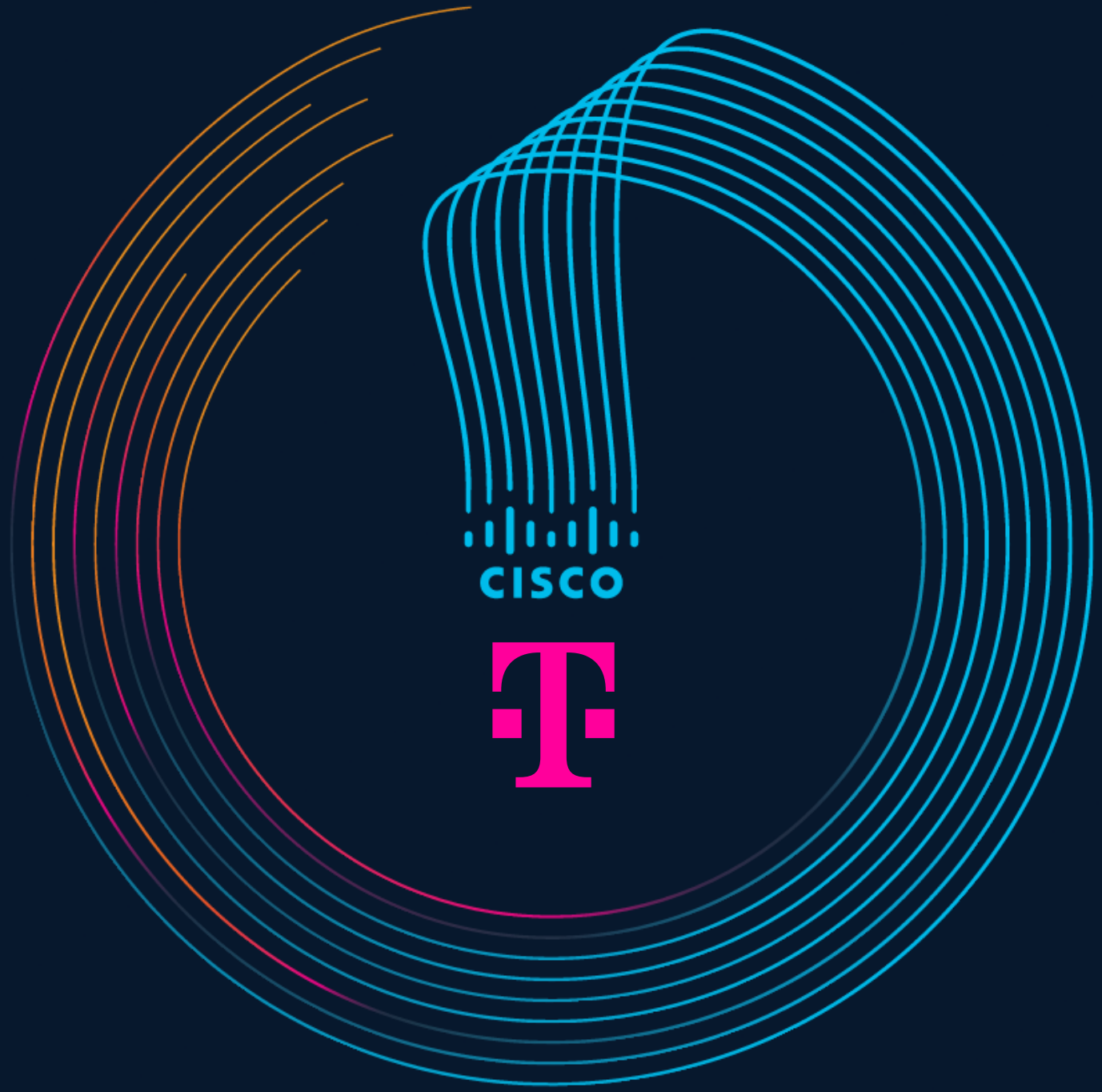
Cisco Security als Managed Service der Telekom

- ✓ Design, Regelset & Einrichtung
- ✓ Security Expertise & Unterstützung
- ✓ Reporting & Analyse
- ✓ Incidentmanagement mit Service Desk
- ✓ Changedurchführung mit fachlicher Beratung

Täglich prasseln viele Bedrohungen auf ihr Unternehmen ein.

Wir spannen einen Schirm auf, um Sie zu schützen!

Danke, Thank you, Merci, Gracias, Grazie, Obrigado, Dank je, Tack, Takk, Tak, Kiitos, Dziękuję, Děkuji, Köszönöm, Mulțumesc, Благодаря, Ευχαριστώ, Спасибо, Дякую, Teşekkür ederim, Terima kasih.


CISCO