

Detection Engineering with Cisco XDR

CISCO Live !

Tooling Native Detections and the Incident Generation Pipeline

Matt Robertson,
Distinguished Engineer

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/#BRKXXX-xxxx>

Agenda

Objective:

Understand Cisco XDR Analytics

- 01 Introduction to Cisco XDR
- 02 Incident Generation Framework
- 03 Native Detections
- 04 Deployment with Meraki
- 05 Summary



It's Thursday!

Generating Incidents with Confidence



About Me

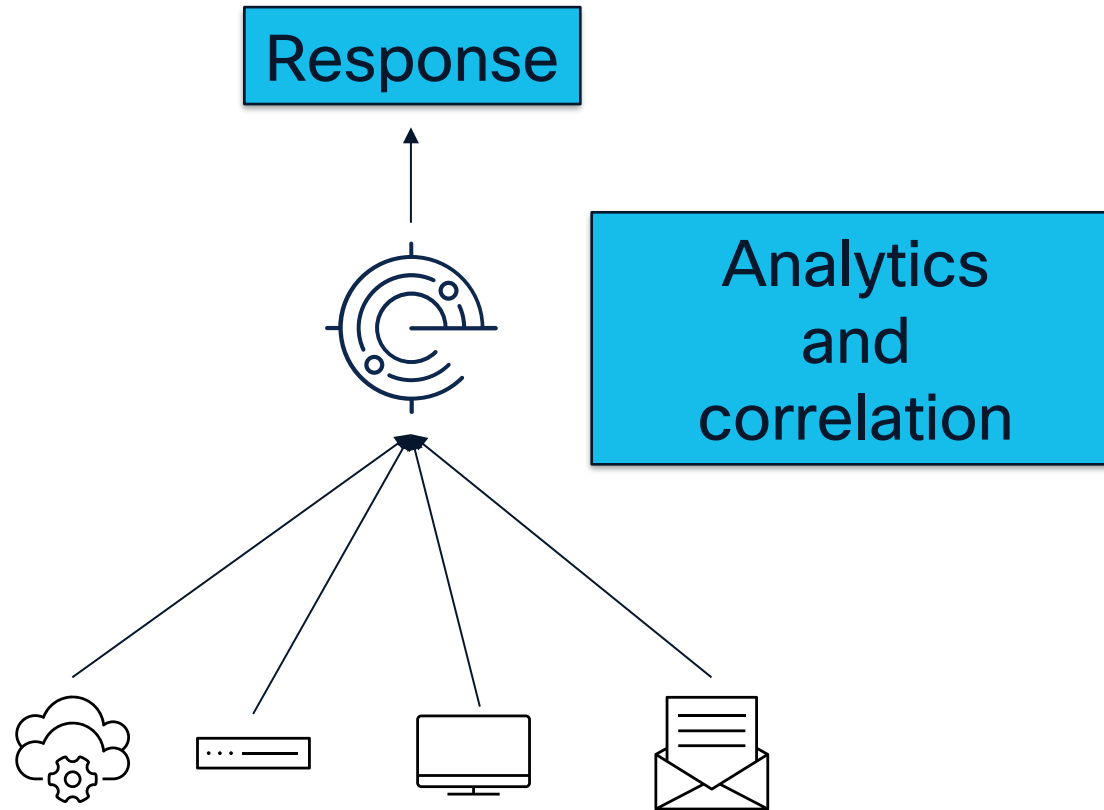


Matt Robertson

- Distinguished Technical Marketing Engineer
- Extended Threat Detection and Security Analytics
- Cisco Live Distinguished Speaker
- 17+ years at Cisco: Development, TME, Lancope
- Canadian eh

What is Cisco XDR?

Cisco XDR

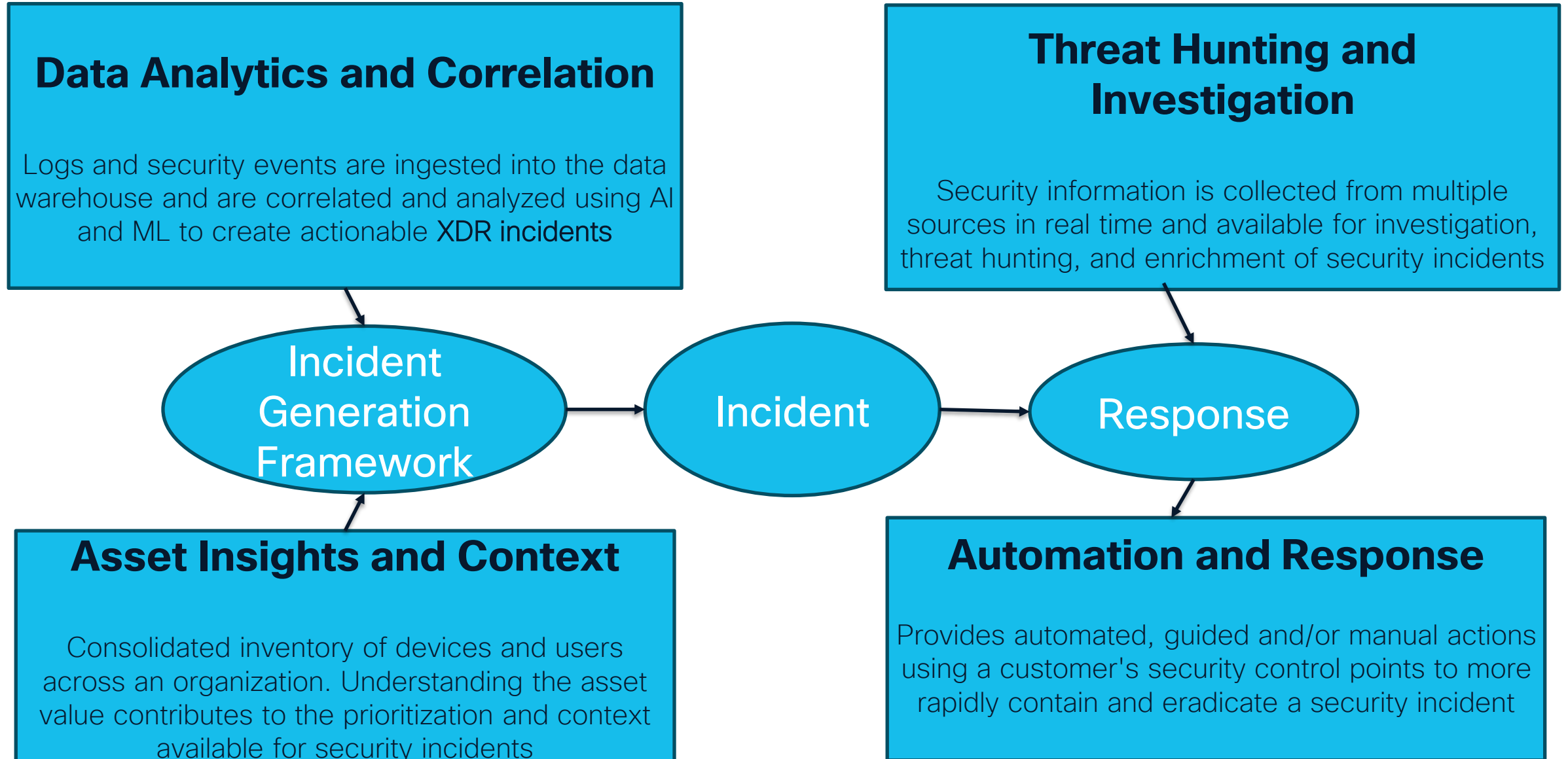


Cisco XDR collects and analyses telemetry from multiple sources to accelerate security operations

1. Collect telemetry from multiple products
2. Application of analytics to that telemetry to arrive at a detection of maliciousness
3. Accelerated/Guided response to that detection

Accelerate that OODA Loop!

Integrations Make XDR Possible



Integrations Make XDR Possible

Data Analytics and Correlation

Logs and security events are ingested into the data warehouse and are correlated and analyzed using AI and ML to create actionable XDR incidents

This Session!

Threat Hunting and Investigation

Security information is collected from multiple sources in real time and available for investigation, threat hunting, and enrichment of security incidents

Incident
Generation
Framework

Incident

Response

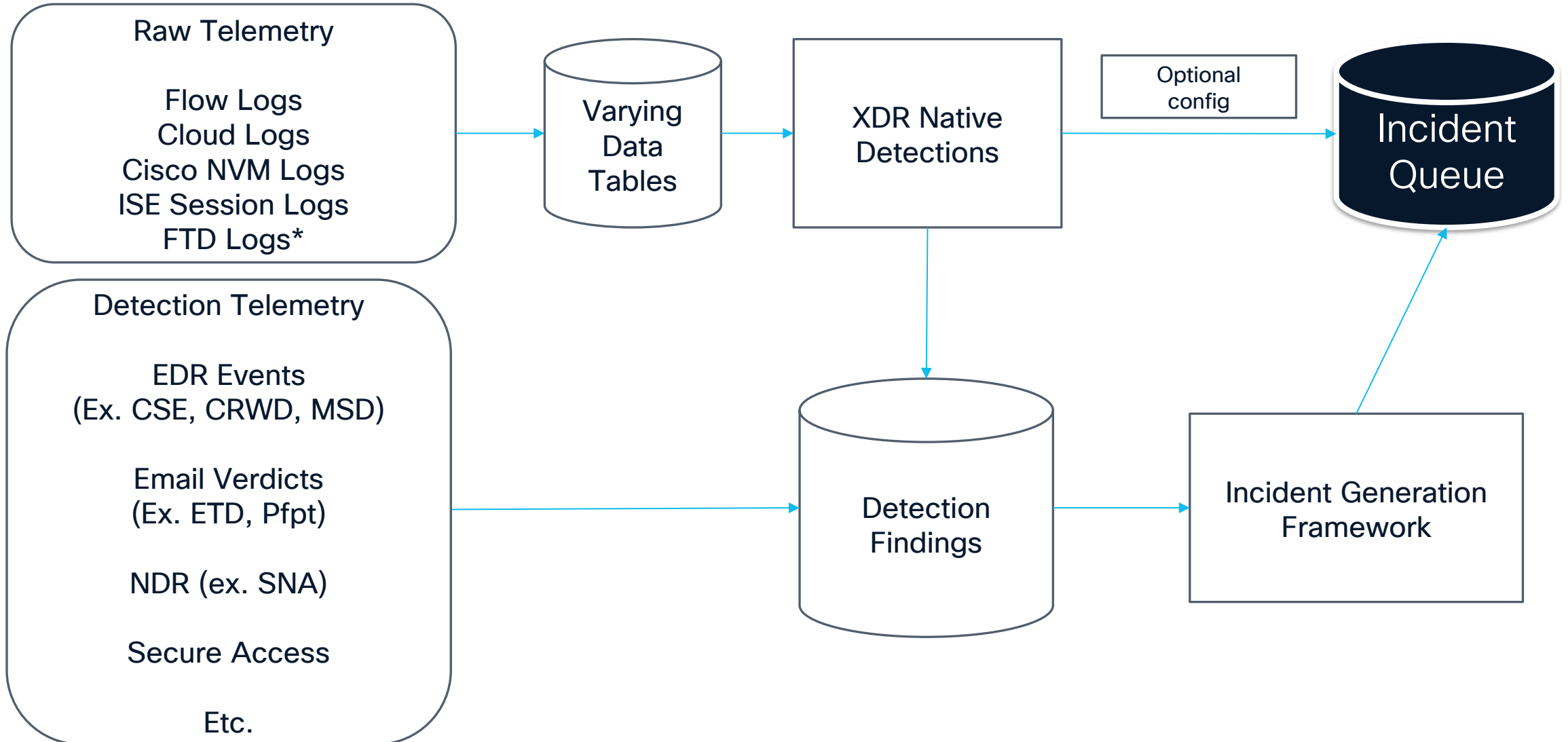
Asset Insights and Context

Consolidated inventory of devices and users across an organization. Understanding the asset value contributes to the prioritization and context available for security incidents

Automation and Response

Provides automated, guided and/or manual actions using a customer's security control points to more rapidly contain and eradicate a security incident

Simplified XDR Data Analytics and Correlation



Incident Generation Framework

What is an XDR Incident?

A data object combining multiple pieces of related security information, allowing you to detect, triage, investigate and respond all in one place

The screenshot displays the Cisco XDR Incidents dashboard. On the left, a sidebar contains navigation icons. The main area is titled 'Incidents' and shows a summary of 35 incidents, with 2 new and 1 open. Below this is a search bar and a table of incidents. The table has columns for Priority, Name, and Sources. The first incident has a priority of 750 and is titled 'Abnormal data upload from endpoint 10[.]1[.]1[.]11'. The second incident, which is highlighted, has a priority of 720 and is titled 'Executed malware and suspicious file downloads on doug-windows11'. The third incident has a priority of 450 and is titled 'Suspect Data Loss on 10[.]160[.]160[.]100'. On the right side of the dashboard, a detailed view of the selected incident is shown. It includes the title 'Executed malware and suspicious file downloads on doug-windows11', a priority of 720, a status of 'Hold: Legal', and a report by 'Cisco XDR Analytics' on '2025-09-26T19:38:03.530Z'. It also shows a 'Priority score breakdown' with a total of 720, composed of 72 Detection Risk and 10 Asset Value at Risk. The sources listed are 'Cisco Secure Endpoint', 'Cisco Secure Network Analytics', and 'XDR Endpoint'.

Priority	Name	Sources
750	Abnormal data upload from endpoint 10[.]1[.]1[.]11	Cisco Secure Network Analytics XDR Endpoint XDR Network
720	Executed malware and suspicious file downloads on doug-windows11	Cisco Secure Endpoint Cisco Secure Network Analytics XDR Endpoint
450	Suspect Data Loss on 10[.]160[.]160[.]100	Cisco Secure Network Analytics XDR Network

Object is visible in the Incident Queue in the XDR UI

Important Note: An XDR Incident is not directly equitable to a detection.

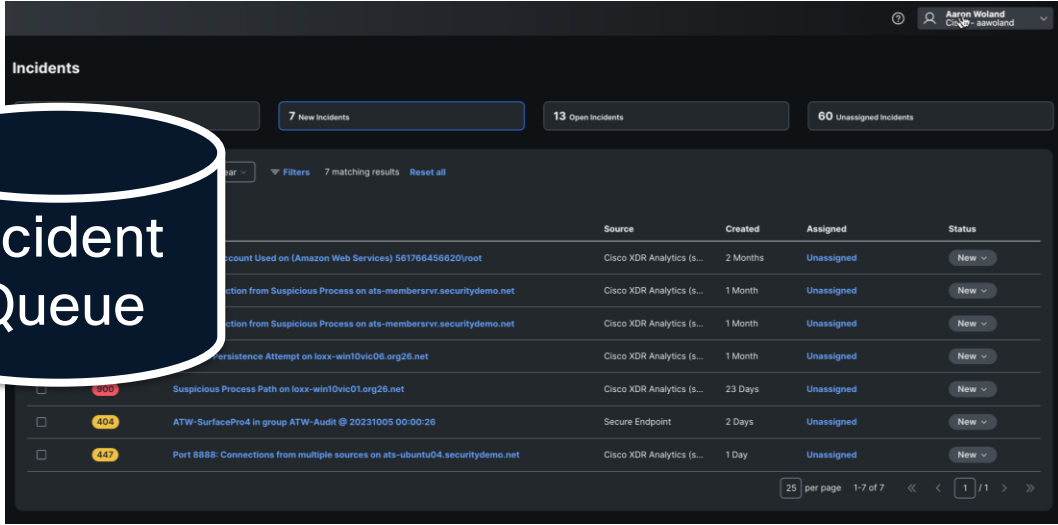
Where do incidents come from?

XDR Incident Generation Framework (IGF)

Workflows and other custom integrations

API

Incident Queue



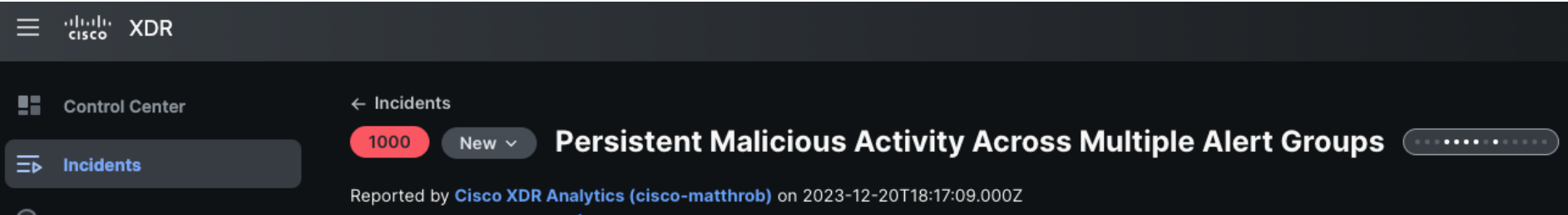
The screenshot shows the 'Incidents' dashboard in Cisco XDR. It features a table with columns: Source, Created, Assigned, and Status. The table lists several incidents, including those from 'Cisco XDR Analytics' and 'Secure Endpoint'. The status of all incidents shown is 'Unassigned'. The dashboard also includes filters and a '7 matching results' indicator.

Source	Created	Assigned	Status
Account Used on (Amazon Web Services) 561766456620/root	2 Months	Unassigned	New
Action from Suspicious Process on ats-membersrvr.securitydemo.net	1 Month	Unassigned	New
Action from Suspicious Process on ats-membersrvr.securitydemo.net	1 Month	Unassigned	New
Persistence Attempt on loxx-win10vic06.org26.net	1 Month	Unassigned	New
Suspicious Process Path on loxx-win10vic01.org26.net	23 Days	Unassigned	New
ATW-SurfacePro4 in group ATW-Audit @ 20231005 00:00:26	2 Days	Unassigned	New
Port 8888: Connections from multiple sources on ats-ubuntu04.securitydemo.net	1 Day	Unassigned	New

Once an Incident is created it is enriched with data from supported integrations

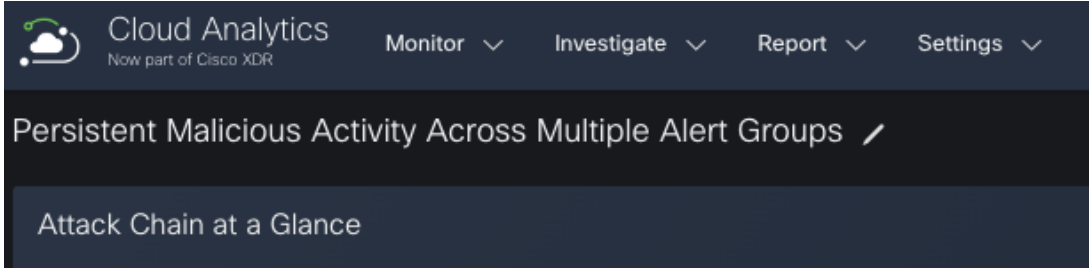
Aside: A note about UI's

Main XDR User Interface



SOC dashboard

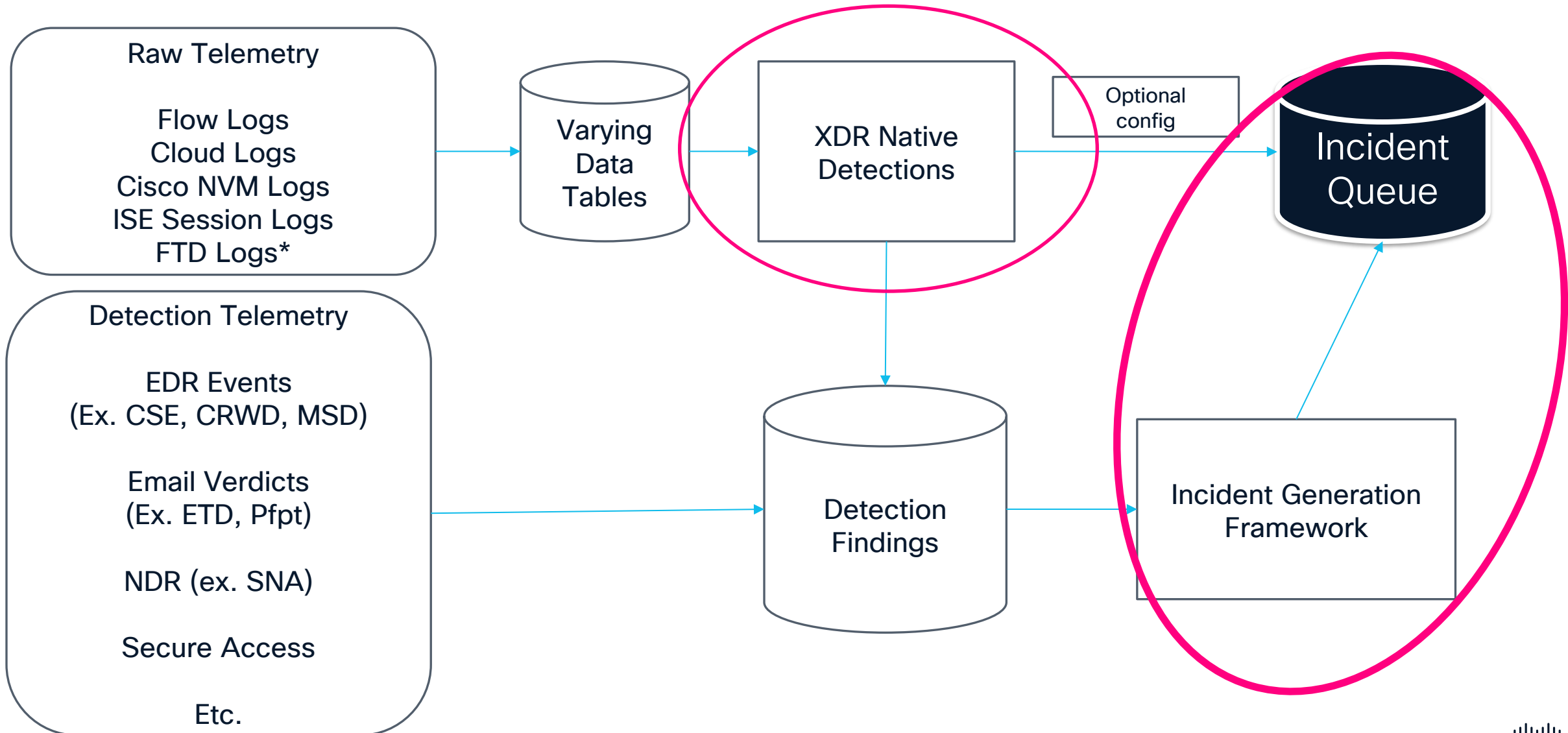
Native Detections



Secure Cloud Analytics, also known as XDR Analytics

"Detection Engineering" dashboard. Admin for analytics stack.

Important Distinction in Terms



Important Distinction in Terms

XDR Native Detection (SCA Alert)

XDR creates alerts (verdicts) from downstream sources that have no native verdicts:
NetFlow, NVM, Cloud logs, ISE, FTD

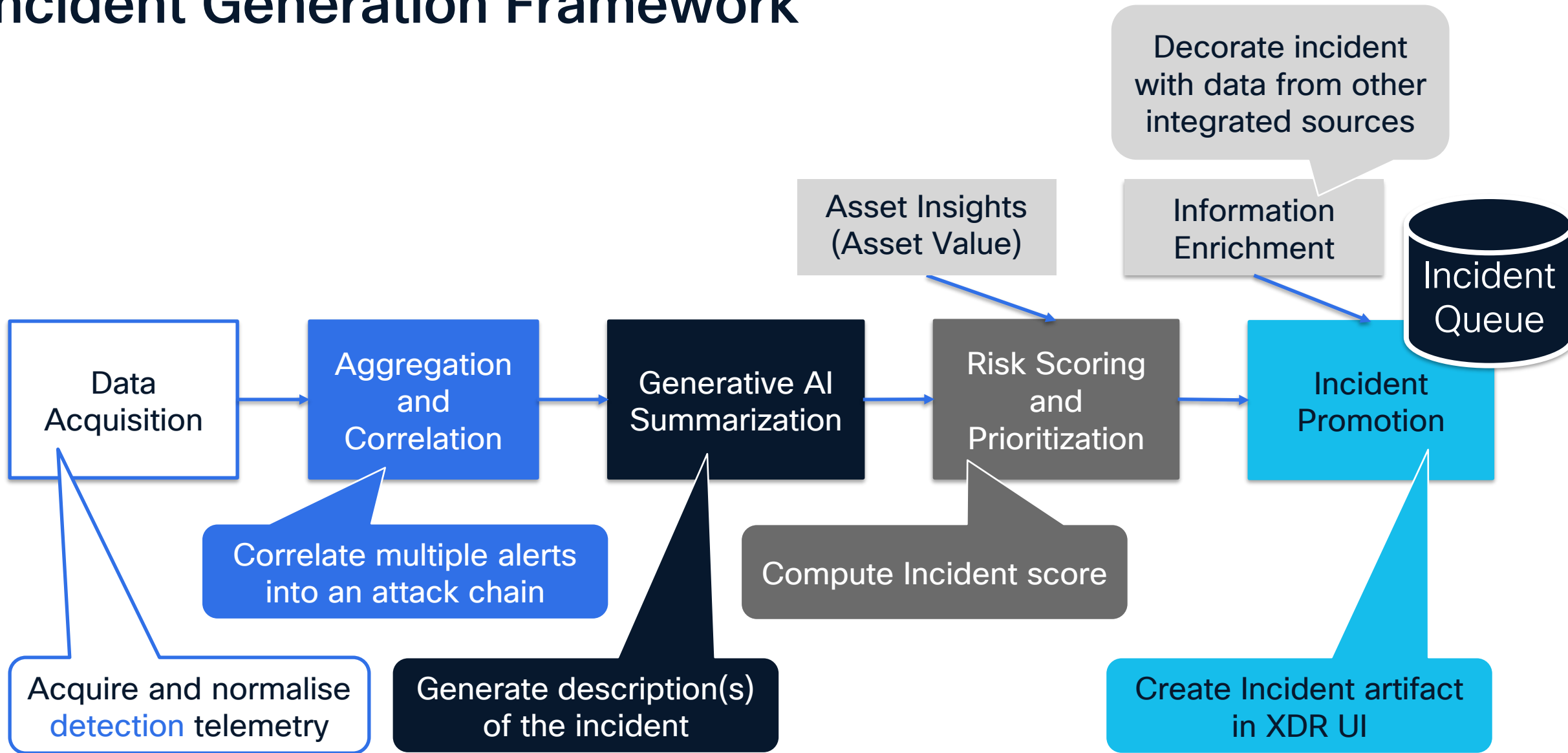
Incident: Extended (Correlated) Detection

XDR collects and extends data sources that have verdicts:
Native detections, EDRs, ETD, SNA, etc

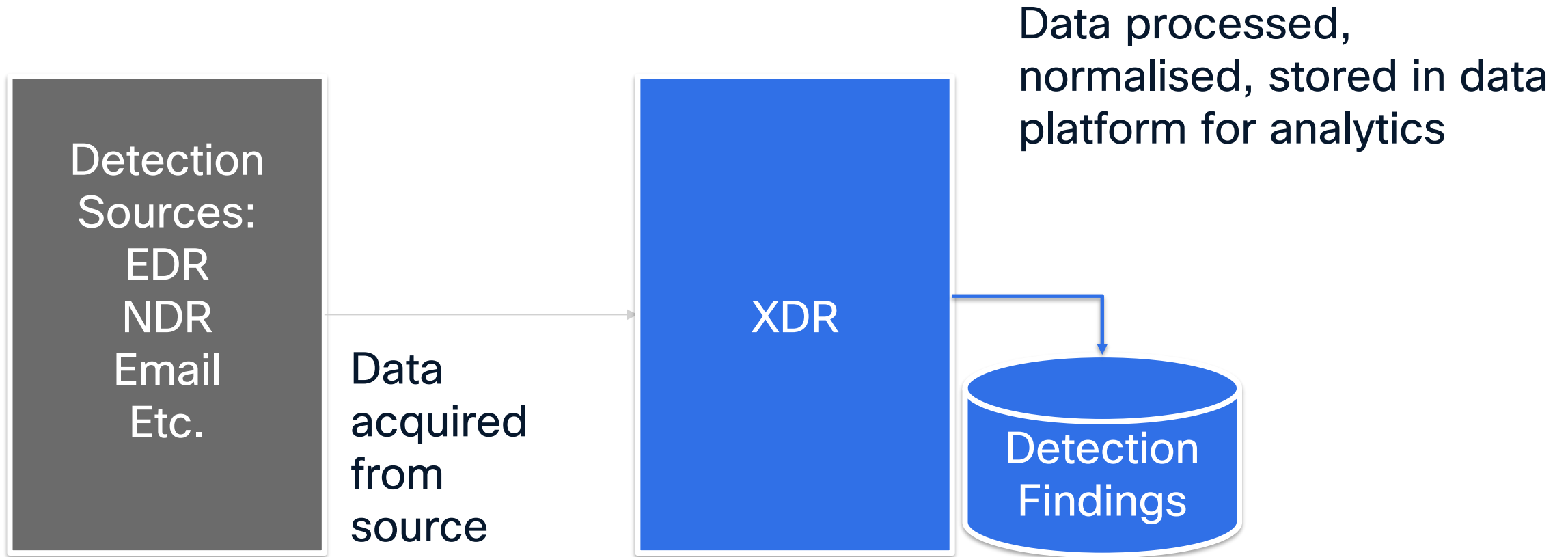
XDR Incident Generation Objective:

Aggregate and Correlate artifacts from integrated telemetry sources to recreate the timeline of a security event

Incident Generation Framework



Data Acquisition and Normalisation



Detection Findings

Detection telemetry ingested into XDR will show in the Detection Findings window

Investigate

Investigation

Detection findings

Detection findings

Q Search

Last 7 days

Source

Severity

8 results

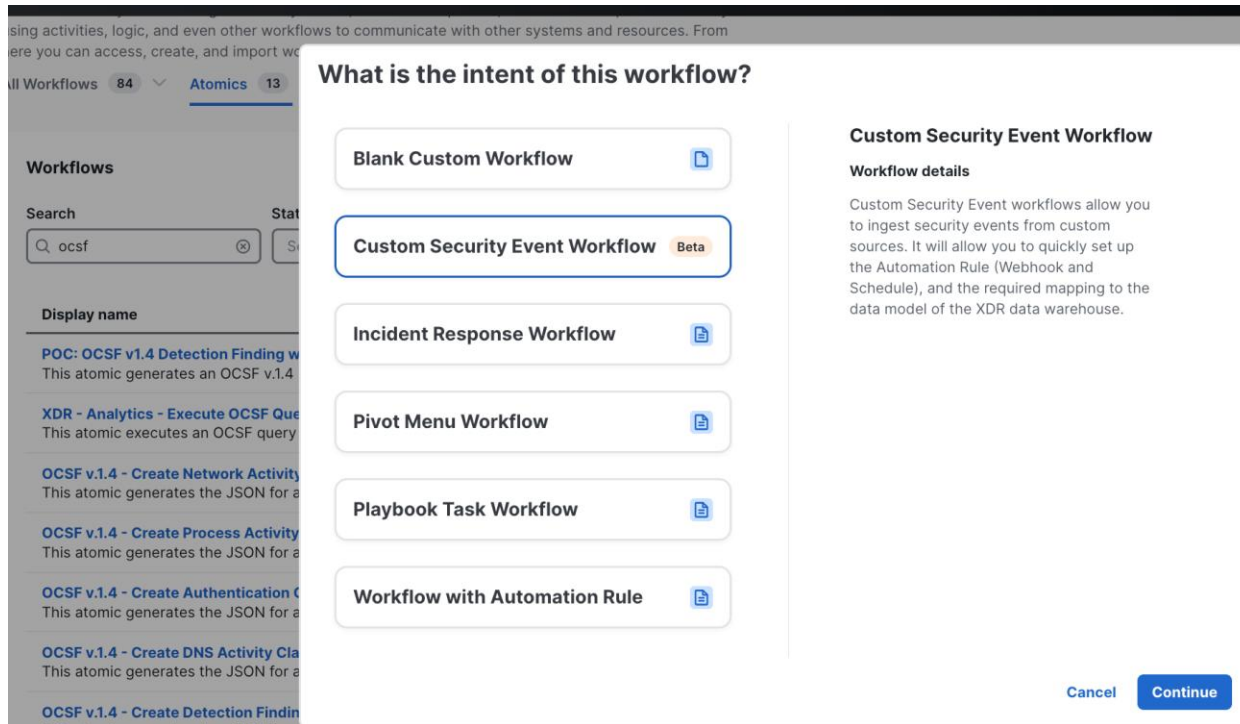
Name	Date created	Last verified	Source	Severity	Finding count	Data status	Related incidents
Suspect Data Hoarding	2025-10-22T19:35:00.000Z	2025-10-22T19:37:00.853Z	Cisco Secure Network Analytics	High	1	Analyzed	Intrusion Detection Spike on ona
Suspect Data Loss	2025-10-21T18:40:00.000Z	2025-10-21T18:41:57.786Z	Cisco Secure Network Analytics	High	1	Analyzed	Intrusion Detection Spike on ona
Suspect Data Hoarding	2025-10-21T18:35:00.000Z	2025-10-21T18:36:57.577Z	Cisco Secure Network Analytics	High	1	Analyzed	Intrusion Detection Spike on ona
System Binary Executed from an Unusual Location - Suspicious Endpoint Activity	2025-10-21T18:30:09.000Z	2025-10-22T20:22:20.074Z	Cisco XDR	High	4	Analyzed	Intrusion Detection Spike on ona
IDS Notice Spike - Intrusion Detection System Notice	2025-10-21T18:29:02.000Z	2025-10-21T19:58:59.813Z	Cisco XDR	High	14	Analyzed	—
Suspect Data Loss	2025-10-20T05:55:00.000Z	2025-10-20T05:56:53.788Z	Cisco Secure Network Analytics	High	1	Analyzed	Intrusion Detection Spike on ona
Suspect Data Loss	2025-10-19T06:05:00.000Z	2025-10-19T06:06:51.213Z	Cisco Secure Network Analytics	High	1	Analyzed	Intrusion Detection Spike on ona
Suspect Data Loss	2025-10-18T06:20:00.000Z	2025-10-18T06:21:48.021Z	Cisco Secure Network Analytics	High	1	Analyzed	Intrusion Detection Spike on ona

Detection title

Source

Related Incident

New: Custom Security Event Workflow



- directly ingest security events into detection findings for correlation in incident generation framework
- Available for network and email today
- Either needs to be a push (Webhook) or pull (API) method

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

Security event type* ⓘ

Email ✓

Network

Select an HTTP target to use ⓘ

Select or create a schedule automation rule ⓘ

[Cancel](#) [Continue](#)

Ingest network and email security events Atomics

All workflows 61 ▾ **Atomics** 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 ⓘ

Detection Severity ⓘ

Detection Source URL ⓘ

Detection Status ⓘ

Detection Time* ⓘ

Detection Title ⓘ

Module Instance ID* ⓘ

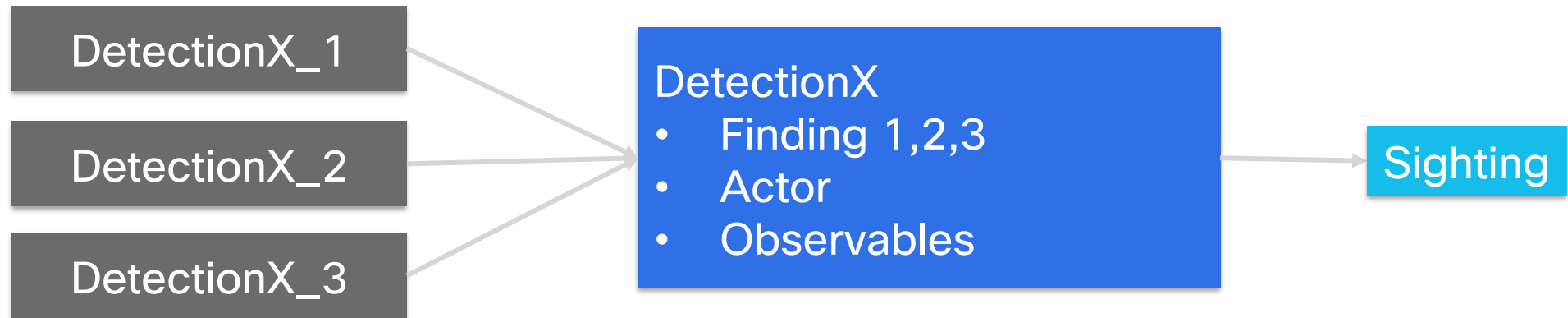
Network Activity Destination Endpoint Hostname ⓘ

Network Activity Destination Endpoint IP (Proxy) ⓘ

Network Activity Destination Endpoint IP Address ⓘ

Aggregation

Reduce duplicative detections to a single finding



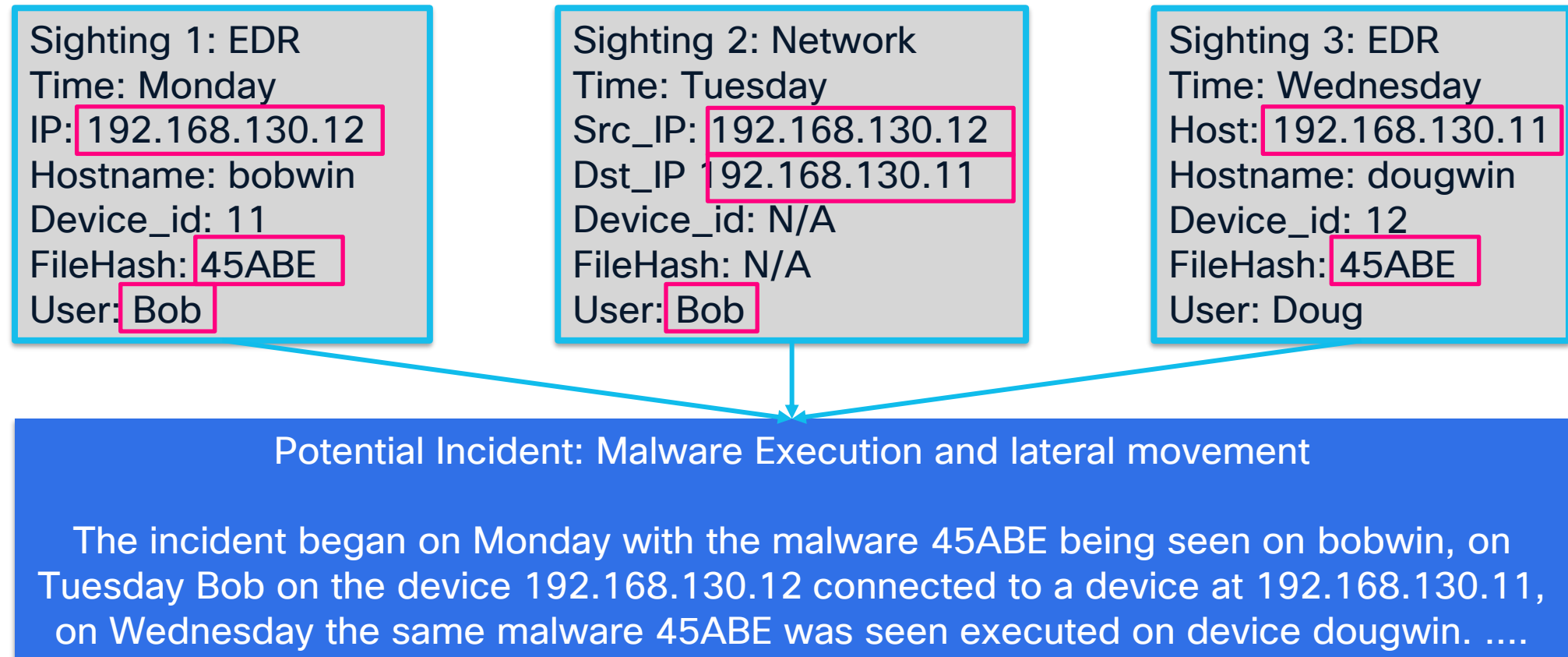
Aggregation = detection_id + detection_type + actor

Aggregation rules:

- Associated to exactly one actor (ex. Device)
- Generate title/description from source
- Maintains lineage: source attributes, severity, groupings, etc.

Correlation

Reconstruct an attack progression by correlating related sightings



Correlation Criteria

Sightings are correlated when they share at least one correlation observable

- Current correlation observables: SCA-ID*, IP Address, Device, Hostname, Username, File/Process Hash, URL

Seven day rolling window correlation timeline: window varies based on detection source-type (ex. Email vs. endpoint vs. native-network)

Couple safeguards:

- Max 10K sightings in an incident
- Max 2K entities per incident

Time-Based Correlation (by Product Category)

Informational as of Nov 2025; Time windows can vary

Pattern A -> B	Email	EDR	NDR	CDR	Identity
Email	Hash - 7 days URL - 7 days User - 7 days	Hash - 7 days URL - 7 days User - 7 days	User - 7 days	User - 7 days	User - 7 days
EDR	Hash - 1 day URL - 2 days User - 1 day	Hash - 7 day URL - 7 days User - 3 day Device - 3 days	Device - 1 day External IP - 1 day	User - 7 day External IP - 7 days Device - 7 days	User - 7 days Device - 7 days
NDR	User - 7 days	Device - 1 day External IP - 1day	Device - 1 day External IP - 1 day	Device - 7 days External IP - 7 days	Device - 7 days
CDR	User - 7 days	Device - 7 days External IP - 7 days User - 7 days	Device - 7 days External IP - 7 days	External IP - 7 days User - 7 days	User - 7 days
Identify	User - 7 days	Device - 7 days User - 7 days	Device - 7 days	User - 7 days	User - 7 days

Promotion Criteria

Promotion: An Incident is created in the User Interface

Priority	Name	Source	Created	Assigned	Status
590	ExecutedMalware.ioc	Cisco XDR Analytics	2 Hours	Unassigned	New

1. Contains at least 2 different sightings of different:
 - Detection Source
 - Detection Type
 - Actor
 - For SNA and ETD sightings must have at least one other detection source
2. Single Sightings are promoted if:
 - Source if EDR and severity if Critical or High
 - No more than 10 single sighting incidents per day

AI Summarization

990

Open

Multiple Suspicious Activities Detected on Internal Devices

.....

Reported by Cisco XDR Analytics on 2024-10-23T18:41:52.761Z

[View detailed description](#)

The incident occurred between Oct 23 2024 and Oct 30 2024. Several suspicious activities were detected including a connection to a TOR IP address and interactions with unusual external servers, both identified by ScaDetections. Additionally, malware activity was detected by CiscoSecureEndpoint. AI-generated [less](#)

Description

This incident began on **October 23, 2024** when **ScaDetections** identified a **Connection to TOR IP Address - Suspicious Endpoint Activity** finding group involving **user hoser** and **device 2daf249e-8bae-4476-b708-e6019c964c93** with 2 findings. Shortly after, the same **device** was involved in three other detection types by **ScaDetections**: an **Internal Connection Watchlist Hit - Internal Connection Watchlist** with 37 findings, and two **Unusual External Server - Watchlist Interaction** finding groups with a total of 103 findings including **Externallp 128.107.78.9** and intervention of another **device f44ba0f0-38b0-45a5-8145-17ead042f3cd**. Additionally, one occurrence of **Unusual External Server - New External Server** was detected on the primary **device** and **Externallp 128.107.78.9**, another instance involved the secondary **device f44ba0f0-38b0-45a5-8145-17ead042f3cd**.

A few days later, on **October 28, 2024**, **CiscoSecureEndpoint** detected a **Mosquito File Artifact** involving the same **device 2daf249e-8bae-4476-b708-e6019c964c93**. Following this, **ScaDetections** identified multiple suspicious activities on the same **device** and user **hoser**: a **Powershell RDP Connection - Suspicious Endpoint Activity** with 2 findings, and two **Unusual External Server - Persistent External Server** finding groups involving both the primary and the secondary internal **devices** and **Externallp 128.107.78.9**.

Later the same day, **CiscoSecureEndpoint** detected an **ExecutedMalware.ioc** on **device 2daf249e-8bae-4476-b708-e6019c964c93**. This was followed by a **Malicious Process Detected - Suspicious Endpoint Activity** by **ScaDetections** on the same **device** with 4 findings.

The last detected activity was on **October 29, 2024**, where **EmailThreatDefense** reported 1 finding of **Mail reported as malware** involving **user hoser**.

AI-generated

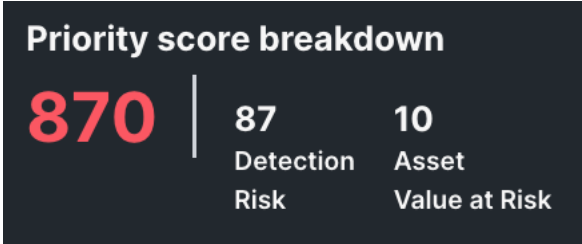
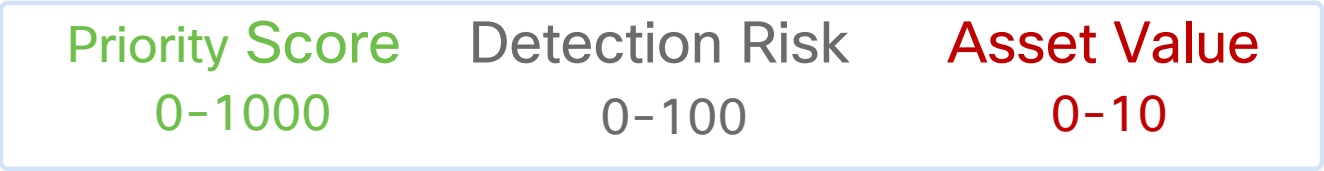
Close

Title and executive summary of incident

Long description

Incident Scoring and Prioritisation

Incidents prioritized by business impact and asset value



Total priority score used to prioritize incidents

Detection Risk computed using data model leveraging multiple value including:

- MITRE TTP Financial Risk
- Number of MITRE TTPs
 - Source Severity

User Defined Asset Value represent the value of the asset involved in the incident

Incidents		
9 Incidents		0 New Incidents
<div><div>Q Search</div><div>×</div><div>9 matching results</div><div>≡ Filters</div></div>		
☐	Priority	Name
☐	1000	Potential Persistence Attempt on victim-win-4
☐	1000	Potential Persistence Attempt on victim-win-0
☐	1000	Attack Chain 4
☐	1000	Executed Malware on victim-win-2
☐	1000	Attack Chain 70
☐	1000	Threat Spotlight: New MortalKombat ransomware and Lapla...
☐	818	IDS Notice Spike on 10.0.26.5
☐	765	Azure Permissive Security Group for TD&R RSA
☐	392	victim-win-6.org1.net in group Audit @ 20230414 02:36:02

Aside: Asset Value Configuration

- Configured on device page
- Default is 10

Note:
Only devices known to
Asset Insights will appear
here

The screenshot displays the Cisco XDR interface for configuring a device. The sidebar on the left contains navigation links: Control Center, Incidents, Investigate, Intelligence, Automate, Devices, Inventory, Sources, Deployment, Audit Logs, Profiles, Device Events, Administration, Integrations, On-Premises Appliances, and API Clients. The main content area is titled 'VICTIM-WIN-4' and shows a dropdown menu for 'Device Value' with options: No Value, 1 (Not Critical), 2, 3 (Less Critical), 4, 5, 6 (Somewhat Critical), and 7. The '10' value is selected. Below the dropdown is an 'Update' button. The device details section includes: Associated Users, Last Active (2023-05-09), Location (NA), Hostname (VICTIM-WIN), Local IPs (10.0.1.23), Public IPs (20.114.75.23), Macs (00:0d:3a:75:00:00), Hardware Id, and Serial Number (0000-0001-9124-5765-2782-5837-93). The 'Seen in Sources' section shows a CrowdStrike entry with 'Last Seen: 2023-05-09T23:50:00.000Z'. The 'Security Products' section shows Firewall (NA), Disk Encryption (NA), and Cisco Secure Endpoint (Not enabled).

Incident Updates

New sightings can correlate into an existing incident

Incidents can merge if new sightings create correlation

IMPORTANT:

The Title and Description are updated as an incident is updated

Closed incidents are not updated.

Incidents are not updated if there has been no update in the last seven days

Incident Merging Criteria

Incident 1	Incident 2	Merge Behaviour
New (oldest)	New	Merge the contents of Incident 2 into Incident 1. Close Incident 2 and link to Incident 1.
Open (oldest)	New	Merge the contents of Incident 2 into Incident 1. Close Incident 2 and link to Incident 1.
Open	New (oldest)	Merge the contents of Incident 1 into Incident 2. Do not close Incident 1 and link to Incident 2.
Open	Open (oldest)	Merge the contents of Incident 1 into Incident 2. Do not close Incident 1 and link to Incident 2.

Note: Incidents created via API (bypassing the IGF) are not merged

Custom Incidents: Bypassing the IGF



Splunk - Search Network Events (generic) - Cisco XDR Incident

Version 1.0 [Release notes](#)



Average rating

Average rating 5 out of 5 (2 ratings)

 Community

This workflow enhances security management by automating the process of identifying and managing network security events using Splunk and Cisco XDR. It performs scheduled searches for new logs, creating or updating XDR Incidents based on event severity and target status. By default, it focuses on Critical and High Severity Events to minimize noise and improve scalability. Users can customize the workflow by mapping specific Splunk event fields such as Source IP, Destination IP, and MITRE Tactics, ensuring accurate threat detection and response. Additionally, it allows for automation scheduling, such as a 10-minute interval, facilitating continuous monitoring and timely incident response. This integration streamlines security operations, reduces manual workload, and enhances the organization's ability to respond to threats efficiently.

[Read less](#)

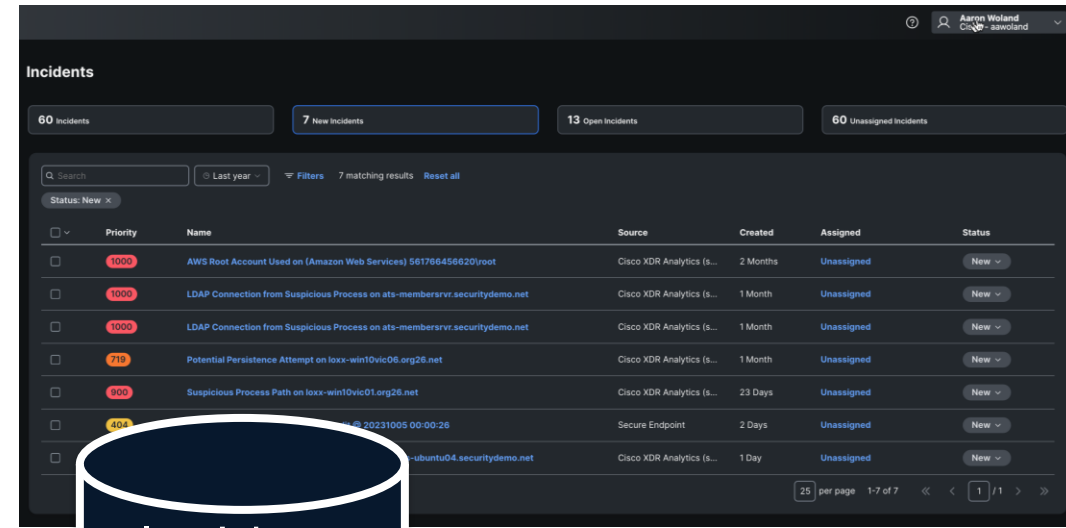
Incidents can be directly created using the API

Several workflows available in the exchange.

Ex. Splunk query

Incident Generation Summary

- Have multiple detection sources:
 - Favourites: Native detections, Secure Access, Endpoint
- Consider custom integrations



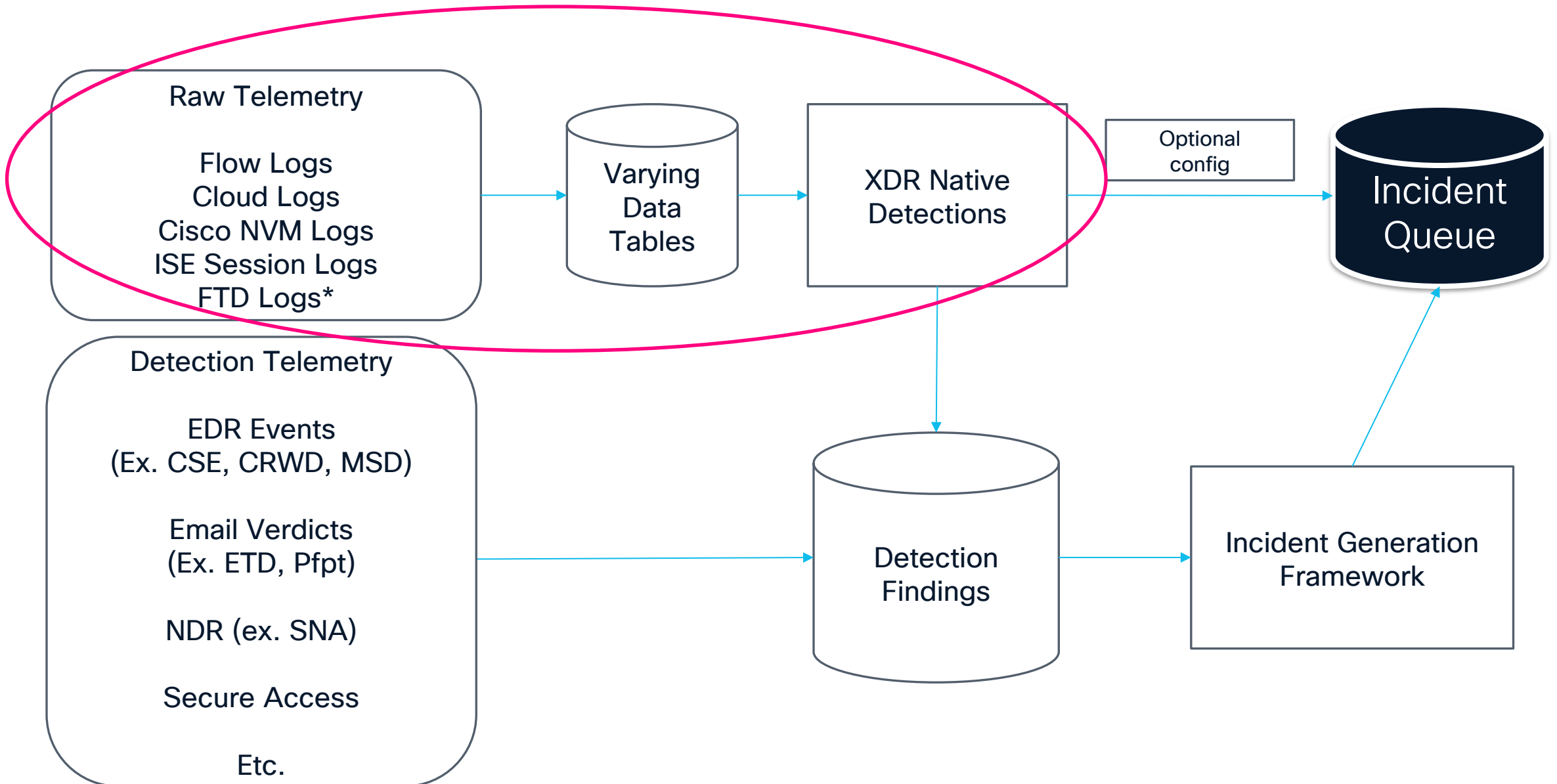
The screenshot shows the 'Incidents' dashboard with a table of incident records. The table has columns for Priority, Name, Source, Created, Assigned, and Status. The incidents listed include AWS Root Account Used, LDAP Connection from Suspicious Process, and Potential Persistence Attempt. A blue callout bubble labeled 'Incident Queue' is overlaid on the table.

Priority	Name	Source	Created	Assigned	Status
1000	AWS Root Account Used on (Amazon Web Services) 561766456620/root	Cisco XDR Analytics (s...	2 Months	Unassigned	New
1000	LDAP Connection from Suspicious Process on ats-membersrvr.securitydemo.net	Cisco XDR Analytics (s...	1 Month	Unassigned	New
1000	LDAP Connection from Suspicious Process on ats-membersrvr.securitydemo.net	Cisco XDR Analytics (s...	1 Month	Unassigned	New
719	Potential Persistence Attempt on loxx-win10vic06.org26.net	Cisco XDR Analytics (s...	1 Month	Unassigned	New
900	Suspicious Process Path on loxx-win10vic01.org26.net	Cisco XDR Analytics (s...	23 Days	Unassigned	New
404	20231005 00:00:26	Secure Endpoint	2 Days	Unassigned	New
	ubuntu04.securitydemo.net	Cisco XDR Analytics (s...	1 Day	Unassigned	New

More Data => More (and better) Incidents

Native Detections

Simplified XDR Data Analytics and Correlation



Native Detections: Creating Security Value from Data

Data Sources:

- Network Flow Logs
- Firewall Logs
- Cloud Logs
- Network Visibility Module (NVM) logs
- Identity Services Engine



Alert:

Notification of potential malicious or suspicious activity

Observation:
Facts observed about an
entity's behaviour

$P(A|B)$: Some behavioural alerts are dictated by a probability model: the probability that the (set of) observations is an alert given what is known of the entity and the environment. Often identified by language such as “abnormally large” and require history.

Entity Modelling

https://<account>.obsrvbl.com/#/device/summary/?id=36260



Identify “Entities” and track state over time:

- Ex. IP address, Endpoint (CSC), Lambda function., etc.

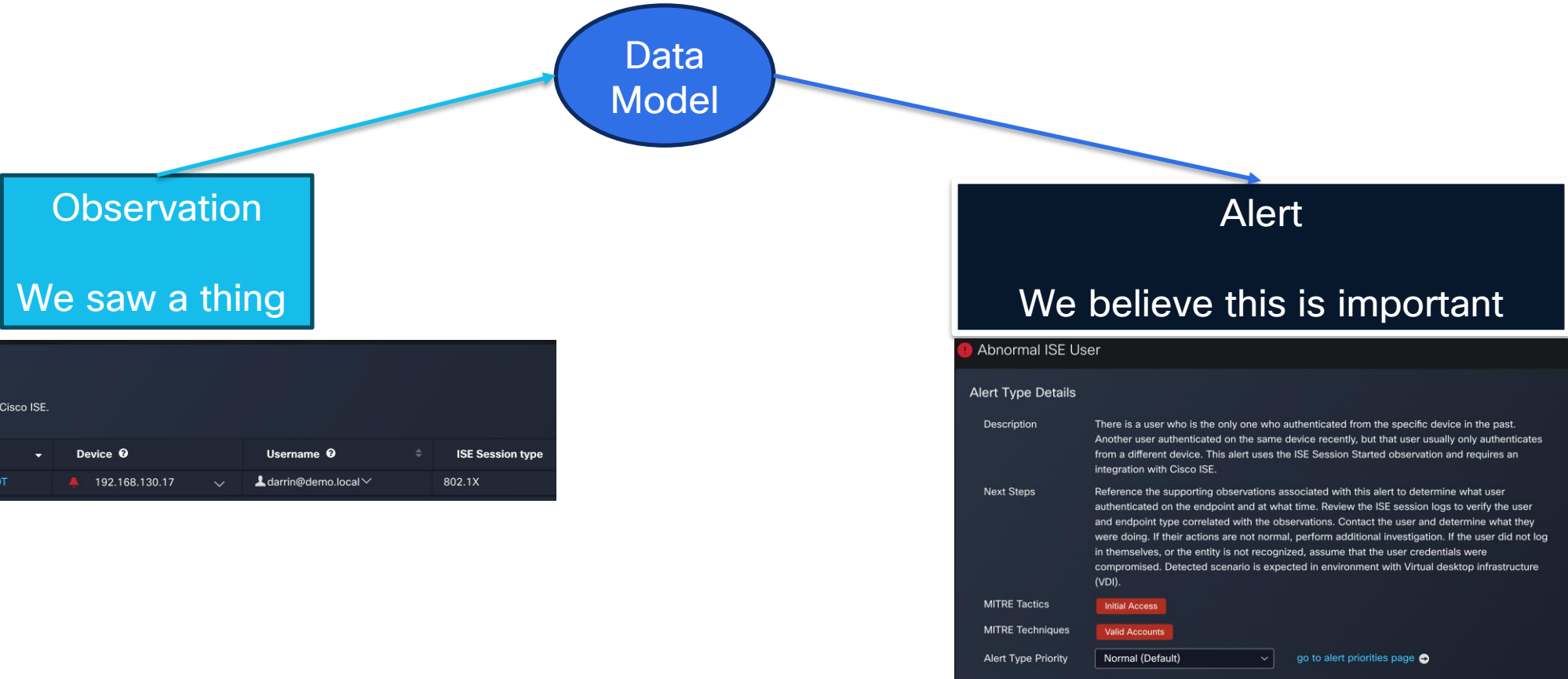
Identified by an SCA-ID

Has state: Roles, Observations

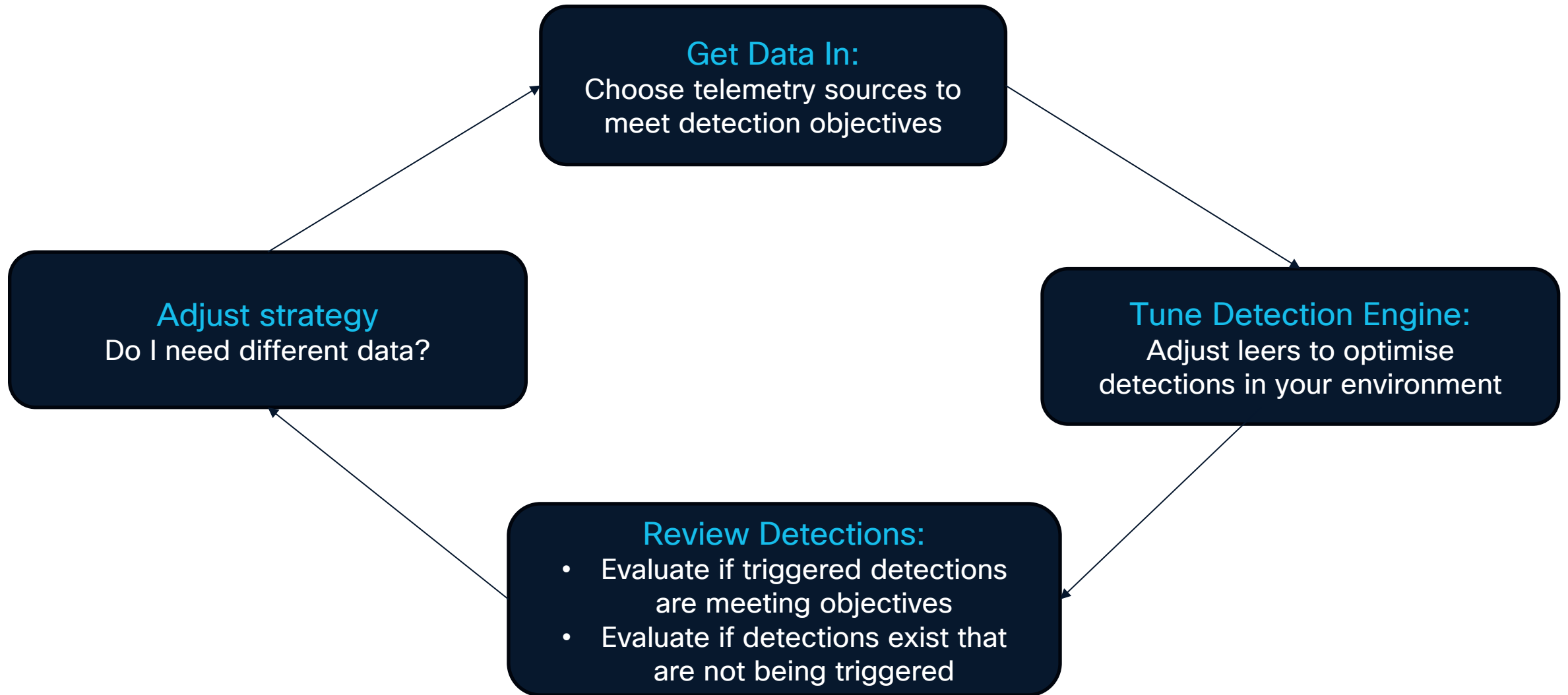
Based on a combination of roles, observations and other threat intelligence SCA will generate an Alert

Observations and Alerts

https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/cloud/reference/Alerts_and_Observations_DV_4_13.pdf



Getting value out of the Native Detection System



Get Data In:

Data powers observations, which power alerts

XDR Network

- NetFlow/IPFIX
- Cisco ETA telemetry
- Firewall*
- Passive DNS via ONA

XDR Endpoint

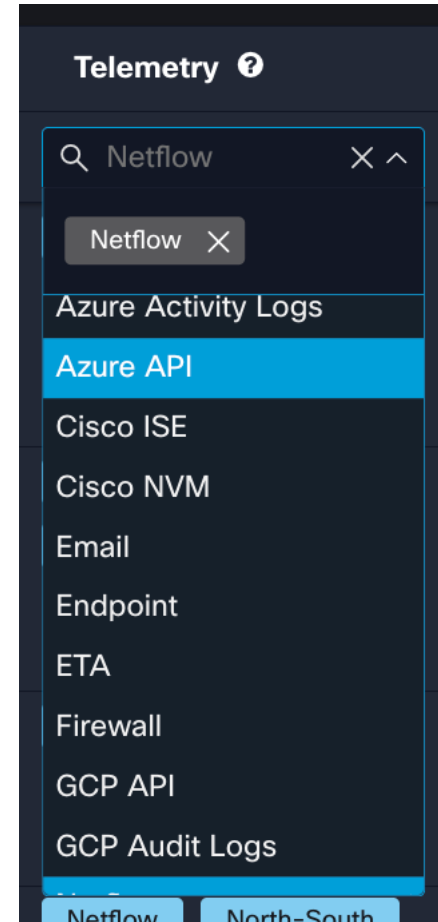
- **Cisco Secure Client Network Visibility Module**

XDR Cloud

- AWS logs
- GCP logs
- Azure logs

XDR Identity

- **Cisco Identity Services Engine**
 - **via Observable Network Appliance (ONA)**



*Firewall logs are considered telemetry for native XDR Network detections:

- Connection events are converted to flow log equivalent and power “NetFlow” observations/alerts
- Intrusion, file and malware events power Firewall-only

Tuning Native Alerts

Best practice: Define subnets and their sensitivity

- Three levers to tune/adjust native alerts:
- 1. Define Subnets and sensitivity
 - 2. Enable/Disable Alerts
 - 3. Alert priority

Subnet Name	Sensitivity	Static	New Device Alerts
<input type="text" value="10.70.70.0/24"/>			
10.70.70.0/24 (PCI Servers)	High	☒	☐

20 Per Page

Low
Normal
High

1-1 of 1 results

Review [Alert FAQs](#) for more general information about alerts. Review the [Subnet Sensitivity Matrix](#) to understand how subnet sensitivity and alert priorities affect the alerting behavior.

Alert Type	Observation Types	Cisco XDR ...	Enabled	Priority
<input type="text" value="powershell rdp"/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>
<div>> Powershell RDP Connection</div> <div>The system utility Powershell was seen making connections over the RDP port, which is indicative of RDP connections.</div>	<div>Suspicious Endpoint Activity</div>	☐	☒ Default: Enabled	Normal

Low
Normal
High

Enable/Disable and Priority

Native Alerts can become incidents

Bypassing the Incident Generation Framework, while simultaneously going through the IGF.

Alerts/Watchlists

Review [Alert FAQs](#) for more general information about alerts. Review the [Subnet Sensitivity Matrix](#) to understand how subnet sensitivity and alert priorities are configured.

Alert Type	Observation Types	History	Priority	Cisco XDR ...	Enabled
Abnormal ISE User There is a user who is the only one who authenticated from the specific device in the past. Another user authenticated on the same device recently, but that user usually only authenticates from a different device.	• ISE Session Started	36 Days	Normal Default Priority: Normal	☐	☐ Default: Disabled
Abnormal User A user session was created on an endpoint that does not normally see sessions with this user.	• Session Opened	36 Days	Normal Default Priority: Normal	☒	☒ Default: Enabled

Publish the incident to Cisco XDR automatically when an alert of this type occurs. You can enable publishing to Cisco XDR if alert type publishing is enabled.

Alerts can be configured to be published directly to XDR as an incident.

Use discretion:
Can result in many
(redundant) incidents

Splunk HEC
Webhooks/Services

Overview

Services and webhooks allow us to send notification messages when alerts are published. This service sends events to a Splunk HTTP Event Collector for monitoring.



Webex Teams
Webhooks/Services

Overview

Services and webhooks allow us to send notification messages when alerts are published. Note that this service requires you to add our bot (stealthy@sparkbot.io) to the space in which you wish to receive notifications.

Alerts and/or notifications
can be published to other
systems on occurrence.

Review Detections

Detection findings							
Q Search		Last 7 days	Source	Severity	30 results		
Name	Date created	Last verified	Source	Severity	Finding count	Data status	Related incidents
User Watchlist Hit - Watchlist Interaction	2025-10-29T14:30:00.000Z	2025-10-29T16:32:44.778Z	Cisco XDR	Critical	4	Analyzed	—
User Watchlist Hit - Watchlist Interaction	2025-10-28T21:00:00.000Z	2025-10-28T21:50:15.041Z	Cisco XDR	Critical	1	Analyzed	—
Domain internetbadguys.com in categories Phishing, Computer Security	2025-10-28T18:57:05.000Z	2025-10-28T18:59:27.104Z	Cisco Secure Access	Unknown	1	Analyzed	Suspicious File Download Observed on IP 192.168.1130.124
Domain internetbadguys.com in categories Phishing, Computer Security	2025-10-28T18:57:05.000Z	2025-10-28T18:59:27.104Z	Cisco Secure Access	Unknown	1	Analyzed	Suspicious File Download Observed on IP 192.168.1130.124

Evaluate if triggered detections are meeting objectives:
Too noisy? Not noisy enough?
Alerts are being correlated into incidents?

Alerts are being correlated into incidents?

Close Alert

Was this alert helpful?

Yes

No

Snooze this alert(s)?

Alert(s):

Type	Scope	Value
User Watchlist Hit	Source	192.168.170.2

Don't show the alert matching the above criteria for a period of:

Don't snooze

Cancel

Submit

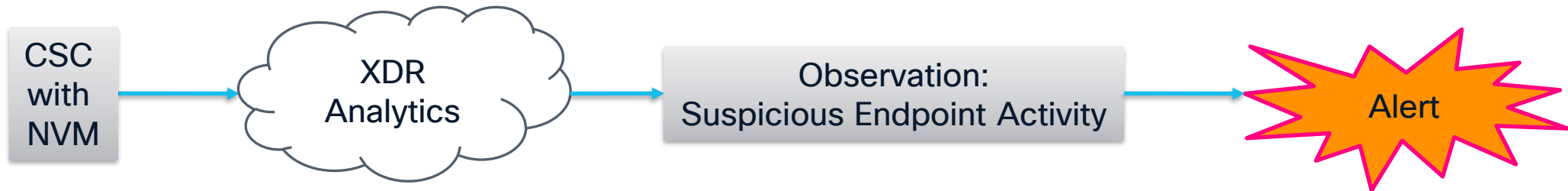
Evaluate if detections exist that are
not being triggered:
Review possible alerts

Digging into some alert types

XDR Network:
(Behavioural detections
from Flow Logs)

XDR
Endpoint:
(NVM)

XDR Endpoint Detections: What they are?



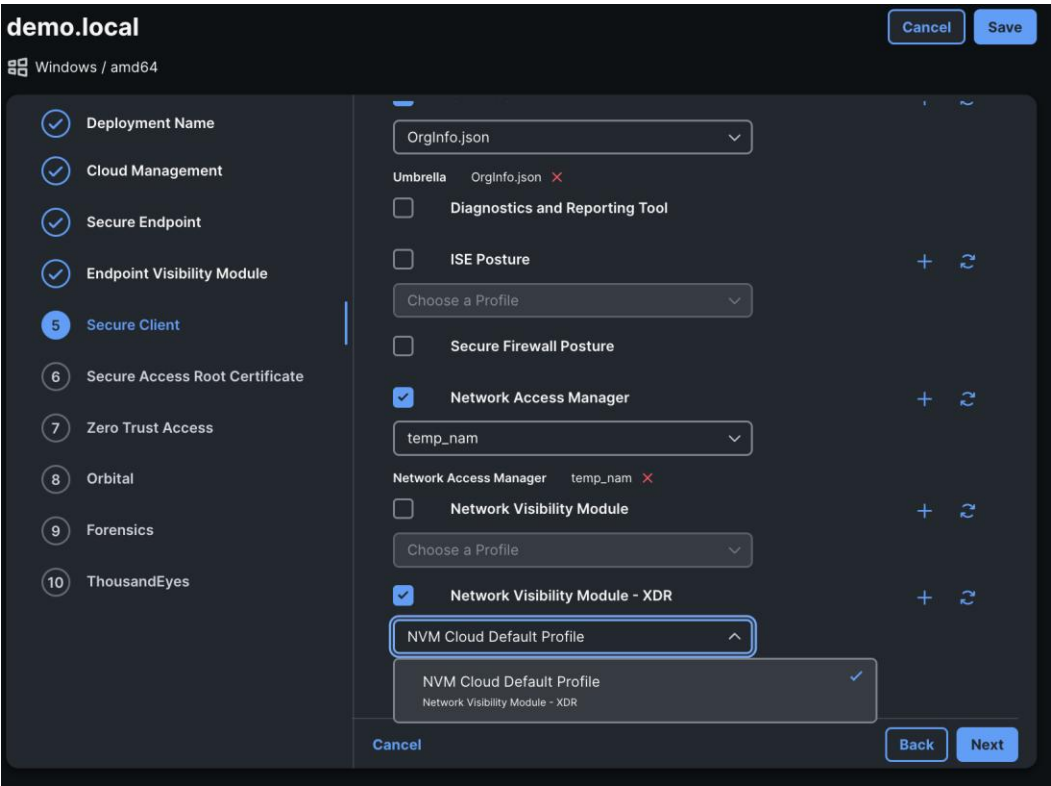
Alert Type	Telemetry	MITRE ATT&CK Ta...	MITRE ATT&CK Te...	Enabled
<div>Alert Type</div>	<div>€ Cisco NVM</div>	<div></div>	<div></div>	<div></div>
<div>> ADEplorer Domain Discovery</div> <div>ADEplorer, a Sysinternals executable, was used to gather information on domain trusts relationships. This information can be leveraged by adversaries to identify lateral movement opportunities.</div>	<div>Cisco NVM</div>	<div>Discovery</div>	<div>Domain Trust Discov...</div>	<div><div></div>Default: Disabled</div>
<div>> Base64 Encoding Detected</div> <div>Base64 strings were detected as part of the PowerShell command line. Detection is based on a combination of regular expressions and encoded commands. Attackers often use Base64 encoding as an obfuscation technique to hide malicious activity executed via PowerShell. However, it may also indicate legitimate administrative activity.</div>	<div>Cisco NVM</div>	<div>Defense Evasion</div>		
<div>> Certify Active Directory CS Enumeration</div> <div>The Certify.exe C# tool was used to enumerate AD Certificate Services or abuse a vulnerable certificate template using default low-privileged groups. Adversaries can use this tool to confirm discovery of vulnerable certificate templates and use them as an alternative means of authentication for unauthorized system access and further lateral network movement.</div>	<div>Cisco NVM</div>	<div>Discovery</div> <div>Credential Access</div>		
<div>> Cloud Metadata Service Credential Access</div> <div>A request to one of the public cloud Instance Metadata Service endpoints was made for credentials. This is common adversary behavior.</div>	<div>Cisco NVM</div>	<div>Credential Access</div>	<div>Cloud Instance Meta...</div>	<div><div></div>Default: Disabled</div>
<div>> Cloud Spreadsheet API C2 Channel</div>	<div>Cisco NVM</div>	<div>Exfiltration</div>	<div>Exfiltration Over C2 ...</div>	<div><div></div></div>

Unique visibility of endpoint details and network connections.

Really useful for detecting living off the land binaries.

XDR Endpoint Detections: Configuration

Deploy CSC with NVM to Windows/Mac endpoints:
Must use CSC Cloud Management (available in XDR)



Enable/Disable NVM Alerts

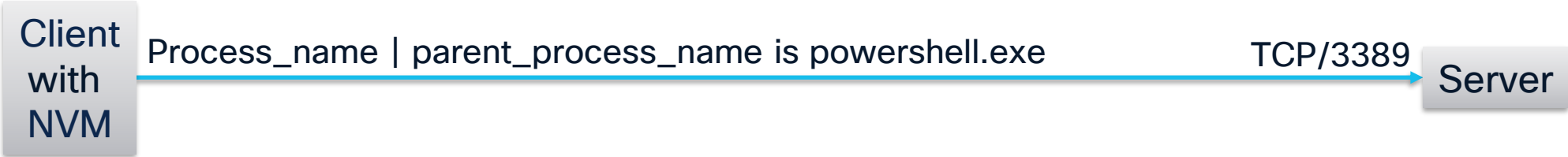
Alert Type	Observation Types	History	Priority	Enabled	Telemetry	Cisco XDR
ADExplorer Domain Discovery	Suspicious Endpoint Activity	0 Days	Normal	☒	Cisco NVM	☐
Base64 Encoding Detected	Suspicious Endpoint Activity	0 Days	Normal	☒	Cisco NVM	☐
Certify Active Directory CS Enumeration	Suspicious Endpoint Activity	0 Days	Normal	☒	Cisco NVM	☐

Note:

Many NVM alerts are disabled by default.
Some are recommended to stay that way as they can be noisy in certain environments
(ex. Suspicious Process Path)

Example NVM Alert: Powershell RDP Connection

Alert Type	Telemetry	MITRE ATT&CK Ta...	MITRE ATT&CK Te...	Enabled	Observation Types
= powershell RDP	€ Cisco NVM	▼	▼	▼	▼
<div>PowerShell RDP Connection</div> <div>The system utility Powershell was seen making connections over the RDP port, which is indicative of RDP connections.</div>	Cisco NVM	Lateral Movement	Remote Desktop Pro...	<div><div></div></div> <div>Default: Enabled</div>	<div>Suspicious Endpoint Activity</div>
<div>Next Steps: Investigate the supporting evidence and determine if this behavior was authorized. If not, broaden the scope of investigation to establish the scope of the incident.</div>					



! Powershell RDP Connection

Alert Type Details

Description

The system utility Powershell was seen making connections over the RDP port, which is indicative of RDP connections.

Next Steps

Investigate the supporting evidence and determine if this behavior was authorized. If not, broaden the scope of investigation to establish the scope of the incident.

MITRE Tactics

Lateral Movement

MITRE Techniques

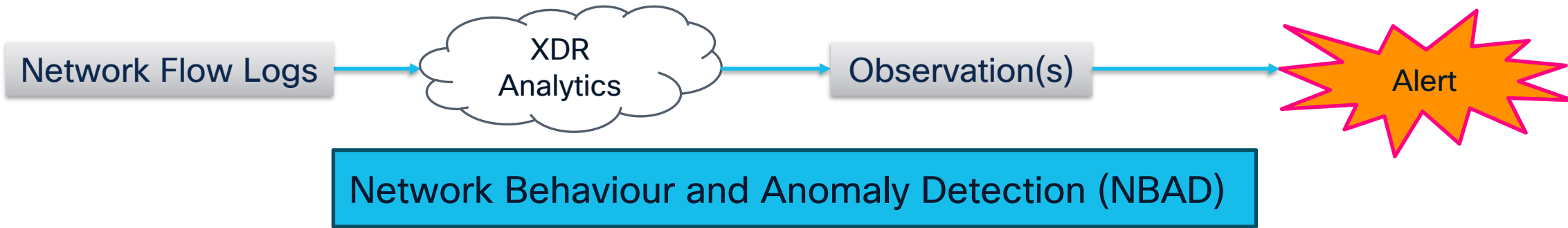
Remote Desktop Protocol

Alert Type Priority

Normal (Default)

[go to alert priorities page](#)

XDR Network: What are they?



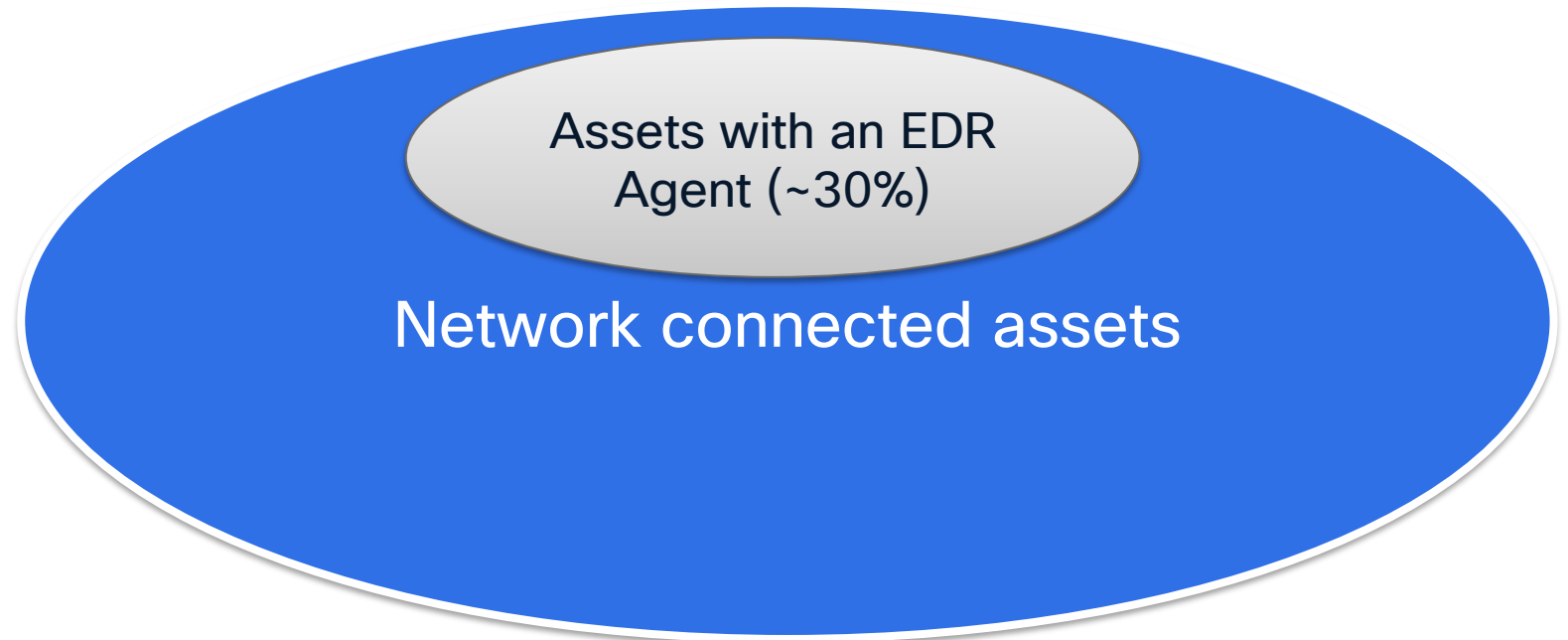
Alert Type	Telemetry	Observation Types	History	MITRE ATT&CK Ta...	MITRE ATT&CK Te...
<div>▼</div>	<div>3 Selections</div>	<div>▼</div>		<div>▼</div>	<div>▼</div>
<div>></div> Amplification Attack Device sent traffic with a profile that suggests participation in an amplification attack. This may indicate the device is part of a botnet.	<div>Netflow</div> <div>North-South</div>	<div>•</div> Traffic Amplification	0 Days	<div>Impact</div>	<div>Reflection Amplificat...</div>
<div>></div> Anomalous AWS Workspace An AWS Virtual Workspace used a new anomalous behavioral profile (e.g., the host connected to many devices over BitTorrent). This may be an indication of malware or misuse.	<div>Netflow</div> <div>North-South</div>	<div>•</div> Anomalous Profile	14 Days	<div>Execution</div>	<div>Cloud Administratio...</div>
<div>></div> Anomalous Mac Workstation An Apple Mac Workstation used a new anomalous behavioral profile (e.g., the host connected to many devices over BitTorrent). This may be an indication of malware or misuse.	<div>Netflow</div> <div>North-South</div>	<div>•</div> Anomalous Profile	14 Days	<div>Execution</div>	
<div>></div> Anomalous Windows Workstation A Windows workstation used a new anomalous behavioral profile (e.g., the host connected to many devices over BitTorrent). This may be an indication of malware or misuse.	<div>Netflow</div> <div>North-South</div>	<div>•</div> Anomalous Profile	14 Days	<div>Execution</div>	
<div>></div> Attendance Drop Device is normally active for most of the day, but its activity dropped across multiple profiles (e.g., SSH Server, FTP Server). This may indicate that the device is no longer operational.	<div>Netflow</div>	<div>•</div> Historical Outlier	14 Days	<div>Impact</div>	<div>Endpoint Denial of S...</div>
<div>></div> Azure Exposed Services An open service like a dashboard or a database is exposed to the Internet. This may indicate that sensitive data are inadvertently exposed.	<div>Azure API</div> <div>Netflow</div>	<div>•</div> Azure Exposed Services	0 Days	<div>Reconnaissance</div>	<div>Gather Victim Host I...</div>
<div>></div> Country Set Deviation Device has significantly deviated from the set of countries it usually communicates with. This may indicate a device is compromised.	<div>Netflow</div> <div>North-South</div>	<div>•</div> Country Set Deviation	36 Days	<div>Command and Cont...</div> <div>Exfiltration</div> <div>Initial Access</div>	<div>Valid Accounts</div>

Network behaviours indicative of suspicious and/or malicious activity.

Why NBAD?

Many of the devices connected to the network, wired and wireless, do not run an endpoint security client (EDR).

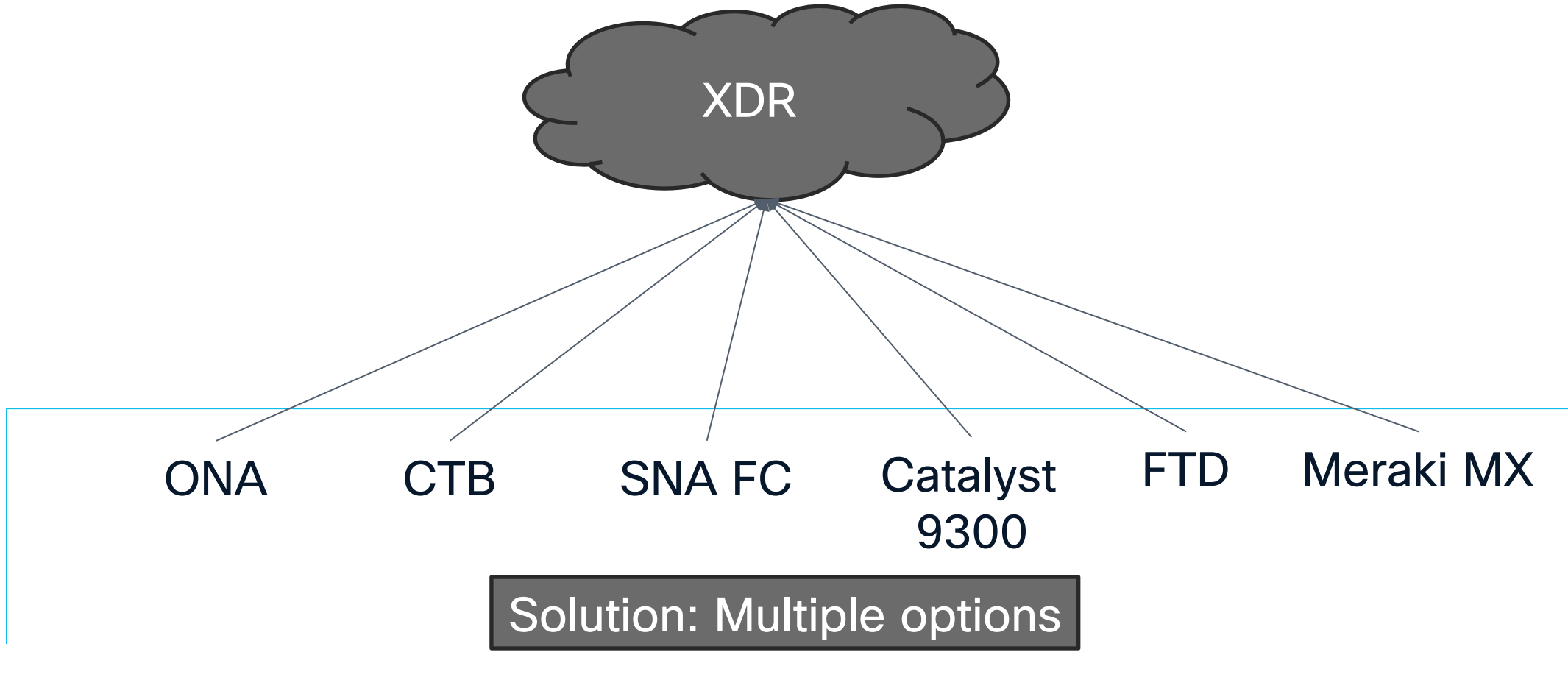
- IOT (MRI, cameras)
- Smart building
- Card readers
- Infrastructure
- Printers
- Phones
- Scanners
- TVs
- Etc.



Threat actors are increasingly using these “other” network connected assets as their point of presence/operations

XDR: Getting Network Data In

Problem: Getting on-premises network data into a SaaS product



XDR Network: Tuning

Best practice: Define subnets and their sensitivity

Subnet Name	Sensitivity ?	Static ?	New Device Alerts ?
<div>= 10.70.70.0/24</div> <div>10.70.70.0/24 (PCI Servers)</div>	High	☒	☐

20 Per Page

Low
Normal
High

1-1 of 1 results

Define watchlists

Doublecheck telemetry

Alert Type	Observation Types	History ?	Priority ?	Enabled ?	Telemetry ?	Cisco XDR ...
<div><div>Country Watchlist: Protocol Violation</div><div>Device tried to communicate with a host in a user-supplied watchlisted country on an illegal protocol / port combination (e.g., UDP on port 22). This may indicate the presence of a malicious covert communications channel.</div></div>	<div>Bad Protocol</div>	0 Days	Normal Default Priority: Normal	☒ Default: Disabled	<div>ETA</div> <div>Netflow</div> <div>North-South</div>	☐

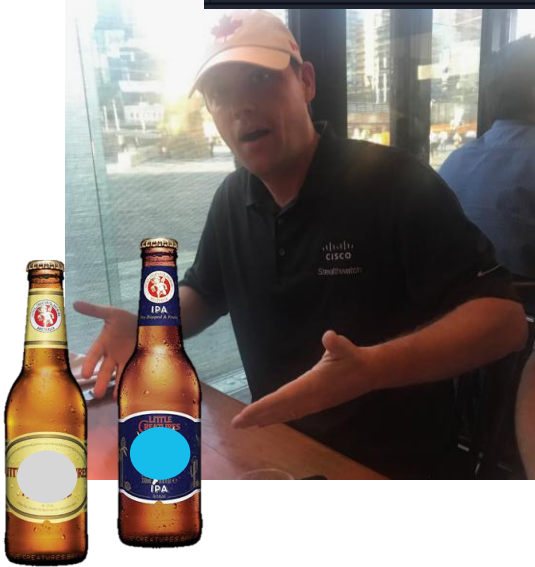
Read about observations and history

Enable/Disable and Priority

Note: User watchlist alerts are not correlated into incidents today

Example Network Threat Detection: Data Exfiltration

Alert Type	Observation Types	History ?	Priority ?	Enabled ?	Telemetry ?	Cisco XDR ...	MITRE ATT&CK Ta...
<div>▼</div>	<div>[-] Potential Data Forwarding × ▼</div>		<div>▼</div>	<div>▼</div>	<div>[-] Netflow × ▼</div>	<div>▼</div>	<div>▼</div>
<div>Potential Data Exfiltration Device downloaded data from an internal device that it doesn't communicate with regularly. Shortly after that, the device uploaded a similar amount of data to an external device. This may indicate that sensitive data is compromised.</div>	<div>• Potential Data Forwarding</div>	<div>0 Days</div>	<div>High Default Priority: Normal</div>	<div>☒ Enabled Default: Disabled</div>	<div><div>East-West</div><div>Netflow</div><div>North-South</div></div>	<div>☐</div>	<div>Exfiltration</div>



Important data repository



Outside repository

Downloads sensitive data

Malicious Actor

Exfiltrates data

Example Network Flow log Detection

	Alert Type ^	Observation Types	History ⓘ ⚙	MITRE ATT&CK Ta...	MITRE ATT&CK Te...
	<div>= Outbound Traffic</div>	<div>⌵</div>		<div>⌵</div>	<div>⌵</div>
>	<div>Outbound Traffic Spike</div> <div>Device started sending a much larger amount of traffic to external destinations than before. This may indicate data exfiltration.</div>	<div><ul style="list-style-type: none">Record Profile OutlierNew Large Connection (External)Record Metric Outlier</div>	14 Days	<div>Exfiltration</div> <div>Impact</div>	<div>Network Denial of S...</div> <div>Automated Exfiltration</div>



✔ Outbound Traffic Spike

Alert Type Details

Description

Device started sending a much larger amount of traffic to external destinations than before. This may indicate data exfiltration.

Next Steps

Reference the supporting evidence to determine the nature of the traffic and where it was sent (e.g., a large Dropbox upload). If the traffic is suspicious, contact the user or machine owner to determine why the traffic was moved externally. Block traffic as needed at the perimeter.

MITRE Tactics

Exfiltration

Impact

MITRE Techniques

Network Denial of Service

Automated Exfiltration

Alert Type Priority

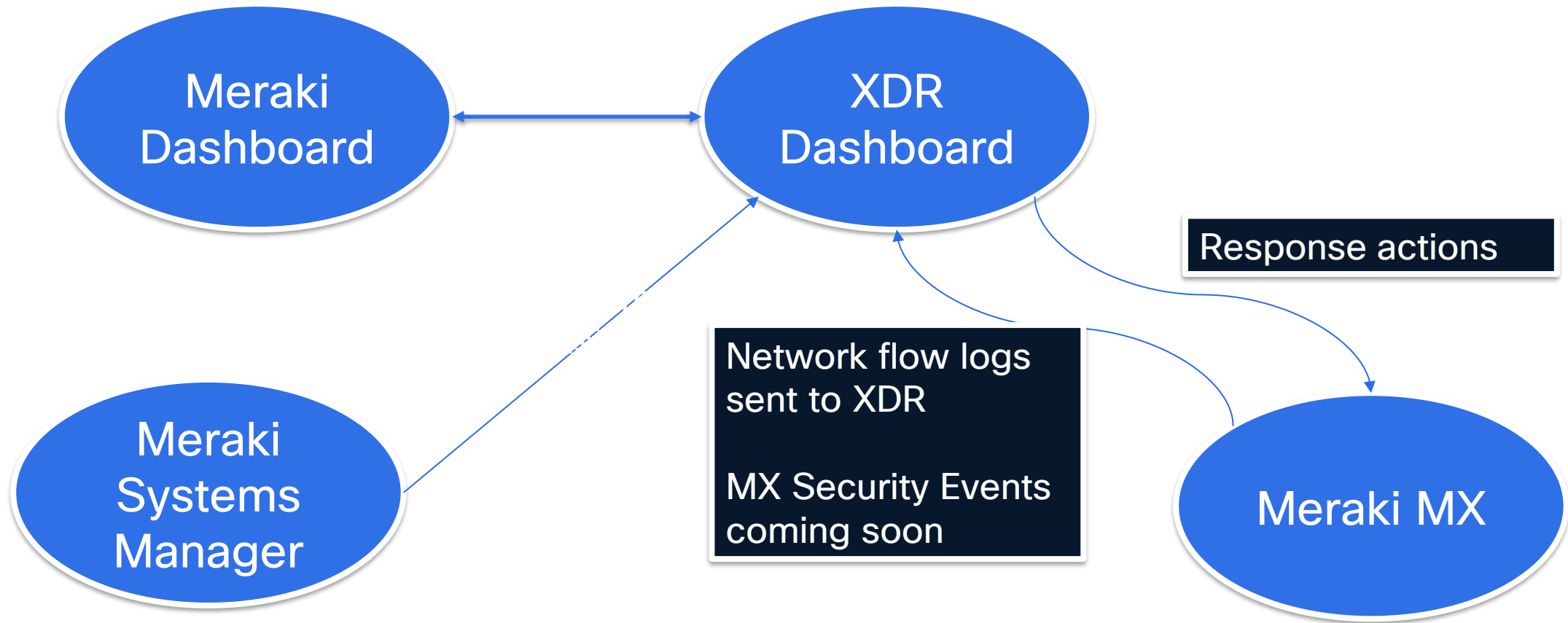
Low (Default)

go to alert priorities page ↻

Example Deployment with Meraki

High Level: Meraki-XDR Integration Today

Meraki MX with Cisco XDR deployment is extraordinarily easy



Meraki and XDR Requirements

Licensing

- Cisco XDR Essentials, Advantage, or Premier license
- Cisco Meraki Advanced Security, SD-WAN+, Essentials or Advantage license.

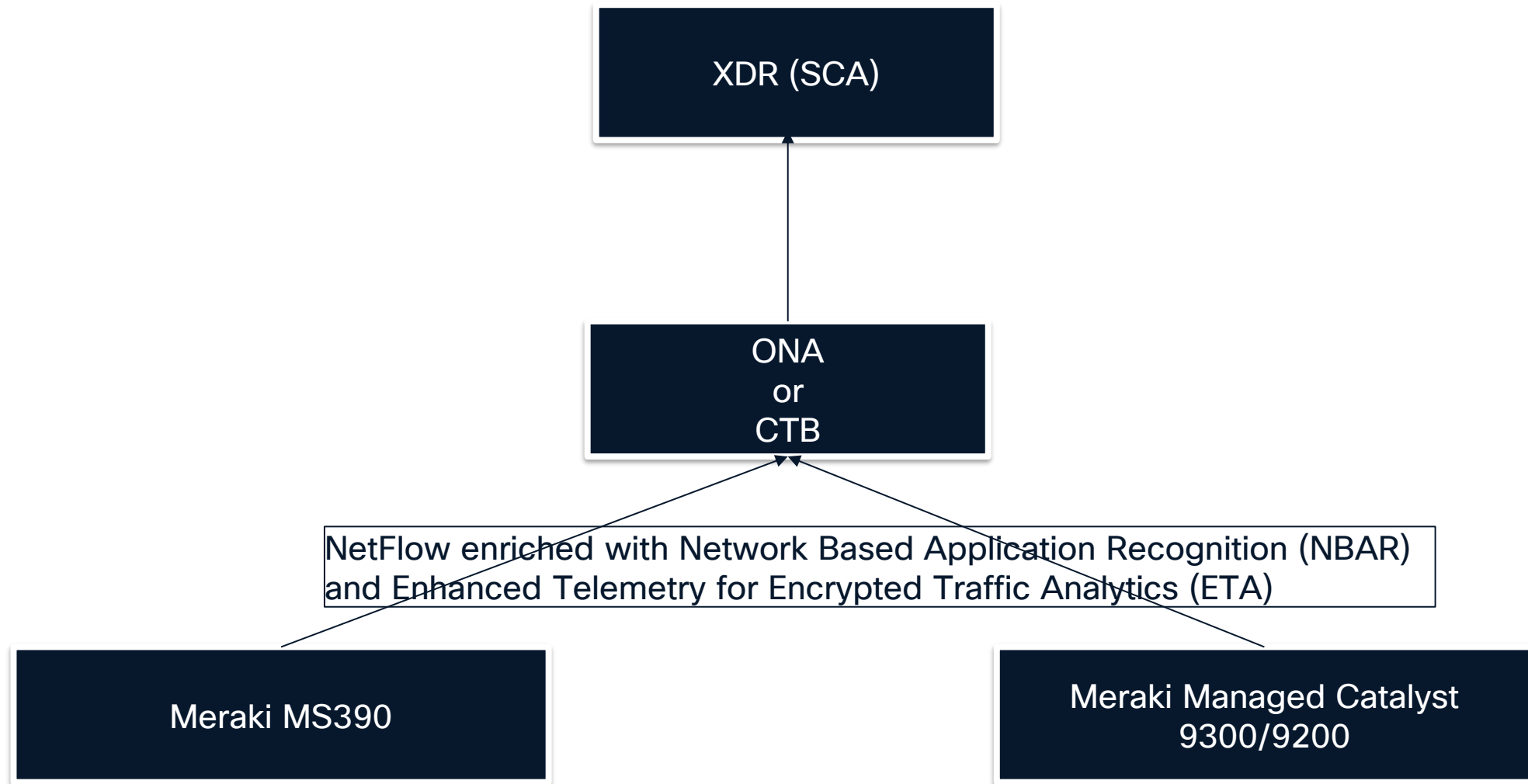
Firmware

- Meraki MX Appliances running Firmware 19.1.4 or newer
- Firmware restrictions per platform are documented [here](#)

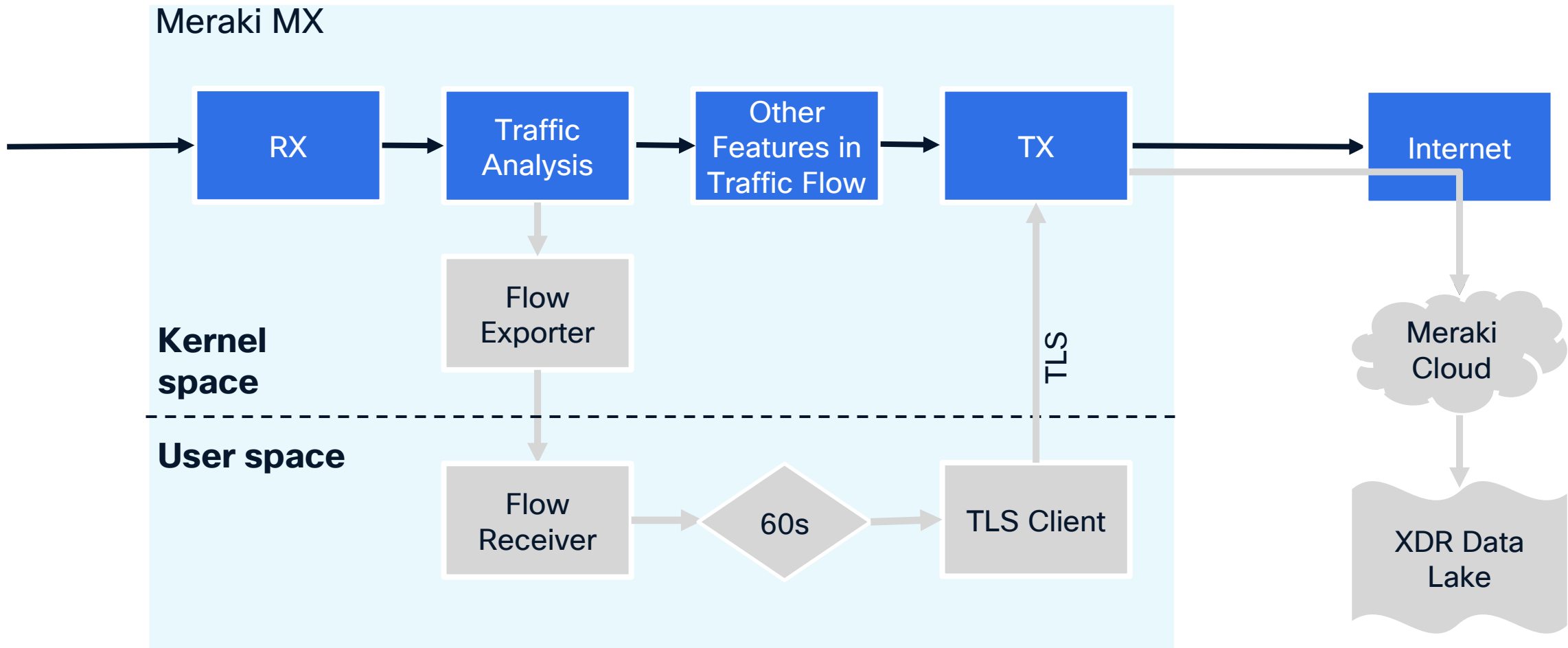
Platforms

- Z3, Z4
- MX67, 68, 75, 85, 95, 105, 250, 450
- Virtual MX – S/M/L
- Not supported: vMX-XL, MX650, older platforms incompatible with 19.x such as the MX100, MX84, MX64

Other Meraki NetFlow Exporters



MX Telemetry Packet Flow



What's in a Namespace?

	Time	Namespace ?	IP	Connected_IP
	filter by custom range ...		= 192.168.192.100	
>	2025-10-30 10:29:55 PDT	meraki:460175:N_573083052583264647:Q3FA-LXHU-BP6E	192.168.192.100	184.28.149.157
>	2025-10-27 13:24:13 PDT	on-prem:ONA:ona	192.168.192.100	208.67.22...

Namespace:

- SCA concept to delineate a uniquely named portion of a deployment
- Inside of a namespace an entity is considered unique
- In a standard deployment there is usually only one namespace:
 - NVM, firewall, ONA, CTB exporters map to the default namespace



SCA tracks entities by a device ID: a device ID is unique inside of a namespace

The problem of the overlapping IP



Meraki Networks



Meraki + Namespace: Monitoring Overlapping IP Addresses

Each Meraki MX is considered a new namespace: allowing creation of SCA IDs based on (MX-id, IP)

IP*

192.168.192.100

Start/End date

2025-11-01 00:00:00 PDT

2025-11-01 00:00:00 PDT

Day

2025-11-01 (US/Pacific)

IP

192.168.192.100

20

Per Page

Device (sjcampus-windows11-pos)

Device (192.168.192.100)

Device (192.168.192.100)

Device Report | sjcampus-windows11-pos

Device Outline

Last updated: yesterday 2025-11-01

sjcampus-windows11-pos

more actions

Name

sjcampus-windows11-pos

IPs

192.168.192.100

Hostnames

sjcampus-windows11-pos

Subnets

192.168.192.0/24 (Retail)

Entity Groups

Retail POS Terminals

Open Alerts

1

Int Connections

0

Ext Connections

0

Hostname

RETAIL-SJBRANCH-POS-WINDOWS11

OS Name

WinNT

OS Version

10.0.22621

Device Manufa...

VMware, Inc.

Mac Address

005056ba2e79

Sensors

ona,ctb-broker,10.1.1.200

Sensor Types

CTB,ONA,SAL

Exporters

10.1.1.1,192.168.138.1,FTD

Device Report | 192.168.192.100

Device Outline

Last updated: yesterday 2025-11-01

192.168.192.100

more actions

Name

192.168.192.100

IPs

192.168.192.100

Roles

Remote Desktop Server

Entity Groups

Retail POS Terminals

Open Alerts

0

Int Connections

1

Ext Connections

44

ATTENDANCE

Normally Active 1:57:34 to 21:30:00

Demo(s)

Summary

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.

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

Parting Thoughts

Simplify your security operations with Cisco XDR!

Behaviour-based detections are a critical component of the modern security operations centre

Meraki and XDR combination is something truly special



Final Parting Thought

Keep your eyes open
and
don't have your beer stolen.



Thank you

CISCO Live !

