Security Operations Simplified

Cisco XDR

Jon Felder
XDR AE Evangelist, – TX, OK, AR, LA, AL, MS

Combating Analyst Burnout & Tool Sprawl in 2025: How Cisco XDR Empowers Cybersecurity Teams to do More

The cybersecurity landscape in 2025 presents unprecedented challenges with increasing threats and operational complexity. Analysts are overwhelmed, risking burnout as they navigate an expanding arsenal of tools. "But burnout isn't only an HR problem anymore. It's also an advanced persistent threat to cybersecurity." We are ratifying our unified approach to threat detection and response, empowering security teams to work smarter, faster, and more effectively. Join us as we unpack solutions that transform cybersecurity operations and help teams reclaim control over their workload and security posture.

JF

The Hidden Threat, Analyst Burnout: The Silent Killer of Cybersecurity

1

Cybersecurity workforce shortage

With 3.5 million job vacancies, the global cybersecurity workforce shortage is arguably the greatest vulnerability businesses face today.

2

50%+ of SOC analysts consider leaving the field

Burnout from Alert Fatigue, Tool Sprawl and Lack of Integration, Manual and Repetitive Tasks, and Lack of Standardized Processes

3

Loss of institutional knowledge = advantage for adversaries

Lifecycle Services Conversation Guide, maintaining institutional knowledge is a challenge due to high turnover rates and decentralized IT structures. This lack of continuity in expertise and processes can lead to vulnerabilities that adversaries exploit.

4

"Cyber incidents occur every 39 seconds on average."

Roughly 739 incidents will occur before today's workday concludes...

Cisco XDR on Cisco.com

The Escalating Crisis of Analyst Burnout

Burnout Epidemic

76% of security professionals report burnout, a critical issue undermining team effectiveness and retention.

Short Tenure

Security analysts typically last only 2.1 years, leading to talent shortages and continuous onboarding costs.

Consequences

Burnout drives human errors responsible for 68% of breaches, directly influencing organizational risk and costs.

Hidden Costs

Beyond turnover and healthcare, burnout damages morale and long-term productivity.

Cisco XDR on Cisco.com

"Fatigue leads to vulnerability and malicious actors know it."

The Volume of Numbers Are Overwhelming

- Average of 2,244 attacks per day per organization in 2025
- 71% of SOC staff rate their workload as a 6-9 out of 10 in difficulty
- Investigating 1 day's worth of alerts would take 61+ days
- Ransomware attack occurs every 19 seconds...
- "Fatigue leads to vulnerability - and malicious actors know it."

In a hybrid, multi-vendor, multi-vector universe:

Everyone is an insider

+30%

of all incidents involved stolen credentials or malicious insiders

Attacks start from anywhere

45%

of breaches occurred in the cloud, and 19% due to a compromise at a business partner

Alert fatigue is worse

37%

of IT and SecOps pros say swelling alert volume, complexity increases job difficulty

Expanding attack surface

22%

increase in the average cost of a data breach where hybrid work was a factor

The Unmanageable Tool Sprawl

Too Many Tools

Organizations deploy an average of 75 security tools, creating complexity and fragmentation.

- 35% of analysts' time spent switching tools
- Only 29% of alerts actually get investigated
- Siloed data causes missed threats
- Aging "best-in-class" tools don't always work together
- Analysts overwhelmed by multiple dashboards and false positives

Impact on Security

This environment leads to delayed response, increased false positives, and compromised threat detection.

Streamlined integration is essential to overcome this sprawling chaos.

Cisco XDR on Cisco.com

Secret Sauce: Telemetry data source importance

The top six data sources that customers believe are essential for an XDR are Endpoint, Network, Firewall, Identity, Email and DNS

	Essential	
	Count	Share
Endpoint	255	85.0%
Network	226	75.3%
Firewall	207	69.0%
Identity	191	63.7%
Email	179	59.7%
DNS	140	46.7%
Public Cloud	137	45.7%
Non-Security Sources	36	12.0%

Cisco Secure Endpoint

Cisco/ Meraki (Networking)

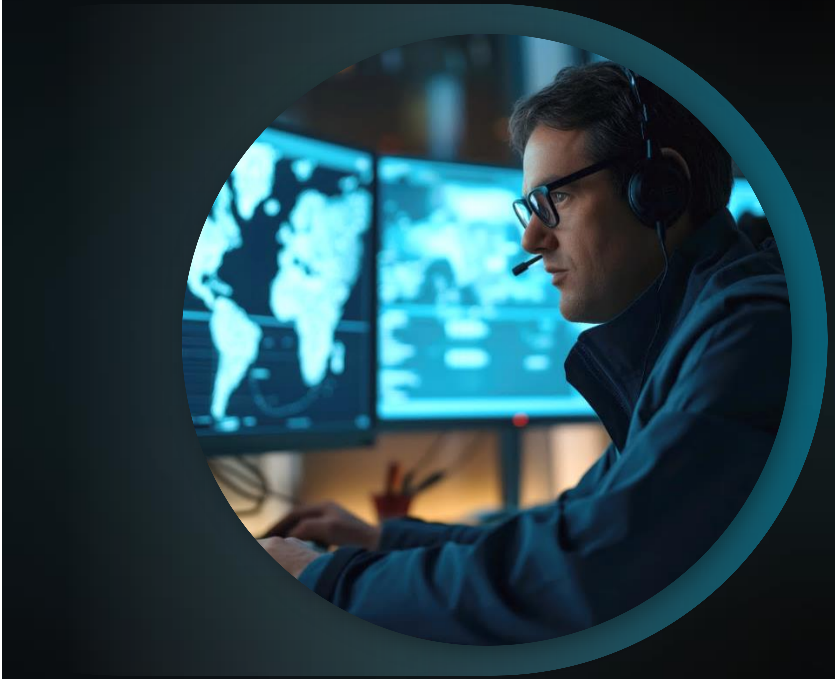
Firewall Threat Defense (FTD)

Duo

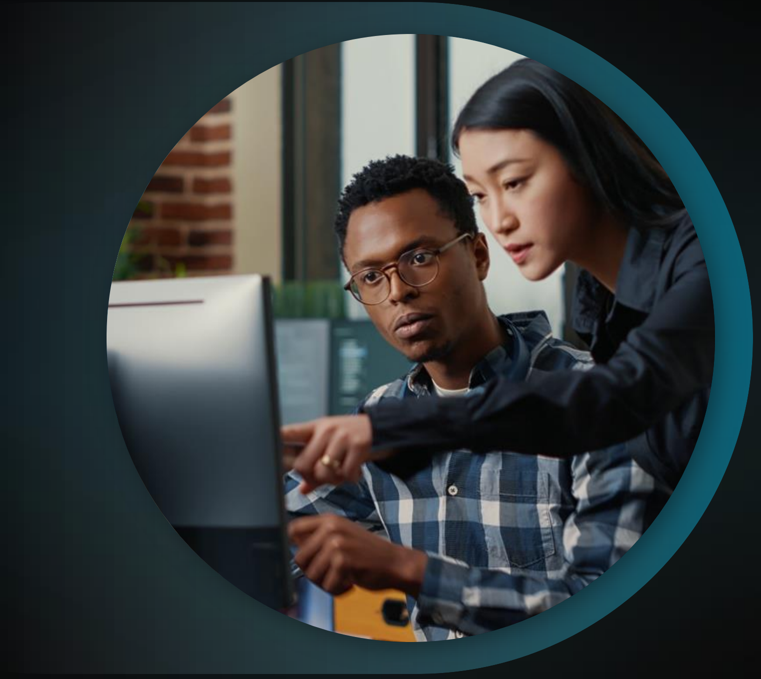
Email Threat Defense (ETD)

Umbrella

What SecOps wants



“I want to have a correlated view of alerts across my environment.”



"I need my security tools to help me work with speed, accuracy, and confidence."

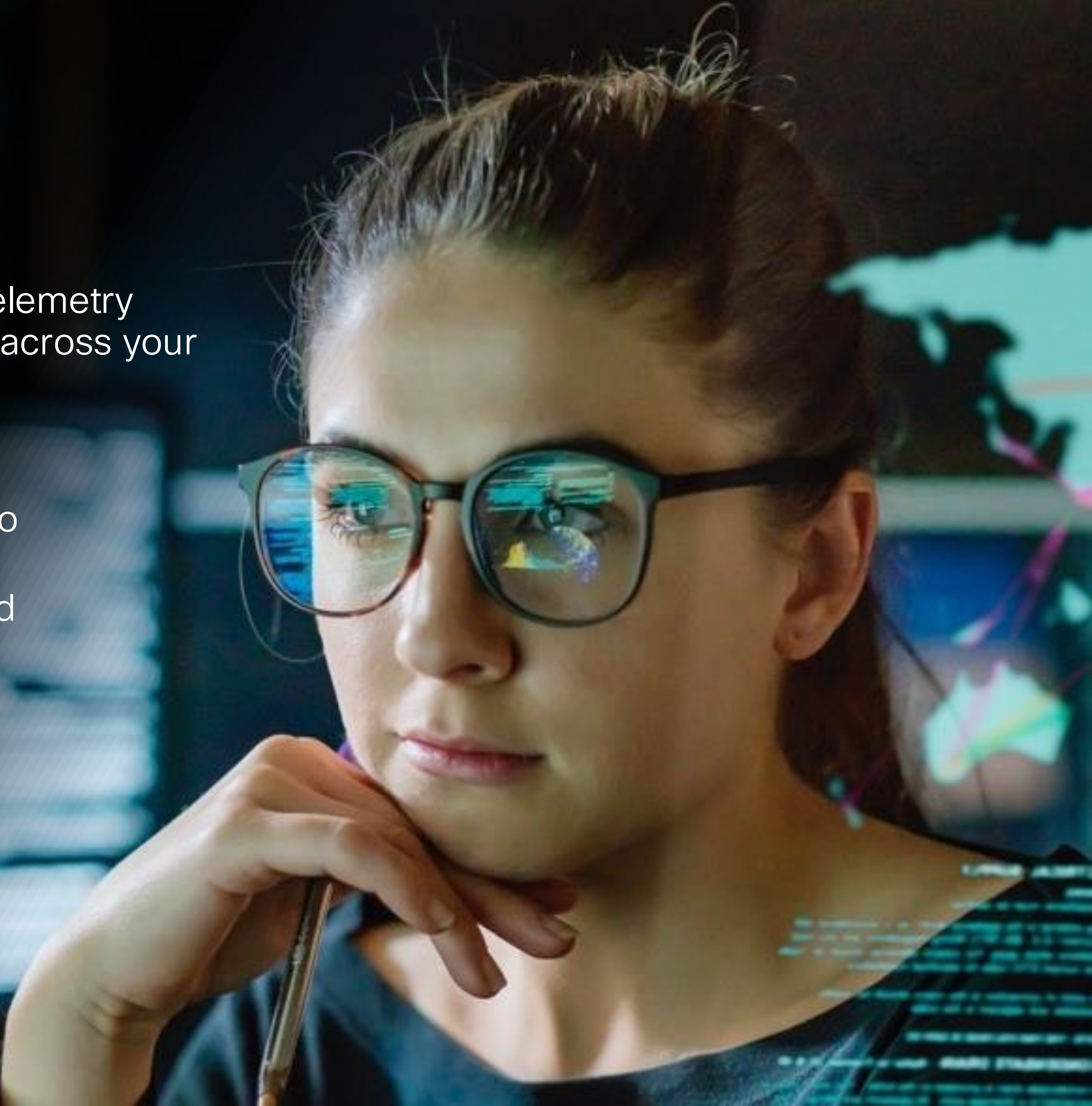
"I want my team to remediate threats with guidance and automated playbooks.”

The XDR promise

Collection of detections and raw telemetry from multiple sensor technologies across your environment

Application of advanced analytics to the collected and normalized evidence to produce correlated and prioritized detections of malicious activity

Guided responses across multiple control planes to quickly and effectively contain, mitigate, and eradicate the threat



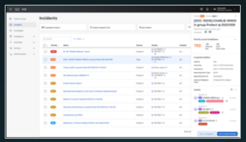
What does an effective XDR look like?

Telemetry from native and third-party control points

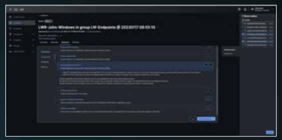
- Endpoint
- Network
- Email
- Cloud
- Identity
- Firewall...

Cisco XDR
Open and risk-based

Analytics & correlation



Streamlined investigation



Automation & response

Threat intel

Asset & user context

MITRE

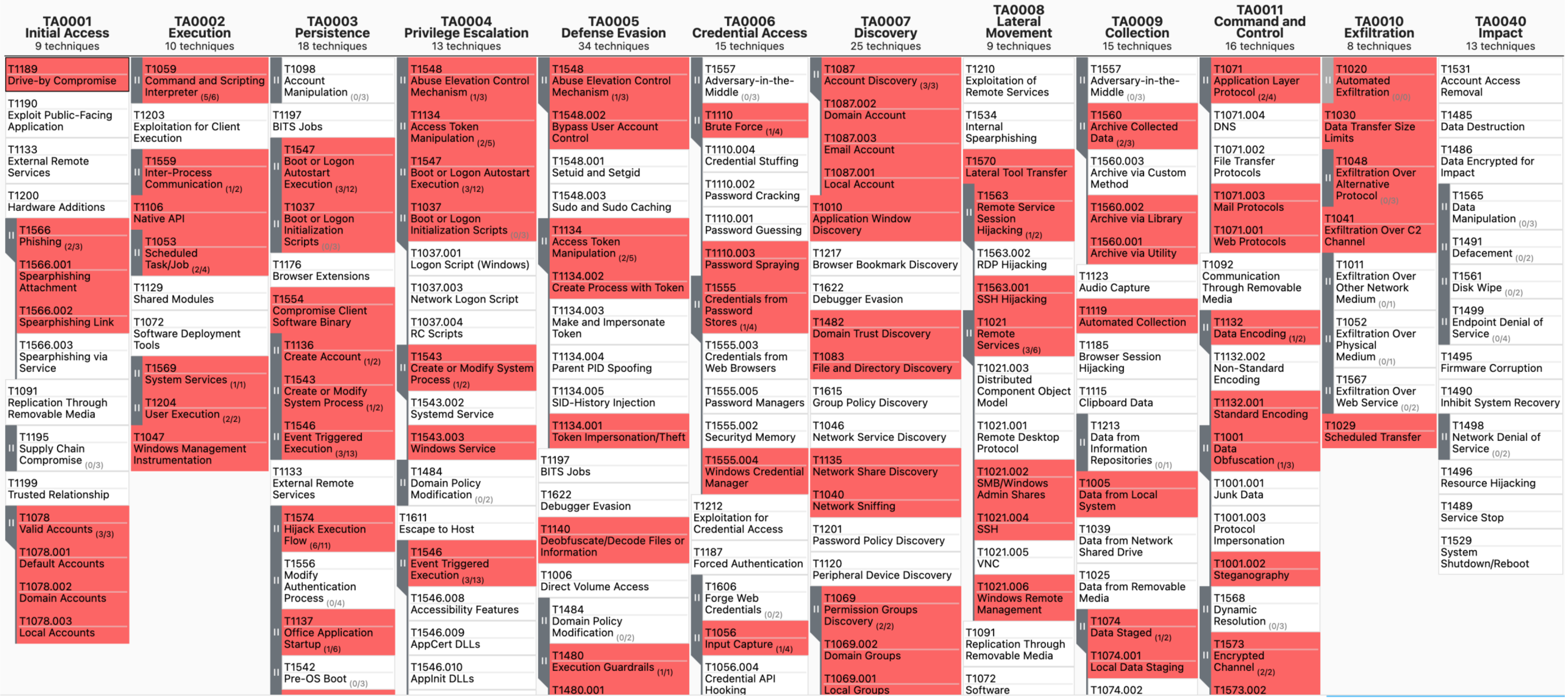
Streamlined investigations, shortening time from detection to response

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

How Can we Detect and Respond to all of these?



TA0001 Initial Access
9 techniques

- T1189 Drive-by Compromise
- T1190 Exploit Public-Facing Application
- T1133 External Remote Services
- T1200 Hardware Additions
- T1566 Phishing (2/3)
  - T1566.001 Spearphishing Attachment
  - T1566.002 Spearphishing Link
  - T1566.003 Spearphishing via Service
- T1091 Replication Through Removable Media
- T1195 Supply Chain Compromise (0/3)
- T1199 Trusted Relationship
- T1078 Valid Accounts (3/3)
  - T1078.001 Default Accounts
  - T1078.002 Domain Accounts
  - T1078.003 Local Accounts

TA0002 Execution
10 techniques

- T1059 Command and Scripting Interpreter (5/6)
- T1203 Exploitation for Client Execution
- T1559 Inter-Process Communication (1/2)
- T1106 Native API
- T1053 Scheduled Task/Job (2/4)
- T1129 Shared Modules
- T1072 Software Deployment Tools
- T1569 System Services (1/1)
- T1204 User Execution (2/2)
- T1047 Windows Management Instrumentation

TA0003 Persistence
18 techniques

- T1098 Account Manipulation (0/3)
- T1197 BITS Jobs
- T1547 Boot or Logon Autostart Execution (3/12)
- T1037 Boot or Logon Initialization Scripts (0/3)
- T1176 Browser Extensions
- T1554 Compromise Client Software Binary
- T1136 Create Account (1/2)
- T1543 Create or Modify System Process (1/2)
- T1546 Event Triggered Execution (3/13)
- T1133 External Remote Services
- T1574 Hijack Execution Flow (6/11)
- T1556 Modify Authentication Process (0/4)
- T1137 Office Application Startup (1/6)
- T1542 Pre-OS Boot (0/3)

TA0004 Privilege Escalation
13 techniques

- T1548 Abuse Elevation Control Mechanism (1/3)
- T1134 Access Token Manipulation (2/5)
- T1547 Boot or Logon Autostart Execution (3/12)
- T1037 Boot or Logon Initialization Scripts (0/3)
  - T1037.001 Logon Script (Windows)
  - T1037.003 Network Logon Script
  - T1037.004 RC Scripts
- T1543 Create or Modify System Process (1/2)
  - T1543.002 Systemd Service
  - T1543.003 Windows Service
- T1484 Domain Policy Modification (0/2)
- T1611 Escape to Host
- T1546 Event Triggered Execution (3/13)
  - T1546.008 Accessibility Features
  - T1546.009 AppCert DLLs
  - T1546.010 AppInit DLLs

TA0005 Defense Evasion
34 techniques

- T1548 Abuse Elevation Control Mechanism (1/3)
  - T1548.002 Bypass User Account Control
  - T1548.001 Setuid and Setgid
  - T1548.003 Sudo and Sudo Caching
- T1134 Access Token Manipulation (2/5)
  - T1134.002 Create Process with Token
  - T1134.003 Make and Impersonate Token
  - T1134.004 Parent PID Spoofing
  - T1134.005 SID-History Injection
  - T1134.001 Token Impersonation/Theft
- T1197 BITS Jobs
- T1622 Debugger Evasion
- T1140 Deobfuscate/Decode Files or Information
- T1006 Direct Volume Access
- T1484 Domain Policy Modification (0/2)
- T1480 Execution Guardrails (1/1)
  - T1480.001

TA0006 Credential Access
15 techniques

- T1557 Adversary-in-the-Middle (0/3)
- T1110 Brute Force (1/4)
  - T1110.004 Credential Stuffing
  - T1110.002 Password Cracking
  - T1110.001 Password Guessing
  - T1110.003 Password Spraying
- T1555 Credentials from Password Stores (1/4)
  - T1555.003 Credentials from Web Browsers
  - T1555.005 Password Managers
  - T1555.002 Securityd Memory
  - T1555.004 Windows Credential Manager
- T1212 Exploitation for Credential Access
- T1187 Forced Authentication
- T1606 Forge Web Credentials (0/2)
- T1056 Input Capture (1/4)
  - T1056.004 Credential API Hooking

TA0007 Discovery
25 techniques

- T1087 Account Discovery (3/3)
  - T1087.002 Domain Account
  - T1087.003 Email Account
  - T1087.001 Local Account
- T1010 Application Window Discovery
- T1217 Browser Bookmark Discovery
- T1622 Debugger Evasion
- T1482 Domain Trust Discovery
- T1083 File and Directory Discovery
- T1615 Group Policy Discovery
- T1046 Network Service Discovery
- T1135 Network Share Discovery
- T1040 Network Sniffing
- T1201 Password Policy Discovery
- T1120 Peripheral Device Discovery
- T1069 Permission Groups Discovery (2/2)
  - T1069.002 Domain Groups
  - T1069.001 Local Groups

TA0008 Lateral Movement
9 techniques

- T1210 Exploitation of Remote Services
- T1534 Internal Spearphishing
- T1570 Lateral Tool Transfer
- T1563 Remote Service Session Hijacking (1/2)
  - T1563.002 RDP Hijacking
  - T1563.001 SSH Hijacking
- T1021 Remote Services (3/6)
  - T1021.003 Distributed Component Object Model
  - T1021.001 Remote Desktop Protocol
  - T1021.002 SMB/Windows Admin Shares
  - T1021.004 SSH
  - T1021.005 VNC
  - T1021.006 Windows Remote Management
- T1091 Replication Through Removable Media
- T1072 Software

TA0009 Collection
15 techniques

- T1557 Adversary-in-the-Middle (0/3)
- T1560 Archive Collected Data (2/3)
  - T1560.003 Archive via Custom Method
  - T1560.002 Archive via Library
  - T1560.001 Archive via Utility
- T1123 Audio Capture
- T1119 Automated Collection
- T1185 Browser Session Hijacking
- T1115 Clipboard Data
- T1213 Data from Information Repositories (0/1)
- T1005 Data from Local System
- T1039 Data from Network Shared Drive
- T1025 Data from Removable Media
- T1074 Data Staged (1/2)
  - T1074.001 Local Data Staging
  - T1074.002

TA0011 Command and Control
16 techniques

- T1071 Application Layer Protocol (2/4)
  - T1071.004 DNS
  - T1071.002 File Transfer Protocols
  - T1071.003 Mail Protocols
  - T1071.001 Web Protocols
- T1092 Communication Through Removable Media
- T1132 Data Encoding (1/2)
  - T1132.002 Non-Standard Encoding
  - T1132.001 Standard Encoding
- T1001 Data Obfuscation (1/3)
  - T1001.001 Junk Data
  - T1001.003 Protocol Impersonation
  - T1001.002 Steganography
- T1568 Dynamic Resolution (0/3)
- T1573 Encrypted Channel (2/2)
  - T1573.002

TA0010 Exfiltration
8 techniques

- T1020 Automated Exfiltration (0/0)
- T1030 Data Transfer Size Limits
- T1048 Exfiltration Over Alternative Protocol (0/3)
- T1041 Exfiltration Over C2 Channel
- T1011 Exfiltration Over Other Network Medium (0/1)
- T1052 Exfiltration Over Physical Medium (0/1)
- T1567 Exfiltration Over Web Service (0/2)
- T1029 Scheduled Transfer

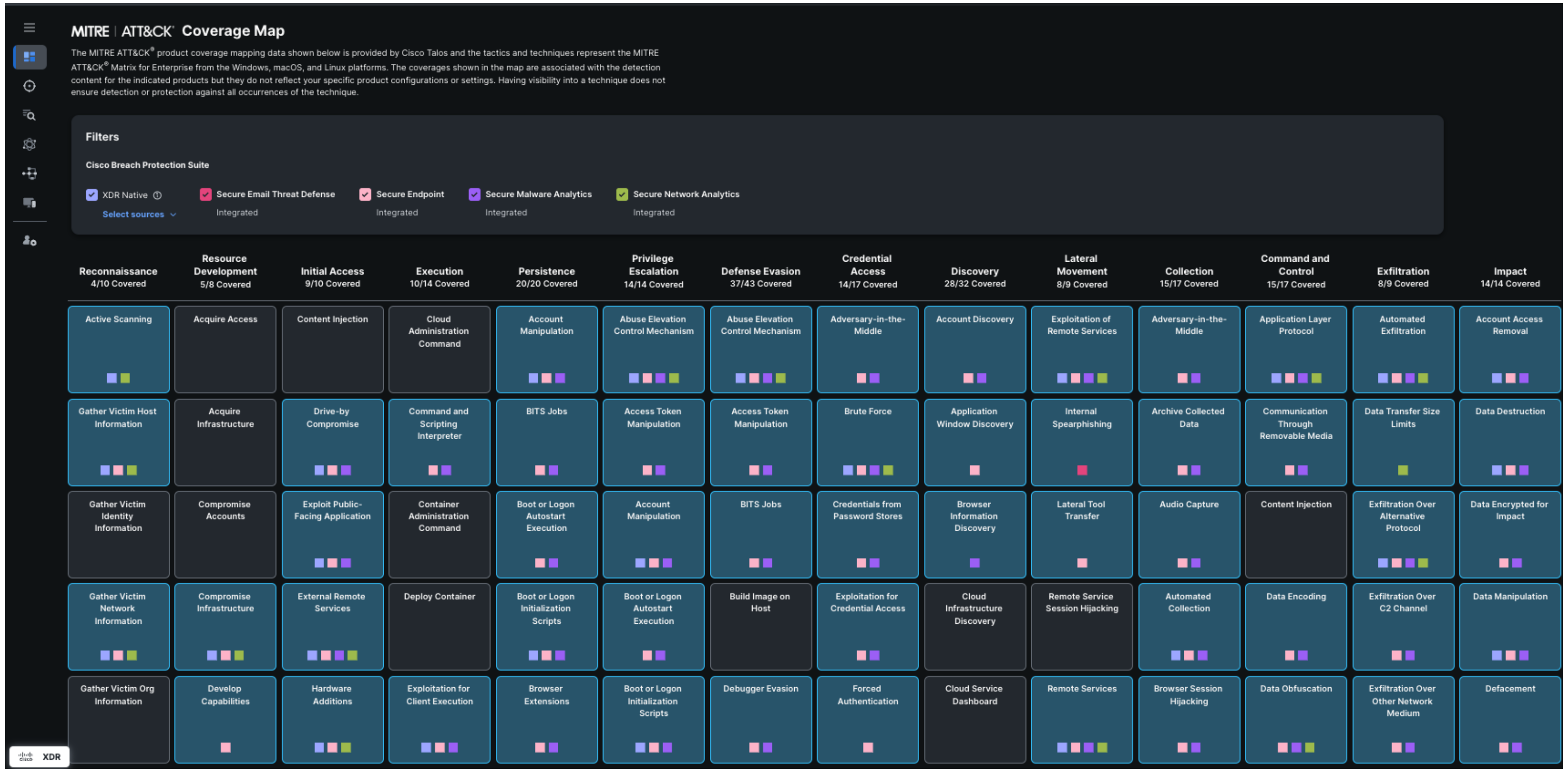
TA0040 Impact
13 techniques

- T1531 Account Access Removal
- T1485 Data Destruction
- T1486 Data Encrypted for Impact
- T1565 Data Manipulation (0/3)
- T1491 Defacement (0/2)
- T1561 Disk Wipe (0/2)
- T1499 Endpoint Denial of Service (0/4)
- T1495 Firmware Corruption
- T1490 Inhibit System Recovery
- T1498 Network Denial of Service (0/2)
- T1496 Resource Hijacking
- T1489 Service Stop
- T1529 System Shutdown/Reboot

MITRE ATT&CK coverage mapping in Cisco XDR

Protection against adversary tactics and techniques

NEW!



MITRE | ATT&CK® Coverage Map

The MITRE ATT&CK® product coverage mapping data shown below is provided by Cisco Talos and the tactics and techniques represent the MITRE ATT&CK® Matrix for Enterprise from the Windows, macOS, and Linux platforms. The coverages shown in the map are associated with the detection content for the indicated products but they do not reflect your specific product configurations or settings. Having visibility into a technique does not ensure detection or protection against all occurrences of the technique.

Filters

Cisco Breach Protection Suite

☑ 🟦 XDR Native ⓘ
Select sources ⌄

☑ 🟥 Secure Email Threat Defense – Integrated

☑ 🩷 Secure Endpoint – Integrated

☑ 🟪 Secure Malware Analytics – Integrated

☑ 🟩 Secure Network Analytics – Integrated

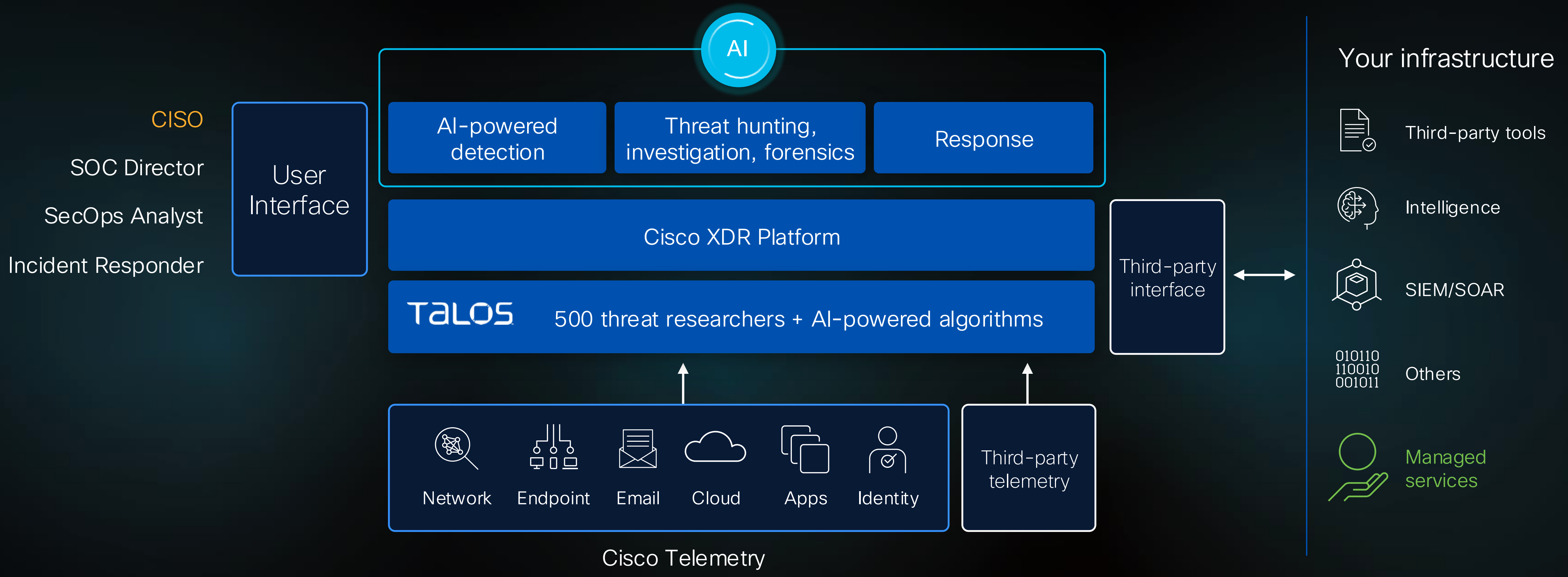
Reconnaissance 4/10 Covered	Resource Development 5/8 Covered	Initial Access 9/10 Covered	Execution 10/14 Covered	Persistence 20/20 Covered	Privilege Escalation 14/14 Covered	Defense Evasion 37/43 Covered	Credential Access 14/17 Covered	Discovery 28/32 Covered	Lateral Movement 8/9 Covered	Collection 15/17 Covered	Command and Control 15/17 Covered	Exfiltration 8/9 Covered	Impact 14/14 Covered
Active Scanning 🟦🟩	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation 🟦🩷🟪	Abuse Elevation Control Mechanism 🟦🩷🟪🟩	Abuse Elevation Control Mechanism 🟦🩷🟪🟩	Adversary-in-the-Middle 🩷🟪	Account Discovery 🩷🟪	Exploitation of Remote Services 🟦🩷🟪🟩	Adversary-in-the-Middle 🩷🟪	Application Layer Protocol 🟦🩷🟪🟩	Automated Exfiltration 🟦🩷🟪🟩	Account Access Removal 🟦🩷🟪
Gather Victim Host Information 🟦🩷🟩	Acquire Infrastructure	Drive-by Compromise 🟦🩷🟪	Command and Scripting Interpreter 🩷🟪	BITS Jobs 🩷🟪	Access Token Manipulation 🩷🟪	Access Token Manipulation 🩷🟪	Brute Force 🟦🩷🟪🟩	Application Window Discovery 🩷	Internal Spearphishing 🟥	Archive Collected Data 🩷🟪	Communication Through Removable Media 🩷🟪	Data Transfer Size Limits 🟩	Data Destruction 🟦🩷🟪
Gather Victim Identity Information	Compromise Accounts	Exploit Public-Facing Application 🟦🩷🟪	Container Administration Command	Boot or Logon Autostart Execution 🩷🟪	Account Manipulation 🟦🩷🟪	BITS Jobs 🩷🟪	Credentials from Password Stores 🩷🟪	Browser Information Discovery 🟪	Lateral Tool Transfer 🩷	Audio Capture 🩷🟪	Content Injection	Exfiltration Over Alternative Protocol 🟦🩷🟪🟩	Data Encrypted for Impact 🩷🟪
Gather Victim Network Information 🟦🩷🟩	Compromise Infrastructure 🟦🩷🟩	External Remote Services 🟦🩷🟪🟩	Deploy Container	Boot or Logon Initialization Scripts 🟦🩷🟪	Boot or Logon Autostart Execution 🩷🟪	Build Image on Host	Exploitation for Credential Access 🩷🟪	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Automated Collection 🟦🩷🟪	Data Encoding 🩷🟪	Exfiltration Over C2 Channel 🩷🟪	Data Manipulation 🟦🩷🟪
Gather Victim Org Information	Develop Capabilities 🩷	Hardware Additions 🟦🩷🟩	Exploitation for Client Execution 🟦🩷🟪	Browser Extensions 🩷🟪	Boot or Logon Initialization Scripts 🟦🩷🟪	Debugger Evasion 🩷🟪	Forced Authentication 🩷	Cloud Service Dashboard	Remote Services 🟦🩷🟪🟩	Browser Session Hijacking 🩷🟪	Data Obfuscation 🩷🟪🟩	Exfiltration Over Other Network Medium 🩷🟪	Defacement 🩷🟪

Automated

quickly identify

Full visibility

Complexity, simplified with an AI–first XDR



Power of data

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

Power of analytics

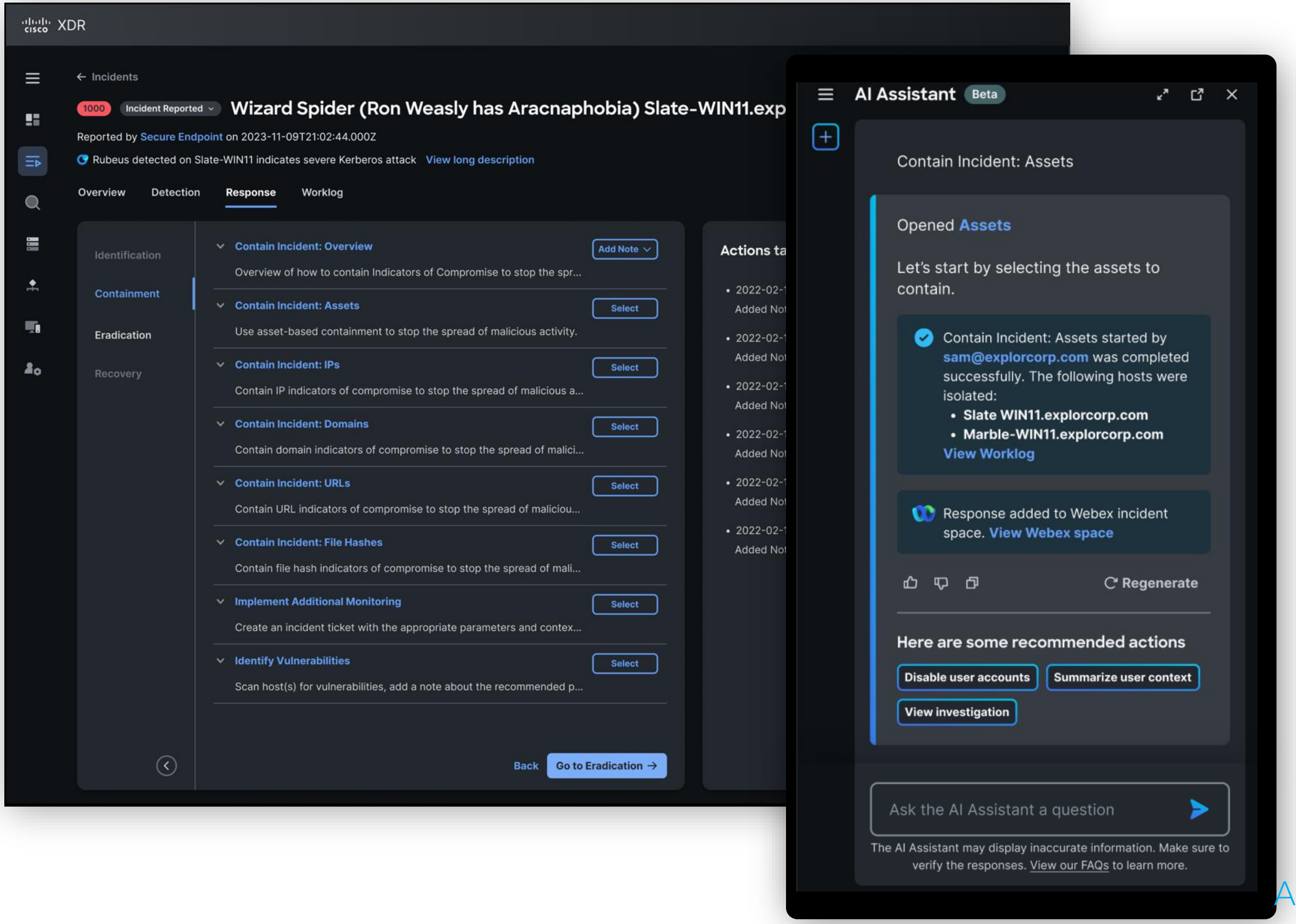
Clear prioritization with behavioral analytics and identity first platform

Power of AI

Automated playbooks and response guidance accelerated with Generative AI assistant

Automation and AI Reducing the Load: Assist security teams, augment human insight, and automate complex workflows

NEW!



Wizard Spider (Ron Weasly has Aracnaphobia) Slate-WIN11.exp

Reported by Secure Endpoint on 2023-11-09T21:02:44.000Z

Rubeus detected on Slate-WIN11 indicates severe Kerberos attack View long description

Contain Incident: Overview
Overview of how to contain Indicators of Compromise to stop the spr...

Contain Incident: Assets
Use asset-based containment to stop the spread of malicious activity.

Contain Incident: IPs
Contain IP indicators of compromise to stop the spread of malicious a...

Contain Incident: Domains
Contain domain indicators of compromise to stop the spread of malici...

Contain Incident: URLs
Contain URL indicators of compromise to stop the spread of maliciou...

Contain Incident: File Hashes
Contain file hash indicators of compromise to stop the spread of mali...

Implement Additional Monitoring
Create an incident ticket with the appropriate parameters and contex...

Identify Vulnerabilities
Scan host(s) for vulnerabilities, add a note about the recommended p...

- 2022-02-1
  Added Not
- 2022-02-1
  Added Not
- 2022-02-1
  Added Not
- 2022-02-1
  Added Not
- 2022-02-1
  Added Not
- 2022-02-1
  Added Not

Contain Incident: Assets

Opened Assets

Let's start by selecting the assets to contain.

Contain Incident: Assets started by sam@explorcorp.com was completed successfully. The following hosts were isolated:
- **Slate WIN11.explorcorp.com**
- **Marble-WIN11.explorcorp.com**

View Worklog

Response added to Webex incident space. View Webex space

Here are some recommended actions

The AI Assistant may display inaccurate information. Make sure to verify the responses. View our FAQs to learn more.

Optimize remediation tactics

Expand visibility across domains:Before-and-after of alert volumes, showing reduction of Prioritized threats

Enhance support for decision making:AI ensures analysts focus on what truly matters."

Ask me about our Meraki MX Integration in Cisco XDR

Shift the focus to outcomes

XDR-driven outcomes

Detect sooner

Where are we most exposed to risk?

How good are we at detecting attacks early?

Speed up investigations

How quickly are we able to understand the full scope and entry vectors of attacks?

Prioritize by impact

Are we prioritizing the attacks that represent the largest material impacts to our business?

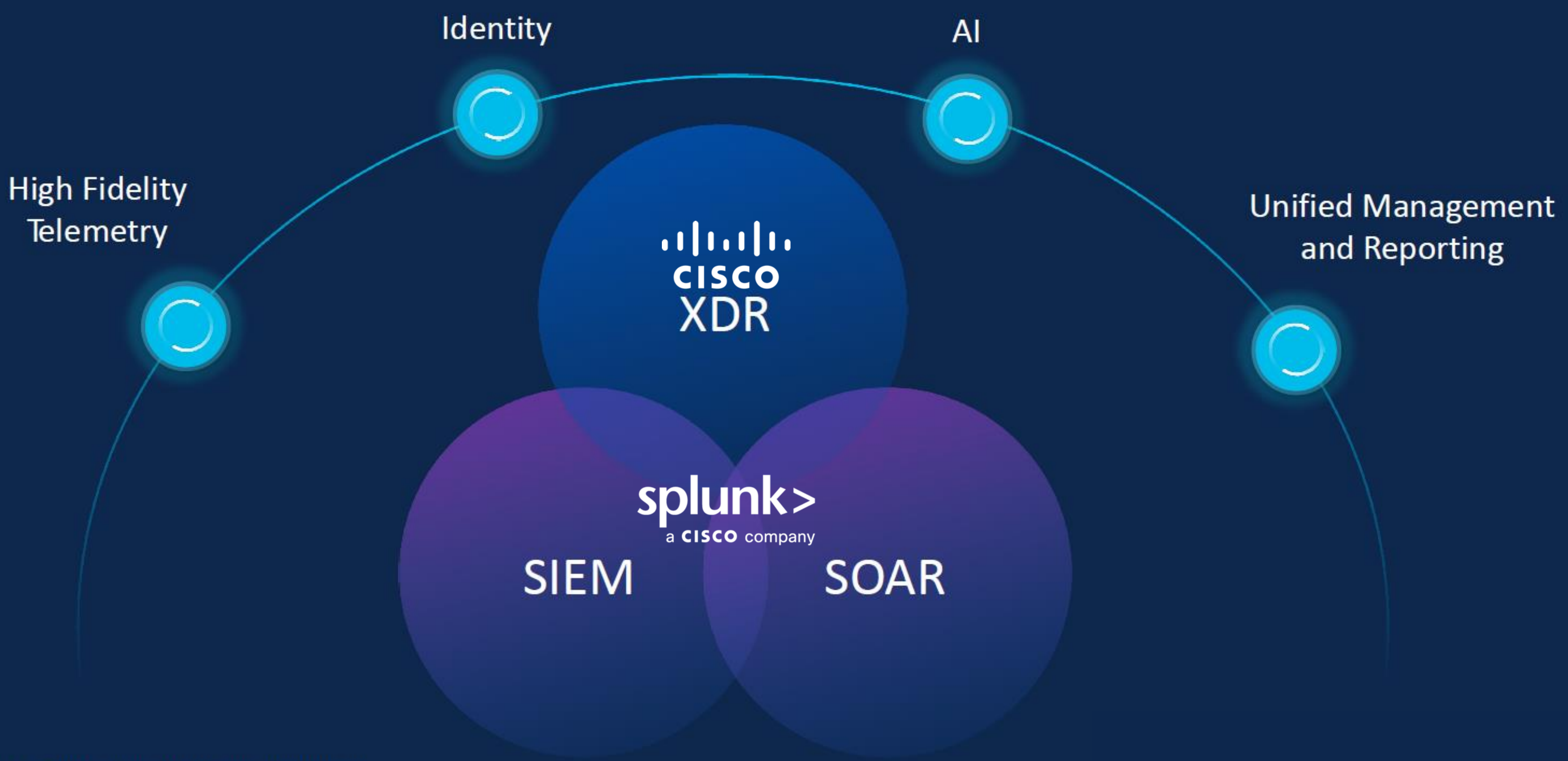
Accelerate response

How fast can we respond?

How much can SecOps automate?

Quantifiably getting better?

Cisco is Delivering the SOC of the Future



Cisco’s Delivering the SOC of the Future

SIEM

Great at answering complex questions

“Show me all failed login attempts for the last 12 hours from our U.K. subsidiary”

XDR

Great at notifying you of an incident

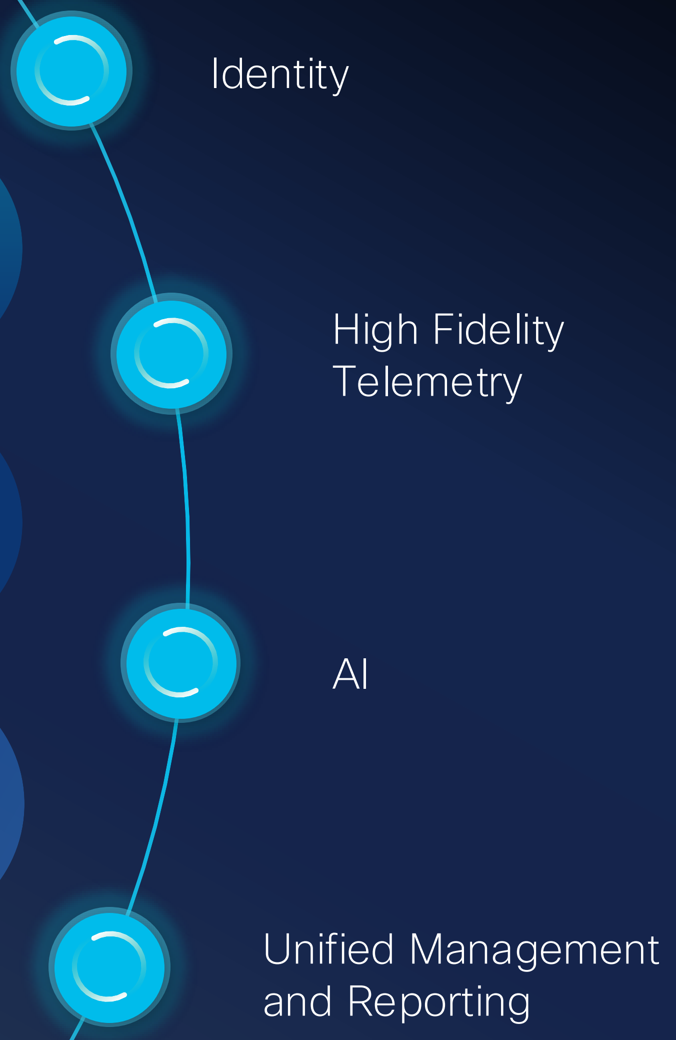
“PowerShell created an internal network connection never seen before. This might be ransomware!!!”

SOAR

Great at automating workflows & response actions

“Initiate a password reset for all U.K. employees.”

”Quarantine the affected endpoint and take a snapshot of all our data center servers.”



What hurts?

- Unsure about our ability to respond to sophisticated threats like ransomware
- Need improvement in security operations metrics and productivity
- Currently utilizing too many disparate tools. (e.g., EDR, NDR, and others)
- Too many single function point products resulting from the ‘best in breed’.
- Lack ability to effectively manage security operations in house.
- Understaffed SOC Undermanned (talent shortage)
- Lack of defined playbooks to determine next steps after detection
- Concerned about the effectiveness of current security tools
- Gaps created by current point product strategy
- Limited productivity of individual analysts or IT staff
- Struggling to address alert fatigue (too much noise, hard to make sense of it) received from individual security products
- Overwhelmed with number of tools and dashboards required to resolve potential incidents
- Numerous manual time-consuming repetitive tasks
- Manually correlating events across multiple telemetry sources takes hours or days
- Constantly escalating events to determine next steps

How we help!

“Healthier, more resilient teams = stronger security and our most valuable resource is your people.”

Cisco XDR supports analysts by integrating with their existing stacks

Highlighting how improved morale and reduced turnover after adopting tools that simplified their workflows

Organizational Impact

- Reduced turnover and increased morale
- Faster response times and fewer breaches
- A stronger, more sustainable security posture

"71% of SOC staff agree about their burnout is a reason for departure: The pain is real.” Cisco XDR eases the burden.

Share a testimonial from a CISO who credits Cisco XDR with transforming their SOC's efficiency and effectiveness 3.

Stressed SOC Team

Thriving SOC Team

Cisco XDR vs Other XDR Vendors

☑ - Yes ❌ - No ❓ - Maybe

	cisco XDR	Others
Natively ingest network telemetry for superior detection and response eliminating blind spots	☑	❌
EDR is not required to be the same as the XDR vendor (no endpoint lock-in)	☑	❌
Best-in-class, proven security analytics included at no additional cost	☑	❌
Talos Threat Intelligence Feed and AI Engines included at no additional cost	☑	❌
90-day retention for telemetry standard and upgradable to 180 or 365 days	☑	❌
Context applied to Incidents for advanced prioritization	☑	❌
Leverages world's most widely deployed VPN for visibility to user and device behavior on & off network	☑	❌
Incident Creation from 3rd Party Telemetry supported (Advantage and Premier)	☑	❌
Cisco Native Integrations at no additional cost	☑	❌
Curated 3rd Party integrations included and custom integrations available (Advantage and Premier)	☑	❌
Ability to create an incident from IOT/OT/Medical devices without endpoint agents or probes	☑	❌
Average 5 minutes to detect/quarantine and 15-30 minutes to vetted report for XDR Premier	☑	❌
96.5% False Positive catch rate for XDR Premier	☑	❌
Allow direct communication to SOC analyst and customer retains full access to the console XDR Premier	☑	❌

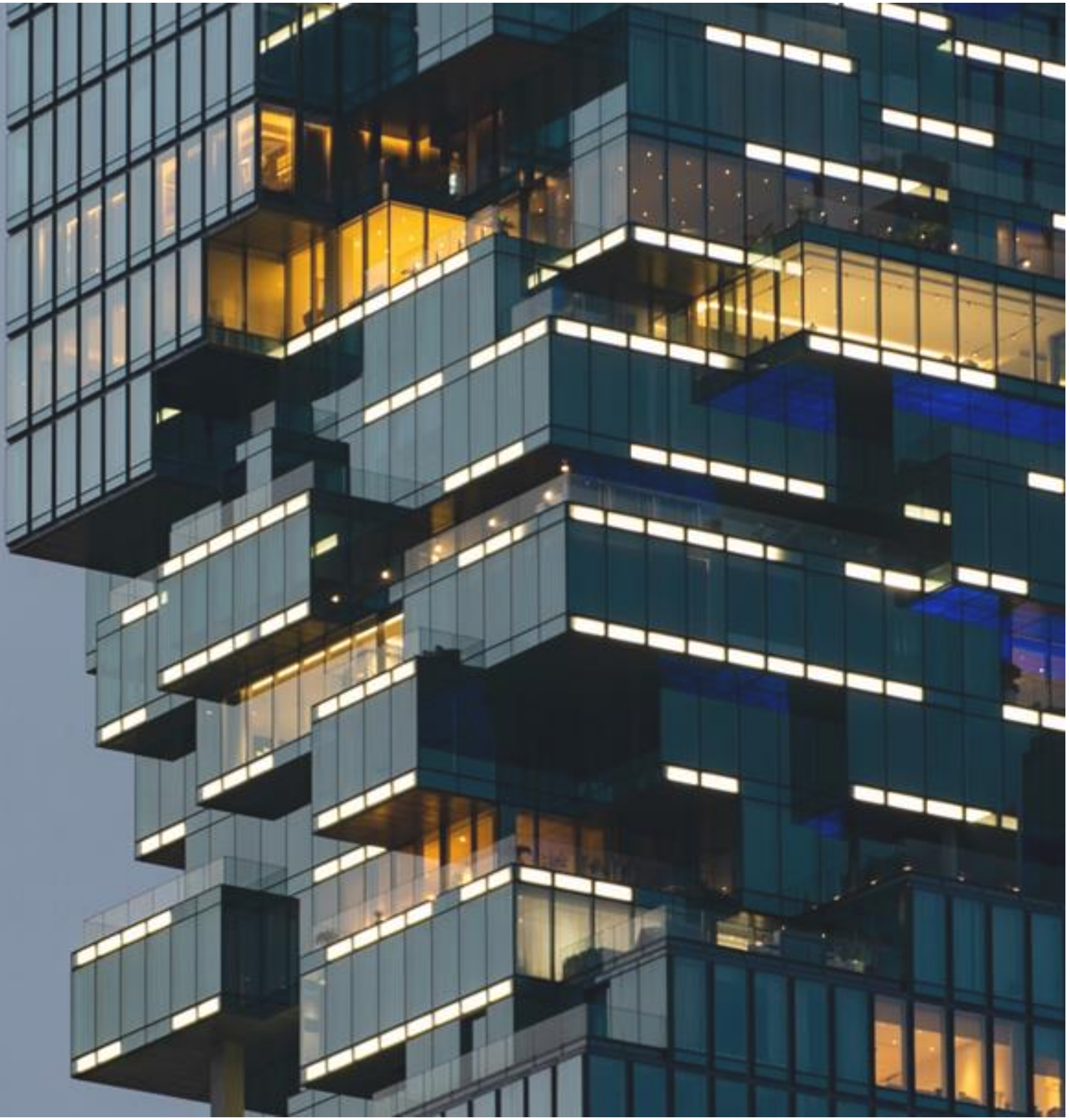
Valuable Takeaways about Cisco XDR

- Cisco is the Only XDR out of 90 vendors in the XDR market with an NDR, IDR, and AI Assistant included at no extra cost
- Flexible Licensing model is done by employee knowledge base worker count not Endpoint and server count like traditional XDR vendors
- Can ingest telemetry and NetFlow from directly from Cisco Catalyst and Meraki switches
- Open Architecture Vs. Native
- Automated Ransomware Recovery w/Cohesity

Video Overview of Cisco XDR

See Cisco XDR in Action Guided Demo

Learn more at cisco.com/go/xdr



CISCO

The bridge to possible