cisco Live!

Let’s go

cisco 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 | 𝕏 @aaronwoland | in aaronwoland

$ 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 2!

Fun fact 3: Working through his Cyber Security Master’s Degree from SANS Institute (~05/24)

Sarcasm

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

Webex App

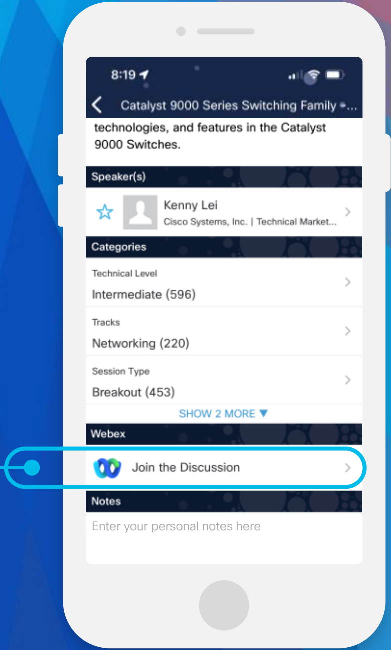
Questions?

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

How

1. Find this session in the Cisco Events 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 February 23, 2024.



8:19

Catalyst 9000 Series Switching Family ...

technologies, and features in the Catalyst 9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

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..."

CISCO
SECURE

CISCO The bridge to possible

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…

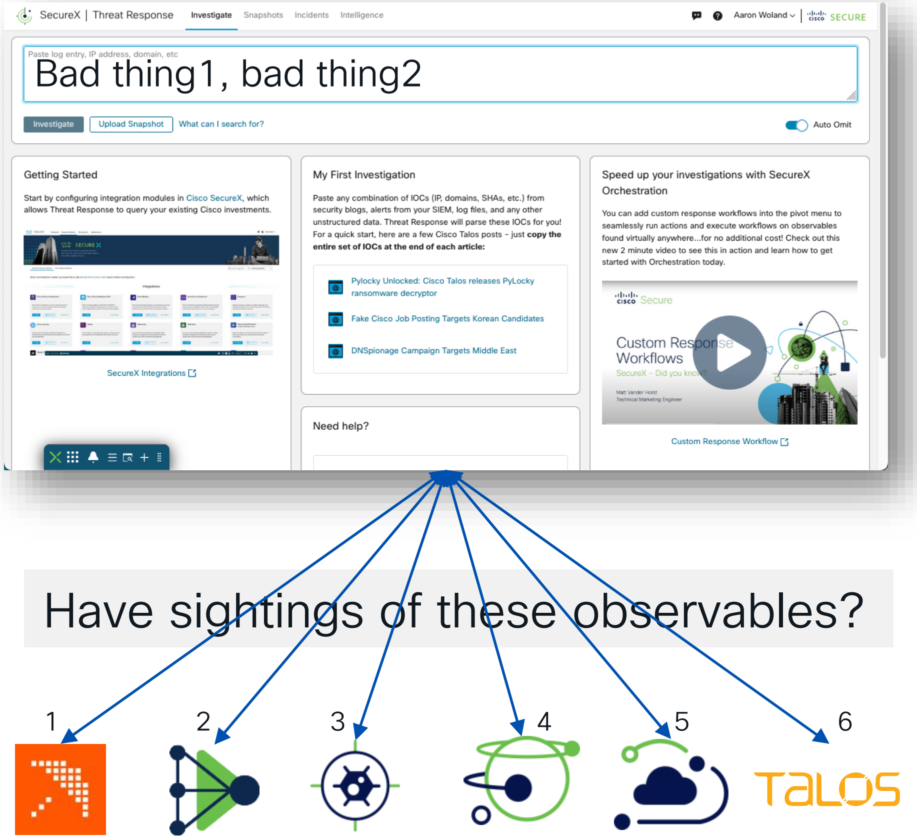
Agenda

- 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



SecureX | Threat Response

Paste log entry, IP address, domain, etc

Bad thing1, bad thing2

Getting Started

Start by configuring integration modules in Cisco SecureX, which allows Threat Response to query your existing Cisco investments.

SecureX Integrations

My First Investigation

Paste any combination of IOCs (IP, domains, SHAs, etc.) from security blogs, alerts from your SIEM, log files, and any other unstructured data. Threat Response will parse these IOCs for you! For a quick start, here are a few Cisco Talos posts - just **copy the entire set of IOCs at the end of each article:**

- Pylocky Unlocked: Cisco Talos releases PyLocky ransomware decryptor
- Fake Cisco Job Posting Targets Korean Candidates
- DNSpionage Campaign Targets Middle East

Need help?

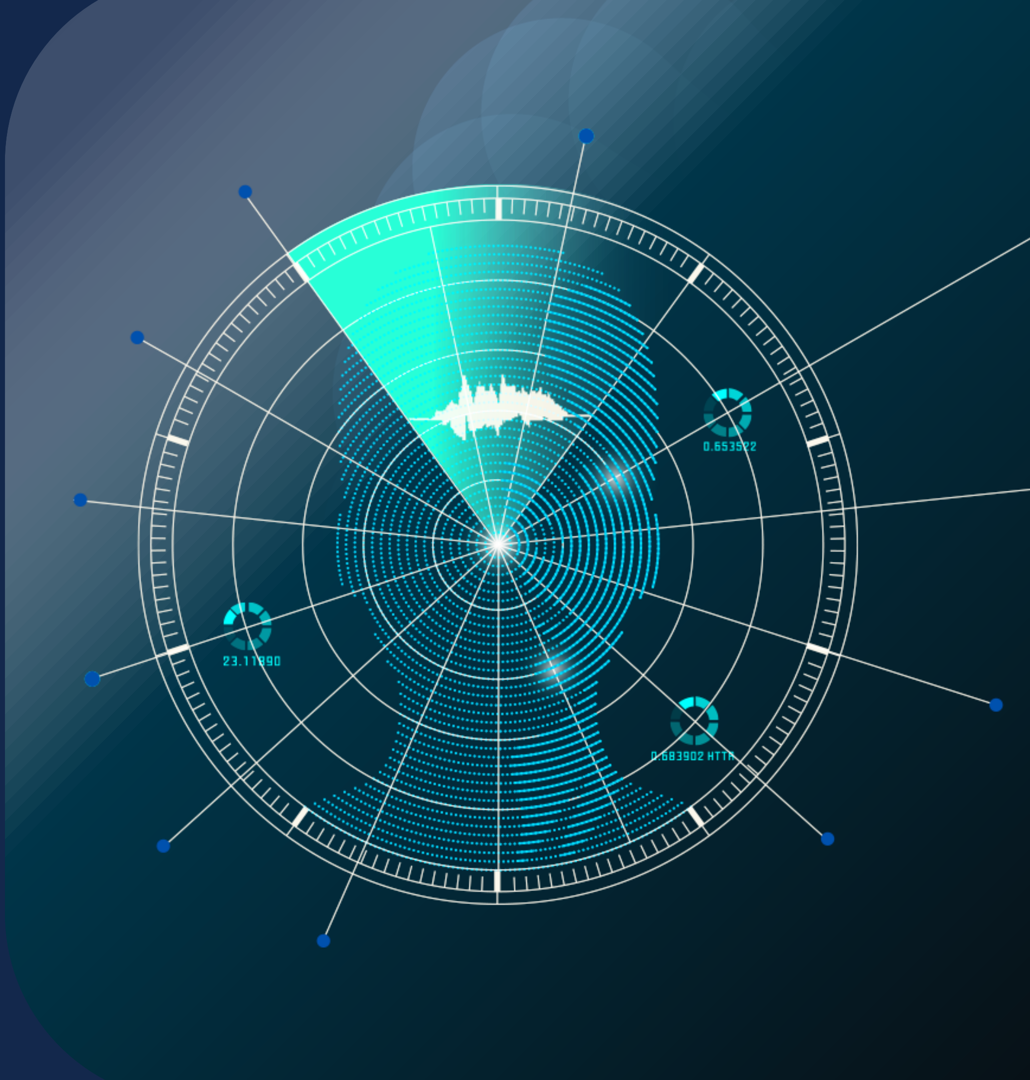
Speed up your investigations with SecureX Orchestration

You can add custom response workflows into the pivot menu to seamlessly run actions and execute workflows on observables found virtually anywhere...for no additional cost! Check out this new 2 minute video to see this in action and learn how to get started with Orchestration today.

Custom Response Workflow

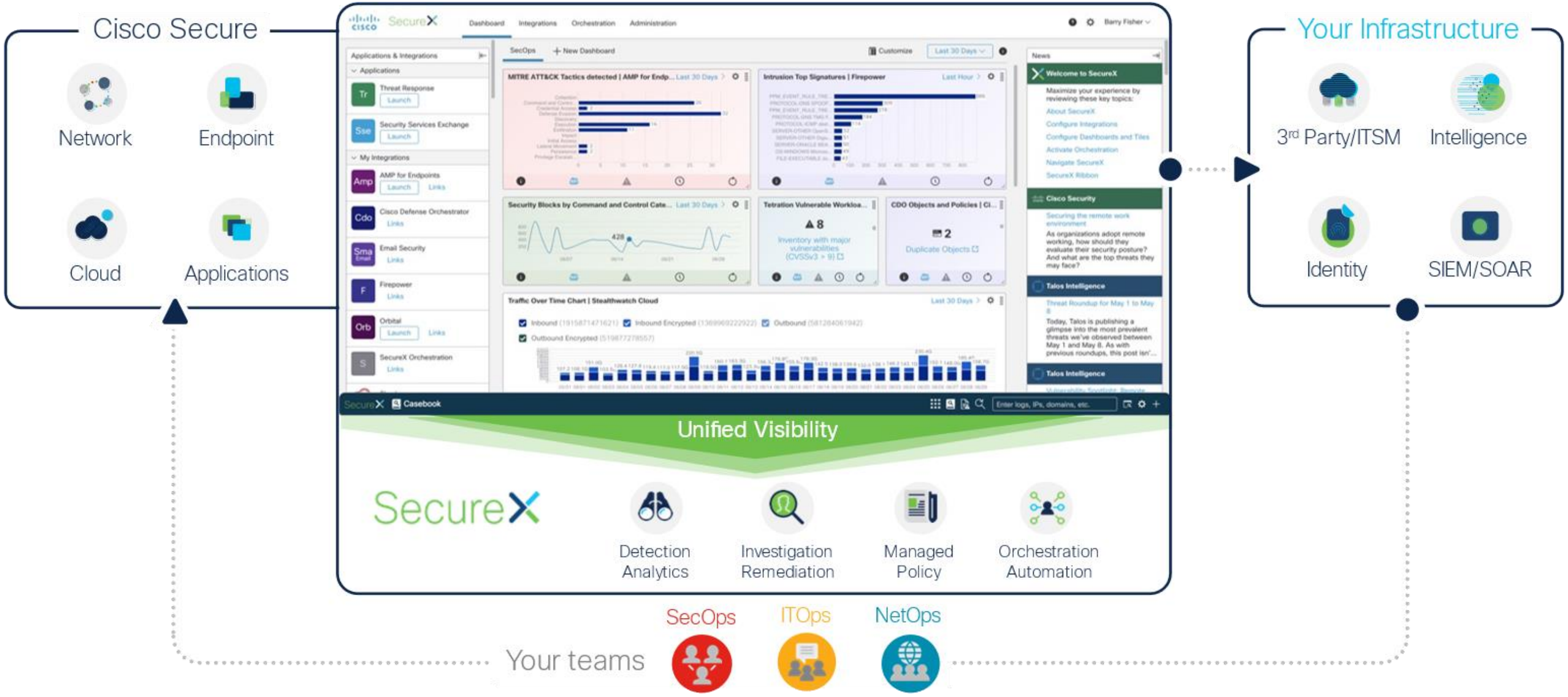
Have sightings of these observables?

Then in 2020...



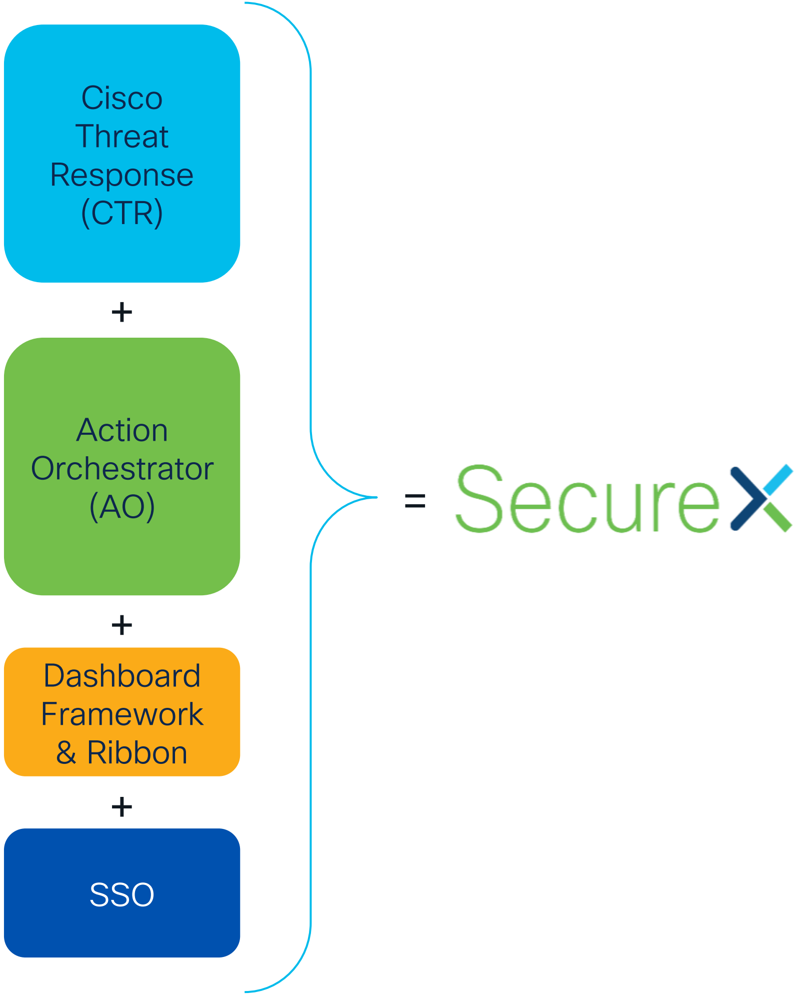
Introduced SecureX May of 2020

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

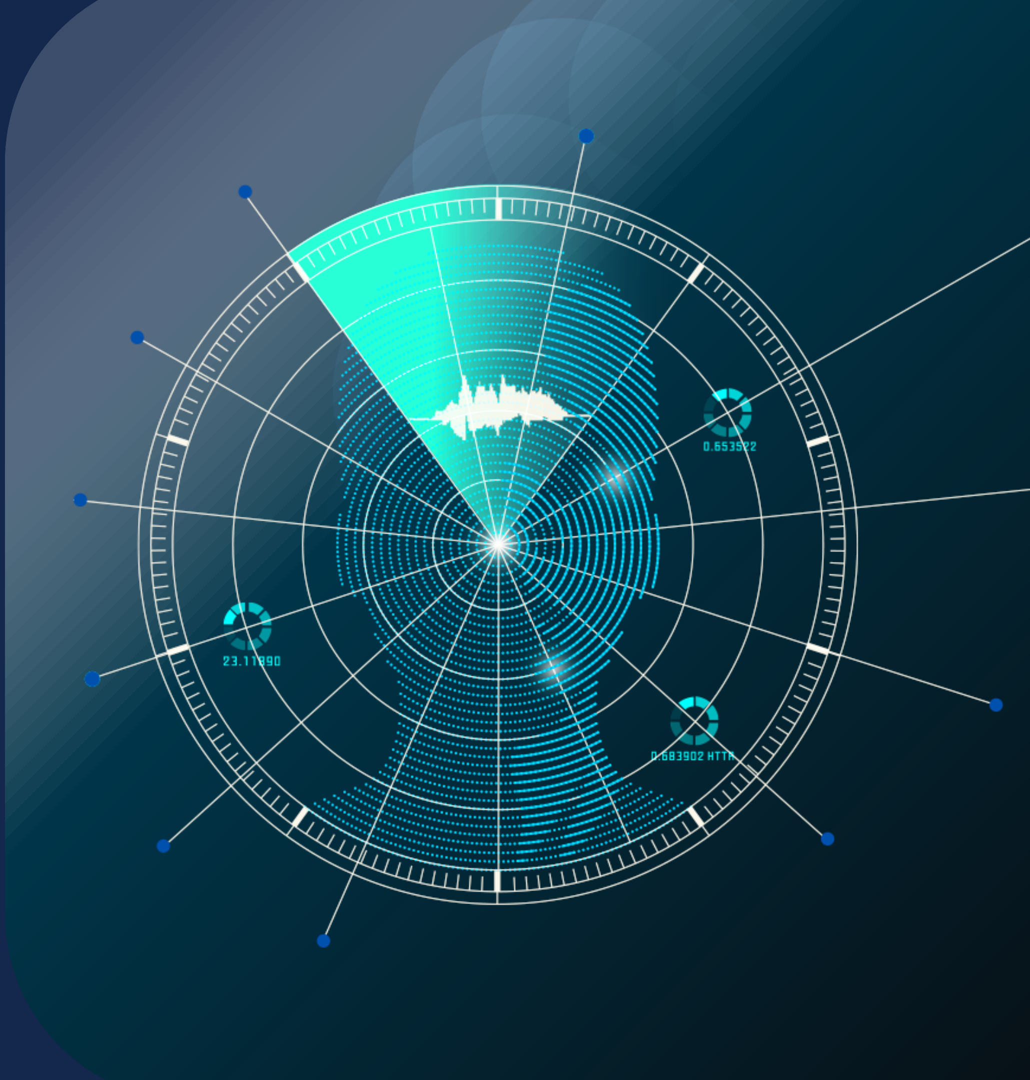


SecureX was to be THE Platform

- 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"*



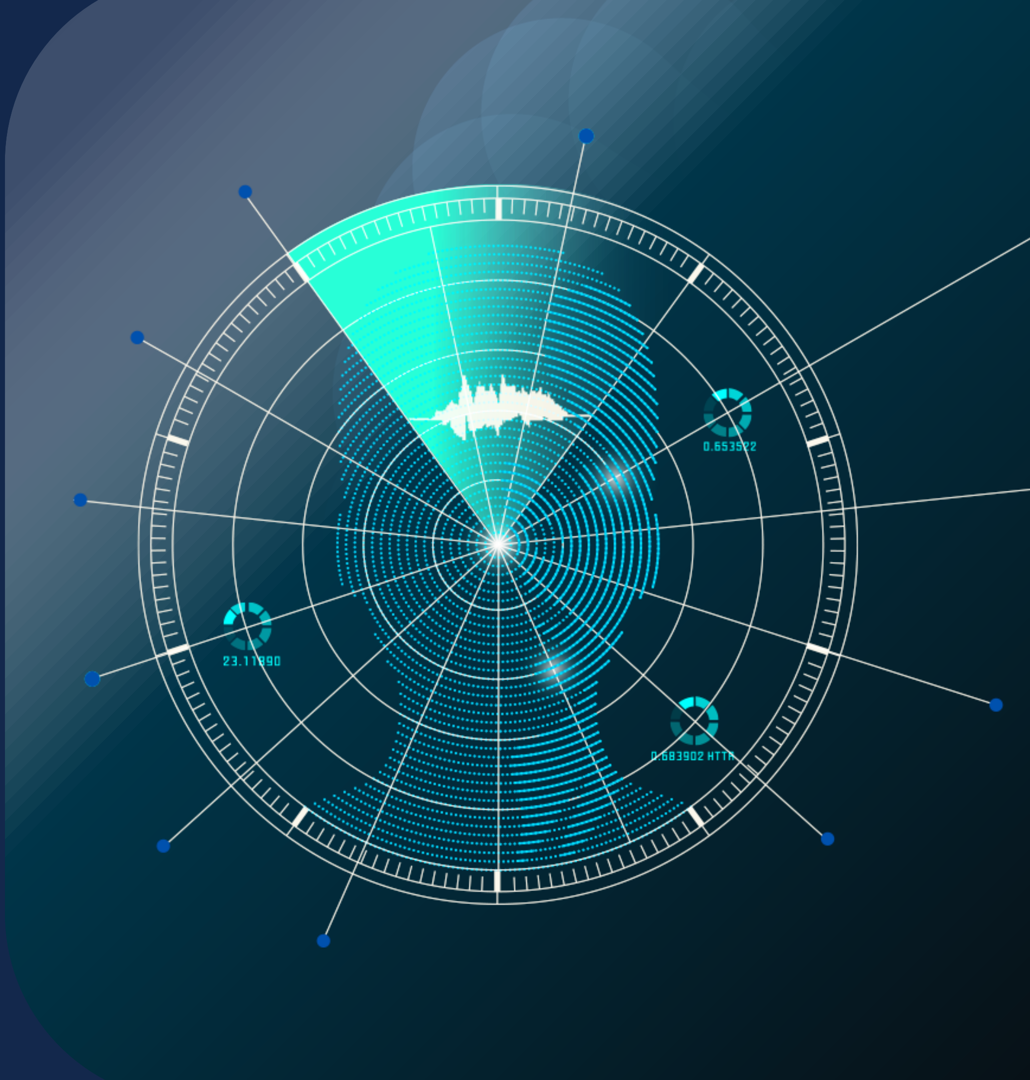
“Cisco SecureX is a leader for XDR”

- 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

1 Invests millions in research

Hired external research and design company to augment us

2 Invested heavily internally

Expanding our User Experience & Interface Teams

3 Blind & Sighted Interviews

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

4 Extensive Hiring of Experts

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

5 Restructured our Products

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

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

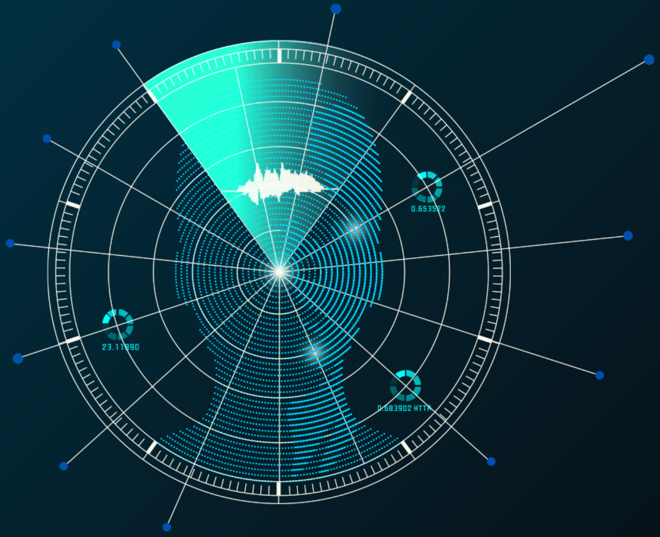
Adversary
Turla

// Nickname

Snake,
Venomous Bear,
Uroburos,
Group 88,
Waterbug

The adversary: What do we know?

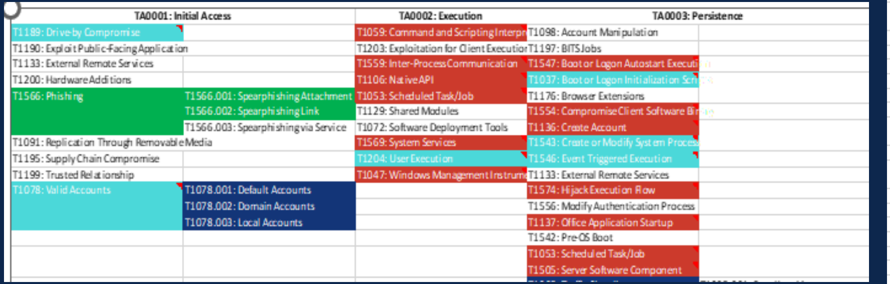
- Estonian intelligence services associate this group with the Russian federal security service (FSB).
- Does NOT deploy advanced tools unless necessary to compromise the target



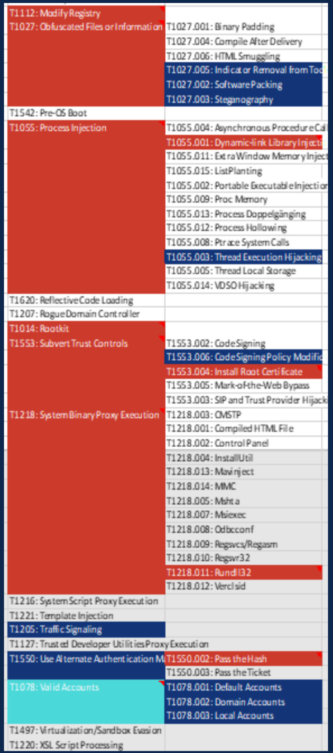
Method:

- 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

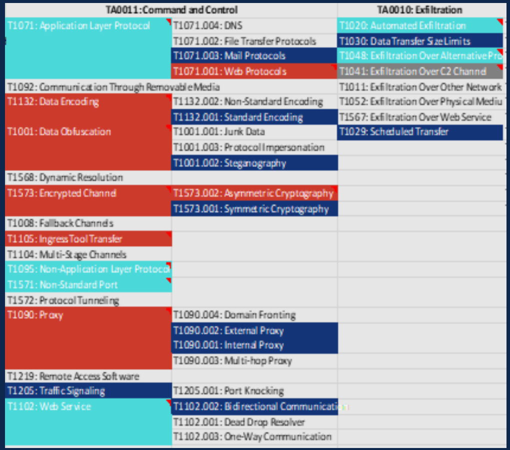
Without XDR, How Can We Detect and Respond to All of This?



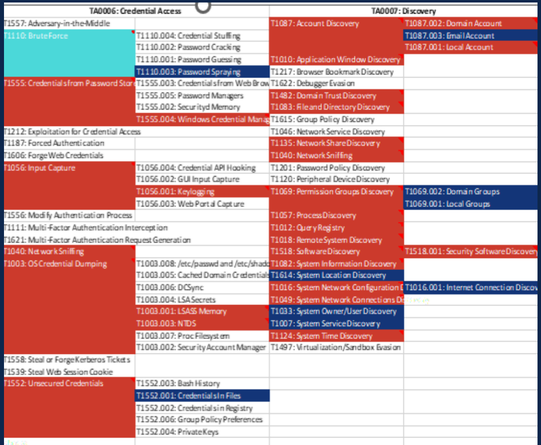
TA0001: Initial Access		TA0002: Execution	TA0003: Persistence	
T1189: Drive-by Compromise		T1059: Command and Scripting Interpr	T1098: Account Manipulation	
T1190: Exploit Public-Facing Application		T1203: Exploitation for Client Executior	T1197: BITS Jobs	
T1133: External Remote Services		T1559: Inter-Process Communication	T1547: Boot or Logon Autostart Executi	
T1200: Hardware Additions		T1106: Native API	T1037: Boot or Logon Initialization Scri	
T1566: Phishing	T1566.001: Spearphishing Attachment	T1053: Scheduled Task/Job	T1176: Browser Extensions	
	T1566.002: Spearphishing Link	T1129: Shared Modules	T1554: Compromise Client Software Bi	
	T1566.003: Spearphishing via Service	T1072: Software Deployment Tools	T1136: Create Account	
T1091: Replication Through Removable Media		T1569: System Services	T1543: Create or Modify System Process	
T1195: Supply Chain Compromise		T1204: User Execution	T1546: Event Triggered Execution	
T1199: Trusted Relationship		T1047: Windows Management Instrume	T1133: External Remote Services	
T1078: Valid Accounts	T1078.001: Default Accounts		T1574: Hijack Execution Flow	
	T1078.002: Domain Accounts		T1556: Modify Authentication Process	
	T1078.003: Local Accounts		T1137: Office Application Startup	
			T1542: Pre-OS Boot	
			T1053: Scheduled Task/Job	
			T1505: Server Software Component	



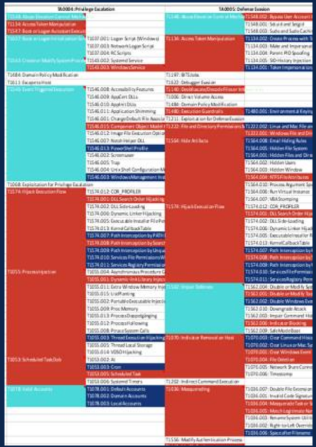
T1112: Modify Registry	
T1027: Obfuscated Files or Information	T1027.001: Binary Padding
	T1027.004: Compile After Delivery
	T1027.006: HTML Smuggling
	T1027.005: Indicator Removal from Too
	T1027.002: Software Packing
	T1027.003: Steganography
T1542: Pre-OS Boot	
T1055: Process Injection	T1055.004: Asynchronous Procedure Cal
	T1055.001: Dynamic-link Library Injecti
	T1055.011: Extra Window Memory Inject
	T1055.015: ListPlanting
	T1055.002: Portable Executable Injection
	T1055.009: Proc Memory
	T1055.013: Process Doppelgänging
	T1055.012: Process Hollowing
	T1055.008: Ptrace System Calls
	T1055.003: Thread Execution Hijacking
	T1055.005: Thread Local Storage
	T1055.014: VDSO Hijacking
T1620: Reflective Code Loading	
T1207: Rogue Domain Controller	
T1014: Rootkit	
T1553: Subvert Trust Controls	T1553.002: Code Signing
	T1553.006: Code Signing Policy Modific
	T1553.004: Install Root Certificate
	T1553.005: Mark-of-the-Web Bypass
	T1553.003: SIP and Trust Provider Hijacki
T1218: System Binary Proxy Execution	T1218.003: CMSTP
	T1218.001: Compiled HTML File
	T1218.002: Control Panel
	T1218.004: InstallUtil
	T1218.013: Mavinject
	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	
T1127: Trusted Developer Utilities Proxy Execution	
T1550: Use Alternate Authentication M	T1550.002: Pass the Hash
	T1550.003: Pass the Ticket
T1078: Valid Accounts	T1078.001: Default Accounts
	T1078.002: Domain Accounts
	T1078.003: Local Accounts
T1497: Virtualization/Sandbox Evasion	
T1220: XSL Script Processing	



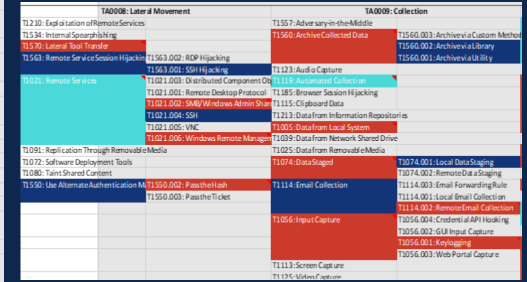
TA0011: Command and Control		TA0010: Exfiltration
T1071: Application Layer Protocol	T1071.004: DNS	T1020: Automated Exfiltration
	T1071.002: File Transfer Protocols	T1030: Data Transfer Size Limits
	T1071.003: Mail Protocols	T1048: Exfiltration Over Alternative Pro
	T1071.001: Web Protocols	T1041: Exfiltration Over C2 Channel
T1092: Communication Through Removable Media		T1011: Exfiltration Over Other Network
T1132: Data Encoding	T1132.002: Non-Standard Encoding	T1052: Exfiltration Over Physical Mediu
	T1132.001: Standard Encoding	T1567: Exfiltration Over Web Service
T1001: Data Obfuscation	T1001.001: Junk Data	T1029: Scheduled Transfer
	T1001.003: Protocol Impersonation	
	T1001.002: Steganography	
T1568: Dynamic Resolution		
T1573: Encrypted Channel	T1573.002: Asymmetric Cryptography	
	T1573.001: Symmetric Cryptography	
T1008: Fallback Channels		
T1105: Ingress Tool Transfer		
T1104: Multi-Stage Channels		
T1095: Non-Application Layer Protocol		
T1571: Non-Standard Port		
T1572: Protocol Tunneling		
T1090: Proxy	T1090.004: Domain Fronting	
	T1090.002: External Proxy	
	T1090.001: Internal Proxy	
	T1090.003: Multi-hop Proxy	
T1219: Remote Access Software		
T1205: Traffic Signaling	T1205.001: Port Knocking	
T1102: Web Service	T1102.002: Bidirectional Communication	
	T1102.001: Dead Drop Resolver	
	T1102.003: One-Way Communication	



TA0006: Credential Access		TA0007: Discovery	
T1557: Adversary-in-the-Middle		T1087: Account Discovery	T1087.002: Domain Account
T1110: Brute Force	T1110.004: Credential Stuffing		T1087.003: Email Account
	T1110.002: Password Cracking		T1087.001: Local Account
	T1110.001: Password Guessing	T1010: Application Window Discovery	
	T1110.003: Password Spraying	T1217: Browser Bookmark Discovery	
T1555: Credentials from Password Stor	T1555.003: Credentials from Web Brow	T1622: Debugger Evasion	
	T1555.005: Password Managers	T1482: Domain Trust Discovery	
	T1555.002: Securityd Memory	T1083: File and Directory Discovery	
	T1555.004: Windows Credential Manag	T1615: Group Policy Discovery	
T1212: Exploitation for Credential Access		T1046: Network Service Discovery	
T1187: Forced Authentication		T1135: Network Share Discovery	
T1606: Forge Web Credentials		T1040: Network Sniffing	
T1056: Input Capture	T1056.004: Credential API Hooking	T1201: Password Policy Discovery	
	T1056.002: GUI Input Capture	T1120: Peripheral Device Discovery	
	T1056.001: Keylogging	T1069: Permission Groups Discovery	T1069.002: Domain Groups
	T1056.003: Web Portal Capture		T1069.001: Local Groups
T1556: Modify Authentication Process		T1057: Process Discovery	
T1111: Multi-Factor Authentication Interception		T1012: Query Registry	
T1621: Multi-Factor Authentication Request Generation		T1018: Remote System Discovery	
T1040: Network Sniffing		T1518: Software Discovery	T1518.001: Security Software Discovery
T1003: OS Credential Dumping	T1003.008: /etc/passwd and /etc/shado	T1082: System Information Discovery	
	T1003.005: Cached Domain Credentials	T1614: System Location Discovery	
	T1003.006: DCSync	T1016: System Network Configuration D	T1016.001: Internet Connection Discov
	T1003.004: LSA Secrets	T1049: System Network Connections Discovery	
	T1003.001: LSASS Memory	T1033: System Owner/User Discovery	
	T1003.003: NTDS	T1007: System Service Discovery	
	T1003.007: Proc Filesystem	T1124: System Time Discovery	
	T1003.002: Security Account Manager	T1497: Virtualization/Sandbox Evasion	
T1558: Steal or Forge Kerberos Tickets			
T1539: Steal Web Session Cookie			
T1552: Unsecured Credentials	T1552.003: Bash History		
	T1552.001: Credentials In Files		
	T1552.002: Credentials in Registry		
	T1552.006: Group Policy Preferences		
	T1552.004: Private Keys		



TA0004: Privilege Escalation		TA0005: Defense Evasion	
T1548: Abuse Elevation Control Mech		T1548: Abuse Elevation Control Mech	T1548.002: Bypass User Account C
T1134: Access Token Manipulation			T1548.001: Setuid and Setgid
T1547: Boot or Logon Autostart Execut			T1548.003: Sudo and Sudo Cachi
T1037: Boot or Logon Initialization Scr	T1037.001: Logon Script (Windows)	T1134: Access Token Manipulation	T1134.002: Create Process with T
	T1037.003: Network Logon Script		T1134.003: Make and Impersonat
	T1037.004: RC Scripts		T1134.004: Parent PID Spoofing
T1543: Create or Modify System Proce	T1543.002: Systemd Service		T1134.005: SID-History Injection
	T1543.003: Windows Service		T1134.001: Token Impersonation
T1484: Domain Policy Modification		T1197: BITS Jobs	
T1611: Escape to Host		T1622: Debugger Evasion	
T1546: Event Triggered Execution	T1546.008: Accessibility Features	T1140: Deobfuscate/Decode Files or Inf	
	T1546.009: AppCert DLLs	T1006: Direct Volume Access	
	T1546.010: AppInit DLLs	T1484: Domain Policy Modification	
	T1546.011: Application Shimming	T1480: Execution Guardrails	T1480.001: Environmental Keying
	T1546.001: Change Default File Associa	T1211: Exploitation for Defense Evasion	
	T1546.015: Component Object Model	T1222: File and Directory Permissions M	T1222.002: Linux and Mac File an
	T1546.012: Image File Execution Optio		T1222.001: Windows File and Dir
	T1546.007: Netsh Helper DLL	T1564: Hide Artifacts	T1564.008: Email Hiding Rules
	T1546.013: PowerShell Profile		T1564.005: Hidden File System
	T1546.002: Screensaver		T1564.001: Hidden Files and Dir
	T1546.005: Trap		T1564.002: Hidden Users
	T1546.004: Unix Shell Configuration M		T1564.003: Hidden Window
	T1546.003: Windows Management Ins		T1564.004: NTFS File Attributes
T1068: Exploitation for Privilege Escalation			T1564.010: Process Argument Sp
T1574: Hijack Execution Flow	T1574.012: COR_PROFILER		T1564.006: Run Virtual Instance
	T1574.001: DLL Search Order Hijacking		T1564.007: VBA Stomping
	T1574.002: DLL Side-Loading	T1574: Hijack Execution Flow	T1574.012: COR_PROFILER
	T1574.006: Dynamic Linker Hijacking		T1574.001: DLL Search Order Hij
	T1574.005: Executable Installer File Per		T1574.002: DLL Side-Loading
	T1574.013: KernelCallbackTable		T1574.006: Dynamic Linker Hijack
	T1574.007: Path Interception by PATH		T1574.005: Executable Installer Fi
	T1574.008: Path Interception by Search		T1574.013: KernelCallbackTable
	T1574.009: Path Interception by Unquo		T1574.007: Path Interception by
	T1574.010: Services File Permissions W		T1574.008: Path Interception by
	T1574.011: Services Registry Permissio		T1574.009: Path Interception by
T1055: Process Injection	T1055.004: Asynchronous Procedure C		T1574.010: Services File Permissi
	T1055.001: Dynamic-link Library Injectio		T1574.011: Services Registry Perm
	T1055.011: Extra Window Memory Inje	T1562: Impair Defenses	T1562.004: Disable or Modify Sys
	T1055.015: ListPlanting		T1562.001: Disable or Modify Too
	T1055.002: Portable Executable Injectio		T1562.002: Disable Windows Eve
	T1055.009: Proc Memory		T1562.010: Downgrade Attack
	T1055.013: Process Doppelgänging		T1562.003: Impair Command His
	T1055.012: Process Hollowing		T1562.006: Indicator Blocking
	T1055.008: Ptrace System Calls		T1562.009: Safe Mode Boot
	T1055.003: Thread Execution Hijacking	T1070: Indicator Removal on Host	T1070.003: Clear Command Histo
	T1055.005: Thread Local Storage		T1070.002: Clear Linux or Mac Sy
	T1055.014: VDSO Hijacking		T1070.001: Clear Windows Event
T1053: Scheduled Task/Job	T1053.002: At		T1070.004: File Deletion
	T1053.003: Cron		T1070.005: Network Share Conne
	T1053.005: Scheduled Task		T1070.006: Timestomp
	T1053.006: Systemd Timers	T1202: Indirect Command Execution	
T1078: Valid Accounts	T1078.001: Default Accounts	T1036: Masquerading	T1036.007: Double File Extension
	T1078.002: Domain Accounts		T1036.001: Invalid Code Signature
	T1078.003: Local Accounts		T1036.004: Masquerade Task or S
			T1036.005: Match Legitimate Nam
			T1036.003: Rename System Utilit
			T1036.002: Right-to-Left Override
			T1036.006: Space after Filename
		T1556: Modify Authentication Process	



TA0008: Lateral Movement		TA0009: Collection	
T1210: Exploitation of Remote Services		T1557: Adversary-in-the-Middle	
T1534: Internal Spearphishing		T1560: Archive Collected Data	T1560.003: Archive via Custom Method
T1570: Lateral Tool Transfer			T1560.002: Archive via Library
T1563: Remote Service Session Hijackin	T1563.002: RDP Hijacking		T1560.001: Archive via Utility
	T1563.001: SSH Hijacking	T1123: Audio Capture	
T1021: Remote Services	T1021.003: Distributed Component Ob	T1119: Automated Collection	
	T1021.001: Remote Desktop Protocol	T1185: Browser Session Hijacking	
	T1021.002: SMB/Windows Admin Share	T1115: Clipboard Data	
	T1021.004: SSH	T1213: Data from Information Repositories	
	T1021.005: VNC	T1005: Data from Local System	
	T1021.006: Windows Remote Managem	T1039: Data from Network Shared Drive	
T1091: Replication Through Removable Media		T1025: Data from Removable Media	
T1072: Software Deployment Tools		T1074: Data Staged	T1074.001: Local Data Staging
T1080: Taint Shared Content			T1074.002: Remote Data Staging
T1550: Use Alternate Authentication M	T1550.002: Pass the Hash	T1114: Email Collection	T1114.003: Email Forwarding Rule
	T1550.003: Pass the Ticket		T1114.001: Local Email Collection
			T1114.002: Remote Email Collection
		T1056: Input Capture	T1056.004: Credential API Hooking
			T1056.002: GUI Input Capture
			T1056.001: Keylogging
			T1056.003: Web Portal Capture
		T1113: Screen Capture	
		T1125: Video 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)

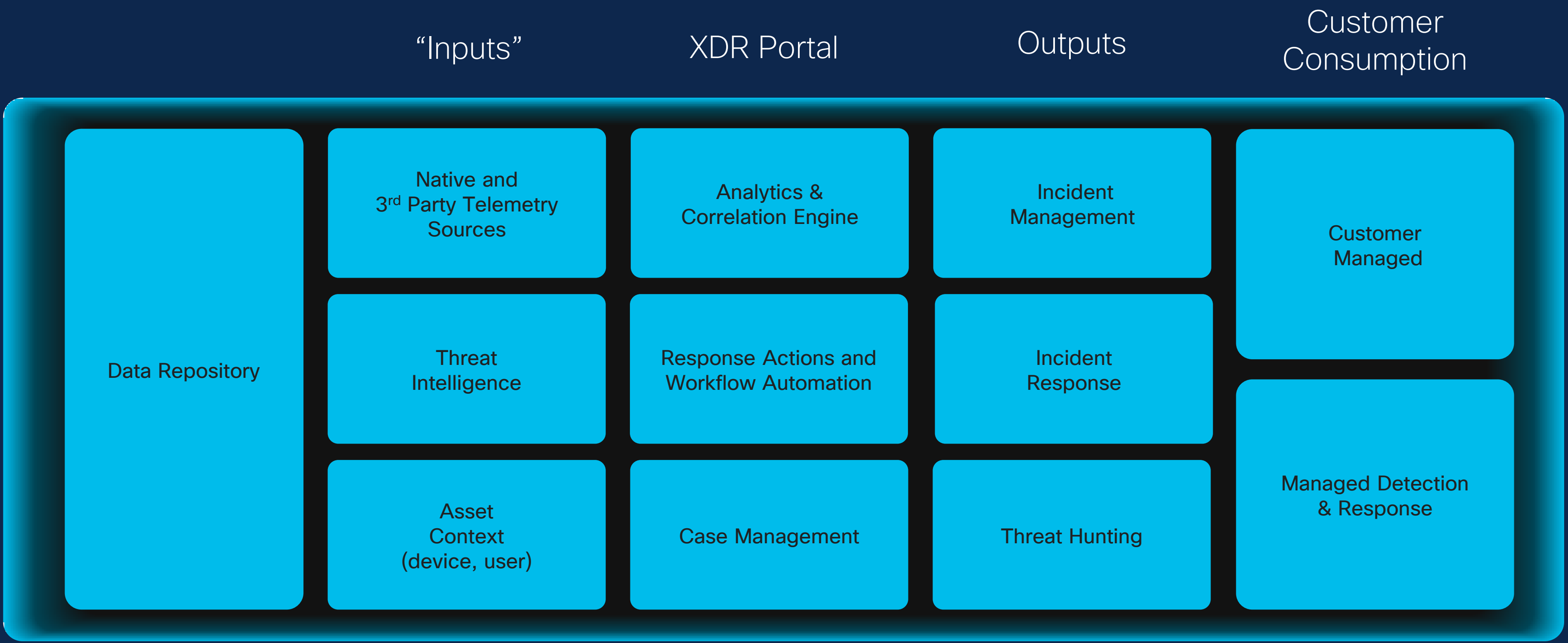
Firewall Threat Defense (FTD)

Duo

Email Threat Defense (ETD)

Umbrella

What Are the Building Blocks of an Ideal XDR Solution?



	“Inputs”	XDR Portal	Outputs	Customer Consumption
Data Repository	Native and 3rd Party Telemetry Sources	Analytics & Correlation Engine	Incident Management	Customer Managed
	Threat Intelligence	Response Actions and Workflow Automation	Incident Response	
	Asset Context (device, user)	Case Management	Threat Hunting	Managed Detection & Response

How do we accomplish this?

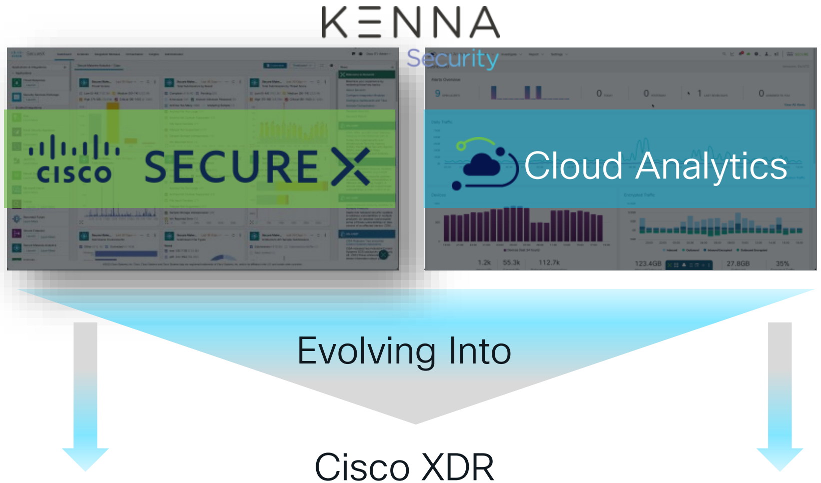
Agenda

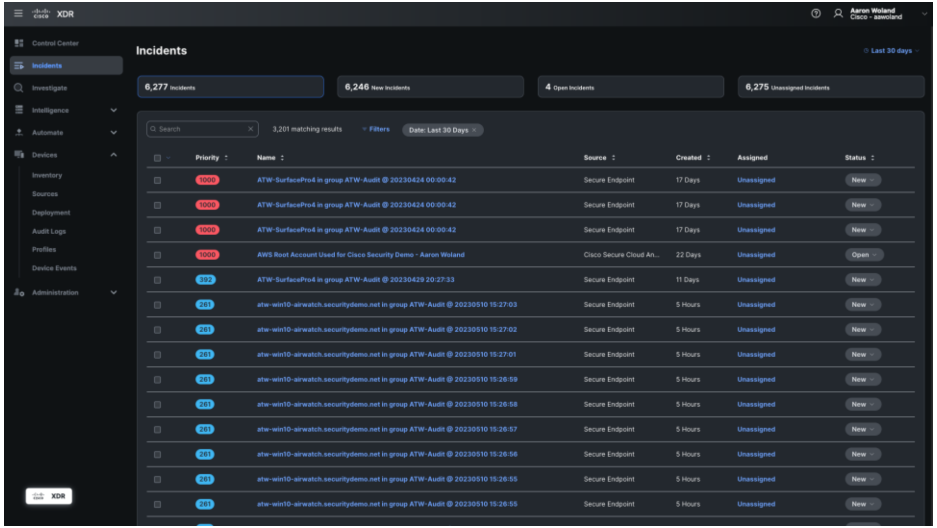
- A History Lesson
- Evolution
- Incident Management & Workflow
- Integrations & Response
- Key XDR Telemetry
- That’s a wrap!

Evolution

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

soon plus OORT
now part of CISCO





Incidents

Last 30 days

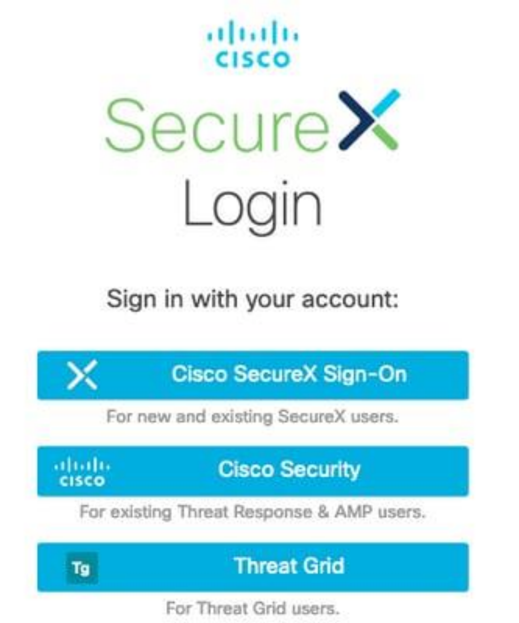
6,277 Incidents | 6,246 New Incidents | 4 Open Incidents | 6,275 Unassigned Incidents

Search | 3,201 matching results | Filters | Date: Last 30 Days

Priority	Name	Source	Created	Assigned	Status
1000	ATW-SurfacePro4 in group ATW-Audit @ 20230424 00:00:42	Secure Endpoint	17 Days	Unassigned	New
1000	ATW-SurfacePro4 in group ATW-Audit @ 20230424 00:00:42	Secure Endpoint	17 Days	Unassigned	New
1000	ATW-SurfacePro4 in group ATW-Audit @ 20230424 00:00:42	Secure Endpoint	17 Days	Unassigned	New
1000	AWS Root Account Used for Cisco Security Demo - Aaron Woland	Cisco Secure Cloud An...	22 Days	Unassigned	Open
392	ATW-SurfacePro4 in group ATW-Audit @ 20230429 20:27:33	Secure Endpoint	11 Days	Unassigned	New
261	atw-win10-airwatch.securitydemo.net in group ATW-Audit @ 20230510 15:27:03	Secure Endpoint	5 Hours	Unassigned	New
261	atw-win10-airwatch.securitydemo.net in group ATW-Audit @ 20230510 15:27:02	Secure Endpoint	5 Hours	Unassigned	New
261	atw-win10-airwatch.securitydemo.net in group ATW-Audit @ 20230510 15:27:01	Secure Endpoint	5 Hours	Unassigned	New
261	atw-win10-airwatch.securitydemo.net in group ATW-Audit @ 20230510 15:26:59	Secure Endpoint	5 Hours	Unassigned	New
261	atw-win10-airwatch.securitydemo.net in group ATW-Audit @ 20230510 15:26:58	Secure Endpoint	5 Hours	Unassigned	New
261	atw-win10-airwatch.securitydemo.net in group ATW-Audit @ 20230510 15:26:57	Secure Endpoint	5 Hours	Unassigned	New
261	atw-win10-airwatch.securitydemo.net in group ATW-Audit @ 20230510 15:26:56	Secure Endpoint	5 Hours	Unassigned	New
261	atw-win10-airwatch.securitydemo.net in group ATW-Audit @ 20230510 15:26:55	Secure Endpoint	5 Hours	Unassigned	New
261	atw-win10-airwatch.securitydemo.net in group ATW-Audit @ 20230510 15:26:55	Secure Endpoint	5 Hours	Unassigned	New

SecureX is no longer “the platform”

The “Cisco Security Cloud” is the platform



SecureX Login

Sign in with your account:

Cisco SecureX Sign-On

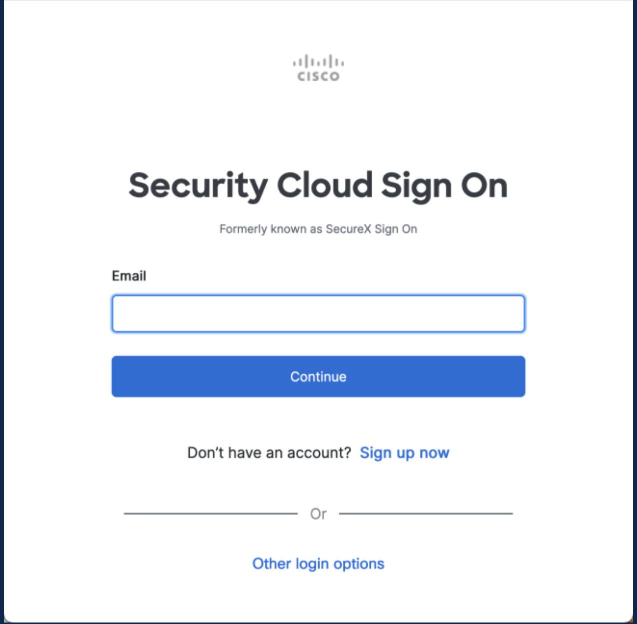
For new and existing SecureX users.

Cisco Security

For existing Threat Response & AMP users.

Threat Grid

For Threat Grid users.



Security Cloud Sign On

Formerly known as SecureX Sign On

Email

Continue

Don’t have an account? Sign up now

Or

Other login options

“XDR is a Security Operations Productivity Tool”

– Me

Top 3 Responsibilities of a SOC

Monitoring and Response

- Continuous monitoring of security systems.
- Alert triage, analysis, and incident response.
- Coordination of response efforts and stakeholder communication.

Operations Management

- Threat hunting, intelligence gathering, and risk assessment.
- Conducting vulnerability assessments and penetration testing.
- Fine-tuning security tools and processes for optimal performance.

Compliance, Education, and Strategy

- Policy development, compliance enforcement, and vendor management.
- Educating users through training and awareness programs.
- Keeping informed on emerging threats to inform security strategy.

Common SOC Duties

Tier 1 (Triage):

- Phishing campaigns
- Phishing file analysis
- IP/domain analysis
- Mobile device wipes
- Email investigations
- 3rd party vulnerability reports – threat hunt
- Escalate to T2

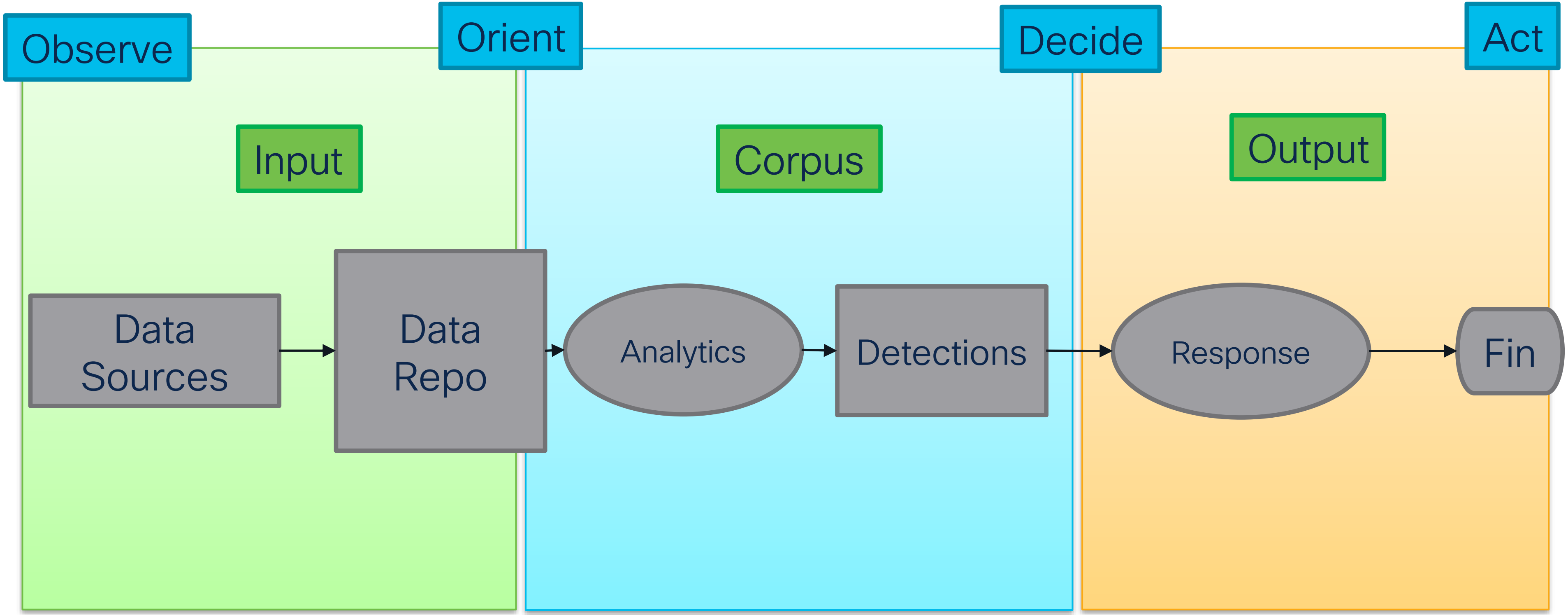
Tier 2 (Sr/Lead):

- IDS/IPS alerts
- Rogue users
- DNS Sinkholing domains
- IP/VPN blocks
- DDoS
- Escalate to CTI/CTA/CTD/IR
- Email pulls
- Account disables/wipes
- Pull forensic package

Shift Lead (Sr/T3):

- Create and Monitor dashboards
- Train new hires
- Make sure everyone is doing their work
- Jump into incidents ad hoc
- Manage the SOC queue
- Interface with vendors

An XDR speeds up the OODA Loop

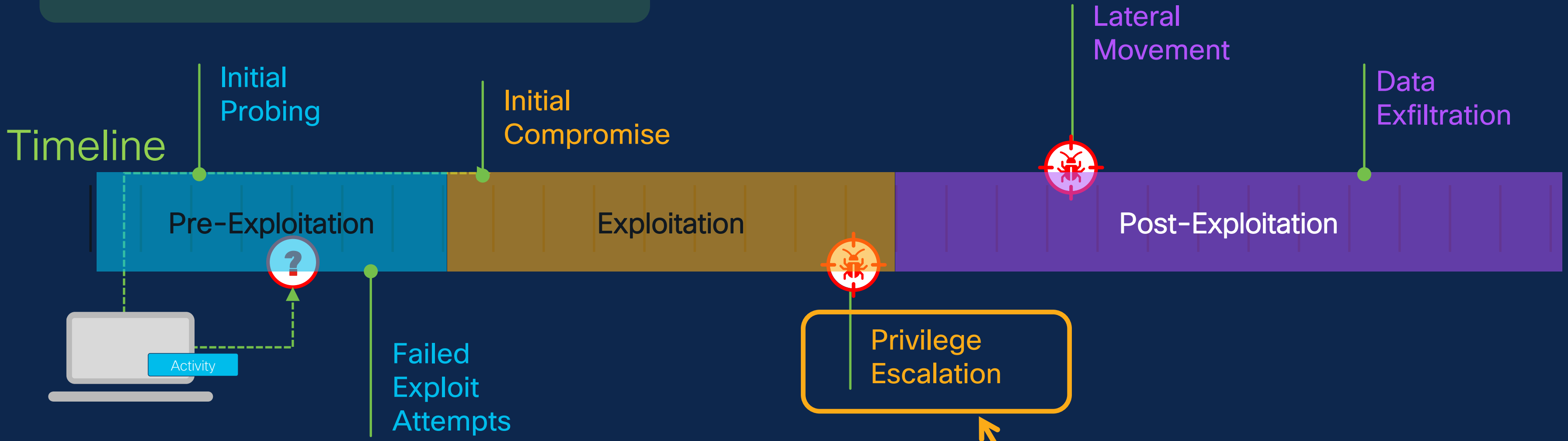


Investigators build out a timeline.

The XDR **automates the timeline** creation

Investigation Timeline – what happened & when?

Responder typically builds out a timeline when investigation



Starting Here, look forward & backwards for correlation to build the timeline / attack graph of "what happened"

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

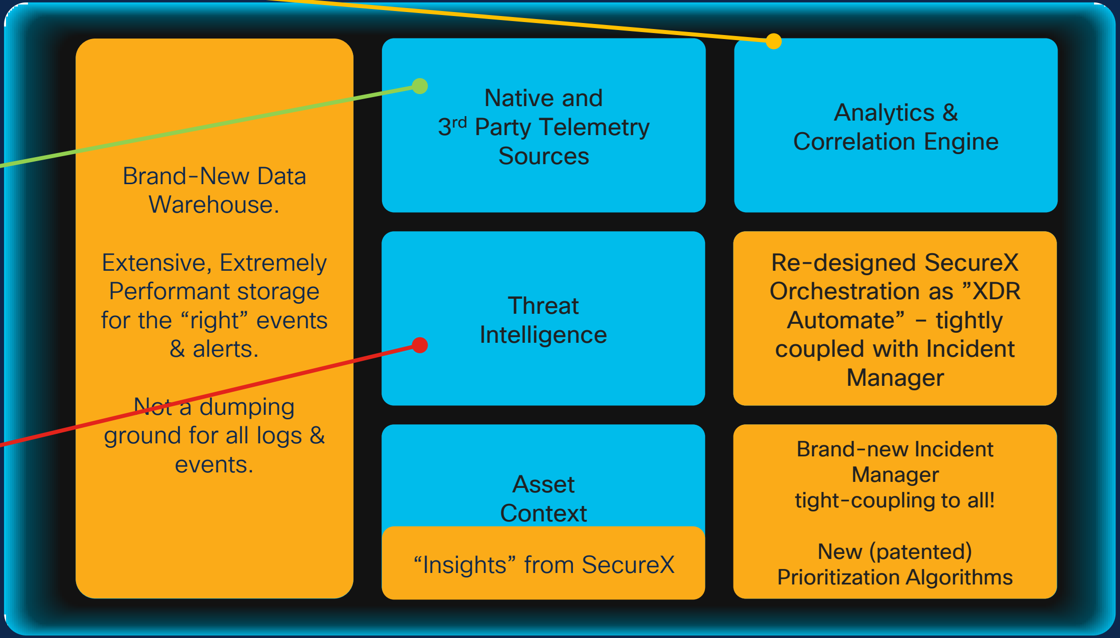
SCA's powerful analytics & correlation engine

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).



Brand-New Data Warehouse.

Extensive, Extremely Performant storage for the "right" events & alerts.

Not a dumping ground for all logs & events.

Native and 3^{rd} Party Telemetry Sources

Analytics & Correlation Engine

Threat Intelligence

Re-designed SecureX Orchestration as "XDR Automate" – tightly coupled with Incident Manager

Asset Context

"Insights" from SecureX

Brand-new Incident Manager tight-coupling to all!

New (patented) Prioritization Algorithms

Agenda

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

Incident Management & Workflow

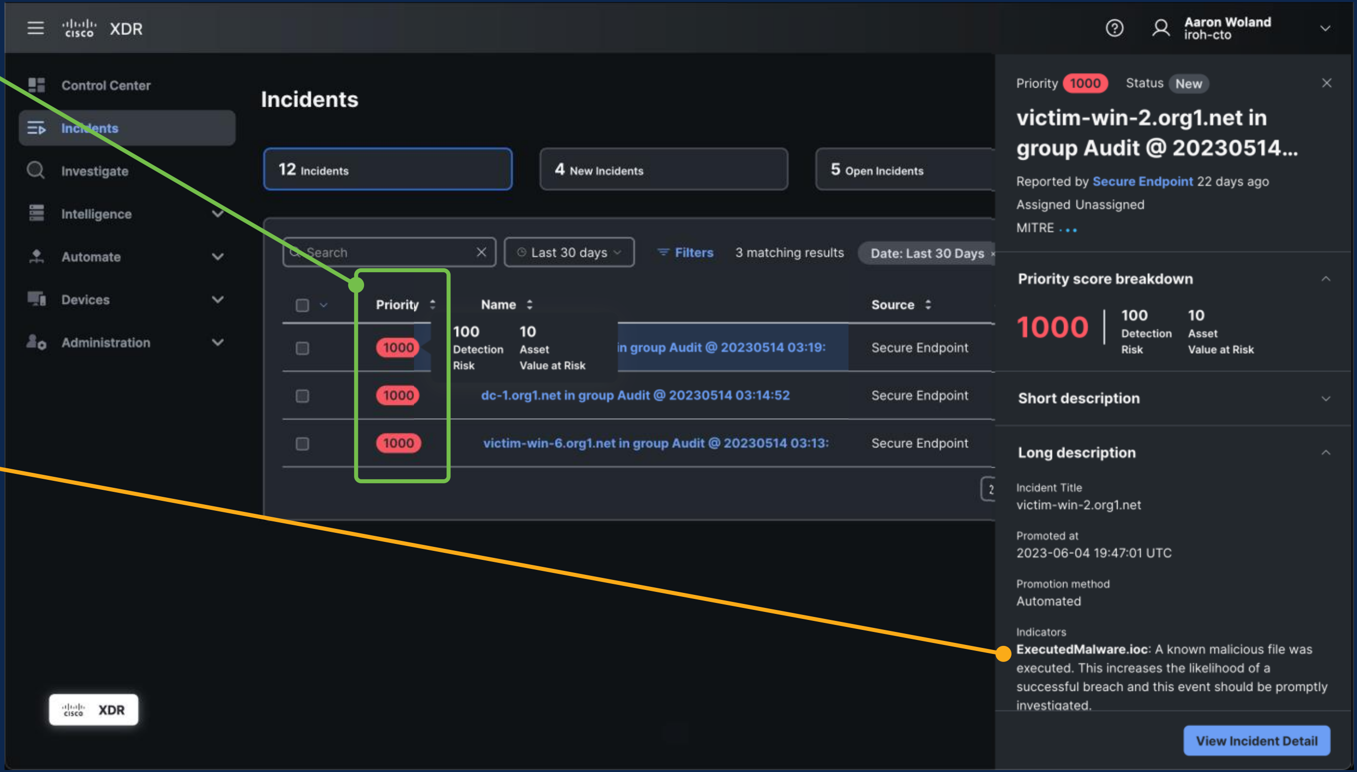
Cisco XDR – Incident Manager

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



Incidents

12 Incidents | 4 New Incidents | 5 Open Incidents

Search | Last 30 days | Filters | 3 matching results | Date: Last 30 Days

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

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

Short description

Long description

Incident Title
victim-win-2.org1.net

Promoted at
2023-06-04 19:47:01 UTC

Promotion method
Automated

Indicators
ExecutedMalware.ioc: A known malicious file was executed. This increases the likelihood of a successful breach and this event should be promptly investigated.

View Incident Detail

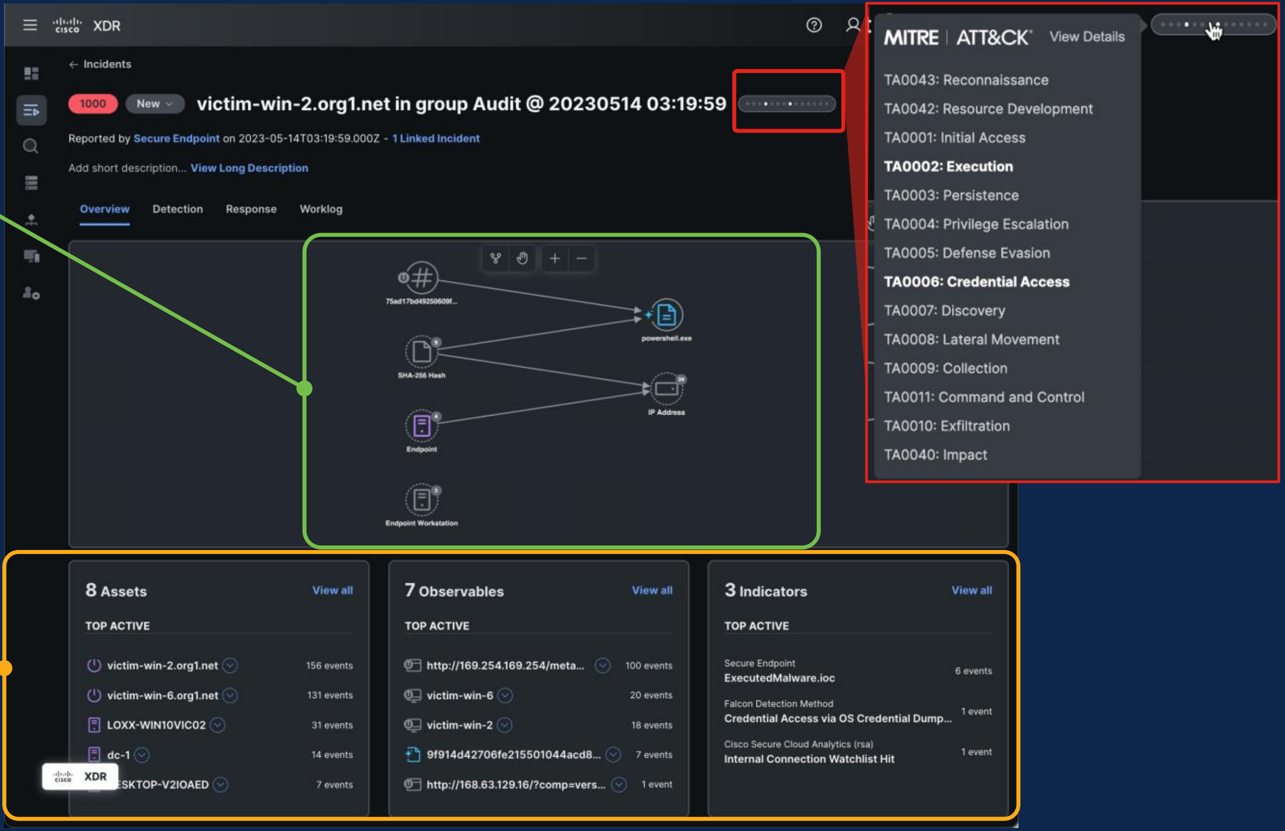
Cisco XDR – Incident Manager / Overview

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.



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

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
ESKTOP-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

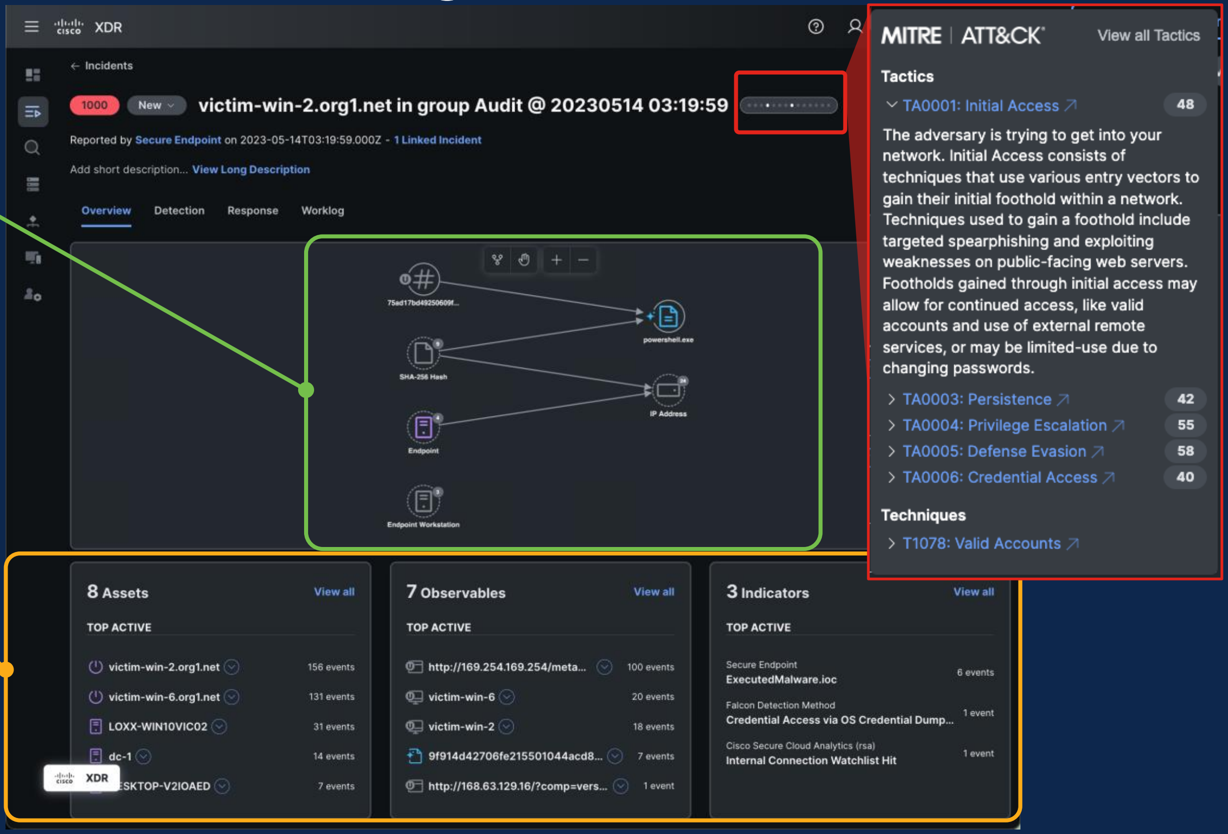
Cisco XDR – Incident Manager / Overview

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.



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

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.

Tactic	Count
TA0003: Persistence	42
TA0004: Privilege Escalation	55
TA0005: Defense Evasion	58
TA0006: Credential Access	40

Techniques

T1078: Valid Accounts

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
ESKTOP-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 Live!

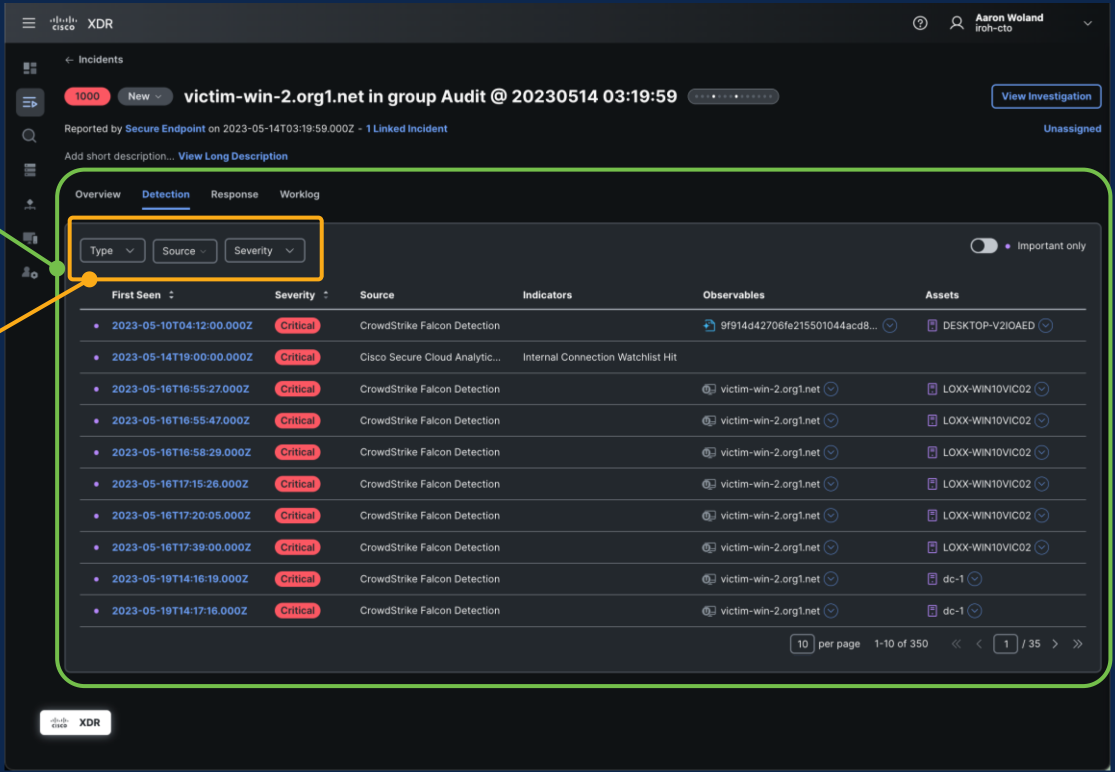
Cisco XDR – Incident Manager / Detection

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



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

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

10 per page 1-10 of 350 1 / 35

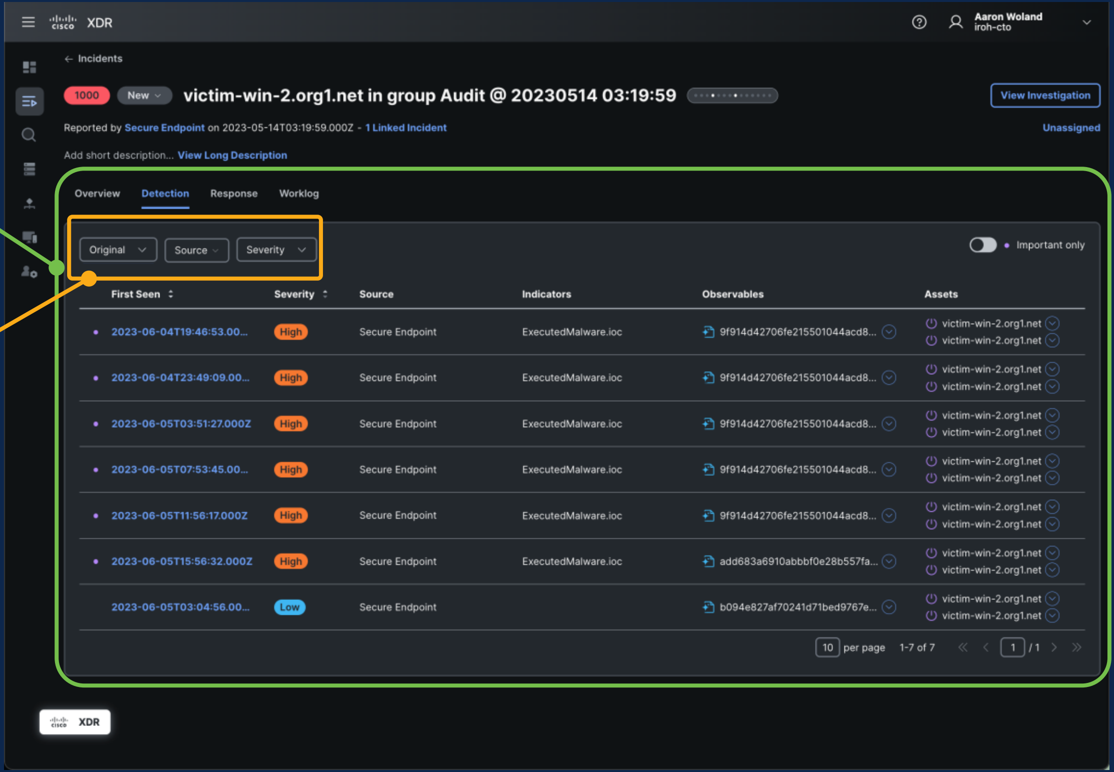
Cisco XDR – Incident Manager / Detection

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



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

First Seen	Severity	Source	Indicators	Observables	Assets
2023-06-04T19:46:53.00...	High	Secure Endpoint	ExecutedMalware.ioc	9f914d42706fe215501044acd8...	victim-win-2.org1.net victim-win-2.org1.net
2023-06-04T23:49:09.00...	High	Secure Endpoint	ExecutedMalware.ioc	9f914d42706fe215501044acd8...	victim-win-2.org1.net victim-win-2.org1.net
2023-06-05T03:51:27.000Z	High	Secure Endpoint	ExecutedMalware.ioc	9f914d42706fe215501044acd8...	victim-win-2.org1.net victim-win-2.org1.net
2023-06-05T07:53:45.00...	High	Secure Endpoint	ExecutedMalware.ioc	9f914d42706fe215501044acd8...	victim-win-2.org1.net victim-win-2.org1.net
2023-06-05T11:56:17.000Z	High	Secure Endpoint	ExecutedMalware.ioc	9f914d42706fe215501044acd8...	victim-win-2.org1.net victim-win-2.org1.net
2023-06-05T15:56:32.000Z	High	Secure Endpoint	ExecutedMalware.ioc	add683a6910abbbf0e28b557fa...	victim-win-2.org1.net victim-win-2.org1.net
2023-06-05T03:04:56.00...	Low	Secure Endpoint		b094e827af70241d71bed9767e...	victim-win-2.org1.net victim-win-2.org1.net

10 per page 1-7 of 7 1 / 1

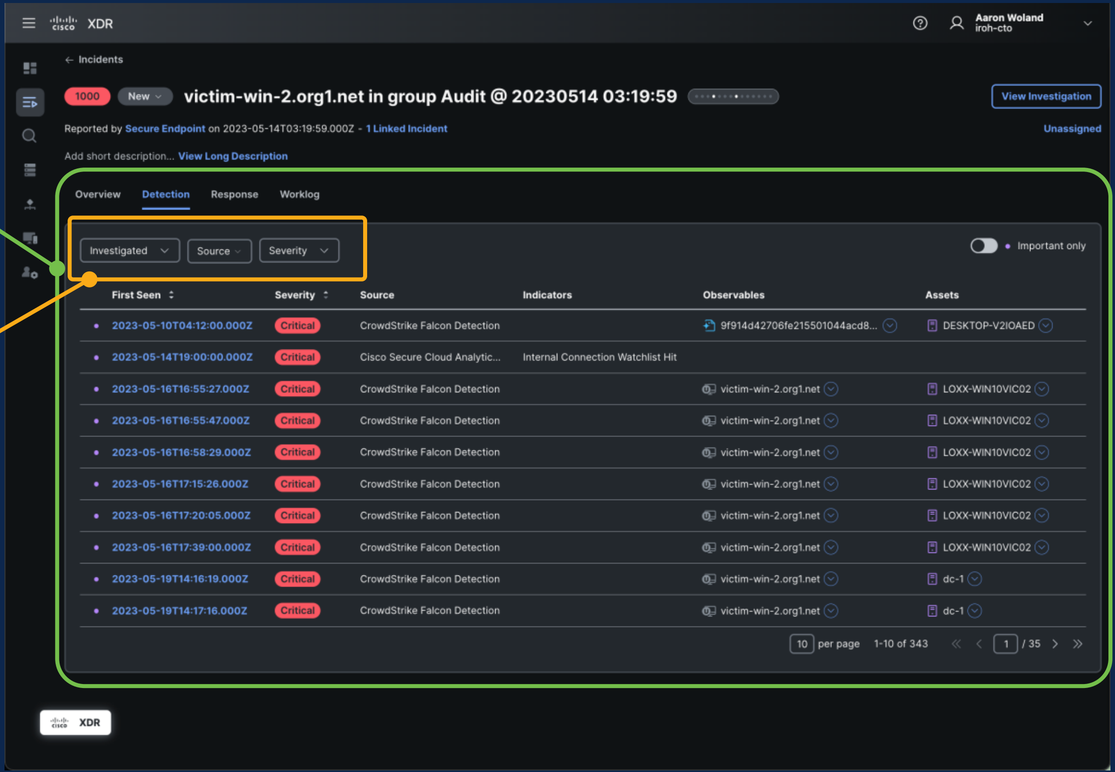
Cisco XDR – Incident Manager / Detection

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



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

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

10 per page 1-10 of 343 1 / 35

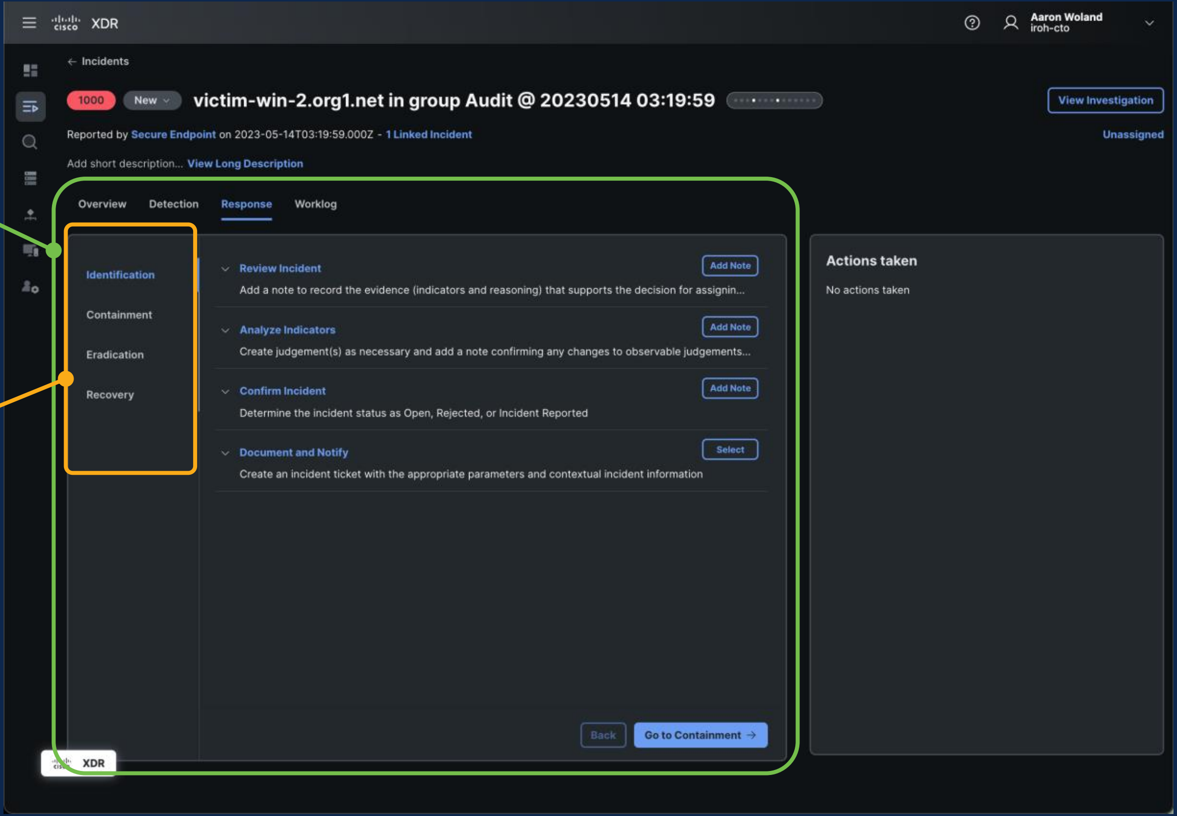
Cisco XDR – Incident Manager / Response

Responses

Content specific for the TTPs in the incident

Step Through

Identification ->
Containment ->
Eradication ->
Recovery



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

Add short description... View Long Description

Review Incident
Add a note to record the evidence (indicators and reasoning) that supports the decision for assignin...

Analyze Indicators
Create judgement(s) as necessary and add a note confirming any changes to observable judgements...

Confirm Incident
Determine the incident status as Open, Rejected, or Incident Reported

Document and Notify
Create an incident ticket with the appropriate parameters and contextual incident information

No actions taken

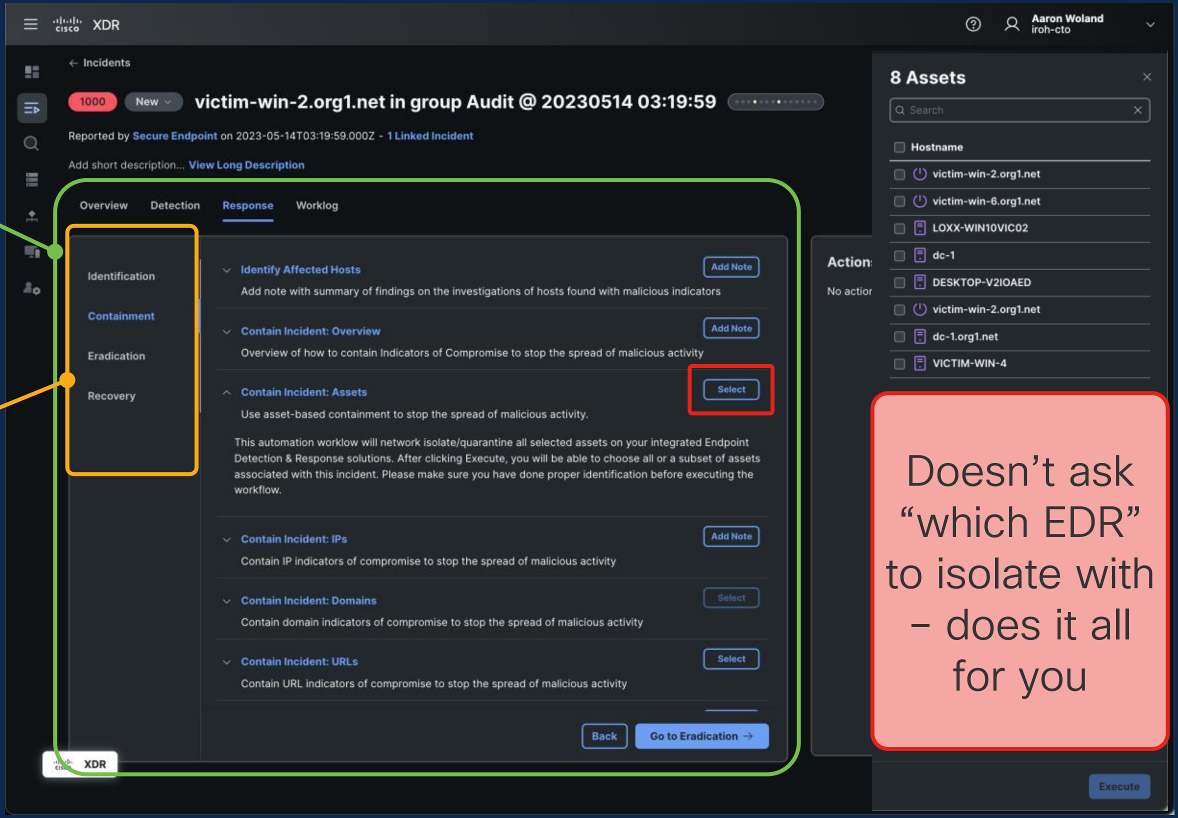
Cisco XDR – Incident Manager / Response

Responses

Content specific for the TTPs in the incident

Step Through

Identification ->
Containment ->
Eradication ->
Recovery



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

Identify Affected Hosts
Add note with summary of findings on the investigations of hosts found with malicious indicators

Contain Incident: Overview
Overview of how to contain Indicators of Compromise to stop the spread of malicious activity

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

This automation workflow will network isolate/quarantine all selected assets on your integrated Endpoint Detection & Response solutions. After clicking Execute, you will be able to choose all or a subset of assets associated with this incident. Please make sure you have done proper identification before executing the workflow.

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

Contain Incident: Domains
Contain domain indicators of compromise to stop the spread of malicious activity

Contain Incident: URLs
Contain URL indicators of compromise to stop the spread of malicious activity

8 Assets

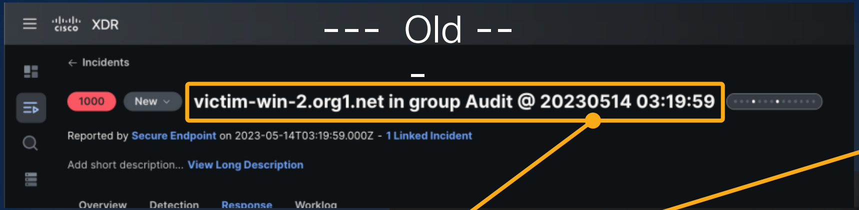
Search

- □ Hostname
- □ victim-win-2.org1.net
- □ victim-win-6.org1.net
- □ LOXX-WIN10VIC02
- □ dc-1
- □ DESKTOP-V2IOAED
- □ victim-win-2.org1.net
- □ dc-1.org1.net
- □ VICTIM-WIN-4

Doesn’t ask “which EDR” to isolate with – does it all for you

Cisco XDR – AI helping the analyst

--- Old --
-



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

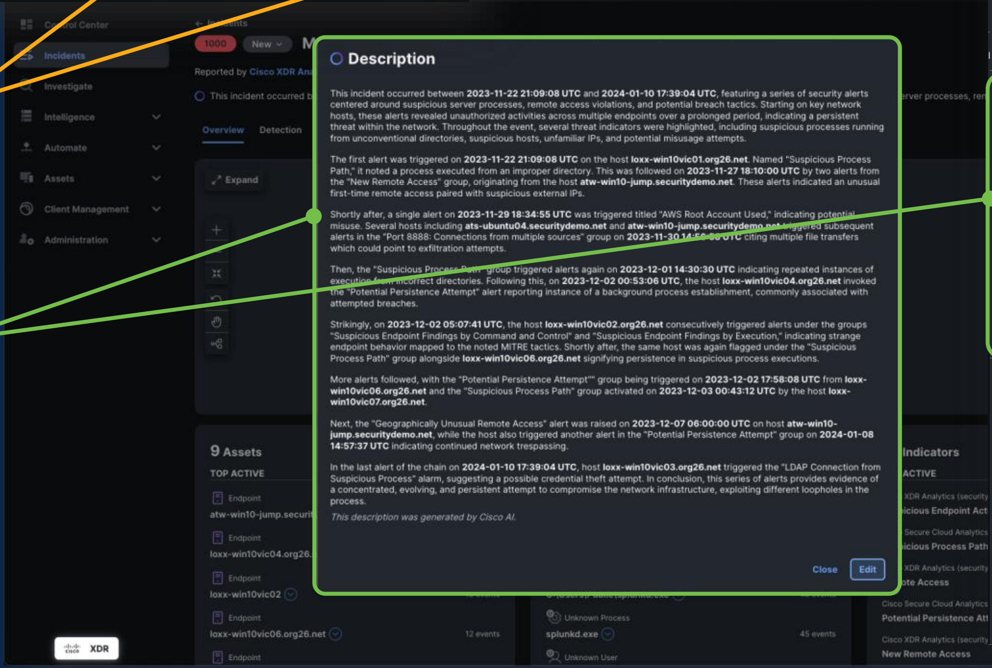
Add short description... View Long Description

Incident Names

Now generated by AI, making them much clearer.

Descriptions

Short and Long Descriptions are also generated by AI now. Significantly decreases effort of the Analyst



Description

This incident occurred between **2023-11-22 21:09:08 UTC** and **2024-01-10 17:39:04 UTC**, featuring a series of security alerts centered around suspicious server processes, remote access violations, and potential breach tactics. Starting on key network hosts, these alerts revealed unauthorized activities across multiple endpoints over a prolonged period, indicating a persistent threat within the network. Throughout the event, several threat indicators were highlighted, including suspicious processes running from unconventional directories, suspicious hosts, unfamiliar IPs, and potential misusage attempts.

The first alert was triggered on **2023-11-22 21:09:08 UTC** on the host **loxx-win10vic01.org26.net**. Named "Suspicious Process Path," it noted a process executed from an improper directory. This was followed on **2023-11-27 18:10:00 UTC** by two alerts from the "New Remote Access" group, originating from the host **atw-win10-jump.securitydemo.net**. These alerts indicated an unusual first-time remote access paired with suspicious external IPs.

Shortly after, a single alert on **2023-11-29 18:34:55 UTC** was triggered titled "AWS Root Account Used," indicating potential misuse. Several hosts including **ats-ubuntu04.securitydemo.net** and **atw-win10-jump.securitydemo.net** triggered subsequent alerts in the "Port 8888: Connections from multiple sources" group on **2023-11-30 14:[illegible] UTC** citing multiple file transfers which could point to exfiltration attempts.

Then, the "Suspicious Process Path" group triggered alerts again on **2023-12-01 14:30:30 UTC** indicating repeated instances of execution from incorrect directories. Following this, on **2023-12-02 00:53:06 UTC**, the host **loxx-win10vic04.org26.net** invoked the "Potential Persistence Attempt" alert reporting instance of a background process establishment, commonly associated with attempted breaches.

Strikingly, on **2023-12-02 05:07:41 UTC**, the host **loxx-win10vic02.org26.net** consecutively triggered alerts under the groups "Suspicious Endpoint Findings by Command and Control" and "Suspicious Endpoint Findings by Execution," indicating strange endpoint behavior mapped to the noted MITRE tactics. Shortly after, the same host was again flagged under the "Suspicious Process Path" group alongside **loxx-win10vic06.org26.net** signifying persistence in suspicious process executions.

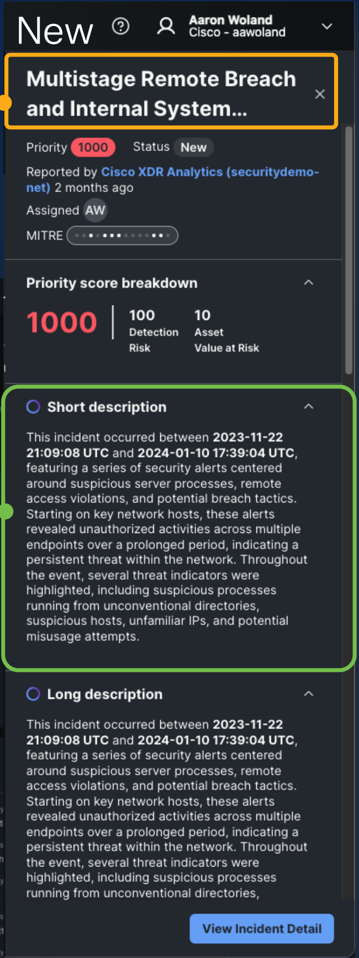
More alerts followed, with the "Potential Persistence Attempt"" group being triggered on **2023-12-02 17:58:08 UTC** from **loxx-win10vic06.org26.net** and the "Suspicious Process Path" group activated on **2023-12-03 00:43:12 UTC** by the host **loxx-win10vic07.org26.net**.

Next, the "Geographically Unusual Remote Access" alert was raised on **2023-12-07 06:00:00 UTC** on host **atw-win10-jump.securitydemo.net**, while the host also triggered another alert in the "Potential Persistence Attempt" group on **2024-01-08 14:57:37 UTC** indicating continued network trespassing.

In the last alert of the chain on **2024-01-10 17:39:04 UTC**, host **loxx-win10vic03.org26.net** triggered the "LDAP Connection from Suspicious Process" alarm, suggesting a possible credential theft attempt. In conclusion, this series of alerts provides evidence of a concentrated, evolving, and persistent attempt to compromise the network infrastructure, exploiting different loopholes in the process.

This description was generated by Cisco AI.

New



Multistage Remote Breach and Internal System...

Priority 1000 Status New

Reported by Cisco XDR Analytics (securitydemo-net) 2 months ago

Assigned AW

MITRE

Priority score breakdown

1000 | 100 Detection Risk | 10 Asset Value at Risk

Short description

This incident occurred between **2023-11-22 21:09:08 UTC** and **2024-01-10 17:39:04 UTC**, featuring a series of security alerts centered around suspicious server processes, remote access violations, and potential breach tactics. Starting on key network hosts, these alerts revealed unauthorized activities across multiple endpoints over a prolonged period, indicating a persistent threat within the network. Throughout the event, several threat indicators were highlighted, including suspicious processes running from unconventional directories, suspicious hosts, unfamiliar IPs, and potential misusage attempts.

Long description

This incident occurred between **2023-11-22 21:09:08 UTC** and **2024-01-10 17:39:04 UTC**, featuring a series of security alerts centered around suspicious server processes, remote access violations, and potential breach tactics. Starting on key network hosts, these alerts revealed unauthorized activities across multiple endpoints over a prolonged period, indicating a persistent threat within the network. Throughout the event, several threat indicators were highlighted, including suspicious processes running from unconventional directories,

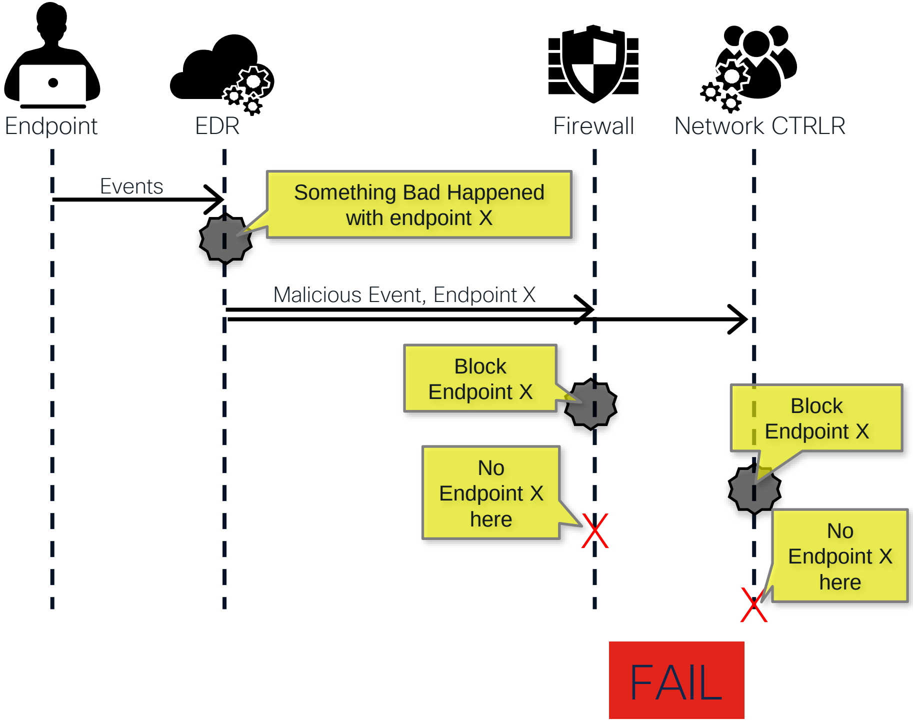
Agenda

- 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

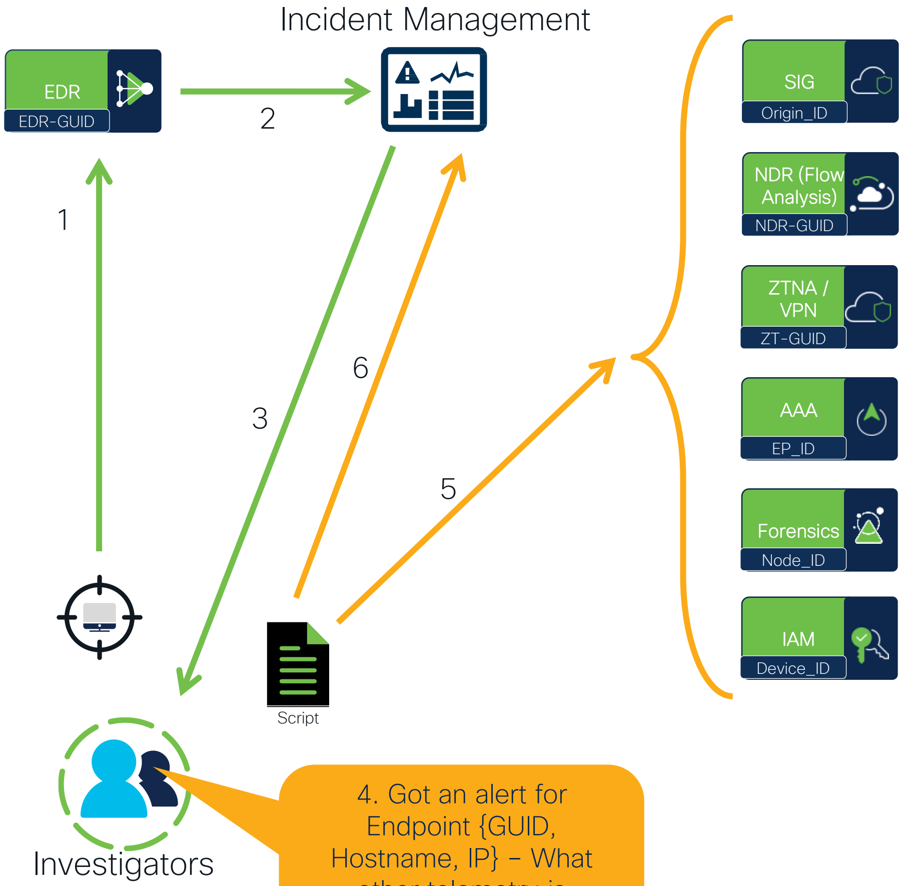


We need a common endpoint "object"

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



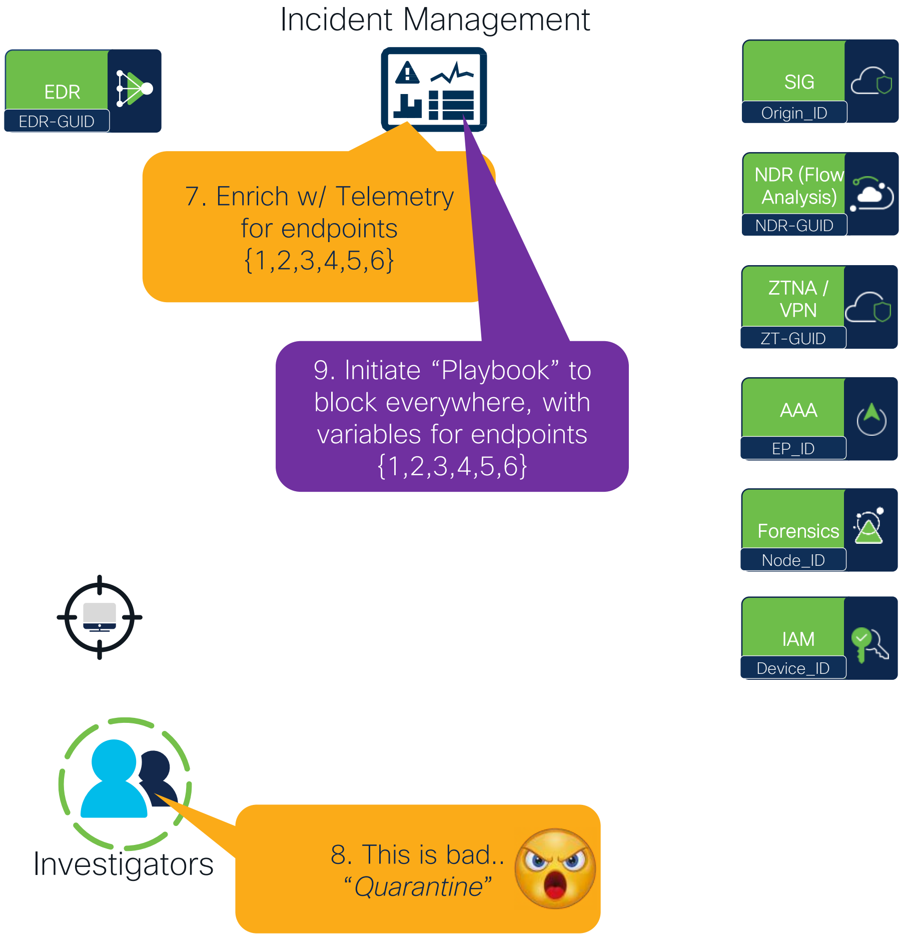
4. Got an alert for Endpoint {GUID, Hostname, IP} – What other telemetry is available for that EP @ that Time?

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



7. Enrich w/ Telemetry for endpoints {1,2,3,4,5,6}

9. Initiate "Playbook" to block everywhere, with variables for endpoints {1,2,3,4,5,6}

8. This is bad.. *"Quarantine"*

SOC Investigation Flow

Note: this is a Generic Example:

a) Playbook initiates isolation via EDR, using the EDR-GUID

b) Playbook blocks domain at SIG

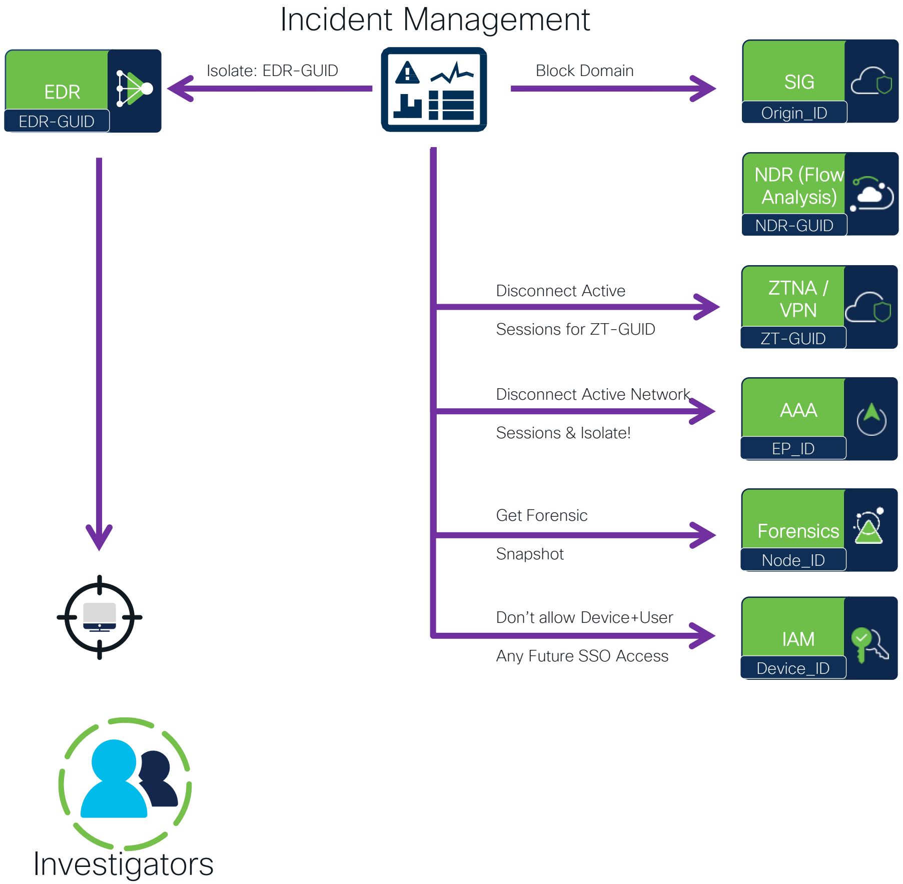
c) Playbook disconnects Active Sessions for ZTNA/VPN & AAA sessions

d) Playbook isolates the endpoint when new AAA session begins

e) Playbook initiates a new forensic snapshot of the infected host

f) Playbook informs IAM solution to deny any future attempts w/ User+Device combination

**Someone needed to build these flows



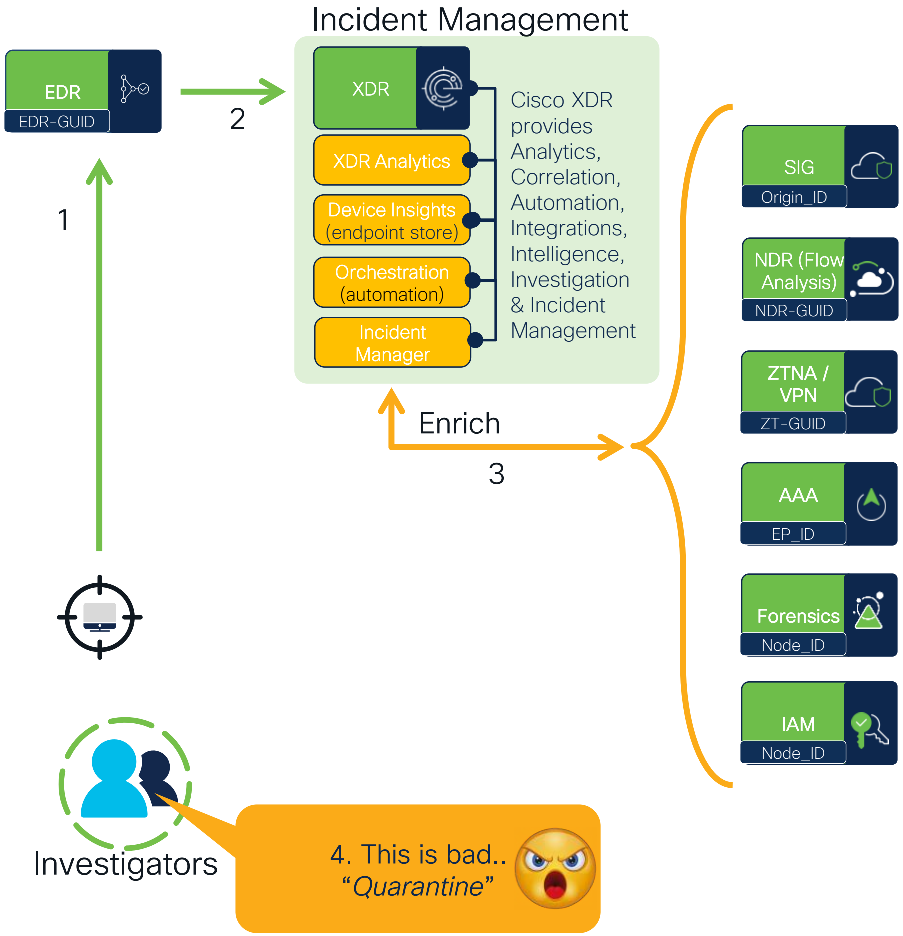
SOC Investigation Flow

With Cisco XDR:

1. EDR detects malicious activity
2. Alert sent to Cisco XDR

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

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



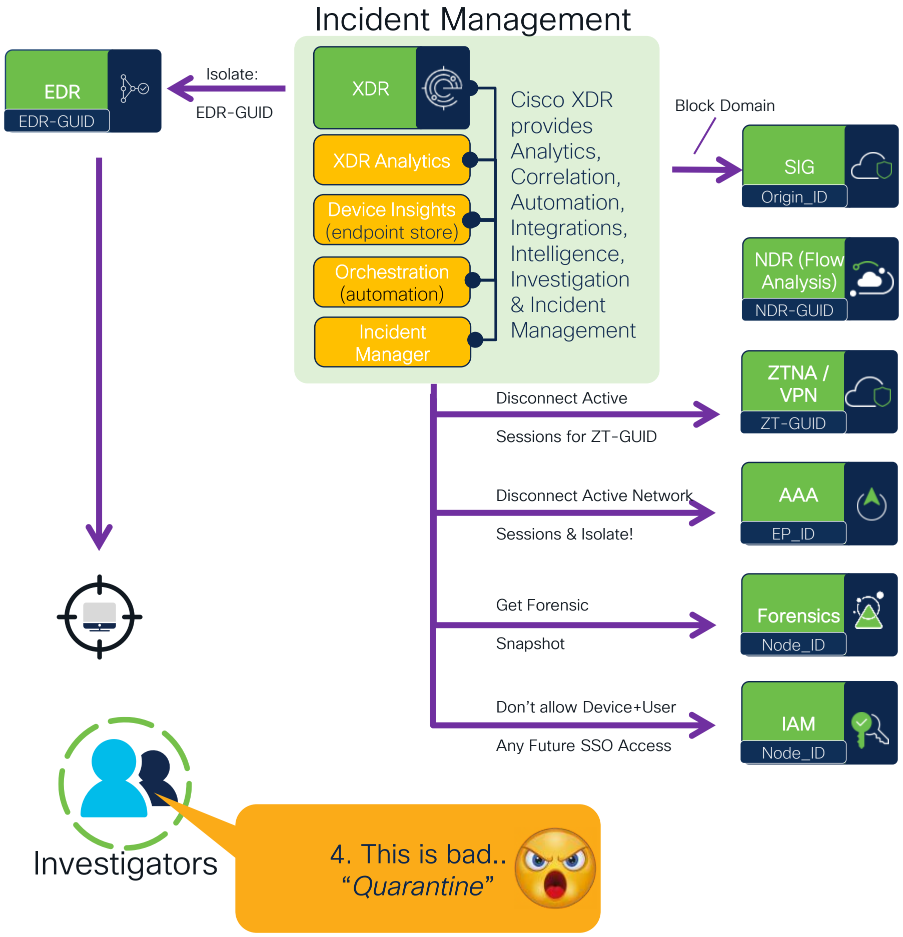
SOC Investigation Flow

With Cisco XDR:

1. EDR detects malicious activity
2. Alert sent to Cisco XDR

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

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



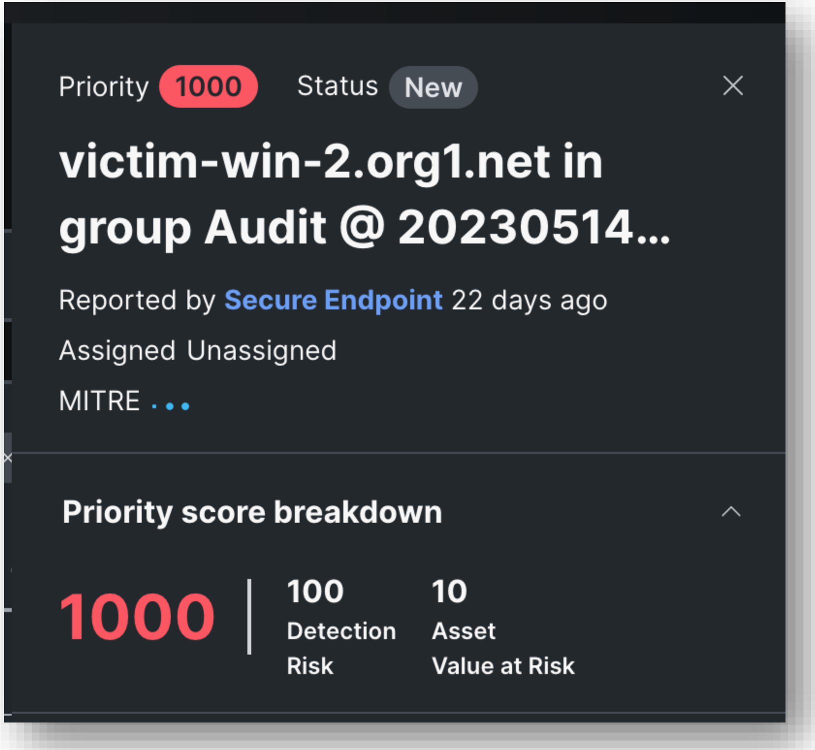
Let’s talk about that prioritization, shall we?

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

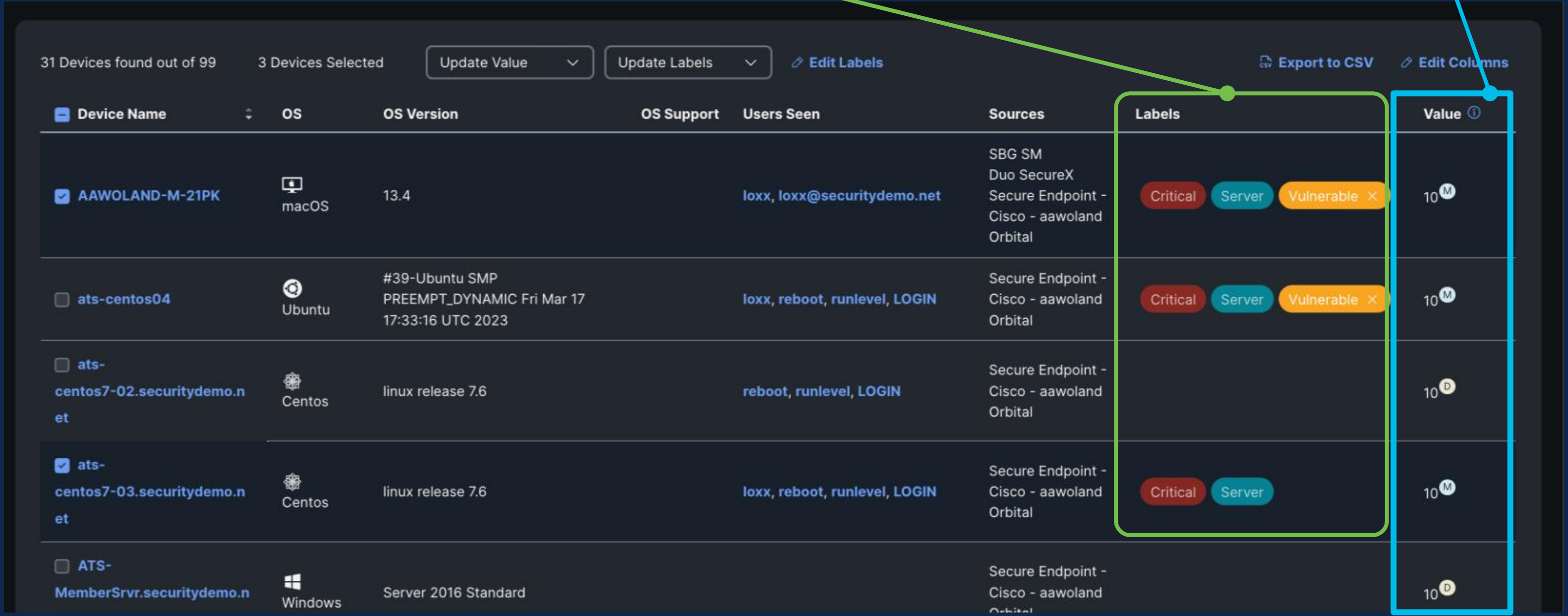
Device Insights in XDR adds some new things

Labels

Describe/group devices – manual and programmatically

Device Value

Value of 1-10.
1 = least valuable
10 = most valuable



31 Devices found out of 99

3 Devices Selected

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.n	Windows	Server 2016 Standard			Secure Endpoint - Cisco - aawoland Orbital		10 D

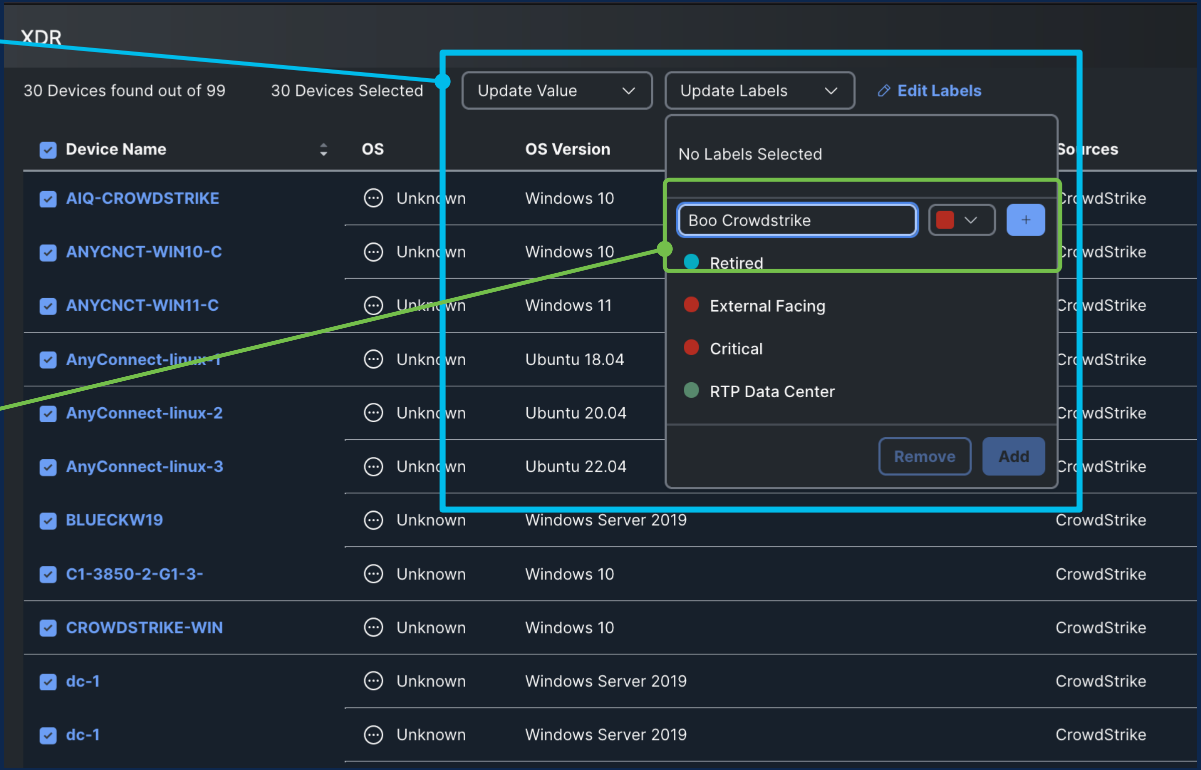
Device Insights in XDR adds some new things

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



XDR

30 Devices found out of 99 | 30 Devices Selected | Update Value | Update Labels | Edit Labels

No Labels Selected

Boo Crowdstrike | +

- ● Retired
- ● External Facing
- ● Critical
- ● RTP Data Center

Remove | Add

☑ 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

cisco Live!

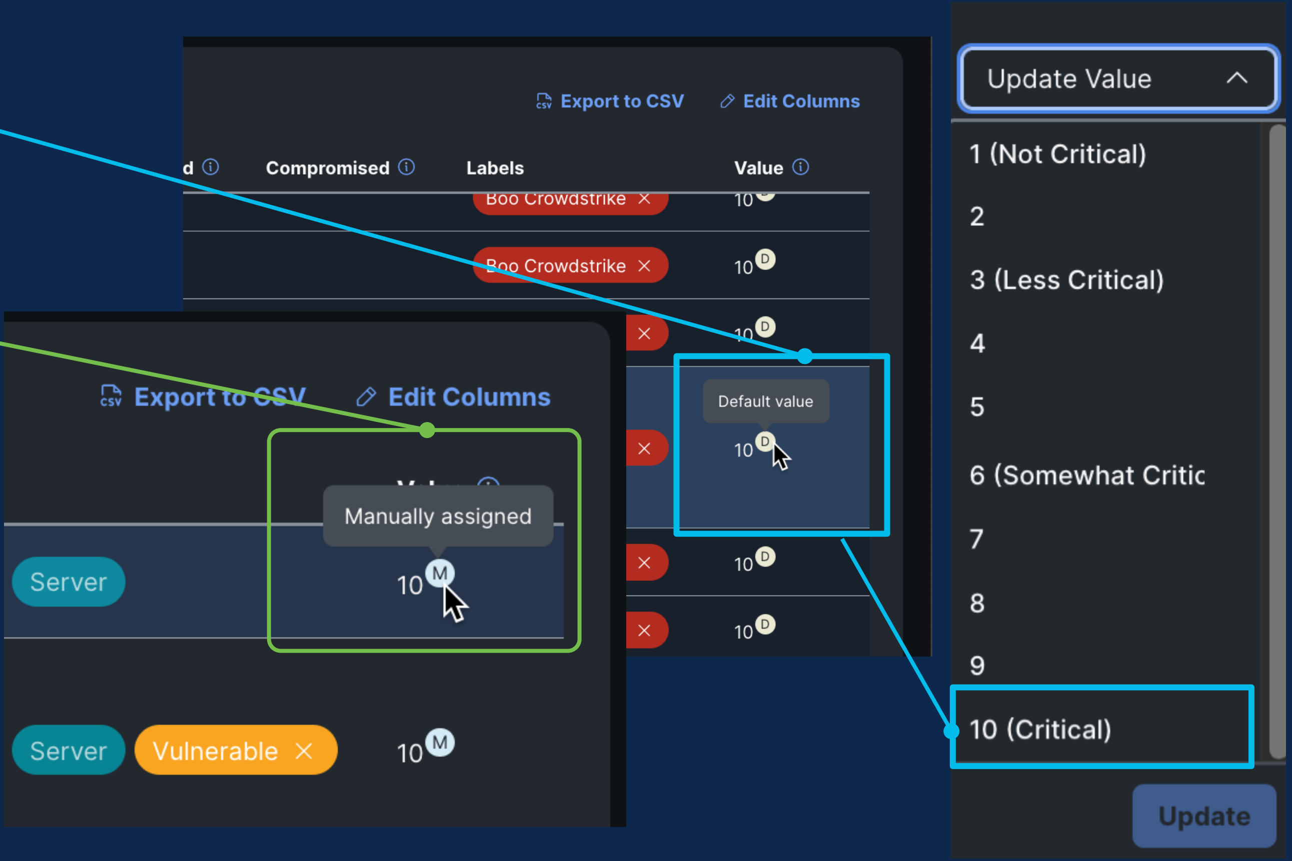
Device Insights in XDR adds some new things

Default Value

The default value is 10 (most valuable)

Manually Assigned

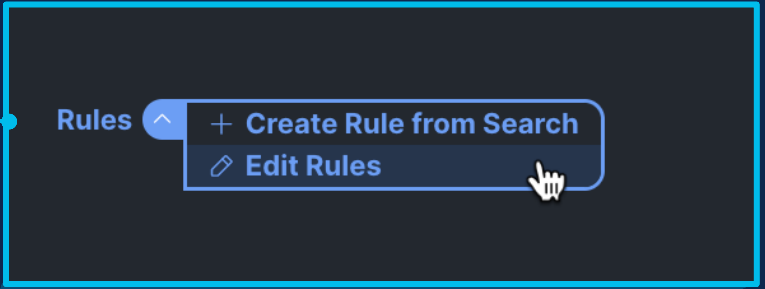
The value is tagged if its manually assigned, which will always "win" in a conflict

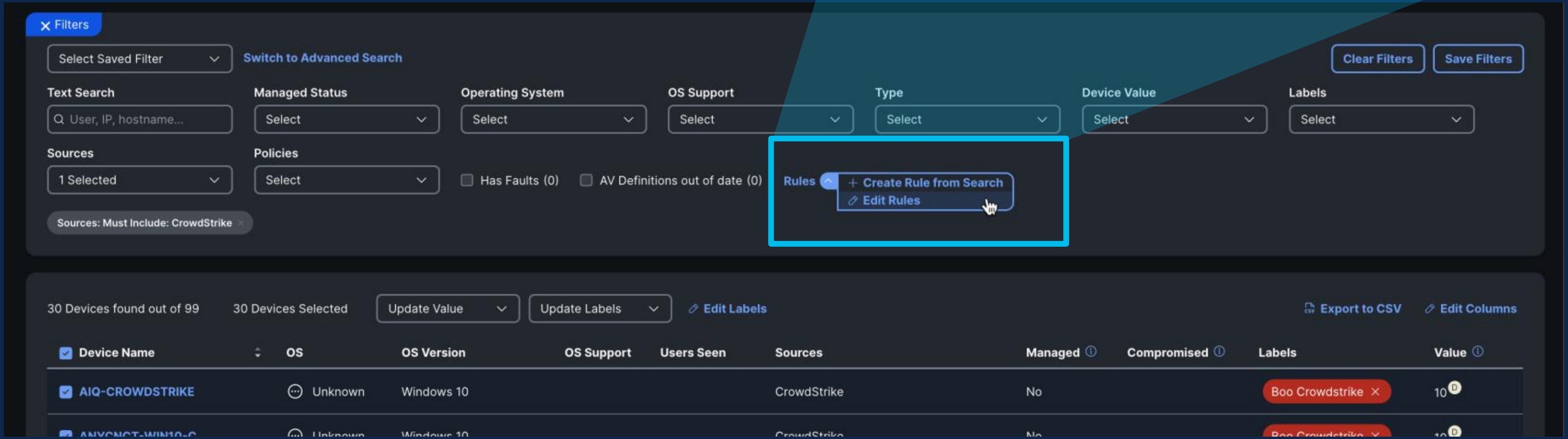


Device Insights in XDR adds some new things

Rules Engine

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





Select Saved Filter

Text Search: User, IP, hostname...

Managed Status: Select

Operating System: Select

OS Support: Select

Type: Select

Device Value: Select

Labels: Select

Sources: 1 Selected

Policies: Select

□ Has Faults (0)

□ AV Definitions out of date (0)

Sources: Must Include: CrowdStrike

30 Devices found out of 99

30 Devices Selected

☑ Device Name	OS	OS Version	OS Support	Users Seen	Sources	Managed	Compromised	Labels	Value
☑ AIQ-CROWDSTRIKE	Unknown	Windows 10			CrowdStrike	No		Boo Crowdstrike ×	10 D
☑ ANYCNCT-WIN10-C	Unknown	Windows 10			CrowdStrike	No		Boo Crowdstrike ×	10 D

Device Insights in XDR adds some new things

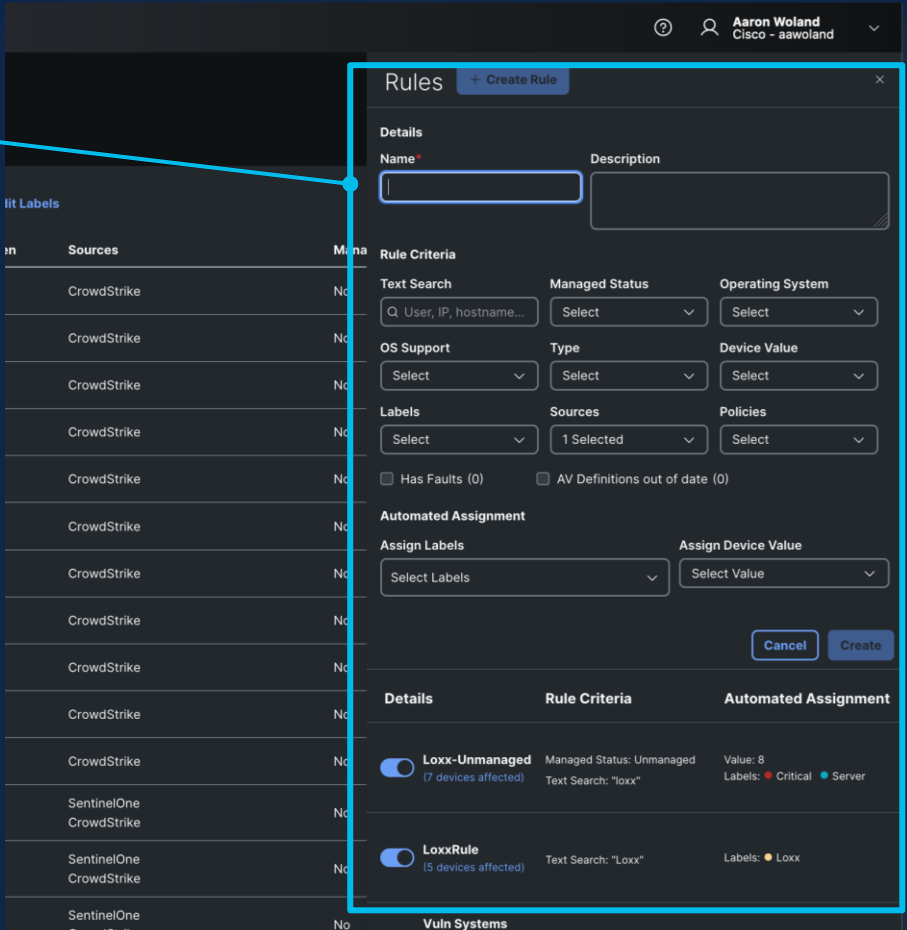
Rules Engine

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.



Rules

Details

Name*

Description

Rule Criteria

Text Search	Managed Status	Operating System
User, IP, hostname...	Select	Select

OS Support	Type	Device Value
Select	Select	Select

Labels	Sources	Policies
Select	1 Selected	Select

☐ Has Faults (0) ☐ AV Definitions out of date (0)

Automated Assignment

Assign Labels	Assign Device Value
Select Labels	Select Value

Cancel Create

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
Vuln Systems		

cisco Live!

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

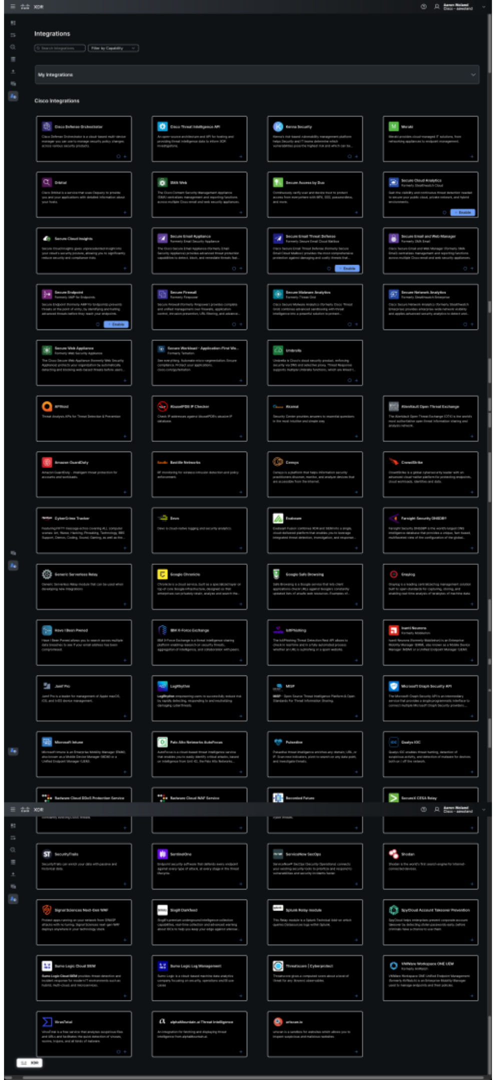
Email Threat Defense (ETD)

Umbrella

Also 3rd Parties

- EDR:
  - Crowstrike
  - Sentinel One
  - MSFT Defender
- NDR:
  - Dark Trace
  - ExtraHop

...And other intel sources



XDR

Integrations

Search Integrations

Filter by Capability

My Integrations

Cisco Integrations

Cisco Defense Orchestrator

Cisco Threat Intelligence API

Kenna Security

Meraki

Orbital

SMA Web

Secure Access by Duo

Secure Cloud Analytics
Formerly Stealthwatch Cloud

Secure Cloud Insights

Secure Email Appliance
Formerly Email Security Appliance

Secure Email Threat Defense
Formerly Secure Email Cloud Mailbox

Secure Email and Web Manager
Formerly SMA Email

Secure Endpoint
Formerly AMP for Endpoints

Secure Firewall
Formerly Firepower

Secure Malware Analytics
Formerly Threat Grid

Secure Network Analytics
Formerly Stealthwatch Enterprise

Secure Web Appliance
Formerly Web Security Appliance

Secure Workload - Application First Wo...
Formerly Tetration

Umbrella

APIVoid

AbuseIPDB IP Checker

Akamai

AlienVault Open Threat Exchange

Amazon GuardDuty

Bastille Networks

Censys

CrowdStrike

CyberCrime Tracker

Devo

Exabeam

Farsight Security DNSDB

Generic Serverless Relay

Google Chronicle

Google Safe Browsing

Graylog

Have I Been Pwned

IBM X-Force Exchange

IsItPhishing

Ivanti Neurons
Formerly MobileIron

Jamf Pro

LogRhythm

MISP

Microsoft Graph Security API

Microsoft Intune

Palo Alto Networks AutoFocus

Pulsedive

Qualys IOC

Radware Cloud DDoS Protection Service

Radware Cloud WAF Service

Recorded Future

SecureX CESA Relay

SecurityTrails

SentinelOne

ServiceNow SecOps

Shodan

Signal Sciences Next-Gen WAF

Sixgill Darkfeed

Splunk Relay module

SpyCloud Account Takeover Prevention

Sumo Logic Cloud SIEM

Sumo Logic Log Management

Threatscore | Cyberprotect

VMWare Workspace ONE UEM
Formerly AirWatch

VirusTotal

alphaMountain.ai Threat Intelligence

urlscan.io

cisco Live!

"I think NVM is Cisco's best kept secret weapon"

-Tom Gillis, SVP & GM – Cisco Secure

~250 million endpoints delivering the most comprehensive set of security services to more than

80,000+ customers worldwide

AnyConnect has been rebranded

AnyConnect

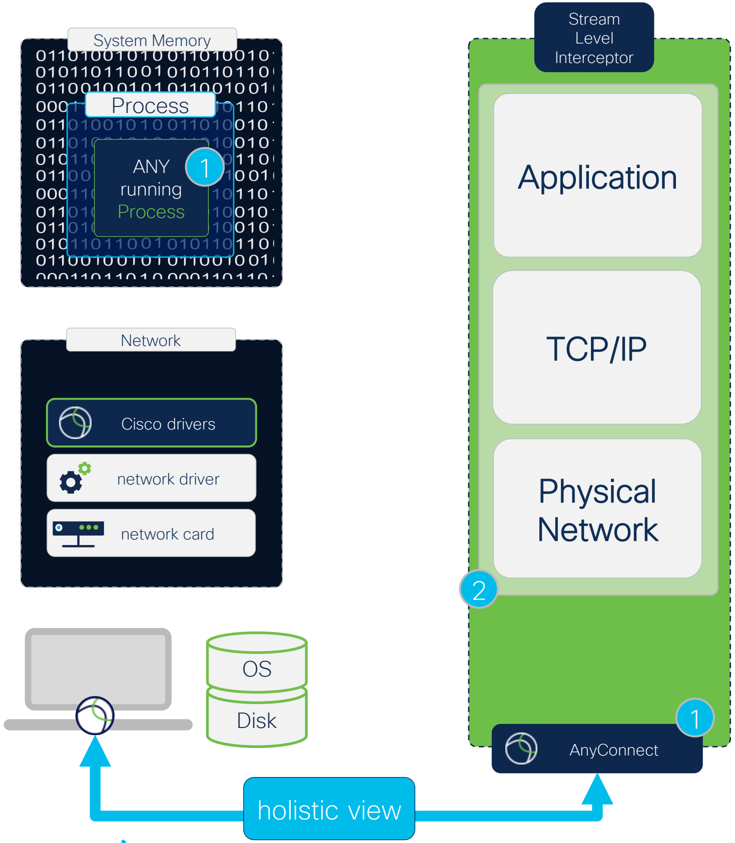
+

Cisco Secure Endpoint (AMP)

=

Cisco Secure Client

Stream Level Interceptor



1

- 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

2

- 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?

SOC = Security Operations Center

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

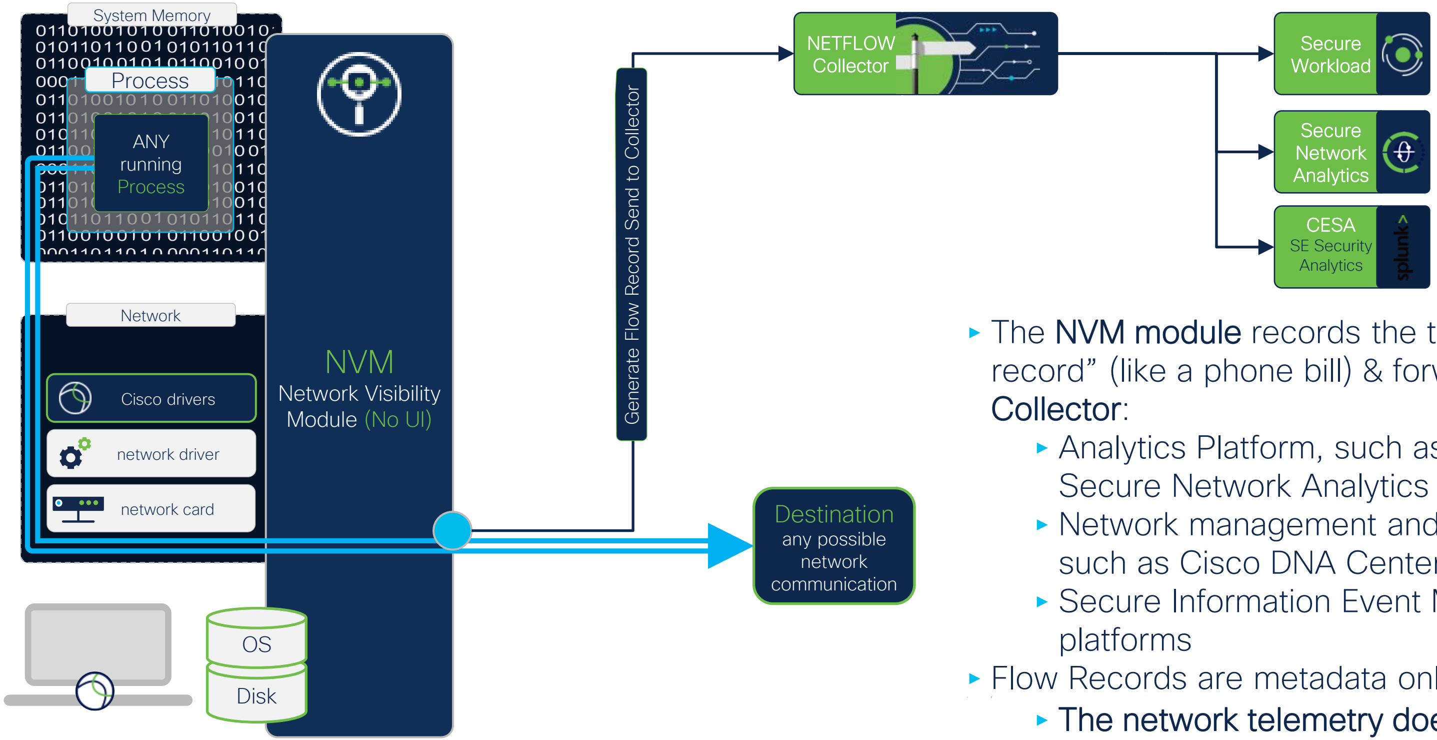
- SANS Instructor
SEC530: Defensible Network Architectures

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”.

Conceived by Vinny Parla back in 2011
Been a product almost since then!

Network Visibility Module

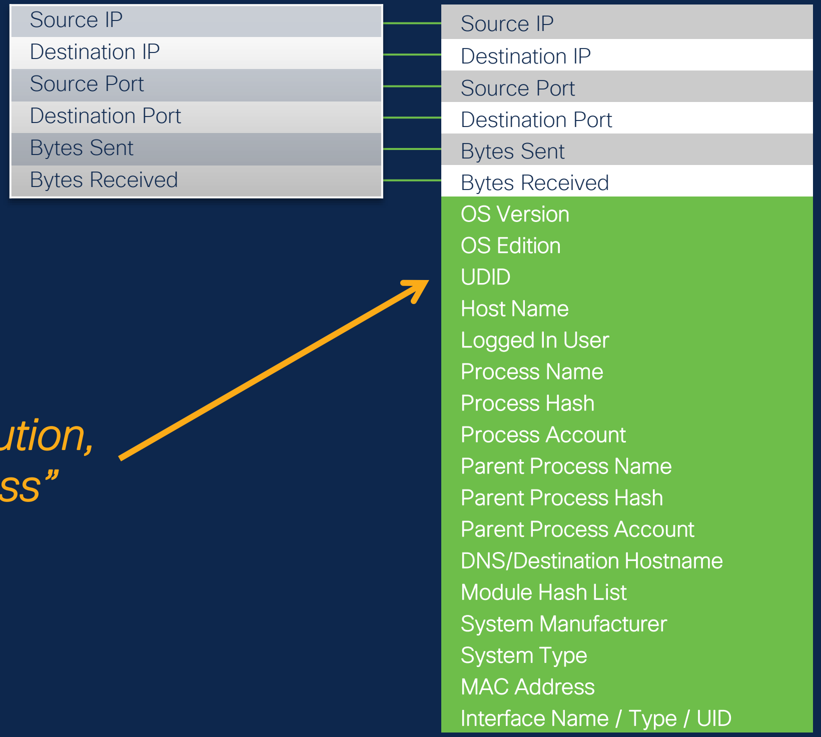


- The **NVM module** records the traffic into a “flow record” (like a phone bill) & forwards it to a **Netflow Collector**:
    - Analytics Platform, such as Secure Workload, Secure Network Analytics or others
    - Network management and automation platforms, such as Cisco DNA Center
    - Secure Information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

Network + Endpoint Visibility Together

Netflow/IPFIX

NVM (IPFIX Formatted)



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

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

True device attribution,
Not just "IP Address"

Deep Endpoint Visibility

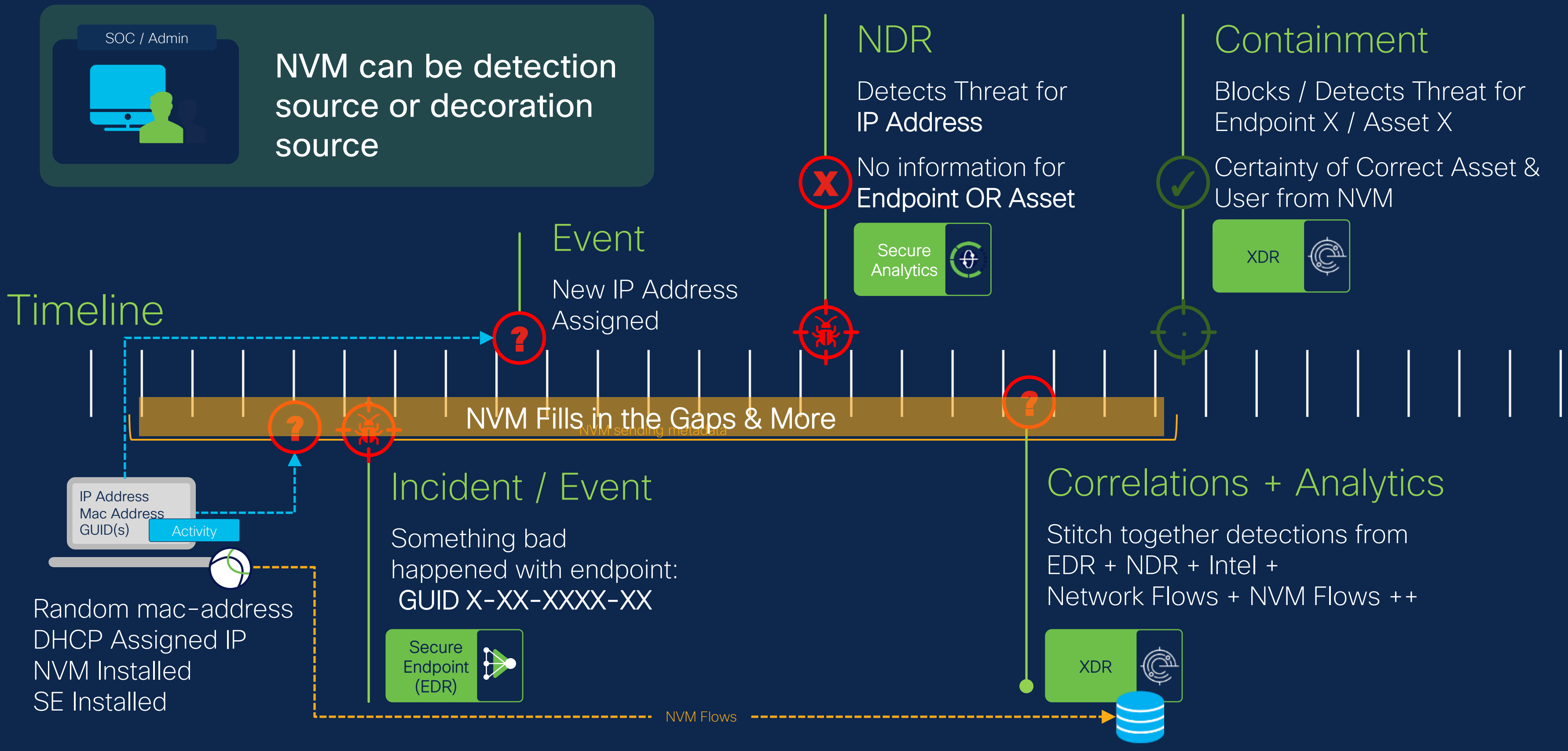
User
Traffic Stats
Processes
Applications
SaaS Used
Accounts
Destinations
Machine Details

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

Investigation Timeline



NVM can be detection source or decoration source

Timeline

NVM Fills in the Gaps & More

Event

New IP Address Assigned

NDR

Detects Threat for **IP Address**

No information for **Endpoint OR Asset**

Containment

Blocks / Detects Threat for Endpoint X / Asset X

Certainty of Correct Asset & User from NVM

Random mac-address
DHCP Assigned IP
NVM Installed
SE Installed

Incident / Event

Something bad happened with endpoint:
GUID X-XX-XXXX-XX

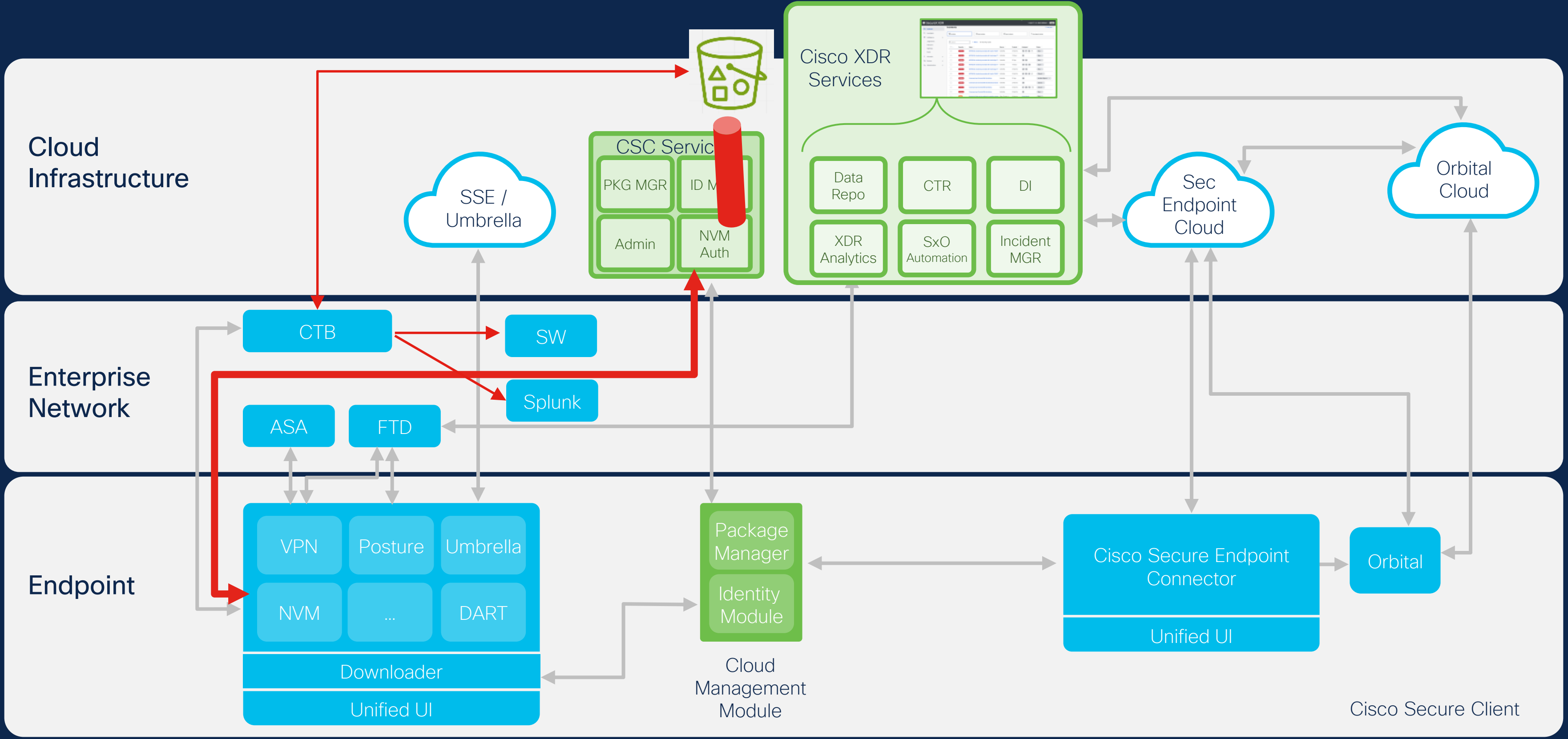
Correlations + Analytics

Stitch together detections from EDR + NDR + Intel + Network Flows + NVM Flows ++

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

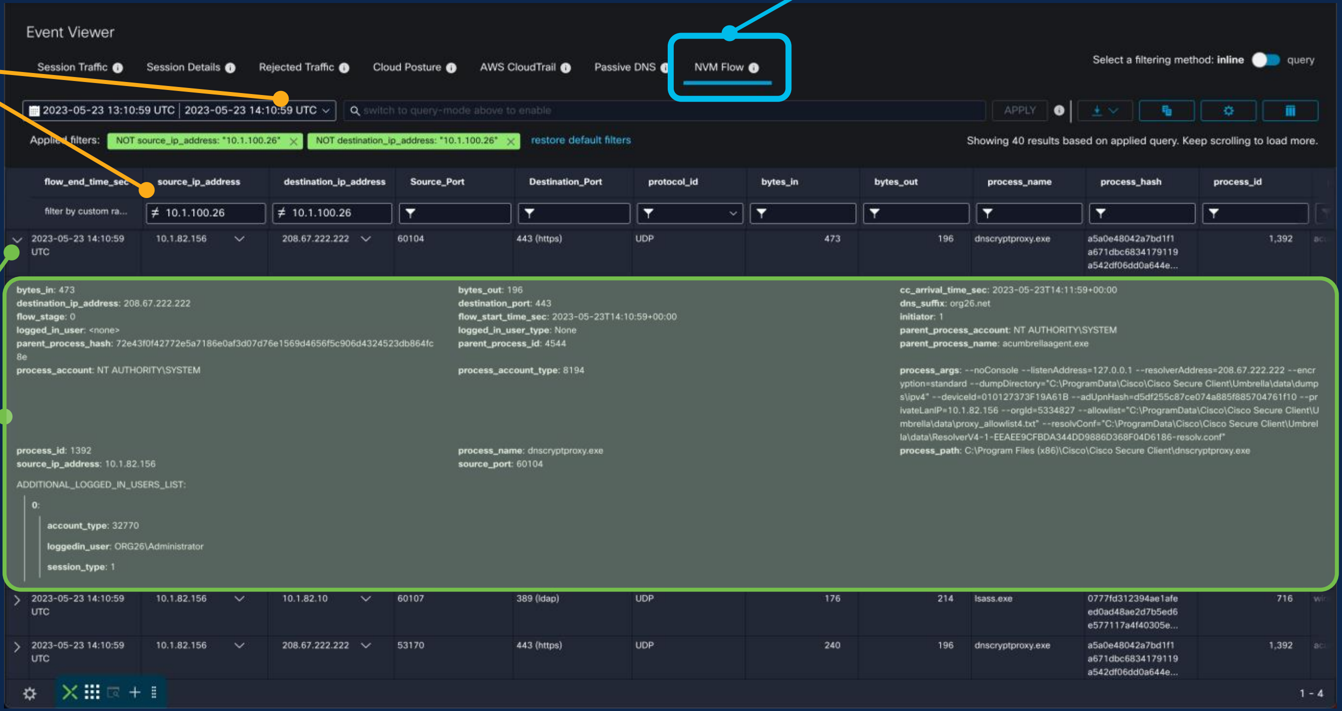
INSTANT FILTERS

Search activity per attribute or many with advanced search.

Telemetry Details

See the detailed telemetry collected from the flow

New NVM Flows Tab



Event Viewer

2023-05-23 13:10:59 UTC | 2023-05-23 14:10:59 UTC

Applied filters: NOT source_ip_address: "10.1.100.26" NOT destination_ip_address: "10.1.100.26" restore default filters

Showing 40 results based on applied query. Keep scrolling to load more.

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
filter by custom ra...	≠ 10.1.100.26	≠ 10.1.100.26								
2023-05-23 14:10:59 UTC	10.1.82.156	208.67.222.222	60104	443 (https)	UDP	473	196	dnscryptproxy.exe	a5a0e48042a7bd1f1 a671dbc6834179119 a542df06dd0a644e...	1,392
2023-05-23 14:10:59 UTC	10.1.82.156	10.1.82.10	60107	389 (ldap)	UDP	176	214	lsass.exe	0777fd312394ae1afe ed0ad48ae2d7b5ed6 e577117a4f40305e...	716
2023-05-23 14:10:59 UTC	10.1.82.156	208.67.222.222	53170	443 (https)	UDP	240	196	dnscryptproxy.exe	a5a0e48042a7bd1f1 a671dbc6834179119 a542df06dd0a644e...	1,392

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:

0:

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

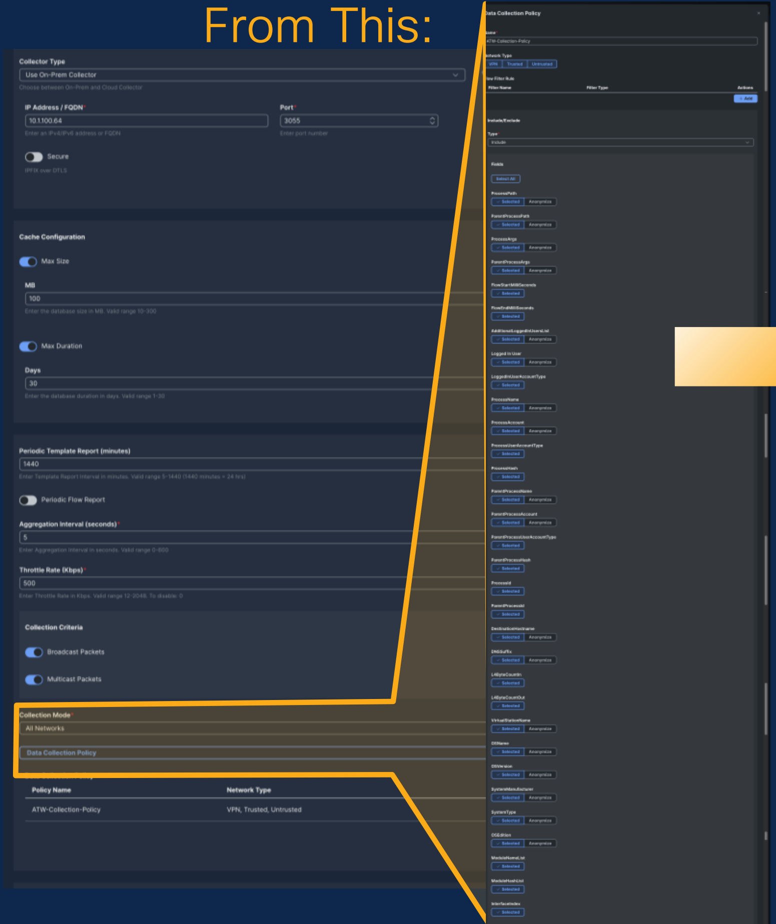
process_name: dnscryptproxy.exe
source_port: 60104

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 --encryption=standard --dumpDirectory="C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\data\dumps\ipv4" --deviceId=010127373F19A61B --adUpnHash=d5df255c87ce074a885f885704761f10 --privateLanIP=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-EEAEE9CFBDA344DD9886D368F04D6186-resolv.conf"
process_path: C:\Program Files (x86)\Cisco\Cisco Secure Client\dnscryptproxy.exe

Simplicity! NVM Profiles

From This:



Collector Type

Use On-Prem Collector

Choose between On-Prem and Cloud Collector

IP Address / FQDN*

10.1.100.64

Enter an IPv4/IPv6 address or FQDN

Port*

3055

Enter port number

Secure

IPFIX over DTLS

Cache Configuration

Max Size

MB

100

Enter the database size in MB. Valid range 10-300

Max Duration

Days

30

Enter the database duration in days. Valid range 1-30

Periodic Template Report (minutes)

1440

Enter Template Report Interval in minutes. Valid range 5-1440 (1440 minutes = 24 hrs)

Periodic Flow Report

Aggregation Interval (seconds)*

5

Enter Aggregation Interval in seconds. Valid range 0-600

Throttle Rate (Kbps)*

500

Enter Throttle Rate in Kbps. Valid range 12-2048. To disable: 0

Collection Criteria

Broadcast Packets

Multicast Packets

Collection Mode*

All Networks

Data Collection Policy

Policy Name	Network Type
ATW-Collection-Policy	VPN, Trusted, Untrusted

Data Collection Policy

Name*

ATW-Collection-Policy

Network Type

VPN | Trusted | Untrusted

Flow Filter Rule

Filter Name	Filter Type	Actions

Include/Exclude

Type*

Include

Fields

Select All

ProcessPath: ✓ Selected | Anonymize

ParentProcessPath: ✓ Selected | Anonymize

ProcessArgs: ✓ Selected | Anonymize

ParentProcessArgs: ✓ Selected | Anonymize

FlowStartMilliSeconds: ✓ Selected

FlowEndMilliSeconds: ✓ Selected

AdditionalLoggedInUsersList: ✓ Selected | Anonymize

Logged In User: ✓ Selected | Anonymize

LoggedInUserAccountType: ✓ Selected

ProcessName: ✓ Selected | Anonymize

ProcessAccount: ✓ Selected | Anonymize

ProcessUserAccountType: ✓ Selected

ProcessHash: ✓ Selected

ParentProcessName: ✓ Selected | Anonymize

ParentProcessAccount: ✓ Selected | Anonymize

ParentProcessUserAccountType: ✓ Selected

ParentProcessHash: ✓ Selected

ProcessId: ✓ Selected

ParentProcessId: ✓ Selected

DestinationHostname: ✓ Selected | Anonymize

DNSSuffix: ✓ Selected | Anonymize

L4ByteCountIn: ✓ Selected

L4ByteCountOut: ✓ Selected

VirtualStationName: ✓ Selected | Anonymize

OSName: ✓ Selected | Anonymize

OSVersion: ✓ Selected | Anonymize

SystemManufacturer: ✓ Selected | Anonymize

SystemType: ✓ Selected | Anonymize

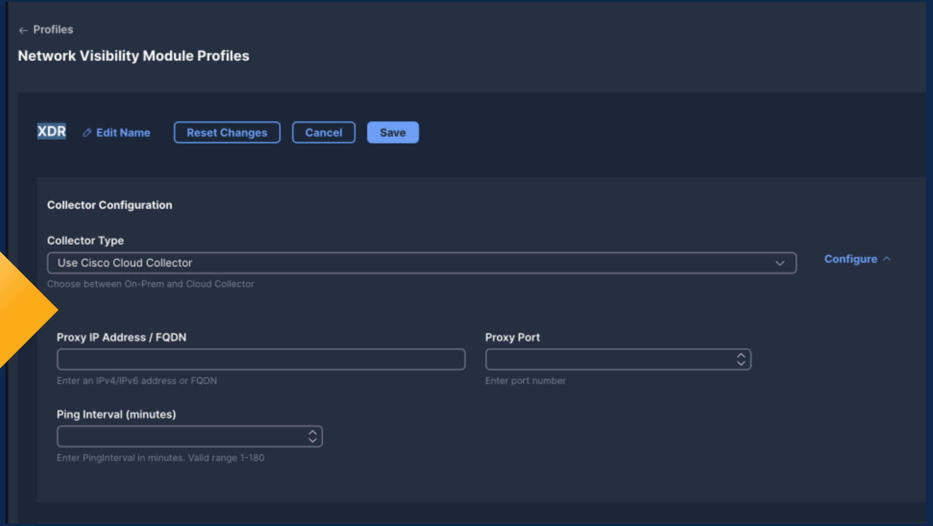
OSEdition: ✓ Selected | Anonymize

ModuleNameList: ✓ Selected

ModuleHashList: ✓ Selected

InterfaceIndex: ✓ Selected

To This:



← Profiles

Network Visibility Module Profiles

XDR

Collector Configuration

Collector Type

Use Cisco Cloud Collector

Configure ^

Choose between On-Prem and Cloud Collector

Proxy IP Address / FQDN

Enter an IPv4/IPv6 address or FQDN

Proxy Port

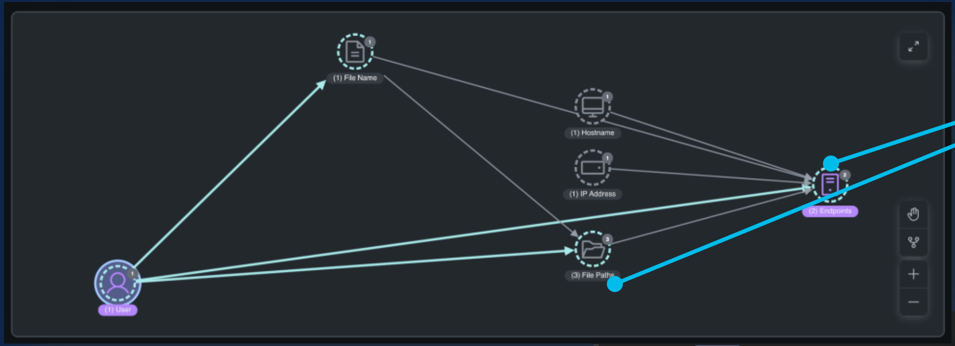
Enter port number

Ping Interval (minutes)

Enter PingInterval in minutes. Valid range 1-180

Default XDR Deployment
- Default CM Profile
- Default NVM Profile
Just download & install, no config needed

NVM Provides Detections and Decorations

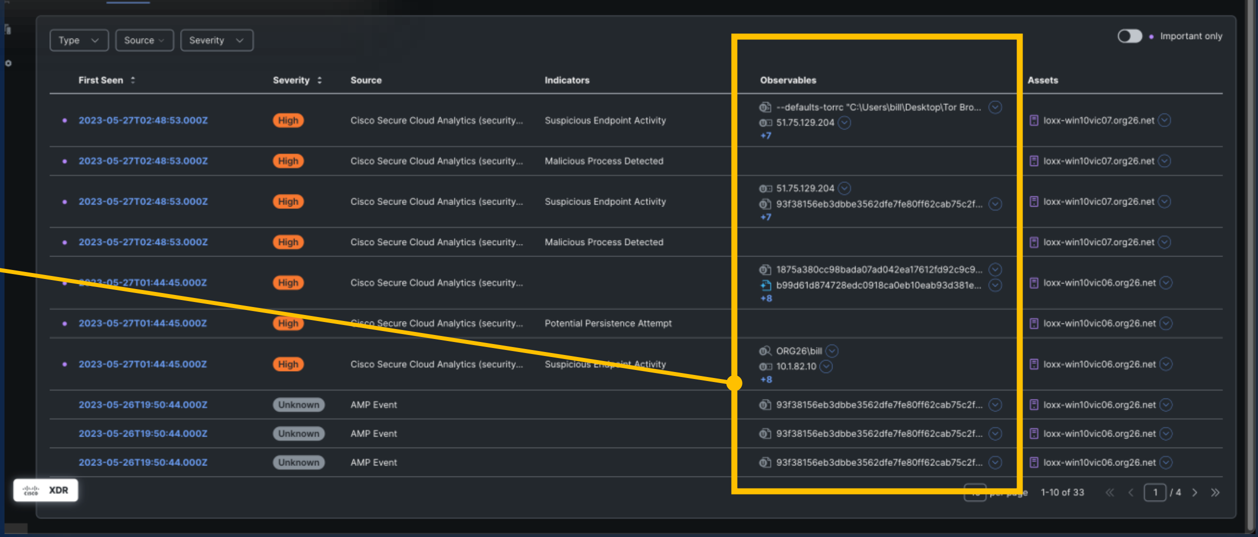


Displays Lateral Movement

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

Direct source of observables

For brand-new detections in XDR Analytics

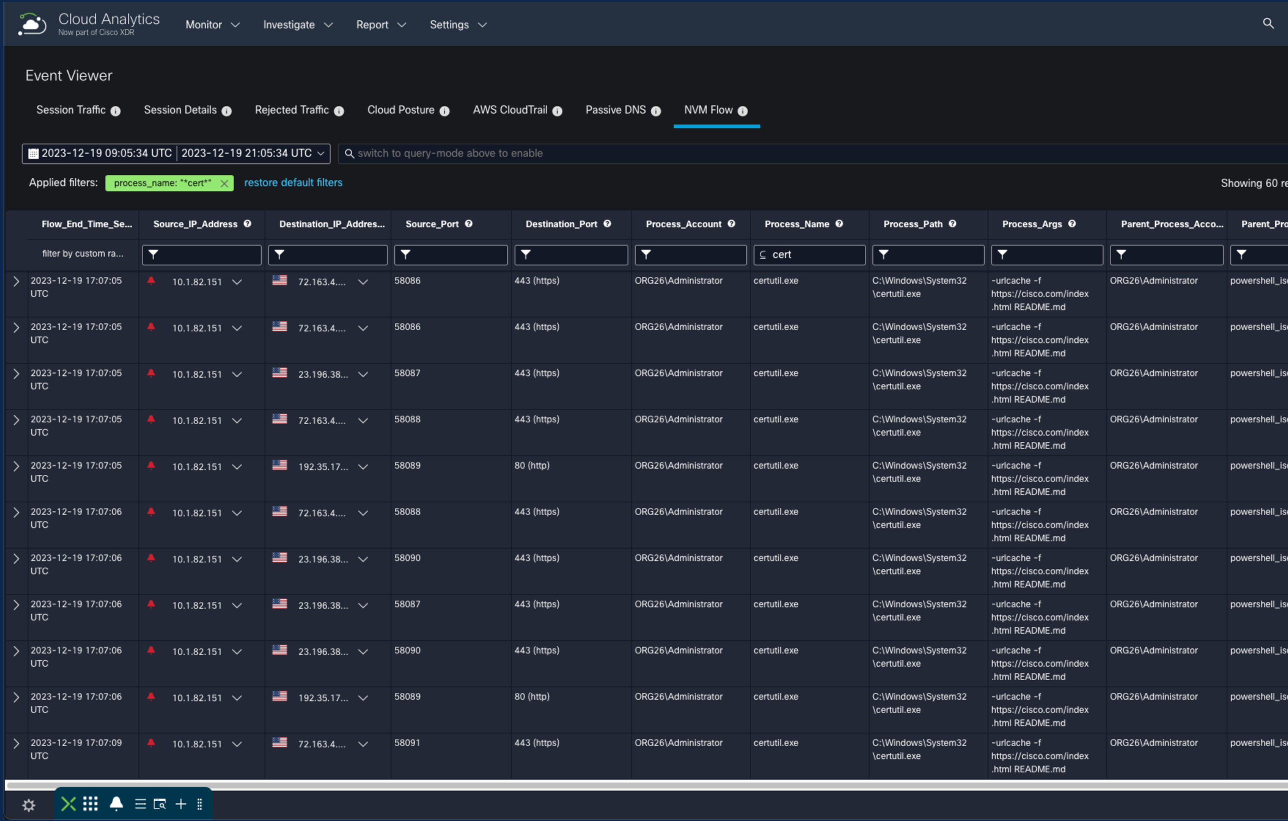


First Seen	Severity	Source	Indicators	Observables	Assets
2023-05-27T02:48:53.000Z	High	Cisco Secure Cloud Analytics (security...	Suspicious Endpoint Activity	--defaults-torrc "C:\Users\bill\Desktop\Tor Bro... 51.75.129.204 +7	loxx-win10vic07.org26.net
2023-05-27T02:48:53.000Z	High	Cisco Secure Cloud 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		93f38156eb3dbbe3562dfe7fe80ff62cab75c2f...	loxx-win10vic06.org26.net
2023-05-26T19:50:44.000Z	Unknown	AMP Event		93f38156eb3dbbe3562dfe7fe80ff62cab75c2f...	loxx-win10vic06.org26.net
2023-05-26T19:50:44.000Z	Unknown	AMP Event		93f38156eb3dbbe3562dfe7fe80ff62cab75c2f...	loxx-win10vic06.org26.net

per page 1-10 of 33 « ‹ 1 / 4 › »

NVM versus SYSMON & Network Event Logs

- NVM Captures all the flows.
- Sysmon captures the first time & never again



Event Viewer

2023-12-19 09:05:34 UTC | 2023-12-19 21:05:34 UTC

switch to query-mode above to enable

Applied filters: process_name: "*cert*" restore default filters

Showing 60 re

Flow_End_Time_Se...	Source_IP_Address	Destination_IP_Addres...	Source_Port	Destination_Port	Process_Account	Process_Name	Process_Path	Process_Args	Parent_Process_Acco...	Parent_Pro
filter by custom ra...						⊆ cert				
2023-12-19 17:07:05 UTC	10.1.82.151	72.163.4....	58086	443 (https)	ORG26\Administrator	certutil.exe	C:\Windows\System32 \certutil.exe	-urlcache -f https://cisco.com/index .html README.md	ORG26\Administrator	powershell_is
2023-12-19 17:07:05 UTC	10.1.82.151	72.163.4....	58086	443 (https)	ORG26\Administrator	certutil.exe	C:\Windows\System32 \certutil.exe	-urlcache -f https://cisco.com/index .html README.md	ORG26\Administrator	powershell_is
2023-12-19 17:07:05 UTC	10.1.82.151	23.196.38...	58087	443 (https)	ORG26\Administrator	certutil.exe	C:\Windows\System32 \certutil.exe	-urlcache -f https://cisco.com/index .html README.md	ORG26\Administrator	powershell_is
2023-12-19 17:07:05 UTC	10.1.82.151	72.163.4....	58088	443 (https)	ORG26\Administrator	certutil.exe	C:\Windows\System32 \certutil.exe	-urlcache -f https://cisco.com/index .html README.md	ORG26\Administrator	powershell_is
2023-12-19 17:07:05 UTC	10.1.82.151	192.35.17...	58089	80 (http)	ORG26\Administrator	certutil.exe	C:\Windows\System32 \certutil.exe	-urlcache -f https://cisco.com/index .html README.md	ORG26\Administrator	powershell_is
2023-12-19 17:07:06 UTC	10.1.82.151	72.163.4....	58088	443 (https)	ORG26\Administrator	certutil.exe	C:\Windows\System32 \certutil.exe	-urlcache -f https://cisco.com/index .html README.md	ORG26\Administrator	powershell_is
2023-12-19 17:07:06 UTC	10.1.82.151	23.196.38...	58090	443 (https)	ORG26\Administrator	certutil.exe	C:\Windows\System32 \certutil.exe	-urlcache -f https://cisco.com/index .html README.md	ORG26\Administrator	powershell_is
2023-12-19 17:07:06 UTC	10.1.82.151	23.196.38...	58087	443 (https)	ORG26\Administrator	certutil.exe	C:\Windows\System32 \certutil.exe	-urlcache -f https://cisco.com/index .html README.md	ORG26\Administrator	powershell_is
2023-12-19 17:07:06 UTC	10.1.82.151	23.196.38...	58090	443 (https)	ORG26\Administrator	certutil.exe	C:\Windows\System32 \certutil.exe	-urlcache -f https://cisco.com/index .html README.md	ORG26\Administrator	powershell_is
2023-12-19 17:07:06 UTC	10.1.82.151	192.35.17...	58089	80 (http)	ORG26\Administrator	certutil.exe	C:\Windows\System32 \certutil.exe	-urlcache -f https://cisco.com/index .html README.md	ORG26\Administrator	powershell_is
2023-12-19 17:07:09 UTC	10.1.82.151	72.163.4....	58091	443 (https)	ORG26\Administrator	certutil.exe	C:\Windows\System32 \certutil.exe	-urlcache -f https://cisco.com/index .html README.md	ORG26\Administrator	powershell_is

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

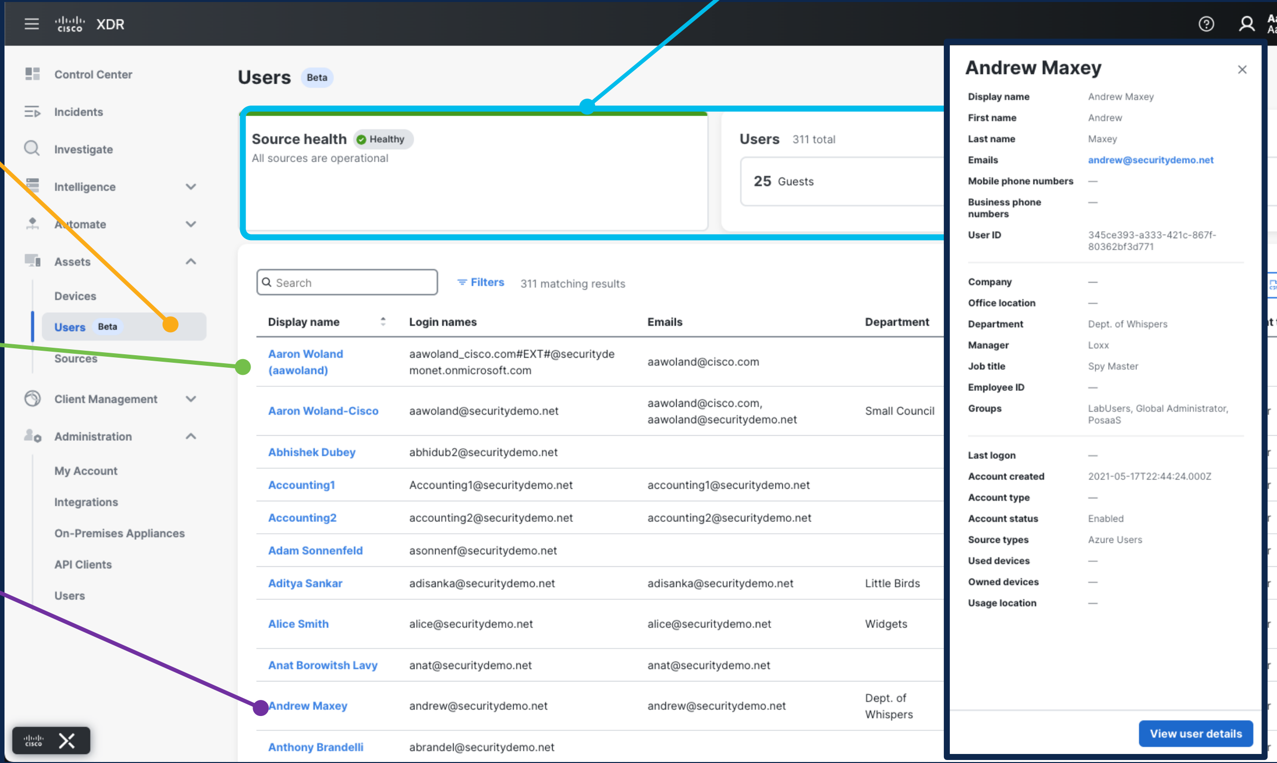
User “inventory” is a subset of “Assets” category

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.



Users Beta

Source health ✓ Healthy
All sources are operational

Users 311 total
25 Guests

Search ⩸ Filters 311 matching results

Display name	Login names	Emails	Department
Aaron Woland (aawoland)	aawoland_cisco.com#EXT#@securitydemonet.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 logon	—
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

User Details Page

Top Devices Used / Owned

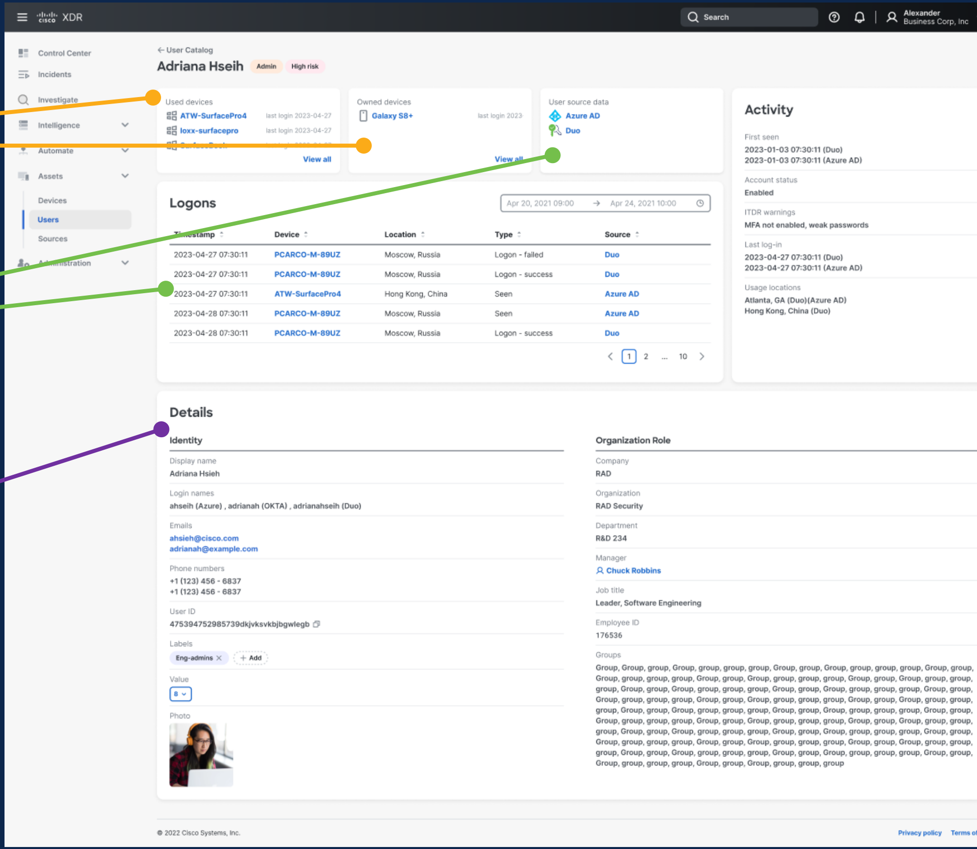
Click “View All” for Progressive Disclosure list of all devices

Where Seen

List of all sources merged for this user & recent logon events for user

More Details

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



Adriana Hseih Admin High risk

Used devices
ATW-SurfacePro4 last login 2023-04-27
loxx-surfacepro last login 2023-04-27
View all

Owned devices
Galaxy S8+ last login 2023
View all

User source data
Azure AD
Duo

Activity

First seen
2023-01-03 07:30:11 (Duo)
2023-01-03 07:30:11 (Azure AD)

Account status
Enabled

ITDR warnings
MFA not enabled, weak passwords

Last log-in
2023-04-27 07:30:11 (Duo)
2023-04-27 07:30:11 (Azure AD)

Usage locations
Atlanta, GA (Duo)(Azure AD)
Hong Kong, China (Duo)

Logons

Apr 20, 2021 09:00 → Apr 24, 2021 10:00

Timestamp	Device	Location	Type	Source
2023-04-27 07:30:11	PCARCO-M-89UZ	Moscow, Russia	Logon - failed	Duo
2023-04-27 07:30:11	PCARCO-M-89UZ	Moscow, Russia	Logon - success	Duo
2023-04-27 07:30:11	ATW-SurfacePro4	Hong Kong, China	Seen	Azure AD
2023-04-28 07:30:11	PCARCO-M-89UZ	Moscow, Russia	Seen	Azure AD
2023-04-28 07:30:11	PCARCO-M-89UZ	Moscow, Russia	Logon - success	Duo

< 1 2 ... 10 >

Details

Identity

Display name
Adriana Hsieh

Login names
ahseih (Azure) , adrianah (OKTA) , adrianahseih (Duo)

Emails
ahsieh@cisco.com
adrianah@example.com

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

User ID
475394752985739dkjvksvkbjbgwlegb

Labels
Eng-admins ✕ + Add

Value
8

Photo

Organization Role

Company
RAD

Organization
RAD Security

Department
R&D 234

Manager
Chuck Robbins

Job title
Leader, Software Engineering

Employee ID
176536

Groups
Group, Group, group, Group, group, group, group

© 2022 Cisco Systems, Inc.

Privacy policy Terms o

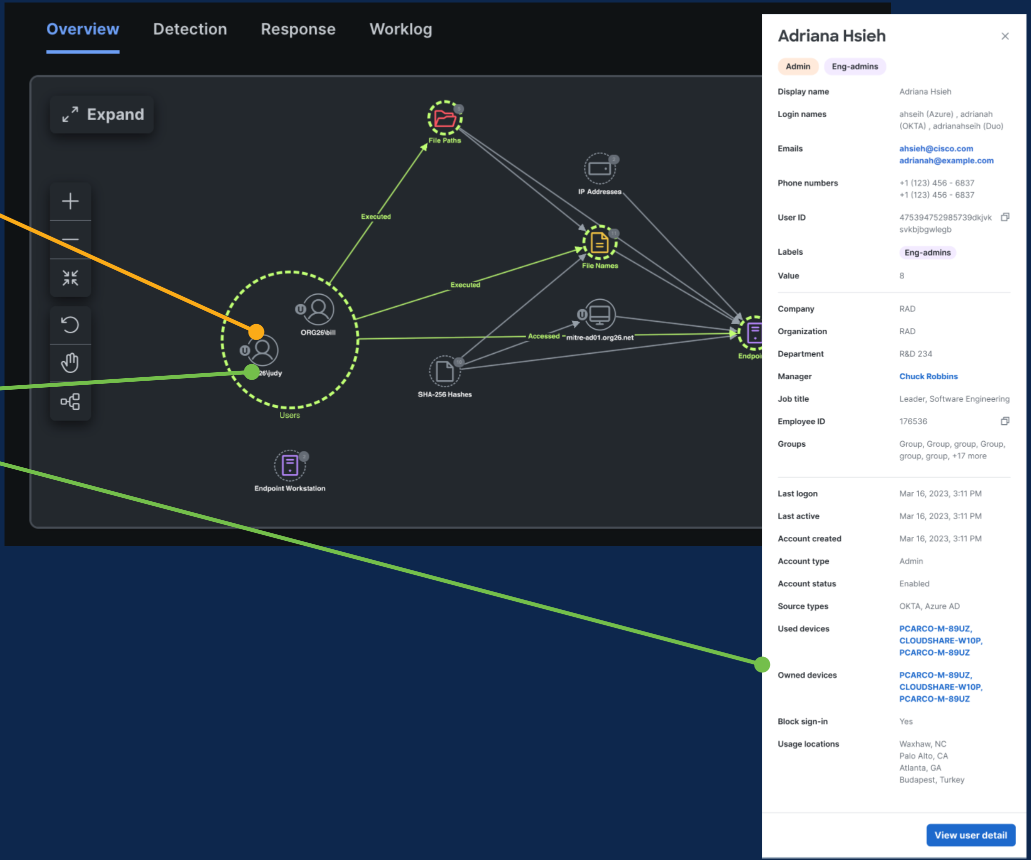
User Context In an Investigation / Incident Management

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



Adriana Hsieh

Admin Eng-admins

Display name	Adriana Hsieh
Login names	ahseih (Azure) , adrianah (OKTA) , adrianahseih (Duo)
Emails	ahsieh@cisco.com adrianah@example.com
Phone numbers	+1 (123) 456 - 6837 +1 (123) 456 - 6837
User ID	475394752985739dkjvksvkbjbgwlegb
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 logon	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-89UZ, CLOUDSHARE-W10P, PCARCO-M-89UZ
Owned devices	PCARCO-M-89UZ, CLOUDSHARE-W10P, PCARCO-M-89UZ
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

OORT

now part of CISCO

Cisco Identity Intelligence

Why OORT?

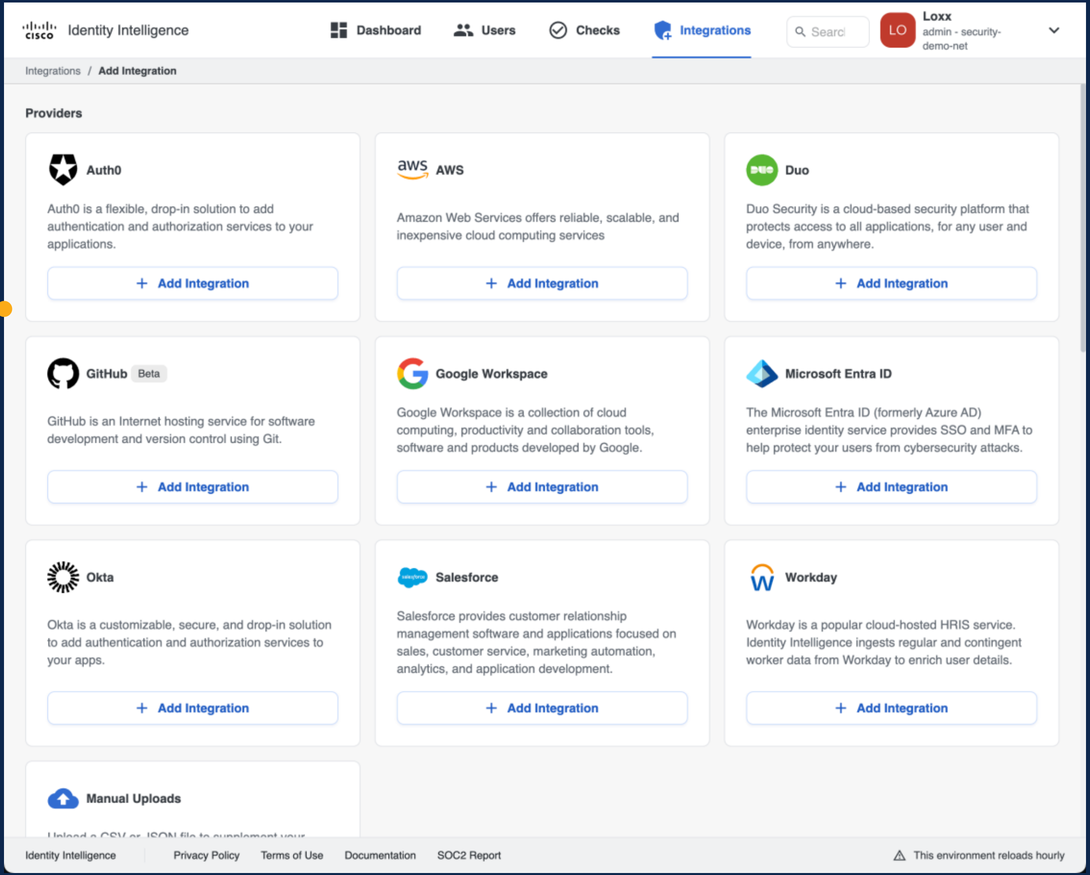
- Tech & Talent Acquisition
- Literally the team that wrote Device Insights – left Cisco & created Oort
- Practically tailor-made for this integration

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

Note: these screens are from the original Oort UI

Integrations!!

Cisco Identity Intelligence integrates w/ many key (cloud-based) ID sources already.



Integrations / **Add Integration**

Providers

Auth0

Auth0 is a flexible, drop-in solution to add authentication and authorization services to your applications.

+ Add Integration

AWS

Amazon Web Services offers reliable, scalable, and inexpensive cloud computing services

+ 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.

+ Add Integration

Google Workspace

Google Workspace is a collection of cloud computing, productivity and collaboration tools, software and products developed by Google.

+ Add Integration

Microsoft Entra ID

The Microsoft Entra ID (formerly Azure AD) enterprise identity service provides SSO and MFA to help protect your users from cybersecurity attacks.

+ 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. Identity Intelligence ingests regular and contingent worker data from Workday to enrich user details.

+ Add Integration

Manual Uploads

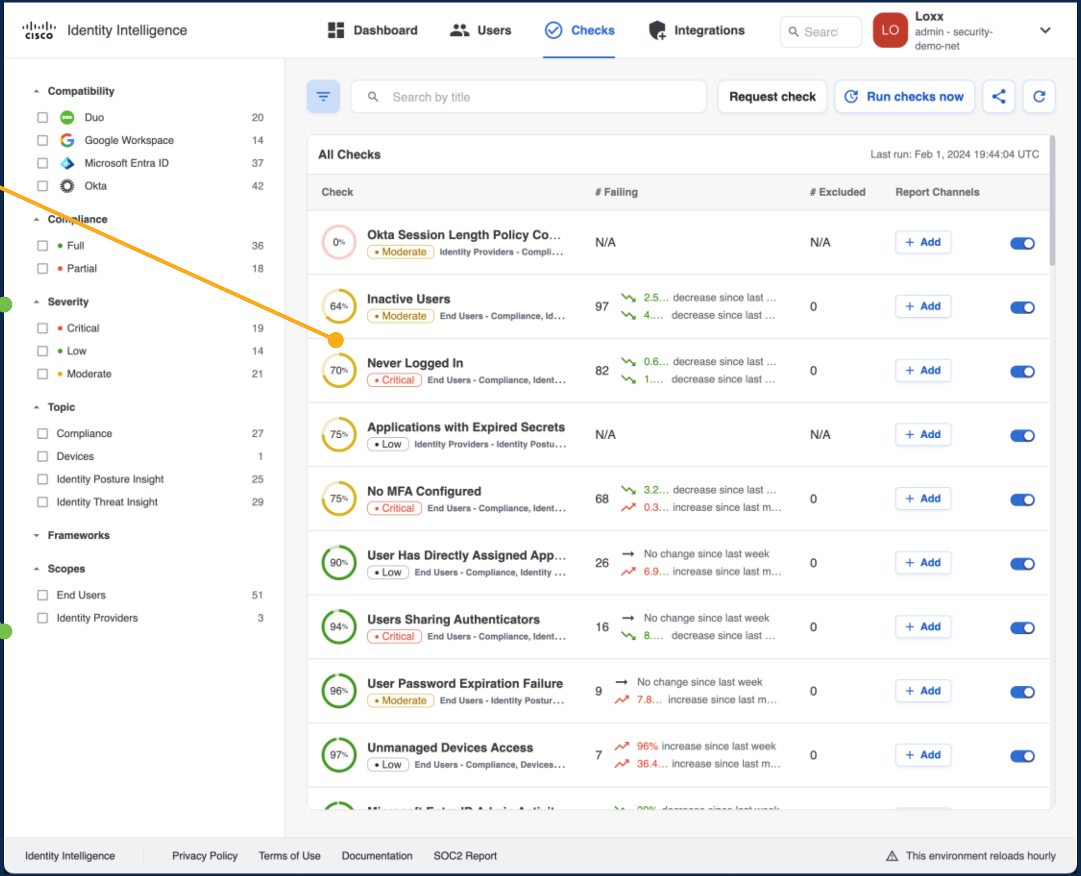
Upload a CSV or JSON file to supplement your

Checks

AKA: Signatures for Detections

Filterable

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



Compatibility

□ Duo	20
□ Google Workspace	14
□ Microsoft Entra ID	37
□ Okta	42

Compliance

□ • Full	36
□ • Partial	18

Severity

□ • Critical	19
□ • Low	14
□ • Moderate	21

Topic

□ Compliance	27
□ Devices	1
□ Identity Posture Insight	25
□ Identity Threat Insight	29

Frameworks

Scopes

□ End Users	51
□ Identity Providers	3

All Checks Last run: Feb 1, 2024 19:44:04 UTC

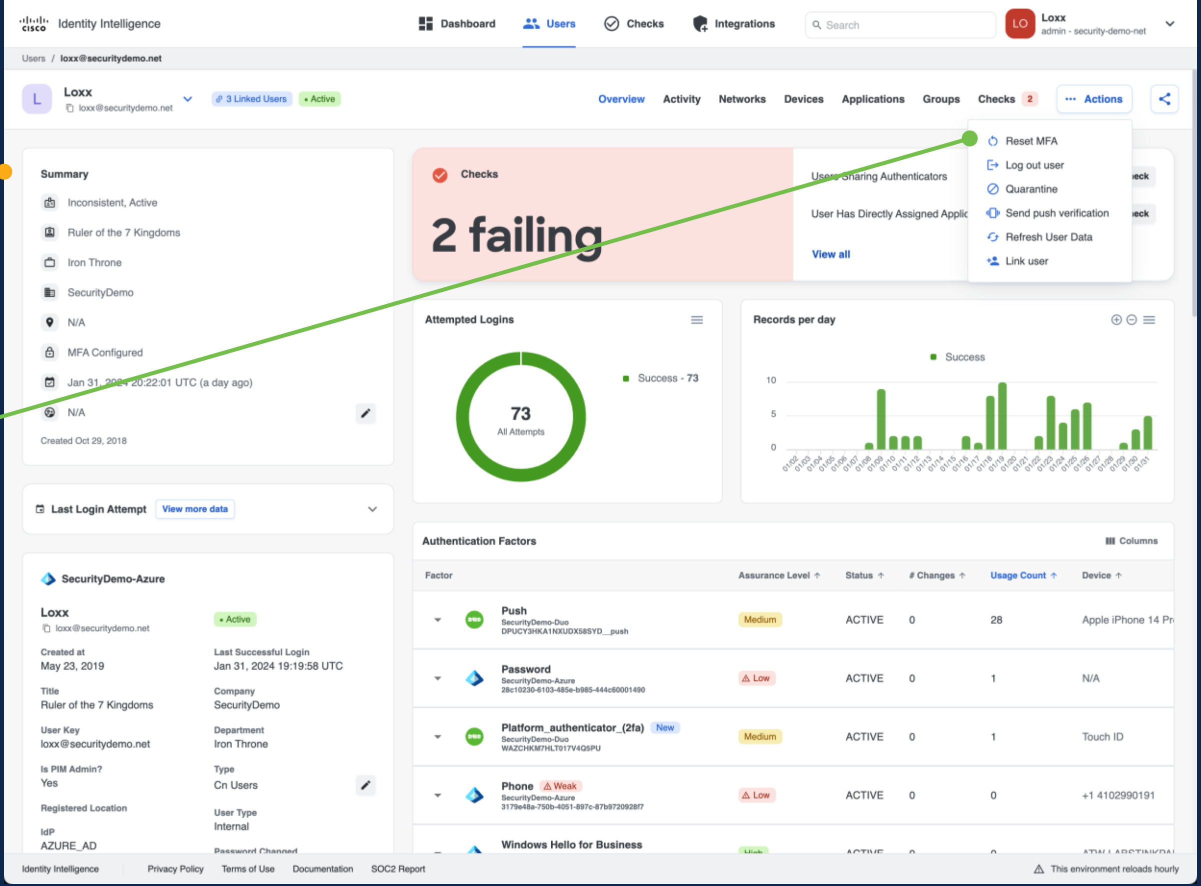
	Check	# Failing		# Excluded	Report Channels	
0%	Okta Session Length Policy Co... • Moderate Identity Providers - Compli...	N/A		N/A	+ Add	●
64%	Inactive Users • Moderate End Users - Compliance, Id...	97	2.5... decrease since last ... 4.... decrease since last ...	0	+ Add	●
70%	Never Logged In • Critical End Users - Compliance, Ident...	82	0.6... decrease since last ... 1.... decrease since last ...	0	+ Add	●
75%	Applications with Expired Secrets • Low Identity Providers - Identity Postu...	N/A		N/A	+ Add	●
75%	No MFA Configured • Critical End Users - Compliance, Ident...	68	3.2... decrease since last ... 0.3... increase since last m...	0	+ Add	●
90%	User Has Directly Assigned App... • Low End Users - Compliance, Identity ...	26	→ No change since last week 6.9... increase since last m...	0	+ Add	●
94%	Users Sharing Authenticators • Critical End Users - Compliance, Ident...	16	→ No change since last week 8.... decrease since last ...	0	+ Add	●
96%	User Password Expiration Failure • Moderate End Users - Identity Postur...	9	→ No change since last week 7.8... increase since last m...	0	+ Add	●
97%	Unmanaged Devices Access • Low End Users - Compliance, Devices...	7	96% increase since last week 36.4... increase since last m...	0	+ Add	●

User Details

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

Response

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



Identity Intelligence

Dashboard | Users | Checks | Integrations | Search | LO Loxx admin - security-demo-net

Users / loxx@securitydemo.net

L Loxx loxx@securitydemo.net | 3 Linked Users | • Active

Overview | Activity | Networks | Devices | Applications | Groups | Checks 2 | ··· Actions

- Reset MFA
- Log out user
- Quarantine
- Send push verification
- Refresh User Data
- Link user

Summary

- Inconsistent, Active
- Ruler of the 7 Kingdoms
- Iron Throne
- SecurityDemo
- N/A
- MFA Configured
- Jan 31, 2024 20:22:01 UTC (a day ago)
- N/A

Created Oct 29, 2018

Checks

2 failing

Users Sharing Authenticators

User Has Directly Assigned Applic

View all

Attempted Logins

Records per day

Last Login Attempt View more data

SecurityDemo-Azure

Loxx • Active
loxx@securitydemo.net

Created at May 23, 2019	Last Successful Login Jan 31, 2024 19:19:58 UTC
Title Ruler of the 7 Kingdoms	Company SecurityDemo
User Key loxx@securitydemo.net	Department Iron Throne
Is PIM Admin? Yes	Type Cn Users
Registered Location	User Type Internal
IdP AZURE_AD	Password Changed

Authentication Factors Columns

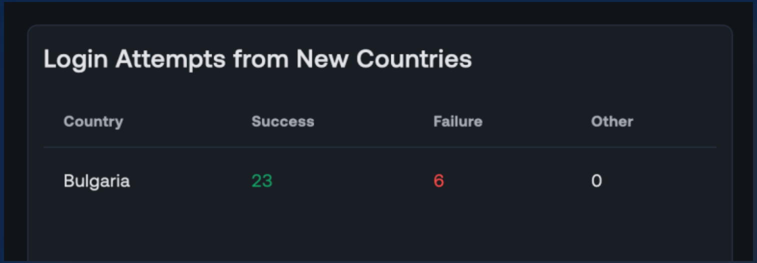
Factor	Assurance Level ↑	Status ↑	# Changes ↑	Usage Count ↑	Device ↑
Push SecurityDemo-Duo DPUCY3HKA1NXUDX58SYD__push	Medium	ACTIVE	0	28	Apple iPhone 14 Pr
Password SecurityDemo-Azure 28c10230-6103-485e-b985-444c60001490	⚠ Low	ACTIVE	0	1	N/A
Platform_authenticator_(2fa) New SecurityDemo-Duo WAZCHKM7HLT017V4Q5PU	Medium	ACTIVE	0	1	Touch ID
Phone ⚠ Weak SecurityDemo-Azure 3179e48a-750b-4051-897c-87b9720928f7	⚠ Low	ACTIVE	0	0	+1 4102990191
Windows Hello for Business	High	ACTIVE	0	0	ATW	ABSTINKPAI

Identity Intelligence | Privacy Policy | Terms of Use | Documentation | SOC2 Report | ⚠ This environment reloads hourly

cisco Live!

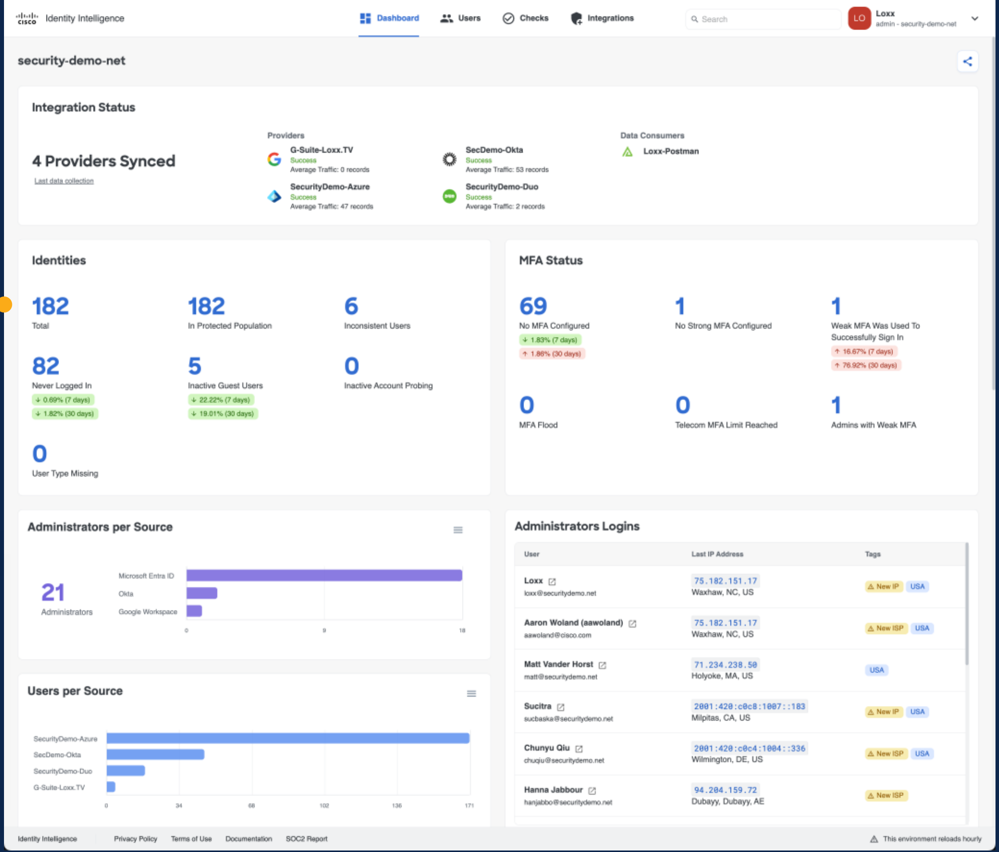
Insights

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



security-demo-net

Integration Status

4 Providers Synced

Last data collection

Providers

- G-Suite-Loxx.TV — Success — Average Traffic: 0 records
- SecurityDemo-Azure — Success — Average Traffic: 47 records
- SecDemo-Okta — Success — Average Traffic: 53 records
- SecurityDemo-Duo — Success — Average Traffic: 2 records

Data Consumers

- Loxx-Postman

Identities

182 Total	182 In Protected Population	6 Inconsistent Users
82 Never Logged In ↓ 0.69% (7 days) ↓ 1.82% (30 days)	5 Inactive Guest Users ↓ 22.22% (7 days) ↓ 19.01% (30 days)	0 Inactive Account Probing
0 User Type Missing		

MFA Status

69 No MFA Configured ↓ 1.83% (7 days) ↑ 1.86% (30 days)	1 No Strong MFA Configured	1 Weak MFA Was Used To Successfully Sign In ↑ 16.67% (7 days) ↑ 76.92% (30 days)
0 MFA Flood	0 Telecom MFA Limit Reached	1 Admins with Weak MFA

Administrators per Source

21 Administrators

Users per Source

Administrators Logins

User	Last IP Address	Tags
Loxx loxx@securitydemo.net	75.182.151.17 Waxhaw, NC, US	⚠ New IP USA
Aaron Woland (aawoland) aawoland@cisco.com	75.182.151.17 Waxhaw, NC, US	⚠ New ISP USA
Matt Vander Horst matt@securitydemo.net	71.234.238.50 Holyoke, MA, US	USA
Sucitra sucbaska@securitydemo.net	2001:420:c0c8:1007::183 Milpitas, CA, US	⚠ New IP USA
Chunyu Qiu chuqiu@securitydemo.net	2001:420:c0c4:1004::336 Wilmington, DE, US	⚠ New ISP USA
Hanna Jabbour hanjabbo@securitydemo.net	94.204.159.72 Dubayy, Dubayy, AE	⚠ New ISP

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

The integration of Cisco Identity Intelligence into Cisco XDR & Duo Security 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
- SecureX EoL in July ‘24, replacement for CSC Management forthcoming

Links

- Retired Session with VERY useful information:
  - BRKSEC-2754 - Device Insights Dedicated Session (OnDemand): Making XDR Investigations and SOAR Automation Work by Unifying Assets https://www.ciscolive.com/on-demand/on-demand-library.html?search=Woland#/video/1676612951781001qAcG
- Public Webex Spaces to Join:
  - XDR Bar (public Webex space): https://eurl.io/#i10UBcGzR
  - Endpoint Bar (Secure Client/AnyConnect): https://eurl.io/#TmrReXaEj

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand. Sessions from this event will be available from February 23.

Other XDR sessions

Matt Vander Horst

Technical Leader

Accelerate your SOC with Cisco XDR

BRKSEC-1023

Tuesday @ 2:00 PM

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

Tuesday @ 4:00 PM

Other Sessions

Serhii Kucherenko

Customer Escalations Engineer

Cisco Secure Client and Device Insights - better together

LABSEC-2776

Walk-in Lab

Steven Chimes

Platform Security Architect

(ZTNA) Demystified - What It Is, Why You Need It and the New Cisco Technologies That Make Frictionless Security Possible

BRKSEC-2079

Friday @ 11:00 AM

Matt Vander Horst

Technical Leader

Getting started with Cisco XDR Automation workflows and atomics -

DEVWKS-1190

Wednesday @ 1:30 PM

Continue your education

CTF booth at World of Solutions

Test your skills and earn Cisco CE Credits*

CTF is gamified Hands-On Cisco Technologies Labs!

* Ask at the booth for the qualifying missions

CISCO
SECURE

CISCO The bridge to possible

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

Let’s go