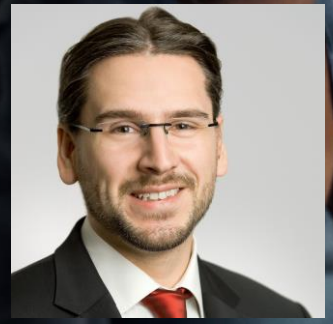
Besser reagieren auf Bedrohungen mit einem risikobasierten XDR-Ansatz

Cisco XDR

Wolfgang Rölz
Cybersecurity Sales Specialist XDR



Stefan Rehberg
Technical Solutions Architect Cybersecurity

11. Juli 2023

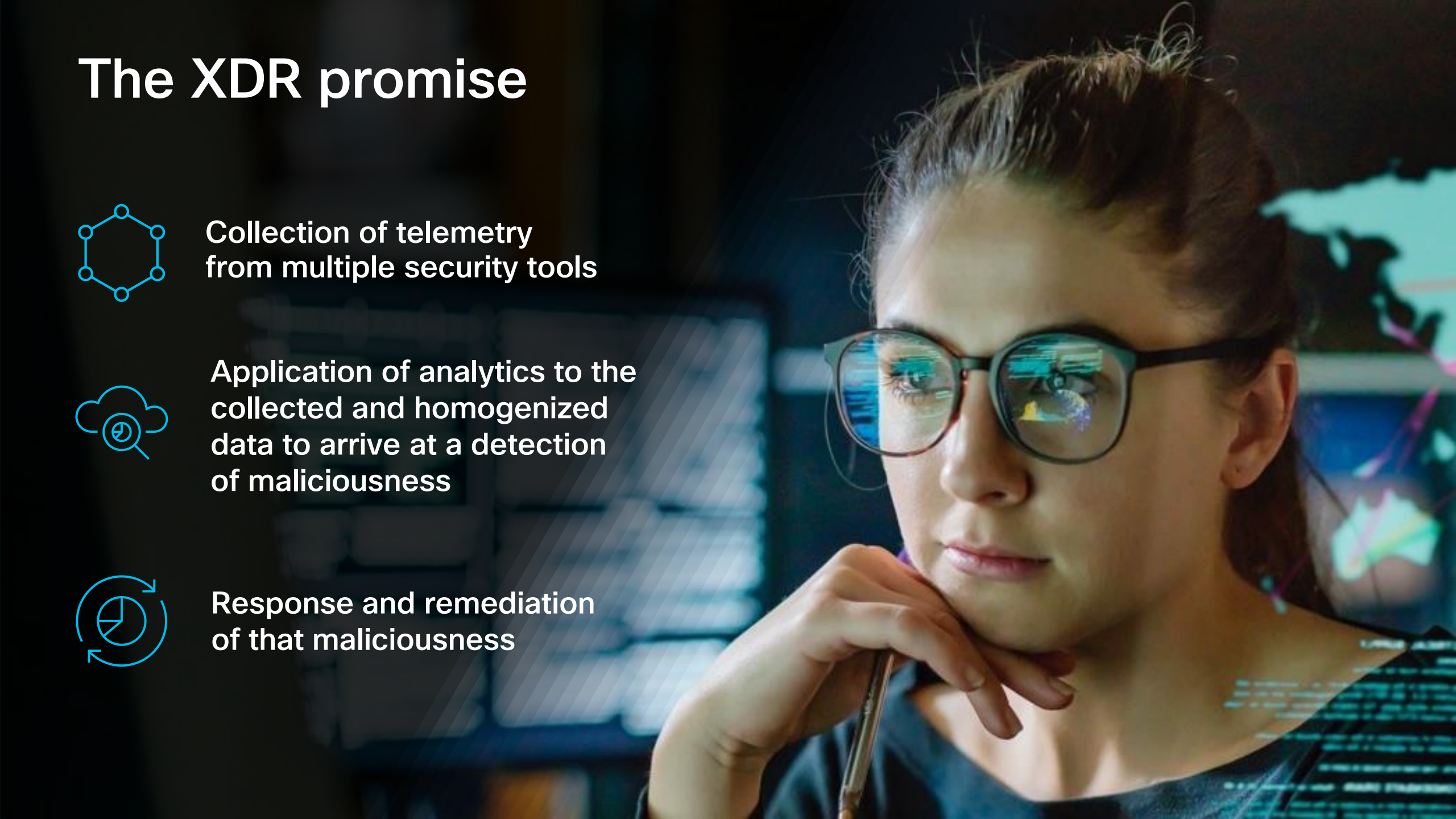
Tactics, Techniques and Procedures (TTPs) that once only impacted nation-states are now being used by every-day attackers

The XDR promise

Collection of telemetry from multiple security tools

Application of analytics to the collected and homogenized data to arrive at a detection of maliciousness

Response and remediation of that maliciousness



Adversary: Turla

// Nicknames

Snake
Venomous Bear
Uroburos
Group 88
Waterbug

Stop advanced threats like ransomware

Most attacks use a sequence like this...

A well-tailored and personalized email causes a user to click...

Which goes to a questionable web site...

Which leads to a strange process being created locally on the user's device...

That process will connect to another machine or directly to their data

T1566: Spear phishing

T1055: Process Injection

T1189: Drive-by Compromise

T1087: Account Discovery: Domain Account

T1570: Lateral Tool Transfer

T1048: System Network Connections Discovery

Vendor A	Vendor C	Vendor E	Vendor G	Vendor D

Anatomy of a real attack (Turla)

Most attacks use a sequence like this...

You need a solution that sees deeply across the entire attack chain

Cisco XDR

Built on the Cisco Security Cloud platform

Lesson from Turla

Only an effective XDR solution can adapt to the changing nature of the threat

Security tools need to focus on the attacker

Turn potential false positives into validated incidents

Focus on initial compromise, lateral movement, privilege escalation and data exfiltration

Simplify with Cisco XDR

Cisco

- Network
- Endpoint
- Email
- Cloud
- Applications
- Identity

Built on the Cisco security platform

Open and extensible | Clear prioritization | Automation and response guidance | Streamlined investigations

Your Infrastructure

- 3rd party tools
- Intelligence
- Others
- SIEM/SOAR

Your SOC

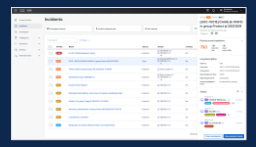
SecOps Analyst | CISO | Incident responder

What does an effective XDR look like?

Telemetry from native and third-party control points

- Endpoint
- Network
- Email
- Cloud
- Identity
- Firewall...

Cisco XDR
Open and risk-based


Analytics & correlation

Streamlined investigation

Automation & response

Threat intel

Asset & user context

MITRE

- Streamlined investigations, shortening time from detection to response
- Prioritized alerts, focusing SOC efforts on threats that pose the most harm
- Automated response actions, meaning threats are mitigated rapidly, and proactive measures taken

Simplify security operations to elevate productivity and stay resilient against the most sophisticated threats

The Cisco approach to XDR

Detect more, act faster, elevate productivity, build resilience

Detect the most sophisticated threats

- Multi-vector detection: network, cloud, endpoint, email, and more
- Enriched incidents with asset insights, threat intel
- Optimized for multi-vendor environments

Act on what truly matters, faster

- Prioritize threats by greatest material risk
- Unified context to streamline investigations
- Evidence-backed recommendations

Elevate productivity

- Focus on what matters and filter out the noise
- Boost limited resources for maximum value
- Automate tasks and focus on, strategic tasks

Build resilience

- Close security gaps
- Anticipate what's next through actionable intel
- Get stronger, everyday with continuous, quantifiable improvement

Delivering XDR to meet your where you are

Cisco XDR

Network

Secure Network Analytics

Cisco networking

Third-party networking

User/ endpoint

Secure Endpoint

Secure Client

Email threat defense

Vulnerability management

Third-party endpoint

Cloud

Secure Cloud Analytics

Umbrella

Public cloud logs

Application & identity

Duo multi-factor authentication

Third-party identity

Services: Talos Incident Response | Managed detection & response

Leveraging the Cisco security cloud

Combining core capabilities including a frictionless experience, open and extensible ecosystem, and AI-driven automation

Third – Party Integrations available for Cisco XDR

EDR:
- CrowdStrike Falcon® Insight
- SentinelOne Endpoint Security
- Microsoft Defender
- Trend Micro Vision One
- Cybereason Endpoint Security
- Palo Alto Networks Cortex XDR

Email Threat Defense:
- Proofpoint Email Protection
- Microsoft O365

Cloud Logs:
- AWS
- Microsoft Azure
- Google Cloud Platform

NGFW:
- Check Point Security Gateway & Management
- Fortinet FortiGate
- Palo Alto Networks Next-Generation Firewall

NDR:
- Darktrace Respond
- ExtraHop Reveal

SIEM:
- Microsoft Sentinel

Application and Identity:
- Microsoft Azure AD

Included in Cisco XDR Advantage

Easy to buy tiers for Cisco XDR

Cisco XDR Essentials

Native integration of the full Cisco security portfolio so analysts can detect and respond to the most sophisticated threats

Cisco XDR Advantage

All features in Essentials
+
Commercially supported and curated integrations with select third-party tools

Cisco XDR Premier

All features in Advantage as a managed service from Cisco. Includes security validation through penetration testing and select Cisco Talos Incident Response services

DEMO TIME

Simplify security operations

Open and flexible approach, optimized for multi-vendor, multi-vector experience

Simplify the user experience and gain visibility and identify threats across network, cloud, endpoint, email, and applications for effective security regardless of vendor or vector.

Threat correlation and clear prioritization to help users see what's most important

Correlate and prioritize alerts across multiple telemetry sources using AI and ML to improve incident response.

Rapid and guided responses to quickly remediate threats and improve analyst efficiency

Rapidly remediate threats and take appropriate action quickly with automation capabilities, orchestration workflows, and guided remediation, freeing up time and resources to focus on strategic tasks.

Essential network insights, providing better understanding of your environment

Leverage network insights to protect against complex threats and bring clarity to security operations. By making the network foundational and going beyond EDR, organizations can identify and prevent advanced threats from evading detection and improve XDR outcomes.


cisco SECURE