



The bridge to possible

# Extended Detection with Cisco XDR

Data, Analytics and Attack Chains

Matt Robertson  
Distinguished Engineer  
BRKSEC-2178

CISCO *Live!*

#CiscoLive

# Cisco Webex App

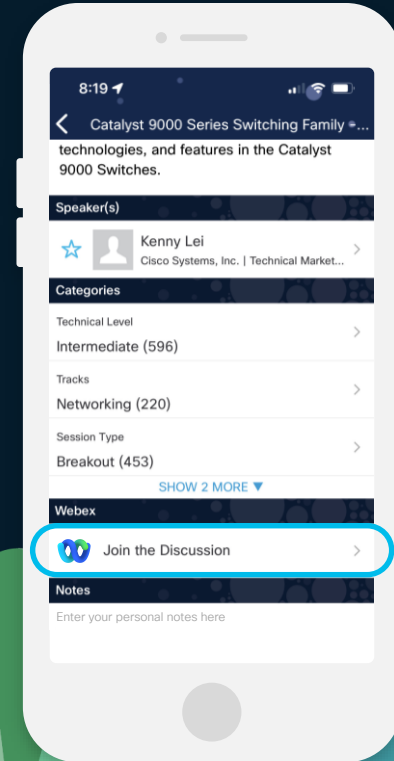
## Questions?

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 June 7, 2024.



# Agenda

## Objective:

Understand Cisco XDR Analytics



## Agenda:

- Intro to Cisco XDR
- Data, Analytics and Detection
- Correlated Incident Generation
- Summary



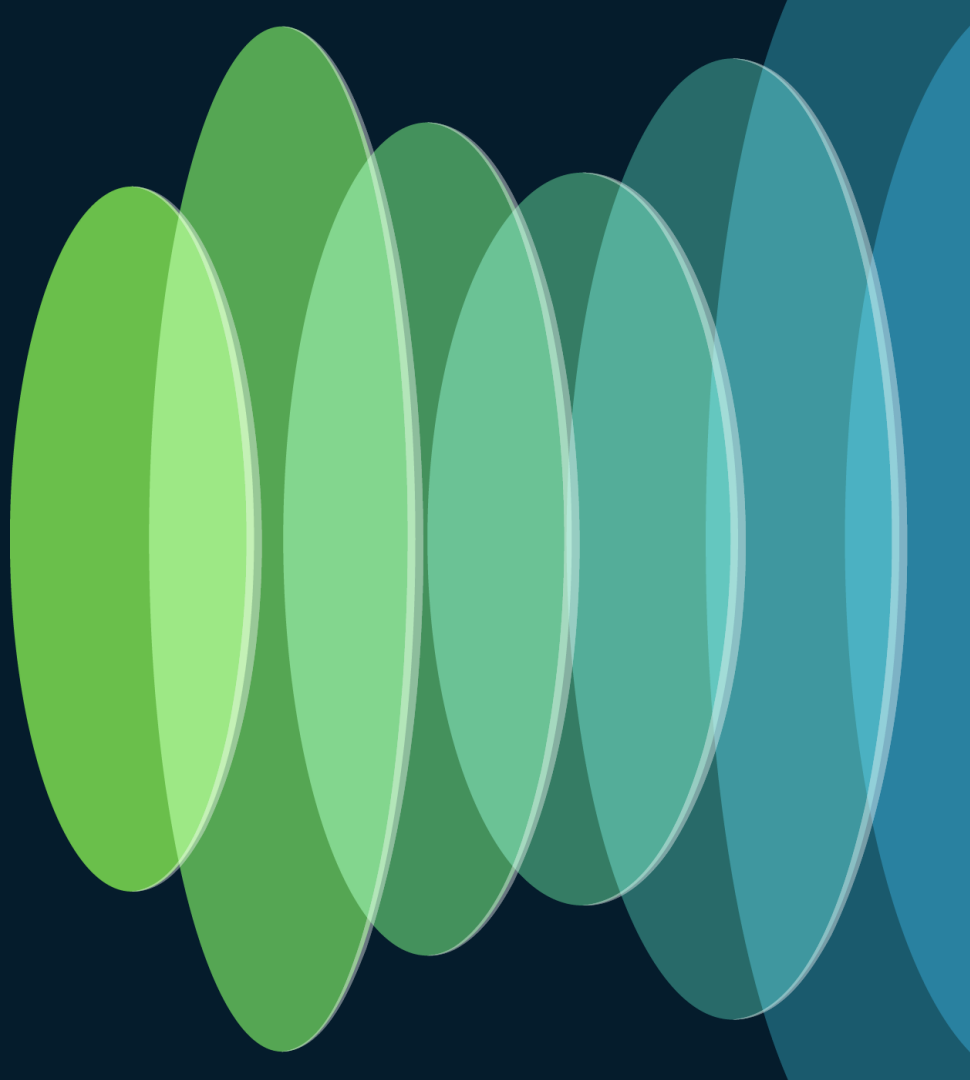
# About Me

## Matt Robertson

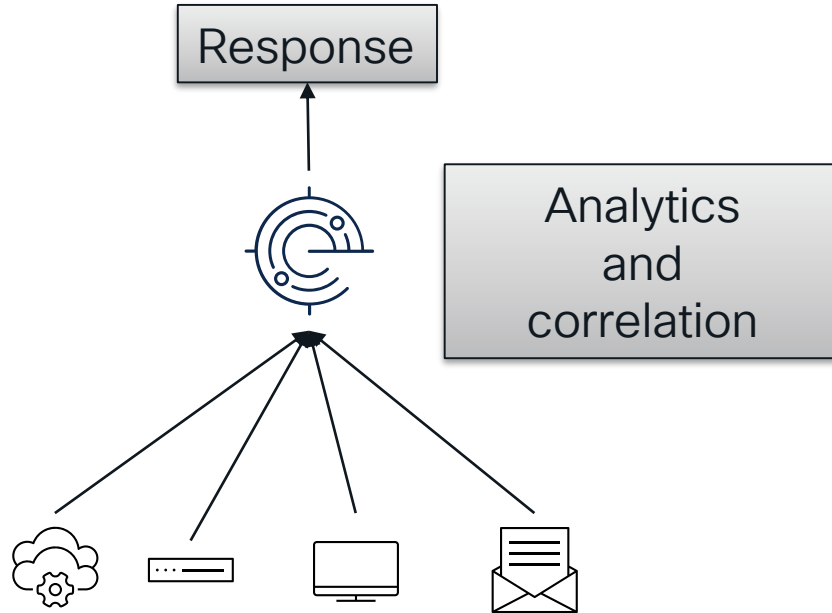
- Distinguished Technical Marketing Engineer
- Extended Threat Detection and Security Analytics
- Cisco Live Distinguished Speaker
- 16+ years at Cisco: Development, TME, Lancope
- Canadian eh



# What is Cisco XDR?



# Cisco XDR



Collection of telemetry from multiple sources

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

Accelerate that OODA Loop!

# 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*

## 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

## 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.

# Some Current Integrations

## Threat Hunting and Investigation

### Data Analytics and Correlation

#### Cisco

- Network Telemetry
- NGFW via SAL Logging
- Identity Service Engine
- Public Cloud Infrastructure
- Secure Client NVM
- Secure Endpoint
- Email Threat Defense

#### 3rd Party

- CrowdStrike
- Microsoft Defender for Endpoint

#### Cisco

- AMP File Reputation
- Global Threat Intelligence
- Secure Client NVM
- Secure Email and Web Manager
- Secure Email Gateway
- Secure Email Threat Defense
- Secure Endpoint
- Secure Firewall (FPR)
- Secure Malware Analytics
- Secure Network Analytics
- Secure Web Appliance
- Threat Intelligence API \*2
- Umbrella
- Talos Intelligence

#### 3rd Party

- Amazon GuardDuty
- CrowdStrike
- Cybereason
- Devo
- Exabeam
- Google Chronicle
- Google Safe Browsing
- Graylog
- Have I Been Pwned
- IBM X-Force Exchange
- IsItPhishing
- LogRhythm
- Microsoft Defender for Endpoint
- Palo Alto Networks AutoFocus
- SentinelOne
- Trend Micro Vision One
- more...



# Some Current Integrations

## Asset Insights and Context

### Cisco

- DUO (Devices)
- Meraki MX
- Orbital
- Secure Access
- Secure Client NVM
- Secure Endpoint
- Umbrella

### 3<sup>rd</sup> Party

- CrowdStrike
- Ivanti Neurons
- Jamf Pro
- Microsoft Azure AD (Users)
- Microsoft Defender for Endpoint
- Microsoft Intune
- SentinelOne
- VMWare Workspace ONE UEM
- ServiceNow SecOps

## Automation and Response

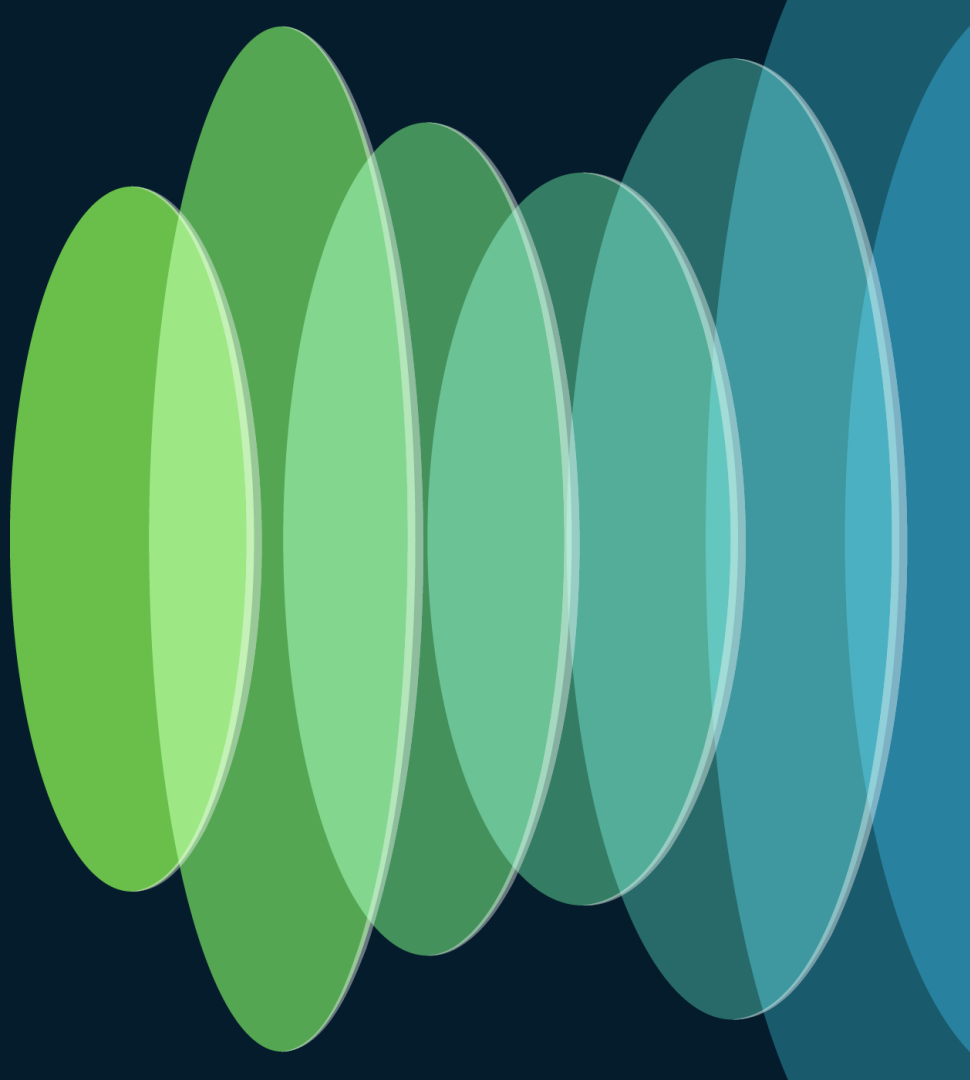
### Cisco

- Adaptive Security Appliance
- Attack Surface Management
- Defense Orchestrator
- Identity Services Engine
- Meraki MX
- Orbital
- Secure Email and Web Manager
- Secure Email Gateway
- Secure Email Threat Defense
- Secure Endpoint
- Secure Firewall (FPR)
- Secure Malware Analytics
- Secure Network Analytics
- Security Management Appliance
- Umbrella
- Vulnerability Management

### 3<sup>rd</sup> Party

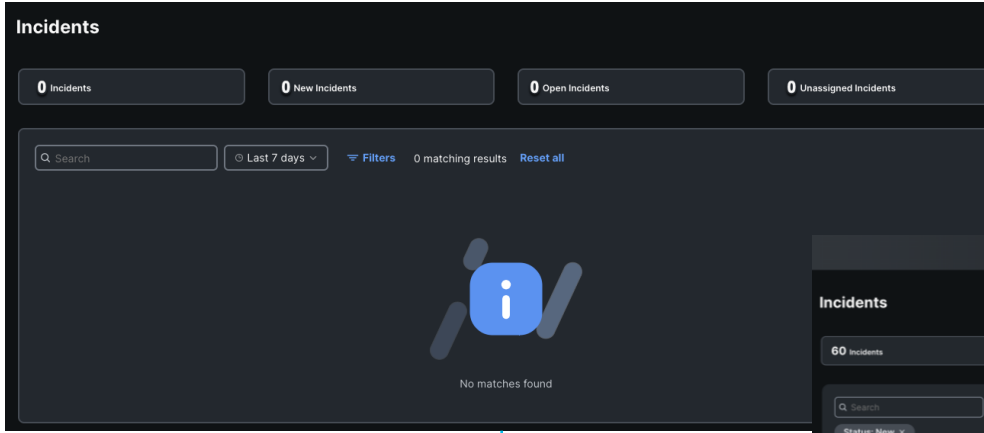
- Amazon Web Services
- CrowdStrike
- Cybereason
- ExtraHop
- Fortinet Fortigate
- Google Cloud Platform
- Jamf Pro
- Microsoft Azure
- Microsoft Azure AD
- Microsoft Defender for Endpoint
- Palo Alto Cortex
- Palo Alto Panorama
- SentinelOne
- Trend Micro Vision One

# Data, Analytics and Detection



# XDR Outcome:

Analytics to the collected & homogenized data to arrive at a detection of maliciousness



How do we get incidents?

The screenshot shows the 'Incidents' dashboard with a search bar and filters. The status summary at the top indicates: 60 Incidents, 7 New Incidents, 13 Open Incidents, and 60 Unassigned Incidents. Below the search bar, it says '7 matching results' and 'Reset all'. A table of incidents is displayed below the filters.

	Priority	Name	Source	Created	Assigned	Status
<input type="checkbox"/>	1000	AWS Root Account Used on (Amazon Web Services) 561766456620/root	Cisco XDR Analytics (s...	2 Months	Unassigned	New
<input type="checkbox"/>	1000	LDAP Connection from Suspicious Process on ats-membersrvr.securitydemo.net	Cisco XDR Analytics (s...	1 Month	Unassigned	New
<input type="checkbox"/>	1000	LDAP Connection from Suspicious Process on ats-membersrvr.securitydemo.net	Cisco XDR Analytics (s...	1 Month	Unassigned	New
<input type="checkbox"/>	719	Potential Persistence Attempt on loxx-win10vic01.org26.net	Cisco XDR Analytics (s...	1 Month	Unassigned	New
<input type="checkbox"/>	900	Suspicious Process Path on loxx-win10vic01.org26.net	Cisco XDR Analytics (s...	23 Days	Unassigned	New
<input type="checkbox"/>	404	ATW-SurfacePro4 in group ATW-Audit @ 20231005 00:00:26	Secure Endpoint	2 Days	Unassigned	New
<input type="checkbox"/>	447	Port 8888: Connections from multiple sources on ats-ubuntu04.securitydemo.net	Cisco XDR Analytics (s...	1 Day	Unassigned	New

25 per page 1-7 of 7 < < 1 / 1 > >

# 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 Analytics interface for an incident titled "AWS Compromise: Root-Level Breach and Remote Access". The interface includes a top navigation bar with tabs for Overview, Detection, Response, and Worklog. A sidebar on the left contains a search bar and a list of assets. The main content area shows a timeline of events, with a highlighted section for "Accessed By/Conn...". Below this, there are two sections: "IP Addresses" and "Endpoints". The "Endpoints" section lists four items: i-09b43c7b5a2314796, aws\_demouser, aws\_admin, and root. A MITRE ATT&CK framework overlay is visible on the right side of the screen, listing various tactics and techniques. At the bottom, there are three summary cards: "6 Assets TOP ACTIVE", "68 Observables TOP ACTIVE", and "15 Indicators TOP ACTIVE".

1000 New AWS Compromise: Root-Level Breach and Remote Access

Reported by Cisco XDR Analytics (cisco-explorcorp-earth) on 2024-04-17T22:23:14.732Z - 2 Linked Incidents

This incident started on the 13th of October, 2023 at 15:12:29 UTC and ended on the 27th of February, 2024 at 00:35:44 UTC. The key concern was...

Overview Detection Response Worklog

Expand

IP Addresses

Endpoints

Accessed By/Conn...

i-09b43c7b5a2314796 aws\_demouser aws\_admin root

MITRE ATT&CK View Details

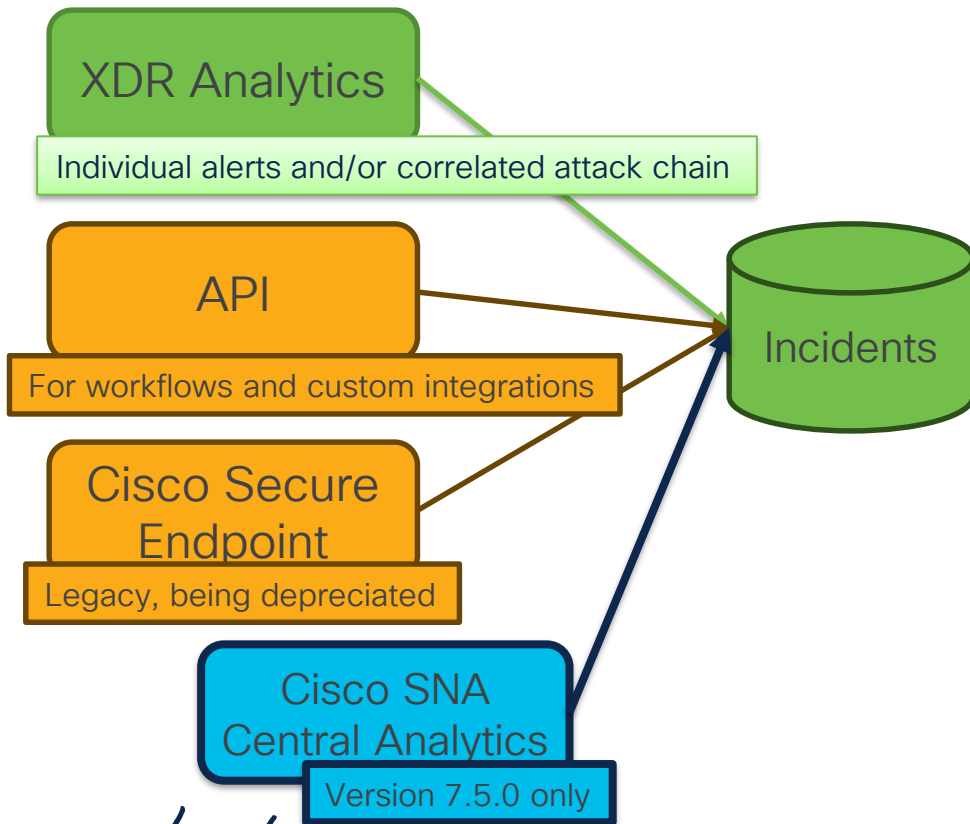
- TA0043: Reconnaissance
- TA0042: Resource Development
- TA0001: Initial Access
- TA0002: Execution
- TA0003: Persistence
- TA0004: Privilege Escalation
- TA0005: Defense Evasion
- TA0006: Credential Access
- TA0007: Discovery
- TA0008: Lateral Movement
- TA0009: Collection
- TA0011: Command and Control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

6 Assets TOP ACTIVE View all

68 Observables TOP ACTIVE View all

15 Indicators TOP ACTIVE View all

# Where do incidents come from? (current status)



**Incidents**

60 Incidents | 7 New Incidents | 13 Open Incidents | 60 Unassigned Incidents

Search: [ ] Last year: [ ] Filters: 7 matching results Reset all

Status: New

<input type="checkbox"/>	Priority	Name	Source	Created	Assigned	Status
<input type="checkbox"/>	1000	AWS Root Account Used on (Amazon Web Services) 56786456820/root	Cisco XDR Analytics (s...	2 Months	Unassigned	New
<input type="checkbox"/>	1000	LDAP Connection from Suspicious Process on ats-membersrvr.securitydemo.net	Cisco XDR Analytics (s...	1 Month	Unassigned	New
<input type="checkbox"/>	1000	LDAP Connection from Suspicious Process on ats-membersrvr.securitydemo.net	Cisco XDR Analytics (s...	1 Month	Unassigned	New
<input type="checkbox"/>	750	Potential Persistence Attempt on lxx-wsl0vic06.org26.net	Cisco XDR Analytics (s...	1 Month	Unassigned	New
<input type="checkbox"/>	900	Suspicious Process Path on lxx-wsl0vic01.org26.net	Cisco XDR Analytics (s...	23 Days	Unassigned	New
<input type="checkbox"/>	400	ATW SurfacePro4 in group ATW-Audit @ 20231005 00:00:36	Secure Endpoint	2 Days	Unassigned	New
<input type="checkbox"/>	647	Port 8888: Connections from multiple sources on ats-ubuntu04.securitydemo.net	Cisco XDR Analytics (s...	1 Day	Unassigned	New

25 per page 1-7 of 7

# Important Distinction in Terms

## Correlation

### Pre-Incident Creation

Data from multiple security tools is analysed to arrive at a detection of maliciousness

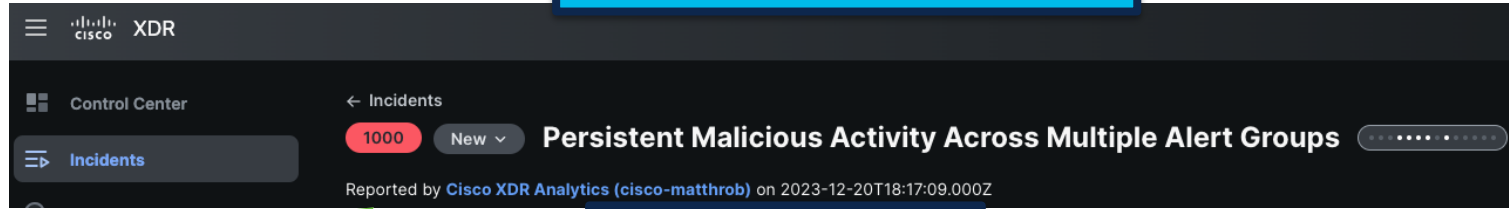
## Enrichment

### Post-Incident Creation

A detection of maliciousness is further enhanced with data from integrated security tools.

# Aside: A note about UI's

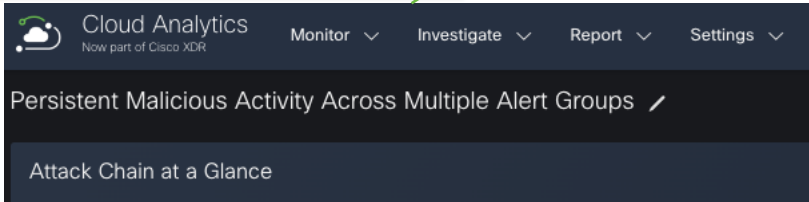
Main XDR User Interface



Attack Chains, Alerts  
exported into Incident  
Manager

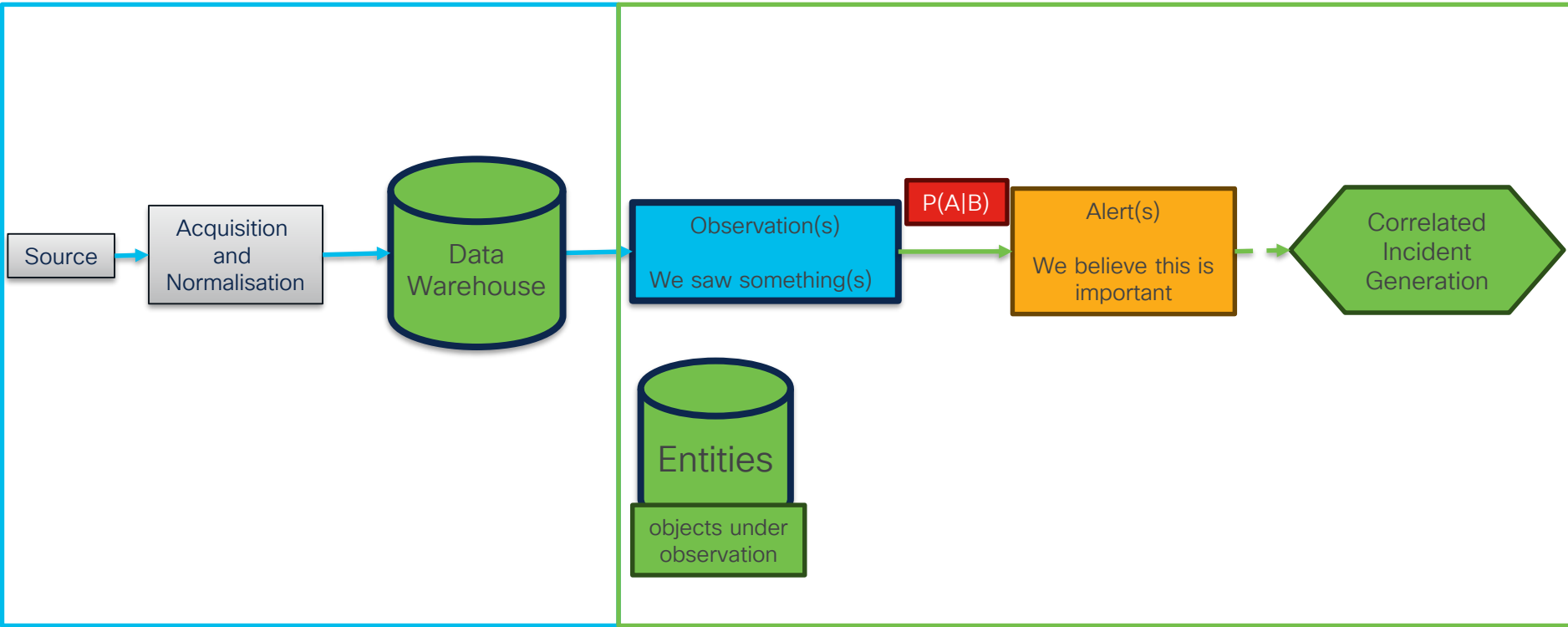
SOC dashboard

Secure Cloud Analytics, also known as  
XDR Analytics



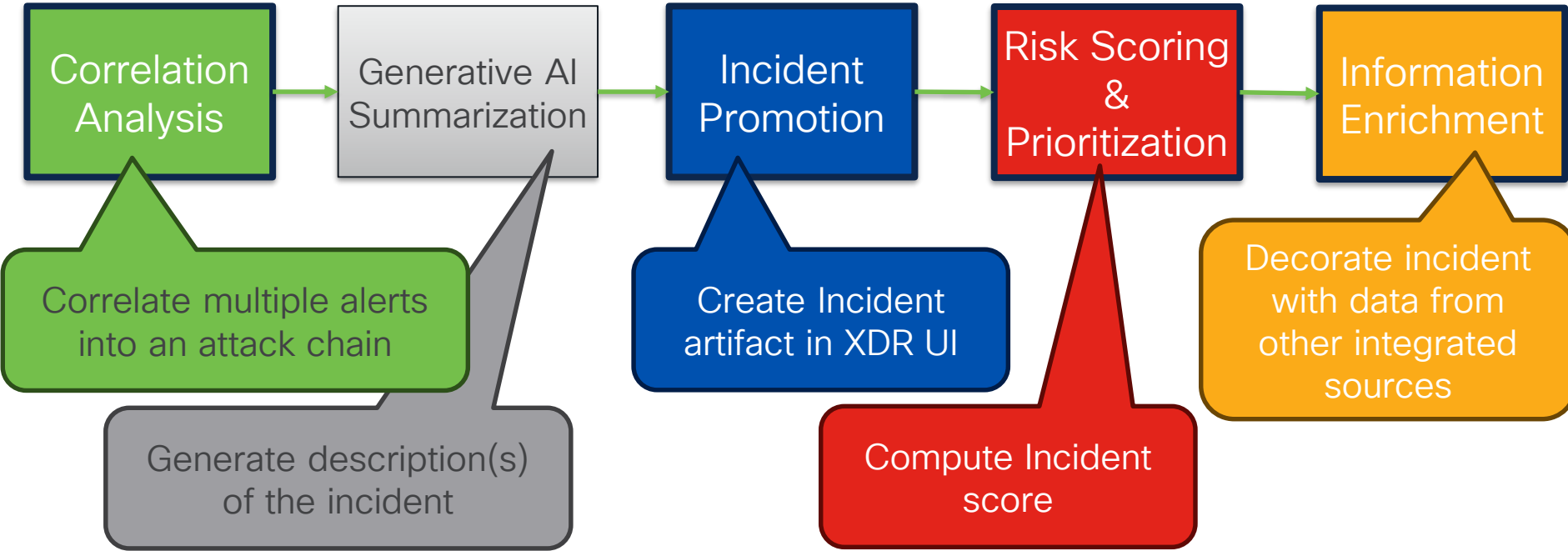
"Detection Engineering" dashboard.  
Admin for analytics stack.

# Data Analytics Pipeline

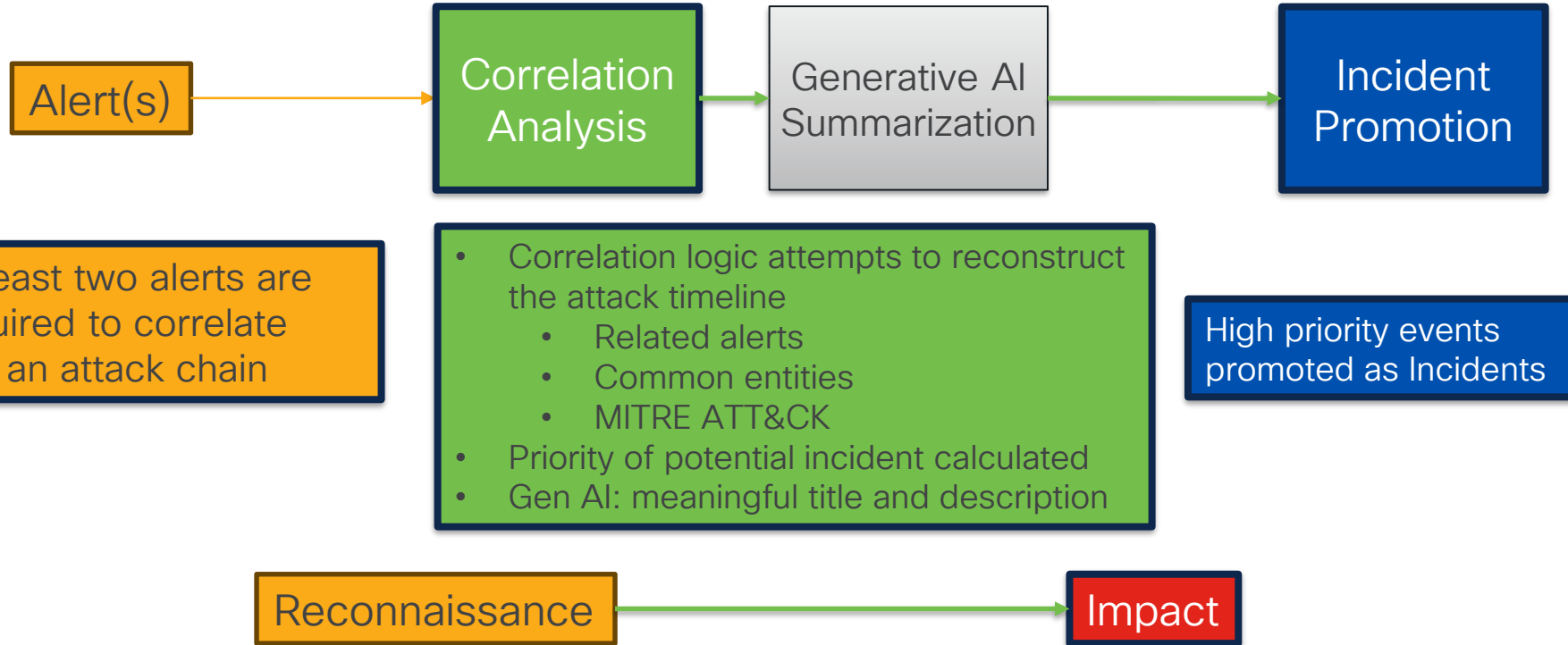




# Correlated Incident Generation



# Correlation Analysis: Attack Chains



# Native Detection vs Extended Detection

## Native

XDR can create alerts from downstream sources that have no native verdicts:  
NetFlow, NVM, Cloud logs, ISE, FTD

High Fidelity, Low Noise

Alerts have passed a threshold for active notification.  
Not all potentially malicious events pass this threshold

## Extended

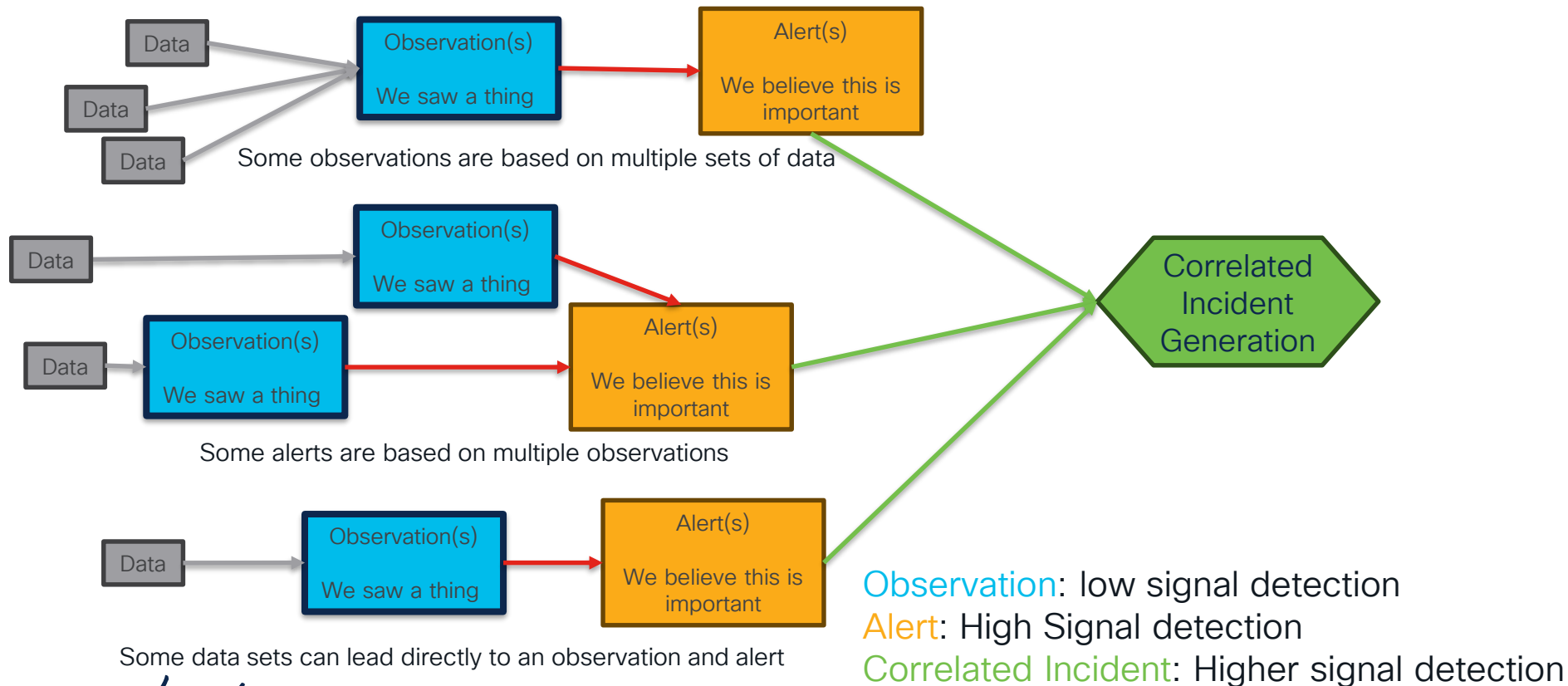
XDR collects and extends downstream data sources that have verdicts:  
EDRs, ETD, NDRs\*, etc

# Creating Security Value from Data



There is an AI/ML model behind observation to alert

# Detection and Correlation



# Alerts Require (Specific) Data

Alert Type	Observation Types	Telemetry	History
<div>▼</div>	<div>▼</div>	<div>2 Selections X ^</div> <div>Endpoint X Cisco ISE X</div> <div>Azure Activity Logs</div> <div>Azure API</div> <div>Cisco ISE ✓</div> <div>Cisco NVM</div> <div>Endpoint ✓</div> <div>ETA</div> <div>Firewall</div> <div>GCP API</div> <div>GCP Audit Logs</div> <div>Netflow</div>	
<div>&gt;</div> <div><b>Abnormal ISE User</b></div> <div>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.</div>	<div>•</div> <div>ISE Session Started</div>		36 Days
<div>&gt;</div> <div><b>Invalid MAC Address</b></div> <div>A device with an unregistered MAC address Organizational Unique Identifier was detected. This is not always malicious, but can indicate an attempt to bypass MAC Access Control (MAC filtering), conduct an Adversary-in-the-Middle technique, or impair other defensive capabilities.</div>	<div>•</div> <div>Invalid MAC Address</div>		0 Days
<div>&gt;</div> <div><b>ISE Jailbroken Device</b></div> <div>A jailbroken device was detected. This does not necessarily indicate an active threat in isolation, but is a vulnerability that may increase organizational risk.</div>	<div>•</div> <div>ISE Suspicious Activity</div>		0 Days
<div>&gt;</div> <div><b>Suspicious Endpoint Findings by Collection</b></div> <div>Suspicious behavior(s) have been noted on the endpoint that is mapped to Collection MITRE tactic</div>	<div>•</div> <div>Suspicious Endpoint Security Finding</div>	<div>Endpoint</div>	0 Days
<div>&gt;</div> <div><b>Suspicious Endpoint Findings by Command and Control</b></div> <div>Suspicious behavior(s) have been noted on the endpoint that is mapped to Command and Control MITRE tactic</div>	<div>•</div> <div>Suspicious Endpoint Security Finding</div>	<div>Endpoint</div>	0 Days

Familiarise yourself with the observations, data and history for specific alerts

Alerts can be configured to be published directly to XDR

Alerts/Watchlists

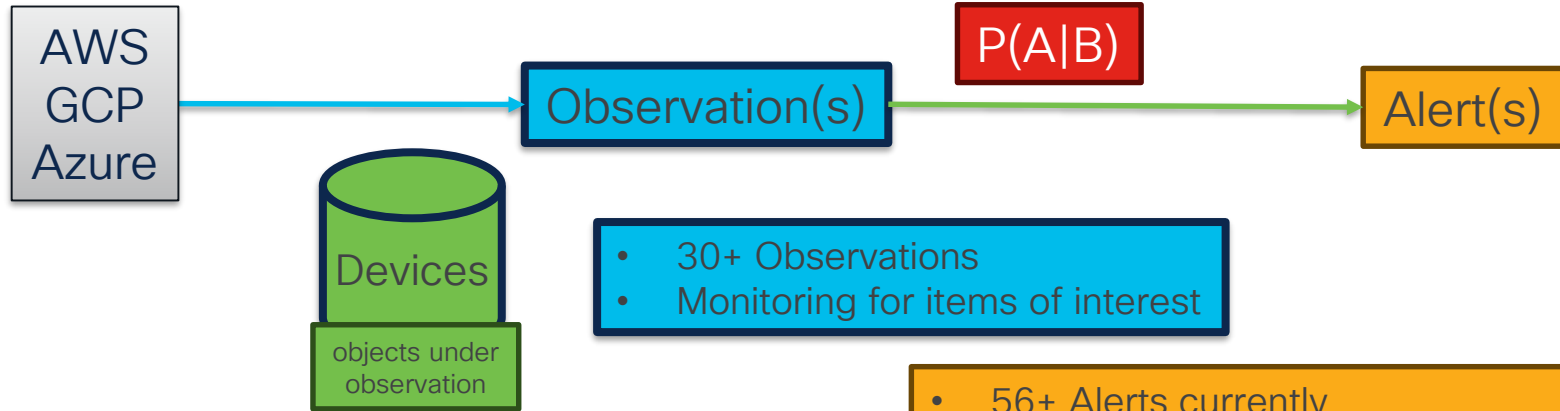
Review [Alert FAQs](#) for more general information about alerts. Review the [Subnet Sensitivity Matrix](#) to understand how subnet sensitivity and alert priorities are configured.

Alert Type	Observation Types	History	Priority	Cisco XDR ...	Enabled
<b>Abnormal ISE User</b> 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	<input type="checkbox"/>	Default: Disabled
<b>Abnormal User</b> 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	<input checked="" type="checkbox"/>	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.

Use discretion; Can result in duplicative incidents.

# IAAS Data Analytics Pipeline

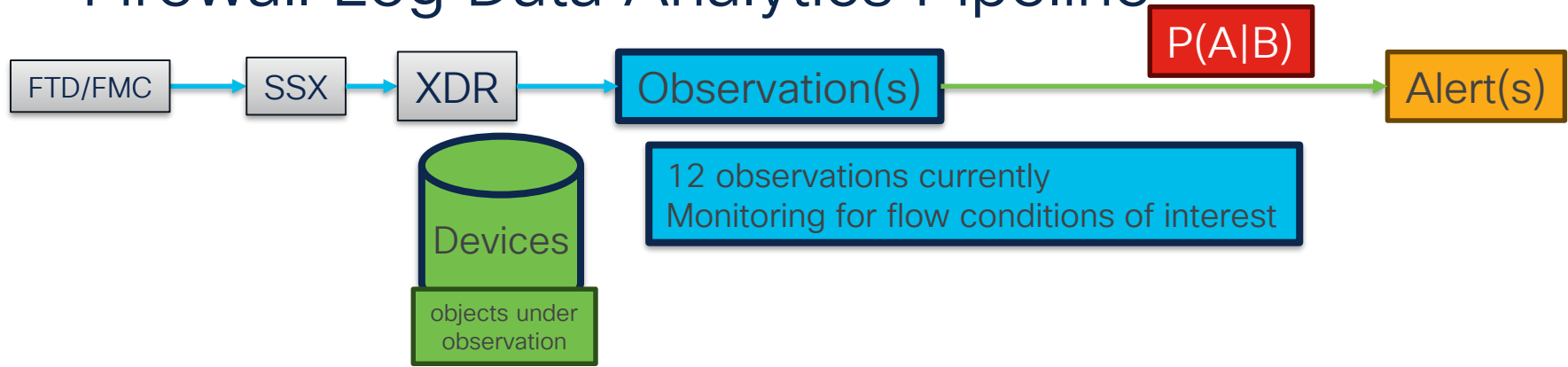


- Integrate on varying service options via API
- Normalise and store data
- Identify devices by numerous cloud objects (user, IP, instance-id, etc.)

- 56+ Alerts currently
- Some alerts are composed of single observation(s)
- Some alerts are composed of multiple observation(s)
- Contain source observations
- Assigned to device
- Correlated into Attack Chains



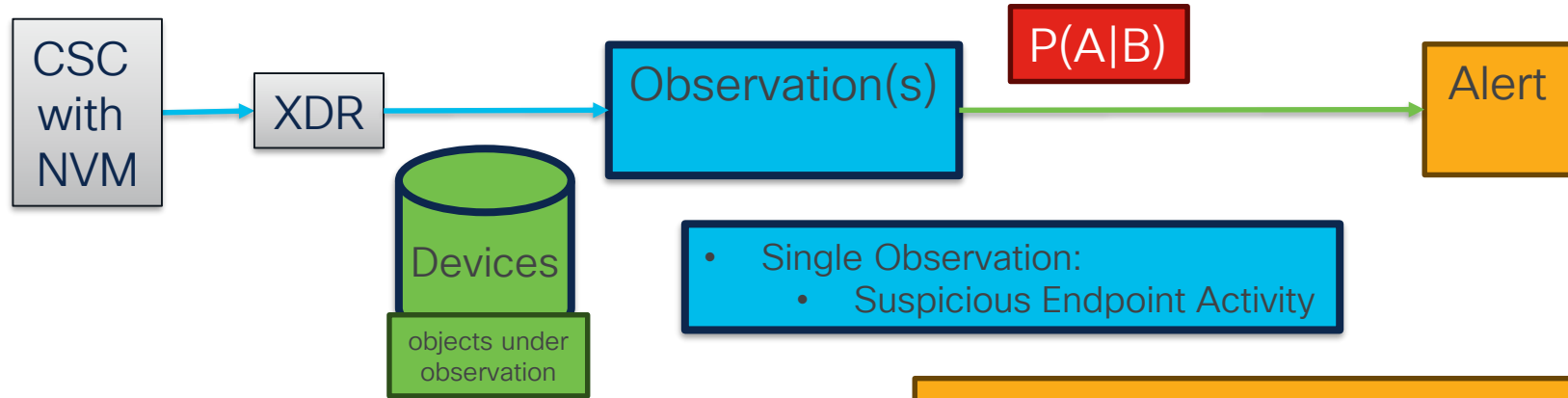
# Firewall Log Data Analytics Pipeline



- Firewall logs (intrusion, malware, file and connection events) sent to Security Services Exchange (SSX)
- Events read off SSX by XDR Analytics
- Logs visible in Event Viewer
- Identify devices by IP Address, Hostname

- 16+ Alerts currently
- Some alerts are composed of single observation(s)
- Some alerts are composed of multiple observation(s)
- Contain source observations
- Assigned to device
- Correlated into Attack Chains

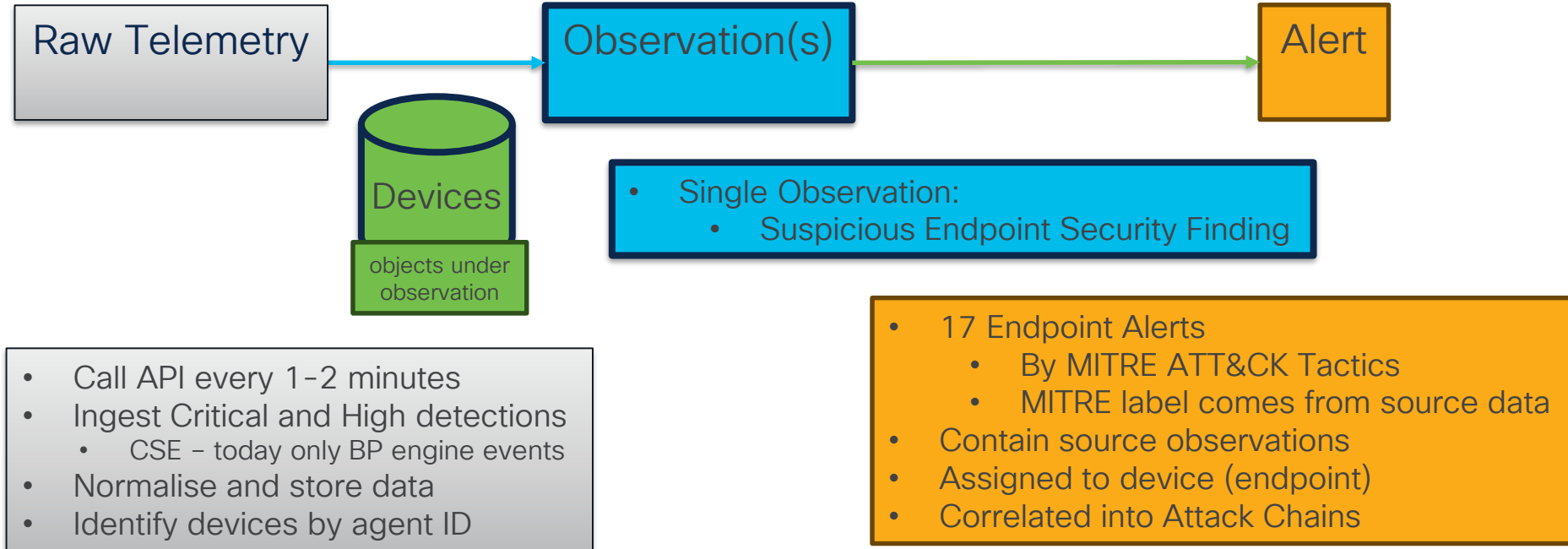
# NVM Data Analytics Pipeline



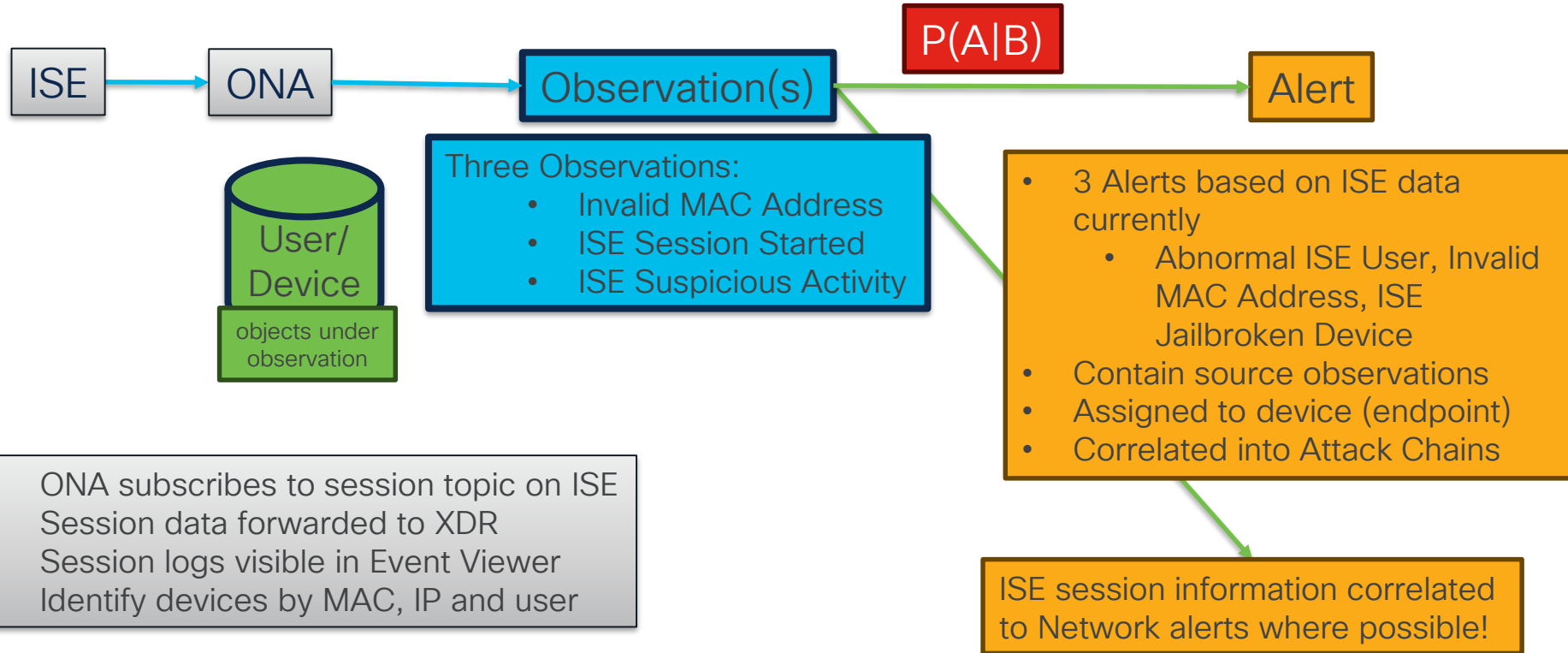
- NVM profile configured to send data direct to XDR cloud
- Normalise and store data
- NVM logs visible in Event Viewer
- Identify devices by agent ID

- 12+ Alerts using NVM data
  - Combination of network and endpoint data artifacts
- Contain source observations
- Assigned to device (endpoint)
- Correlated into Attack Chains

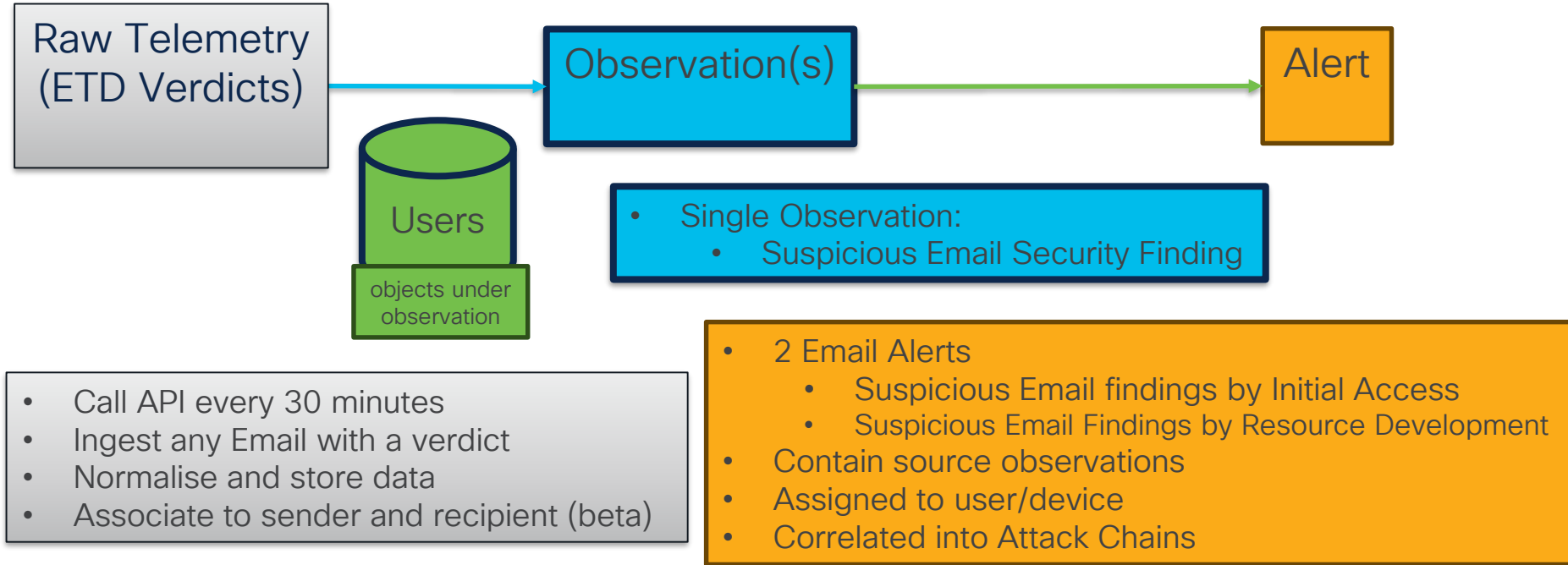
# Endpoint Data Analytics Pipeline (CSE, Crowdstrike, MS Defender)



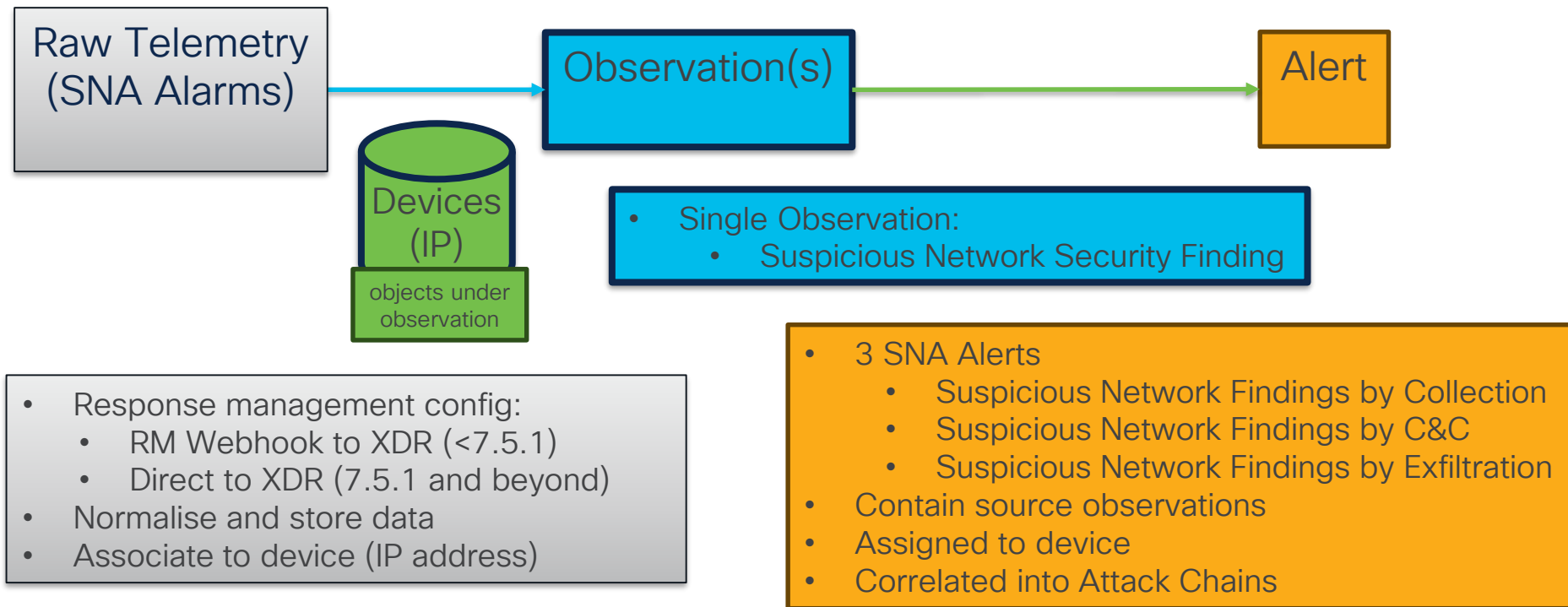
# ISE Data Analytics Pipeline



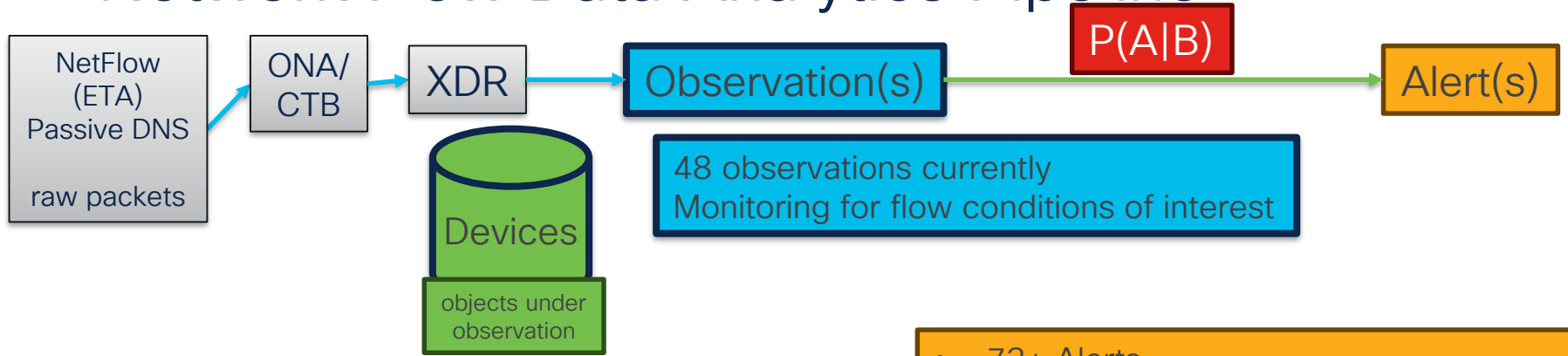
# ETD Data Analytics Pipeline



# SNA Data Analytics Pipeline (Coming soon)



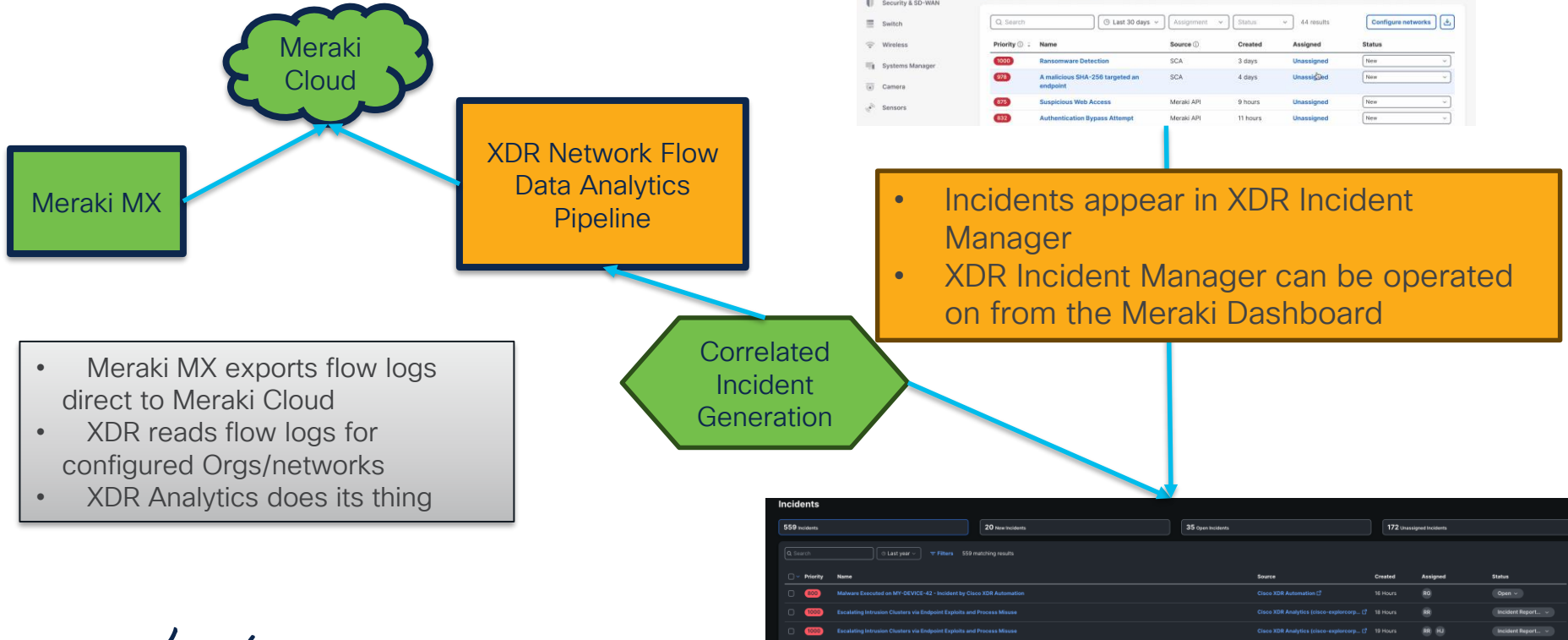
# Network Flow Data Analytics Pipeline



- NetFlow (incl. ETA), Passive DNS, Raw packets sent to:
  - Observable Network Appliance (ONA)
  - Cisco Telemetry Broker (CTB)
- Metadata extracted and sent to XDR
- Flow logs visible in Event Viewer
- Identify devices by IP Address, Hostname

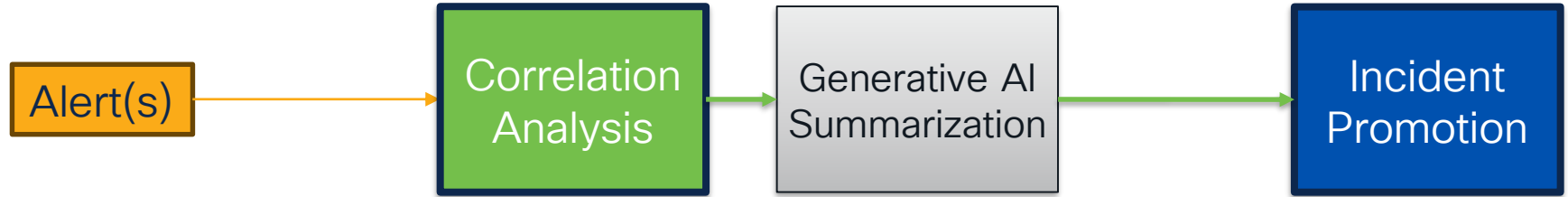
- 73+ Alerts
- Some alerts are composed of single observation(s)
- Some alerts are composed of multiple observation(s)
- Contain source observations
- Assigned to device
- Correlated into Attack Chains

# Coming Soon: Meraki MX!





# Correlation Analysis: Attack Chains



At least two alerts are required to correlate into an attack chain

- Correlation logic attempts to reconstruct the attack timeline
  - Related alerts
  - Common entities
- Priority of potential incident calculated
- Gen AI: meaningful title and description

All attack chains are promoted as Incidents

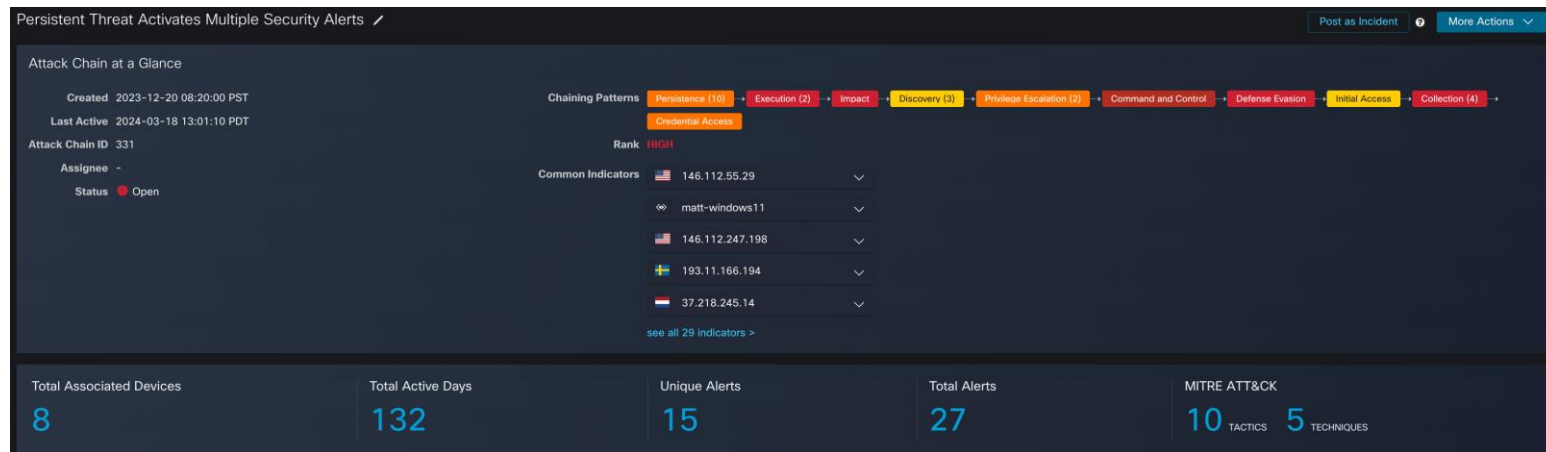
Reconnaissance

Impact

Attack Timeline

# Correlation Analysis (Attack Chains)

Reconstructing the attack timeline based on the Entities involved



Under experimentation: correlation involving on other observables in the alert

# AI Summarization

## Description

This incident spans from **2023-10-26 18:25:56 UTC** to **2024-03-27 16:25:00 UTC** involving a series of suspicious behaviors detected on the endpoint **desktop-h251r26**. The alerts fall into categories outlined by the MITRE tactics and CrowdStrike proprietary tactics. Five groups of alerts chronologically progressing from Execution to Defense Evasion, followed by CrowdStrike Proprietary Tactics, onto Credential Access, and culminating in Command and Control were present.

Initially, at **18:25:56 UTC on 2023-10-26**, the first alert group named **"Suspicious Endpoint Findings by Execution"** was reported with just a single alert. Concurrently with this, another single alert was documented in an alert group named **"Suspicious Endpoint Findings by Defense Evasion"**, indicating an immediate progression of suspicious activities on the same endpoint **desktop-h251r26**.

Continuing on, the next day at **16:53:28 UTC on 2023-10-27**, two more alerts were reported under the group **"Suspicious Endpoint Findings by CrowdStrike Proprietary Tactics"** from host **desktop-h251r26**. These incidences did not map to any standard MITRE tactic mappings, indicating the complexity of malicious activities on the desktop.

Following this, almost two months later, at **16:27:37 UTC on 2023-12-11**, another alert group named **"Suspicious Endpoint Findings by Credential Access"** emerged with 2 alerts. The alerts were mapped to the **Credential Access** MITRE tactic, suggesting an escalation in terms of unauthorized attempt to access sensitive data.

Finally, on **2024-03-27 at 16:25:00 UTC**, a significant shift was noticed with the report of a single alert under the group **"Suspicious Network Findings by Command and Control"**. This alert, unlike the previous ones detected on the endpoint, was detected on the network involving **desktop-h251r26**, indicating the potential presence of a network-based threat attempting to command and control device operations. The entire chain of events suggests that the security incident at **desktop-h251r26** progressed from initial suspicious endpoint behaviors to a network-based threat, which could have potentially compromised system and network integrity.

This description was generated by Cisco AI.

Close

AI generated description of the correlated incident

# Incident Scoring and Prioritisation

Incidents prioritized by business impact and asset value

742

92

Detection  
Risk

8

Asset  
Value at Risk

$$\text{Priority Score} = \text{Detection Risk} \times \text{Asset Value}$$

0-1000                      0-100                      0-10

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

Q Search

9 matching results

Filters

☐

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 Device  
Insights will appear here

The screenshot displays the Cisco XDR Control Center interface. The left sidebar 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 shows the details for a device named 'VICTIM-WIN-4', which is an 'Unknown OS Windows 10'. A dropdown menu for 'Device Value' is open, showing options: No Value, 1 (Not Critical), 2, 3 (Less Critical), 4, 5, 6 (Somewhat Critical), and 7. The 'Security Products' section shows 'Cisco Secure Endpoint' as 'Not enabled' and 'Automatic Updates' as 'NA'. The 'Seen in Sources' section shows a source named 'CrowdStrike' with a 'Last Seen' timestamp of '2023-05-09T23:50:00.000Z'.

**VICTIM-WIN-4**  
Unknown OS Windows 10  
Managed: No + Add Labels  
Device Value: 10 ^

**Details**

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:...
Hardware Id	
Serial Number	0000-0001-9124-5765-2762-5837-93

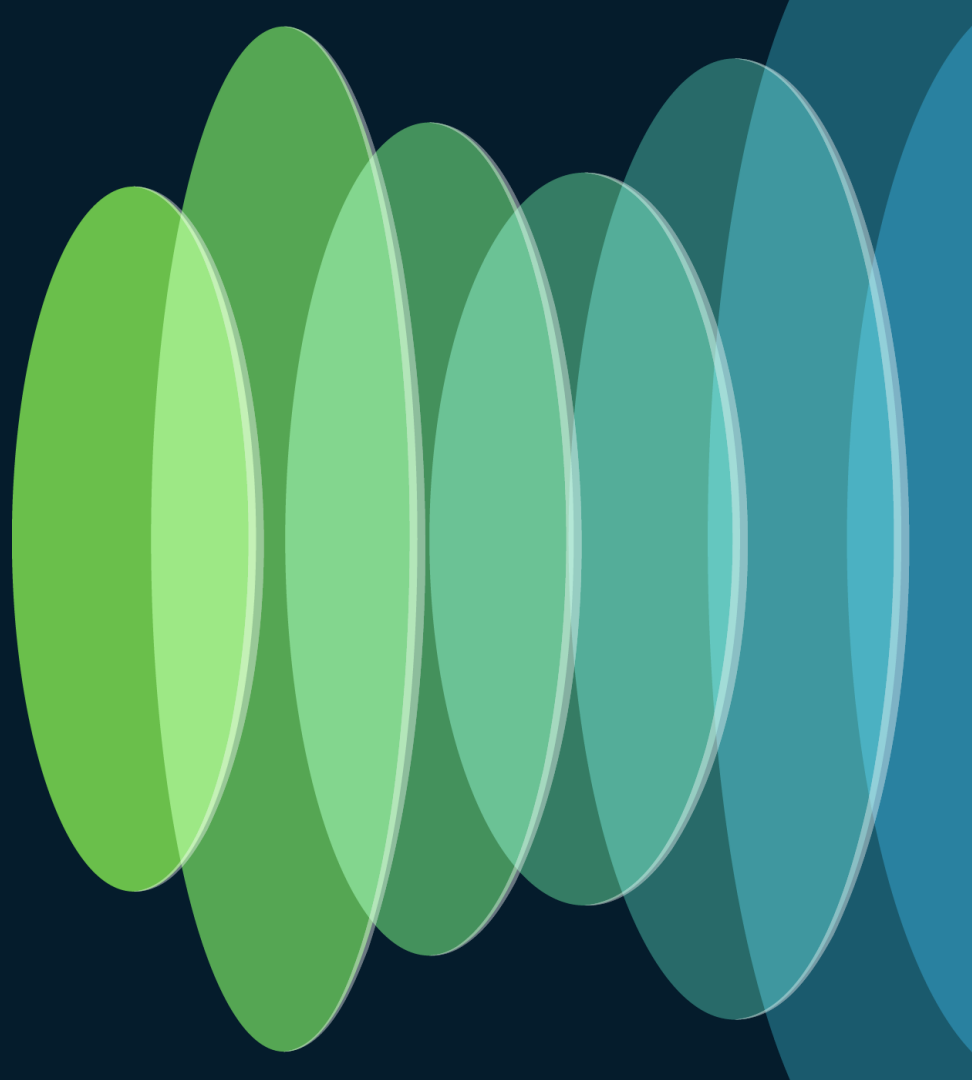
**Seen in Sources**

Source	Last Seen
CrowdStrike	2023-05-09T23:50:00.000Z

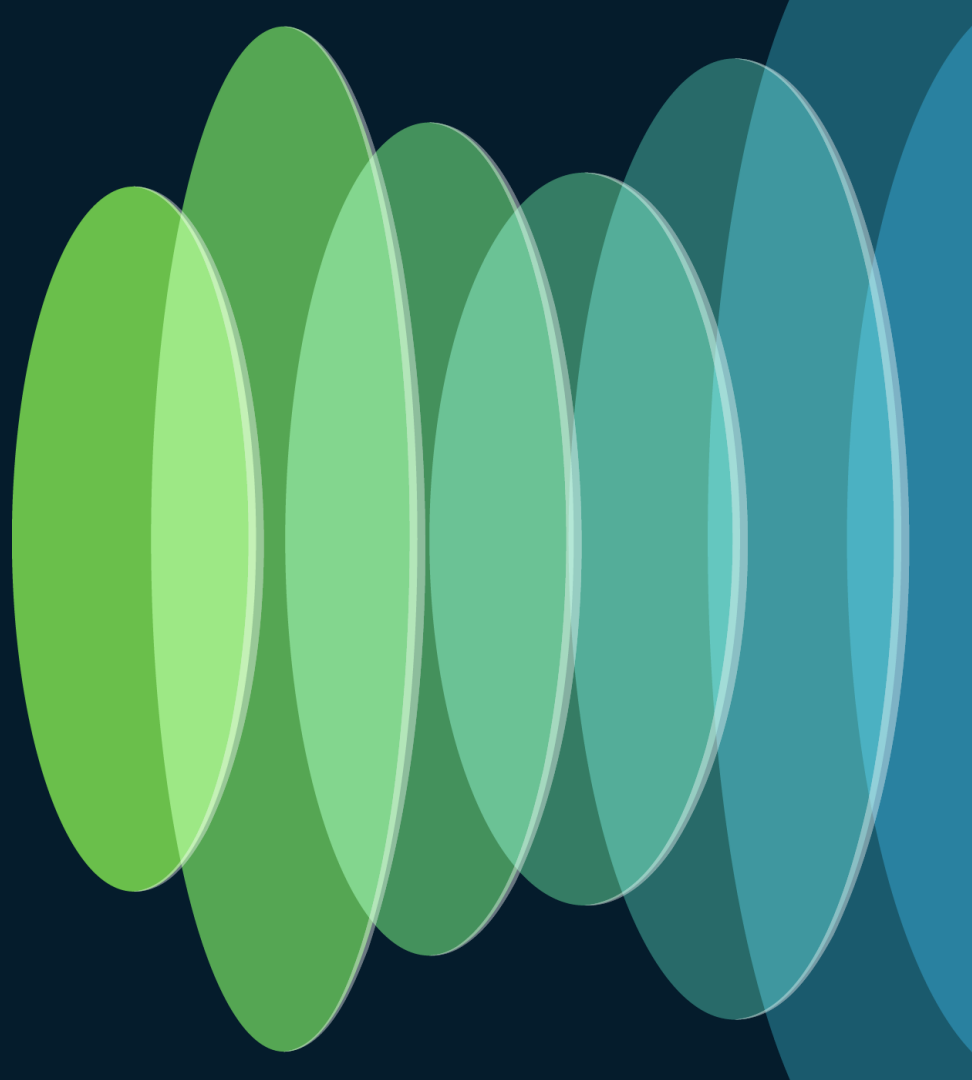
**Security Products**

Product	Status
Firewall	NA
Disk Encryption	NA
Cisco Secure Endpoint	Not enabled
Automatic Updates	NA

# Demo



# Summary



# Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

---



**Earn 100 points** per survey completed and compete on the Cisco Live Challenge leaderboard.

---



Level up and earn **exclusive prizes!**

---



Complete your surveys in the **Cisco Live mobile app**.



# Continue your education

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

# Related Sessions

## XDR Learning Map:

<https://www.ciscolive.com/global/learn/learning-maps/security/breach-protection.html>

Session ID	Title	When
BRKSEC-2113	Cisco XDR – Making sense of the Solution and how it's a Security Productivity Tool	Thursday 1:00 PM
BRKSEC-3019	Visibility, Detection and Response with Cisco Secure Network Analytics	Monday 3:00 PM
BRKSEC-2227	Evaluating and Improving Defenses with MITRE ATT&CK	Thursday 1:00 PM

# Parting Thoughts

Simplify your security operations with Cisco XDR!

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

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





The bridge to possible

# Thank you

CISCO *Live!*

#CiscoLive