SWS COMPUTERSYSTEME
Member of ACP Group

SWS Computersysteme AG

SWS COMPUTERSYSTEME
Member of ACP Group

XDR Extended Detection & Response

SWS COMPUTERSYSTEME
Member of ACP Group

Agenda

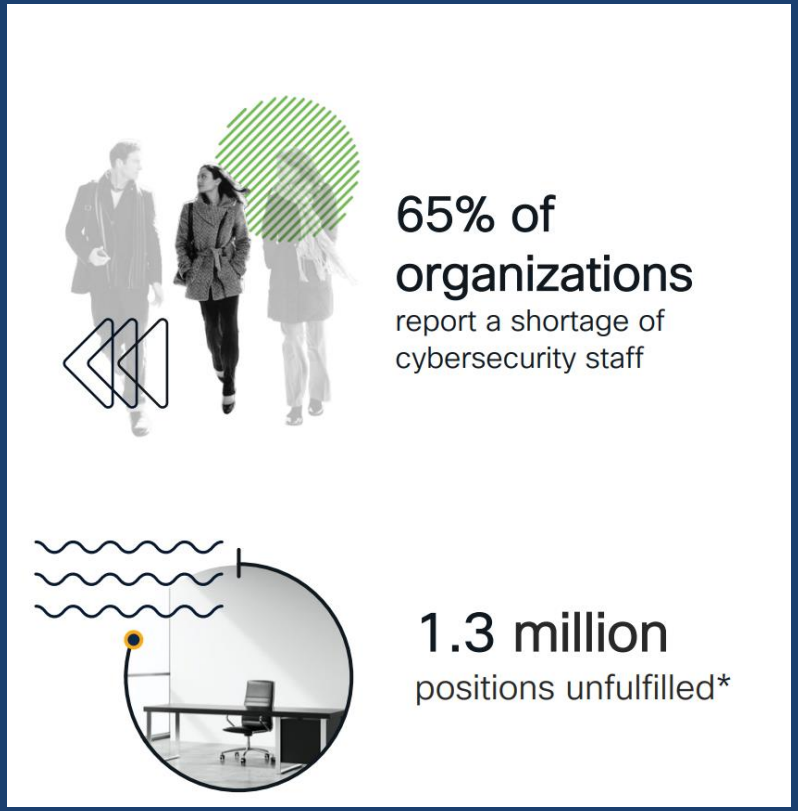
- Herausforderungen
- Was ist XDR?
- Cisco XDR – SecureX
- Visibility mit SecureX - Demo
- Threat Hunting mit SecureX - Demo
- Security Automatisierung mit SecureX - Demo
- 3rd Party Integrationen
- Q&A

Herausforderungen

- Security Informationen in Werkzeuge integrieren
- Standardisierte Prozesse einführen und zeitaufwändige Aufgaben reduzieren
- Teamübergreifende Kommunikation
- Erkennungszeit verkürzen
- Tätigkeiten automatisieren
- Proaktive Security Checks
- Durchgängige Compliance

Herausforderungen im SOC

- Zu viele Alarme & Meldungen aus nicht integrierten bzw. unterschiedlichen Produkten
- Zu wenige Kolleginnen & Kollegen
- Zu viele neue Bedrohungen

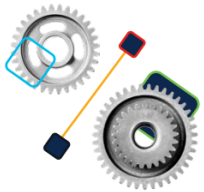


Herausforderungen durch die Hersteller

- Über 3000 Cybersecurity Hersteller / Anbieter
- Produktsilos -> Durchschnittlich 75 Produkte pro Unternehmen
- Alarme von verschiedenen Systemen zu bearbeiten ist sehr schwierig und zeitintensiv

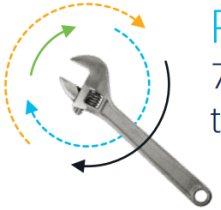
Vast security market

3000+ Cybersecurity vendors[1]



Siloed solution sets

75 security tools on average[2]

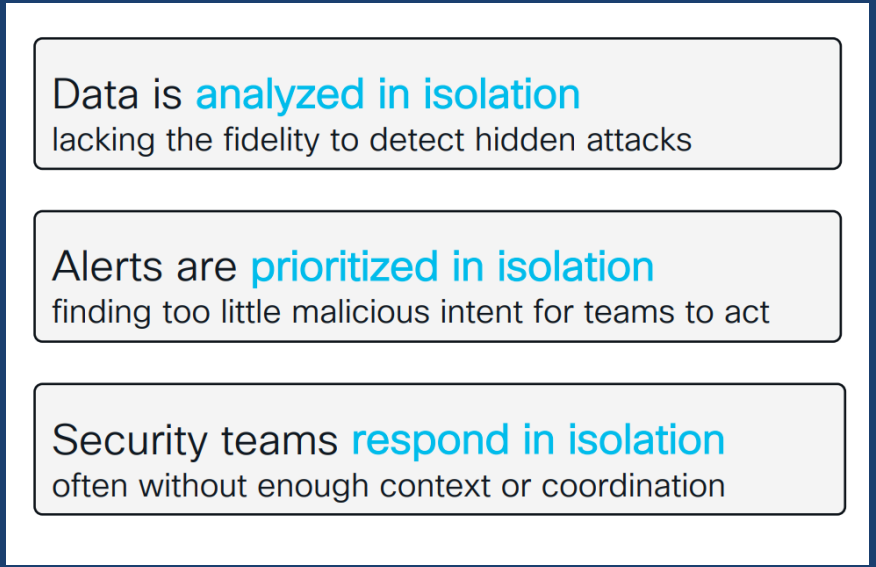


Reduced effectiveness

79% of CISOs say it's difficult to orchestrate alerts[3]

Herausforderungen durch isolierte Produkte

- Nicht Architektur-Übergreifende Lösungen betrachten Security Informationen nur begrenzt
- Versteckte Angriffsziele werden unzureichend aufgedeckt
- Eingeschränkte Reaktion auf Vorfälle im Gesamtkontext



Die Lösung -> XDR!

- Automatisierung reduziert die Last der IT
- Security Lösungen und Informationen zu Bedrohungen teilen sich eine Plattform
- Bedrohungsanalysen werden einfacher & schneller

Agenda

- Herausforderungen
- Was ist XDR?
- Cisco XDR – SecureX
- Visibility mit SecureX - Demo
- Threat Hunting mit SecureX - Demo
- Security Automatisierung mit SecureX - Demo
- 3rd Party Integrationen
- Q&A

Was ist XDR?

- Extended Detection & Response (XDR) ist eine Kombination aus:
  - Network Detection & Response

    - Firewalls, IPS-Systeme, Netflow Analyzers, ..

  - Endpoint Detection & Response

    - Next-Gen Malware Anti-Virus

Was ist XDR?

Die Definition von XDR unterscheidet sich teils unter den Anbietern, aber Grundlegend gilt:

- Integration von unterschiedlichen Security Komponenten und Datenquellen -> X(tended)
- Schnellere und intelligentere Erkennung von Bedrohungen -> D(etection)
- Bedrohungen und Fehlverhalten verfolgen, korrigieren und Maßnahmen automatisieren -> R(esponse)

Network Detection & Response

Bietet

- Erfasst Aktivitäten von on-prem & Cloud Strukturen
- Langzeit Datenanalyse
- Agent-Unabhängige Informationen

Herausforderungen

- Einsicht in Aktivitäten auf Endgeräten
- Verschlüsselte Datenübertragung
- Netzwerk Perimeter Verschiebung

Endpoint Detection & Response

Bietet

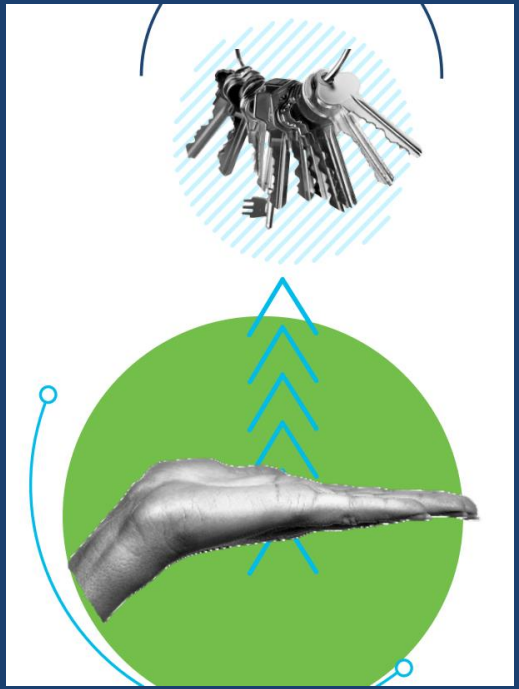
- Direkte Einsicht auf die Bedrohungen
- Mitigierungsmöglichkeit auf Unternehmensgeräten
- Forensische Überprüfung der Geräte möglich

Herausforderungen

- Agent Abhängigkeit
- Bewegung / Ausbreitung von Schadsoftware im Netz
- Benutzerverhalten

Herausforderungen von XDR

- Vollumfängliches XDR ist ein Prozess
- Security Lösungen fehlen zum Teil APIs, kompatible Datenbankstrukturen oder Datennormalisierung
- Schwache Partnerschaften unter den Herstellern können den Ansprüchen oft nicht Herr werden
- Unterschiedliche Definitionen von XDR
- Einige XDR Lösungen erfordern teure Data Lakes



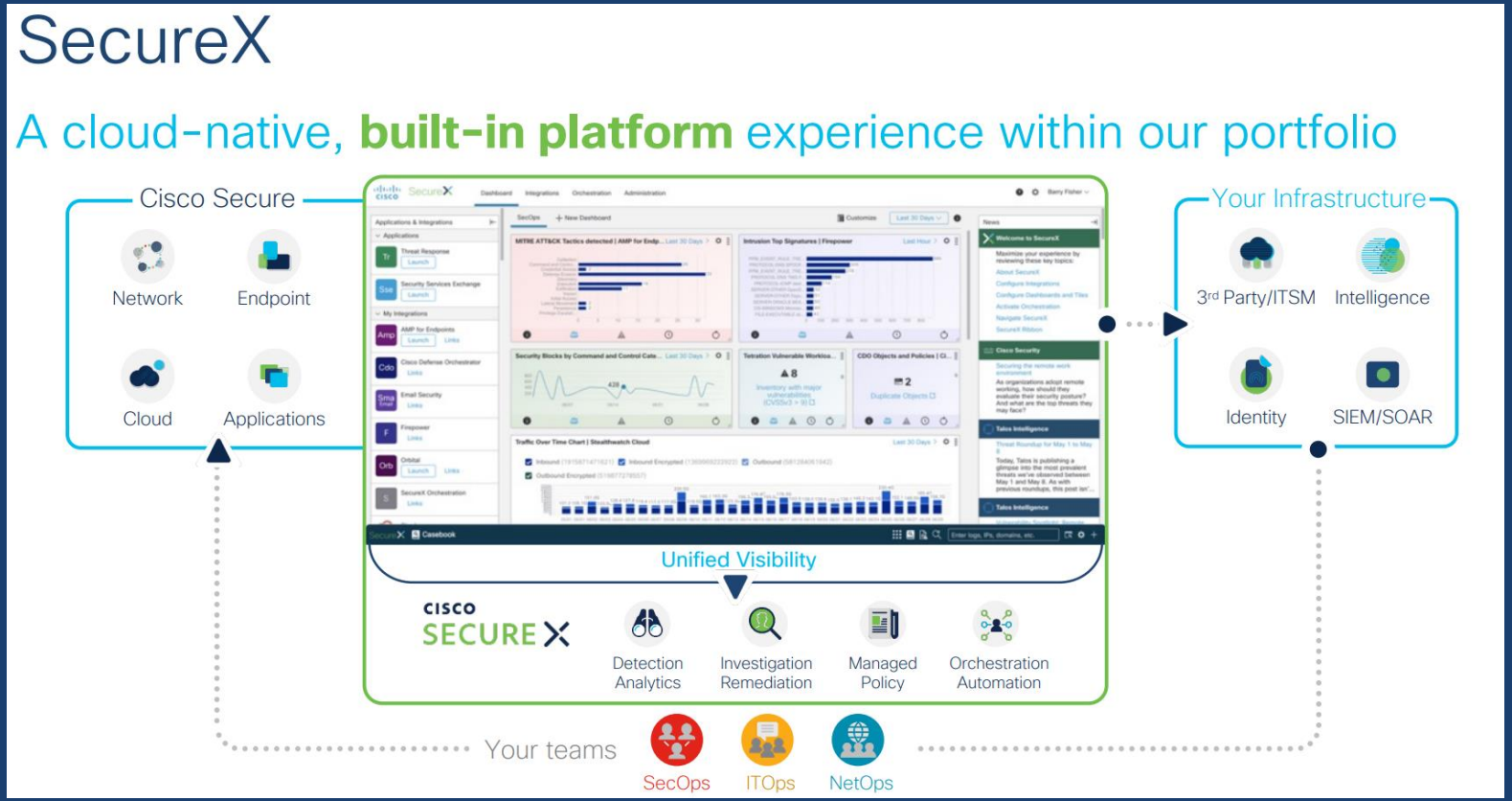
Agenda

- Herausforderungen
- Was ist XDR?
- Cisco XDR – SecureX
- Visibility mit SecureX - Demo
- Threat Hunting mit SecureX - Demo
- Security Automatisierung mit SecureX - Demo
- 3rd Party Integrationen
- Q&A

SWS COMPUTERSYSTEME
Member of ACP Group

Cisco XDR – SecureX

Cisco XDR - SecureX



SecureX Fähigkeiten

SecureX delivering powerful capabilities

Integrated and open for **simplicity**

Unified in one location for **visibility**

Maximized operational **efficiency**

SECURE X

integrations
built-in, pre-built or custom

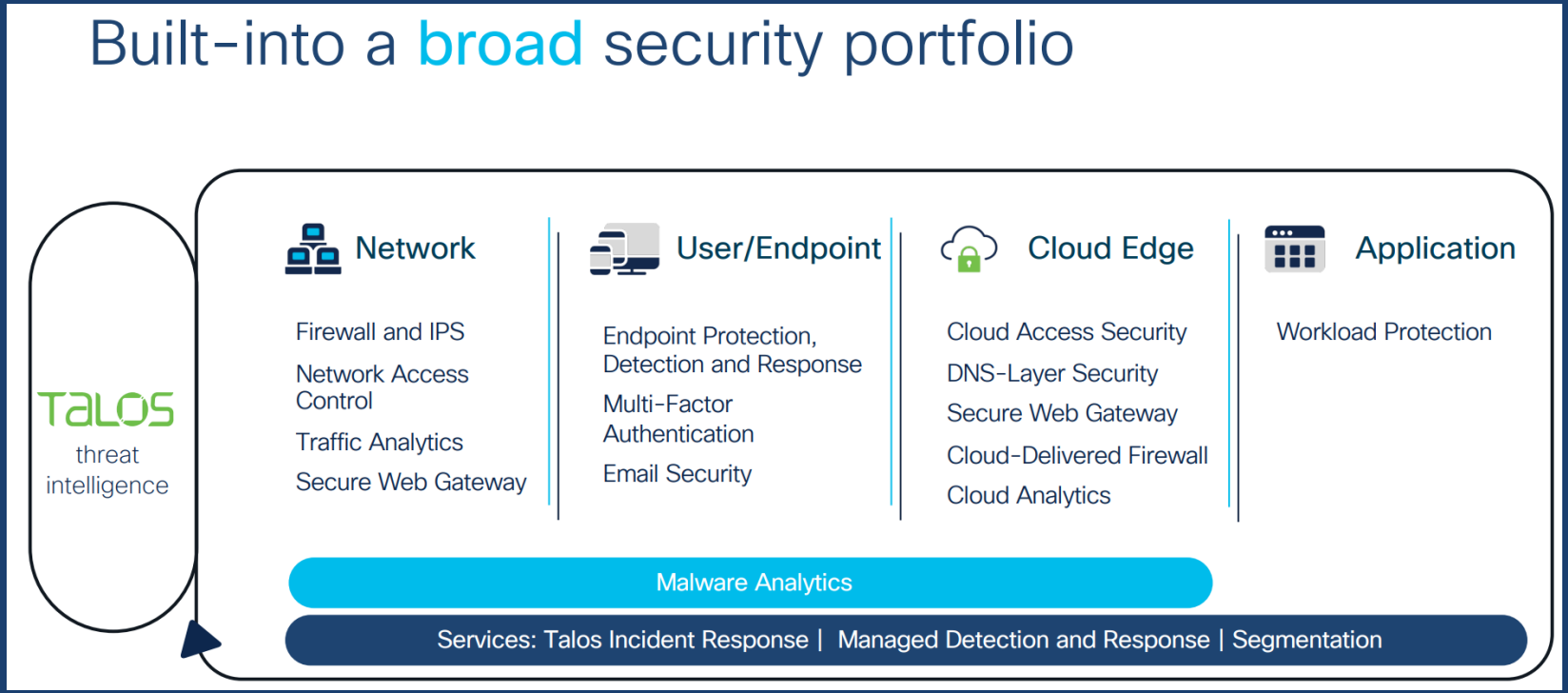
ribbon & sign-on
never leaves you maintains context

dashboard
customizable for what matters to you

threat response
is at the core of the platform

orchestration
drag-drop GUI for no/low code

SecureX Portfolio



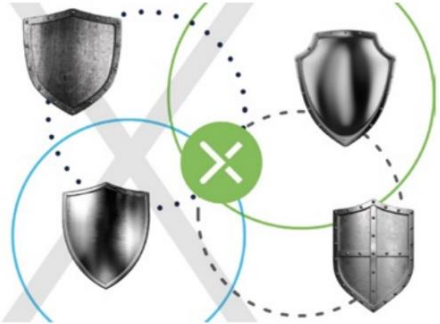
SecureX Threat Intelligence

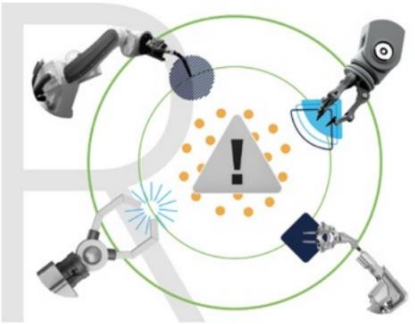
Cisco Talos

- Die größte nicht-behördliche Threat Intelligence Organisation
- Analysiert täglich mehr als 2,2 Billionen Artifakte
- Allein letztes Jahr wurden Kunden vor mehr als 350 Schwachstellen geschützt
- Verarbeitet weltweit die meisten Bedrohungsdaten

SecureX

Cisco delivers the broadest XDR capabilities with...





Built-in eXtensions

Natively connect detection and response capabilities

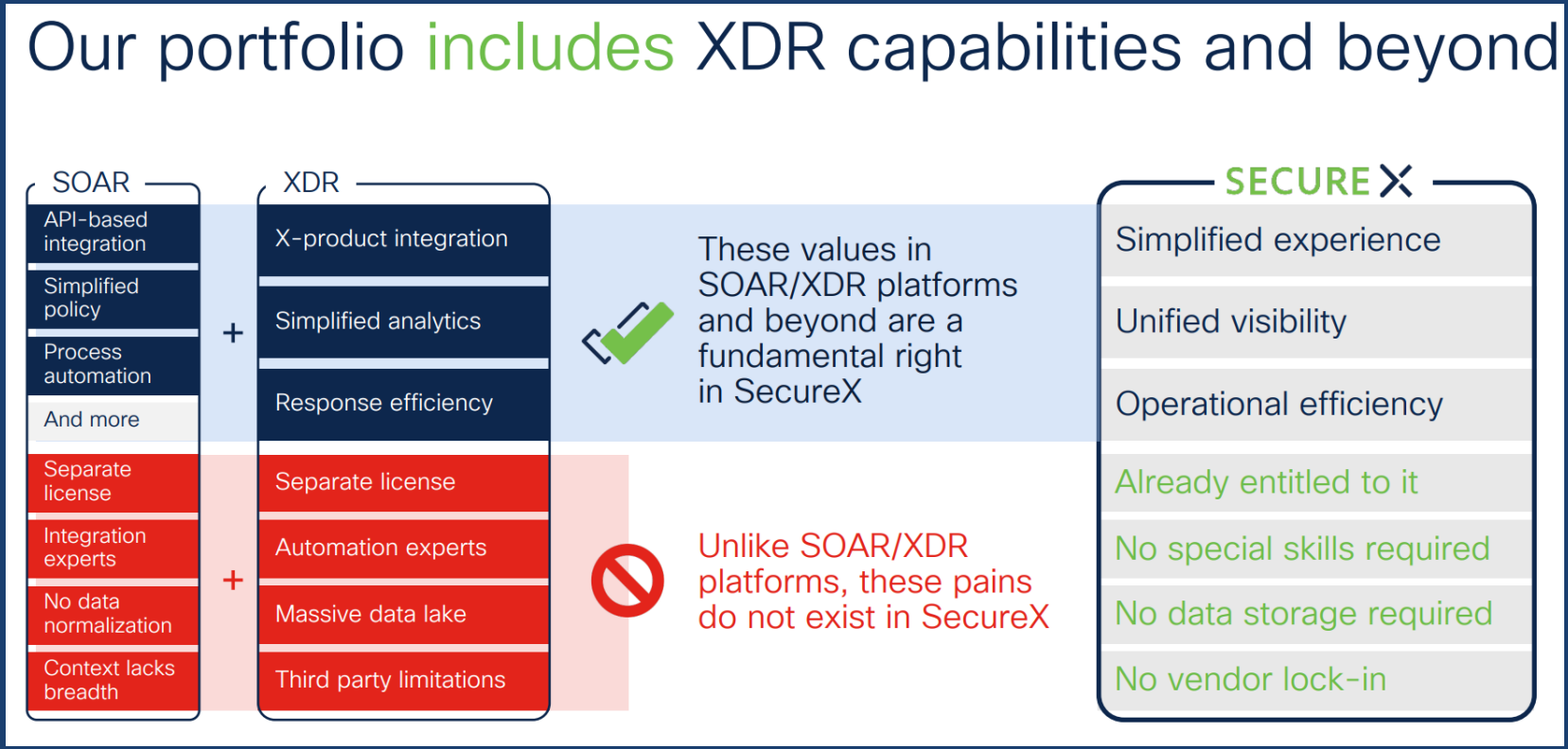
Intelligent Detections

Accurately detect more malicious intent more accurately

Confident Responses

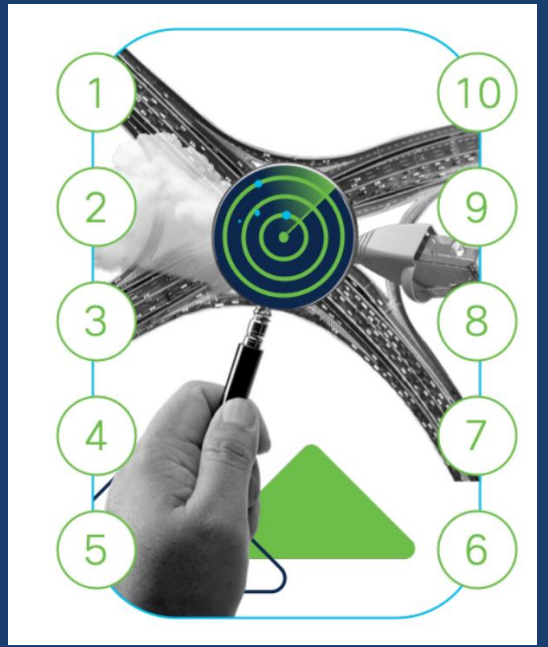
Reduce threat dwell times with playbook-driven automation

Cisco XDR - SecureX



SecureX Einsatzbereiche

- Überwachung von Benutzer & Geräte Aktivitäten, managed oder unmanaged
- Geringere Erkennungszeit von Bedrohungen
- Anreicherung von Threat Intelligence
- Ursachenfindung ab Ausführung bis Zugriff, Lateral Movement bis Exfiltration und mehr
- Bessere Entscheidungsfindung durch Einbindung des MITRE ATT&CK Frameworks
- Plattformübergreifende Anwendung von Policies



Agenda

- Herausforderungen
- Was ist XDR?
- Cisco XDR – SecureX
- SecureX - Demo
- 3rd Party Integrationen
- Q&A

SWS COMPUTERSYSTEME
Member of ACP Group

SecureX - Demo

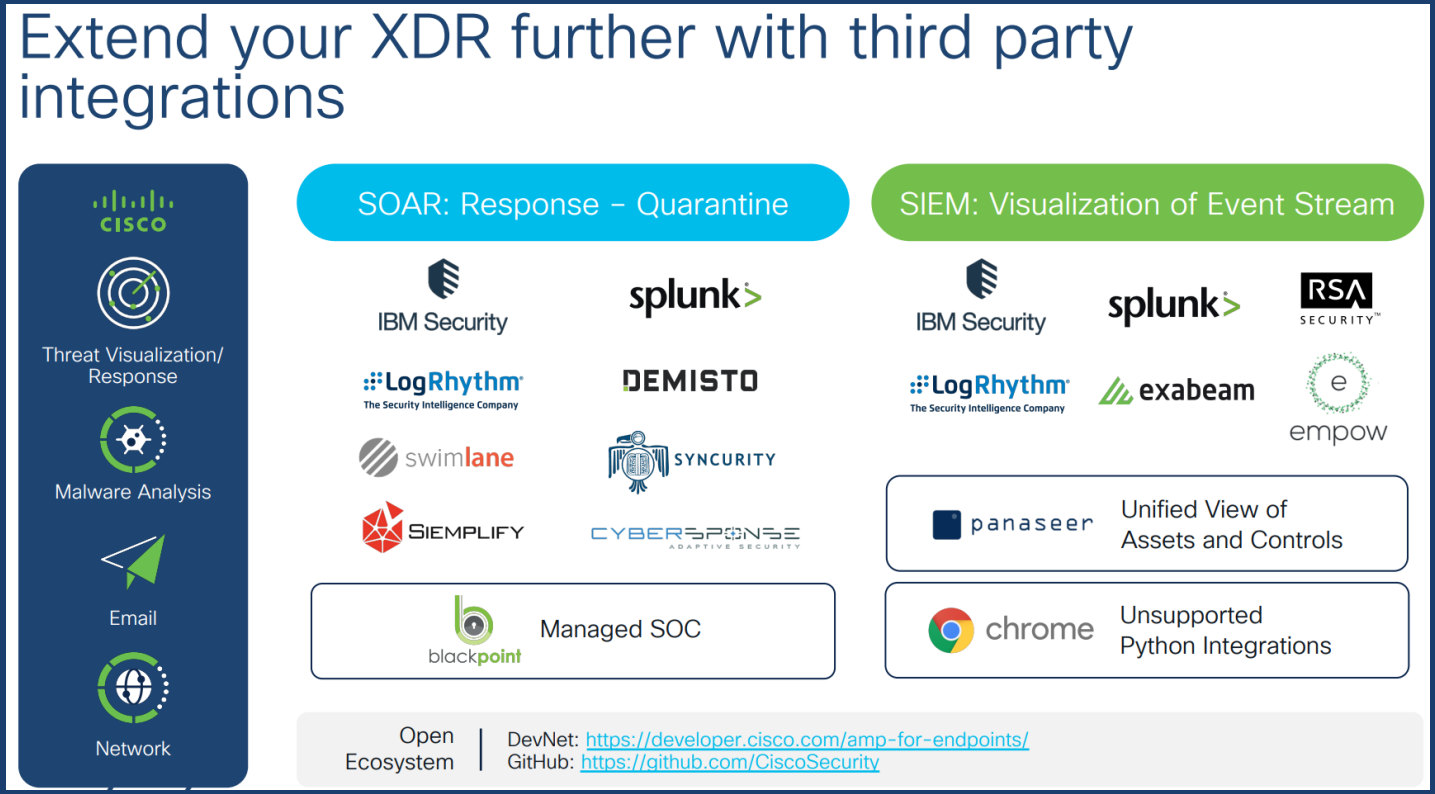
Agenda

- Herausforderungen
- Was ist XDR?
- Cisco XDR – SecureX
- Visibility mit SecureX - Demo
- Threat Hunting mit SecureX - Demo
- Security Automatisierung mit SecureX - Demo
- 3rd Party Integrationen
- Q&A

SWS COMPUTERSYSTEME
Member of ACP Group

3rd Party Integrationen

3rd Party Integrationen



Vielen Dank für Ihre Aufmerksamkeit.

Fragen?

Wir freuen uns auf Ihre weitere Anmeldung für unsere Webinar Serie:

- Sicherer Endpunkt in Kombination mit Visibilität
- Netzwerkanalyse (Firewall, Stealthwatch)
- NAC und MFA