

The XDR Journey

Operationalizing Cisco XDR from 0 to 100

Hanna Jabbour
Technical Marketing Engineer Cisco

cisco Live !

Cisco Webex App

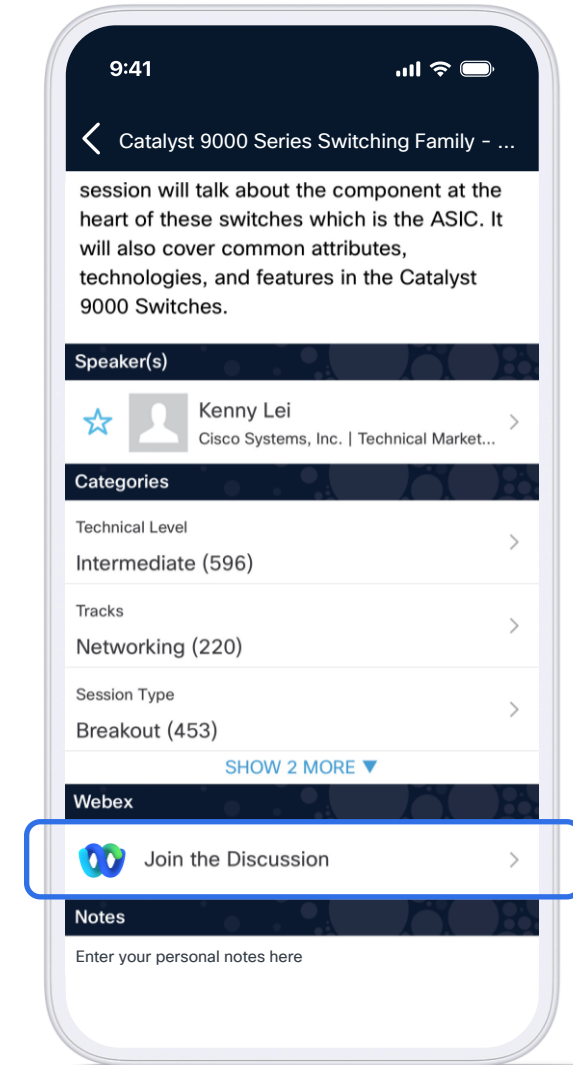
Questions?

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

How

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

Webex spaces will be moderated by the speaker until 14 November 2025.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2531>

Agenda

- 01 Intro
- 02 XDR basics
- 03 What is the base telemetry?
- 04 How to add more data?
- 05 What can automation do ?
- 06 How does it fit in my SOC ?
- 07 Where can I learn more ?

Hanna Elia Jabbour



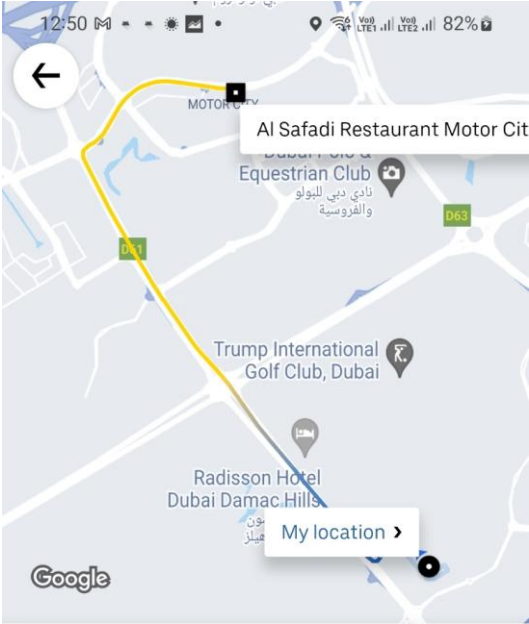
- 15 years of experience in Dev/Network/Security
- TME for XDR and Secure Analytics covering EMEAR/APJ
- Lebanese based out of the Dubai
- Yes, my name is Hanna



Lebanon | Dubai



<https://www.youtube.com/watch?v=INiCIW2VpCI>



Chopper 1 AED 520.00-624.00
Only available for Dubai city tour ⓘ

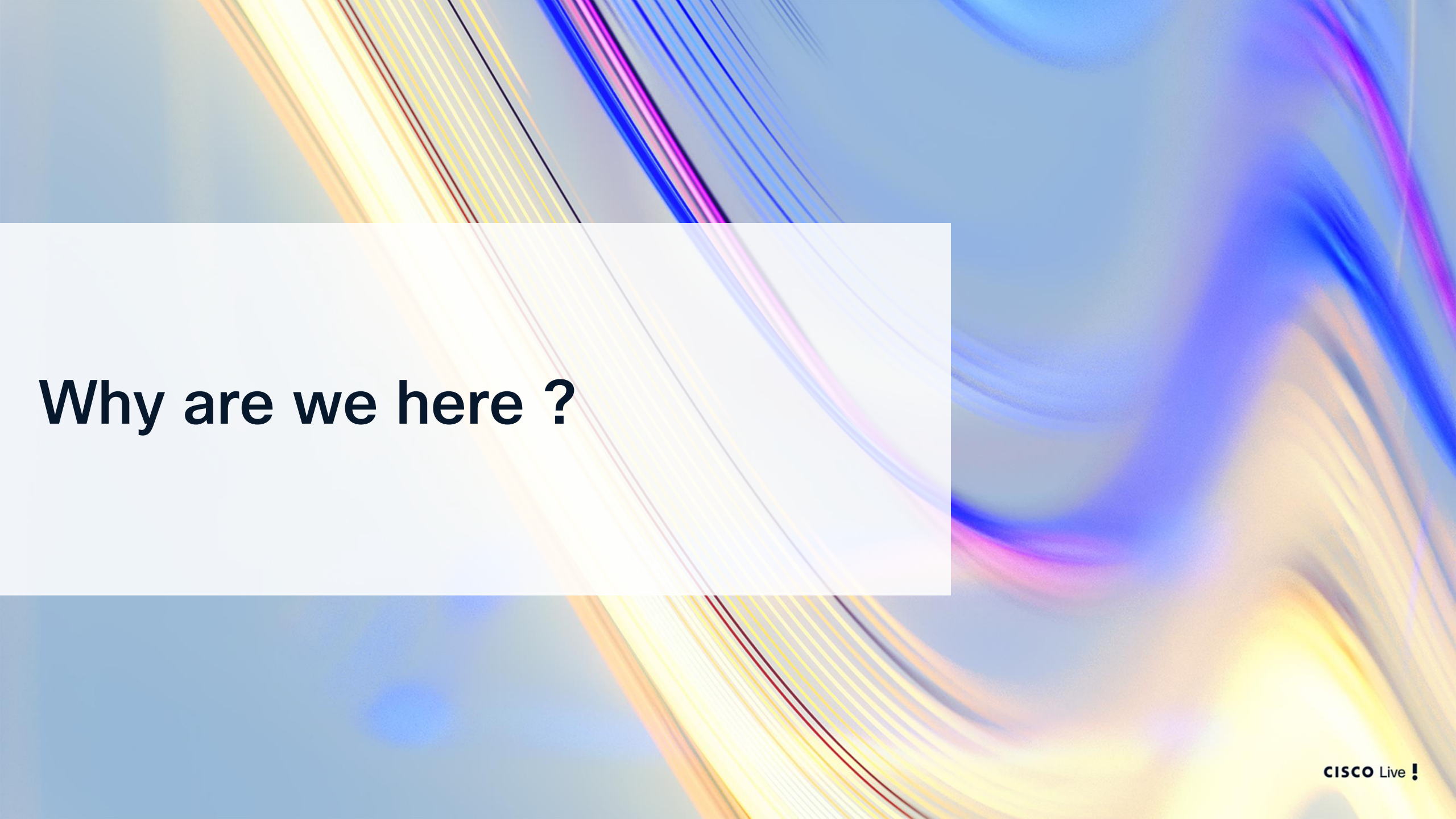
Cash >

No Choppers Available Now



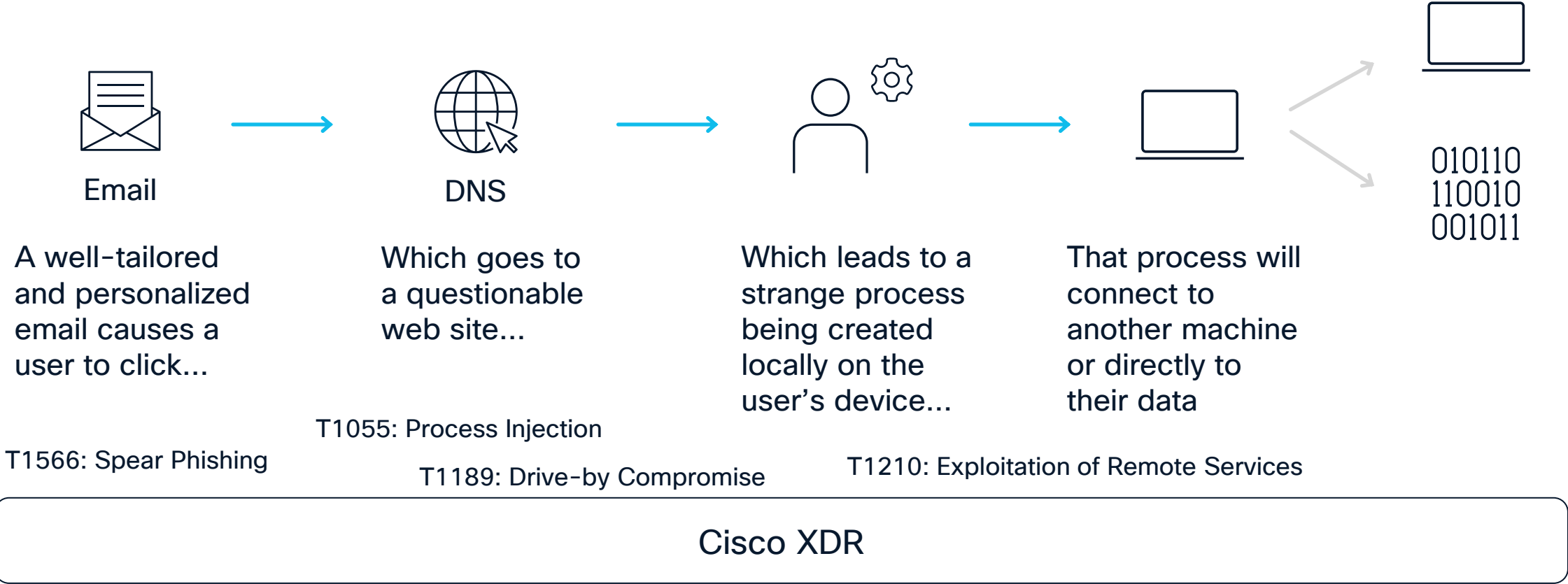
Please Fill Out the Survey





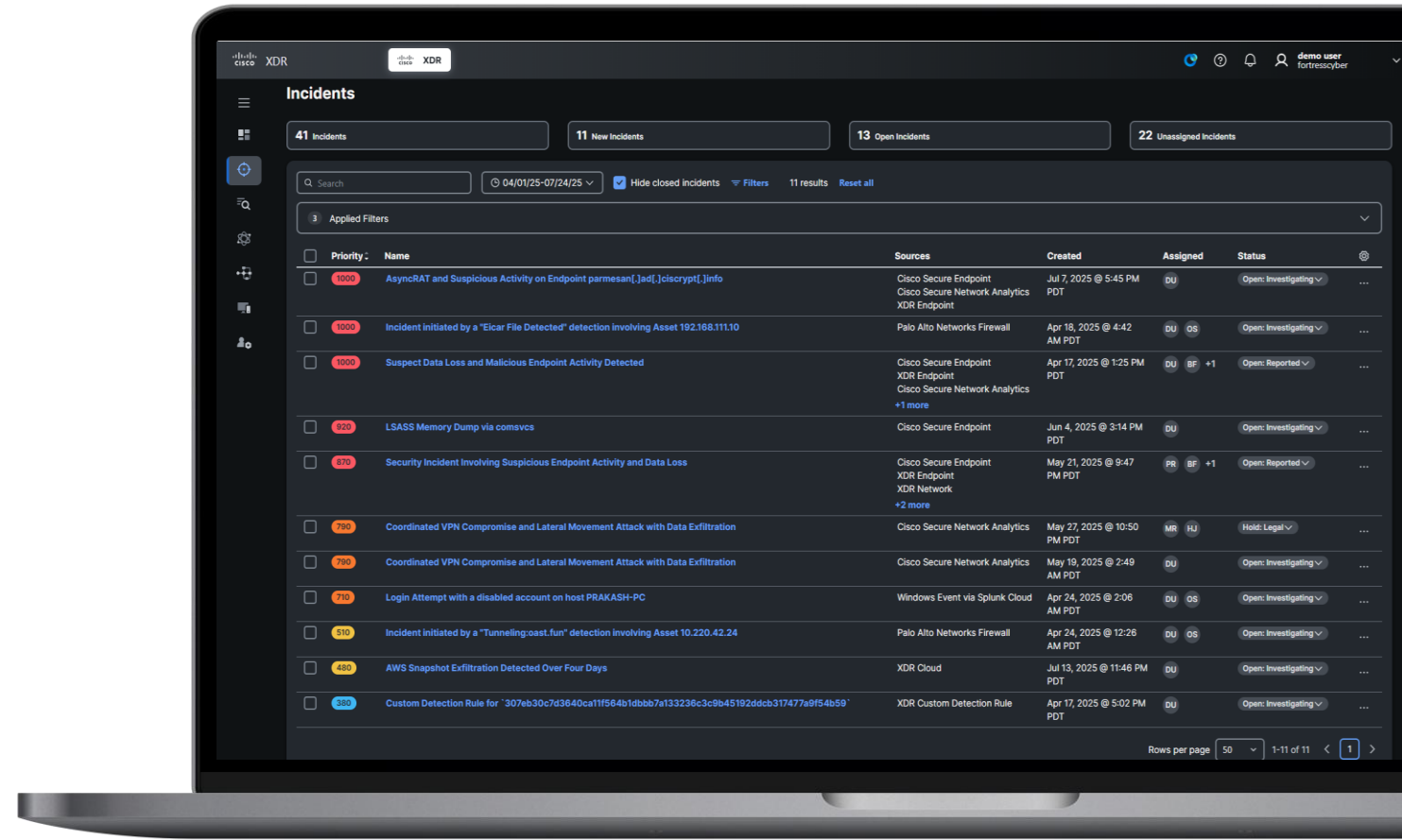
Why are we here ?

How are you detecting advanced threats



Cisco XDR

- Open and extensible platform
- Single detection & response solution for security operations, automated & cloud-first
- Available as a product and managed service

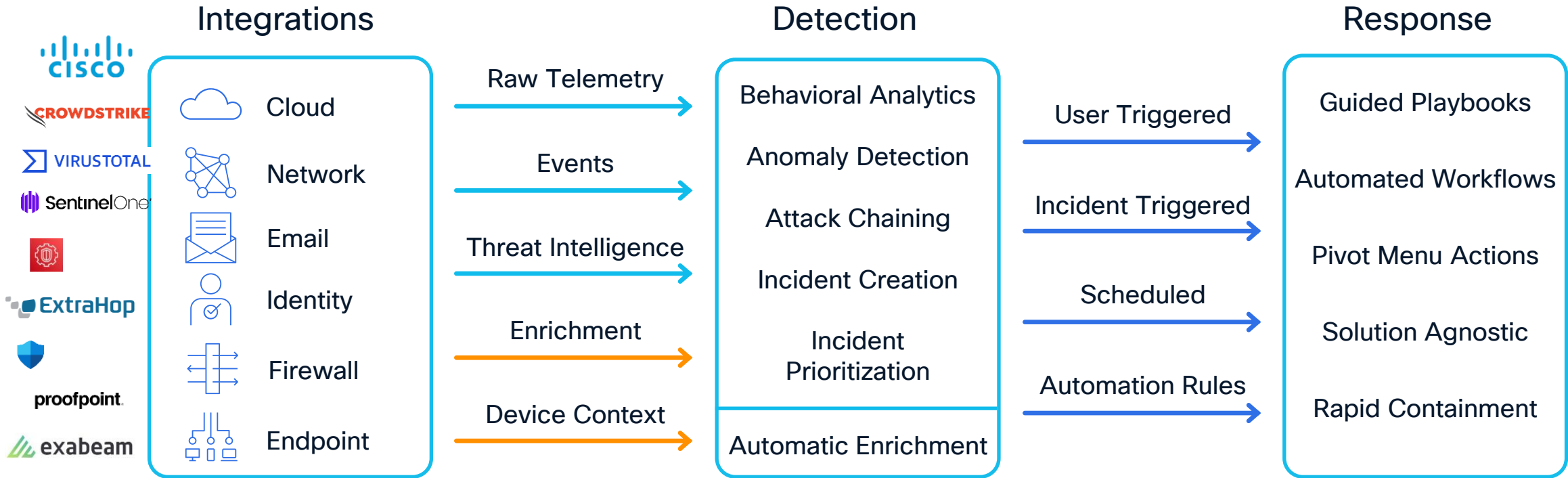


Optimized for
lean teams

Speed to value

Deeply integrated
with the network

High level architecture



Multi-vector telemetry ingest network, cloud, endpoint, email, and more from Cisco and 3rd party

Cross domain alert detections and attack chaining with automated incident prioritization and enrichment

Automated or user triggered responses to block observables using any integrated technology

**Great things are not done by
impulse, but by a series of
small things brought together**

Vincent Van Gogh

Starting the Journey

What do I need from my XDR ?



How does it fit in my SOC ?

How do I respond to the attack?

Which devices / assets were impacted ?

Where the threat started / propagated ?

Telemetry data source importance

Cisco Customer Research

The top six data sources that customers believe are essential for 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%



Why do I need NDR?

Commonly deployed Tools

Firewall

IDS/IPS

Secure Web
Gateways

WAF

NDR

Behavioral
Context Across
Every Connection

Signature and Rules Focused

- Lacks context (who is connecting to who)
- All rules must be pre-defined
- No thresholds for alerting (noisy)

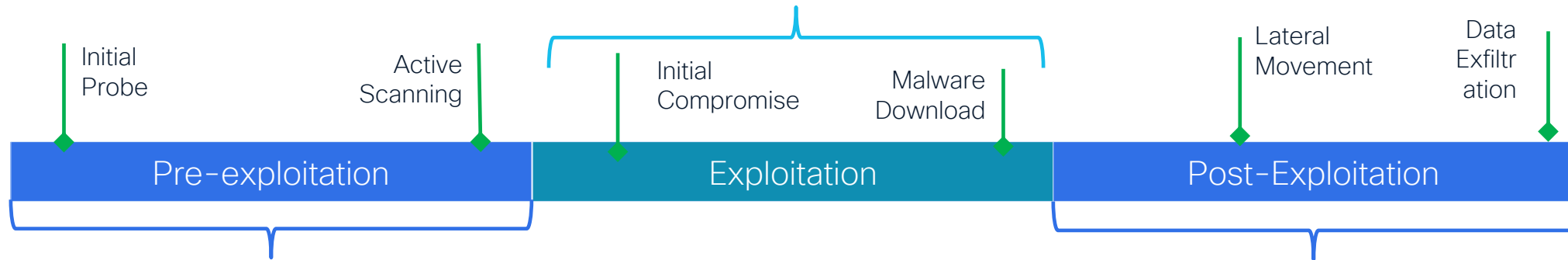
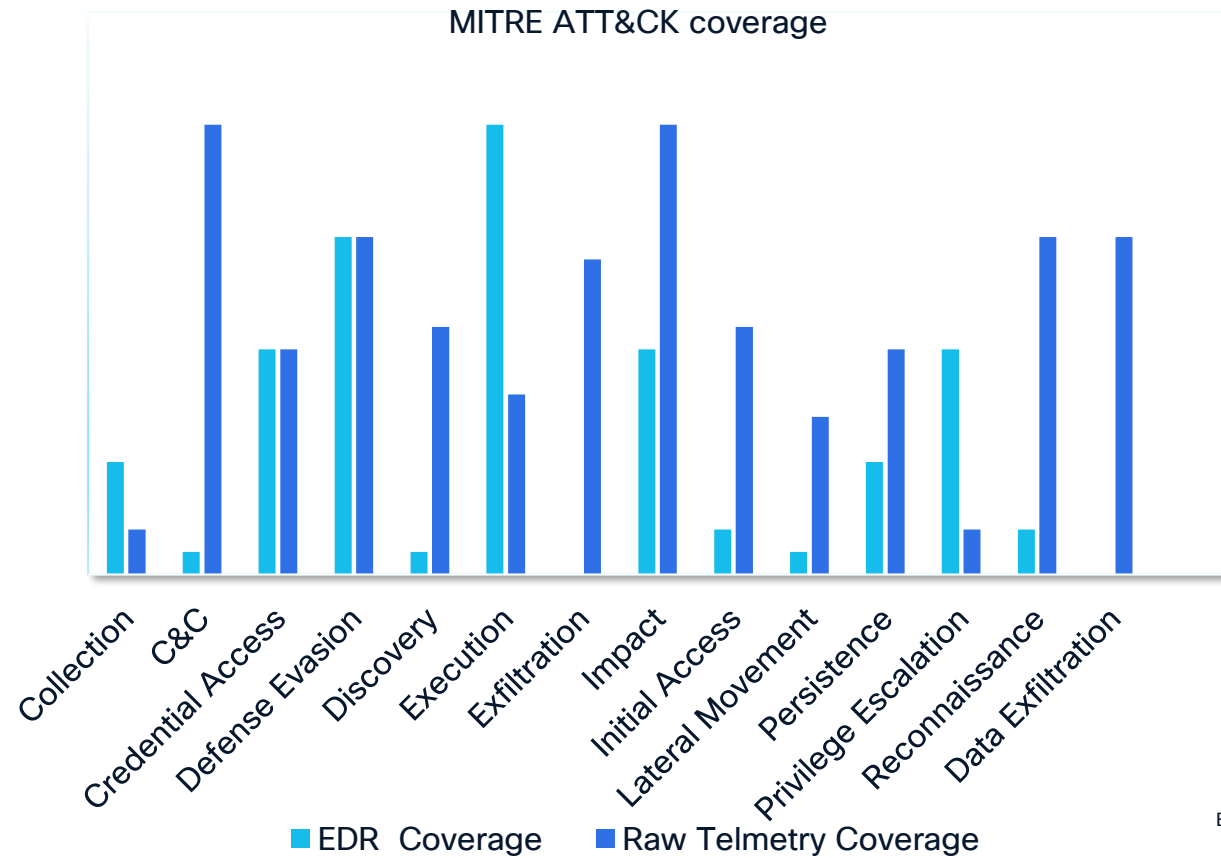
Powered by AI and ML

- Understands Normal behavior
- Can detect new and novel attacks
- Can be finely tuned

Why network telemetry Detection ?

Endpoint Events

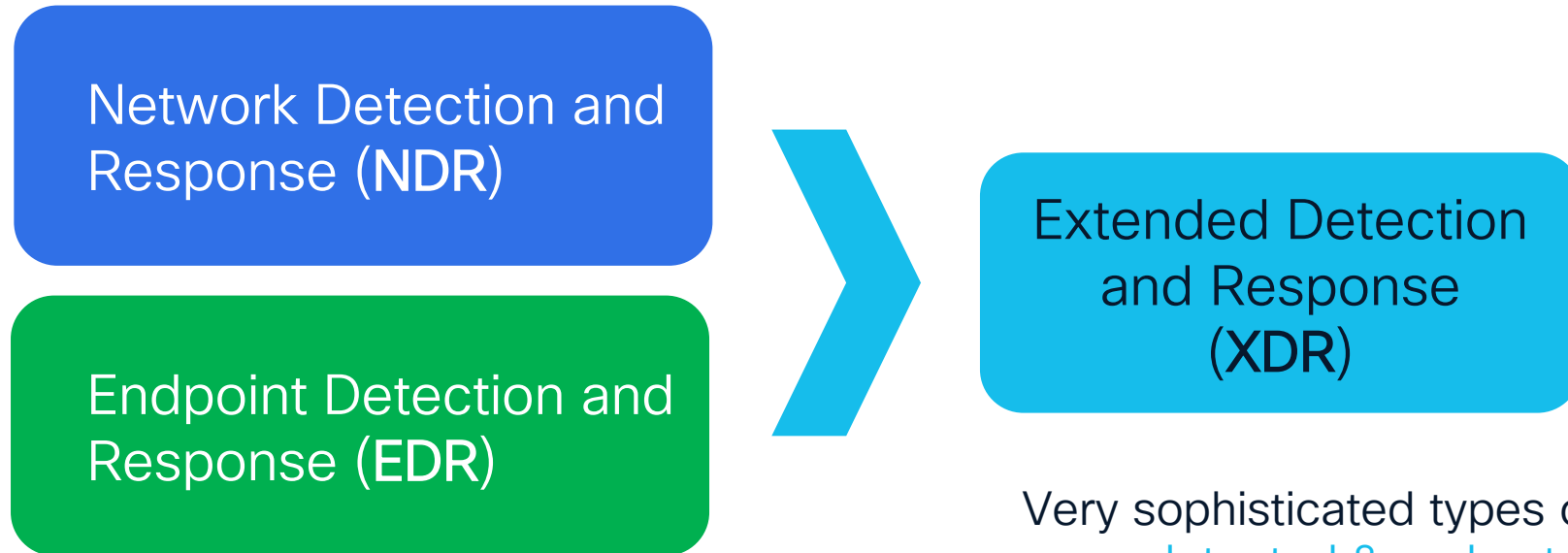
Network Events



- **Endpoint-only** based detections does not provide visibility to initial access, network discovery activities as well as lateral movement and data theft.
- **Network based detection** provide coverage for threats beyond endpoint execution point (before and after) as well as detect threats on devices that can't host endpoint security solutions.
- **Combining Network and Endpoint detection** provides a better coverage for attacks across the different attack TTPs (MITRE).

Combining NDR and EDR is key for XDR

Depending on how you Define your XDR

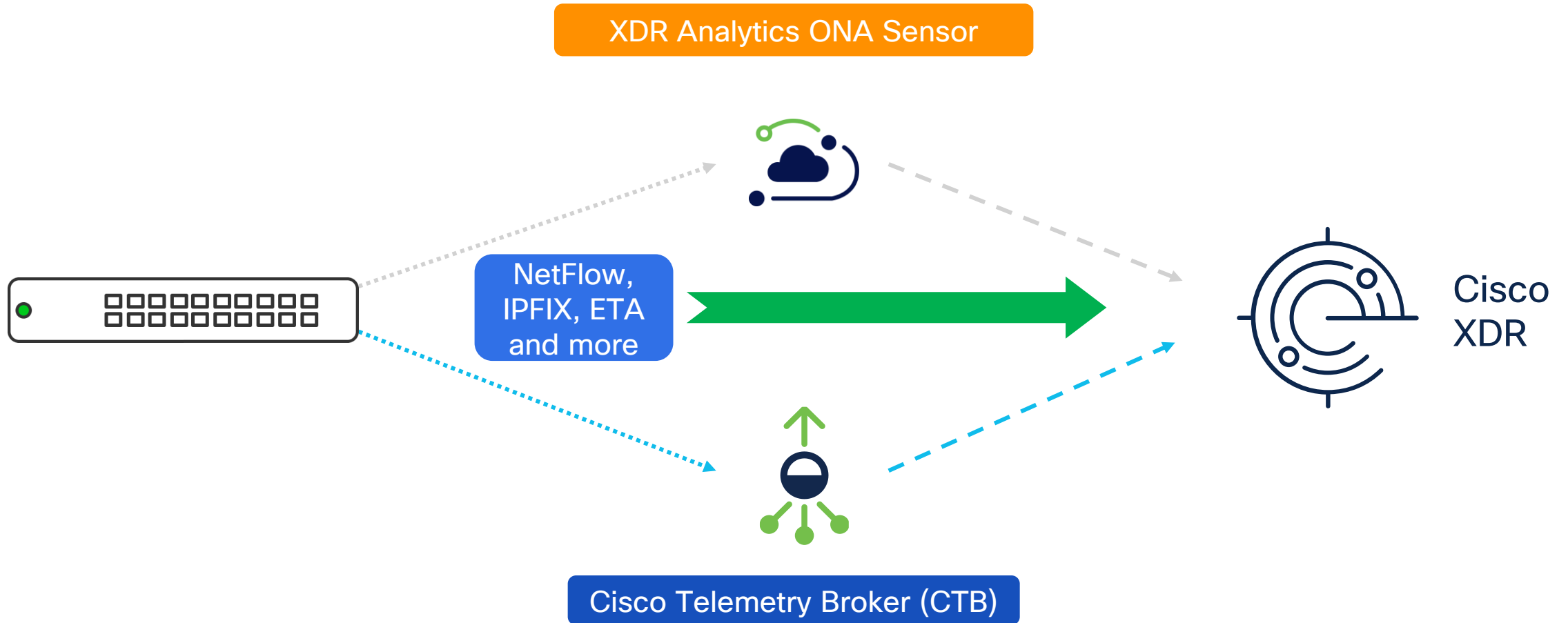


Very sophisticated types of attacks that can ONLY be
detected & understood by combining data from
Network, Endpoint & more.

Where the attack started / propagated ?

The Network

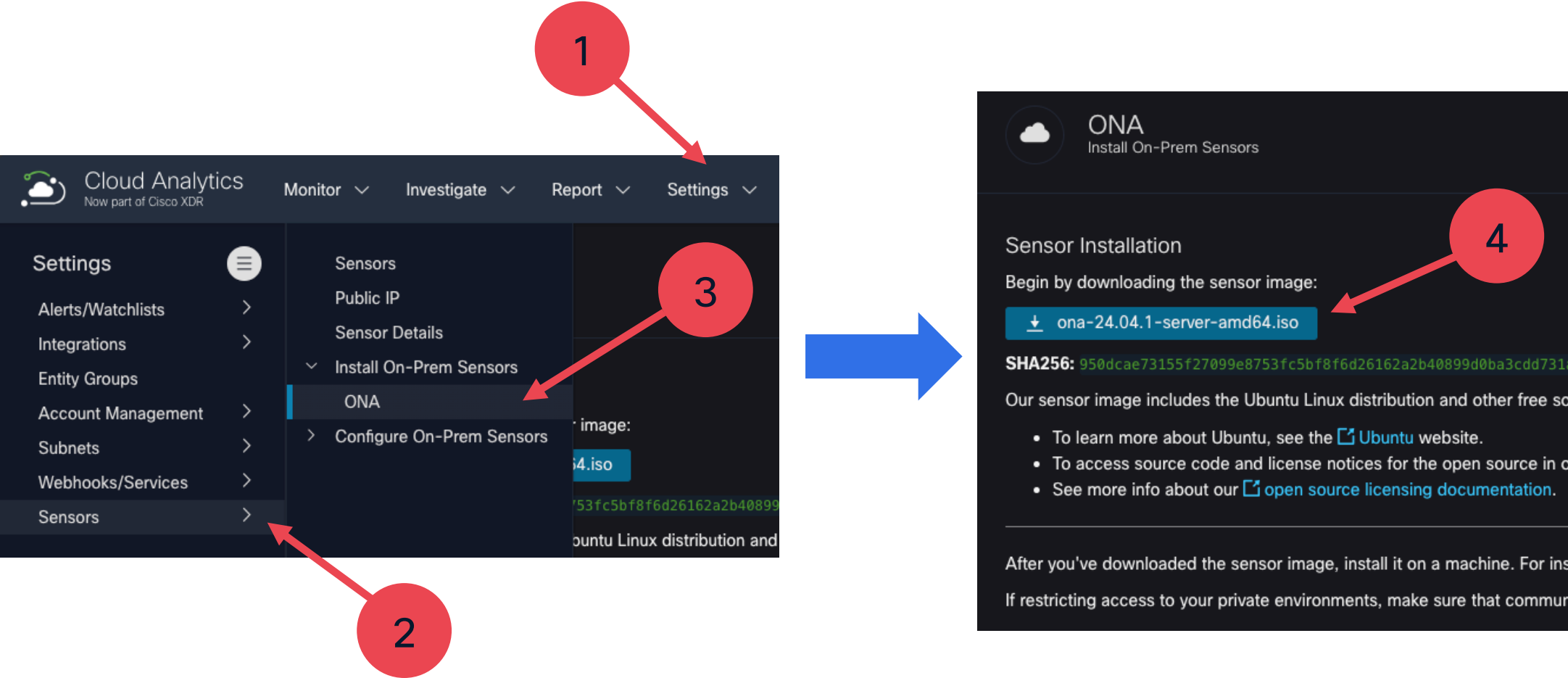
Getting Flows (Raw Telemetry) into XDR



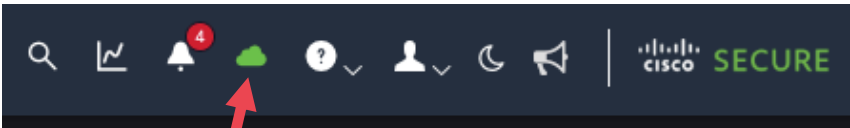
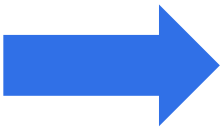
XDR Secure Cloud Analytics ONA Sensor Install

- 1 Log into XDR Analytics (formerly SCA) and navigate to Sensors
- 2 Download the ONA Sensor Appliance ISO
- 3 Install in virtual environment and set a static IP address
- 4 Validate connectivity in the XDR Dashboard
- 5 Configure the IPFIX/NetFlow/ETA Port in XDR Analytics for the sensor

Login to XDR Analytics Download the ISO



Validate Sensor Connectivity to XDR



Cloud Configured On Premises Sensors - ONA

WW-ONA Settings ▾

Hostname: ona-b70352

IP Address: 10.10.0.55

Heartbeat Received: ● 2024-05-29 08:33:11 MDT

Heartbeat Sent: 2024-05-29 08:33:10 MDT

Last Flow Record: ● 2024-05-29 08:20:00 MDT

Flow Exports (NetF... 2024-05-29 08:20:00 MDT

PNA (mirror port): 2024-05-29 08:20:00 MDT

[all sensor details >](#)

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKSEC-2531

Configure IPFIX/ETA/NetFlow

Each type of telemetry on Separate port number

Sensor IP address

Cloud Managed Network - Sensors - ONA

Host: WW-ON-...-b70352

IP Address: 10.10.0.55

Heartbeat Received: 2024-05-2

Heartbeat Sent: 2024-05-2

Last Flow Record: 2024-05-2

Flow Exports (NetF... 2024-05-2

PNA (mirror port): 2024-05-2

Settings

- change name
- configure Netflow/IPFIX
- configure monitoring
- configure Syslog
- configure SNMP
- all sensor details
- delete sensor

Sensor: ona-b70352

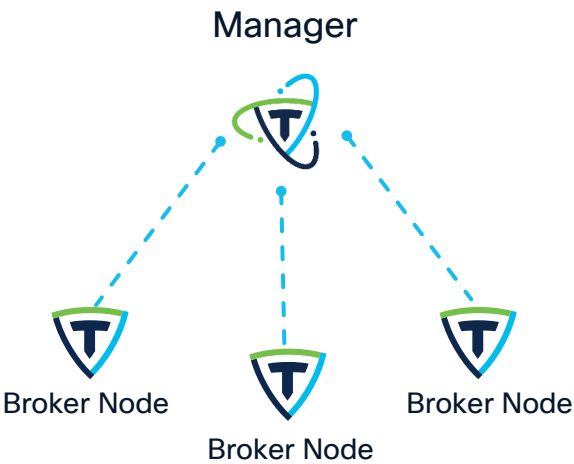
Probe Type	Port	Protocol	Source	State	Enabled	
Enhanced NetFlow (et-analytics)	9996	UDP	Standard	✓	☒	
IPFIX	2055	UDP	Standard	✓	☒	
NetFlow-v9	9995	UDP	Standard	✓	☒	

1-3 of 3 results | 1 / 1

Port/s to use for flow export configuration in dashboard

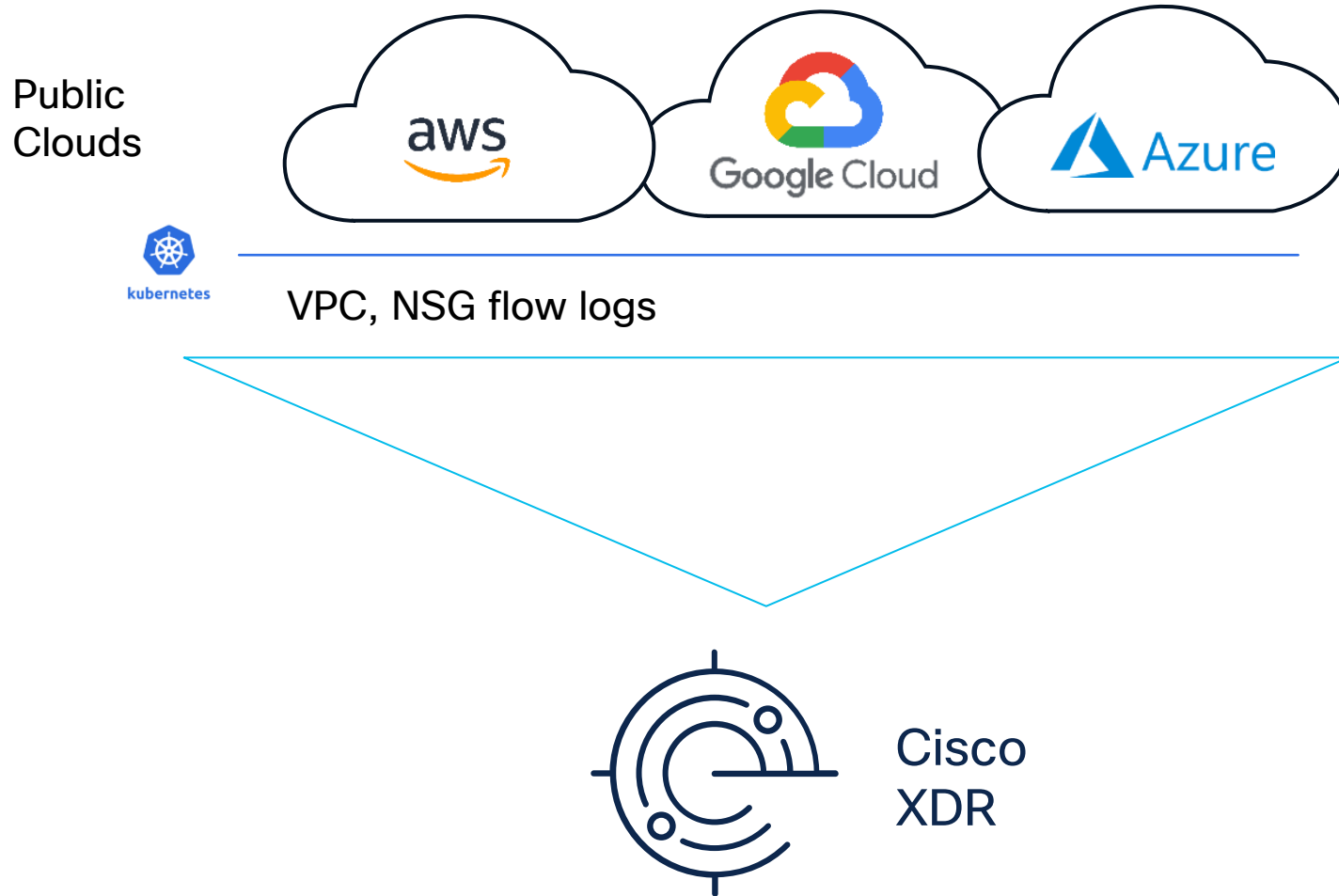
ONA or CTB

	ONA	CTB
Price	\$0	\$ - Ingest
Resource Utilization	Low	High
VMs	1	2
Ingests Netflow,IPFIX,NSEL	✓	✓
Support HA	✗	✓
Easy Install for POVs	✓	✗
Data transform	✗	✓
Syslog Export	✓	✗
ISE Integration	✓	✗
Broker to multiple locations	✗ *Only sends to XDR	✓
Ingest Syslog, Cloud Logs, NVM	✗	✓ *Only applies to SNA
Transform SPAN to IPFIX	✓	✓ *Includes NBAR for S



https://www.cisco.com/c/dam/en/us/td/docs/security/Telemetry_Broker/Deployment/CTB_2_0_1_Virtual_Appliance_Deployment_and_Configuration_Guide_DV_1_0.pdf

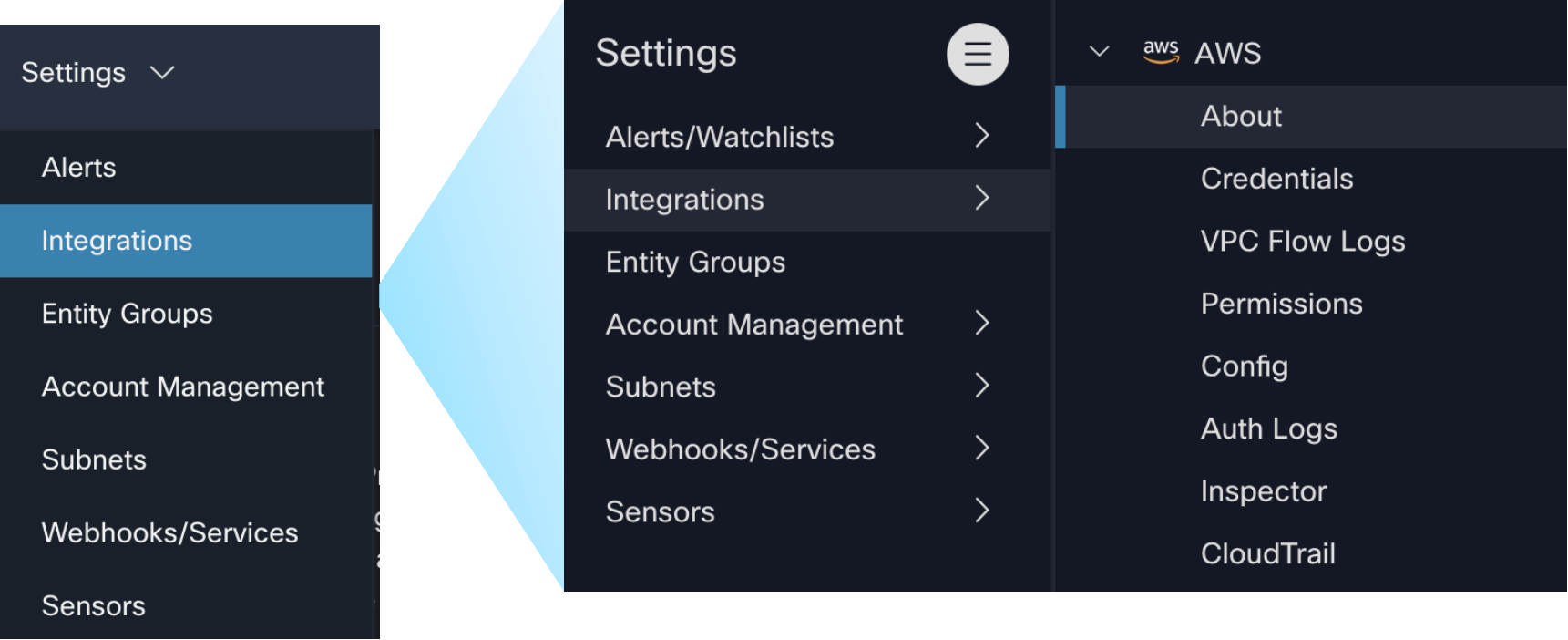
My workloads are in the Cloud



VPC Flow Logs For network analytics and NDR behavioral based detections

Cloud specific Attacks Identity cloud specific attack by ingesting other data with native integration as CloudTrail logs.

AWS Integration Example



Simple but require Privileges

- 1 Create IAM
- 2 Copy ARN to SCA
- 3 Configure VPC and point to S3
- 4 Configure Cloud Trail
- 5 Add S3 path Trail Log bucket name

Meraki Native integration into XDR

Correlation of network findings with other security findings for **comprehensive visibility**.

Simplified connector-less **configuration** for Meraki MX NetFlow to Cisco XDR Cloud.

Asset context from Meraki devices and firewall **response actions** from Cisco XDR.

The screenshot displays the Cisco Meraki Security Center interface. The left sidebar contains navigation options: Global Overview, Organization Explorer (selected), Network all-time-campus-networks, Network-wide, Switching, Insight, and Organization. The main content area is titled 'Security Center' and shows 'MX Summary', 'MX Events', and 'XDR Incidents'. A summary bar indicates 56 Incidents, 8 New Incidents, 26 Open Incidents, and 13 Unassigned Incidents. Below this is a table of incidents with columns for Priority, Name, Source, Created, and Assigned. The first incident, 'Data Loss and Suspicious Activities on Multiple Devices', is highlighted. A right-hand panel provides details for this incident, including its priority (1000), status (Open), and a short description: 'The incident occurred between Oct 23 2024 and Oct 24 2024. A suspect data loss and hoarding were detected on device 320b5646-2d70-4f6d-9ffa-a26154f1e5df by SnaDetections. There were additional suspicious activities on the same and another device involving user obsidian by ScaDetections.' The panel also shows a priority score breakdown (1000) and a list of assets (2) and observables (19).

Priority	Name	Source	Created	Assigned
1000	Data Loss and Suspicious Activities on Multiple Devices	Cisco XDR Analytics	5 days	HJ AS AS
1000	Multiple Masquerading and Credential Theft Attempts Detected	Cisco XDR Analytics	6 days	Unassigned
1000	Multiple HiveCredTheft Detections on User dapqa_1	Cisco XDR Analytics	7 days	AS AS AS
1000	[Terminated] Malicious File Activities Detected by CrowdStrike	Cisco XDR Analytics	8 days	RR
1000	SuspiciousFileWritten	Cisco XDR Analytics	8 days	AS
1000	Multiple Defense Evasion and Credential Theft Attempts Were Terminated	Cisco XDR Analytics	8 days	RR
1000	Powershell Execution Terminated on Multiple Devices	Cisco XDR Analytics	8 days	RR
1000	Repeated Powershell Executions and Masquerading Defense Evasion	Cisco XDR Analytics	13 days	RR
1000	Multiple Privilege Escalation and Defense Evasion Activities	Cisco XDR Analytics	14 days	RR
1000	Malware Executed on MY-DEVICE-42 - Incident by Cisco XDR Automation	Cisco XDR Automation	16 days	SR

How to connect your Meraki MX to Cisco XDR

The screenshot shows the Cisco Meraki dashboard interface. On the left is a sidebar with navigation links: Network, Secure Connect, Network-wide, Assurance, Security & SD-WAN, Wireless, Cameras, Insight, Organization, Access Manager, and Find in Menu. The 'Organization' link is highlighted with a red circle containing the number '1'. A red arrow points from this circle to the 'Integrations' link in a dropdown menu that is open under 'Organization'. The main content area is titled 'Integrations' and has tabs for 'Browse' and 'My integrations'. Under 'Browse', there is a section for 'Cisco Products' with a sub-header 'Catalyst SD-WAN' and a description: 'Connect to a Catalyst SD-WAN overlay to enable simple SD-WAN interconnects.' The dropdown menu also contains a 'Configure' section with links to Settings, Integrations (highlighted with a red arrow), API & Webhooks, Configuration Sync, MDM, Administrators, Camera and Sensor Roles, and License Info.



Meraki

Network

Secure Connect

Network-wide

Assurance

Security & SD-WAN

Wireless

Cameras [Learn more](#)

Insight

Organization

Access Manager [New](#)

Find in Menu

Integrations

BrowseMy integrations

Cisco Products

Innovate and integrate with Cisco products.

Catalyst SD-WAN

Connect to a Catalyst SD-WAN overlay to enable simple SD-WAN interconnects.

SD-WAN

Cisco XDR

Send flow telemetry to identify and prioritize security incidents.

Analytics

Cisco Spaces

Seamless Onboarding, Occupancy Analytics, Device Tracking & more.

Smart Spaces

Splunk

Monitor network and security events in your environment.

Network Security

Ecosystem Partners

Explore and integrate with ecosystem partner applications.

Genea Security

By Genea

Set up to view Genea physical access control events on the Meraki Vision Portal.

Physical access control

PagerDuty

By Cisco

Send Meraki alerts to PagerDuty to respond to network incidents.

Incident Management

[Browse Marketplace](#)

3

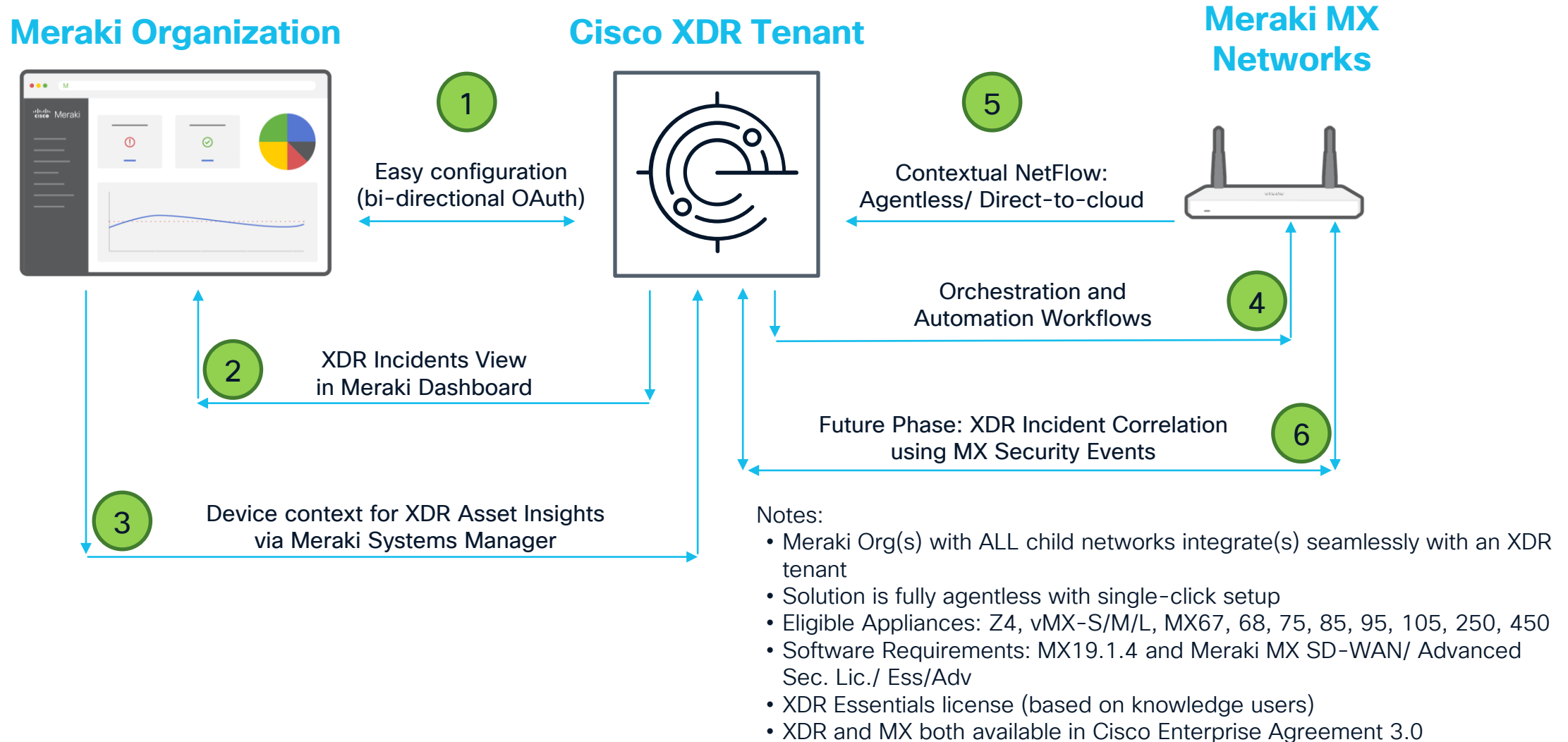


Configure Networks

Select the networks to send flow telemetry to XDR. See [documentation on XDR](#)

The screenshot shows the 'Networks' page with a search bar, a filter icon, and a count of '2 networks'. Below the header is a table with columns: Network, XDR status, Tags, XDR eligibility, Model, Firmware, and License compliant. The first row is highlighted, showing a network that is 'Enabled', 'Eligible', 'MX67W', 'MX 19.2.2', and 'Compliant'. A red box highlights the 'XDR eligibility' column and its value 'Eligible'. A red arrow points to the 'Enable' button in the top right corner.

Meraki MX and Cisco XDR Integration Explained



SNOC ?

NOC

- ✓ Quickly respond to incidents to minimize downtime and impact.
- ✓ A tool that provides real-time monitoring and alerting of events on my network
- ✓ Visibility to my entire organization

SOC

- ✓ A correlated view of security incidents across my environment
- ✓ Security tools to help me work with speed, accuracy and confidence
- ✓ Remediate threats with guidance and automated playbooks.



SNOC

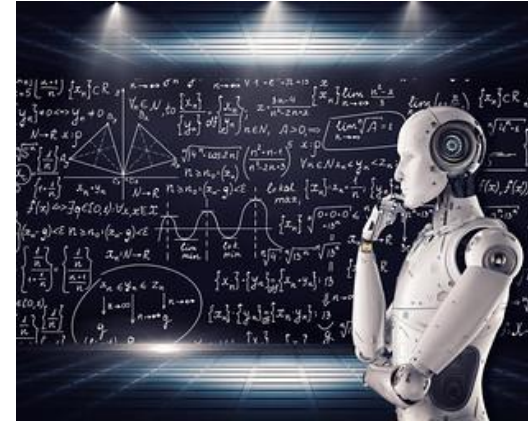
Demo Network Telemetry

What is the Number 1 Initial Access Threat Vector ?

- Email continues to be the #1 threat vector



As attackers are using more advanced techniques, anomalous behavior can be detected using AI/ML based engines.



Targeted attacks are harder to detect with systems that are solely based on global threat feed intelligence.

XDR Incident Generation with Email Threat Defense

Simple API based integration



ETD sightings must have at least one other detection source

Initial Access and Network base telemetry

Which devices / assets were impacted ?

Endpoints

Cisco XDR Integrates with Multiple EDRs

Correlation, Investigation, Response, Asset Insights

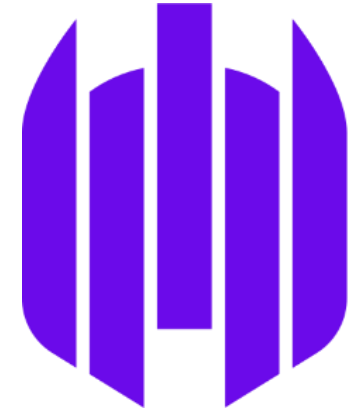
CrowdStrike Falcon



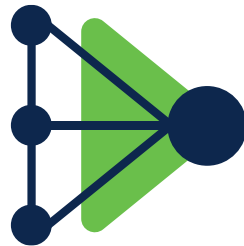
Microsoft
Defender



SentinelOne

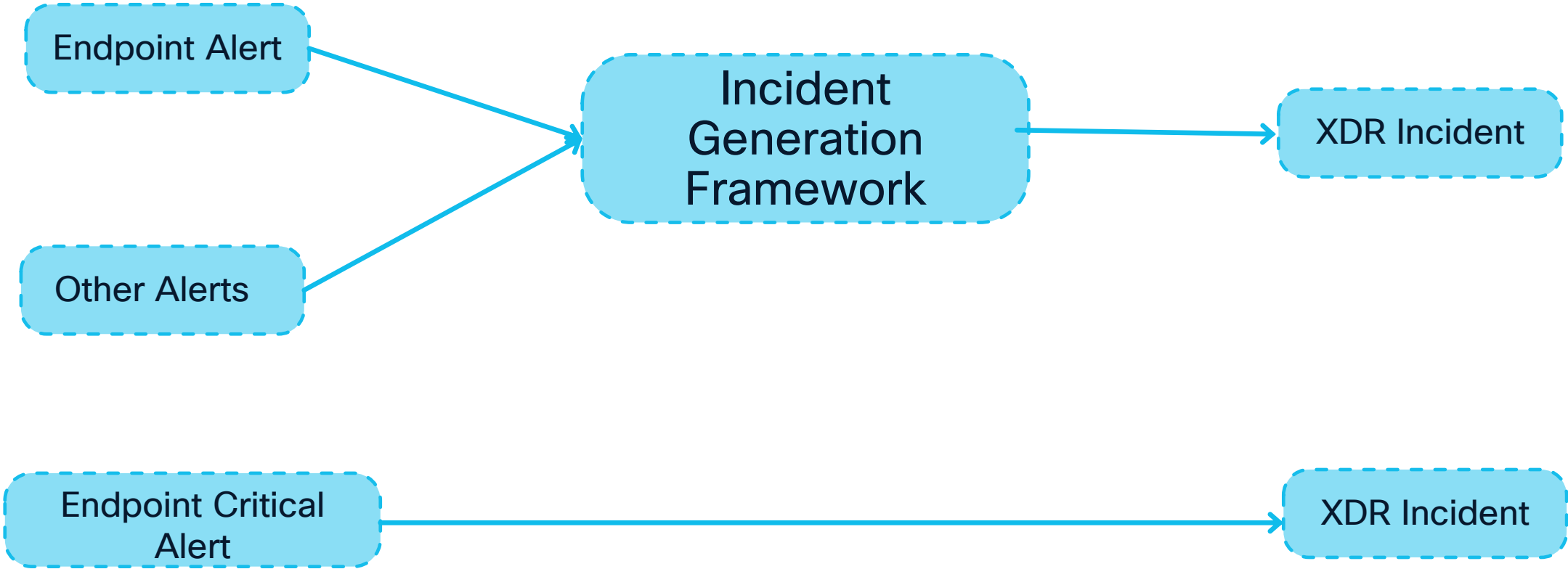


Cisco Secure Endpoint



Demo Integration

XDR Incident Generation with EDRs



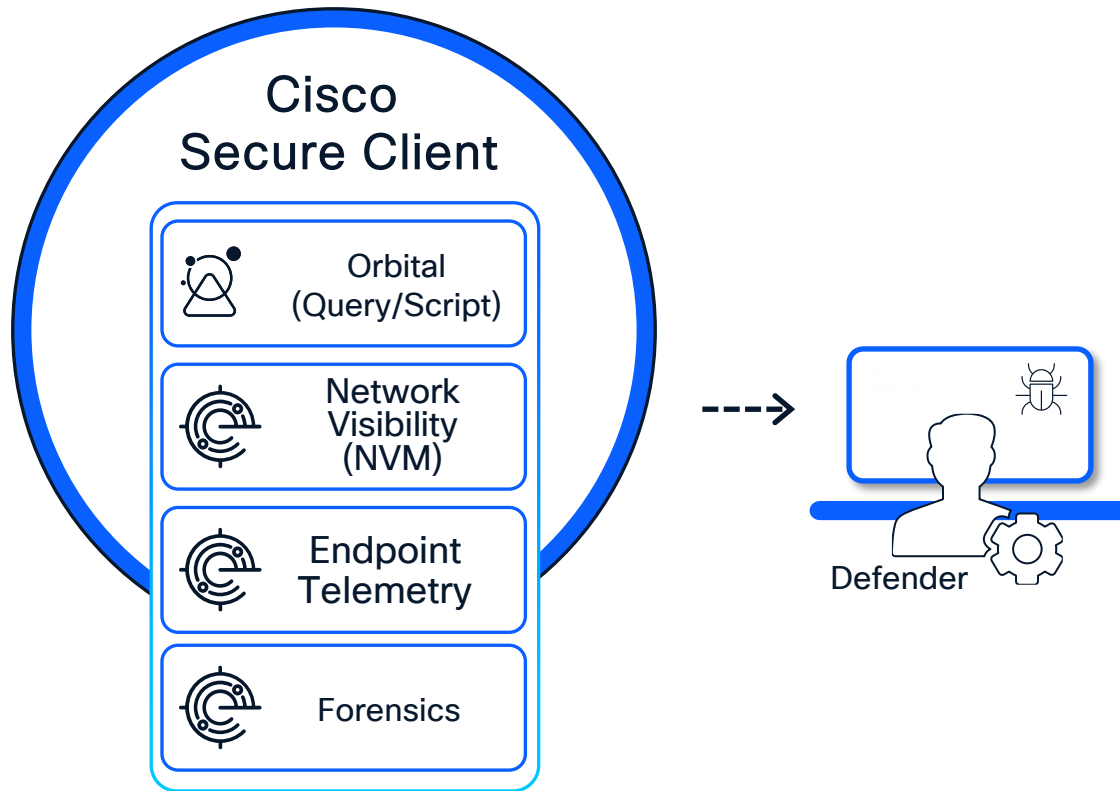
XDR Response with EDR

The screenshot displays the Cisco XDR 'Incidents' page. At the top, it shows '1000 Incident Reported' and 'Malicious Activity Detected Through Multiple Security Tools'. Below this, a detailed description of the incident is provided, mentioning its occurrence on Sep 10 2024 and the detection of suspicious activities. The interface includes tabs for 'Overview', 'Detection', 'Response' (which is active), 'Worklog', and 'Report'. A sidebar on the left lists the response phases: Identification, Containment (highlighted), Eradication, and Recovery. The main panel shows a list of containment actions under the 'Containment' phase, including 'Contain Incident: Assets (Devices)', 'Contain Incident: Assets (Users)', 'Contain Incident: IPs', 'Contain Incident: Domains', 'Contain Incident: URLs', and 'Contain Incident: File Hashes'. Each action has an 'Execute' button. A right-hand panel titled '4 Items' shows a list of items categorized as 'Malicious (1)', 'Unknown (2)', and 'Clean (1)', with a search bar and a 'Select All' option.

Build in Actions for Response

- Isolate a device or a host
- Block file hashes across all endpoints
- Block an IP if the EDR permits it

Expanding EDR with Network Visibility Module

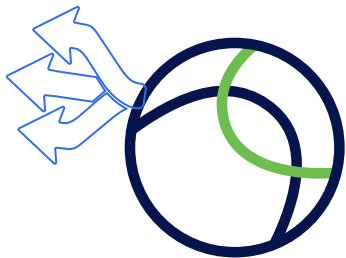


Network Visibility Module (NVM)

- Endpoint Network Flow Logs
- Direct upload of flow data to XDR Analytics engine
- Can be combined with network sources generating flow information

Each Module can be deployed alone

Network + Endpoint Visibility Together



Netflow/IPFIX

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

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

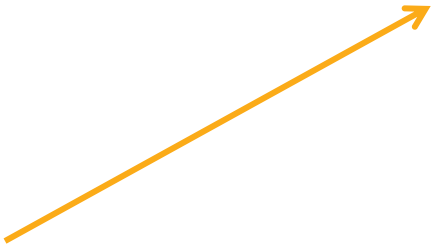
NVM (IPFIX Formatted)

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

Deep Endpoint
Visibility

- User
- Traffic Stats
- Processes
- Applications
- SaaS Used
- Accounts
- Destinations
- Machine Details

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



NVM Event Viewer in XDR Analytics

New NVM Flows Tab

INSTANT FILTERS

Search activity per attribute or many with advanced search.

Telemetry Details

See the detailed telemetry collected from the flow

The screenshot displays the 'Event Viewer' interface with the 'NVM Flow' tab selected. The interface includes a search bar, filter buttons, and a table of network flows. A detailed telemetry view is shown for a selected flow.

Applied filters: NOT source_ip_address: "10.1.100.26" X NOT destination_ip_address: "10.1.100.26" X 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
2023-05-23 14:10:59 UTC	10.1.82.156	208.67.222.222	60104	443 (https)	UDP	473	196	dnscryptproxy.exe	a5a0e48042a7bd1f1a671dbc6834179119a542df06dd0a644e...	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	0777fd312394ae1afe0ad48ae2d7b5ed6e577117a4f40305e...	716
2023-05-23 14:10:59 UTC	10.1.82.156	208.67.222.222	53170	443 (https)	UDP	240	196	dnscryptproxy.exe	a5a0e48042a7bd1f1a671dbc6834179119a542df06dd0a644e...	1,392

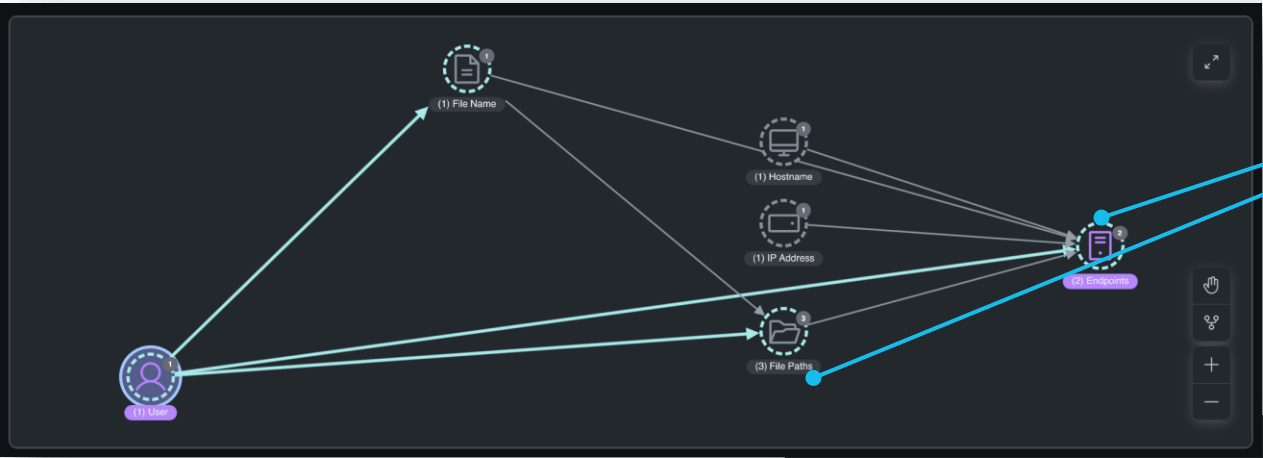
Telemetry Details for selected flow:

- 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\dump s\ipv4" --deviceId=01012737F19A61B --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-EAAEE9CFBDA344DD9886D368F04D6186-resolv.conf"
- process_path: C:\Program Files (x86)\Cisco\Cisco Secure Client\dnscryptproxy.exe

NVM Detections in XDR

Displays Lateral Movement

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



Direct source of observables

For brand-new detections in XDR Analytics

Type	Source	Severity	First Seen	Indicators	Observables	Assets
			2023-05-27T02:48:53.000Z	Cisco Secure Cloud Analytics (security...)	Suspicious Endpoint Activity	loxx-win10vic07.org26.net
			2023-05-27T02:48:53.000Z	Cisco Secure Cloud Analytics (security...)	Malicious Process Detected	loxx-win10vic07.org26.net
			2023-05-27T02:48:53.000Z	Cisco Secure Cloud Analytics (security...)	Suspicious Endpoint Activity	loxx-win10vic07.org26.net
			2023-05-27T02:48:53.000Z	Cisco Secure Cloud Analytics (security...)	Malicious Process Detected	loxx-win10vic07.org26.net
			2023-05-27T01:44:45.000Z	Cisco Secure Cloud Analytics (security...)	Potential Persistence Attempt	loxx-win10vic06.org26.net
			2023-05-27T01:44:45.000Z	Cisco Secure Cloud Analytics (security...)	Suspicious Endpoint Activity	loxx-win10vic06.org26.net
			2023-05-26T19:50:44.000Z	AMP Event		loxx-win10vic06.org26.net
			2023-05-26T19:50:44.000Z	AMP Event		loxx-win10vic06.org26.net
			2023-05-26T19:50:44.000Z	AMP Event		loxx-win10vic06.org26.net

XDR Managed NVM Profiles

From This:

From This:

Collector Type

Use On-Prem Collector

Choose between On-Prem and Cloud Collector

IP Address / FQDN*

10.110.0.4

Enter an IPv4/IPv6 address or FQDN

Port

3055

Enter port number

Secure

WiFi 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 10-2048. 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

Filter Rule

Filter Type

Action

Include/Exclude

Type

Include

Ports

Select All

Phonograph

ParentPhonograph

ProcessIdps

ProcessAlgs

ProcessProcsDps

ProcessProcsDps

ProcessProcsDps

ProcessProcsDps

AddHostLogAndProcAndNet

Logged In User

LoggingCheckAccountType

ProcessName

ProcessAccount

ProcessUserAccountType

ProcessPath

ParentProcessName

ParentProcessPath

ParentProcessUserAccountType

ProcessPath

ProcessId

ParentProcess

DistributionName

IDBuffs

LldpCount

LldpCount

LldpCount

VirtualInterfaceName

CDName

OSName

OSVersion

ProcessNameAndPath

SystemType

OSEdition

ModemSerialNo

ModemSerialNo

ModemSerialNo

InterfaceName

InterfaceType

InterfaceName

SSID

Status

To This:

Profiles

All Profile Types

Q Search By Name

Profile Name	Profile Type	Created
Cloud Management Default Profile	Cloud Management	July 21, 2023 at 12:09:38 PM system
NVM Cloud Default Profile	Network Visibility Module	July 21, 2023 at 12:09:38 PM system
New Profile	Cloud Management	September 24, 2022 at 11:53:53 AM

Default XDR Deployment

- Default Cloud Managed Profile
- Default NVM Profile

Just download & install, no config needed

NVM Demo

The 3 Critical Data Sources for XDR

Endpoint Detections



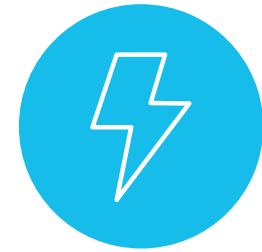
Leverage the detections of Endpoints where the Threat executes

Network Telemetry



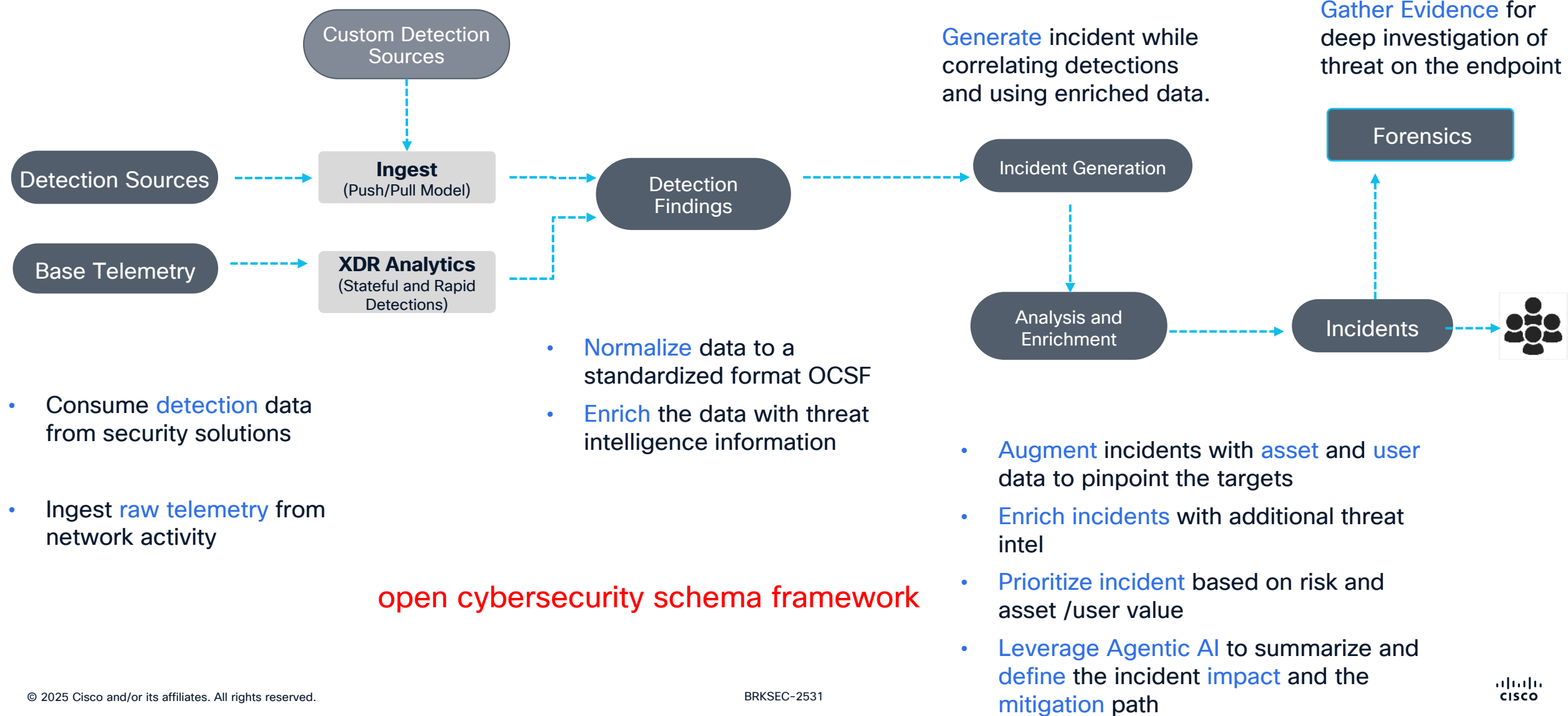
Detect beyond the endpoint into the pre and post execution of a threat

Network Visibility Module



Key Component for Linking Network data and EDR data

How XDR data is processed

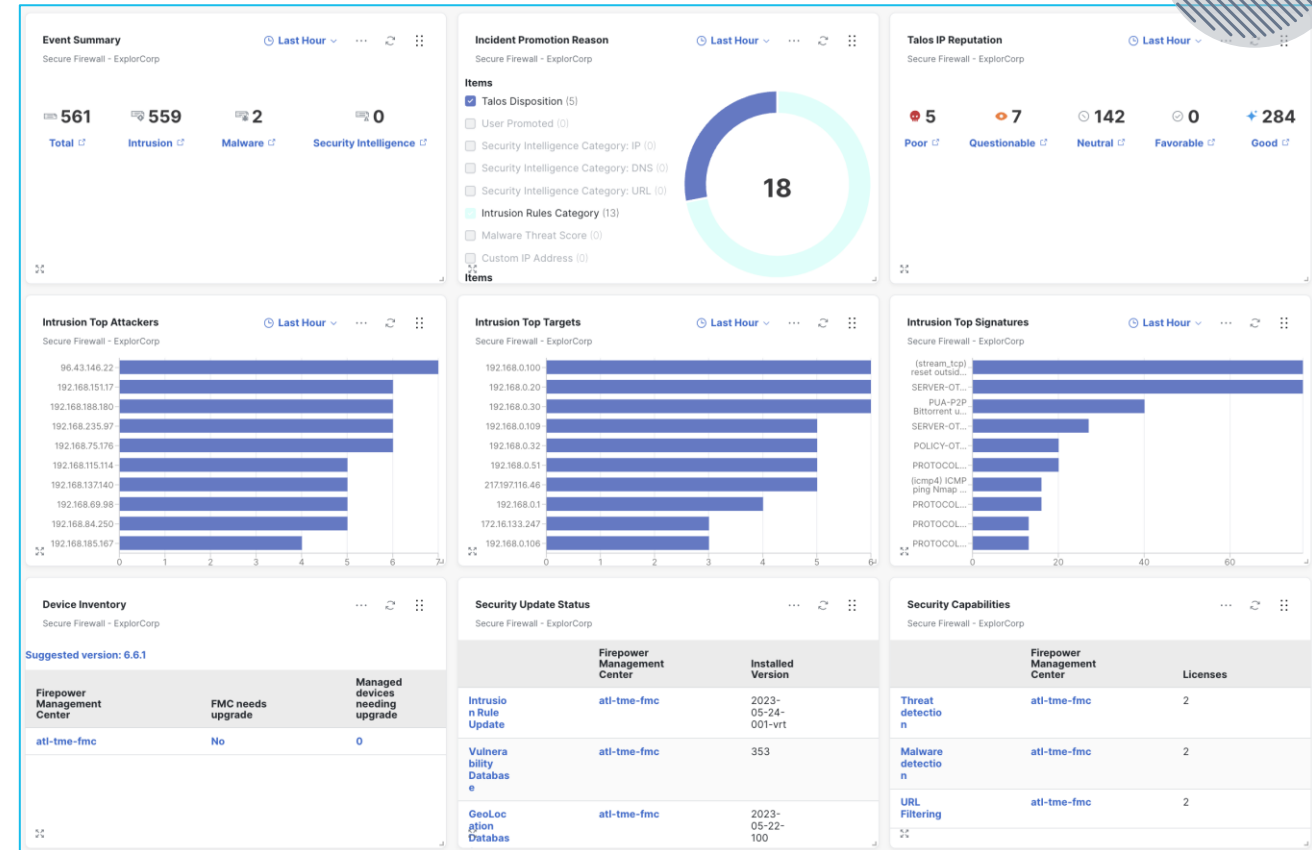


Value Integration: Secure Firewall

<https://www.ciscolive.com/on-demand/on-demand-library.html?search=adi%20sankar&search=adi+sankar#/session/1731453090732001UE9T>

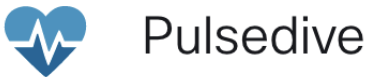
Integrations

- Dashboard
- Investigation
- Connections Events sent to XDR analytics and network detection applied
- Security Events sent to XDR and Used in enrichment and investigation
- Requires SAL+ CDO



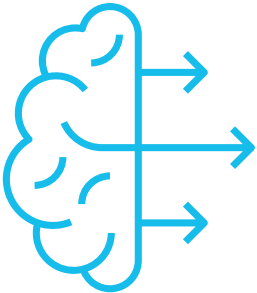
Value Integration :Threat Intelligence is a Key

59.93.19.92		Malicious	IP Addr...	2023-03-31T09:10:13.6... 2023-04-30T09:10:13.6...	TALOS IP B...	High
59.97.169.111		Malicious	IP Addr...	2023-03-31T09:10:13.6... 2023-04-30T09:10:13.6...	TALOS IP B...	High
b0c57.binan...		Malicious	Domain	2023-03-31T08:46:51.4... 2023-04-07T08:46:51....	ZeroDot1 C...	Medium



Pulsedive

and more...



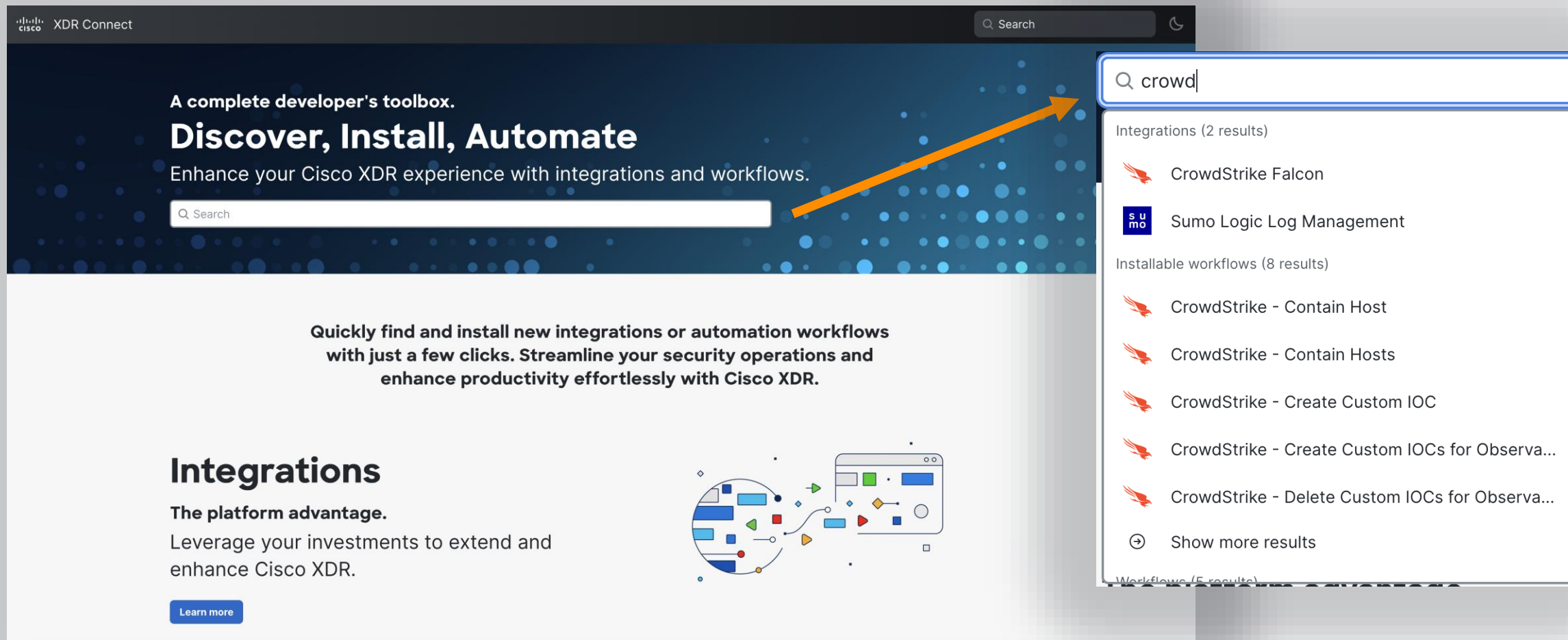
- Use public and private sources of intelligence to achieve better threat identification
- Create and customize your own feeds based on your environment and needs



5 TI sources in 3 minutes

https://youtu.be/7nCRMHo4_9Q?si=cLLTd41w1wSmSL4u

Cisco XDR Connect – Easy Configuration and Integration



The screenshot displays the Cisco XDR Connect web interface. At the top, the header includes the Cisco logo and 'XDR Connect' text, along with a search bar and a moon icon. The main banner features the text 'A complete developer's toolbox. Discover, Install, Automate' and 'Enhance your Cisco XDR experience with integrations and workflows.' Below this is a search bar. A large orange arrow points from this search bar to a magnified view of the search results on the right. The magnified view shows a search for 'crowd' with two integration results: 'CrowdStrike Falcon' and 'Sumo Logic Log Management'. Below these are eight installable workflows, all related to CrowdStrike, including 'Contain Host', 'Contain Hosts', 'Create Custom IOC', 'Create Custom IOCs for Observa...', and 'Delete Custom IOCs for Observa...'. A 'Show more results' link is also present. The bottom section of the main interface is titled 'Integrations' and 'The platform advantage.', with a 'Learn more' button.

A complete developer's toolbox.
Discover, Install, Automate
Enhance your Cisco XDR experience with integrations and workflows.

Q Search

Q Search

Integrations
The platform advantage.
Leverage your investments to extend and enhance Cisco XDR.
[Learn more](#)

Quickly find and install new integrations or automation workflows with just a few clicks. Streamline your security operations and enhance productivity effortlessly with Cisco XDR.

Q Search

Q crowd

Integrations (2 results)

-  CrowdStrike Falcon
-  Sumo Logic Log Management

Installable workflows (8 results)

-  CrowdStrike - Contain Host
-  CrowdStrike - Contain Hosts
-  CrowdStrike - Create Custom IOC
-  CrowdStrike - Create Custom IOCs for Observa...
-  CrowdStrike - Delete Custom IOCs for Observa...
-  Show more results

Workflows (5 results)

* Enhance your Cisco XDR experience with integrations and workflows with [XDR Connect](#)

How do I respond to the attack?

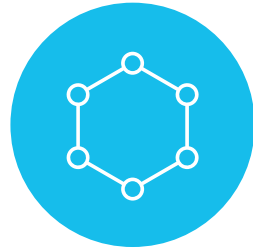
Incident response in four stages

Identify



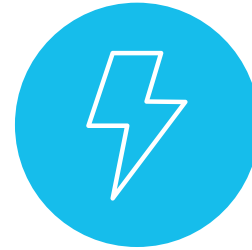
Review the incident and confirm the findings

Contain



Act against impacted hosts, domains, files, etc.

Eradicate



Remediate vulnerabilities and remove malicious content

Recover



Validate remediation and restore impacted services

Robust native response options



Pivot menus

Act on an observable from various places within XDR and other Cisco Secure products



Incident playbooks

Built in Guided, four stage process for incident response, Bring your own playbook and apply it when needed



Automation

Simple or complex workflows that can investigate and respond at machine speed

☐ Hide not applicable tasks

Review Incident

[Generate note](#)

Add a note to record the evidence for assigning a status of Rejected, Open, or Incident Reported.

Analyze Indicators

Action required [Review note](#)

Create judgment(s), as necessary, and add a note confirming any Malicious or Suspicious reputations.

Identify Affected Hosts

Action required [Review note](#)

Add a note with summary of findings on the investigations of hosts found with malicious indicators.

Confirm Incident

Partially complete [Execute](#)

Update the incident status to "Incident Reported" and, if the incident has assignees start a chat room...

Document and Notify

Complete [Execute](#)

Create an incident ticket with the appropriate parameters and contextual incident information.

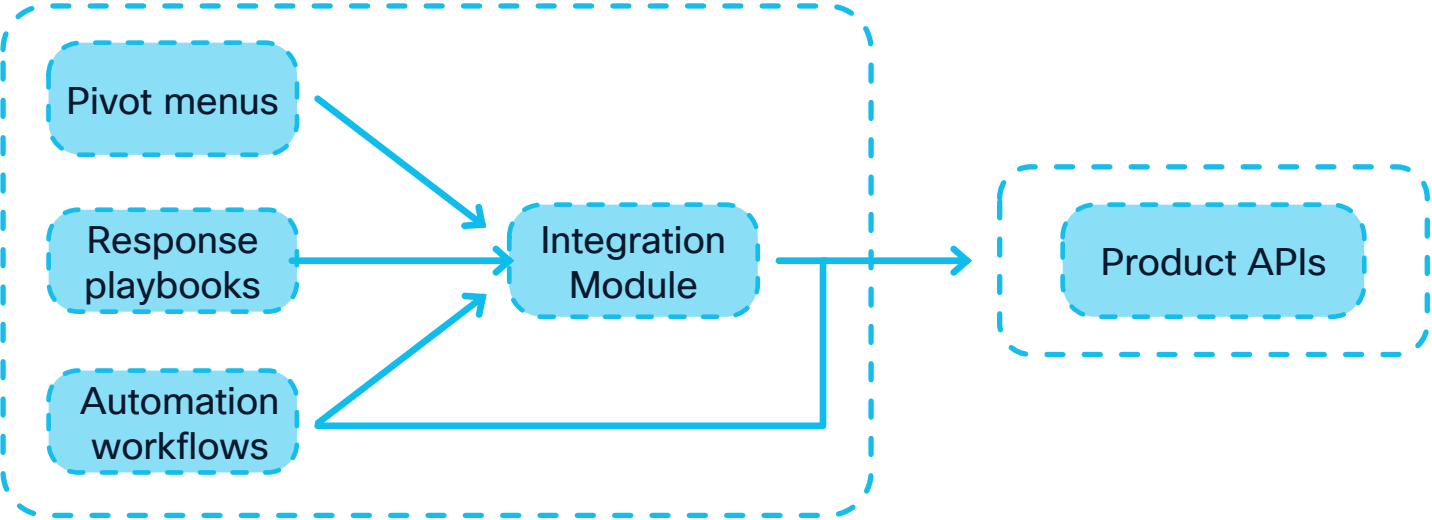
Architecture

Wide variety of actions

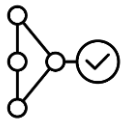
Isolate hosts, block IPs on firewalls, block hostnames in DNS, quarantine messages in a mailbox, and more...

Dynamic Response

Response actions can be automated or user-initiated



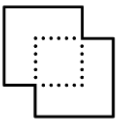
Cisco Products



Endpoint



Cloud Analytics



Firewall



Malware Analytics



MS Defender



CrowdStrike

And many others...

Automation rules

Allow various types of events to cause workflows to run.

- **Approval Task Rule:** An approval task is acted upon within XDR Automation.
- **Email Rule:** An email is received in a pre-defined inbox being monitored for new messages.
- **Incident Rule:** A matching incident is created in the XDR incident manager.
- **Schedule Rule:** A specific date, time, or interval of time has passed.
- **Webhook Rule:** An HTTP call was made to a specific webhook URL.

Triggers

To add a trigger to a workflow, configure an automation rule that determines when a workflow is executed, such as when an incident, specific event occurs, or on a schedule.

Automation Rules Events Webhooks Calendars Schedules

Search

Q Search

×

Type

Select

▼

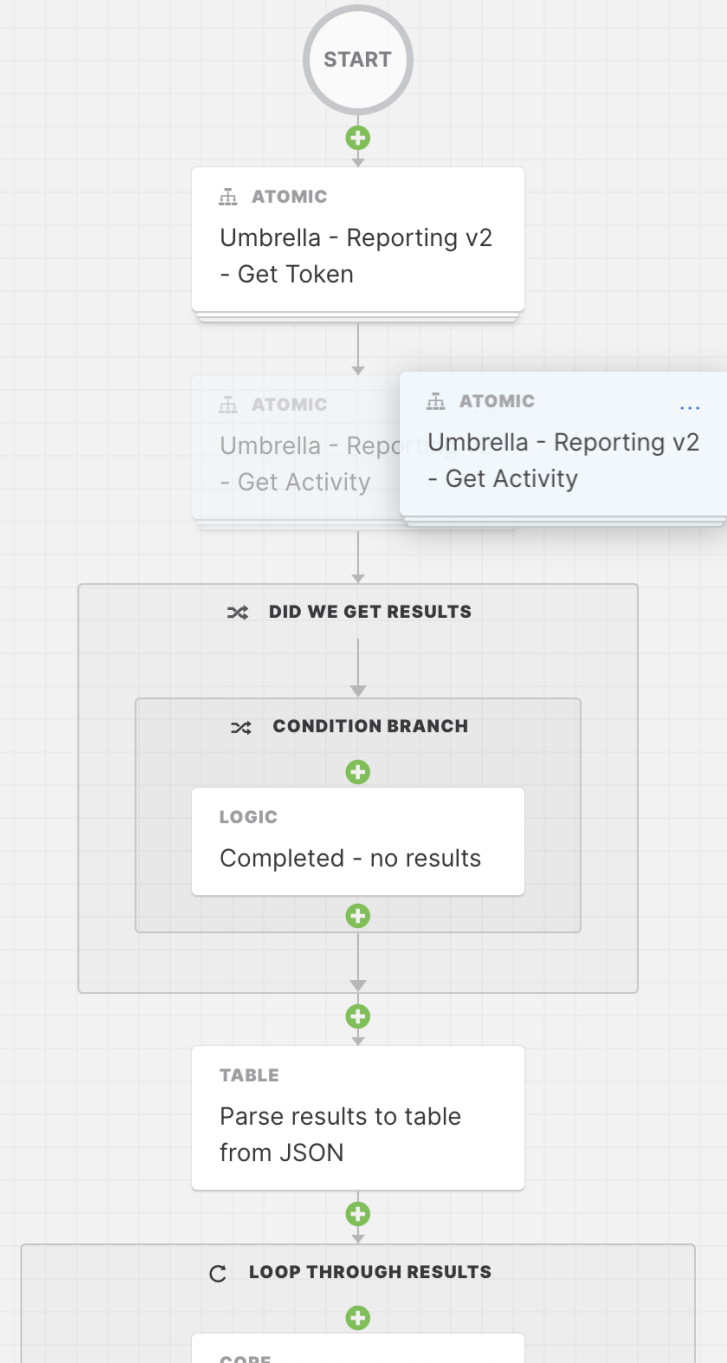
[Reset All](#)

Display name	On/off	Type	Owner
Hourly Workflow	<div></div>	Schedule	user@cisco.com
Incoming Webhook	<div></div>	Webhook	user@cisco.com
Incident Notification	<div></div>	Incident	user@cisco.com

XDR Workflow

A “no to low code” drag and drop editor that allows you to build simple or complex workflows.

- Powers the playbook feature in the incident manager using out of the box workflows.
- Pre-written workflows are available for import from Cisco.
- Wide variety of use cases that are not limited to security or XDR-related outcomes.



Automation Exchange

Exchange allows to find and install automation workflows with community content, ratings and logos.

- **Cisco Managed** – workflows authored by Cisco, including system workflows and atomic actions. Supported by TAC.
- **Cisco Verified** – workflows authored and supported by a Cisco Security Technology Partner.
- **Community** – workflows authored by anyone in the Community. Dependent on license, usually supported by the Cisco DevNet Community on a best-effort basis.
- Third-party repositories.

Exchange

Exchange allows you to find and install workflows that are Cisco Managed, Cisco Verified or have been developed by the Community. Find more information about the content types in [our documentation](#).

[Explore](#) Installed 100 10 Updates available

Search Integration Authorship Type Rating Intent [Reset all](#)

Q Search Select Select Select Select

Featured



Device Insights Test, Cisco Defense Orchestrator

Cisco Managed

4.0 out of 5 ★ 9.9k installs

Searches Secure Malware Analytics for IOCs. Nulla vitae elit libero, a pharetra augue. Maecenas faucibus mollis interdum. Donec id elit non.

Pivot Menu Cisco Duo +3

[Learn More](#) [Install](#)



Lorem ipsum dolor sit amet

Community

4.0 out of 5 ★ 9.9k installs

Searches Secure Malware Analytics for IOCs. Nulla vitae elit libero, a pharetra augue. Maecenas faucibus mollis interdum. Donec id elit non.

Incident Response Cisco Duo +3

[Learn More](#) [Install](#)



Lorem ipsum dolor sit amet

Cisco Validated

4.0 out of 5 ★ 9.9k installs

Searches Secure Malware Analytics for IOCs. Nulla vitae elit libero, a pharetra augue. Maecenas faucibus mollis interdum. Donec id elit non.

Playbook Task Cisco Duo +3

[Learn More](#) [Install](#)

Popular



Lorem ipsum dolor sit amet

Cisco Managed

4.0 out of 5 ★ 9.9k installs

Searches Secure Malware Analytics for IOCs. Nulla vitae elit libero, a pharetra augue. Maecenas faucibus mollis interdum. Donec id elit non.

Playbook Task Cisco Duo +3

[Learn More](#) [Install](#)



CrowdStrike, Meraki, Microsoft Azure

Community

4.0 out of 5 ★ 9.9k installs

Searches Secure Malware Analytics for IOCs. Nulla vitae elit libero, a pharetra augue. Maecenas faucibus mollis interdum. Donec id elit non.

Pivot Menu Cisco Duo +3

[Learn More](#) [Install](#)



Lorem ipsum dolor sit amet

Cisco Validated

4.0 out of 5 ★ 9.9k installs

Searches Secure Malware Analytics for IOCs. Nulla vitae elit libero, a pharetra augue. Maecenas faucibus mollis interdum. Donec id elit non.

Incident Response Cisco Duo +3

[Learn More](#) [Install](#)

All



Lorem ipsum dolor sit amet

Cisco Managed

4.0 out of 5 ★ 9.9k installs

Searches Secure Malware Analytics for IOCs. Nulla vitae elit libero, a pharetra augue. Maecenas faucibus mollis interdum. Donec id elit non.

[Learn More](#) [Install](#)



Lorem ipsum dolor sit amet

Community

4.0 out of 5 ★ 9.9k installs

Searches Secure Malware Analytics for IOCs. Nulla vitae elit libero, a pharetra augue. Maecenas faucibus mollis interdum. Donec id elit non.

[Learn More](#) [Install](#)



Lorem ipsum dolor sit amet

Cisco Validated

4.0 out of 5 ★ 9.9k installs

Searches Secure Malware Analytics for IOCs. Nulla vitae elit libero, a pharetra augue. Maecenas faucibus mollis interdum. Donec id elit non.

[Learn More](#) [Install](#)

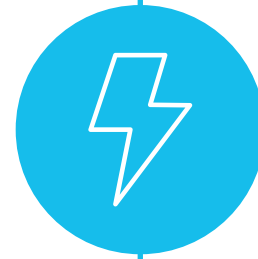
Demo Response

Automation outcomes



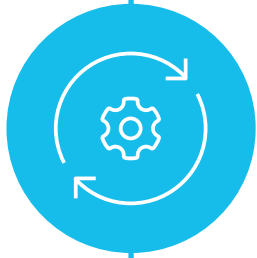
Investigate

Reduce time to investigate by automating data collection and incident generation



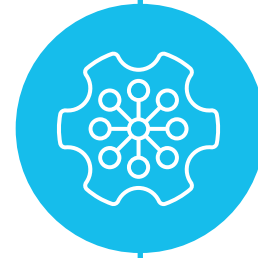
Respond

Automated or one-click responses that can combine multiple products in one action



Simplify

Eliminate repetitive tasks that waste valuable analyst time

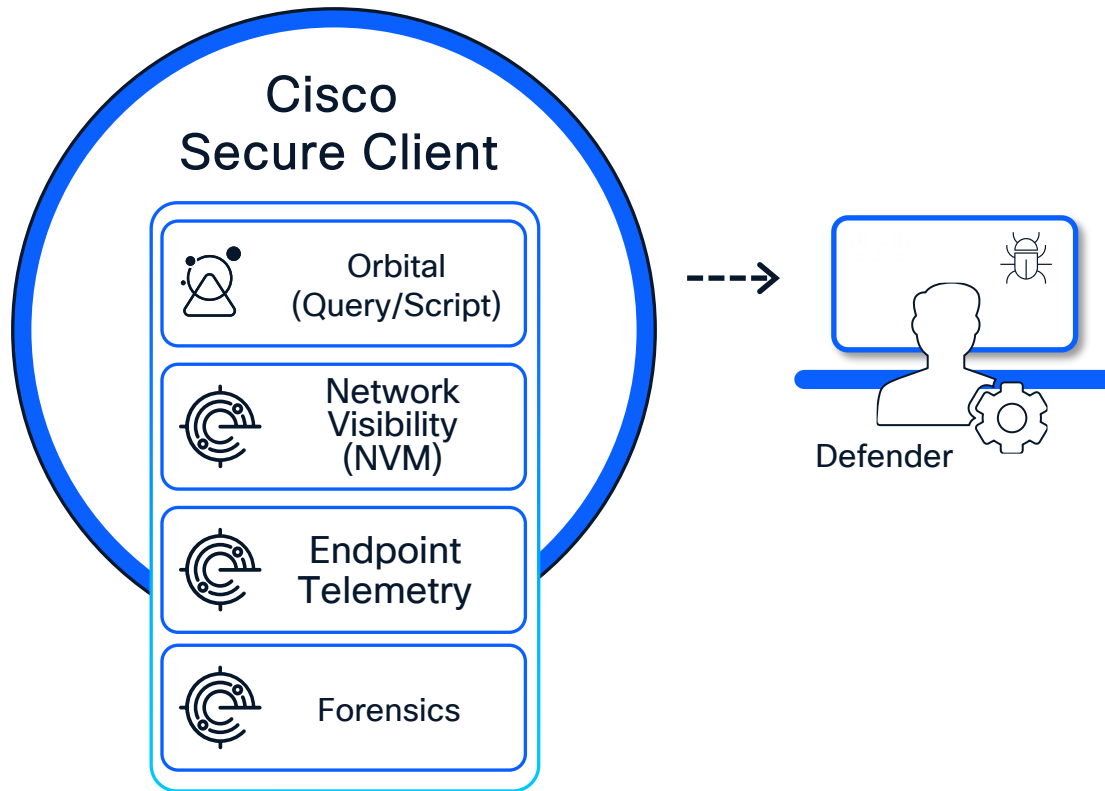


Integrate

Bring products and services together in new ways to address emerging threats

Getting more from your Endpoint

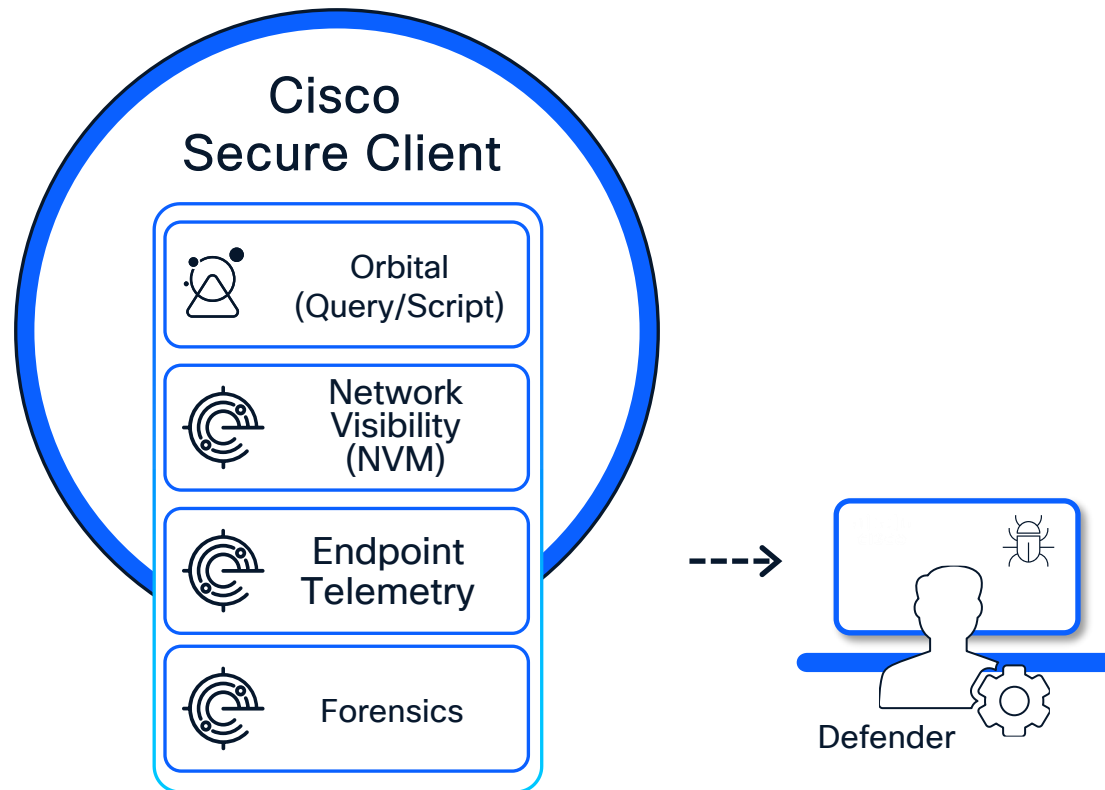
Threat Detection and Response



Orbital

- Easy to use query and response tool
- Highly lightweight
- Allows endpoint queries using simple SQL statements
- Includes an independent python environment to remediate endpoints using python scripts
- 500+ templates in catalog
- MITRE ATT&CK information
- Fully integrated into XDR and endpoint
- Strong API approach

Threat Detection and Response

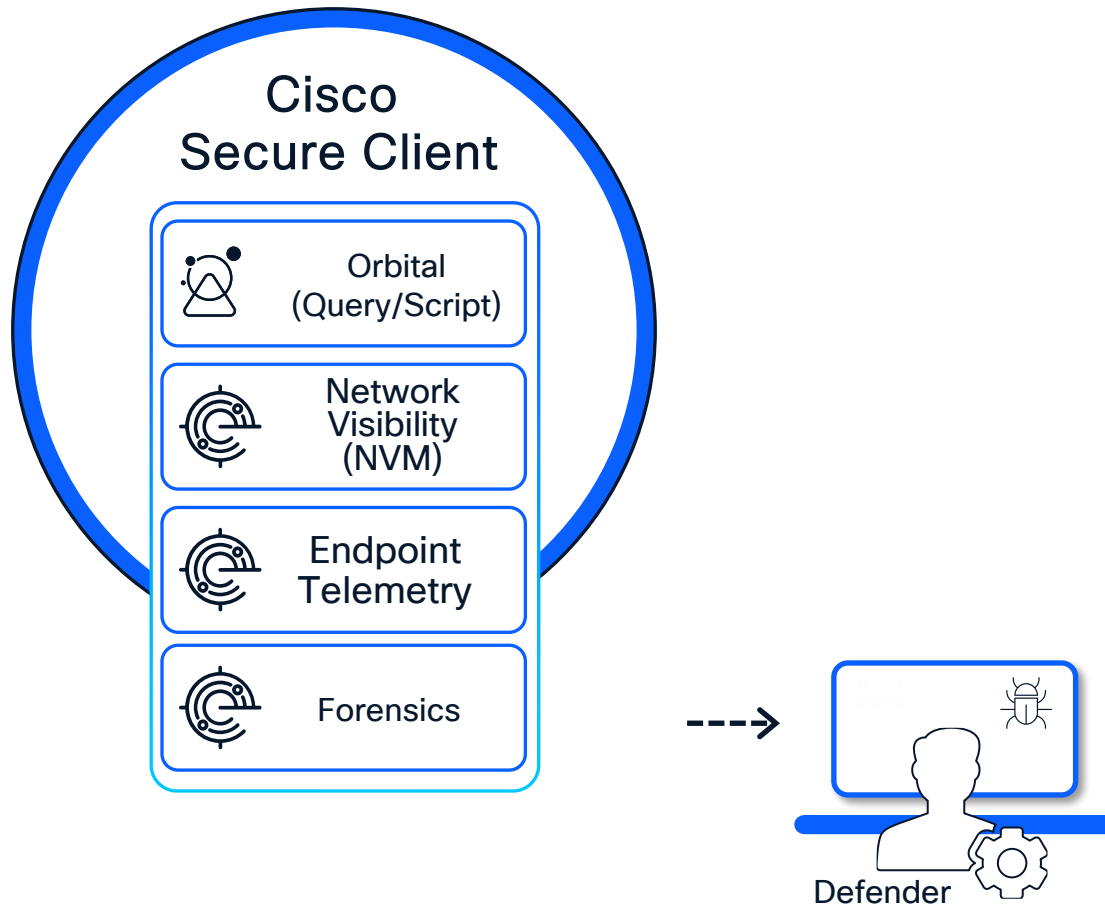


Endpoint Telemetry

- Non-intrusive module to collect endpoint telemetry
- Uploads endpoint telemetry to XDR Analytics engine
- Can be combined with Cisco Endpoint products and third-party endpoint security product
- Combined with NVM, the EVM module allows full insights and analytics into endpoints

Threat Detection and Response

Released 15 October



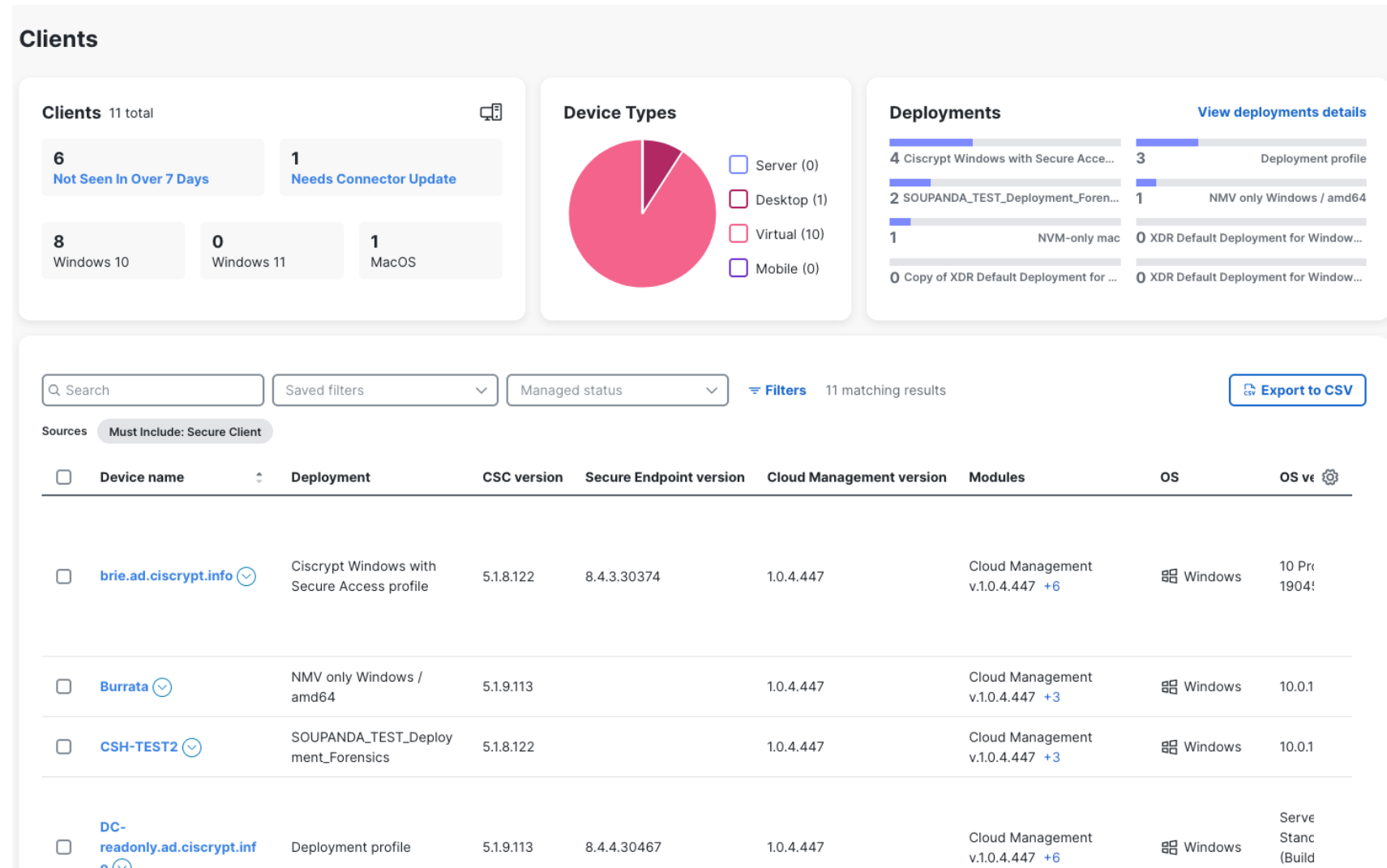
XDR Forensics

- Full Forensics capabilities
- Acquire forensic information for an XDR incident
- Acquisition tasks and Triage tasks (MITRE ATT&CK Attack analyzer) to collect and store forensic data
- Remote Shell and file exchange

How do I manage all of these

Centralized in XDR

- **Inventory of devices** running Secure Client and their status. Another source for XDR Assets.
- **Cloud-based management** of profiles. No more editing XML files and wondering which profile is the most recent.
- **Ability to create and manage multiple deployments.**



Demo on Client Management

Identify The WHO?

Cisco Identity Intelligence

Cisco Identity Intelligence



Users



Machines



Services



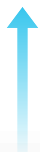
Apps



Data



Behaviors



Auth0

Workday

Okta

GitHub

Ping

Microsoft

Cisco

Google

Amazon

Users:

Cisco Identity Intelligence Integration

- CII is natively provided with XDR for both existing and new customers.
- Customers need to configure their IDPs in Security Cloud Control.
 - Once that happens, data will flow into User Insights and be available in XDR
 - Duo and Entra modules will still live in XDR for Response/Automation actions
- Their IDPs will be available based on their XDR entitlement
 - Essentials: only DUO
 - Advantage/Premier: DUO + all other third parties (ex: Okta, Salesforce, Slack, etc...)

The screenshot displays the user profile for Alex Wilber in the Cisco Identity Intelligence interface. At the top, there is a navigation bar with a 'Back to Users' link, the user's name 'Alex Wilber', and two dropdown menus: 'Add Labels' and 'User value: 10 (Default value)'. The profile is divided into several sections:

- Used devices:** Lists three devices: 'Chrome__Mozilla(WindowsNT;Win;x)AppleWebKit(KHTML,likeGecko...' (last login 2025-05-15), 'EPGWD0T9TLY6U1YTX0JQ (MAZZARELLA)' (last login 2025-05-15), and 'EP7DBLUBVTS3OR989G6N' (last login unavailable). A 'View all' link is present.
- Identity events:** Lists three events: 'users-sharing-authenticators', 'directly-assigned-applications', and 'allow-block-emails'.
- Activity details:** A table showing user activity:

MFA status	Enabled
Usage location	WILMINGTON, DE, US
Last logon	2025-05-15T00:24:40.000Z
Account created	2024-03-07T05:03:31.000Z
Account status	Enabled
Used factors	n_a, password
Used applications	OfficeHome, Microsoft Azure Active Directory, One Outlook Web, Office 365 Exchange Online
IP Addresses	128.107.78.50
- Identity details:** A table showing user identity information:

Display name	Alex Wilber
Login names	alexw@ciscrypt.info
Emails	AlexW@ciscrypt.info, alexw@ciscrypt.info
Phone numbers	—
User ID	f70743c8-2b82-4031-881f-ff31f44cb692_alexw@ciscrypt.info
Sources	Entra ID, Duo, OKTA
- Organization Role:** A table showing organizational details:

Company	—
Department	Marketing
Manager	miriamg@ciscrypt.info
Job title	Marketing Assistant
Employee IDs	—
Groups	Digital Initiative Public Relations, MSFT, Mark 8 Project Team, Retail, Sales and Marketing, U.S. Sales, Everyone

Identity Checks

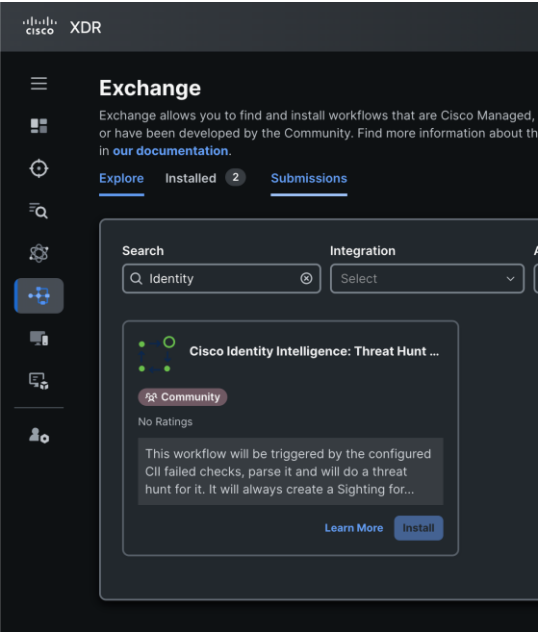
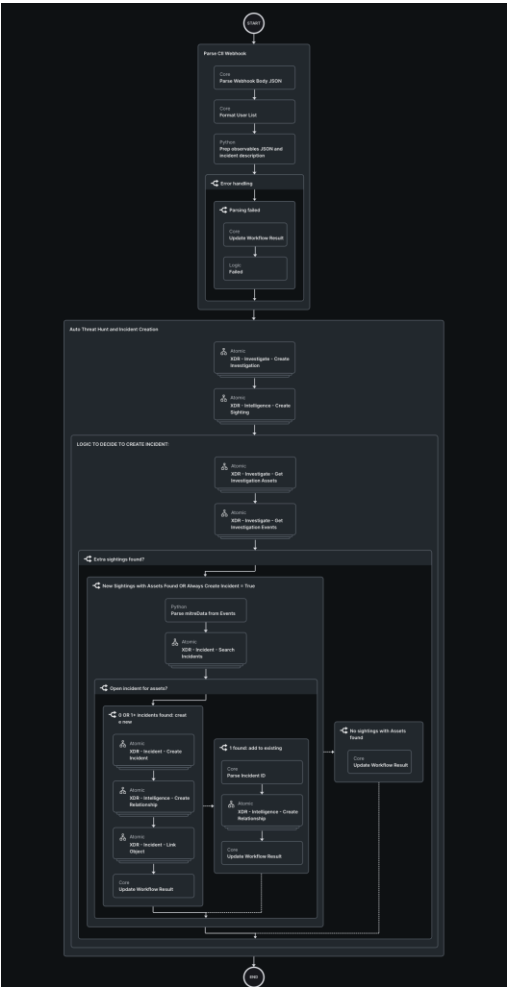
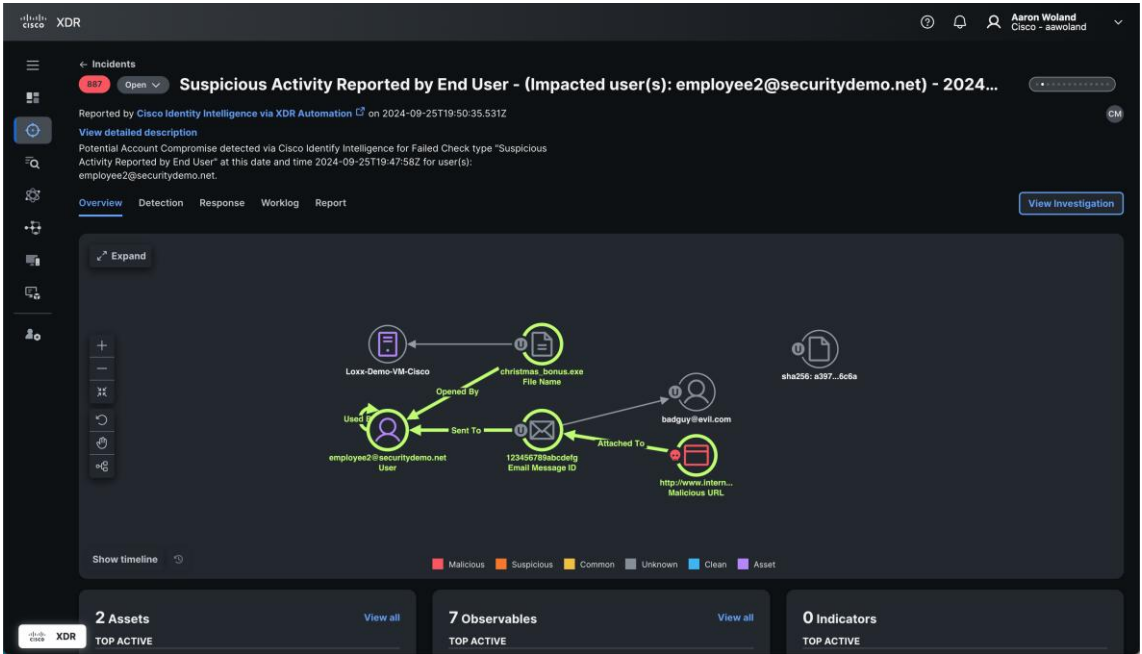
All Checks			Last run: Feb 1, 2025 04:36:13 UTC	
Check	# Failing	# Excluded	Report Channels	
<div><div><div>33%</div><div>No MFA Configured </div><div><div>Critical</div>End Users - Compliance, Identity Posture Insight</div></div></div>	160 → No change since last week → No change since last month	0	<div>+ Add</div>	<div></div>
<div><div><div>78%</div><div>Unused Application for a User </div><div><div>Low</div>End Users - Compliance, Identity Posture Insight</div></div></div>	53 → No change since last week → No change since last month	0	<div>+ Add</div>	<div></div>
<div><div><div>78%</div><div>User in IDP but not in HRIS </div><div><div>Critical</div>End Users - Compliance, Identity Posture Insight</div></div></div>	53 → No change since last week → No change since last month	0	<div>+ Add</div>	<div></div>
<div><div><div>83%</div><div>New Country for Tenant </div><div><div>Moderate</div>End Users - Identity Threat Insight</div></div></div>	40 → No change since last week → No change since last month	0	<div>+ Add</div>	<div></div>
<div><div><div>88%</div><div>Registered Location Mismatch </div><div><div>Low</div>End Users - Identity Threat Insight</div></div></div>	28 → No change since last week → No change since last month	0	<div>+ Add</div>	<div></div>
<div><div><div>90%</div><div>Weak MFA Was Used To Successfully Sign In </div><div><div>Critical</div>End Users - Identity Posture Insight</div></div></div>	22 → No change since last week → No change since last month	0	<div>+ Add</div>	<div></div>
<div><div><div>91%</div><div>No Strong MFA Configured </div><div><div>Moderate</div>End Users - Compliance, Identity Posture Insight</div></div></div>	21 → No change since last week → No change since last month	0	<div>+ Add</div>	<div></div>
<div><div><div>97%</div><div>Access From Dormant Account </div><div><div>Moderate</div>End Users - Compliance, Identity Threat Insight</div></div></div>	7 → No change since last week → No change since last month	0	<div>+ Add</div>	<div></div>

BRKSEC-2531

Cisco Identity Intelligence in XDR Automate

Merges with Incidents

- The CII source events are correlated with the detections from other security products.
- The CII ITDR detection is now part of the attack graph & investigations

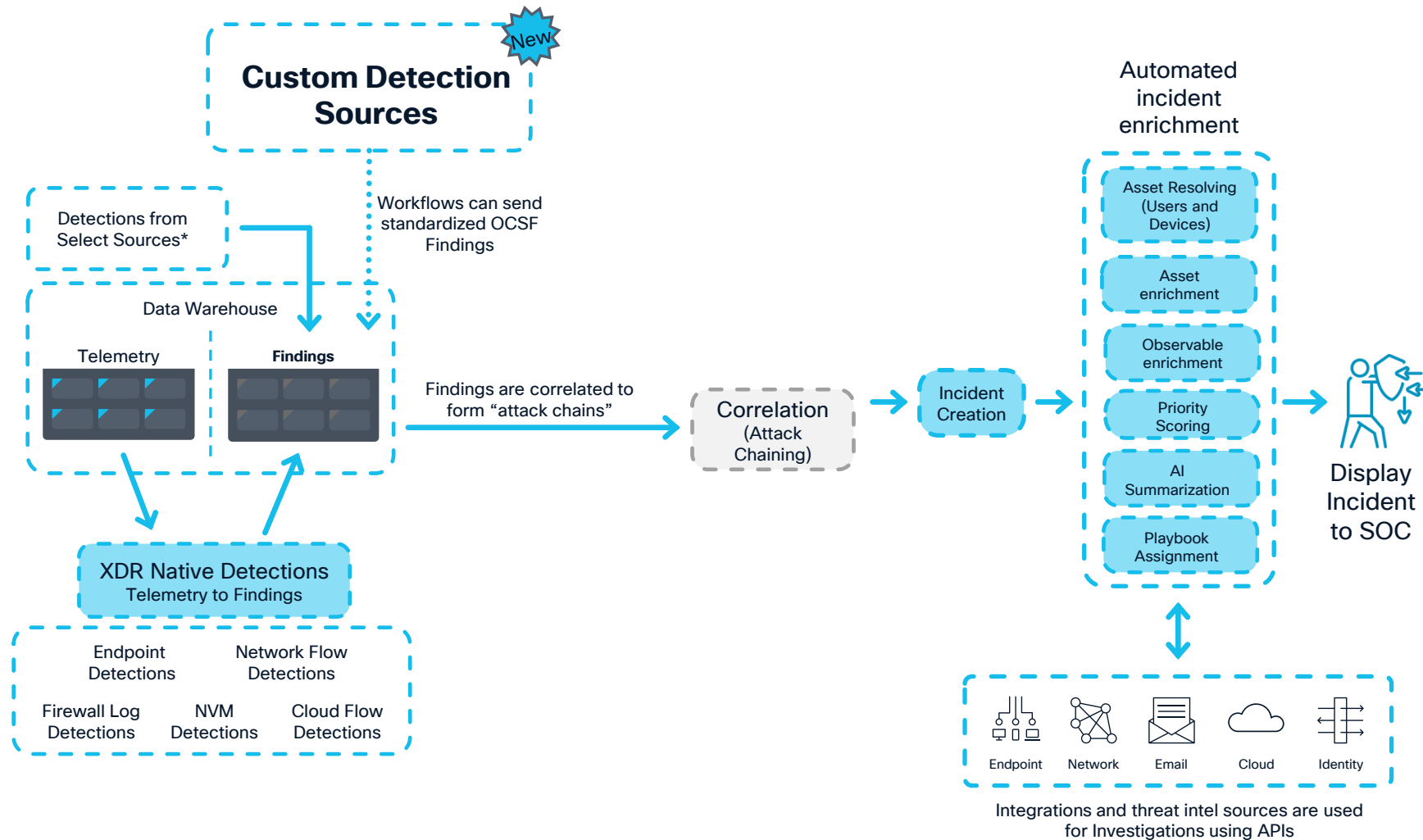


Published in Exchange

- A community-maintained XDR workflow.
- Takes the CII Webhook & parses it.
- Will enrich existing incidents, or if none exist will create a new incident.

Custom Data Ingestion

Incident Generation Pipeline

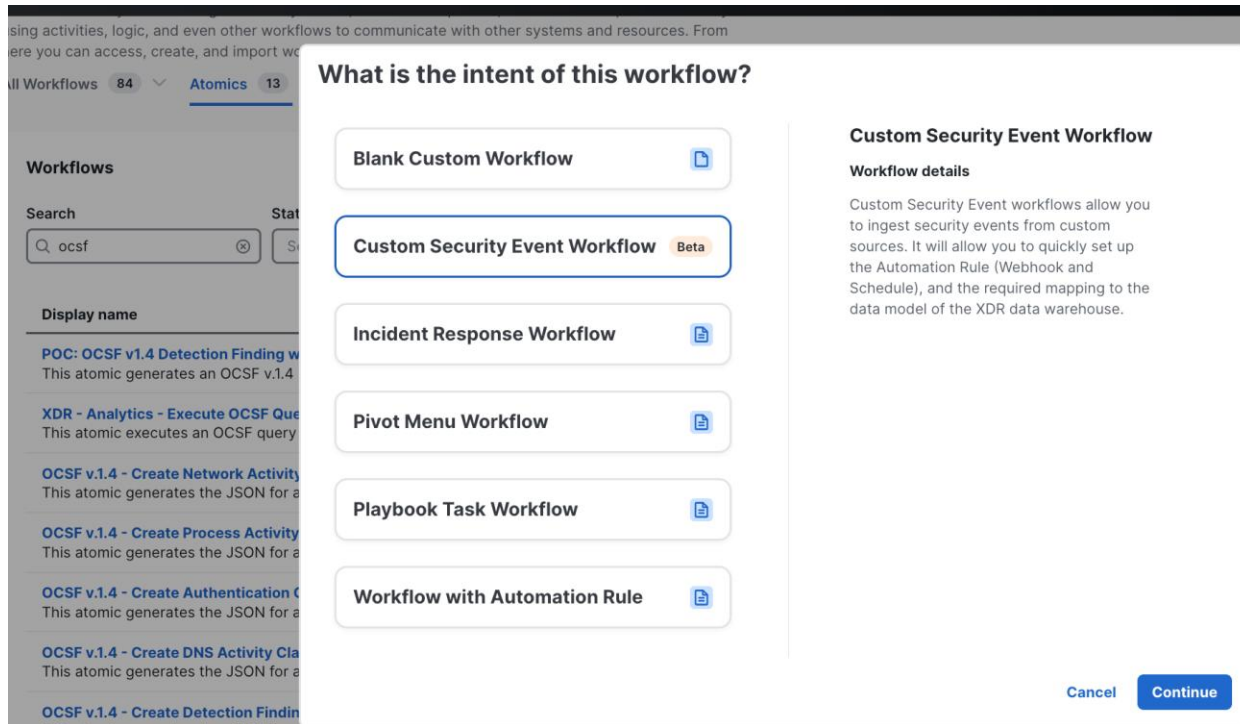


* Cisco Secure Endpoint, CrowdStrike, MS Defender, Cisco ETD, Proofpoint, MS O365, SentinelOne + roadmap

** Coming soon!
CISCO

Custom Security Event Workflow intent

GA September



New Custom Security Event Workflow

Custom Security Event workflows allow you to ingest security events from custom sources. It will allow you to quickly set up the Automation Rule (Webhook and Schedule), and the required mapping to the data model of the XDR data warehouse.

Workflow display name* ⓘ 4 / 64

test

Security event type* ⓘ

Network

Email

Select an HTTP target to use ⓘ

Select

Select or create a schedule automation rule ⓘ

Select

Cancel Continue

- You use this method to directly ingest security events into Analytics platform to be considered in incident generation pipeline
- Available for network and email (MORE event types are coming soon)
- Either needs to be a push (Webhook) or pull (API) method

“Ingest network and email security events” Atomics

All workflows 61 ▾ **Atoms** 3 Recents Favorites 0

Workflows

Search Status Category 3 matching results [Reset all](#)

Display name	Categories
XDR - Analytics - Ingest Network Security Event This atomic ingests network security events from custom sourc...	
XDR - Analytics - Ingest Email Security Event This atomic ingests email security events from custom sources...	
XDR - Analytics - Execute OCSF Query This atomic executes an OCSF query for an observable using on...	

- Simplified OCSF Detection Finding and relevant Activity (Network and Email)
- Focused on outcomes, not on schema specific complexities (e.g. Class IDs)
- Built for standardized and consistent OCSF objects, that can participate in correlation without needing tuning

Unlocked Share Validated View runs Run Settings ▾

Atomic Properties: **XDR - Analytics - Ingest Network Security Event**

XDR - Analytics - Ingest Network Security Event

Detection Raw Data ⓘ
 [X]

Detection Severity ⓘ
 [X]

Detection Source URL ⓘ
 [X]

Detection Status ⓘ
 [X]

Detection Time* ⓘ
 [X]

Detection Title ⓘ
 [X]

Module Instance ID* ⓘ
 [X]

Network Activity Destination Endpoint Hostname ⓘ
 [X]

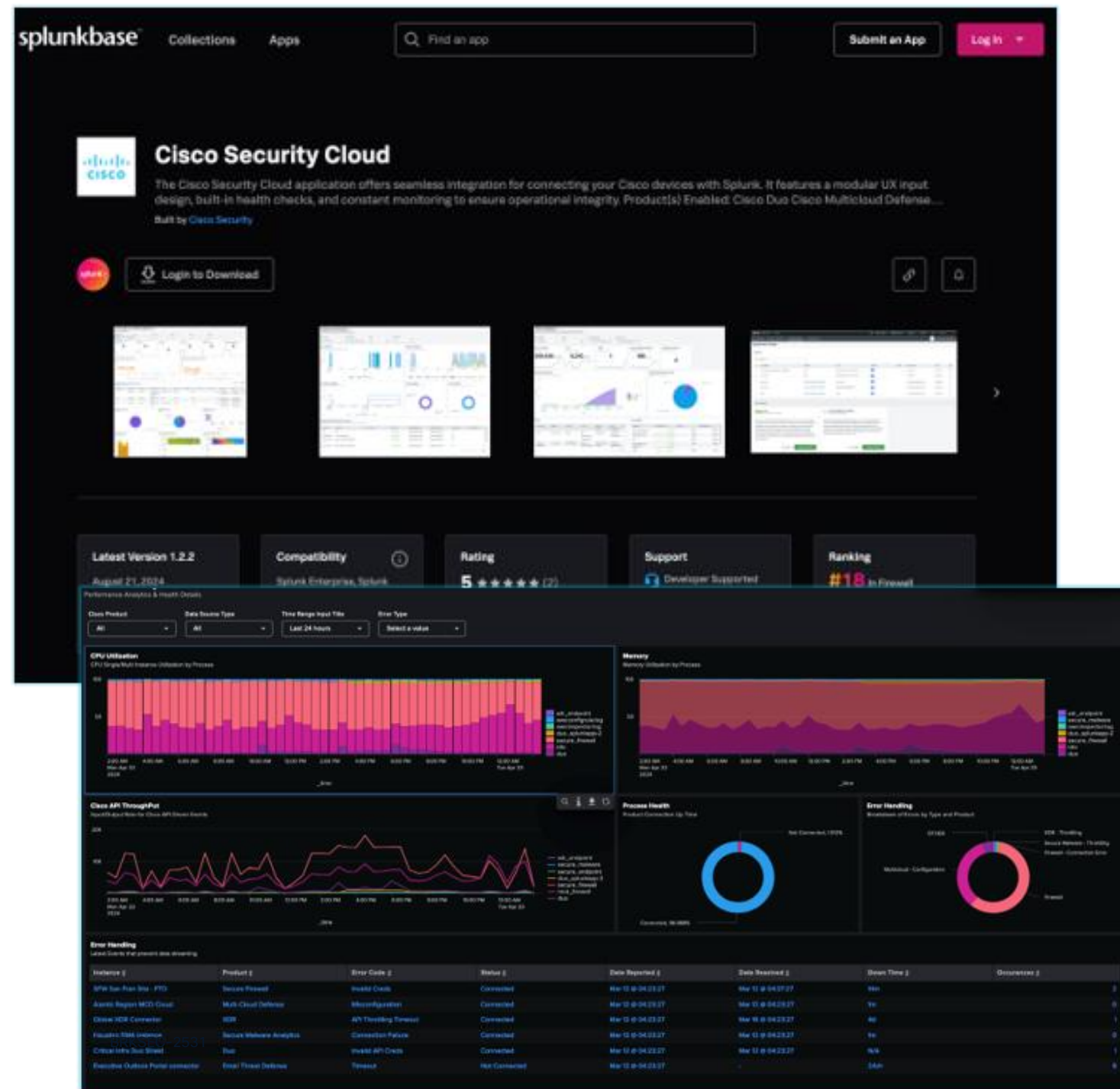
Network Activity Destination Endpoint IP (Proxy) ⓘ
 [X]

Network Activity Destination Endpoint IP Address ⓘ
 [X]

How does this fit into my Larger SOC

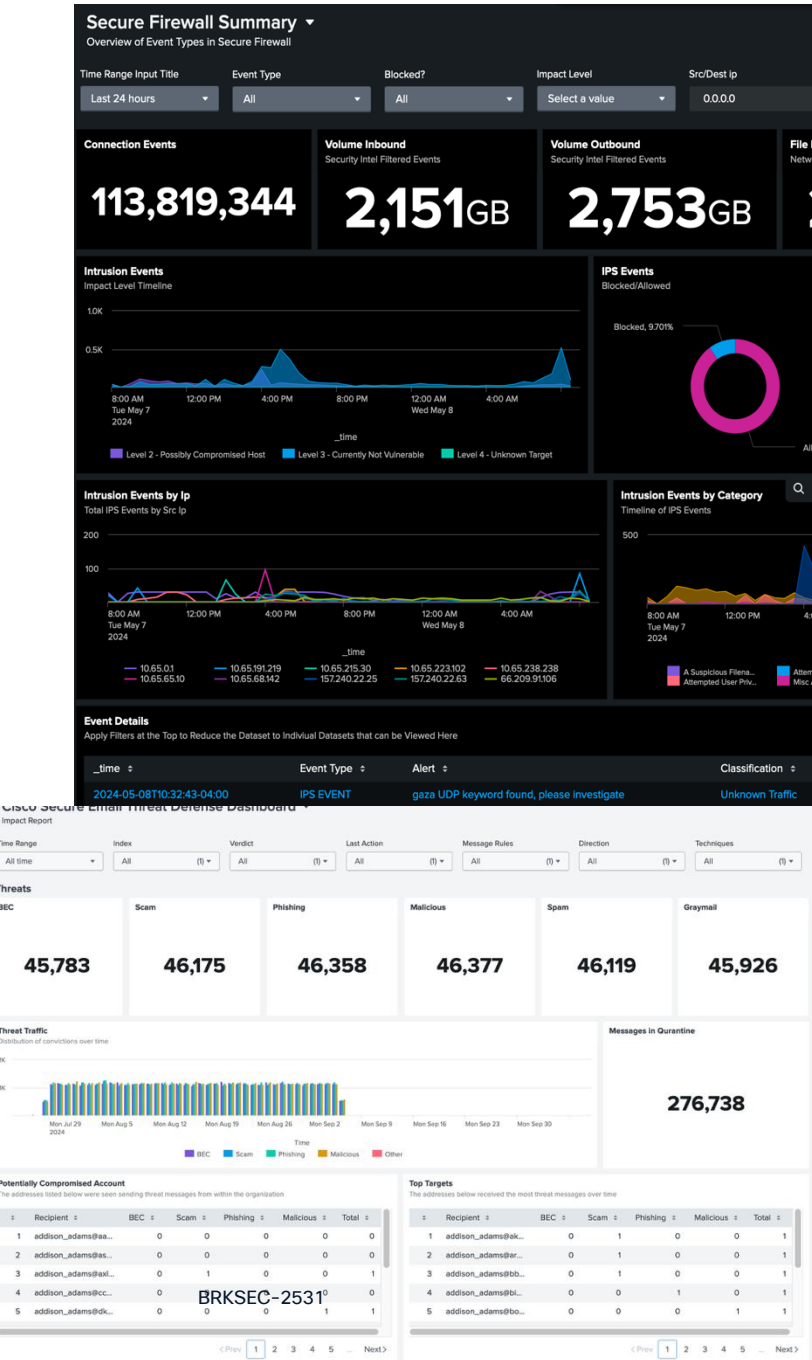
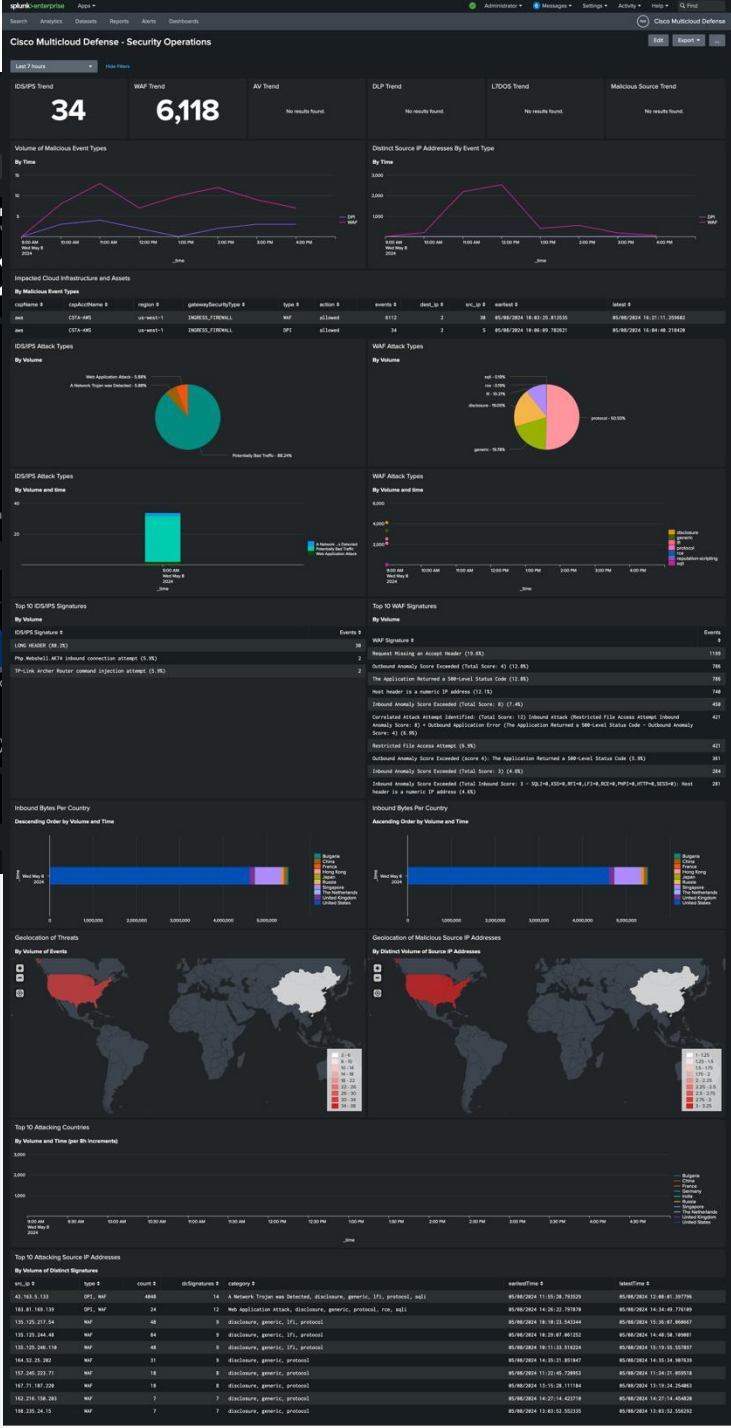
Cisco Security Cloud App

- Single application that packages the capabilities of a TA and App in a single offering based on the gold standard best practice
- The app covers the following Cisco products
 - Secure Network Application
 - XDR
 - Duo
 - Email Threat Defense
 - Multi Cloud Defense
 - Secure Firewall (FTD, Estreamer, ASA)
 - Malware Analytics
 - Secure Endpoint
 - Kenna VI
 - Identity Intelligence
 - AI Defense



Dashboards

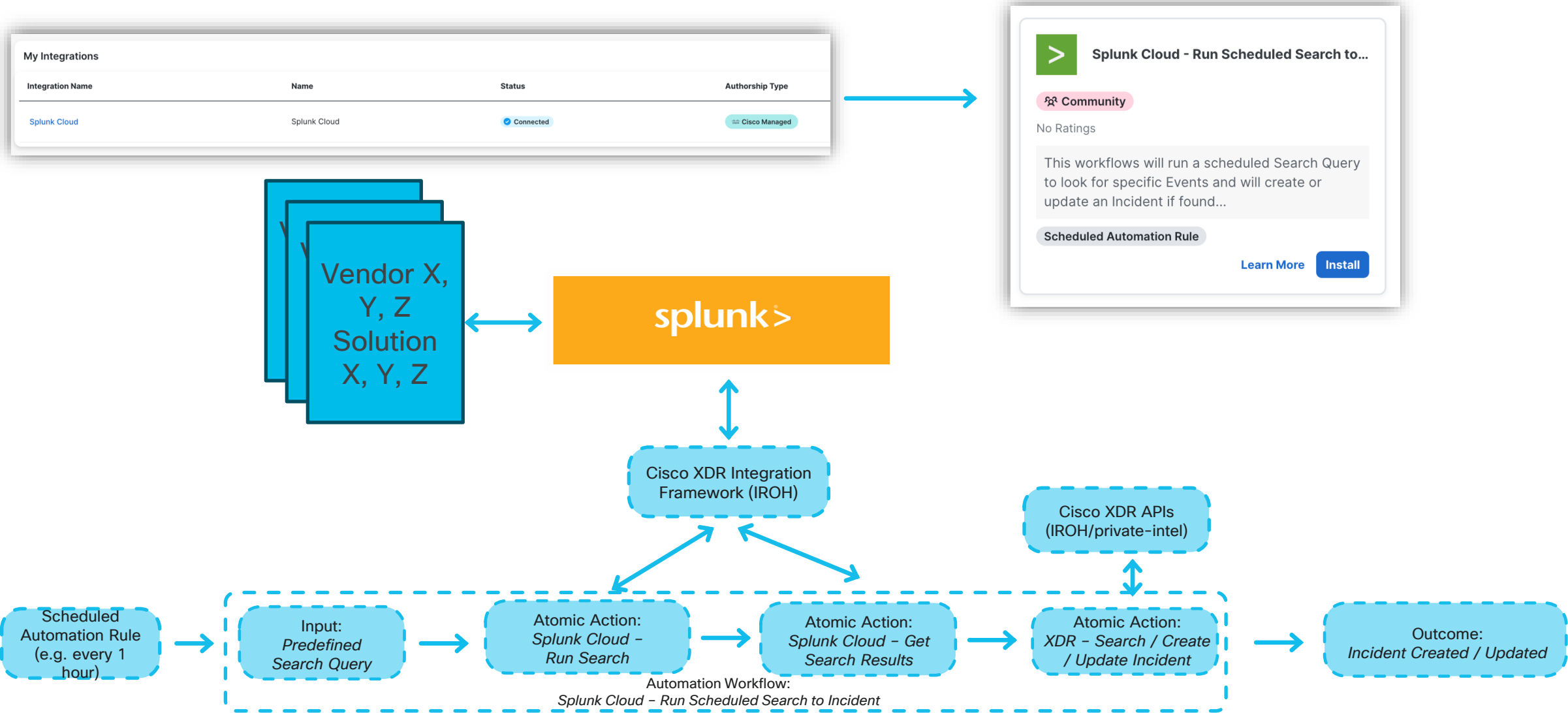
- From High Level View to Detailed Use Cases
- Normalized inputs collected can help facilitate improve query search time
- Pivot back to point products utilizing power of Splunk Search



Demo Cisco Security Cloud

XDR Automation(s) with Splunk

Use Splunk as a Data Source



Example of Customization

- Cisco SMA Malicious submission – XDR incident and notification
- Cisco SMA – Monitor Non-Malicious documents submission
- Palo Alto Networks Firewall – Create Cisco XDR incident – V2
- Splunk – Corelight – Create Cisco XDR incident V2
- Splunk – ThousandEyes – Create XDR create incident V2
- Incident Enrichment – Add Room and Purpose
- Palo Alto Threat Logs to Splunk

Workflows		
Search	Status	Category
<input type="text" value="Q Search"/>	<input type="text" value="Select"/>	<input type="text" value="1 Selected"/>
		15 matching results Reset All
Category Blackhat Automation Add to Saved Filters		
Display name	Categories	Status
Set all my org's Public CSMA Samples to Private queries list of CSMA/TG public samples in the user's org to fetc...	Blackhat Automation	Export completed
Palo Alto Threat Logs to Splunk Collect logs from Palo Alto (PANOS or Panorama) and forward them...	Blackhat Automation	Validated
Invite Non-admin Users to Cisco Stack This workflow invites a user as an non-admin to SecureX, Umbrell...	Blackhat Automation	Export completed
Splunk - Corelight - Create Cisco XDR incident V2 This workflow runs a scheduled search for Suricata and IDS Notic...	Blackhat Automation, Cisco XDR	Validated
Global Incident ID stats - XDR Incident - Clear Event Tabl...	Blackhat Automation	Export completed
Black Hat - Create DB from addressing plan	Blackhat Automation	Export completed
Get Target Info by Name	Blackhat Automation	Export completed
Splunk.- ThousandEyes - Create XDR create incident V2 This workflow runs a scheduled search for ThousandEyes Alert in...	Blackhat Automation	Export completed
Umbrella - Create Cisco XDR incident This workflow runs a scheduled search in Umbrella. if new logs e...	Blackhat Automation	Validated
Palo Alto Networks Firewall - Create Cisco XDR incident - ... This workflow runs a scheduled search in Palo Alto Networks Fire...	Blackhat Automation	Export completed
Cisco SMA Malicious submission - XDR incident and notifica... This workflow runs a scheduled search query in Cisco Secure Malw...	Blackhat Automation	Export completed
Cisco SMA - Monitor Non Malicious documents submission This scheduled workflow executes a search query in Cisco Secure...	Blackhat Automation	Export completed
Black hat - Report Incident - Webex Notification	Blackhat Automation	Export completed
Black hat - XDR New Incident - Webex Notification	Blackhat Automation	Export completed
Incident Enrichment - Add Room and Purpose Enrich the incident with room and location for a target	Blackhat Automation	Export completed

Here in the World of Solution , THE SOC



New Incident Sources (from BlackHat)

☐	540	Network Detection involving Asset 10.220.37.37	Cisco Secure Firewall	2025-04-02T03:01:22.497
☐	380	Network Detection involving Asset 10.220.32.15	Palo Alto Networks Firewall	2025-04-02T02:34:18.677
☐	1000	Possible Phishing Landing involving Asset 10.220.34.40	Corelight NDR	2025-04-02T02:25:42.875
☐	380	Network Detection involving Asset 10.220.38.24	Palo Alto Networks Firewall	2025-04-02T01:25:00.981
☐	1000	Network Detections with Multiple TTPs involving Asset 10.220.37.38	Cisco Secure Firewall	2025-04-02T01:20:56.358
☐	1000	Network Detections with Multiple TTPs involving Asset 10.220.37.40	Corelight NDR	2025-04-02T01:18:06.290
☐	1000	Network Detections with Multiple TTPs involving Asset 192.168.128.182	Corelight NDR	2025-04-02T00:51:38.700
☐	170	DNS or URL Security Hit for Domain claim.titanlab.io	Umbrella	2025-04-02T00:50:37.721
☐	1000	Network Detection involving Asset 10.220.33.22	Corelight NDR	2025-04-02T00:33:20.247
☐	380	Network Detection involving Asset 172.16.6.38	Corelight NDR	2025-04-02T00:32:47.240
☐	380	Network Detection involving Asset 10.220.250.29	Corelight NDR	2025-04-02T00:32:08.086
☐	370	Network Detection involving Asset 10.220.33.12	Cisco Secure Firewall	2025-04-02T00:30:59.427
☐	1000	(P2P BitTorrent) involving Asset 10.220.36.25	Corelight NDR	2025-04-01T10:16:11.586
☐	380	Network Detection involving Asset 10.220.38.18	Palo Alto Networks Firewall	2025-04-01T04:17:54.766

**Great things are not done by
impulse, but by a series of
small things brought together**

Vincent Van Gogh

Today's Key Takeaways:

- **XDR main data sources:** First focus on the main data sources
 - Network Telemetry
 - Endpoint Detection
 - NVM data.
- **XDR Integrations:** Find the right integration to add more context or threat intelligence
- **XDR Automation:** Automate for response and to customize integrations.

Next Steps & Further Engagement:

Reinforce Your Learning: Access the self-paced demos below to solidify today's information.

Action Item: Go to the SOC still Open Tomorrow.

Questions or Discussion? Feel free to connect with me if you'd like to discuss this session further.

Detection Engineering with Cisco XDR: Tooling Native Detections and the Incident Generation Pipeline [BRKSEC-2178]

Schedule

Thursday, Nov 13 | 10:30 AM - 12:00 PM AEDT | Room 220

Home Work– Demo Link

XDR Demo Link

<https://cisco.navattic.com/BRKSEC-2531>

Cisco dCloud

Want hands on what was show in this session? Then ask your Cisco representative to book one of the Cisco dCloud labs mentioned below and get hands on experience of XDR

Cisco Breach Protection Suite – Instant Demo

Published Date: 13-Mar-2025 19:42 Updated Date: 13-Mar-2025 19:42

The Cisco Breach Protection Suite is a set of products designed to provide strong detection, prevention, and response capabilities, while also facilitating better automation and aggregated threat intelligence. Email Threat Defense (ETD) and Secure Endpoint provide an extensive set of capabilities for protecting end users from a wide range of threats; Secure Network Analytics (SNA) provides heuristic anomaly detection for network traffic; and Cisco XDR aggregates data across Cisco and 3rd party security tools to facilitate and automate complex investigations and associated responses.

This demonstration follows [Blind Eagle's cyberattack](#) against our PseudoCo company. Blind Eagle will gain initial access via user execution of a link in a file sent via spearphishing. Once execution is obtained and persistence installed, Blind Eagle downloads and executes the AsyncRAT for additional actions on objective. Characteristics of this campaign include social engineering, open-source modified RATs, exploitation of a single workstation, and theft of browser credentials.

The main use-case flow of this demo illustrates the typical activities of a Security Analyst and Incident Responder, emphasizing the reduction of manual processes and enhancement of threat visibility and response capabilities.

NOTE: Please expand the **Related Documents** link below to access the video. Click **View** to access the demo environment.

★ Favorite  Copy  Related Documents  Info

View

Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.



Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

Please Fill Out the Survey



Continue your education



Visit the Cisco Stand for related demos



Book your one-on-one Meet the Expert meeting



Attend the interactive education with Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Thank you

CISCO Live !

