

The background is a vibrant, abstract graphic featuring a spectrum of colors from red and orange on the left to blue and green on the right. The colors are arranged in a series of overlapping, wavy bands that create a sense of movement and depth. A bright, white, starburst-like light source is positioned on the right side, from which rays of light emanate across the entire scene, enhancing the dynamic feel of the design.

cisco *Live!*

Let's go

#CiscoLiveAPJC



The bridge to possible

Cisco XDR

Making Sense of all the Parts & Pieces

Aaron T. Woland, CCIE #20113

Distinguished Engineer, Threat Detection & Response

loxx@cisco.com | @aaronwoland

BRKSEC-2113

CISCO *Live!*

#CiscoLiveAPJC

\$ whoami



Cisco role: Distinguished Engineer,
Threat Detection & Response

Unofficial title:
“Cisco History Professor”

Experience: Old enough to wonder
how I have been doing this for ~30
years

Fun fact 1: Father of 5 daughters

Fun fact 2: Oldest works for Cisco
now! Youngest is 18 months!

Fun fact 3: Working through his
Cyber Security Master’s Degree
from SANS Institute (~04/24)

Sarcasm

*“If we can’t laugh
at ourselves,
Then we cannot
laugh at anything
at all”*



Cisco Webex App

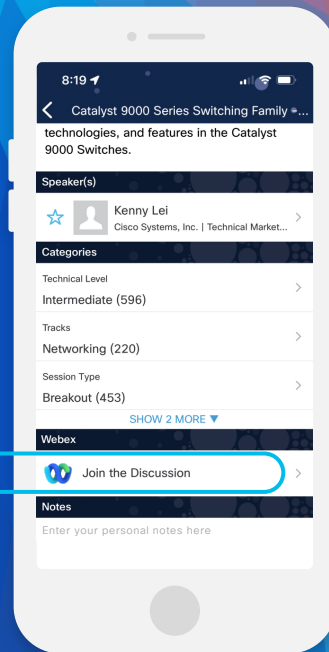
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until December 22, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2113>

Disclaimer: “All Comments
are my own, and are not
representative of Cisco...
Any correlation to real live
persons or situations was
completely unintentional...
Blah Blah Blah...”

Participating in user research gives you a place to share your thoughts and experiences to influence the future of Cisco Secure products.

- You'll hear from us at most once every 90 days.
- Participation is completely optional and you can opt out at any time.

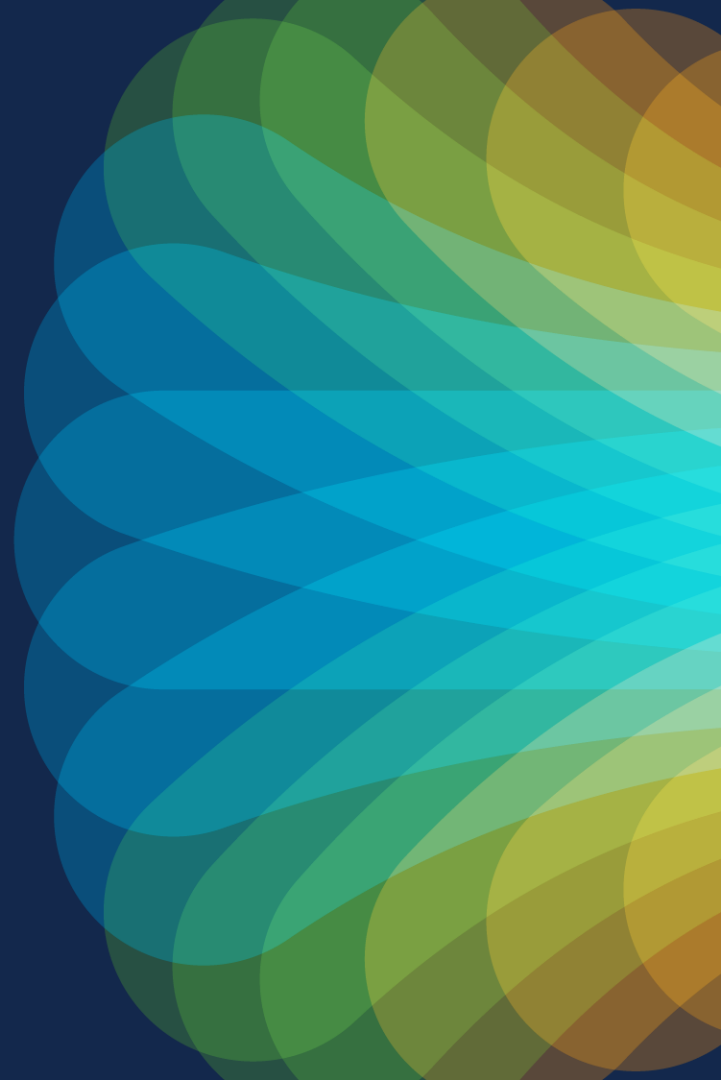


Please fill out the survey



Drop your email in the comments – I WILL respond!

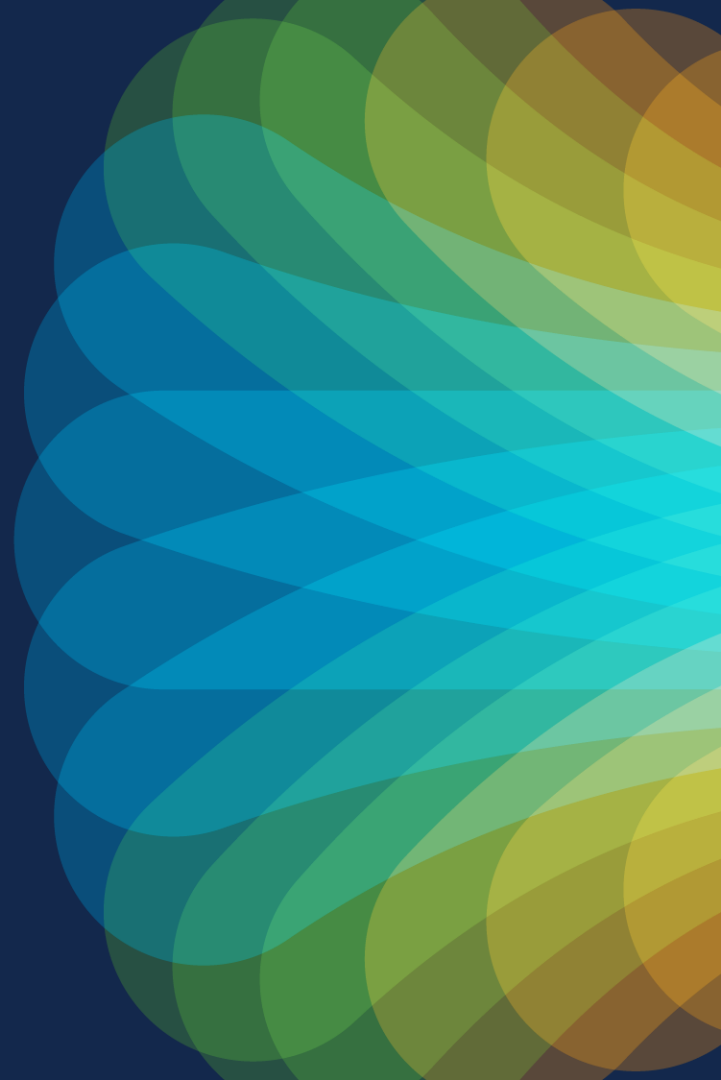
Let's get this
road on the
show...



Agenda

- A History Lesson
- Evolution
- Incident Management & Workflow
- Integrations & Response
- Key XDR Telemetry
- That's a wrap!

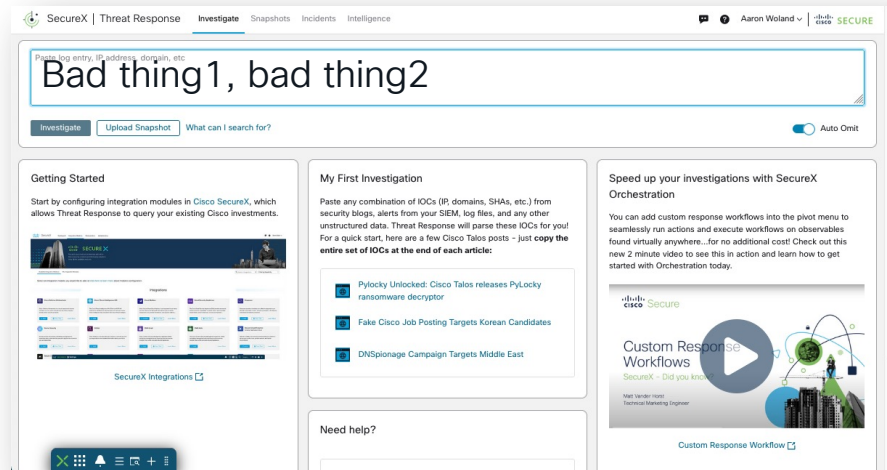
A Little History Lesson



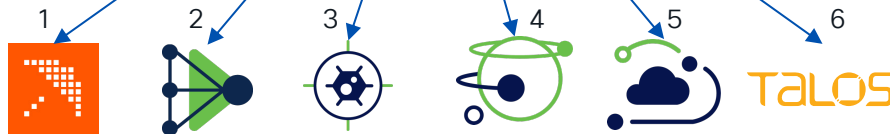
Way Back in 2017

- Security Leadership pet Project: “Visibility”
- Renamed to Cisco Threat Response (2018)
 - Based on history of performing incident response
 - Productizing the process they followed as practitioners
 - Search for “observables” and it enriches from all integrated sources (via APIs) with “findings”
 - Note: Cisco acquires Obsrvbl Networks in same year

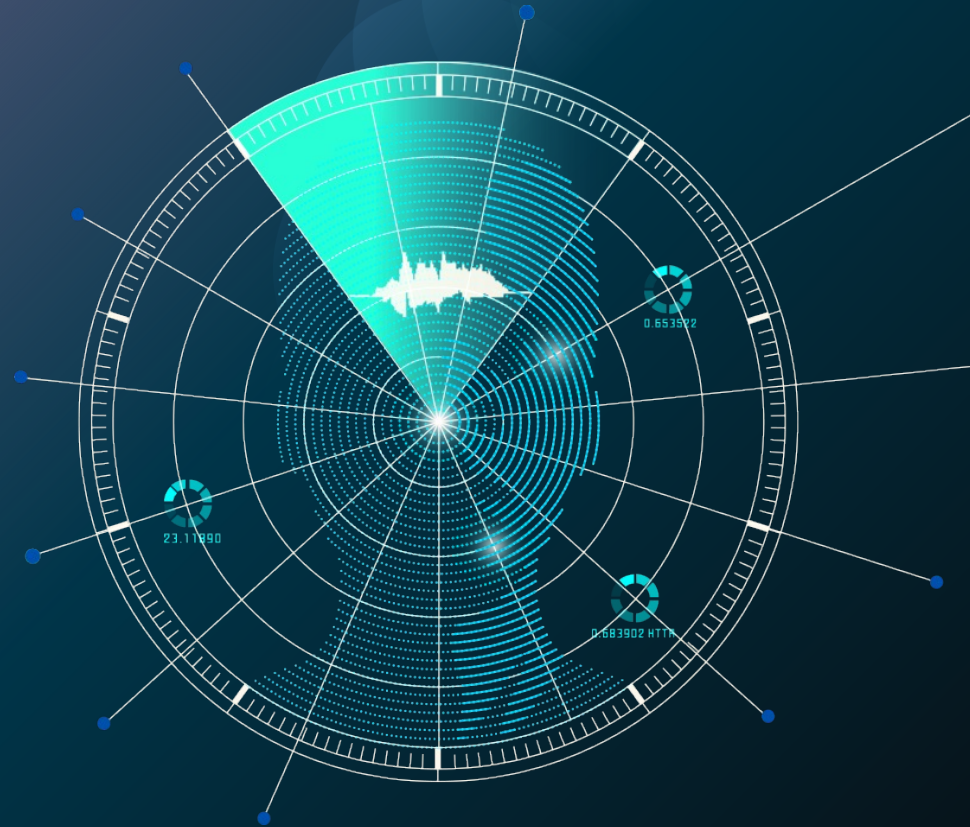
CISCO *Live!*



Have sightings of these observables?



Then in 2020...



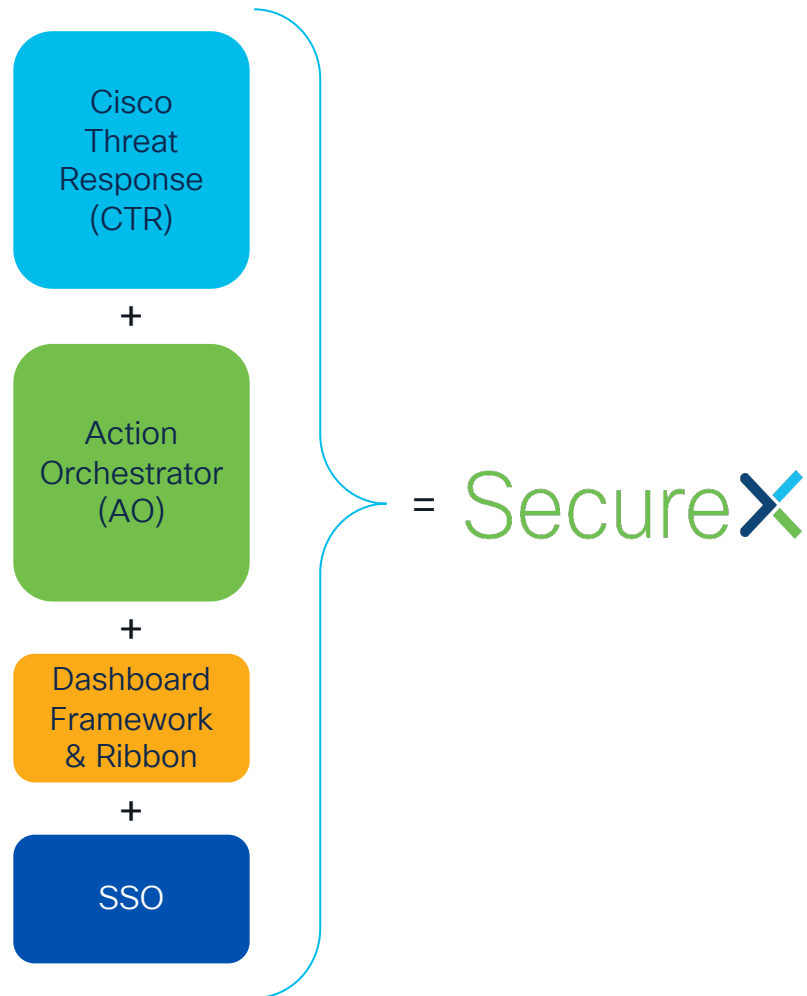
Introduced SecureX May of 2020

A cloud-native, **built-in platform** experience within our portfolio

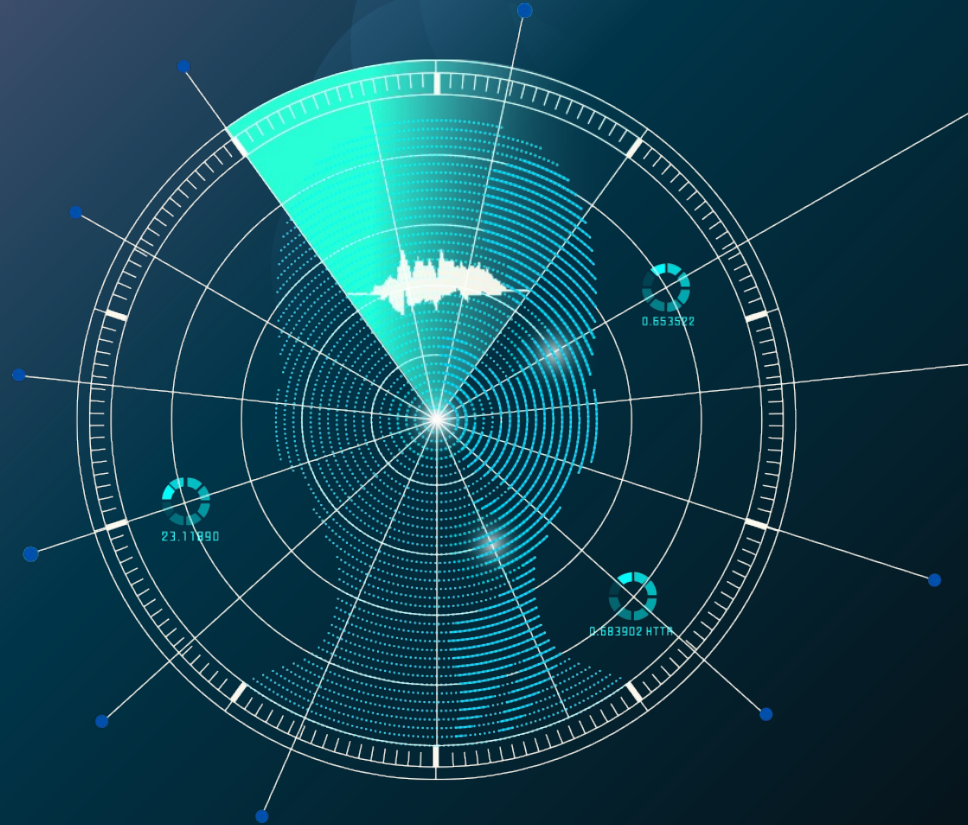


SecureX was to be THE Platform

- Cisco Secure [function]
 - X was to be the central place
 - X leveraged Cisco Threat Response to integrate all Cisco products together
 - X adds a full automation engine we “acquired” from the cloud division
 - X provided the SSO experience for Cisco Security
 - All future UI’s to be built in SecureX



In 2021 analysts
create a new
market category
“*eXtended
detection &
Response*”



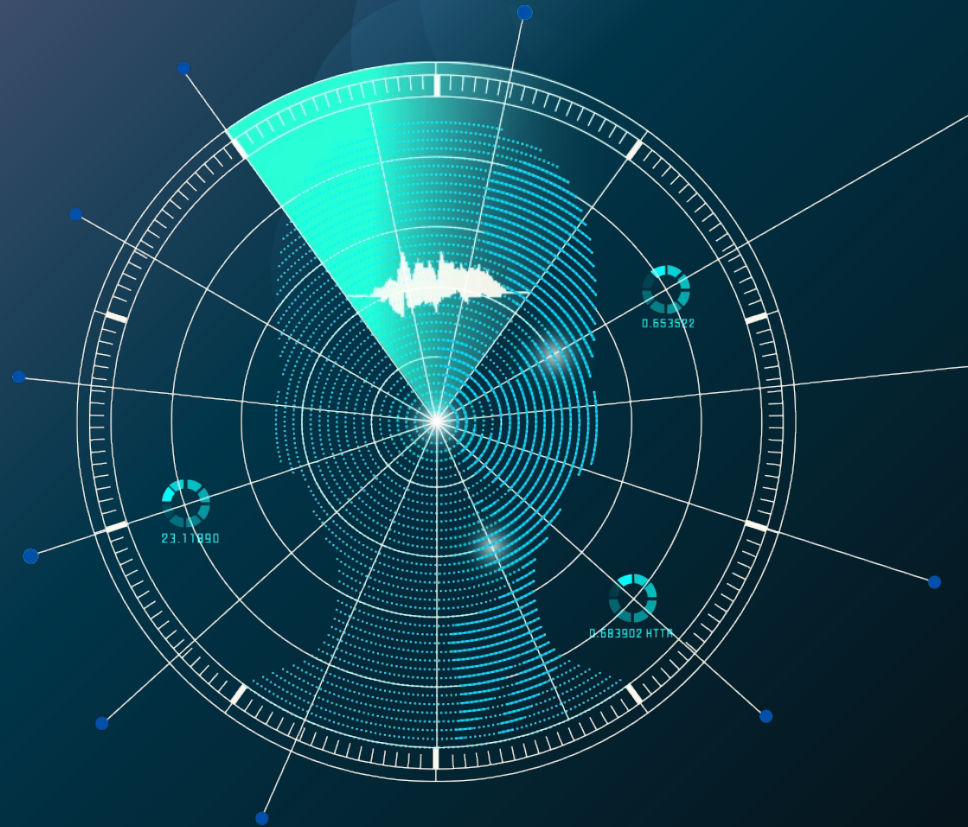
“Cisco SecureX is a leader for XDR”

– Analysts in 2021

*Uhh... “Yes, we ARE”...
Go forth & market it that way...*

- Former Cisco Executive Leaders

Cisco fully
embraces the
XDR concept;
sees it as a
market transition



Let's go!!!!

Cisco dives head-on into XDR space

Hired external research and design company to augment us

1 Invests millions in research

Invested heavily internally

2

Expanding our User Experience & Interface Teams

Customers didn't even know they were talking to Cisco (blind) as well as our own customer feedback

3 Blind & Sighted Interviews

Extensive Hiring of Experts

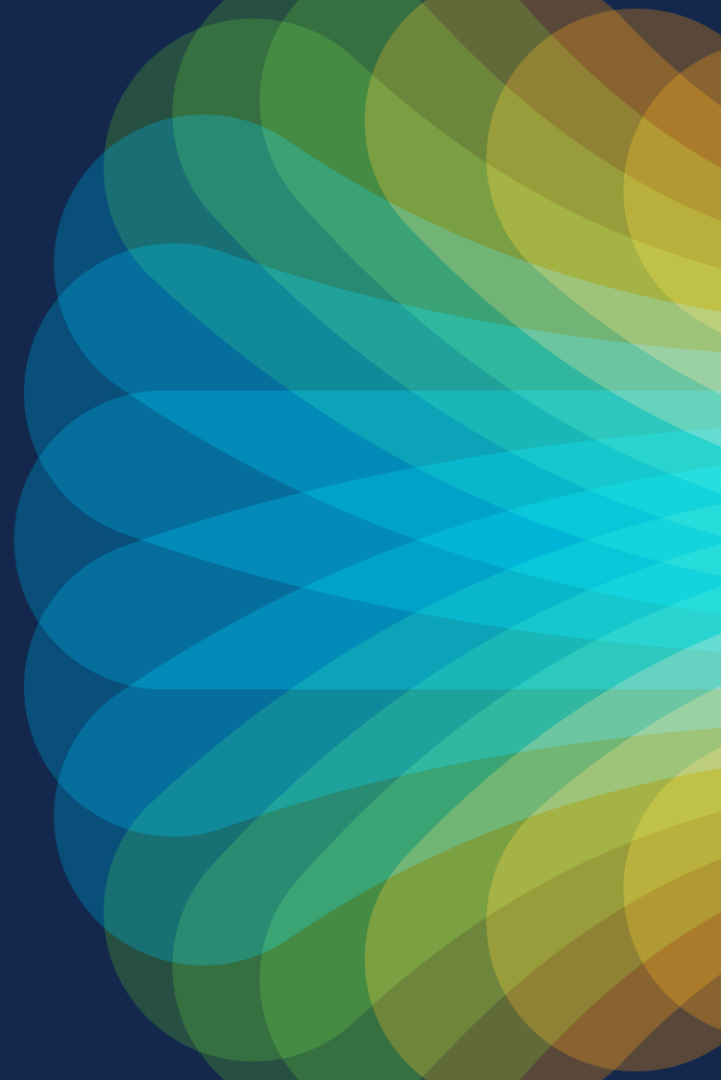
4

Brought in Principal Engineers in key places with tons of incident management / SOC experience

Leveraging the BEST technology to meet the defined experience, not building the experience based on the tech

5 Restructured our Products

What did it
yield?





“ The need for XDR is driven
by the market not meeting
the needs of the SOC”

- XDR Beta Customer

An XDR is an expression of business needs

Where are we **most exposed** to risk? How good are we at detecting attacks **early**?

1 Detect Sooner

Prioritize by Impact

2

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

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

3 Reduce Investigation Time

Accelerate Response

4

How fast can we **confidently respond**
How much can SecOps **automate improving** our time to respond?

Do we have **full visibility** into all our assets? Can we **reliably identify** a device and who uses it?

5 Extend Assets Context



Adversary Turla



// Nickname

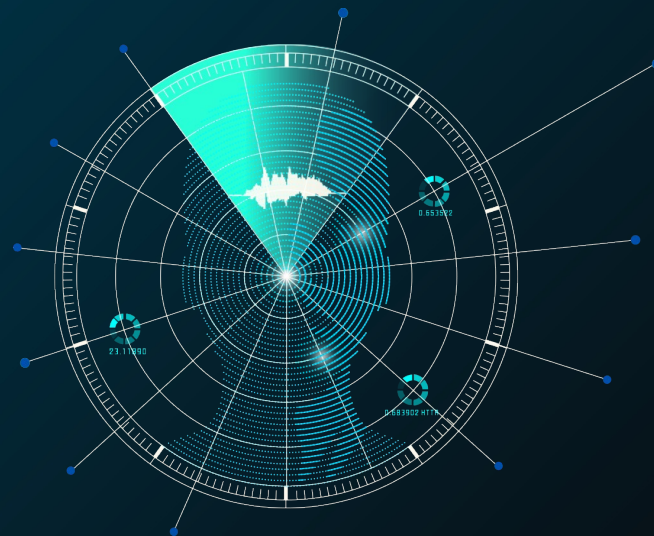
Snake,
Venomous Bear,
Uroburos,
Group 88,
Waterbug

The adversary: What do we know?

- Estonian intelligence services associate this group with the Russian federal security service (FSB).
- Does NOT **deploy advanced tools unless necessary** to compromise the target

Method:

- Prefers watering holes and social engineering to manipulate victims
- Crafted lures are highly tailored to their targets
- Exploit themes related to current events
- First-stage malware typically acts as a filter



Without XDR, How Can We Detect and Respond to All of This?

TA0001: Initial Access	TA0002: Execution	TA0003: Persistence
T1189: Drive-by Compromise	T1059: Command and Scripting Interpreter	T1098: Account Manipulation
T1190: Exploit Public-Facing Application	T1203: Exploitation for Client Execution	T1197: BITS Jobs
T1133: External Remote Services	T1559: Inter-Process Communication	T1547: Boot or Logon Autostart Execution
T1200: Hardware Additions	T1106: Native API	T11037: Boot or Logon Initialization Scripts
T1566: Phishing	T1053: Scheduled Task/Job	T1176: Browser Extensions
T1566.001: Spearphishing Attachment	T1129: Shared Modules	T1554: Compromise Client Software Binaries
T1566.002: Spearphishing Link	T1072: Software Deployment Tools	T1136: Create Account
T1566.003: Spearphishing via Service	T1569: System Services	T1543: Create or Modify System Process
T1091: Replication Through Removable Media	T1204: User Execution	T1546: Event Triggered Execution
T1195: Supply Chain Compromise	T1047: Windows Management Instruments	T1133: External Remote Services
T1199: Trusted Relationship		T1154: Hijack Execution Flow
T1078: Valid Accounts	T11078.001: Default Accounts	T1556: Modify Authentication Process
	T11078.002: Domain Accounts	T1137: Office Application Startup
	T11078.003: Local Accounts	T1542: Pre-OS Boot
		T1053: Scheduled Task/Job
		T1505: Server Software Component

TAD006: Credential Access		TAD007: Discovery
T1557: Adversary-in-the-Middle		T1087: Account Discovery
T1110: BruteForce	T1110.004: Credential Stuffing T1110.005: Password Cracking T1110.001: Password Guessing T1110.003: Password Spraying	T1087.002: Domain Account T1087.003: Email Account T1087.001: Local Account
T1555: Credential from Password Store	T1555.003: Credentials from Web browser T1555.005: Password Managers T1555.002: Secure Internet Memory T1555.004: Windows Credential Manager	T1010: Application Window Discovery T1022: Debugger Evasion T1482: Domain Trust Discovery T1093: Elevated Execution Discovery T1555: Group Policy Discovery
T112: Exploitation for Credential Access		T1046: Network Service Discovery
T1187: Forced Authentication		T1135: Network Share Discovery T1083: Network Sniffing
T1056: Forge Web Content		T1031: Password Policy Discovery T1120: Peripheral Device Discovery
T1056 Input Capture	T1056.004: Credential API Hooking T1056.002: GUI Input Capture T1056.003: Keylogging	T1069: Permission Groups Discovery
	T1056.001: Web Portal Capt ure	T1069.002: Domain Groups T1069.001: Local Groups
T1556: Modify Authentication Process		T1067: Process Discovery T1012: Query Registry
T1111: Multi-Factor Authentication Interception		T1018: Remote System Discovery T1018: Session Discovery
T0121: Multi-Factor Authentication Request Generation		T1014: System Information Discovery T1014: System Location Discovery
T0003 OS Credential Dumping	T1003.008: Jcex/Jshim and Jcat/Jshim T1003.005: Cached Domain Credentials T1003.006: DCSync T1003.004: LSASecrets T1003.001: LSASS Memory T1003.007: NTDS T1003.007: Proc Flattening T1003.002: Security Account Manager	T1016: System Network Configuration T1016.001: Internet Connection Discovery T1016: System Owner User Discovery T1007: System Service Discovery T1124: System Time Discovery T1497: Virtualization/Sandbox Evasion
T1558: Steal or Forge Cookies/Tokens		
T1539: Steal or Forge Kerberos Tickets		
T1552: Unsecured Credentials	T1552.003: Bash History T1552.004: CPanel Logs T1552.002: Credentials in Registry T1552.006: Group Policy Preferences T1552.004: Private Keys	

Mobile Package Installation		Mobile Database Installer	
Android 7/20/2012: Google Script Minimizer 7/20/2012: Google Script Editor 7/20/2012: Google Analytics 7/20/2012: Google Analytics	7/20/2012: Google Script Minimizer 7/20/2012: Google Script Editor 7/20/2012: Google Analytics 7/20/2012: Google Analytics	7/20/2012: Google Script Minimizer 7/20/2012: Google Script Editor 7/20/2012: Google Analytics 7/20/2012: Google Analytics	7/20/2012: Google Script Minimizer 7/20/2012: Google Script Editor 7/20/2012: Google Analytics 7/20/2012: Google Analytics
iOS 7/20/2012: AppleScript 7/20/2012: AppleScript 7/20/2012: AppleScript 7/20/2012: AppleScript	7/20/2012: AppleScript 7/20/2012: AppleScript 7/20/2012: AppleScript 7/20/2012: AppleScript	7/20/2012: AppleScript 7/20/2012: AppleScript 7/20/2012: AppleScript 7/20/2012: AppleScript	7/20/2012: AppleScript 7/20/2012: AppleScript 7/20/2012: AppleScript 7/20/2012: AppleScript
Windows 7/20/2012: Windows 7/20/2012: Windows 7/20/2012: Windows 7/20/2012: Windows	7/20/2012: Windows 7/20/2012: Windows 7/20/2012: Windows 7/20/2012: Windows	7/20/2012: Windows 7/20/2012: Windows 7/20/2012: Windows 7/20/2012: Windows	7/20/2012: Windows 7/20/2012: Windows 7/20/2012: Windows 7/20/2012: Windows
Linux 7/20/2012: Linux 7/20/2012: Linux 7/20/2012: Linux 7/20/2012: Linux	7/20/2012: Linux 7/20/2012: Linux 7/20/2012: Linux 7/20/2012: Linux	7/20/2012: Linux 7/20/2012: Linux 7/20/2012: Linux 7/20/2012: Linux	7/20/2012: Linux 7/20/2012: Linux 7/20/2012: Linux 7/20/2012: Linux
Mac OS X 7/20/2012: Mac OS X 7/20/2012: Mac OS X 7/20/2012: Mac OS X 7/20/2012: Mac OS X	7/20/2012: Mac OS X 7/20/2012: Mac OS X 7/20/2012: Mac OS X 7/20/2012: Mac OS X	7/20/2012: Mac OS X 7/20/2012: Mac OS X 7/20/2012: Mac OS X 7/20/2012: Mac OS X	7/20/2012: Mac OS X 7/20/2012: Mac OS X 7/20/2012: Mac OS X 7/20/2012: Mac OS X
Other 7/20/2012: Other 7/20/2012: Other 7/20/2012: Other 7/20/2012: Other	7/20/2012: Other 7/20/2012: Other 7/20/2012: Other 7/20/2012: Other	7/20/2012: Other 7/20/2012: Other 7/20/2012: Other 7/20/2012: Other	7/20/2012: Other 7/20/2012: Other 7/20/2012: Other 7/20/2012: Other

T1122: Modify Registry	T1027.001: Binary Padding
T1027: Obfuscated Files or Information	T1027.004: Compile After Delivery
	T1027.005: HTML Smuggling
	T1027.005: Indicate or Removal from Tool
	T1027.002: Software Packing
	T1027.003: Steganography
T1542: Pre-OS Boot	T1055.004: Asynchronous Procedure Call
T1055: Process Injection	T1055.001: Dynamic Link Library Injection
	T1055.011: Extra Window Manager Injection
	T1055.015: List Planning
	T1055.002: Portable Executable Injection
	T1055.009: Proc. Memory
	T1055.013: Process Doppelganging
	T1055.012: Process Hollowing
	T1055.008: Process System Calls
	T1055.003: Thread Execution Hijacking
	T1055.005: Thread Local Storage
	T1055.014: VMOS Hijacking
T1620: Reflective Code Loading	
T1207: Rogue Domain Controller	
T1014: Rootkit	T1553.002: Code Signing
T1553: Subvert Trust Controls	T1553.006: Code Signing Policy Modification
	T1553.007: Install Root Certs on SCA
	T1553.005: Mark of the Web Bypass
	T1553.003: SIP and Trust Provider Hijacking
T1218: System Binary Proxy Execution	T1218.003: CMSTP
	T1218.001: Compiled HTML File
	T1218.002: Control Panel
	T1218.004: InstallUtil
	T1218.013: Msconfig
	T1218.014: MMC
	T1218.005: Mshta
	T1218.007: Msiexec
	T1218.008: Odbcconf
	T1218.009: Regsvcs/Regasm
	T1218.010: Regsvr32
	T1218.011: Rundll32
	T1218.012: Verclsid
T1216: System Script Proxy Execution	
T1221: Template Injection	
T1205: Traffic Signaling	T1550.002: Pass the Hash
	T1550.003: Pass the Ticket
T1217: Trust of Developer Utilities Proxy Execution	
T1550: Use Alternate Authentication Mechanism	T1078.001: Default Accounts
	T1078.002: Domain Accounts
	T1078.003: Local Accounts
T1497: Virtualization/Sandbox Evasion	
T1490: Win32-System-Resource Hijacking	

TA0011: Command and Control		TA0010: Exploitation	
T11071: Application Layer Protocol	T11071.004: DNS	T11020: Automated Exploitation	
	T11071.002: File Transfer Protocols	T11030: Data Transfer Size Limits	
	T11071.003: Mail Protocols	T11048: Exploitation Over Alternative Ports	
	T11071.001: Web Protocols	T11041: Exploitation Over C2 Channel	
T11092: Communication Through Removable Media		T11011: Exploitation Over Other Network	
T11132: Data Encoding	T1132.002: Non-Standard Encoding	T11052: Exploitation Over Physical Media	
	T1132.001: Standard Encoding	T11567: Exploitation Over Web Service	
T11001: Data Obfuscation	T11001.001: Junk Data	T11029: Scheduled Transfer	
	T11001.003: Protocol Impersonation		
	T11001.002: Steganography		
T11568: Dynamic Resolution			
T11573: Encrypted Channel	T11573.002: Asymmetric Cryptography		
	T11573.001: Symmetric Cryptography		
T11008: Failback Channels			
T11105: Ingress Tool Transfer			
T11104: Multi-Stage Channels			
T11095: Non-Application Layer Protocols			
T11571: Non-Standard Port			
T11572: Protocol Tunneling			
T11090: Proxy	T11090.004: Domain Fronting		
	T11090.002: External Proxy		
	T11090.001: Internal Proxy		
	T11090.003: Multi-Hop Proxy		
T11219: Remote Access Software			
T11205: Traffic Signaling	T11205.001: Port Knocking		
T11102: Web Service	T11102.002: Bidirectional Communication		
	T11102.001: Dead Drop Resolver		
	T11102.003: One-Way Communication		

TA0009: Lateral Movement		TA0008: Collection	
T11210: Exploitation of Remote Services		T11557: Adversary Join-in-the-Middle	
T11234: Internal Searchlighting		T11560: Archive/Collected Data	T11560.003: Archive via Custom Method
T11570: Local Mail Transfer			T11560.002: Archive via Library
T11543: Remote Service Session Hijacking	T11563.003: RDP Hijacking		T11560.001: Archive via Email
	T11563.001: SSH Hijacking	T11123: Audio Capture	
T11031: Remote Service	T11021.003: Distributed Component Objects	T11139: Automated Collection	
	T11021.002: Remote Desktop Protocol	T11135: Browser Session Hijacking	
	T11021.001: Remote Desktop Protocol	T11115: Clipboard Data	
	T11021.004: SSH	T11213: Data from Information Repositories	
	T11021.005: VNC	T11005: Data from Local System	
	T11021.006: Windows Remote Manager	T11039: Data from Remote Shared Drive	
T11091: Replication Through Removable Media		T11025: Data from Removable Media	
T11072: Software Deployment Tools		T11074: Data Staging	T11074.001: Local Data Staging
T11080: Taint Shared Contents			T11074.002: Remote Data Staging
			T1114.003: Email Forwarding Rule
			T1114.001: Local Email Collection
			T1114.002: Remote Email Collection
T11530: Use Alternate Authentication Methods	T11550.003: Remote Shell	T11056.004: Credentials API Hooking	
	T11550.002: Password Tricker	T11056.003: GUI Input Capture	
		T11056.001: Remote Desktop	
		T11056.002: Web Portal Capture	
		T11113: Screen Capture	

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 Client



Cisco/ Meraki (Networking)



Firewall Threat Defense (FTD)



Duo

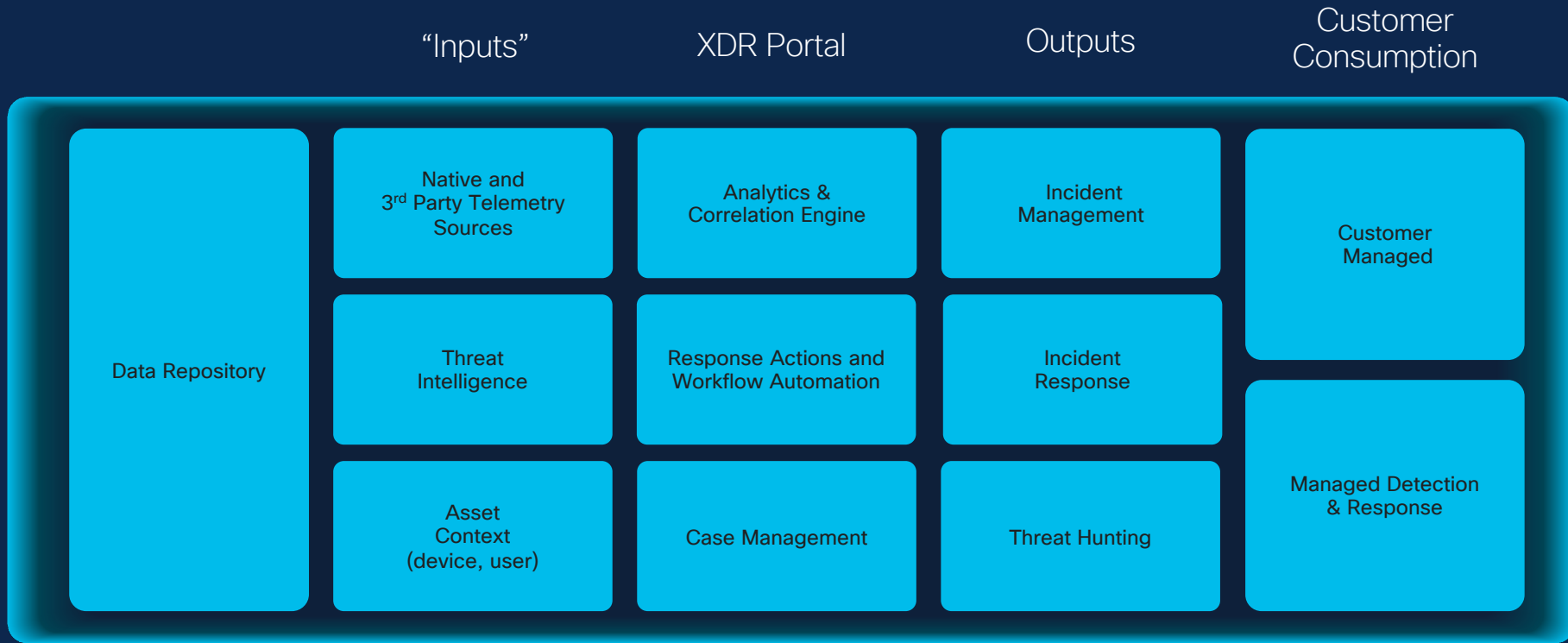


Email Threat Defense (ETD)

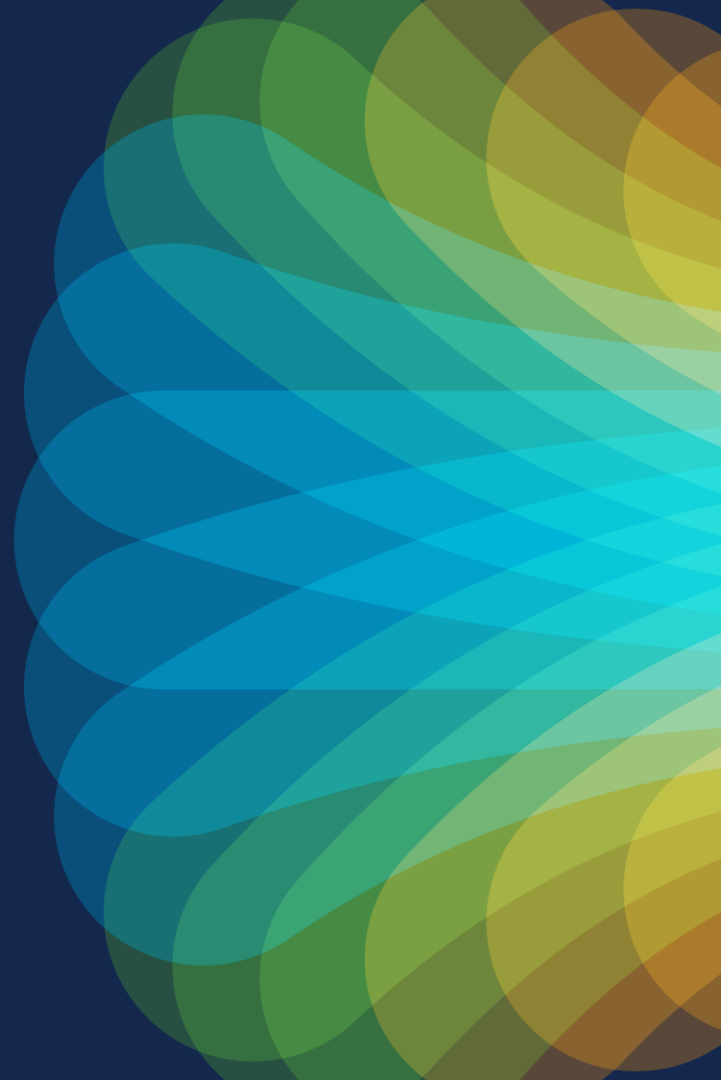


Umbrella

What Are the Building Blocks of an Ideal XDR Solution?



How do we
accomplish this?



Agenda

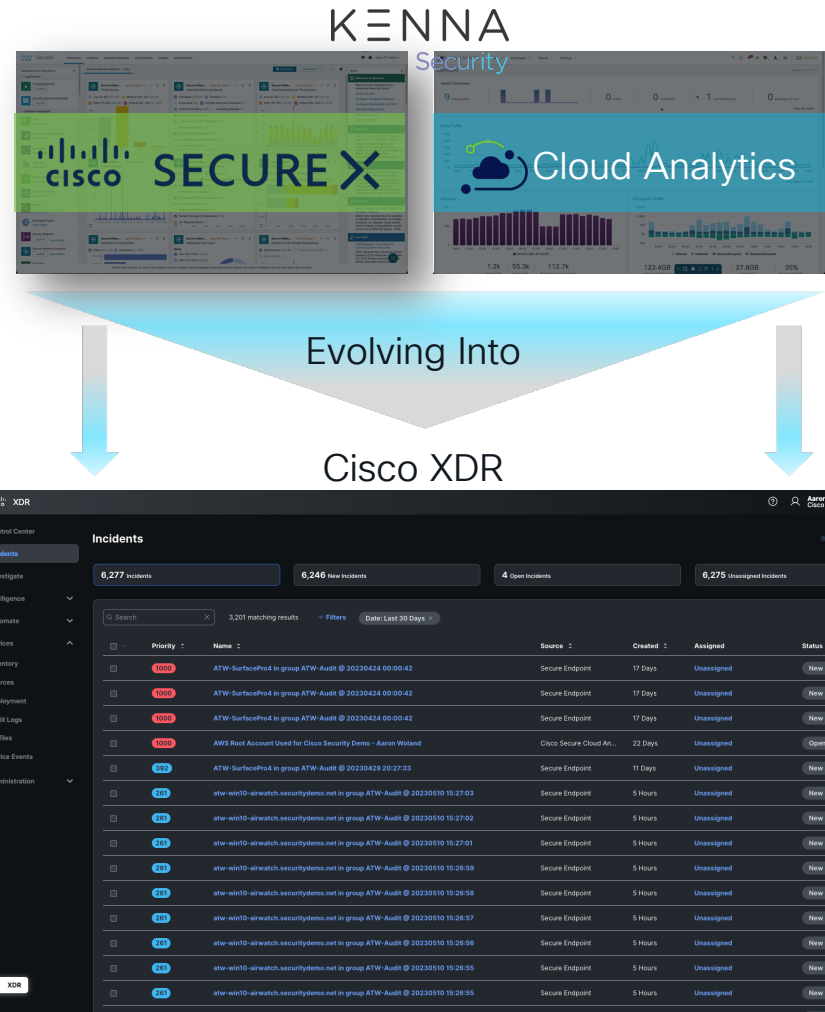
- A History Lesson
- Evolution
- Incident Management & Workflow
- Integrations & Response
- Key XDR Telemetry
- That's a wrap!

Evolution

- Parts of SecureX
- *Plus* Secure Cloud Analytics
- *Plus* Kenna Intellectual Property
- *Plus* New Tech
- *EQUALS* Cisco XDR

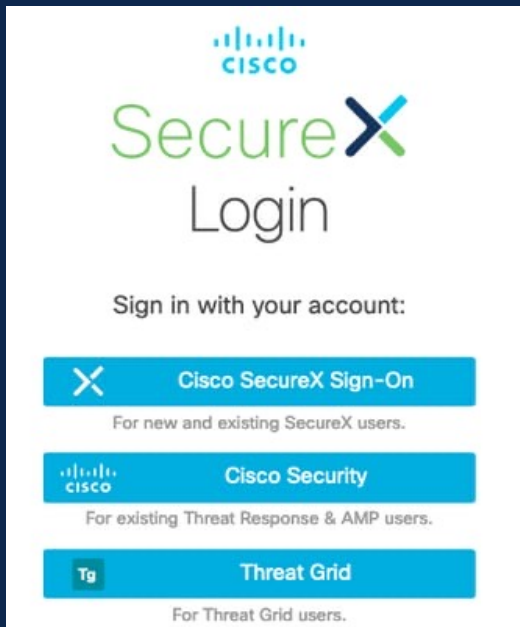
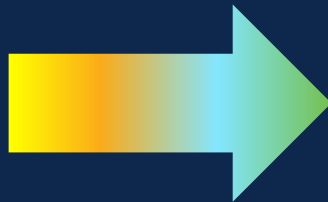
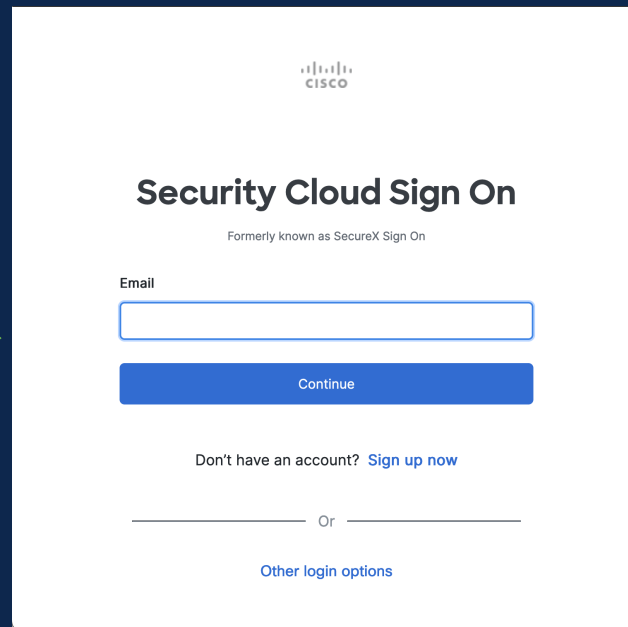
cisco *Live!*

soon plus **ORT**
now part of cisco



SecureX is no longer “the platform”

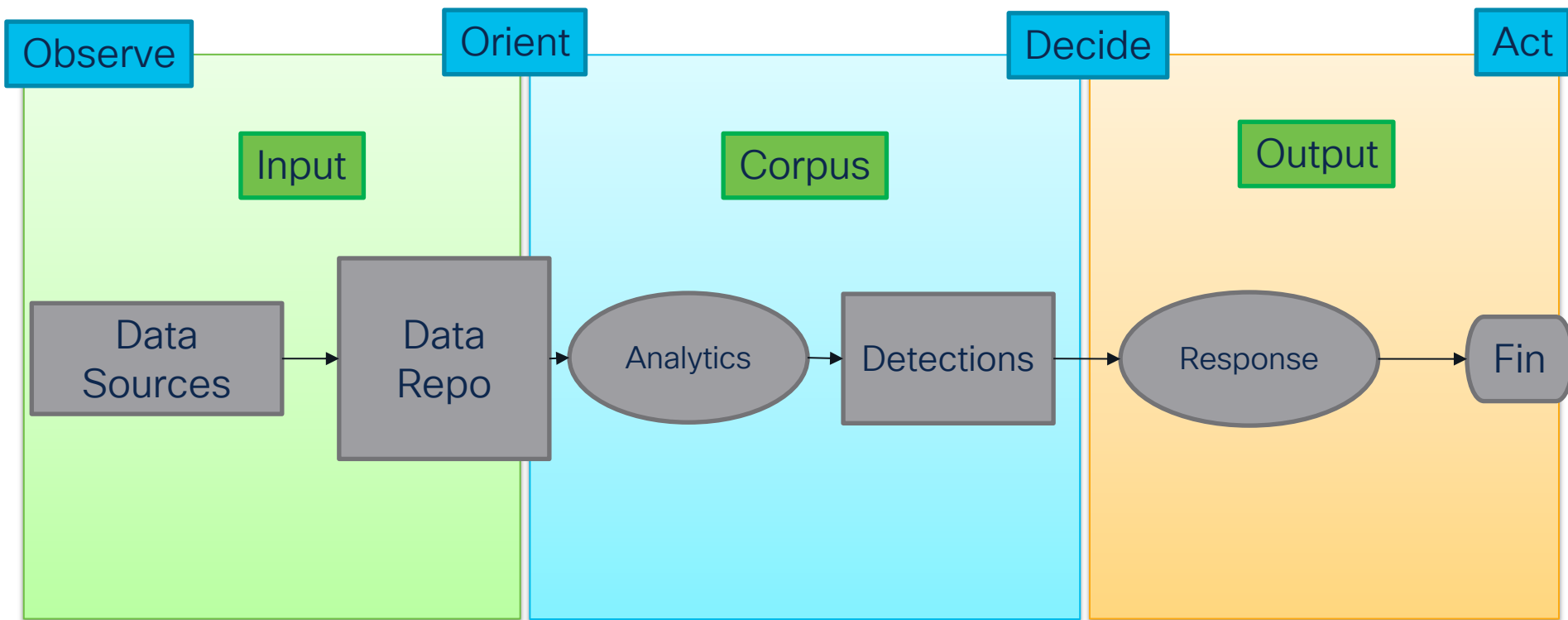
The “Cisco Security Cloud” is the platform



*“XDR is a Security Operations
Productivity Tool”*

- Me

An XDR speeds up the OODA Loop



Investigators build
out a timeline.

The XDR
**automates the
timeline** creation

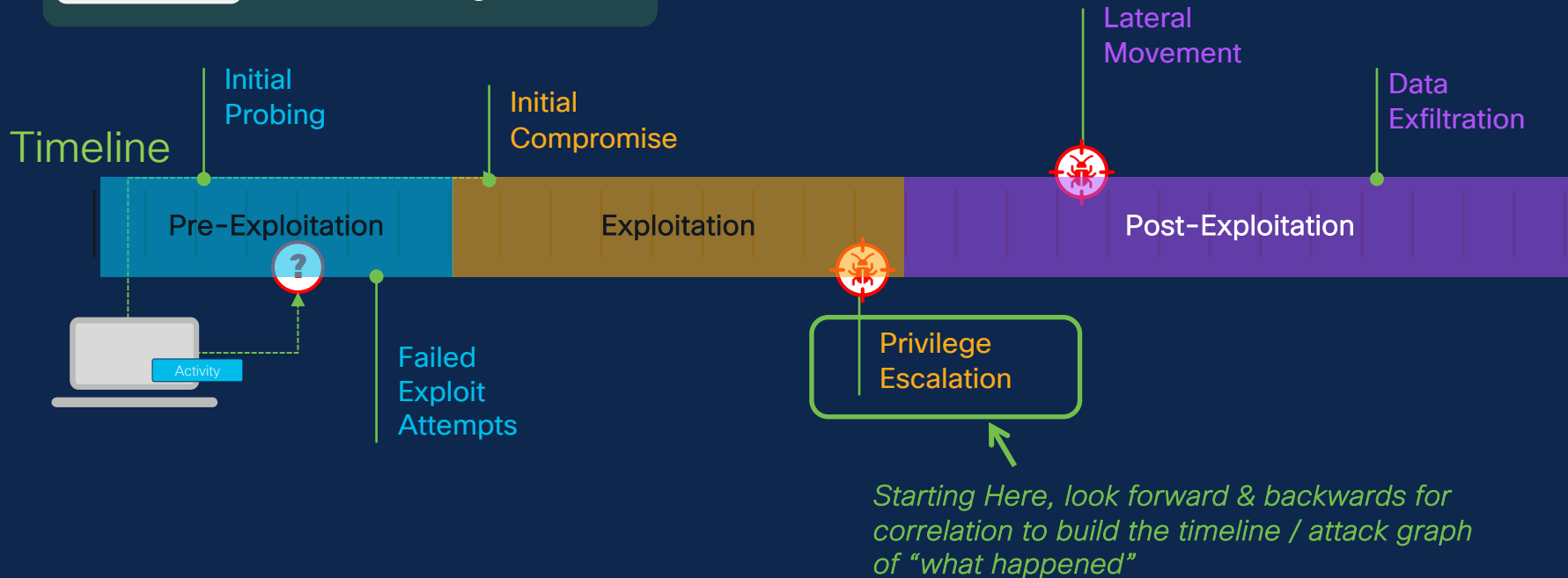


Investigation Timeline – what happened & when?

SOC / Admin



Responder typically builds out a timeline when investigation



So how can we get
the XDR to work
across all those all
those
attacks/TTPs?

We need Analytics & Correlation, not just Sightings

Obsrvbl Analytics Engine

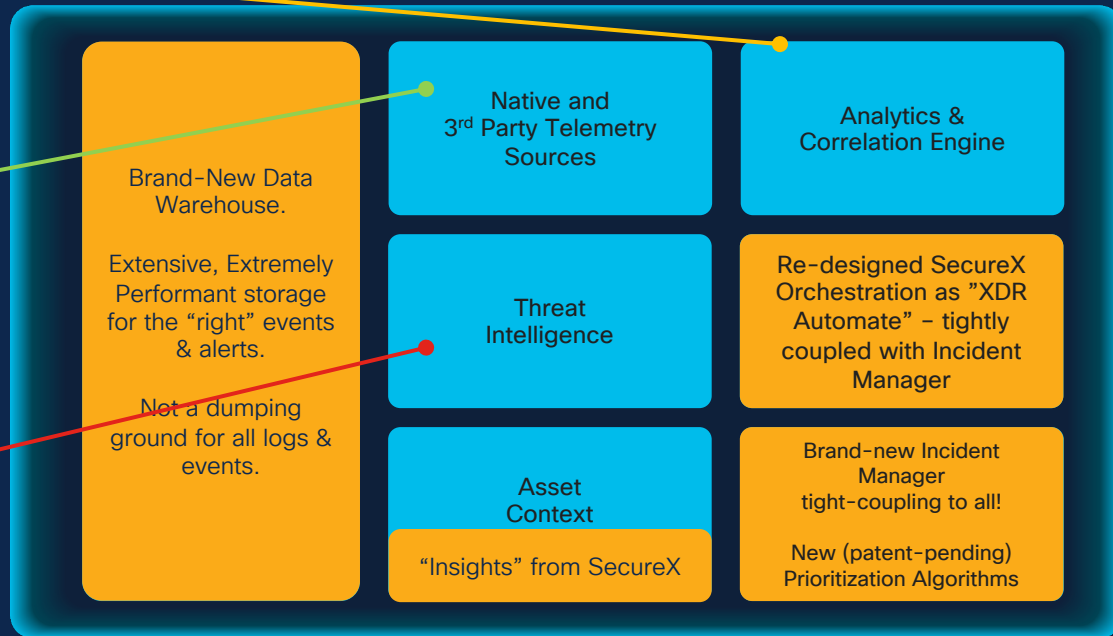
SCA's powerful analytics & correlation engine, to bring together much of the missing.

SecureX & SCA Integrations

Merged the integration frameworks from SecureX & Cloud Analytics – for a new & improved integration model.

External Enrichments

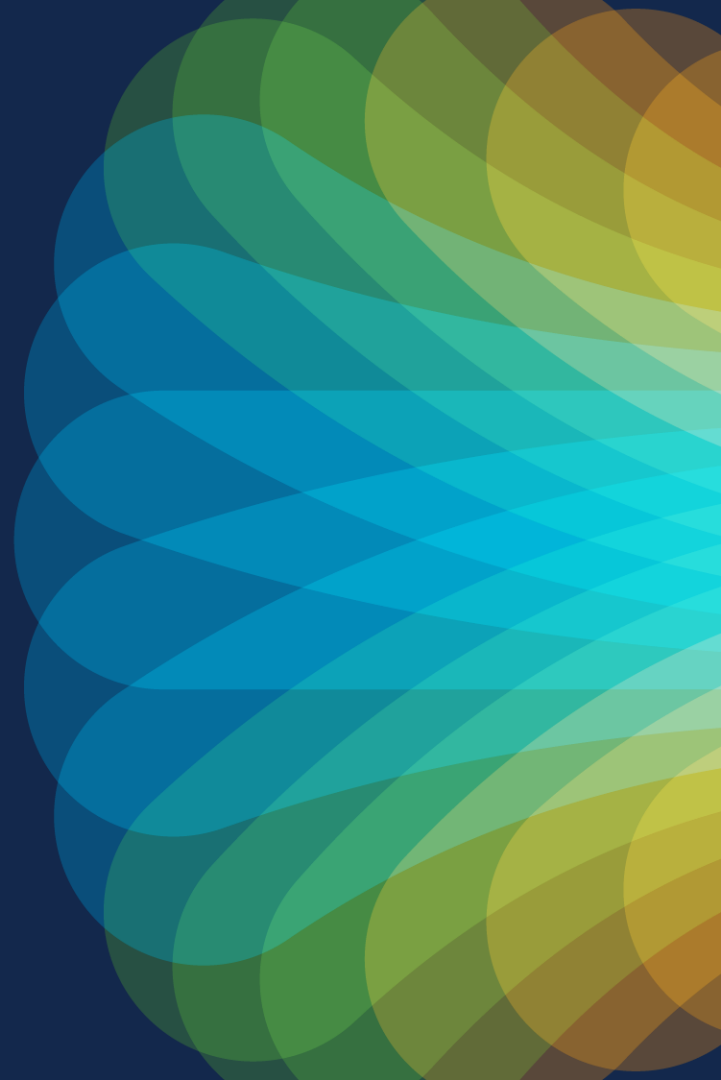
The enrichment protocols from SecureX, without requiring storage of all data in Data Repo (like SIEM would have to do).



Agenda

- A History Lesson
- Evolution
- Incident Management & Workflow
- Integrations & Response
- Key XDR Telemetry
- That's a wrap!

Incident Management & Workflow



Cisco XDR – Incident Manager

Prioritized Queue

Leverages (patent pending) advanced algorithm from Kenna Scientist based on Asset Value + Risk of the TTPs

Incident Summary

Progressive Disclosure of more details of the incident – Priority Details, Short / Long Descriptions, TTPs

The screenshot displays the Cisco XDR Incident Manager interface. On the left is a navigation sidebar with options: Control Center, Incidents (selected), Investigate, Intelligence, Automate, Devices, and Administration. The main area is titled 'Incidents' and shows a summary of 12 incidents, with 4 new and 5 open. Below this is a table of incidents, with the first three rows highlighted by a green box. The table has columns for checkboxes, Priority (all 1000), Name, and Source. The first row is 'in group Audit @ 20230514 03:19:...' from 'Secure Endpoint'. The second row is 'dc-1.org1.net in group Audit @ 20230514 03:14:52' from 'Secure Endpoint'. The third row is 'victim-win-6.org1.net in group Audit @ 20230514 03:13:...' from 'Secure Endpoint'. To the right of the table is a detailed view for the first incident, 'victim-win-2.org1.net in group Audit @ 20230514...'. This view shows the priority score breakdown (1000 total, 100 Detection Risk, 10 Asset Value at Risk), a short description, and a long description. The long description includes the incident title, promotion details, and indicators, such as 'ExecutedMalware.io: A known malicious file was executed. This increases the likelihood of a successful breach and this event should be promptly investigated.' A 'View Incident Detail' button is at the bottom right of the details panel.

	Priority	Name	Source
☐	1000	100 Detection Risk	in group Audit @ 20230514 03:19:...
☐	1000	10 Asset Value at Risk	dc-1.org1.net in group Audit @ 20230514 03:14:52
☐	1000		victim-win-6.org1.net in group Audit @ 20230514 03:13:...

Incident Details:

- Incident Title:** victim-win-2.org1.net
- Promoted at:** 2023-06-04 19:47:01 UTC
- Promotion method:** Automated
- Indicators:** ExecutedMalware.io: A known malicious file was executed. This increases the likelihood of a successful breach and this event should be promptly investigated.

Cisco XDR – Incident Manager / Overview

Overview

Diagram to summarize the incident. *Not* the detailed investigative diagram.

Assets / Observables & Indicators

Top active listed with total count called out at the top.

Incidents

1000 New **victim-win-2.org1.net in group Audit @ 20230514 03:19:59**

Reported by Secure Endpoint on 2023-05-14T03:19:59.000Z - 1 Linked Incident

Add short description... [View Long Description](#)

Overview Detection Response Worklog

Diagram:

- 75ed17bd4925000f...
- SHA-256 Hash
- Endpoint
- Endpoint Workstation
- powershell.exe
- IP Address

MITRE | ATT&CK View Details

- TA0043: Reconnaissance
- TA0042: Resource Development
- TA0001: Initial Access
- TA0002: Execution**
- TA0003: Persistence
- TA0004: Privilege Escalation
- TA0005: Defense Evasion
- TA0006: Credential Access**
- TA0007: Discovery
- TA0008: Lateral Movement
- TA0009: Collection
- TA0011: Command and Control
- TA0010: Exfiltration
- TA0040: Impact

8 Assets View all

TOP ACTIVE

- victim-win-2.org1.net 156 events
- victim-win-6.org1.net 131 events
- LOXX-WIN10VIC02 31 events
- dc-1 14 events
- SKTOP-V2IOAED 7 events

7 Observables View all

TOP ACTIVE

- http://169.254.169.254/meta... 100 events
- victim-win-6 20 events
- victim-win-2 18 events
- 9f914d42706fe215501044acd8... 7 events
- http://168.63.129.16/?comp=vers... 1 event

3 Indicators View all

TOP ACTIVE

- Secure Endpoint ExecutedMalware.ioc 6 events
- Falcon Detection Method Credential Access via OS Credential Dump... 1 event
- Cisco Secure Cloud Analytics (rsa) Internal Connection Watchlist Hit 1 event

Cisco XDR – Incident Manager / Overview

Overview

Diagram to summarize the incident. *Not* the detailed investigative diagram.

Assets / Observables & Indicators

Top active listed with total count called out at the top.

Incidents

1000 New **victim-win-2.org1.net in group Audit @ 20230514 03:19:59**

Reported by Secure Endpoint on 2023-05-14T03:19:59.000Z - 1 Linked Incident

Add short description... [View Long Description](#)

Overview Detection Response Worklog

Assets / Observables & Indicators

- 8 Assets** [View all](#)
 - TOP ACTIVE
 - victim-win-2.org1.net** 156 events
 - victim-win-6.org1.net** 131 events
 - LOXX-WIN10VIC02** 31 events
 - dc-1** 14 events
 - SKTOP-V2IOAED** 7 events
- 7 Observables** [View all](#)
 - TOP ACTIVE
 - http://169.254.169.254/meta...** 100 events
 - victim-win-6** 20 events
 - victim-win-2** 18 events
 - 9f914d42706fe215501044acd8...** 7 events
 - http://168.63.129.16/?comp=vers...** 1 event
- 3 Indicators** [View all](#)
 - TOP ACTIVE
 - Secure Endpoint ExecutedMalware.ioc** 6 events
 - Falcon Detection Method Credential Access via OS Credential Dump...** 1 event
 - Cisco Secure Cloud Analytics (rsa) Internal Connection Watchlist Hit** 1 event

MITRE | ATT&CK [View all Tactics](#)

Tactics

- TA0001: Initial Access** 48
 - The adversary is trying to get into your network. Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network. Techniques used to gain a foothold include targeted spearphishing and exploiting weaknesses on public-facing web servers. Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords.
- TA0003: Persistence** 42
- TA0004: Privilege Escalation** 55
- TA0005: Defense Evasion** 58
- TA0006: Credential Access** 40

Techniques

- T1078: Valid Accounts**

Cisco XDR – Incident Manager / Detection

Detection

Used to show the events that have been correlated into this incident

Types of Events

Original: the alert sent to XDR
Investigated: correlated events

The screenshot displays the Cisco XDR Incident Manager interface. At the top, the incident title is "victim-win-2.org1.net in group Audit @ 20230514 03:19:59". Below the title, there are tabs for "Overview", "Detection", "Response", and "Worklog". The "Detection" tab is currently selected. A table of events is shown, with columns for "First Seen", "Severity", "Source", "Indicators", "Observables", and "Assets". The events are listed in descending order of "First Seen" time. The "Severity" column shows "Critical" for all events. The "Source" column shows "CrowdStrike Falcon Detection". The "Indicators" column shows "Internal Connection Watchlist Hit". The "Observables" column shows "victim-win-2.org1.net". The "Assets" column shows "DESKTOP-V2IOAED" and "LOXX-WIN10VIC02". A green box highlights the "Detection" tab and the table of events. An orange box highlights the "Type", "Source", and "Severity" filters at the top of the table. A green arrow points from the "Detection" tab to the "Types of Events" section. An orange arrow points from the "Types of Events" section to the "Original: the alert sent to XDR" text.

First Seen	Severity	Source	Indicators	Observables	Assets
2023-05-10T04:12:00.000Z	Critical	CrowdStrike Falcon Detection		9f914d42706fe215501044acd8...	DESKTOP-V2IOAED
2023-05-14T19:00:00.000Z	Critical	Cisco Secure Cloud Analytic...	Internal Connection Watchlist Hit		
2023-05-16T16:55:27.000Z	Critical	CrowdStrike Falcon Detection		victim-win-2.org1.net	LOXX-WIN10VIC02
2023-05-16T16:55:47.000Z	Critical	CrowdStrike Falcon Detection		victim-win-2.org1.net	LOXX-WIN10VIC02
2023-05-16T16:58:29.000Z	Critical	CrowdStrike Falcon Detection		victim-win-2.org1.net	LOXX-WIN10VIC02
2023-05-16T17:15:26.000Z	Critical	CrowdStrike Falcon Detection		victim-win-2.org1.net	LOXX-WIN10VIC02
2023-05-16T17:20:05.000Z	Critical	CrowdStrike Falcon Detection		victim-win-2.org1.net	LOXX-WIN10VIC02
2023-05-16T17:39:00.000Z	Critical	CrowdStrike Falcon Detection		victim-win-2.org1.net	LOXX-WIN10VIC02
2023-05-19T14:16:19.000Z	Critical	CrowdStrike Falcon Detection		victim-win-2.org1.net	dc-1
2023-05-19T14:17:16.000Z	Critical	CrowdStrike Falcon Detection		victim-win-2.org1.net	dc-1

Cisco XDR – Incident Manager / Detection

Detection

Used to show the events that have been correlated into this incident

Types of Events

Original: the alert sent to XDR
Investigated: correlated events

The screenshot displays the Cisco XDR Incident Manager interface. At the top, the incident title is "victim-win-2.org1.net in group Audit @ 20230514 03:19:59". Below the title, there are tabs for "Overview", "Detection", "Response", and "Worklog". The "Detection" tab is selected, showing a list of events. A green box highlights the "Original" filter button, and an orange box highlights the "Source" and "Severity" filter buttons. The table below shows a list of events with columns for "First Seen", "Severity", "Source", "Indicators", "Observables", and "Assets".

First Seen	Severity	Source	Indicators	Observables	Assets
2023-06-04T19:46:53.00...	High	Secure Endpoint	Executed/Malware.loc	9f914d42706fe215501044acd8...	victim-win-2.org1.net
2023-06-04T23:49:09.00...	High	Secure Endpoint	Executed/Malware.loc	9f914d42706fe215501044acd8...	victim-win-2.org1.net
2023-06-05T03:51:27.000Z	High	Secure Endpoint	Executed/Malware.loc	9f914d42706fe215501044acd8...	victim-win-2.org1.net
2023-06-05T07:53:45.00...	High	Secure Endpoint	Executed/Malware.loc	9f914d42706fe215501044acd8...	victim-win-2.org1.net
2023-06-05T11:56:17.000Z	High	Secure Endpoint	Executed/Malware.loc	9f914d42706fe215501044acd8...	victim-win-2.org1.net
2023-06-05T15:56:32.000Z	High	Secure Endpoint	Executed/Malware.loc	add683ae910abbbf0e28b557fa...	victim-win-2.org1.net
2023-06-05T03:04:56.00...	Low	Secure Endpoint		b094e827af70241d71bed9767e...	victim-win-2.org1.net

Cisco XDR – Incident Manager / Detection

Detection

Used to show the events that have been correlated into this incident

Types of Events

Original: the alert sent to XDR

Investigated: correlated events

The screenshot displays the Cisco XDR Incident Manager interface. At the top, the incident title is "victim-win-2.org1.net in group Audit @ 20230514 03:19:59". Below the title, there are tabs for "Overview", "Detection", "Response", and "Worklog". The "Detection" tab is selected, showing a list of events. A green box highlights the "Investigated" filter button, and an orange box highlights the "Severity" filter button. The table below shows a list of events with columns for "First Seen", "Severity", "Source", "Indicators", "Observables", and "Assets".

First Seen	Severity	Source	Indicators	Observables	Assets
2023-05-10T04:12:00.000Z	Critical	CrowdStrike Falcon Detection		9f914d42706fe215501044acd8...	DESKTOP-V2IOAED
2023-05-14T19:00:00.000Z	Critical	Cisco Secure Cloud Analytic...	Internal Connection Watchlist Hit		
2023-05-16T16:55:27.000Z	Critical	CrowdStrike Falcon Detection		victim-win-2.org1.net	LOXX-WIN10VIC02
2023-05-16T16:55:47.000Z	Critical	CrowdStrike Falcon Detection		victim-win-2.org1.net	LOXX-WIN10VIC02
2023-05-16T16:58:29.000Z	Critical	CrowdStrike Falcon Detection		victim-win-2.org1.net	LOXX-WIN10VIC02
2023-05-16T17:15:26.000Z	Critical	CrowdStrike Falcon Detection		victim-win-2.org1.net	LOXX-WIN10VIC02
2023-05-16T17:20:05.000Z	Critical	CrowdStrike Falcon Detection		victim-win-2.org1.net	LOXX-WIN10VIC02
2023-05-16T17:39:00.000Z	Critical	CrowdStrike Falcon Detection		victim-win-2.org1.net	LOXX-WIN10VIC02
2023-05-19T14:16:19.000Z	Critical	CrowdStrike Falcon Detection		victim-win-2.org1.net	dc-1
2023-05-19T14:17:16.000Z	Critical	CrowdStrike Falcon Detection		victim-win-2.org1.net	dc-1

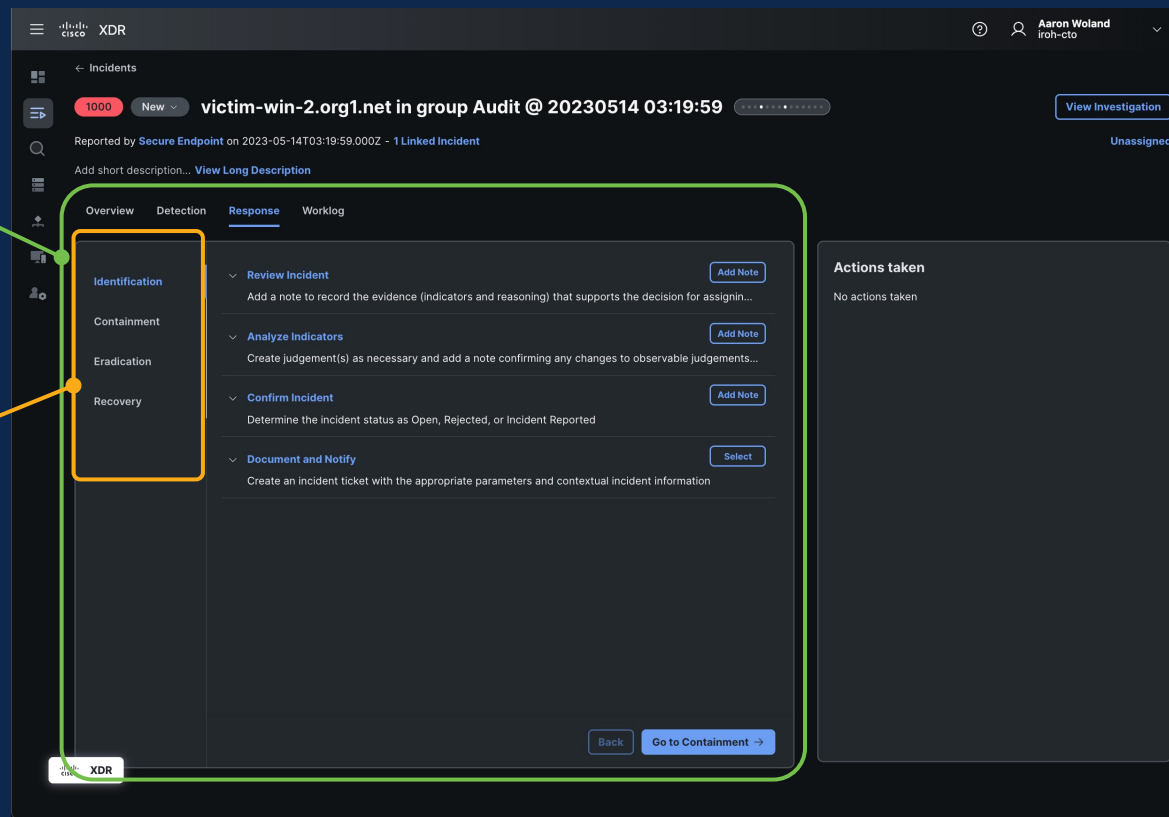
Cisco XDR – Incident Manager / Response

Responses

Content specific for the TTPs in the incident

Step Through

Identification ->
Containment ->
Eradication ->
Recovery



Cisco XDR – Incident Manager / Response

Responses

Content specific for the TTPs in the incident

Step Through

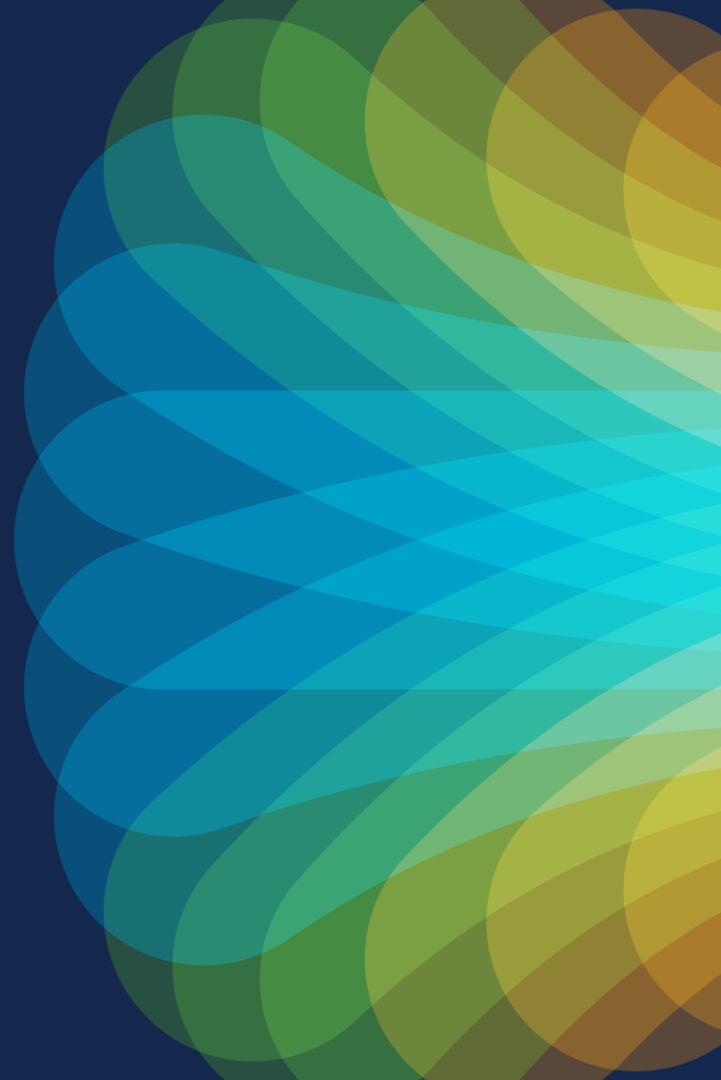
Identification ->
Containment ->
Eradication ->
Recovery

The screenshot displays the Cisco XDR Incident Manager interface. The top navigation bar shows the 'Incidents' section with a count of 1000 and a 'New' button. The incident title is 'victim-win-2.org1.net in group Audit @ 20230514 03:19:59'. The 'Response' tab is selected, showing a list of response actions. The 'Contain Incident: Assets' section is highlighted with a red box, and the 'Select' button is also highlighted. A green box outlines the 'Response' tab and the 'Identify Affected Hosts' section. A red callout box on the right contains the text: 'Doesn't ask "which EDR" to isolate with - does it all for you'. The top right shows the user 'Aaron Woland' and the bottom right has an 'Execute' button.

Agenda

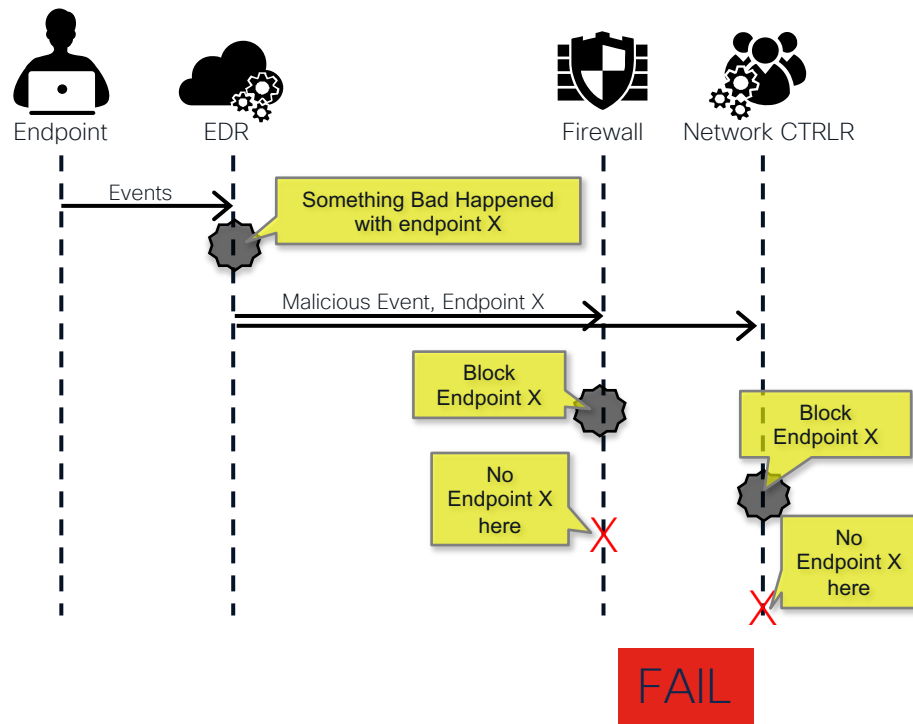
- A History Lesson
- Evolution
- Incident Management & Workflow
- Integrations & Response
- Key XDR Telemetry
- That's a wrap!

Integrations & Response



State of Industry: *no common identities*

- You see this with SIEM & SOAR
- Each product views endpoint in its own way.
 - GUID (specific to product)
 - IP Address (ephemeral & changes all the time)
 - Mac Address (ephemeral, private, unavailable, duplicative)
- Making the products work together is a challenge

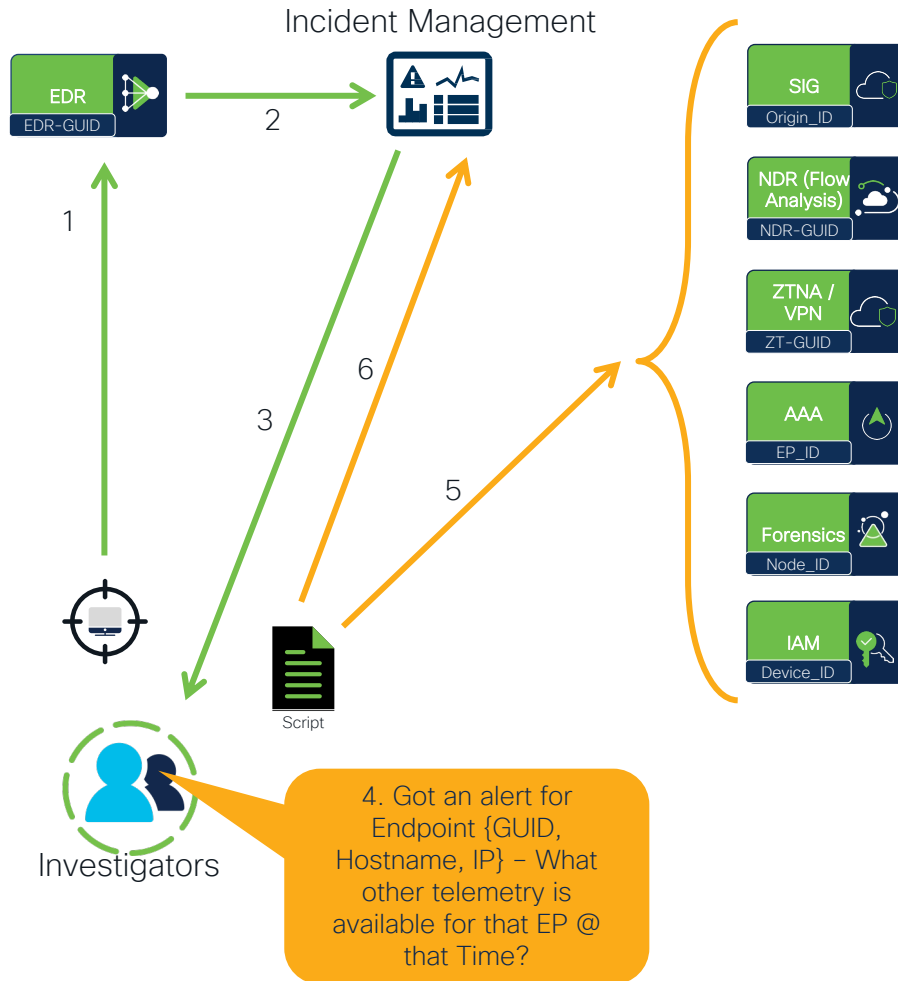


We need a common endpoint “object”

SOC Investigation Flow

Note: this is a Generic Example:

1. EDR detects malicious activity
2. Alerts fired off to an incident management system
3. Investigators are notified of new incident
4. Investigator takes endpoint details from EDR & runs script
5. Script retrieves all IDs from the other sources of telemetry (none are the same)
6. Script updates the Incident Manager with new Observables to enrich investigation with

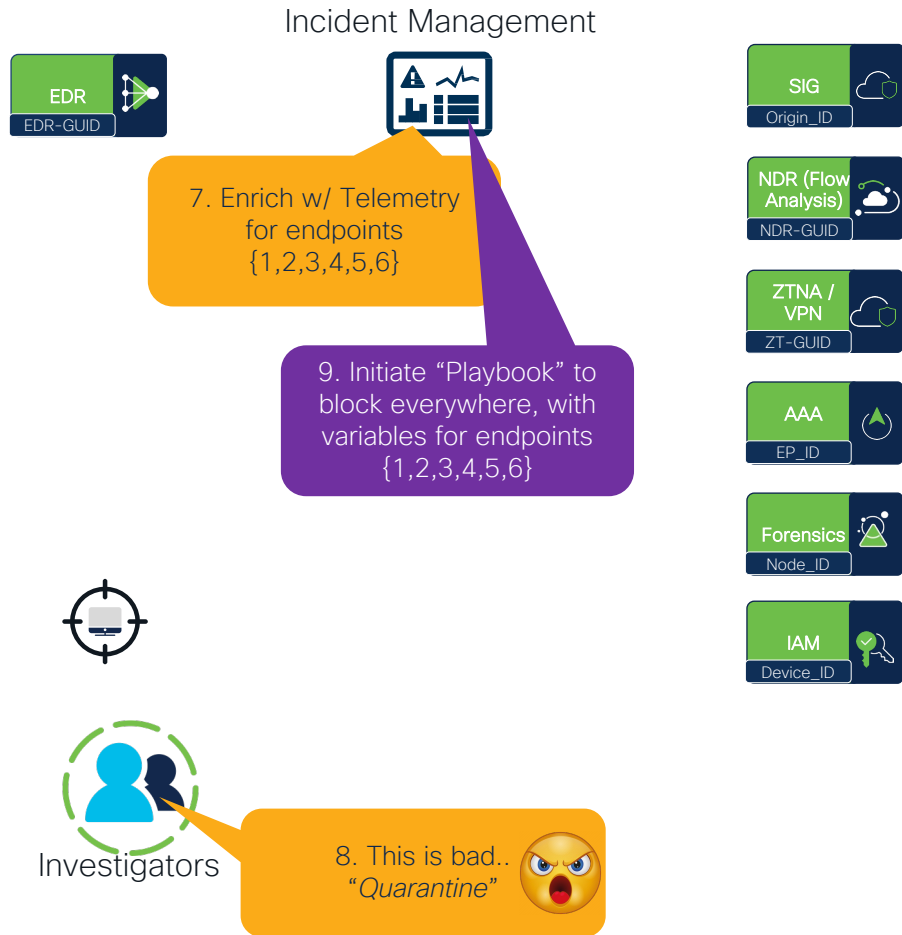


SOC Investigation Flow

Note: this is a Generic Example:

7. Incident Manager churns through new telemetry from sources, for their endpoint identifiers
8. Investigator realizes this is bad & initiates the “*all powerful*” *Quarantine option*
9. Incident Management Tool(s) initiate the playbook to respond in all enforcement points

**Someone needed to build these flows

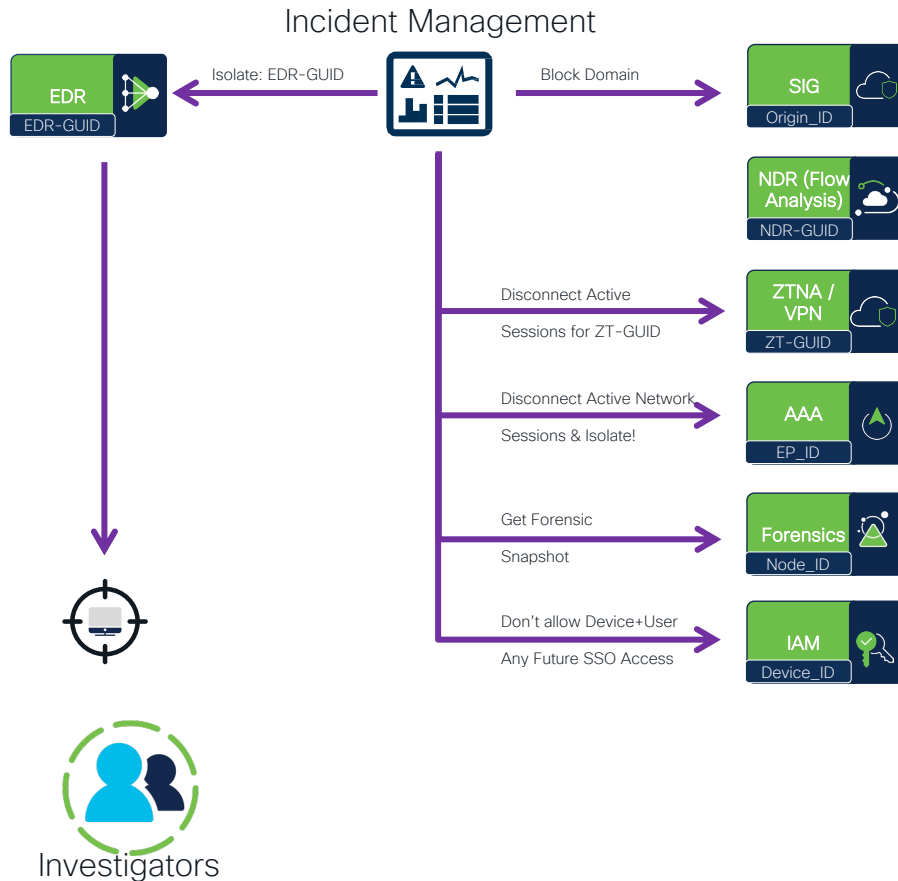


SOC Investigation Flow

Note: this is a Generic Example:

- Playbook initiates isolation via EDR, using the EDR-GUID
- Playbook blocks domain at SIG
- Playbook disconnects Active Sessions for ZTNA/VPN & AAA sessions
- Playbook isolates the endpoint when new AAA session begins
- Playbook initiates a new forensic snapshot of the infected host
- Playbook informs IAM solution to deny any future attempts w/ User+Device combination

**Someone needed to build these flows



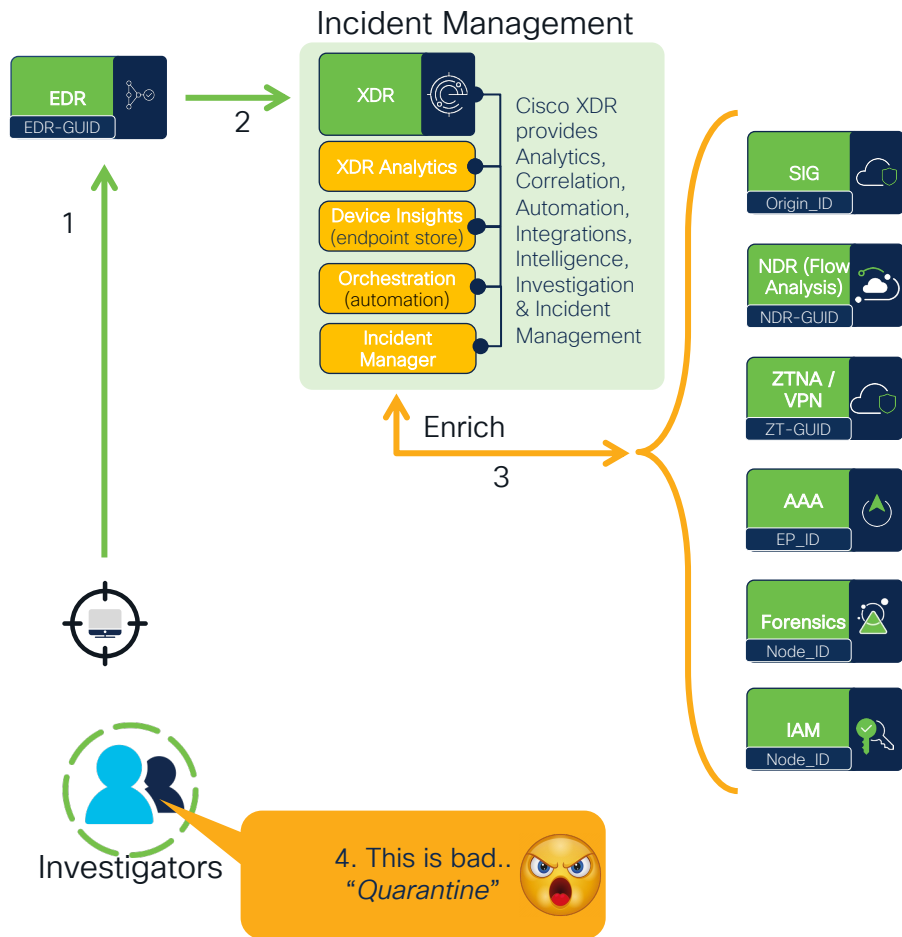
SOC Investigation Flow

With Cisco XDR:

1. EDR detects malicious activity
2. Alert sent to Cisco XDR
3. Alert prioritized in XDR Analytics.

Device Insights has all unique IDs from the *Integrated Security Products*
4. Alert prioritized in XDR Analytics.

Incident enriched from each integrated security product & intelligence source
5. Investigator can see it all & take action
6. Response leverages the correct ID for each source



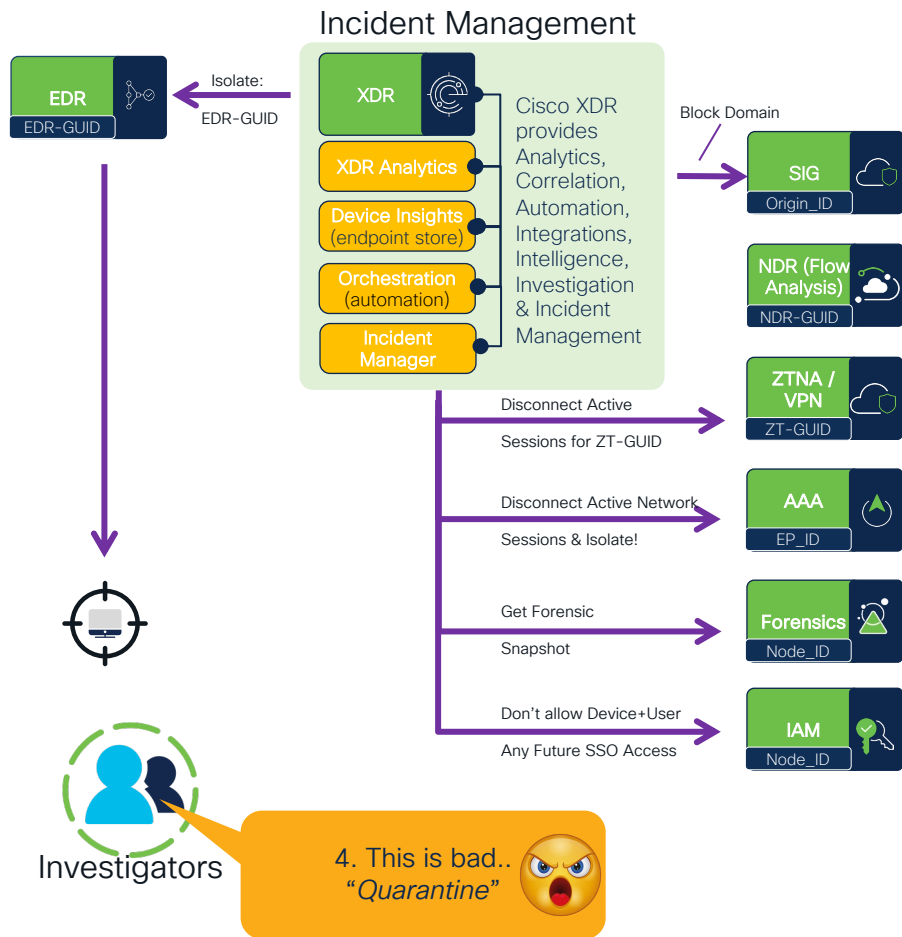
SOC Investigation Flow

With Cisco XDR:

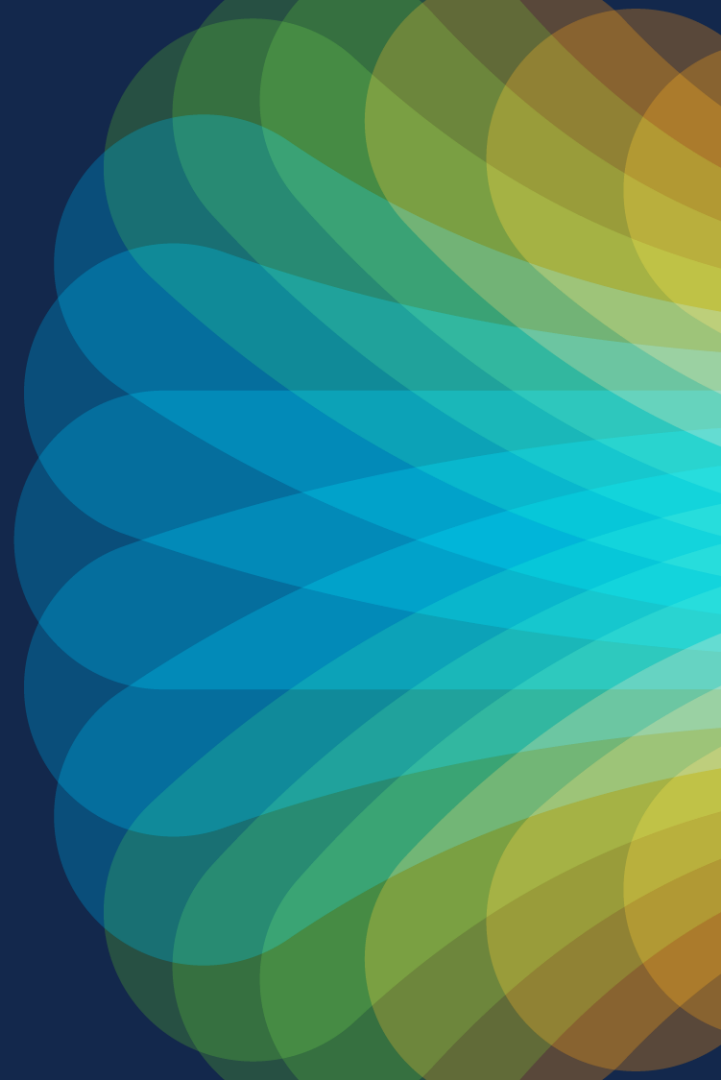
1. EDR detects malicious activity
2. Alert sent to Cisco XDR
3. Alert prioritized in XDR Analytics.

Device Insights has all unique IDs from the *Integrated Security Products*
4. Incident enriched from each integrated security product & intelligence source

Investigator can see it all & take action
5. Response leverages the correct ID for each source



Let's talk about
that
prioritization,
shall we?



Incident Priority

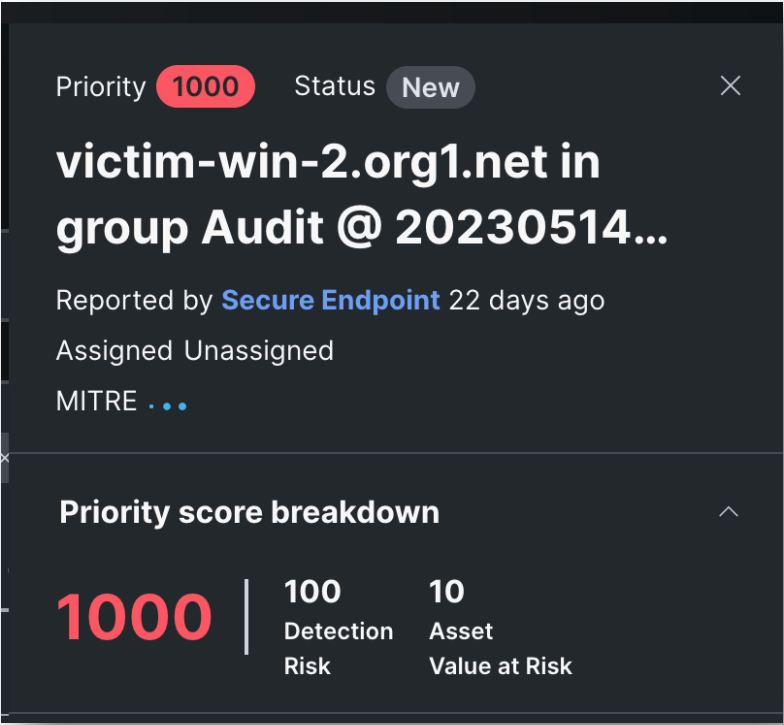
- At its core: It's the combo of:

Detection Risk

+

Asset Value

- Where does that value come from?



Priority **1000** Status **New** ×

victim-win-2.org1.net in group Audit @ 20230514...

Reported by **Secure Endpoint** 22 days ago

Assigned Unassigned

MITRE ...

Priority score breakdown ^

1000	100 Detection Risk	10 Asset Value at Risk
-------------	------------------------------	----------------------------------

Device Insights in XDR adds some new things

Labels

Describe/group devices – manual and programmatically

Device Value

Value of 1-10.

1 = least valuable

10 = most valuable

Device Name	OS	OS Version	OS Support	Users Seen	Sources	Labels	Value
☒ AAWOLAND-M-21PK	macOS	13.4		loxx, loxx@securitydemo.net	SBG SM Duo SecureX Secure Endpoint - Cisco - aawoland Orbital	Critical Server Vulnerable	10 ^M
☐ ats-centos04	Ubuntu	#39-Ubuntu SMP PREEMPT_DYNAMIC Fri Mar 17 17:33:16 UTC 2023		loxx, reboot, runlevel, LOGIN	Secure Endpoint - Cisco - aawoland Orbital	Critical Server Vulnerable	10 ^M
☐ ats-centos7-02.securitydemo.net	Centos	linux release 7.6		reboot, runlevel, LOGIN	Secure Endpoint - Cisco - aawoland Orbital		10 ^D
☒ ats-centos7-03.securitydemo.net	Centos	linux release 7.6		loxx, reboot, runlevel, LOGIN	Secure Endpoint - Cisco - aawoland Orbital	Critical Server	10 ^M
☐ ATS-MemberSrvr.securitydemo.net	Windows	Server 2016 Standard			Secure Endpoint - Cisco - aawoland Orbital		10 ^D

Device Insights in XDR adds some new things

Update in Bulk

Can update the labels and values of all selected assets in bulk, from inventory screen.

Create in-line

Can even create and apply new labels in-line

The screenshot shows the XDR interface with a table of 30 devices. A modal titled 'Edit Labels' is open, showing a list of labels to be applied to the selected devices. The modal includes a search bar, a list of labels, and buttons to 'Remove' or 'Add' labels.

Device Name	OS	OS Version	Sources
AIQ-CROWDSTRIKE	Unknown	Windows 10	CrowdStrike
ANYCNCT-WIN10-C	Unknown	Windows 10	CrowdStrike
ANYCNCT-WIN11-C	Unknown	Windows 11	CrowdStrike
AnyConnect-linux-1	Unknown	Ubuntu 18.04	CrowdStrike
AnyConnect-linux-2	Unknown	Ubuntu 20.04	CrowdStrike
AnyConnect-linux-3	Unknown	Ubuntu 22.04	CrowdStrike
BLUECKW19	Unknown	Windows Server 2019	CrowdStrike
C1-3850-2-G1-3-	Unknown	Windows 10	CrowdStrike
CROWDSTRIKE-WIN	Unknown	Windows 10	CrowdStrike
dc-1	Unknown	Windows Server 2019	CrowdStrike
dc-1	Unknown	Windows Server 2019	CrowdStrike

Edit Labels Modal:

- Search: Boo CrowdStrike
- Labels: Retired, External Facing, Critical, RTP Data Center
- Buttons: Remove, Add

Device Insights in XDR adds some new things

Default Value

The default value is 10 (most valuable)

Manually Assigned

The value is tagged if its manually assigned, which will always “win” in a conflict

The screenshot displays the Cisco XDR Device Insights interface. It features a table with columns for device status (e.g., 'Compromised'), labels (e.g., 'Boo Crowdstrike'), and a 'Value' column. A dropdown menu is open for the 'Value' column, showing a scale from 1 to 10. A red box highlights the '10 (Critical)' option, and a blue box highlights the 'Manually assigned' tag on a device. The interface also includes buttons for 'Export to CSV', 'Edit Columns', and 'Update Value'.

Status	Labels	Value
Compromised	Boo Crowdstrike	10
Compromised	Boo Crowdstrike	10
Compromised	Boo Crowdstrike	10
Compromised	Boo Crowdstrike	10
Compromised	Boo Crowdstrike	10
Compromised	Boo Crowdstrike	10
Compromised	Boo Crowdstrike	10
Compromised	Boo Crowdstrike	10
Compromised	Boo Crowdstrike	10
Compromised	Boo Crowdstrike	10

Value Scale:

- 1 (Not Critical)
- 2
- 3 (Less Critical)
- 4
- 5
- 6 (Somewhat Critic)
- 7
- 8
- 9
- 10 (Critical)

Update Value

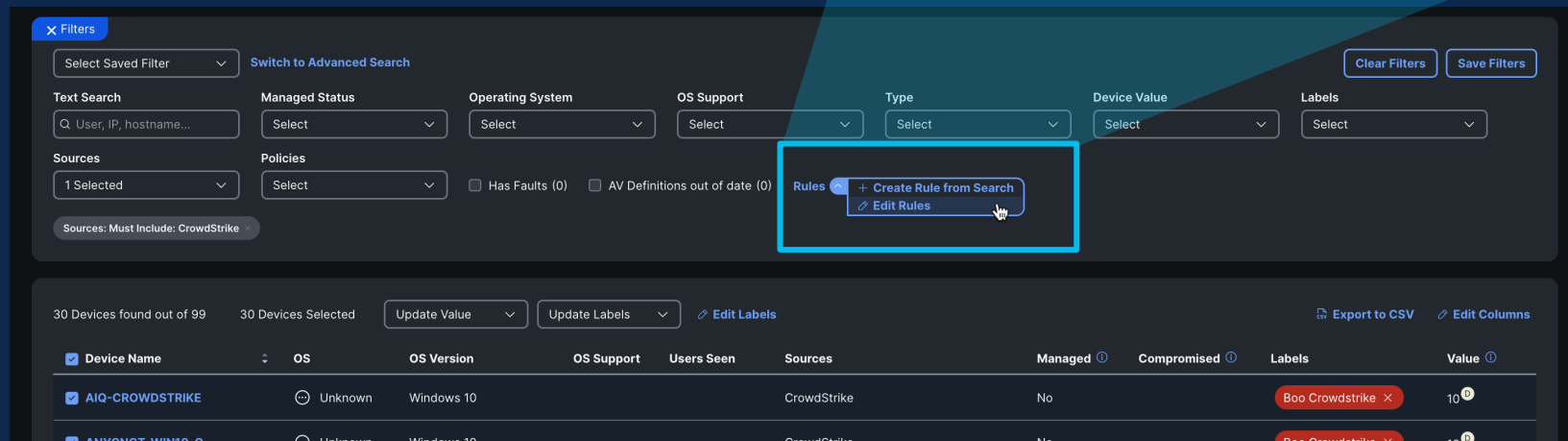
Update

Device Insights in XDR adds some new things

Rules Engine

Based on Insights
“Search”. Apply
values / labels when
rules are met.

Rules  + Create Rule from Search
 Edit Rules



The screenshot displays the XDR Rules Engine interface. At the top, there's a search bar with the text "Q User, IP, hostname...". Below the search bar, there are several filter sections: "Managed Status", "Operating System", "OS Support", "Type", "Device Value", and "Labels". Each section has a "Select" dropdown menu. There are also checkboxes for "Has Faults (0)" and "AV Definitions out of date (0)". A "Sources" section shows "1 Selected" and a "Sources: Must Include: CrowdStrike" filter. A "Rules" dropdown menu is highlighted with a red box, showing options to "+ Create Rule from Search" and "Edit Rules". Below the filters, there's a table of devices. The table has columns for "Device Name", "OS", "OS Version", "OS Support", "Users Seen", "Sources", "Managed", "Compromised", "Labels", and "Value". The first row shows a device named "AIQ-CROWDSTRIKE" with OS "Unknown", OS Version "Windows 10", OS Support "CrowdStrike", Users Seen "No", Sources "CrowdStrike", Managed "No", Compromised "No", Labels "Boo CrowdStrike", and Value "10".

Device Insights in XDR adds some new things

Rules Engine

Based on Insights “Search”. Apply values / labels when rules are met.

May enable / disable rules

May change or delete them

Can use existing searches or create a new search in the rule editor.

The screenshot displays the Cisco XDR Rules Engine interface. A modal window titled "Rules" is open, showing the configuration for a new rule. The modal is divided into several sections:

- Details:** Includes a "Name" field (with a blue border) and a "Description" field.
- Rule Criteria:** Contains three columns of criteria:
 - Text Search:** A search bar with the placeholder "User, IP, hostname...".
 - Managed Status:** A dropdown menu with "Select" as the current value.
 - Operating System:** A dropdown menu with "Select" as the current value.
 - OS Support:** A dropdown menu with "Select" as the current value.
 - Type:** A dropdown menu with "Select" as the current value.
 - Device Value:** A dropdown menu with "Select" as the current value.
 - Labels:** A dropdown menu with "Select" as the current value.
 - Sources:** A dropdown menu with "1 Selected" as the current value.
 - Policies:** A dropdown menu with "Select" as the current value.
- Automated Assignment:** Includes two checkboxes: "Has Faults (0)" and "AV Definitions out of date (0)".
- Assign Labels:** A dropdown menu with "Select Labels" as the current value.
- Assign Device Value:** A dropdown menu with "Select Value" as the current value.

At the bottom of the modal, there are "Cancel" and "Create" buttons. Below the modal, a table lists existing rules:

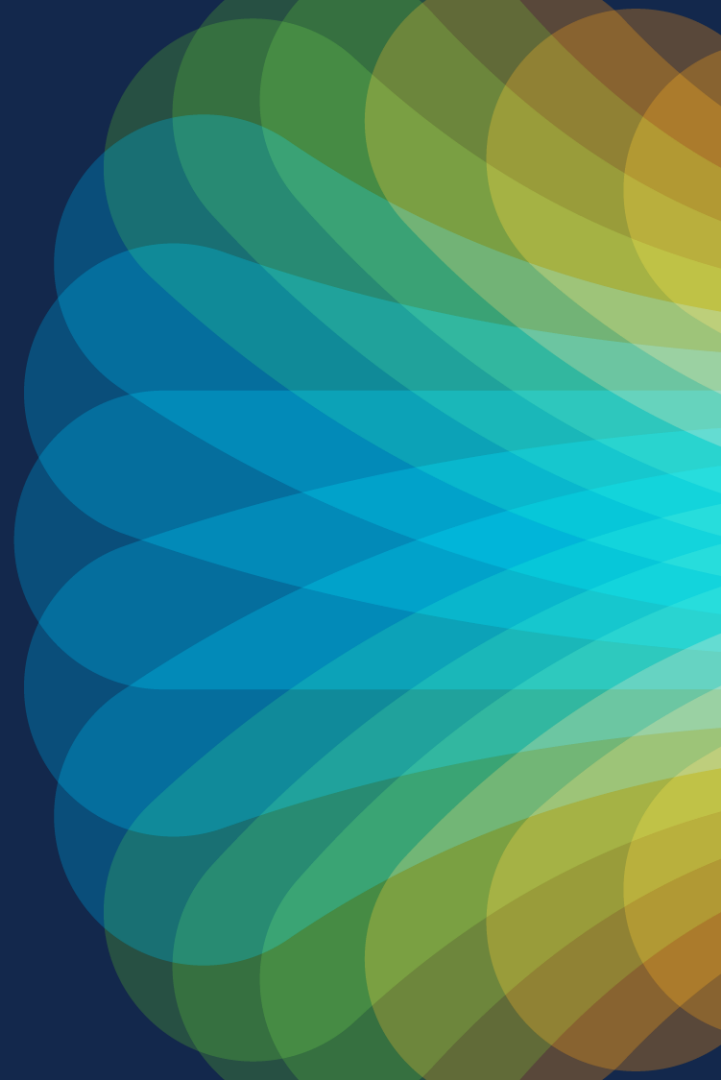
Details	Rule Criteria	Automated Assignment
☒ Loxx-Unmanaged (7 devices affected)	Managed Status: Unmanaged Text Search: "loxx"	Value: 8 Labels: ● Critical ● Server
☒ LoxxRule (5 devices affected)	Text Search: "Loxx"	Labels: ● Loxx

The background shows a table of device insights with columns for "Sources" and "Managed Status".

Agenda

- A History Lesson
- Evolution
- Incident Management & Workflow
- Integrations & Response
- Key XDR Telemetry
- That's a wrap!

Telemetry, Telemetry & more Telemetry



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

Also 3rd Parties

- EDR:



- Crowstrike



- Sentinel One



- MSFT Defender

- NDR:

- Dark Trace



- ExtraHop



CISCO *Live!*



“I think NVM is Cisco’s best kept secret weapon”

-Tom Gillis, SVP & GM – Cisco Secure





For years, we've been preaching:



*is
more
than*



AnyConnect has been rebranded



AnyConnect

+



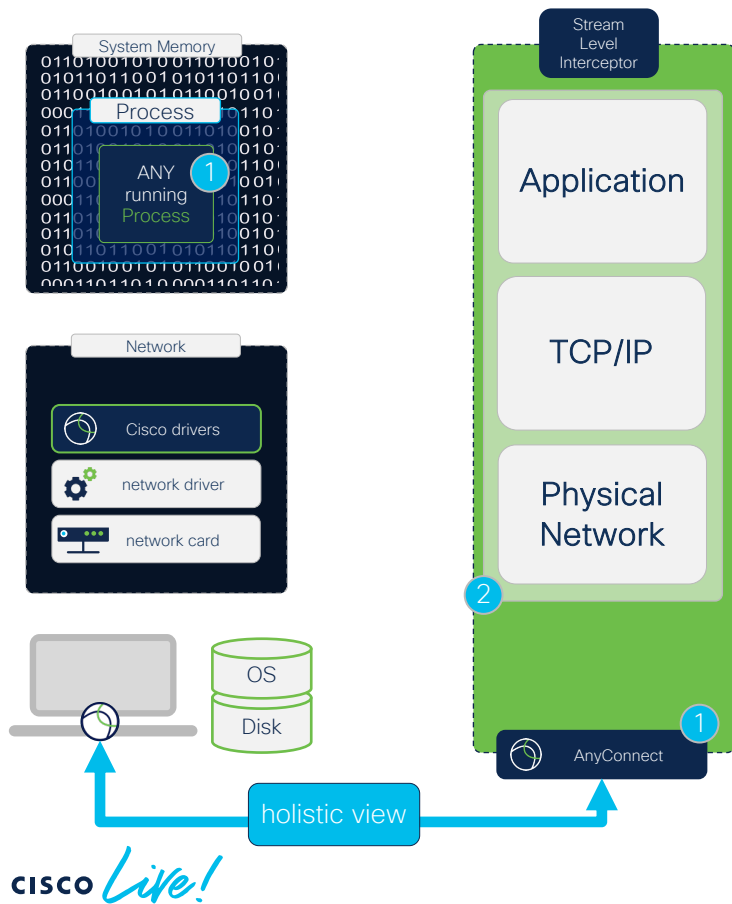
Cisco Secure
Endpoint (AMP)

=



Cisco Secure
Client

Stream Level Interceptor

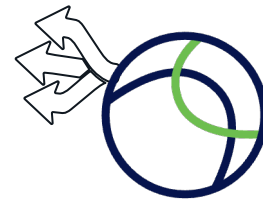


- ▶ The **Stream Level Interceptor** included in Secure Client (AnyConnect) enables a full holistic, pre-encrypted view on the endpoint network activity
- ▶ This core function from Cisco Secure Client makes the solution so powerful
- ▶ It enables other modules like the Umbrella Module or/and NVM to work
- ▶ This holistic view examines & manipulates information for any network communication
 - ▶ from the running application
 - ▶ to the physical network layer

Why does this
matter to the
SOC, or for the
Cisco XDR?

“Network Telemetry is Critical to a Defensible Network. It’s too bad that we cannot get NetFlow from the Endpoint”

– SANS Instructor
SEC530: Defensible Network Architectures

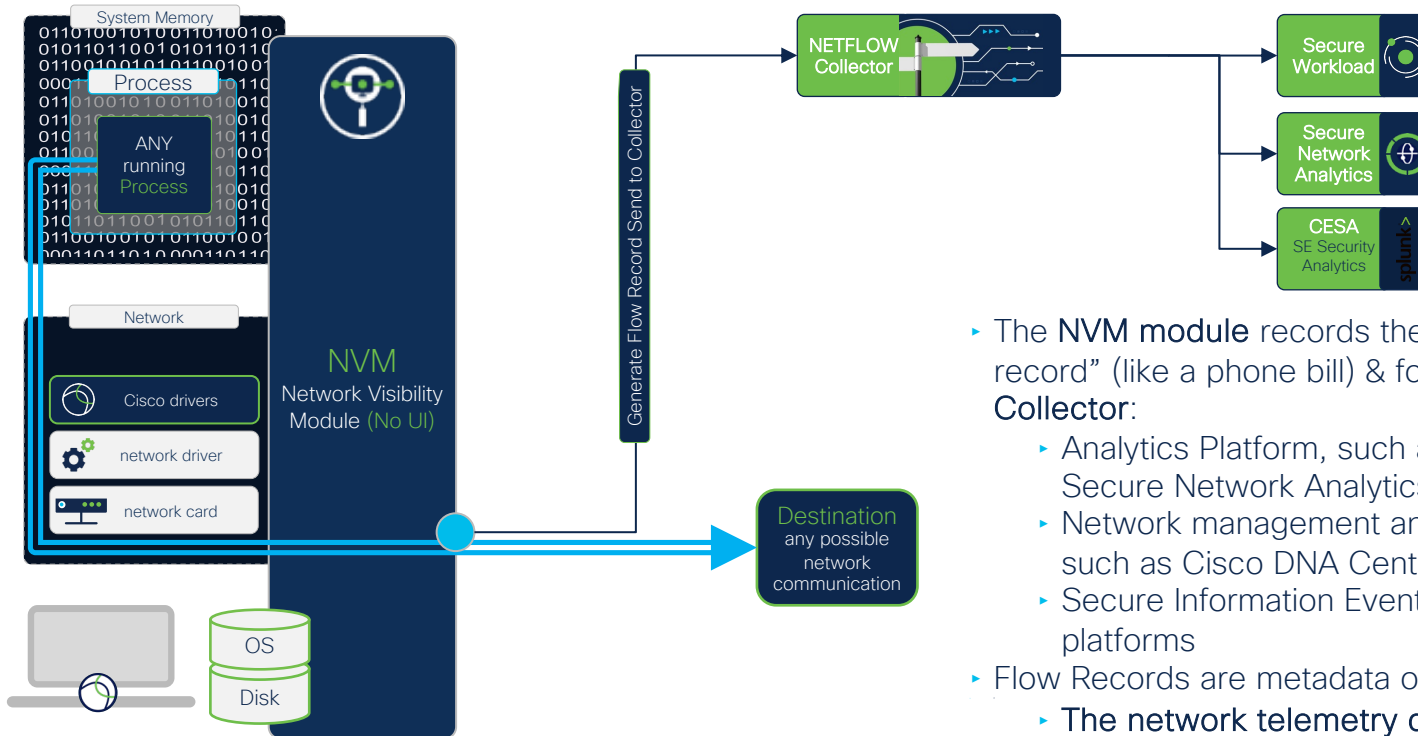


Network Visibility Module (NVM)

- Creates a flow record of every network connection from endpoint
 - User, Process, Machine Info, etc.
 - Works On and Off Prem
 - Sends Data in IPFIX (NetFlow) based “nvzFlow”.



Network Visibility Module



- ▶ The **NVM module** records the traffic into a “flow record” (like a phone bill) & forwards it to a **Netflow Collector**:
 - ▶ Analytics Platform, such as Secure Workload, Secure Network Analytics or others
 - ▶ Network management and automation platforms, such as Cisco DNA Center
 - ▶ Secure Information Event Management (SIEM) platforms
- ▶ Flow Records are metadata only:
 - ▶ The network telemetry does not include any payload!

Network + Endpoint Visibility Together



Netflow/IPFIX

Source IP
Destination IP
Source Port
Destination Port
Bytes Sent
Bytes Received

Source IP
Destination IP
Source Port
Destination Port
Bytes Sent
Bytes Received

NVM (IPFIX Formatted)

*True device attribution,
Not just "IP Address"*



OS Version
OS Edition
UDID
Host Name
Logged In User
Process Name
Process Hash
Process Account
Parent Process Name
Parent Process Hash
Parent Process Account
DNS/Destination Hostname
Module Hash List
System Manufacturer
System Type
MAC Address
Interface Name / Type / UID

Deep Endpoint
Visibility

User
Traffic Stats
Processes
Applications
SaaS Used
Accounts
Destinations
Machine Details

Sure, this is cool – but
why should you care?

*“NVM says: not just this IP is talking to this IP on these ports[...] It actually has **this application is opening this connection**”*

-Michael Scheck, Director Cisco CSIRT

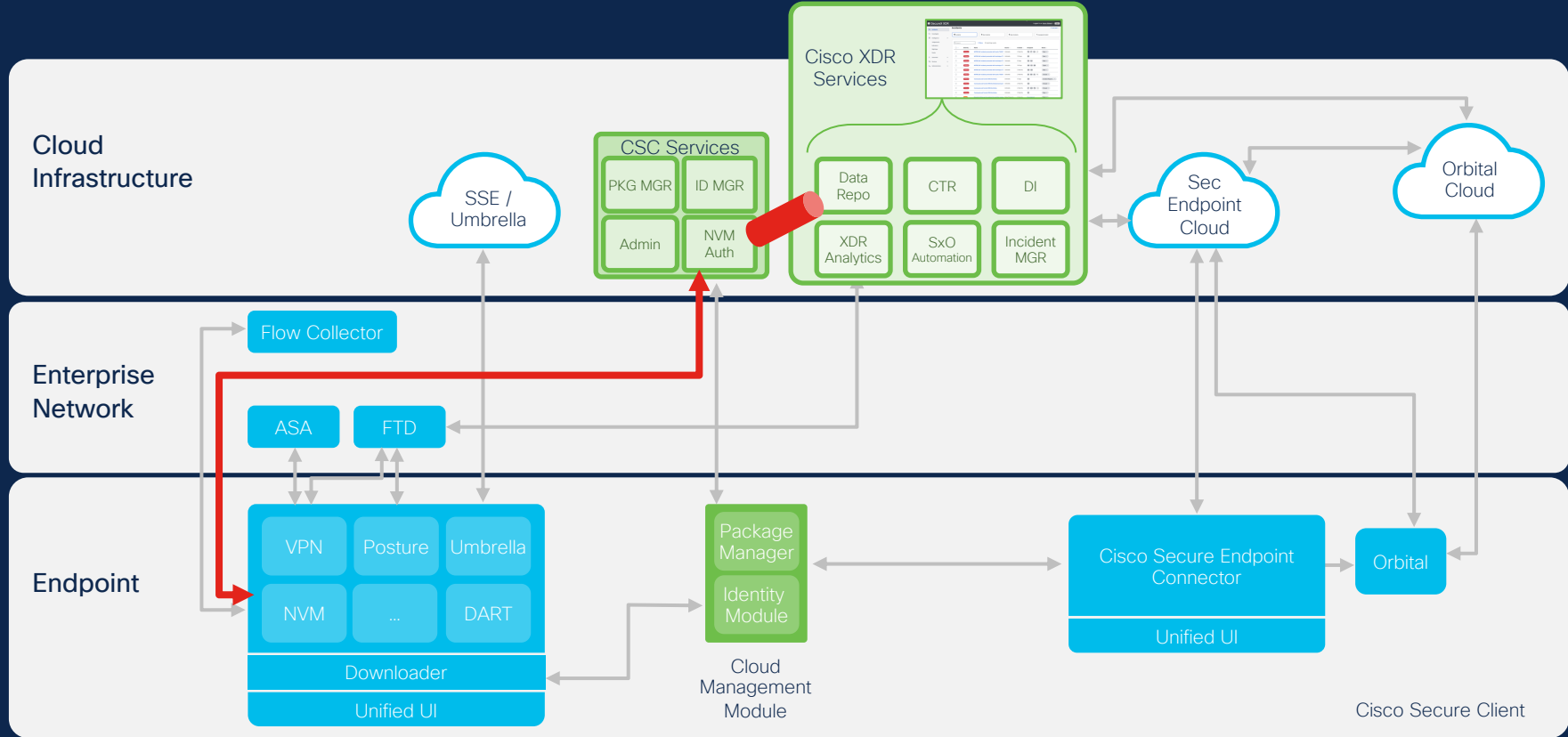
CISCO *Live!*



NVM is now a key component of the Cisco XDR

- Default CSC Deployment
 - Default CM Profile
 - Default NVM Profile – set to the XDR
- NVM sends direct to cloud
 - Requires Cloud Managed CSC
 - Provides ID & Secure transport
 - Can be cloud or onPrem, not both (today)

Cisco Secure Client / XDR – Architecture



NVM Event Viewer in XDR Analytics

New NVM Flows Tab

INSTANT FILTERS

Search activity per attribute or many with advanced search.

Telemetry Details

See the detailed telemetry collected from the flow

The screenshot displays the NVM Event Viewer interface. At the top, there are tabs for Session Traffic, Session Details, Rejected Traffic, Cloud Posture, AWS CloudTrail, Passive DNS, and NVM Flow (which is highlighted). A search bar and filter controls are visible. Below the tabs, a table lists network flows with columns for flow_end_time_sec, source_ip_address, destination_ip_address, Source_Port, Destination_Port, protocol_id, bytes_in, bytes_out, process_name, process_hash, and process_id. A detailed telemetry view is shown for a selected flow, displaying various attributes such as bytes_in, destination_ip_address, flow_stage, logged_in_user, parent_process_hash, process_account, process_id, source_ip_address, and process_name.

flow_end_time_sec	source_ip_address	destination_ip_address	Source_Port	Destination_Port	protocol_id	bytes_in	bytes_out	process_name	process_hash	process_id
2023-05-23 14:10:59 UTC	10.1.82.156	208.67.222.222	60104	443 (https)	UDP	473	196	dnscryptproxy.exe	a5a0e48042a7bd1f11a671dbc6834179119a542df06dd0a644e...	1,392

Telemetry Details:

- bytes_in: 473
- destination_ip_address: 208.67.222.222
- flow_stage: 0
- logged_in_user: <none>
- parent_process_hash: 72e43f0f42772e5a7186e0af3d07d76e1569d4656f5c906d4324523db864fc8e
- process_account: NT AUTHORITY\SYSTEM
- process_id: 1392
- source_ip_address: 10.1.82.156
- ADDITIONAL_LOGGED_IN_USERS_LIST: []
- account_type: 32770
- loggedin_user: ORG26\Administrator
- session_type: 1
- bytes_out: 196
- destination_port: 443
- flow_start_time_sec: 2023-05-23T14:10:59+00:00
- logged_in_user_type: None
- parent_process_id: 4544
- process_account_type: 8194
- process_name: dnscryptproxy.exe
- source_port: 60104
- cc_arrival_time_sec: 2023-05-23T14:11:59+00:00
- dns_suffix: org26.net
- initiator: 1
- parent_process_account: NT AUTHORITY\SYSTEM
- parent_process_name: acumbrellaagent.exe
- process_args: --noConsole --listenAddress=127.0.0.1 --resolverAddress=208.67.222.222 --encryptorStandard --dumpDirectory="C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\data\dump" --ipw4 --deviceid=010127373f19A61B --adUpnHash=dsdf255c87ce074a885f88570676110 --privateNetIp=10.1.82.156 --orgId=5334827 --allowlist="C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\data\proxy_allowlist4.txt" --resolvConf="C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\data\ResolverV4-1-EAE9ECFBD344D9886D368F04D6186-resolv.conf"
- process_path: C:\Program Files (x86)\Cisco\Cisco Secure Client\dnscryptproxy.exe

Simplicity! NVM Profiles

From This:

The screenshot shows a complex configuration page for XDR. It includes sections for Collector Type (Use On-Prem Collector), Cache Configuration (Max Size, Max Duration), Periodic Template Report (1440), Periodic Flow Report, Aggregation Interval (5), Throttle Rate (500), Collection Criteria (Broadcast Packets, Multicast Packets), and Collection Mode (All Networks). A yellow arrow points from the 'From This' text to the 'To This' text, indicating a transition to a simpler configuration page.

To This:

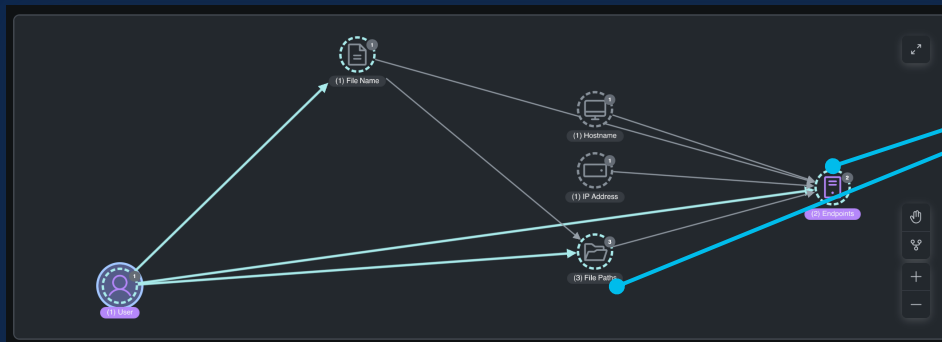
The screenshot shows a simplified configuration page for XDR. It includes sections for Collector Configuration (Collector Type: Use Cisco Cloud Collector), Proxy IP Address / FQDN, Proxy Port, and Ping Interval (minutes). A yellow arrow points from the 'From This' text to the 'To This' text, indicating a transition to a simpler configuration page.

Default XDR Deployment

- Default CM Profile
- Default NVM Profile

Just download & install, no config needed

NVM Provides Detections and Decorations



Displays Lateral Movement

Provides the East-West & North-South visibility and correlation

Direct source of observables

For brand-new detections in XDR Analytics

Type	Source	Severity				Important only
First Seen	Severity	Source	Indicators	Observables	Assets	
• 2023-05-27T02:48:53.000Z	High	Cisco Secure Cloud Analytics (security...	Suspicious Endpoint Activity	• --defaults-torrc "C:\Users\bill\Desktop\Tor Bro... 51.75.129.204 +7	loxx-win10vic07.org26.net	
• 2023-05-27T02:48:53.000Z	High	Cisco Secure Cloud Analytics (security...	Malicious Process Detected		loxx-win10vic07.org26.net	
• 2023-05-27T02:48:53.000Z	High	Cisco Secure Cloud Analytics (security...	Suspicious Endpoint Activity	51.75.129.204 93f38156eb3dbbe3562dfe7fe80ff62cab75c2f... +7	loxx-win10vic07.org26.net	
• 2023-05-27T02:48:53.000Z	High	Cisco Secure Cloud Analytics (security...	Malicious Process Detected		loxx-win10vic07.org26.net	
• 2023-05-27T01:44:45.000Z	High	Cisco Secure Cloud Analytics (security...		1875a380cc98bada07ad042ea17612fd92c9c9... b99d61d874728edc0918ca0eb10eab93d381e... +8	loxx-win10vic06.org26.net	
• 2023-05-27T01:44:45.000Z	High	Cisco Secure Cloud Analytics (security...	Potential Persistence Attempt		loxx-win10vic06.org26.net	
• 2023-05-27T01:44:45.000Z	High	Cisco Secure Cloud Analytics (security...	Suspicious Endpoint Activity	ORG26/bill 10.1.82.10 +8	loxx-win10vic06.org26.net	
2023-05-26T19:50:44.000Z	Unknown	AMP Event			loxx-win10vic06.org26.net	
2023-05-26T19:50:44.000Z	Unknown	AMP Event			loxx-win10vic06.org26.net	
2023-05-26T19:50:44.000Z	Unknown	AMP Event			loxx-win10vic06.org26.net	

XDR

Page 1 of 33 << < 1 / 4 > >>

Identity is a
critical
component of
any XDR



Identity in XDR

- Not only human (user) identity
 - Already covered the importance of device identity
 - Human identity is also a critical aspect of an incident
 - For Context: who was involved
 - For Detection: Identity based attacks

Users Inventory Page (in Beta)

Key Metrics Displayed

Assets > Users

User “inventory” is a subset of “Assets” category

Merged Inventory

Filterable, Sortable, Summary-Level of merged user accounts from all integrated sources.

Progressive Disclosure

Click on User for a User Details “Drawer”. Click on manager for drawer of manager’s details.

Assets > Users

Source health Healthy
All sources are operational

Users 311 total

35 Results

Search Filters 311 matching results

Display name	Login names	Emails	Department
Aaron Woland (aawoland)	aawoland_cisco.com#EXT#@securitydemo.net monet.onmicrosoft.com	aawoland@cisco.com	
Aaron Woland-Cisco	aawoland@securitydemo.net	aawoland@cisco.com, aawoland@securitydemo.net	Small Council
Abhishek Dubey	abhidub2@securitydemo.net		
Accounting1	Accounting1@securitydemo.net	accounting1@securitydemo.net	
Accounting2	accounting2@securitydemo.net	accounting2@securitydemo.net	
Adam Sonnenfeld	asonnenf@securitydemo.net		
Aditya Sankar	adisanka@securitydemo.net	adisanka@securitydemo.net	Little Birds
Alice Smith	alice@securitydemo.net	alice@securitydemo.net	Widgets
Anat Borowitsh Lavy	anat@securitydemo.net	anat@securitydemo.net	
Andrew Maxey	andrew@securitydemo.net	andrew@securitydemo.net	Dept. of Whispers
Anthony Brandelli	abrandel@securitydemo.net		

Andrew Maxey

Display name Andrew Maxey
First name Andrew
Last name Maxey
Emails andrew@securitydemo.net
Mobile phone numbers —
Business phone numbers —
User ID 345ce393-a333-421c-867f-80362bf3d771

Company —
Office location —
Department Dept. of Whispers
Manager Loxx
Job title Spy Master
Employee ID —
Groups LabUsers, Global Administrator, PosaaS

Last login —
Account created 2021-05-17T22:44:24.000Z
Account type —
Account status Enabled
Source types Azure Users
Used devices —
Owned devices —
Usage location —

[View user details](#)

Top Devices Used / Owned

Where Seen

All properties of the user: Group Memberships, Org Structure, Picture (if available), all Email addresses



User Context In an Investigation / Incident Management

Details for User “Assets”

Becomes the User Object,
instead of generic data

Progressive Disclosure

Clicking the user in the graph
would display the User Details
”drawer” within the window

The screenshot displays a security investigation interface with a dark theme. At the top, there are tabs for 'Overview', 'Detection', 'Response', and 'Worklog'. The main area shows a graph with a central 'Users' node (labeled 'ORCID:all') connected to various asset nodes like 'File Paths', 'File Names', 'IP Addresses', 'SHA-256 Hashes', and 'Endpoint Workstation'. A 'File Paths' node is highlighted with a red dashed circle. A 'Users' node is also highlighted with a green dashed circle. A 'Drawer' is open on the right side, displaying details for 'Adriana Hsieh'. The drawer has tabs for 'Admin' and 'Eng-admins'. It lists various attributes such as Display name, Login names, Emails, Phone numbers, User ID, Labels, Value, Company, Organization, Department, Manager, Job title, Employee ID, Groups, Last login, Last active, Account created, Account type, Account status, Source types, Used devices, Owned devices, Block sign-in, and Usage locations. A 'View user detail' button is at the bottom right of the drawer.

Adriana Hsieh

Admin Eng-admins

Display name: Adriana Hsieh

Login names: ahsieh (Azure), adrianah (OKTA), adrianahsieh (Duo)

Emails: ahsieh@cisico.com, adrianah@exsample.com

Phone numbers: +1 (123) 456 - 6837, +1 (123) 456 - 6837

User ID: 475394752985739dkyk, svrbjbgwlego

Labels: Eng-admins

Value: 8

Company: RAD

Organization: RAD

Department: R&D 234

Manager: Chuck Robbins

Job title: Leader, Software Engineering

Employee ID: 176536

Groups: Group, Group, group, group, group, group, +17 more

Last login: Mar 16, 2023, 3:11 PM

Last active: Mar 16, 2023, 3:11 PM

Account created: Mar 16, 2023, 3:11 PM

Account type: Admin

Account status: Enabled

Source types: OKTA, Azure AD

Used devices: PCARCO-M-88UZ, CLOUDSHARE-WYOP, PCARCO-M-88UZ

Owned devices: PCARCO-M-88UZ, CLOUDSHARE-WYOP, PCARCO-M-88UZ

Block sign-in: Yes

Usage locations: Waxhaw, NC, Palo Alto, CA, Atlanta, GA, Budapest, Turkey

[View user detail](#)

Identities lead to Identity Threat Detection & Response (ITDR)

- Identity-based attacks are on the rise
- Threat actors are exploiting the “identity sprawl” from cloud adoption & ZT style policies
 - Ex: MFA Flooding / MFA Fatigue
- Leverage compromised credentials, users w/ improper privileges



dORT

now part of **CISCO**

CISCO *Live!*

Why OORT?

- Tech & Talent Acquisition
- Literally the team that wrote Device Insights – left Cisco & created this w/ acquisition in mind
- Practically tailor-made for this integration

- Leader in ITDR market
- Large influencer / advisor for Identity Security with the major analysts
- Data Scientists / Engineering team with leaders in Identity Security

Integrations!!

OORT integrates w/ many key (cloud-based) ID sources already.

The screenshot shows the OORT web interface. At the top, there's a navigation bar with the OORT logo, a search bar, and links to Dashboard, Users, Checks, and Integrations. The user is logged in as 'Loxx admin - security-demo-net'. The main section is titled 'Integrations / Add Integration'. Under the 'Providers' section, there are nine cards, each representing a different integration provider. Each card includes the provider's logo, name, a brief description, and an 'Add Integration' button. The providers are: Auth0, Azure AD, Duo, GitHub (Beta), Google Workspace, Okta, Salesforce, Workday, and Manual Uploads. At the bottom, there's a 'Notification Targets' section which is currently empty. The footer contains links to oort.io, Privacy Policy, Terms of Use, Documentation, and SOC2 Report, along with a note that the environment reloads hourly.

OORT Search users, IPs and more... Dashboard Users Checks Integrations

Loxx admin - security-demo-net

Integrations / Add Integration

Providers

- Auth0**
Auth0 is a flexible, drop-in solution to add authentication and authorization services to your applications.
[+ Add Integration](#)
- Azure AD**
The Azure AD enterprise identity service provides SSO and MFA to help protect your users from cybersecurity attacks.
[+ Add Integration](#)
- Duo**
Duo Security is a cloud-based security platform that protects access to all applications, for any user and device, from anywhere.
[+ Add Integration](#)
- GitHub Beta**
GitHub is an Internet hosting service for software development and version control using Git. It provides the distributed version control of Git plus access control, bug tracking, software feature requests, task management, continuous integration, and wikis for every project.
[+ Add Integration](#)
- Google Workspace**
Google Workspace is a collection of cloud computing, productivity and collaboration tools, software and products developed by Google.
[+ Add Integration](#)
- Okta**
Okta is a customizable, secure, and drop-in solution to add authentication and authorization services to your apps.
[+ Add Integration](#)
- Salesforce**
Salesforce provides customer relationship management software and applications focused on sales, customer service, marketing automation, analytics, and application development.
[+ Add Integration](#)
- Workday**
Workday is a popular cloud-hosted HRIS service. Oort ingests regular and contingent worker data from Workday to enrich user details.
[+ Add Integration](#)
- Manual Uploads**
Upload a CSV or JSON file to supplement your integration data and analyze the data within Oort.
[Upload file](#)

Notification Targets

oort.io Privacy Policy Terms of Use Documentation SOC2 Report

This environment reloads hourly

Checks

AKA: Signatures for Detections

Filterable

All checks are categorized, assigned to applicable ID sources, and fully filterable

The screenshot displays the Cisco Duo Checks interface. The left sidebar provides filters for Compatibility (Azure AD, Duo, Okta), Severity (Critical, Low, Moderate), and Topic (ASD Essential 8, ASD Level 3, CIS 4.3, CIS 5.3, CIS 5.4, CIS 5.5, CIS 5.6, CIS 6.3, CIS 6.4, CIS 6.5, CMMC AC.2.010, CMMC IA.3.083, CMMC IA.3.084, CMMC SC.3.187, Compliance, Devices, Identity Posture Insight, Identity Threat Insight, Mitre ATT&CK T1078, Mitre ATT&CK T1078.004, Mitre ATT&CK T1097.004). The main panel shows a list of checks with columns for Check, # Failing, and # Excluded. Checks include 'Never Logged In' (77% failing, 39 failing), 'Applications with Expired Secrets' (78% failing, N/A failing), 'Azure Admin Activity Anomaly' (98% failing, 2 failing), 'Inactive Guest Users' (98% failing, 2 failing), 'Unused Application for a User' (99% failing, 1 failing), 'Access from Denied Countries' (100% failing, 0 failing), 'Active Account under Heavy Attack' (100% failing, 0 failing), 'Activity From Untrustworthy ISP' (100% failing, 0 failing), and 'Rare Browser Activity' (100% failing, 0 failing).

User Details

Will merge this data into “User Insights” & the user-details

Response

OORT has minimal responses already; which will tied into XDR incidents & response.

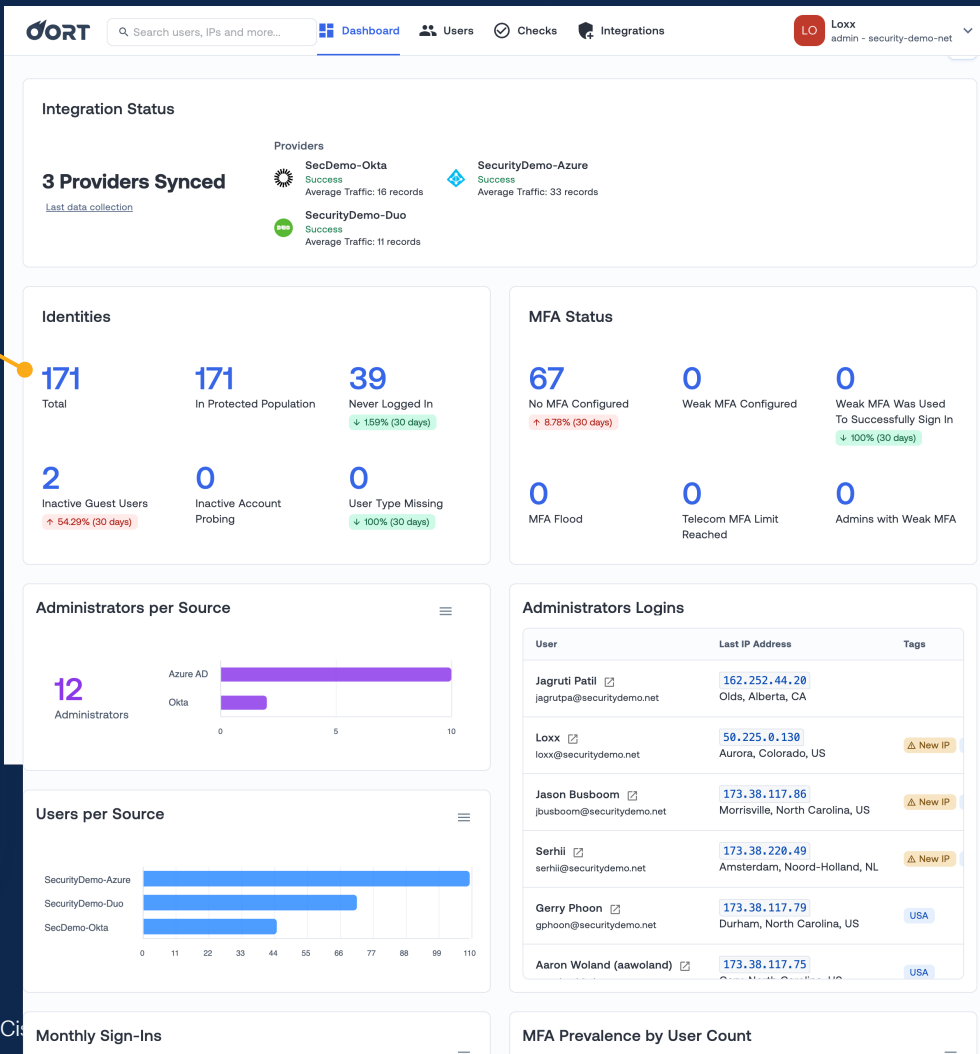
The screenshot displays the OORT user interface for a user named Aaron Woland (aawoland@cisco.com). The page is divided into several sections:

- Summary:** A list of user attributes including Inconsistent, N/A, MFA Configured, and Last Login Attempt (Jun 15, 2023 20:28:50 UTC).
- Attempted Logins:** A donut chart showing 3 attempts. A dropdown menu is open over this section, listing actions: Reset MFA, Log out user, Quarantine, Refresh User Data, and Link user.
- Records per day:** A bar chart showing the number of successful logins per day.
- Authentication Factors:** A table listing the user's authentication factors, including TOTP (SecDemo-Okta).

The bottom of the page features a footer with links to oort.io, Privacy Policy, Terms of Use, Documentation, and SOC2 Report, along with a note that the environment reloads hourly.

Insights

Provides detailed statistics on the identities merged, the MFA status(es), administrative logins, etc..



Login Attempts from New Countries

Country	Success	Failure	Other
Bulgaria	23	6	0

Identity Security split into 2 distinct focuses

Level-Setting

- Identity Threat Detection & Response (ITDR)
 - **REACTIVE**
 - Leverages detections and analytics across all identity and authentication sources in the organization
 - Integrates Identity-related threats into the incidents for a complete picture
 - Eg: MFA Flood attack or Impossible Time Travel (ITT).
- Identity Security Posture Management (ISPM)
 - **PROACTIVE**
 - Focuses on misconfigurations, policy infractions.
 - Eg: Weak / no MFA configured

XDR

Duo

The integration of Oort into Cisco is active work in progress

Keep an eye out!

Agenda

- A History Lesson
- Evolution
- Incident Management & Workflow
- Integrations & Response
- Key XDR Telemetry
- That's a wrap!

So... What Happens Now?

- XDR is a new product, and Cisco is charging for it.
- SecureX can migrate to Cisco XDR.
- Secure Cloud Analytics becomes XDR.

- All existing integrations for SecureX & SCA will continue to work.
- All existing orchestration workflows will continue to work.
- SecureX will continue to exist for CSC management & existing customers who did not migrate to XDR
- No end-of-life has been announced for SecureX (yet)

Please fill out the survey



Drop your email in the comments – I WILL respond!



Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.



Meet the Expert Opening Hours:

Tuesday	3:00pm – 7:00pm
Wednesday	11:15am – 7:00pm
Thursday	9:30am – 4:00pm
Friday	10:30am – 1:30pm

Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt



Continue your education



- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Other XDR sessions



Matthew Robertson
Distinguished TME

Extended Detection with
Cisco XDR: Security
analytics across the
enterprise

BRKSEC-2178

Wednesday @ 4:00 PM



Aaron Woland
Distinguished TME

Cisco's Unified Agent:
Cisco Secure Client.
Bringing AMP,
AnyConnect, Orbital &
Umbrella together

BRKSEC-2834

Thursday @ 9:00 AM



Aaron Woland
Distinguished TME

Cisco XDR - Making sense
of the Solution and how it's
a Security Productivity Tool

BRKSEC-2113

Friday @ 1:30 PM

Participating in user research gives you a place to share your thoughts and experiences to influence the future of Cisco Secure products.

- You'll hear from us at most once every 90 days.
- Participation is completely optional and you can opt out at any time.





The bridge to possible

Thank you



#CiscoLiveAPJC

The background features a vibrant, multi-colored abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of colorful rays in shades of blue, green, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go

#CiscoLiveAPJC