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

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2178

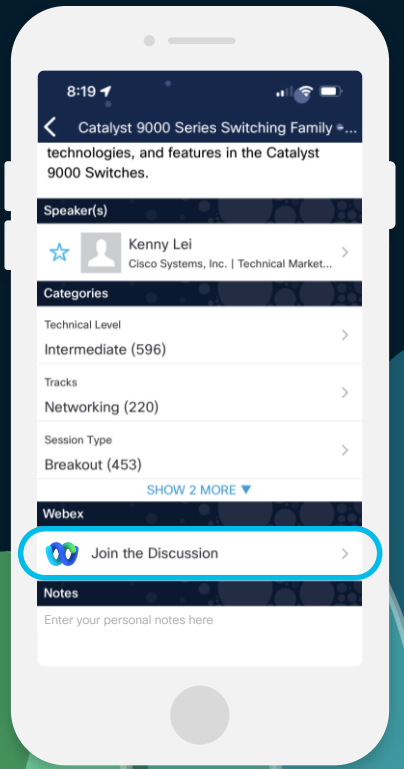
Questions?

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:

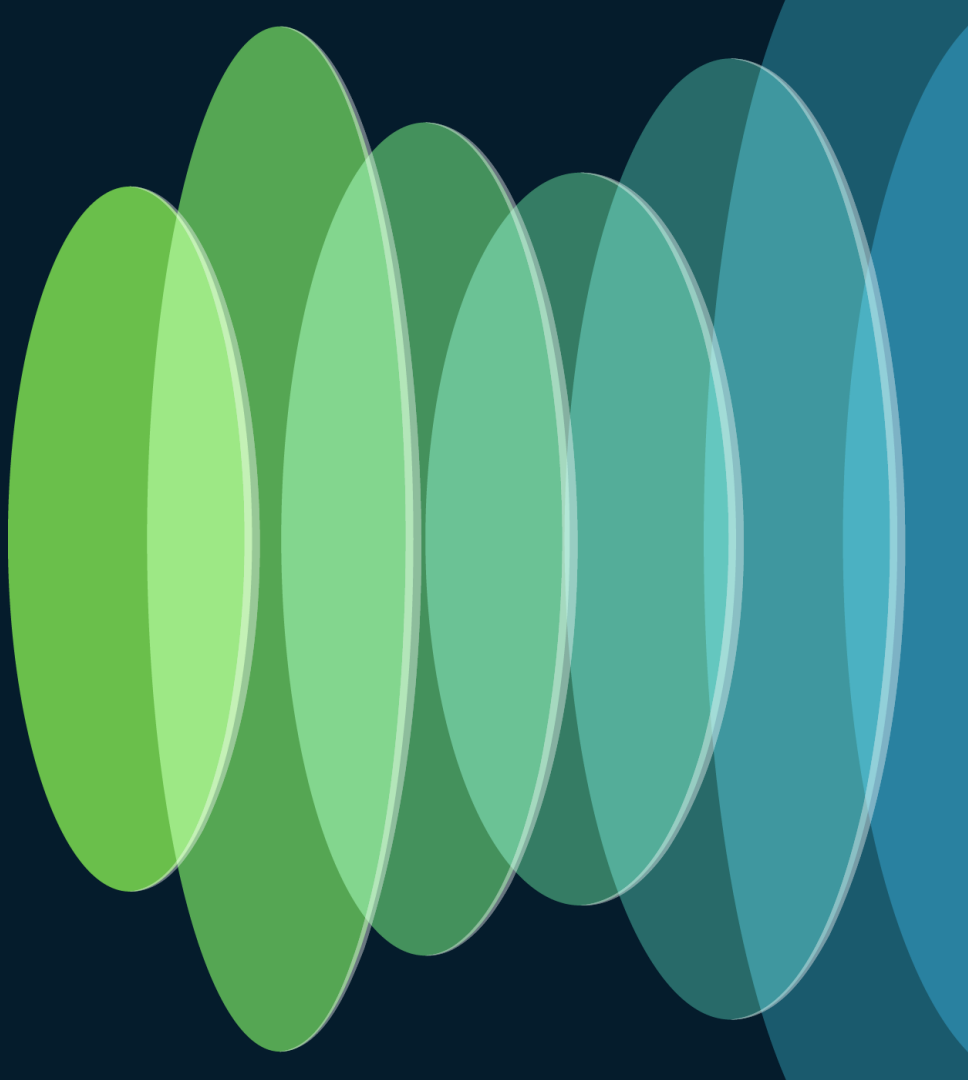
- Intro to Cisco XDR
- Data, Analytics and Detection
- Correlated Incident Generation
- Summary

About Me

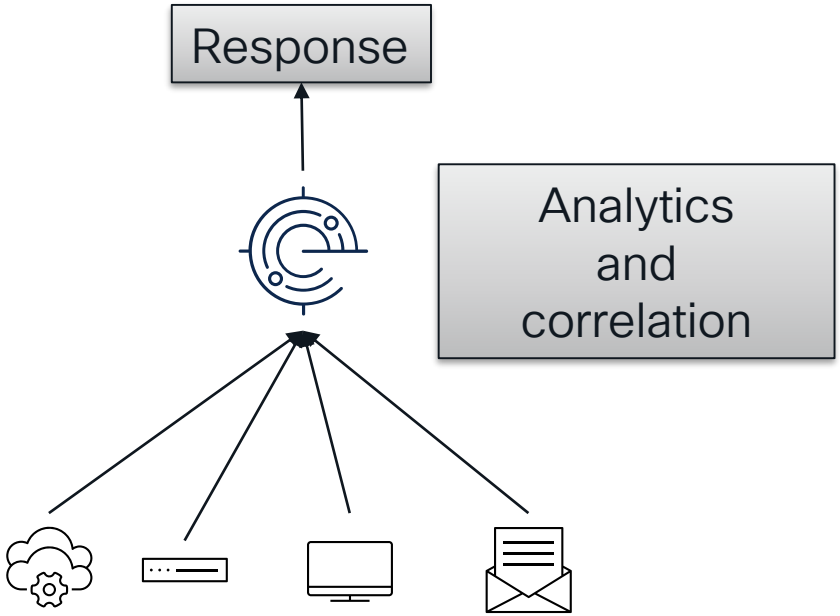
Matt Robertson

- 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



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

Accelerate that OODA Loop!

BRKSEC-2113 – Cisco SecureX XDR: Making sense of the solution and how it's a Security Productivity Tool - Aaron Woland, Friday Dec 8 @ 1:30 pm

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

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

Threat Hunting and Investigation

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

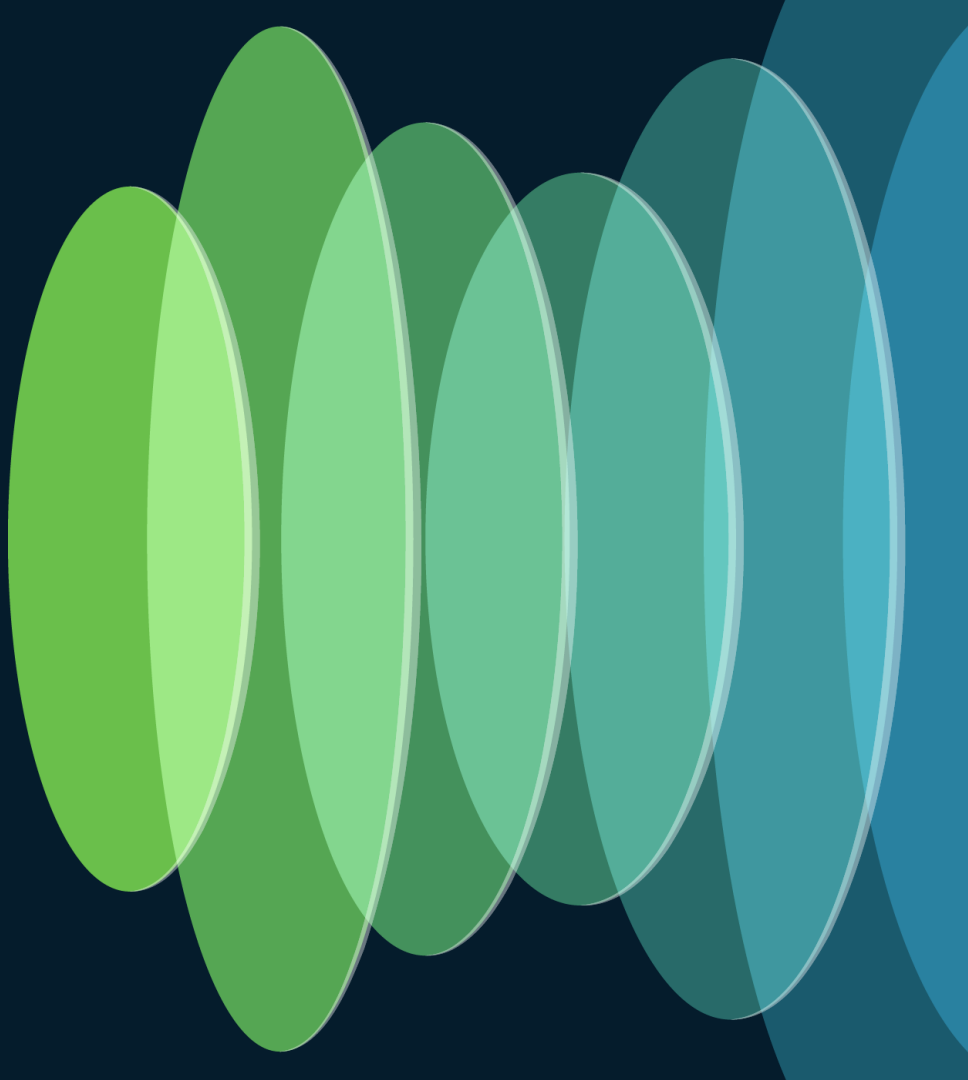
3rd Party
- CrowdStrike
- Ivanti Neurons
- Jamf Pro
- Microsoft Azure AD (Users)
- Microsoft Defender for Endpoint
- Microsoft Intune
- SentinelOne
- VMWare Workspace ONE UEM
- ServiceNow SecOps

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

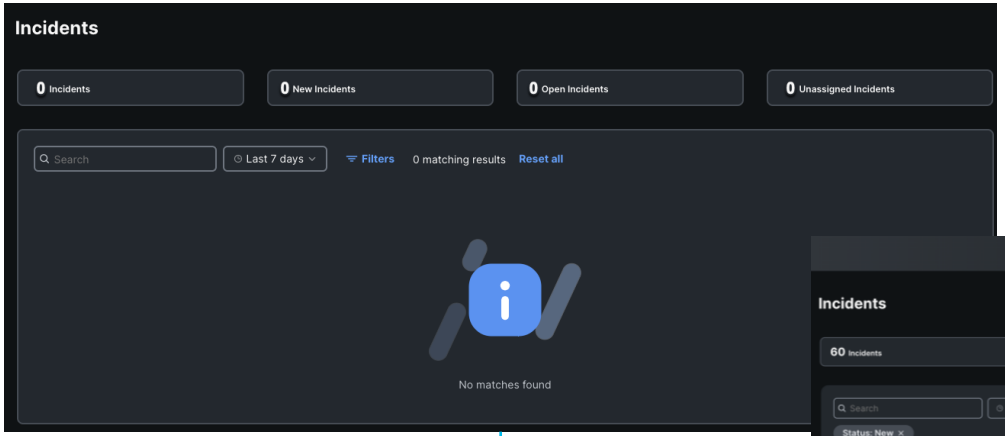
3rd Party
- Amazon Web Services
- CrowdStrike
- Cybereason
- ExtraHop
- Fortinet Fortigate
- Google Cloud Platform
- Jamf Pro
- Microsoft Azure
- Microsoft Azure AD
- Microsoft Defender for Endpoint
- Palo Alto Cortex
- Palo Alto Panorama
- SentinelOne
- Trend Micro Vision One

Data, Analytics and Detection

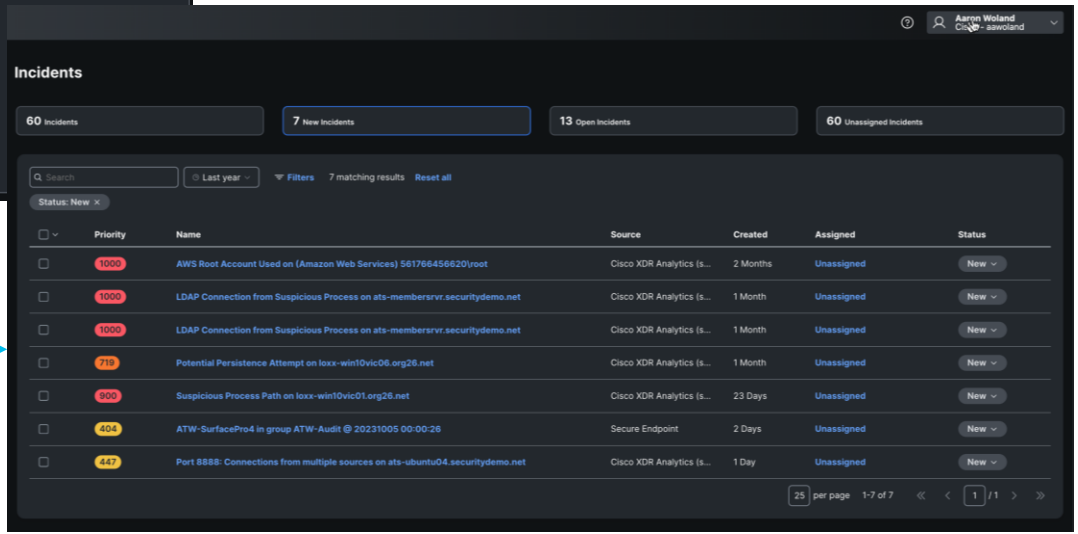


XDR Outcome:

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

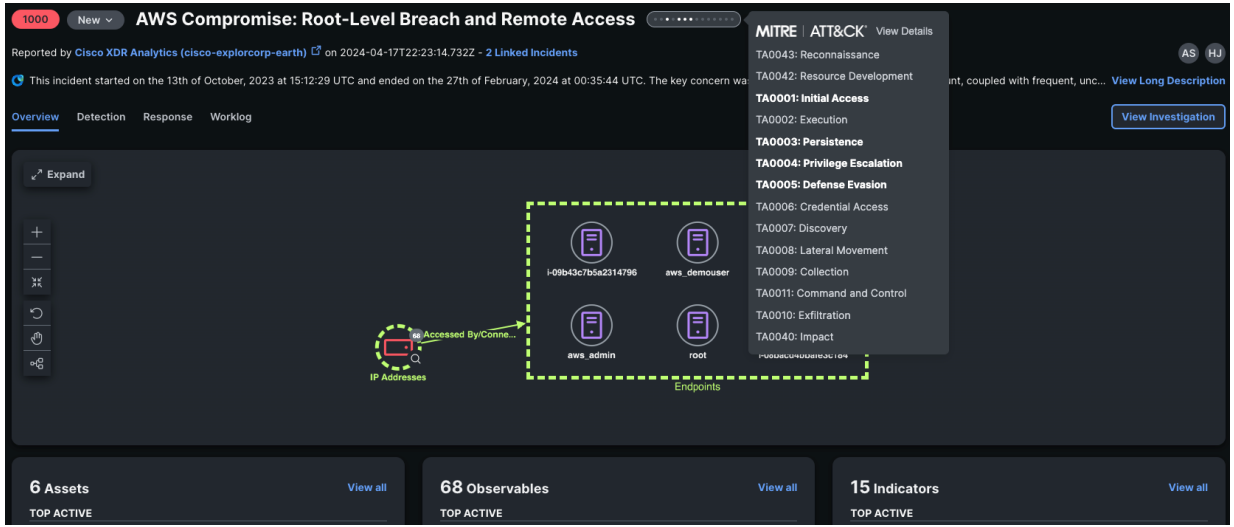


How do we get incidents?

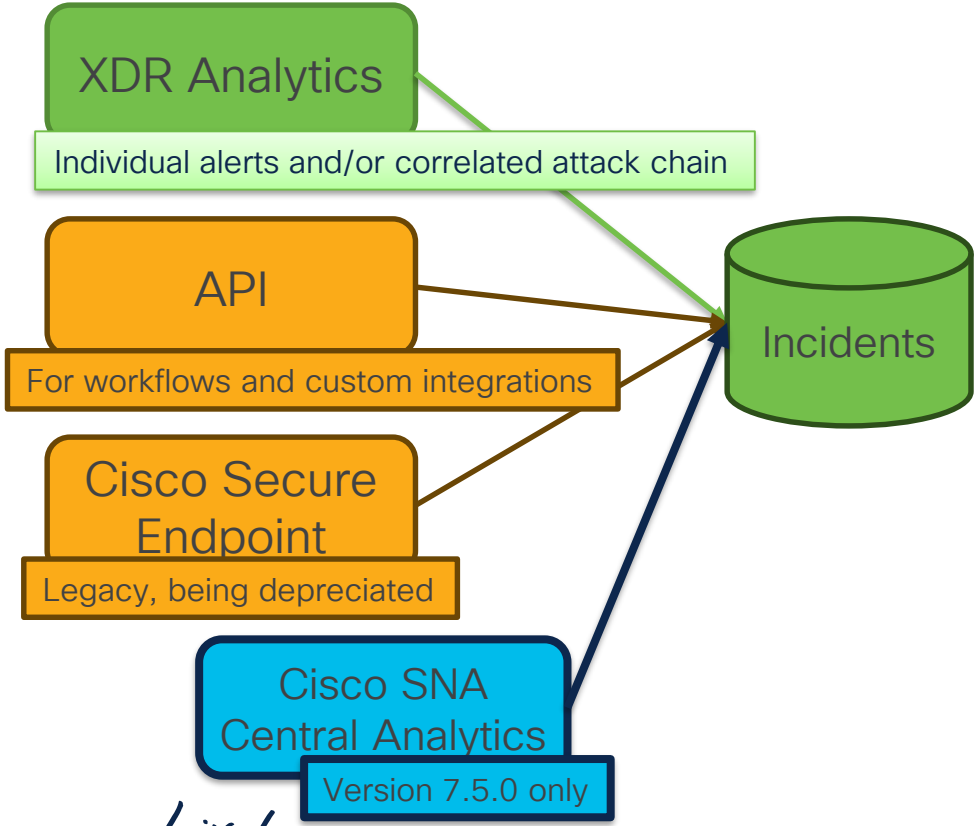


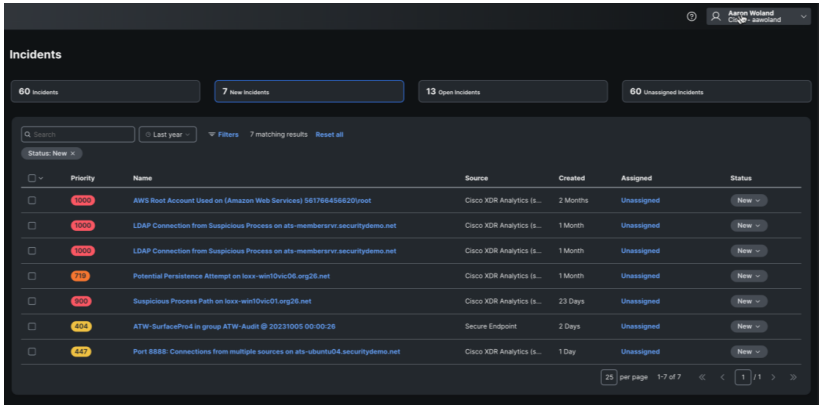
What is an XDR Incident?

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



Where do incidents come from? (current status)





Important Distinction in Terms

Correlation

Pre-Incident Creation

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

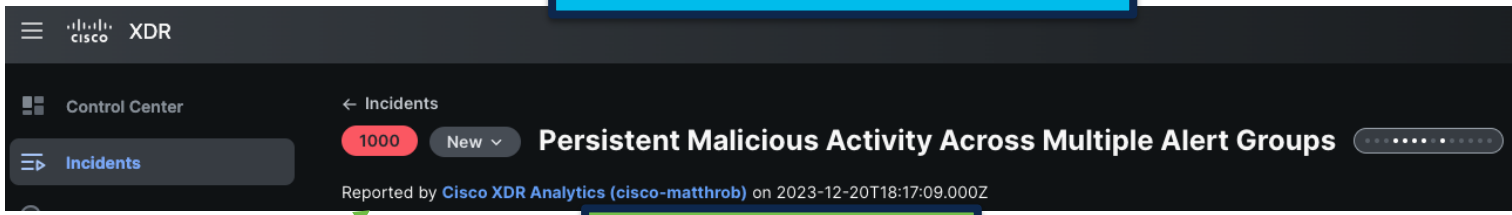
Enrichment

Post-Incident Creation

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

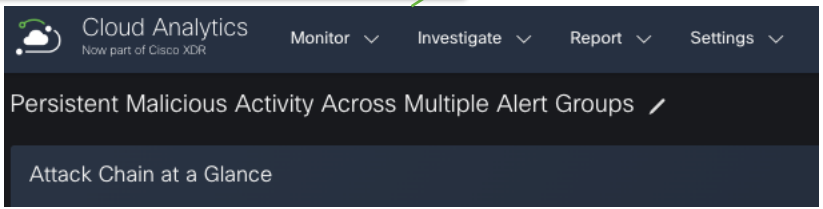
Aside: A note about UI's

Main XDR User Interface



SOC dashboard

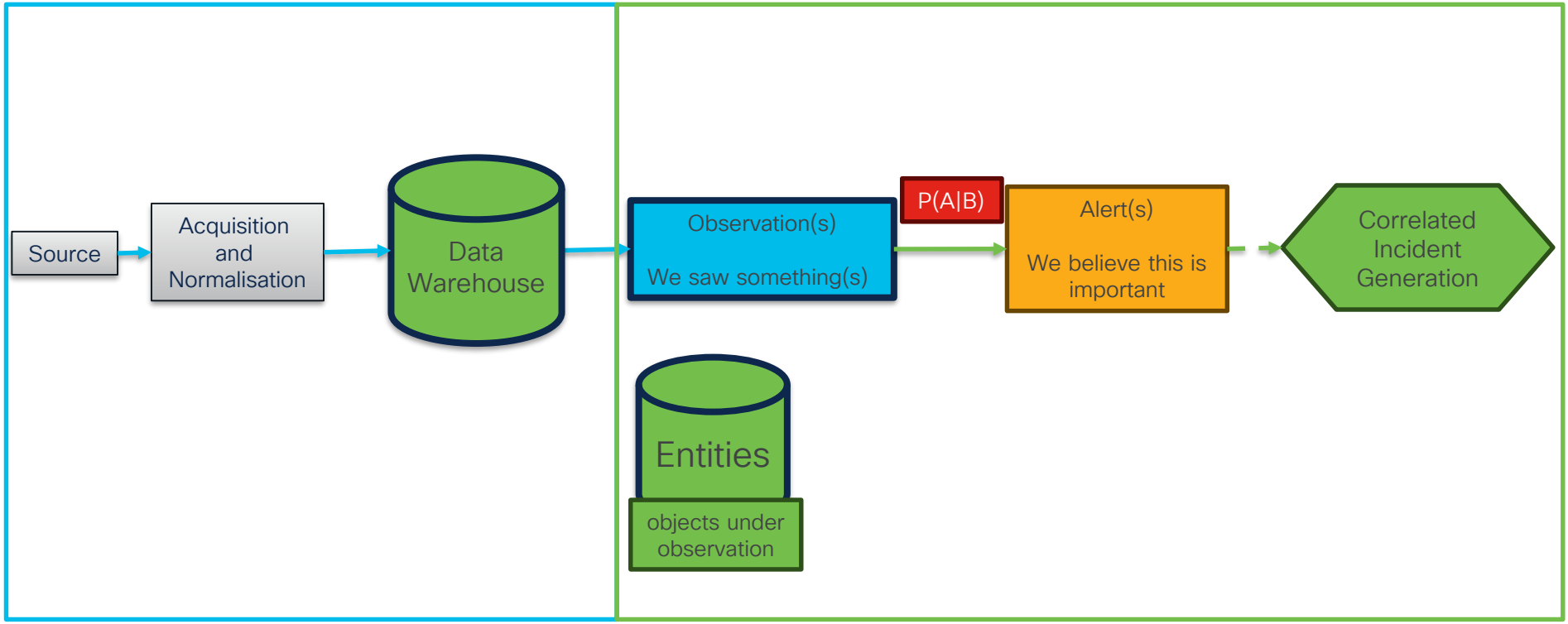
Attack Chains, Alerts exported into Incident Manager



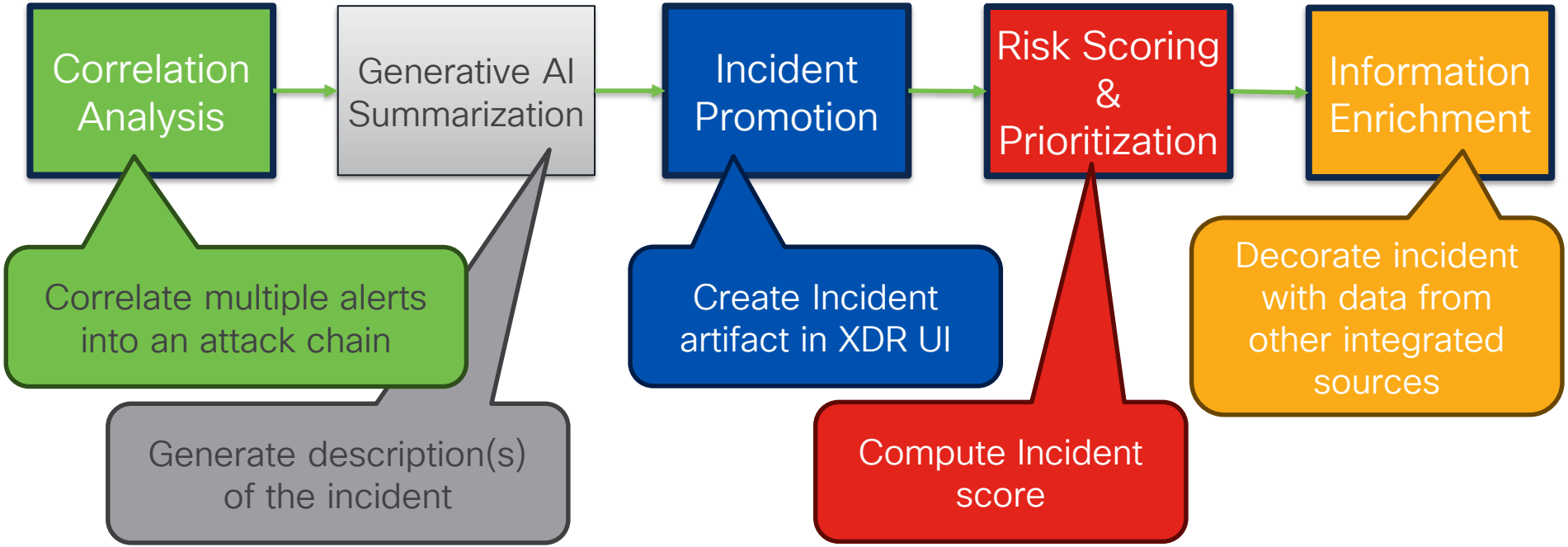
Secure Cloud Analytics, also known as XDR Analytics

"Detection Engineering" dashboard. Admin for analytics stack.

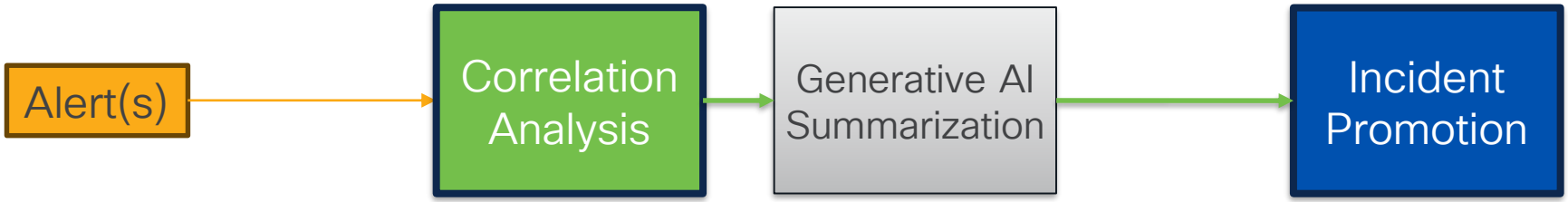
Data Analytics Pipeline



Correlated Incident Generation



Correlation Analysis: Attack Chains



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

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

High priority events promoted as Incidents

Native Detection vs Extended Detection

Native

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

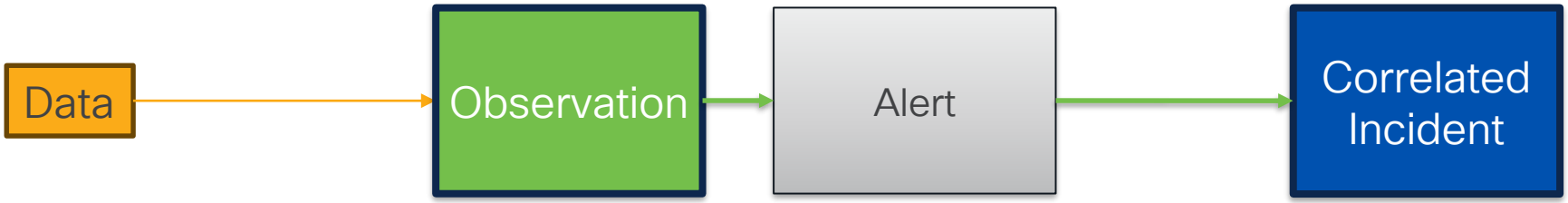
Extended

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

High Fidelity, Low Noise

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

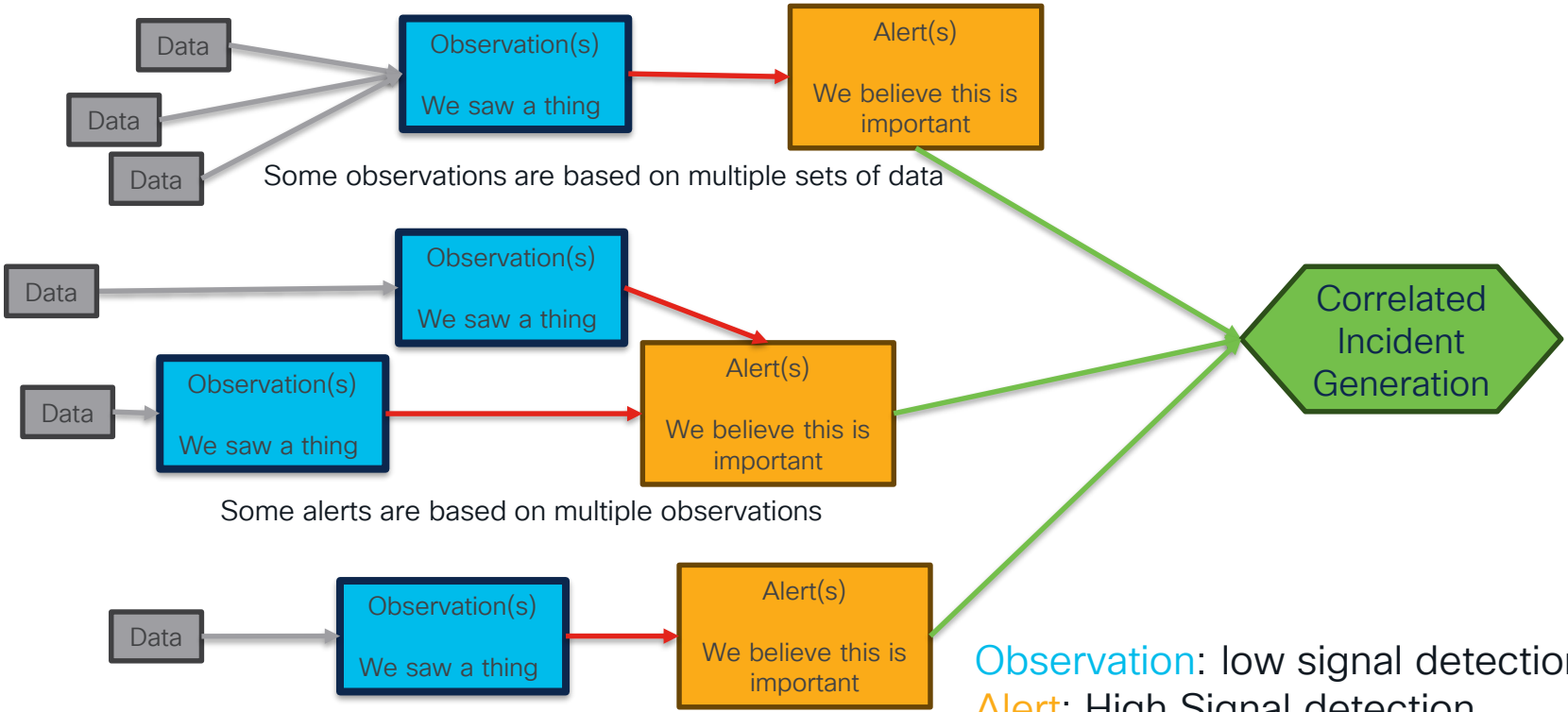
Creating Security Value from Data



P(A|B)

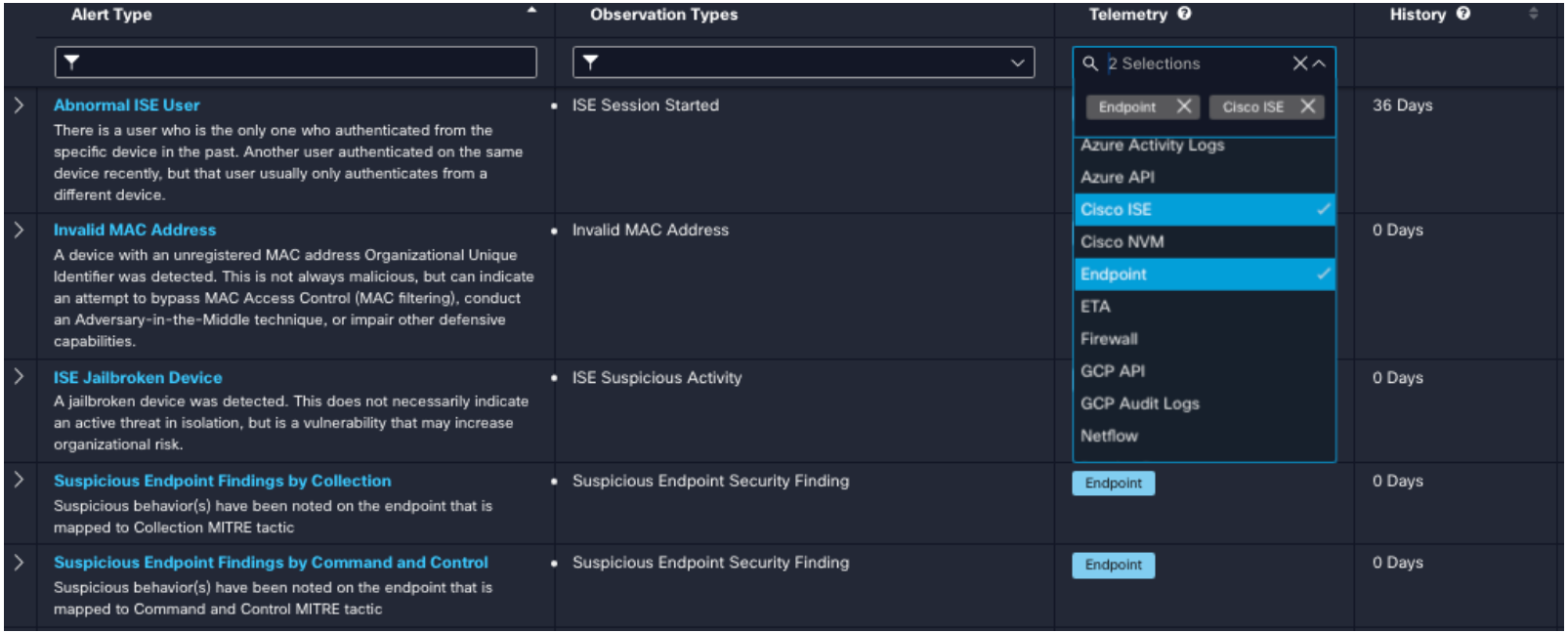
There is an AI/ML model behind observation to alert

Detection and Correlation



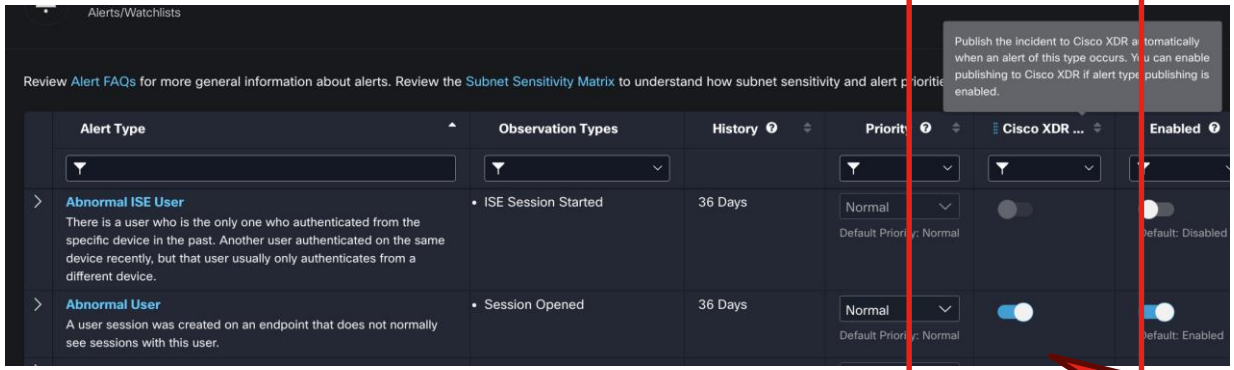
Observation: low signal detection
Alert: High Signal detection
Correlated Incident: Higher signal detection

Alerts Require (Specific) Data



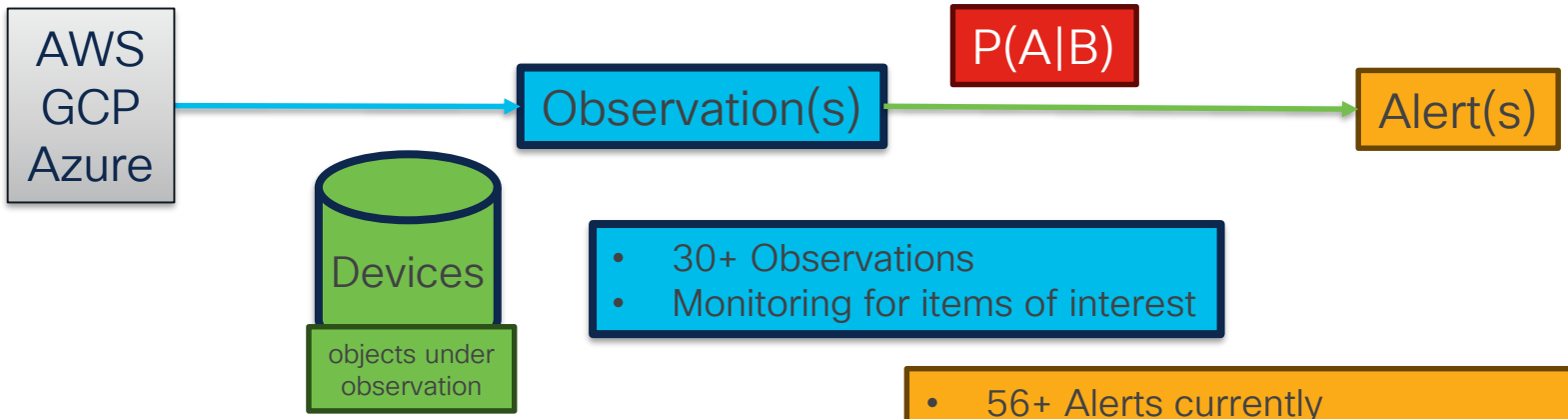
Familiarise yourself with the observations, data and history for specific alerts

Alerts can be configured to be published directly to XDR



Use discretion; Can result in duplicative incidents.

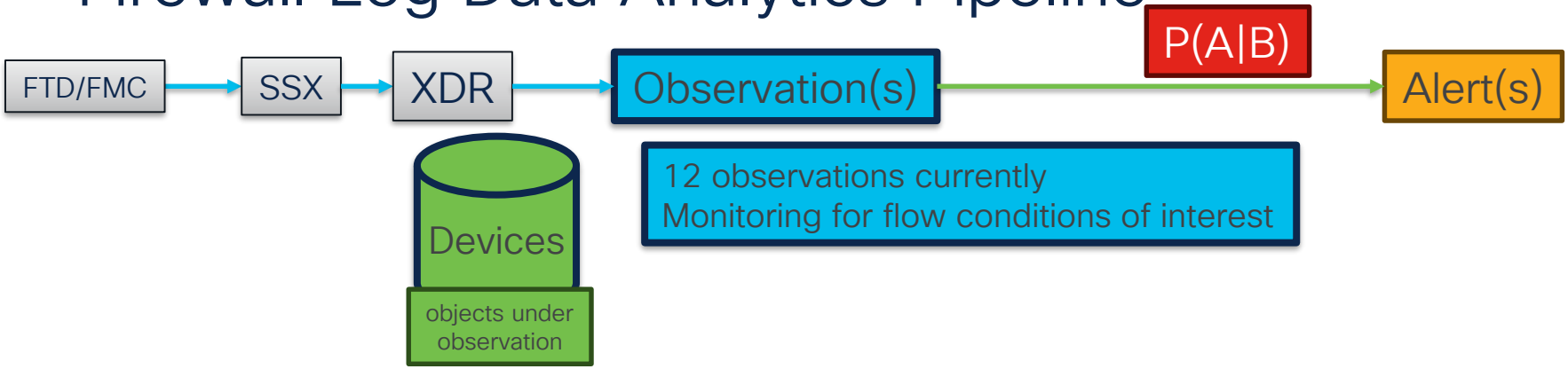
IAAS Data Analytics Pipeline



- 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

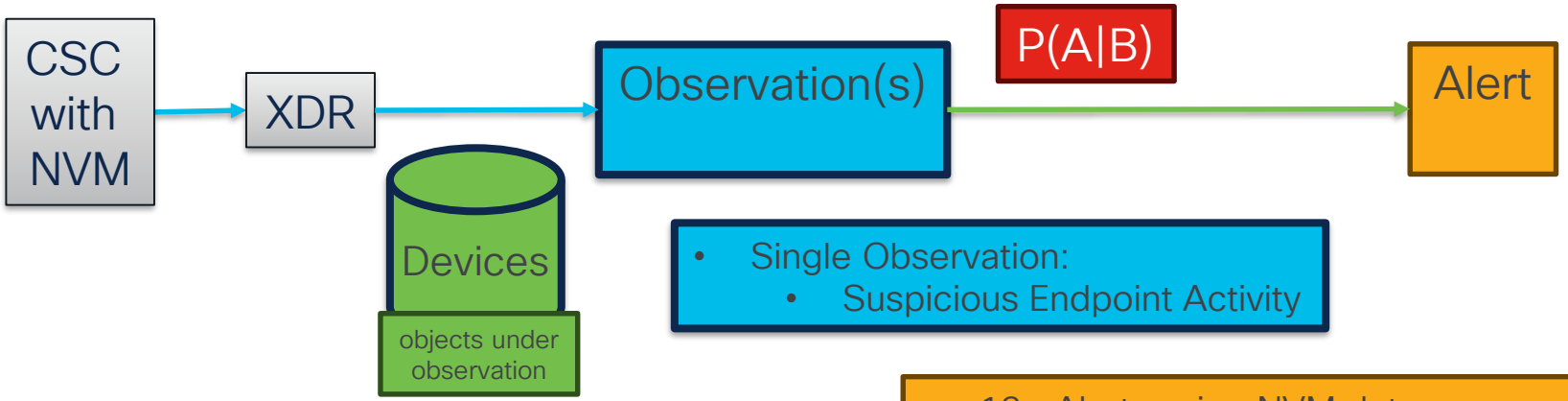
Firewall Log Data Analytics Pipeline



- 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

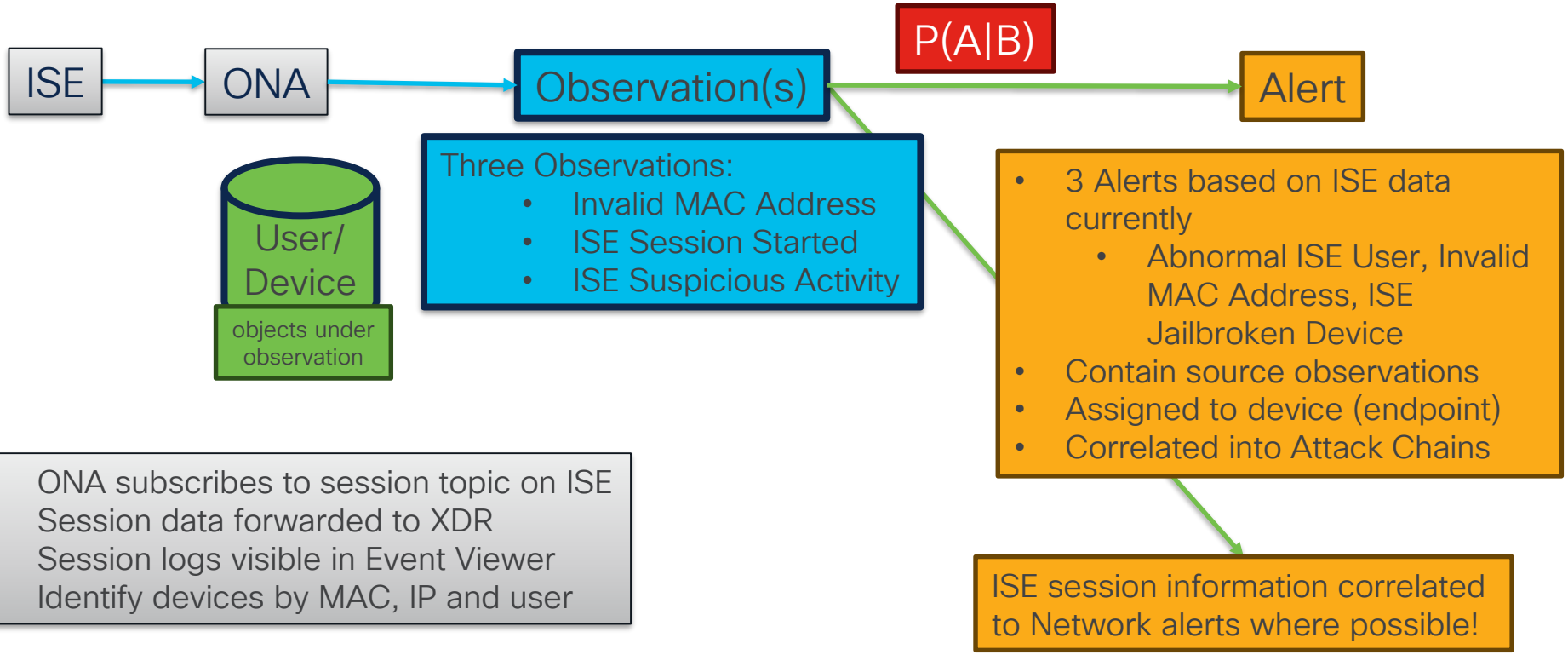
- 12+ Alerts using NVM data
  - Combination of network and endpoint data artifacts
- Contain source observations
- Assigned to device (endpoint)
- Correlated into Attack Chains

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

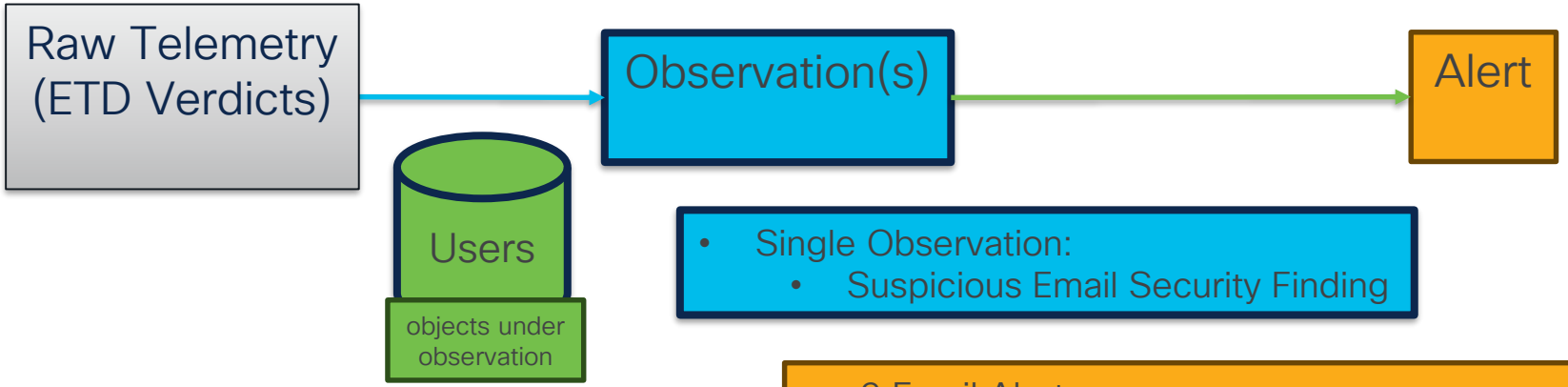
- Call API every 1-2 minutes
- Ingest Critical and High detections
  - CSE – today only BP engine events
- Normalise and store data
- Identify devices by agent ID

- 17 Endpoint Alerts
  - By MITRE ATT&CK Tactics
  - MITRE label comes from source data
- Contain source observations
- Assigned to device (endpoint)
- Correlated into Attack Chains

ISE Data Analytics Pipeline



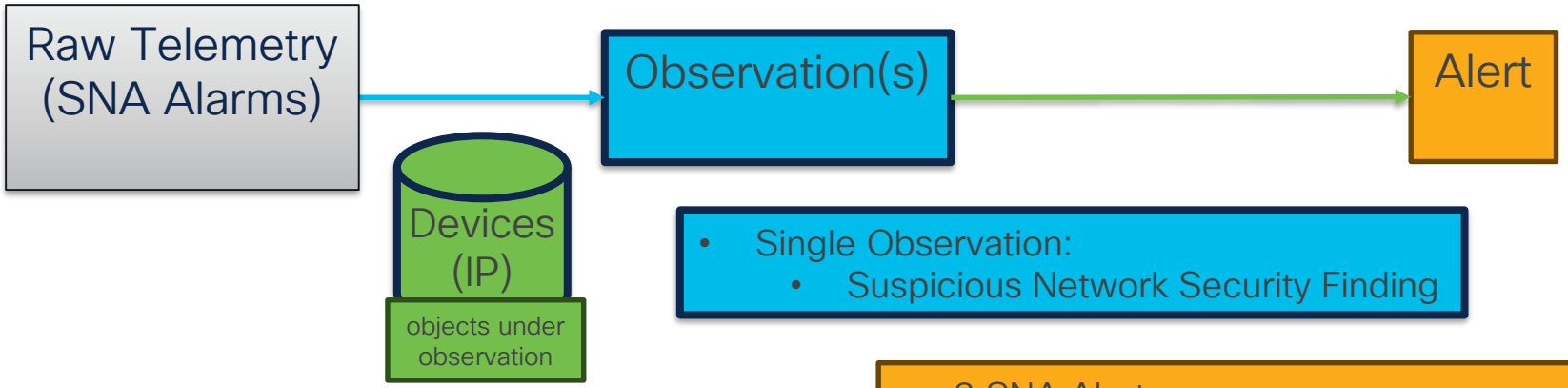
ETD Data Analytics Pipeline



- Call API every 30 minutes
- Ingest any Email with a verdict
- Normalise and store data
- Associate to sender and recipient (beta)

- 2 Email Alerts
  - Suspicious Email findings by Initial Access
  - Suspicious Email Findings by Resource Development
- Contain source observations
- Assigned to user/device
- Correlated into Attack Chains

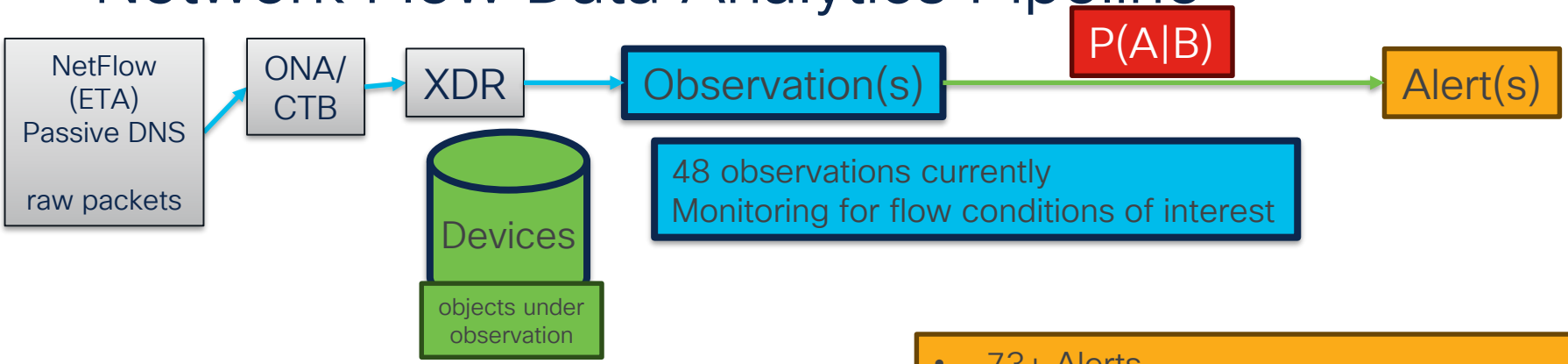
SNA Data Analytics Pipeline (Coming soon)



- Response management config:
  - RM Webhook to XDR (<7.5.1)
  - Direct to XDR (7.5.1 and beyond)
- Normalise and store data
- Associate to device (IP address)

- 3 SNA Alerts
  - Suspicious Network Findings by Collection
  - Suspicious Network Findings by C&C
  - Suspicious Network Findings by Exfiltration
- Contain source observations
- Assigned to device
- Correlated into Attack Chains

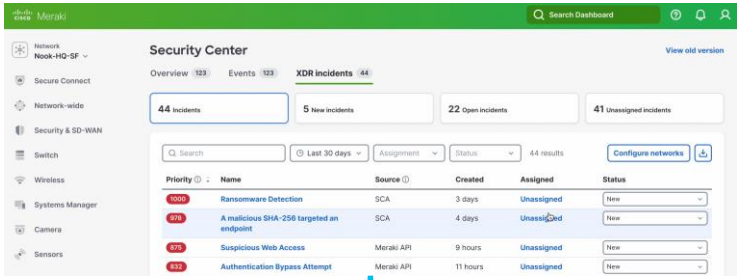
Network Flow Data Analytics Pipeline



- 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!



Meraki Cloud

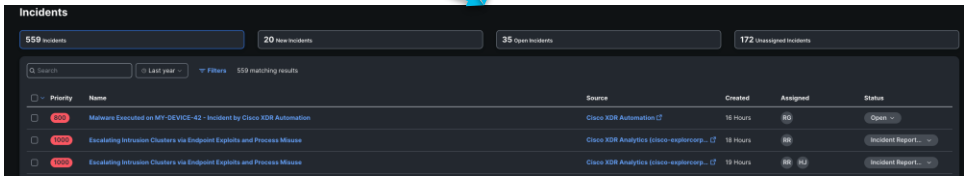
Meraki MX

XDR Network Flow Data Analytics Pipeline

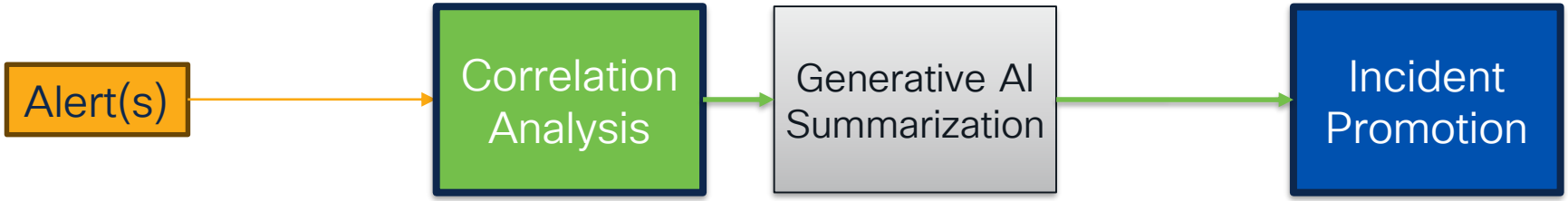
Correlated Incident Generation

- Incidents appear in XDR Incident Manager
- XDR Incident Manager can be operated on from the Meraki Dashboard

- Meraki MX exports flow logs direct to Meraki Cloud
- XDR reads flow logs for configured Orgs/networks
- XDR Analytics does its thing



Correlation Analysis: Attack Chains



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

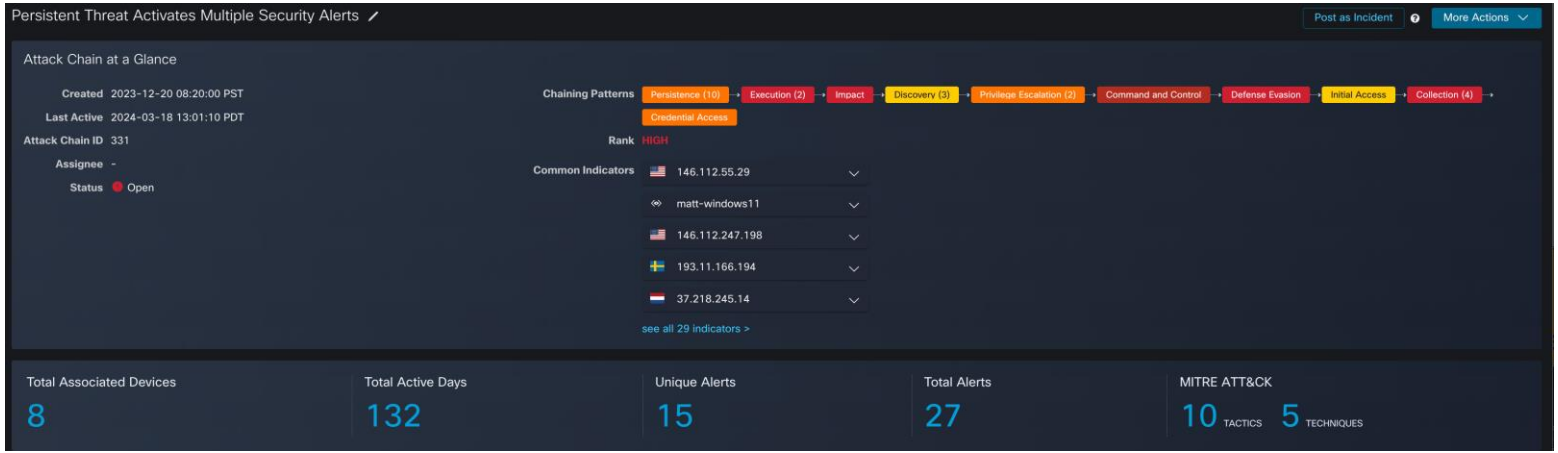
- Correlation logic attempts to reconstruct the attack timeline
  - Related alerts
  - Common entities
- Priority of potential incident calculated
- Gen AI: meaningful title and description

All attack chains are promoted as Incidents

Attack Timeline

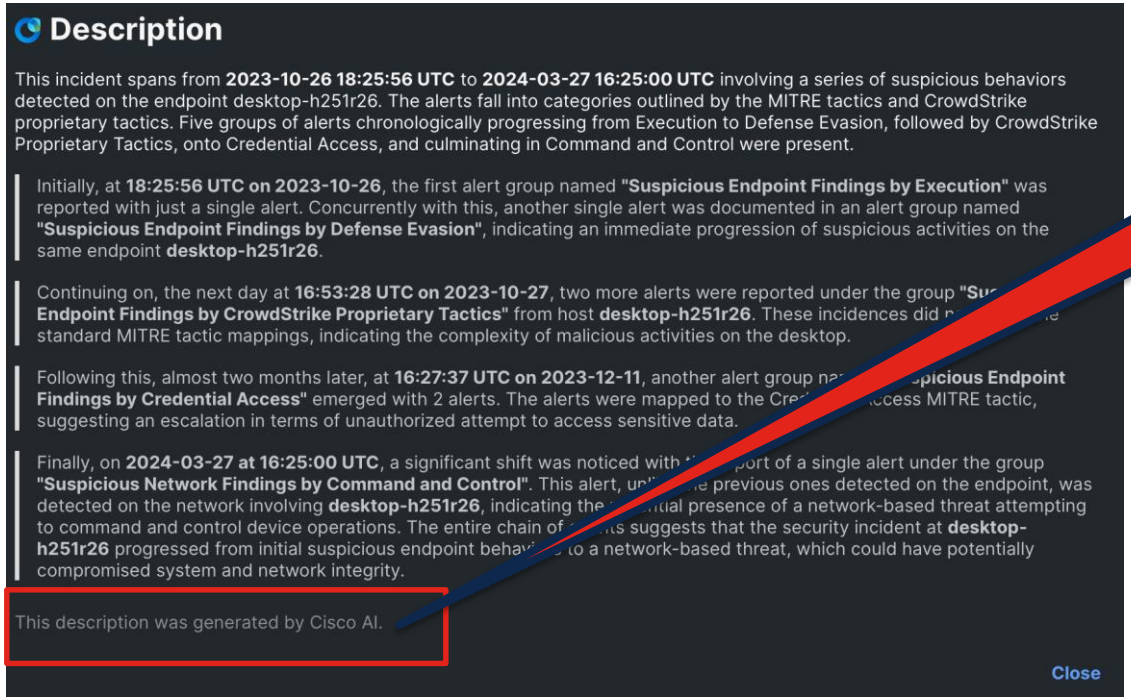
Correlation Analysis (Attack Chains)

Reconstructing the attack timeline based on the Entities involved



Under experimentation: correlation involving on other observables in the alert

AI Summarization



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

Priority Score = Detection Risk x Asset Value

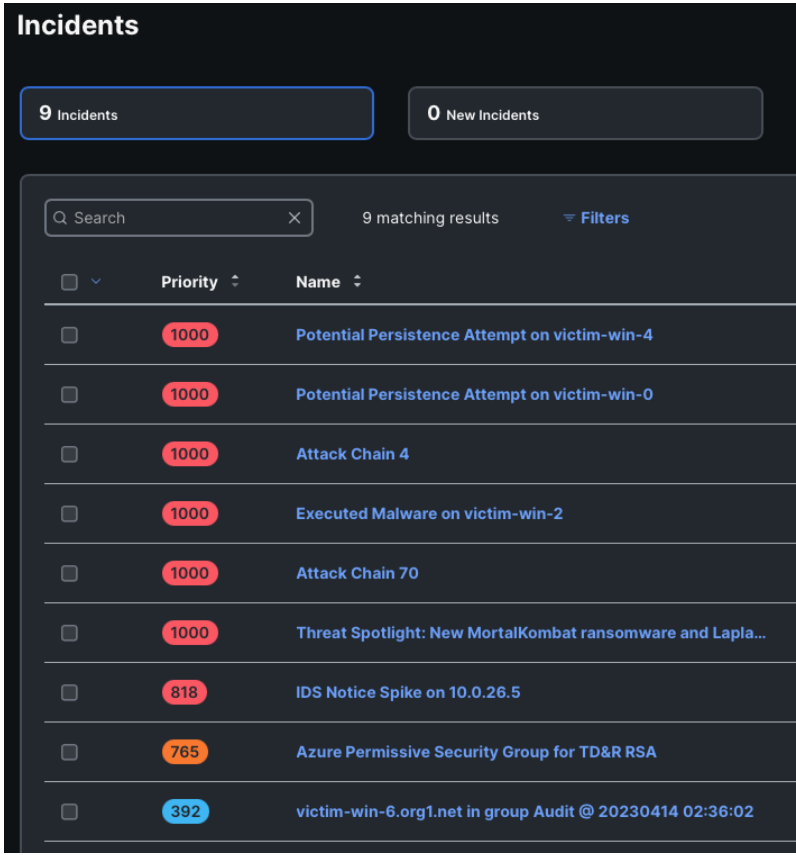
0-1000 0-100 0-10

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

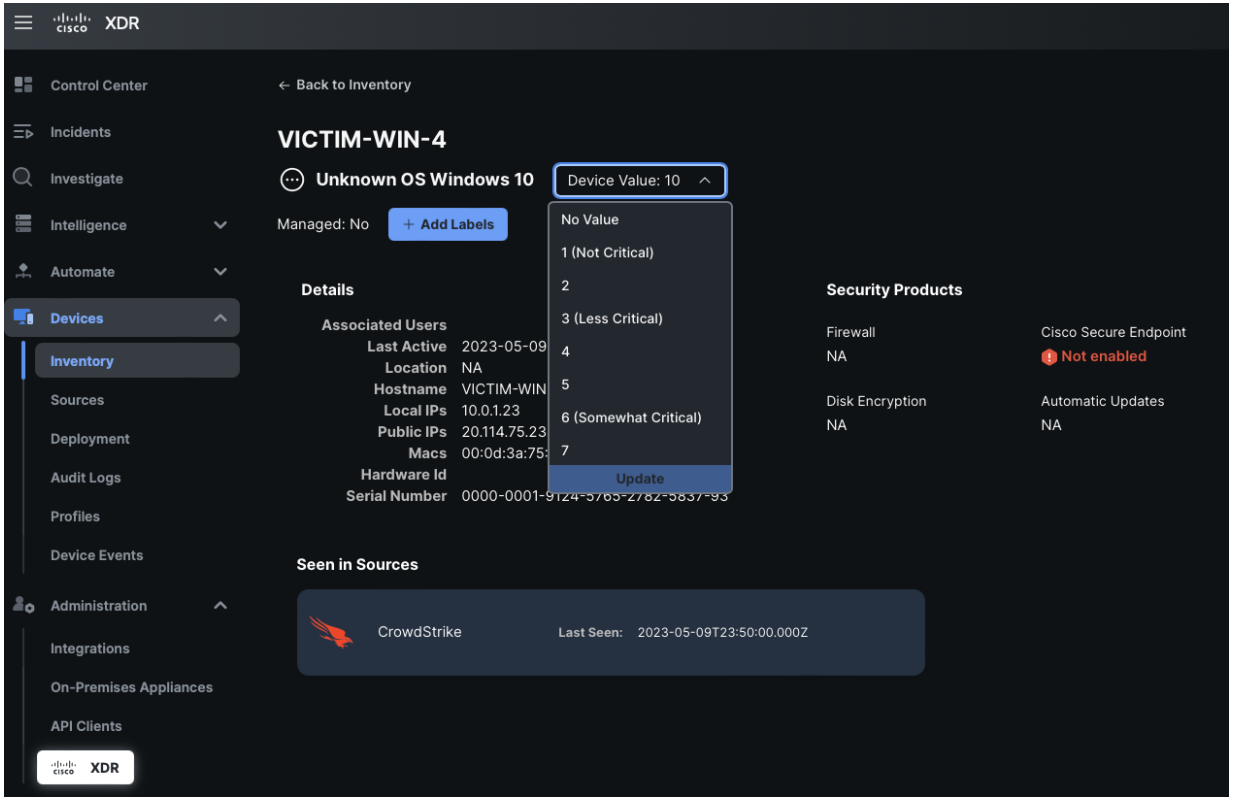
User Defined Asset Value represent the value of the asset involved in the incident



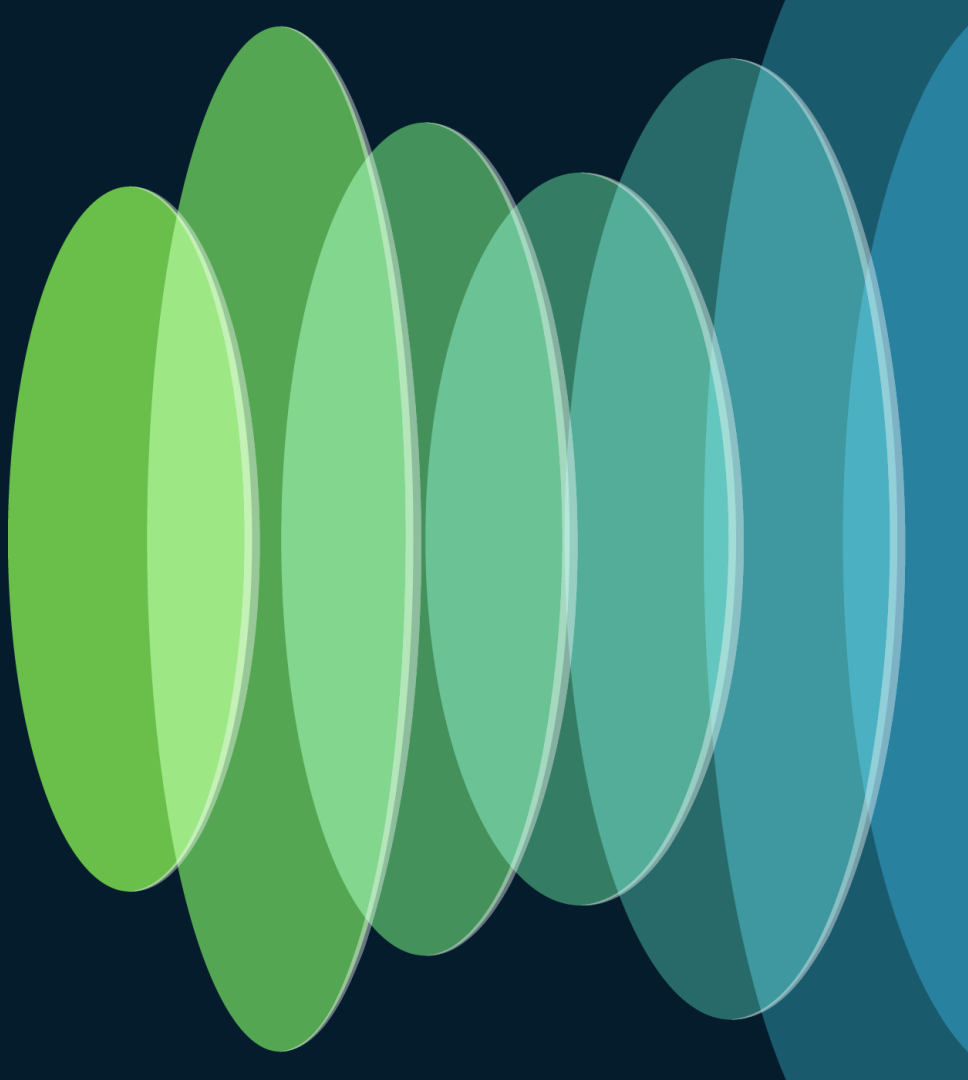
Aside: Asset Value Configuration

- Configured on device page
- Default is 10

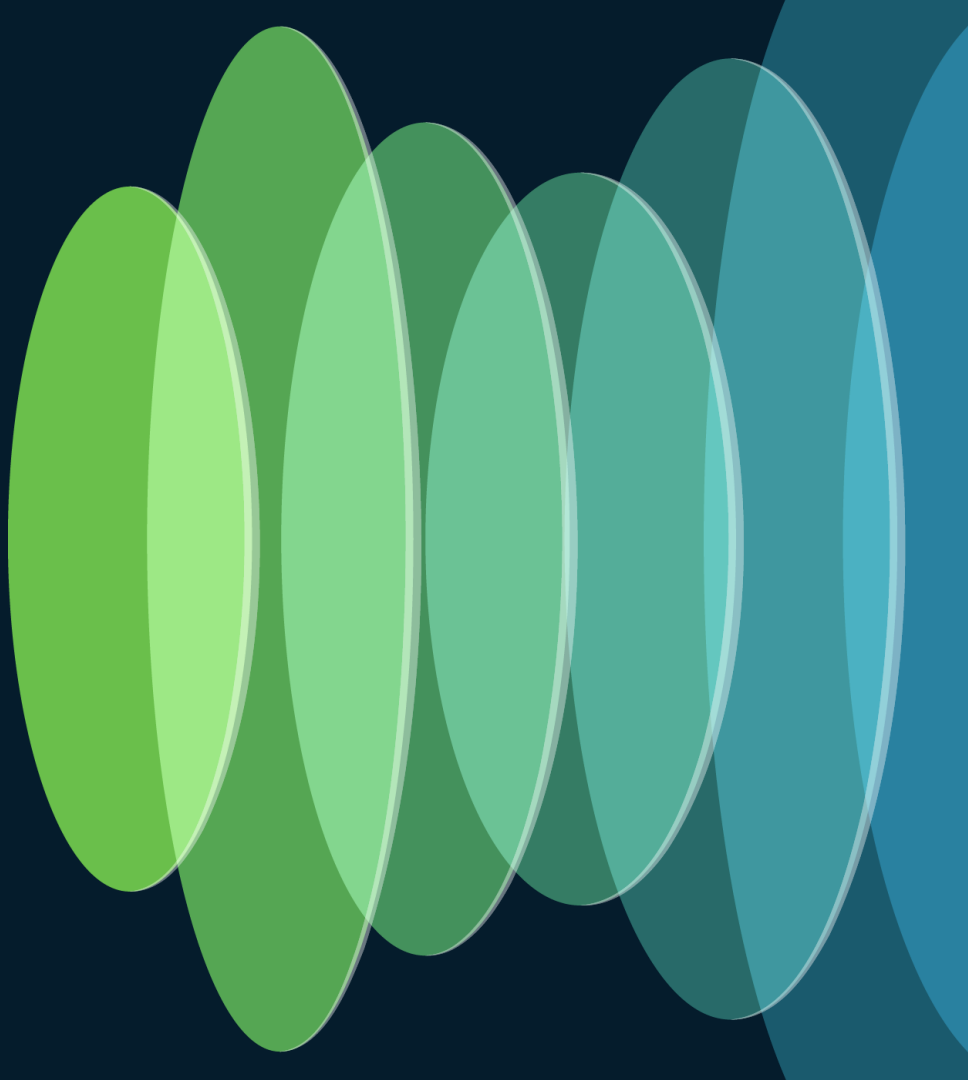
Note:
Only devices known to Device Insights will appear here



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

Related Sessions

XDR Learning Map:
https://www.ciscolive.com/global/learn/learning-maps/security/breach-protection.html

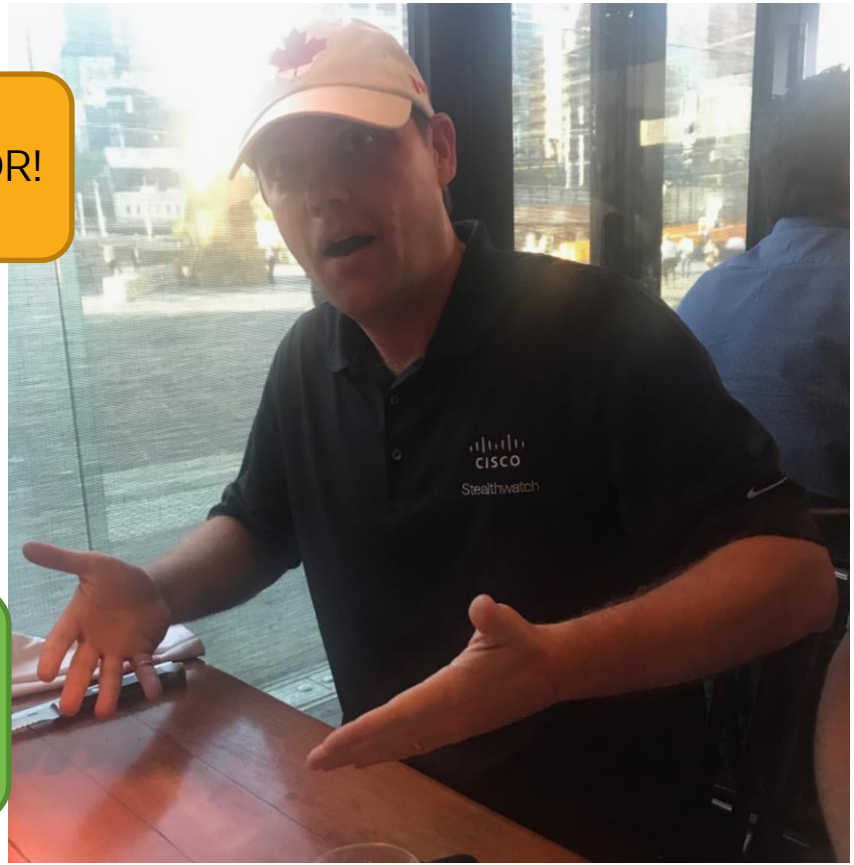
Session ID	Title	When
BRKSEC-2113	Cisco XDR – Making sense of the Solution and how it's a Security Productivity Tool	Thursday 1:00 PM
BRKSEC-3019	Visibility, Detection and Response with Cisco Secure Network Analytics	Monday 3:00 PM
BRKSEC-2227	Evaluating and Improving Defenses with MITRE ATT&CK	Thursday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

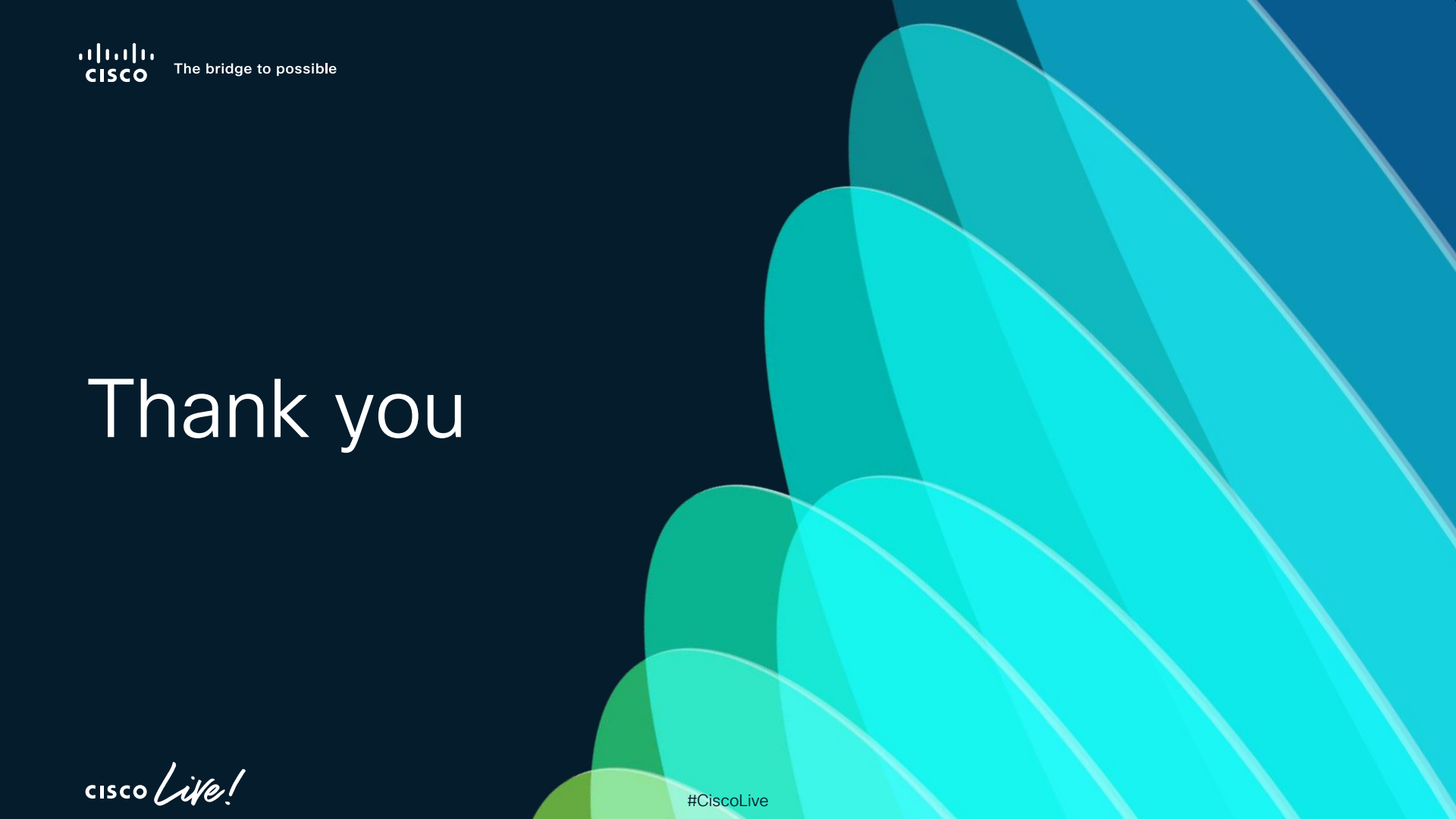
Parting Thoughts

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