

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Extended Detection with Cisco XDR

Data, Analytics and Attack Chains

Matt Robertson
Distinguished Engineer
BRKSEC-2178

CISCO *Live!*

#CiscoLiveAPJC

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 November 15, 2024.



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



Agenda

Objective:
Understand Cisco XDR Analytics

- Introduction to Cisco XDR
- Incident Generation Framework
- Native Detections
- Get SNOC'd
- 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



Public Service Announcement

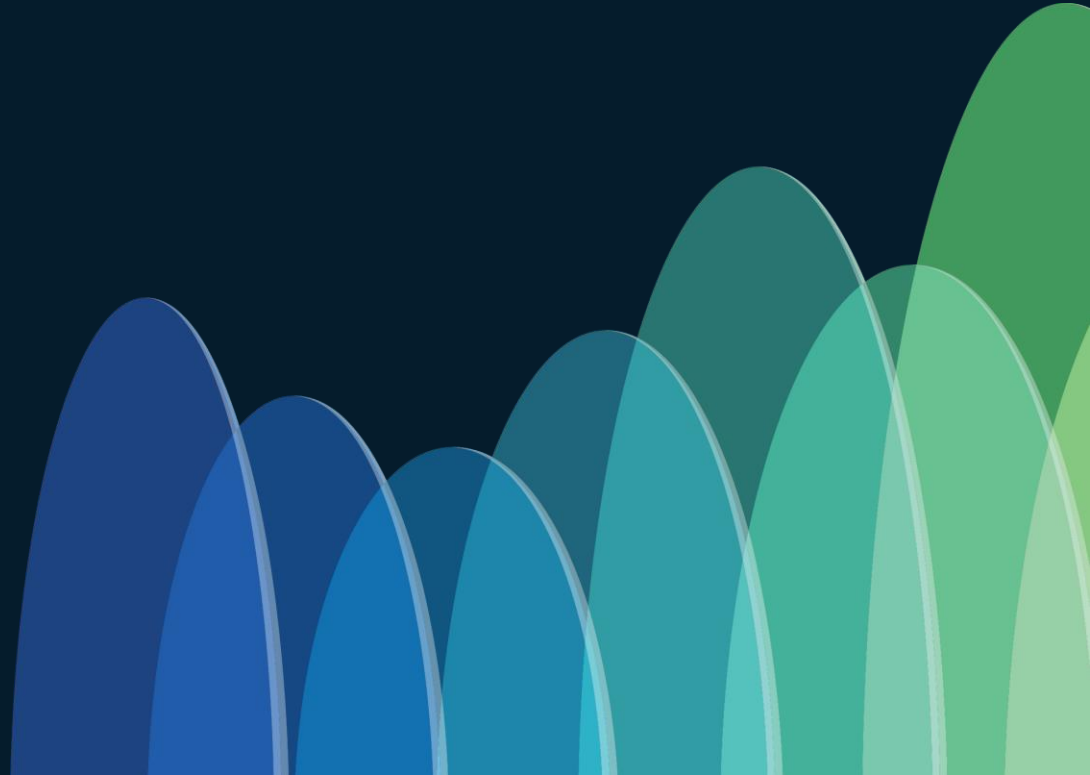


Darrin Miller:
Beer Thief

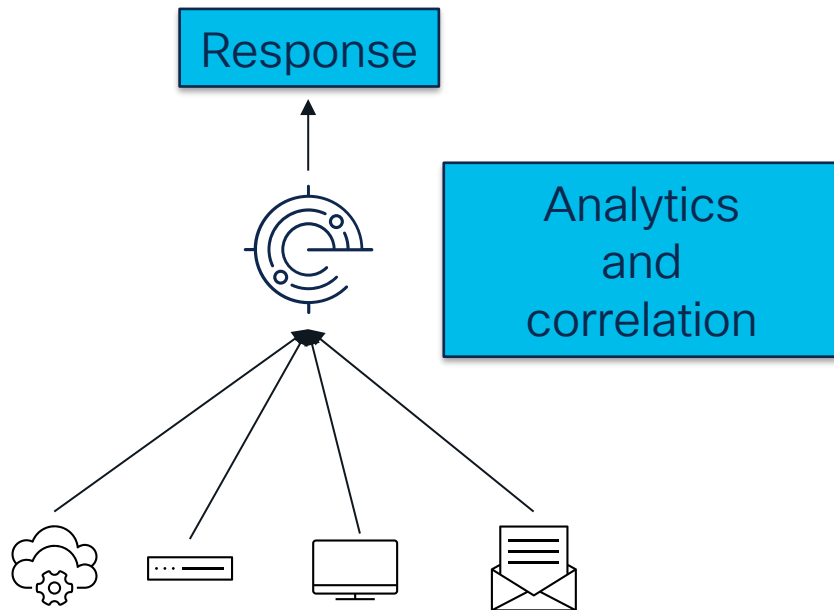


Alex Burger:
Probably not
a beer thief

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!

Collection of telemetry from multiple sources

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

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

Detection Analytics & Correlation (not complete)

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

Cisco

- Network Telemetry (NetFlow/ IPFIX)
- Firewall: FPR & ASA (via SAL)
- Identity Services Eng. (via SCA sensor)
- Secure Client NVM (Windows)
- Secure Endpoint*
- Secure Email Threat Defense
- Secure Network Analytics
- Meraki MX direct to XDR Cloud
- Secure Client NVM (MacOS)

3rd Party

- Crowdstrike Falcon
- Microsoft Defender for Endpoint
- Public Cloud Infrastructure
 - AWS
 - Azure
 - Google Cloud Platform
- Proofpoint
- Microsoft Defender for O365

Asset Insights & Context (not complete)

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

Cisco

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

3rd Party

- CrowdStrike
- Checkpoint
- Ivanti Neurons
- Jamf Pro
- Microsoft Azure AD (Users)
- Microsoft Defender for Endpoint
- Microsoft Intune
- SentinelOne
- VMWare Workspace ONE UEM
- ServiceNow SecOps
- Cybereason
- Trend Micro Vision One
- Palo Alto Cortex XDR

Threat Hunting & Investigation (not complete)

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

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

- Akamai
- 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
- Palo Alto Cortex
- Checkpoint
- More...

Automation & Response (not complete)

Provides automated, guided and manual actions to streamline SecOps, including incident response, threat analysis, team communications, and more

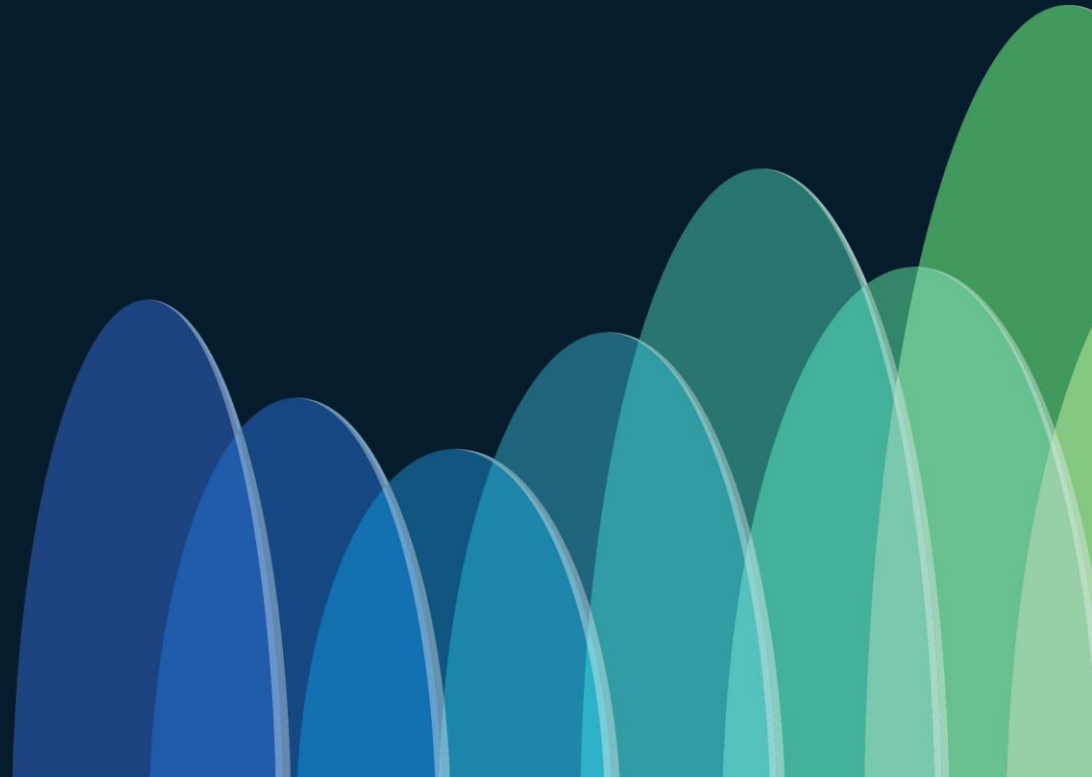
Cisco

- 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
- Checkpoint
- ExtraHop
- Fortinet Fortigate
- Google Cloud Platform
- Jamf Pro
- Microsoft Azure
- Microsoft Azure AD
- Microsoft Defender for Endpoint
- Microsoft Defender for O365
- Palo Alto NGFW
- Palo Alto Cortex XDR
- Palo Alto Panorama
- Checkpoint
- SentinelOne
- Trend Micro Vision One
- Cohesity (ARR)
- Slack
- More...

Incident Generation Framework



Important!

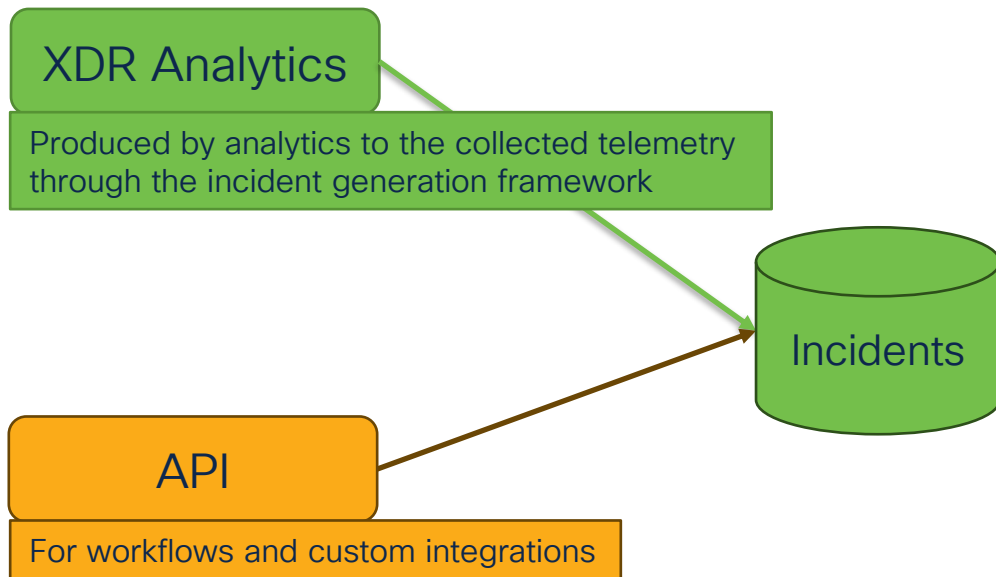
Incident Generation Framework significantly changed Oct 23, 2024

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 header with a "1000" status indicator, a "New" filter, and a "View Details" button. The incident is reported by "Cisco XDR Analytics (cisco-explorcorp-earth)" on "2024-04-17T22:23:14.732Z" and is linked to "2 Linked Incidents". A timeline indicates the incident started on "13th of October, 2023 at 15:12:29 UTC" and ended on "27th of February, 2024 at 00:35:44 UTC". The main content area shows a graph with "IP Addresses" and "Endpoints" connected by a "Accessed By/Connection" link. A "MITRE ATT&CK" sidebar lists various tactics and techniques, including "Reconnaissance", "Resource Development", "Initial Access", "Execution", "Persistence", "Privilege Escalation", "Defense Evasion", "Credential Access", "Discovery", "Lateral Movement", "Collection", "Command and Control", "Exfiltration", and "Impact". At the bottom, there are three summary cards: "6 Assets" (TOP ACTIVE), "68 Observables" (TOP ACTIVE), and "15 Indicators" (TOP ACTIVE).

Where do incidents come from? (Current status)



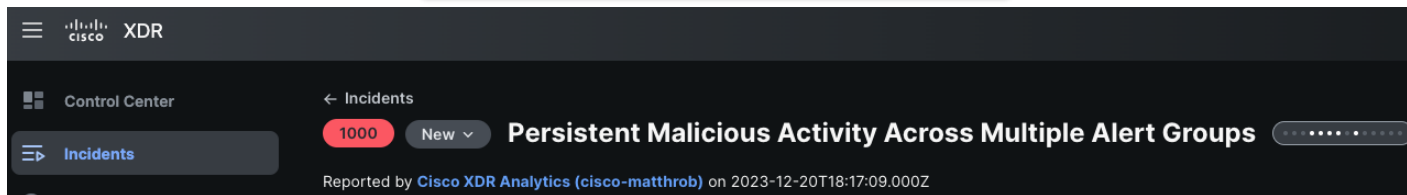
The screenshot shows the 'Incidents' dashboard in a dark theme. At the top, there are filters for 'Status' (New, Open, Unassigned) and a search bar. Below the filters is a table of incidents. The table has columns for Priority, Name, Source, Created, Assigned, and Status. The incidents listed are:

Priority	Name	Source	Created	Assigned	Status
High	AWS Root Account Used on Amazon Web Services [5076848820]root	Cisco XDR Analytics (s...	2 Months	Unassigned	New
High	LDAP Connection from Suspicious Process on ats-member01v securitydelta.net	Cisco XDR Analytics (s...	1 Month	Unassigned	New
High	LDAP Connection from Suspicious Process on ats-member01v securitydelta.net	Cisco XDR Analytics (s...	1 Month	Unassigned	New
High	Potential Persistence Attempt on box-wm70v0106.arg26.net	Cisco XDR Analytics (s...	1 Month	Unassigned	New
High	Suspicious Process Path on box-wm70v0106.arg26.net	Cisco XDR Analytics (s...	23 Days	Unassigned	New
High	ATW-Surfacelink4 in group ATW-Audit @ 20231005 00:00:26	Secure Endpoint	2 Days	Unassigned	New
High	Port 8888: Connections from multiple sources on ats-ubuntu04v securitydelta.net	Cisco XDR Analytics (s...	1 Day	Unassigned	New

At the bottom of the table, there is a pagination bar showing '25 per page' and '1 of 7'.

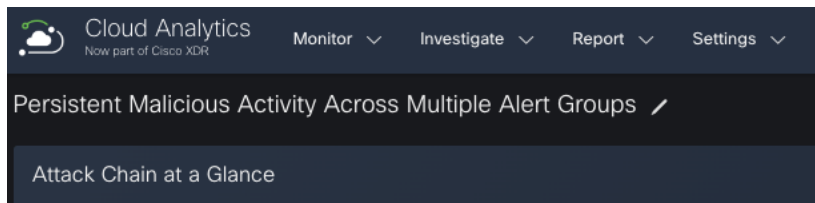
Aside: A note about UI's

Main XDR User Interface



SOC dashboard

Native Alerts, Incidents



Secure Cloud Analytics, also known as
XDR Analytics

"Detection Engineering" dashboard.
Admin for analytics stack.

Important Distinction in Terms

Native Detection

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

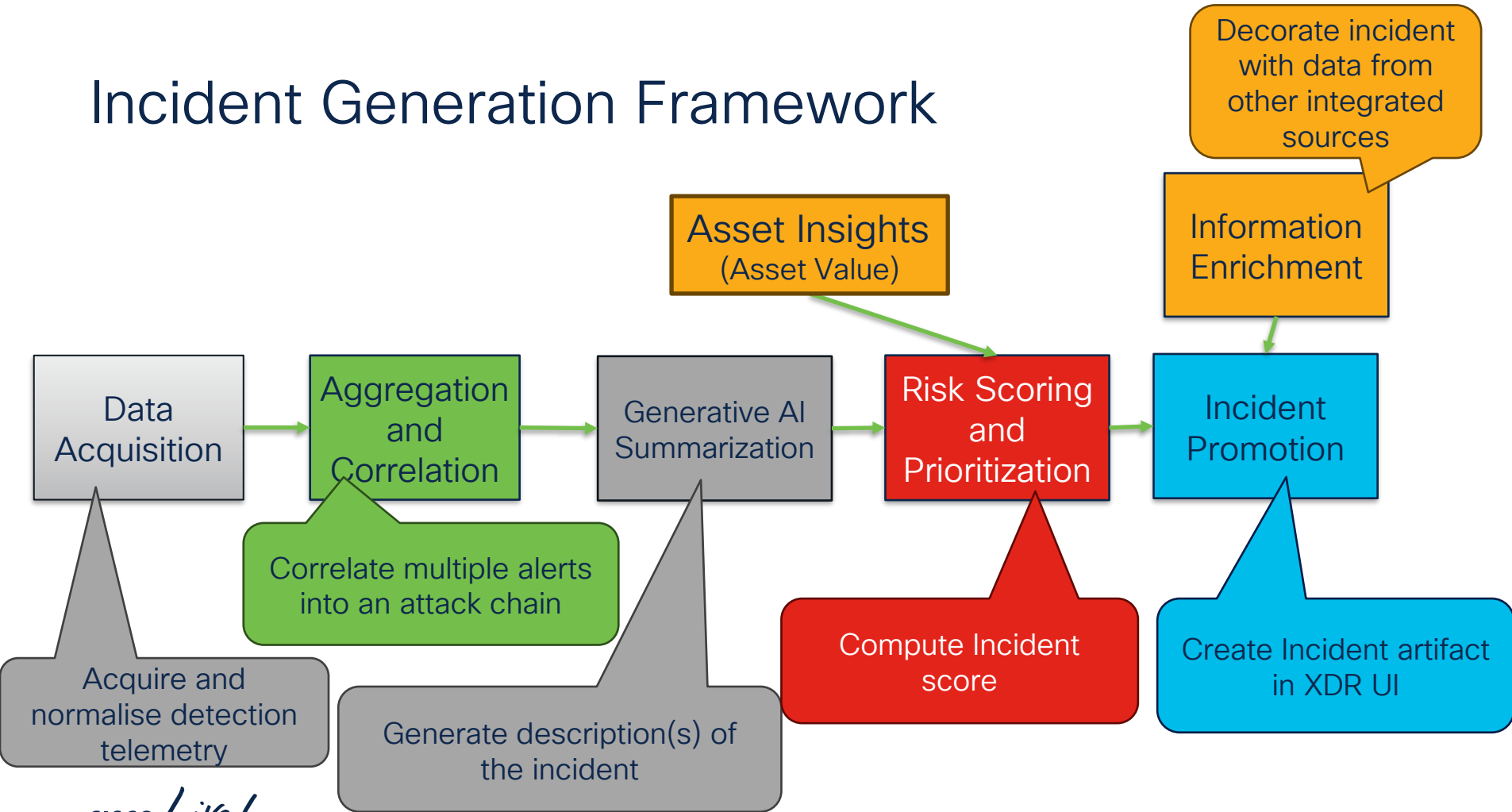
Extended (Correlated) Detection

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

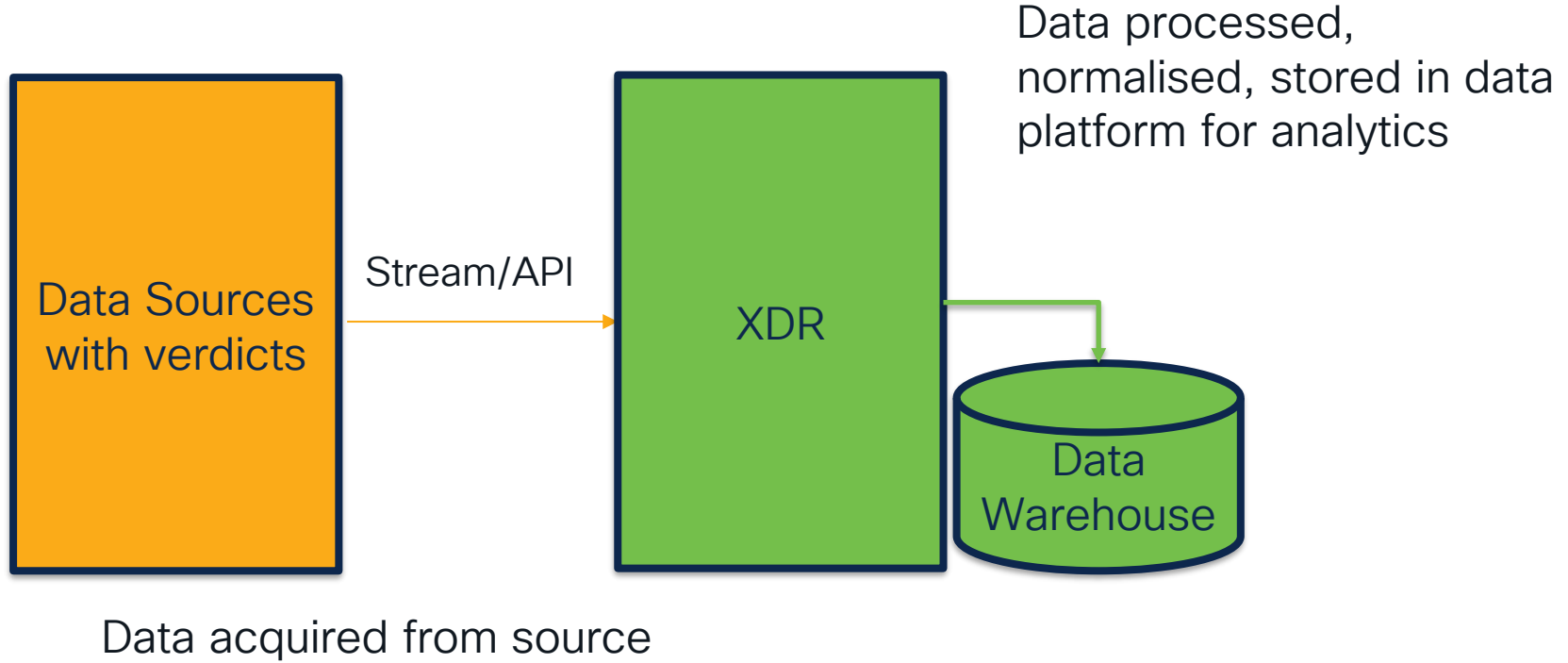
XDR Incident Generation Objective:

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

Incident Generation Framework



Data Acquisition and Normalisation

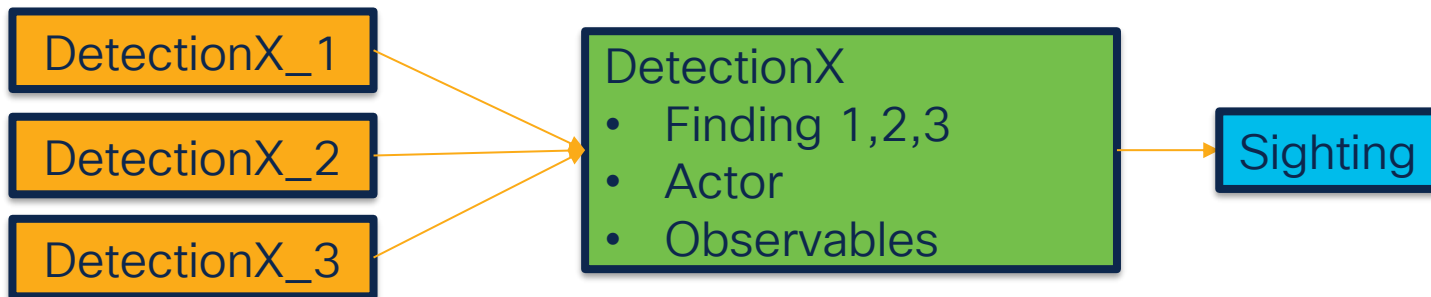


Data Acquisition and Normalisation

Data Source	Type	Frequency of Ingestion/Normalisation	Data Ingested
XDR Native Detections	Stream	Immediate (post alert generation)	Alerts and associated observations
ETD	Stream	60 minutes	ETD envelopes with verdicts
CSE	Stream	2 minutes	Behavioural Protection Detection Engine, Cloud IOC <ul style="list-style-type: none">• Critical, High• <i>Medium, Low</i>
Crowdstrike	API	10 minutes	Legacy Detections <ul style="list-style-type: none">• Critical, High• <i>Medium, Low</i>
Proofpoint	API	10 minutes	Messages delivered and clicks permitted
MSDE	API	10 minutes	Alerts and supporting evidence <ul style="list-style-type: none">• Critical, High• <i>Medium, Low</i>
O365	API	10 minutes	Alerts and supporting evidence <ul style="list-style-type: none">• Critical, High
SNA	Stream	60 minutes	Security Alerts: <ul style="list-style-type: none">• Data Hoarding• Suspect Data Loss• Bot Infected Host C&C

Aggregation

Reduce duplicative detections to a single finding



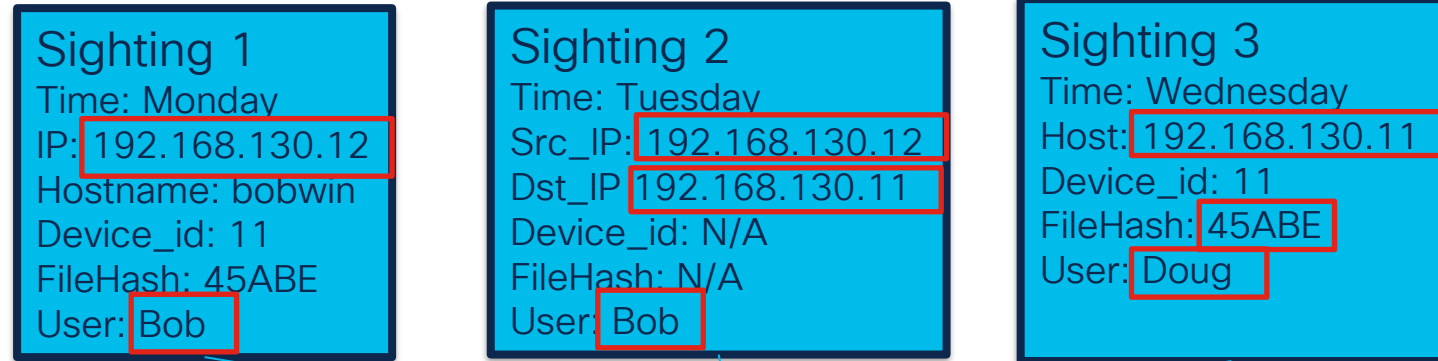
Aggregation = detection_id + detection_type + actor

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



Potential Incident: Malware Execution and lateral movement

The incident began on Monday With the final sighting on Wednesday with the same malware executed on a different device

Correlation Criteria

Sightings are correlated when they share at least one correlation observable

- Current correlation observables: IP Address, Device, Hostname, Username, File/Process Hash

Seven day rolling window correlation timeline

Couple safeguards:

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

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

Open [illegible]

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-4d76-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-4d76-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, **CiscoSecuEndpoint** 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**.

Close

CISCO *Live!*

#CiscoLiveAPJC

#BRKSEC_2178

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

28

Title and executive summary of incident

Long description

Incident Scoring and Prioritisation

Incidents prioritized by business impact and asset value

742 92 8
Detection Risk 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

Incidents

9 Incidents 0 New Incidents

Q Search X 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. On the left is a navigation sidebar with options: Control Center, Incidents, Investigate, Intelligence, Automate, Devices (selected), 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 a scale from 1 (Not Critical) to 7 (Somewhat Critical), with '10' selected. The 'Details' section lists attributes: 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 (0000-0001-9124-5765-2782-8837-93). The 'Seen in Sources' section shows a 'CrowdStrike' source with a 'Last Seen' timestamp of 2023-05-09T23:50:00.000Z. On the right, the 'Security Products' section lists 'Firewall' (NA, Not enabled) and 'Disk Encryption' (NA, Automatic Updates).

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

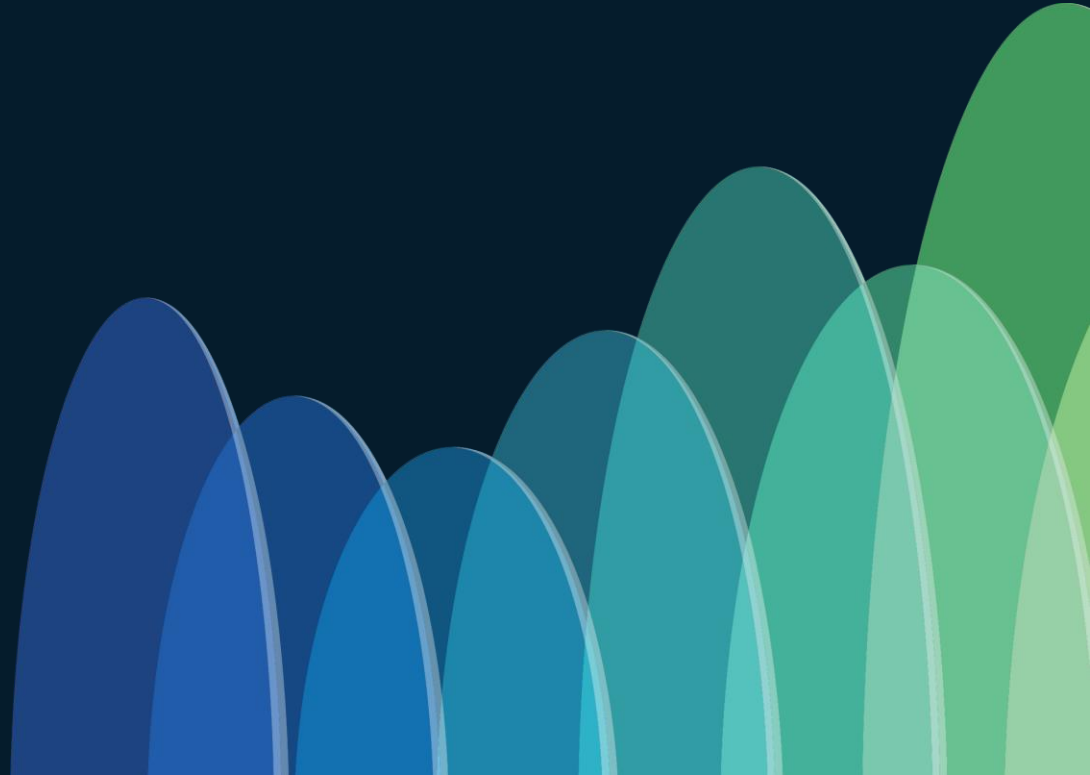
Closed incidents are not updated.

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

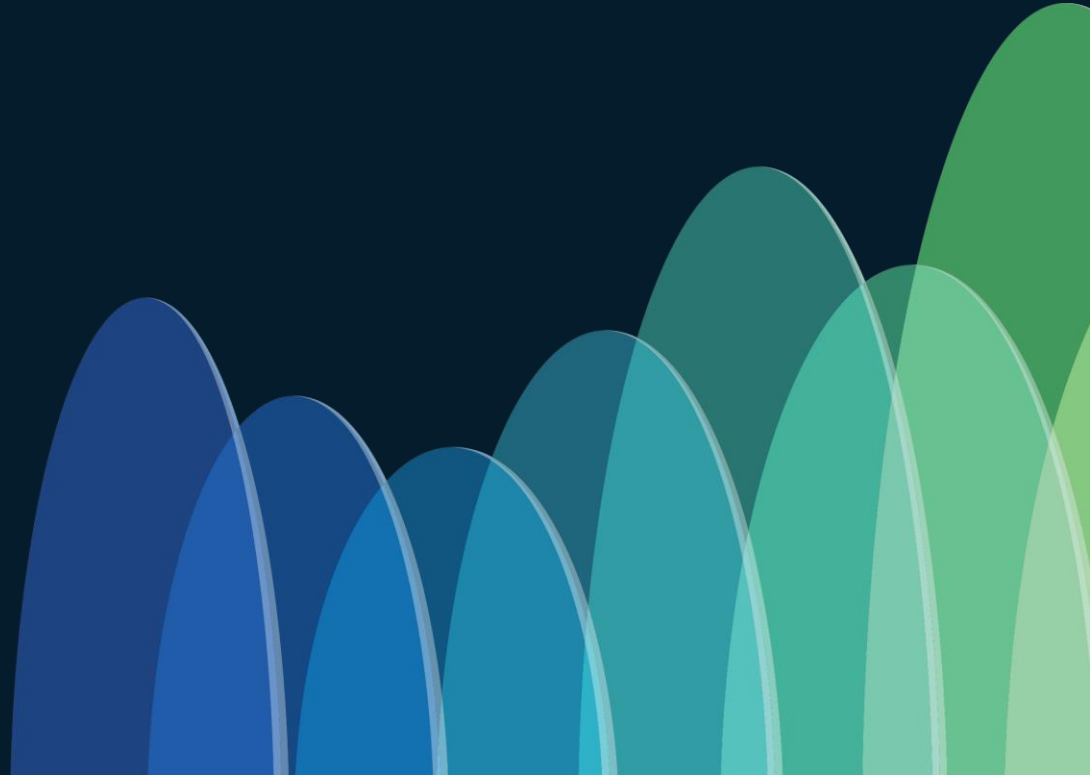
Incident Merging Criteria

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.

Demo



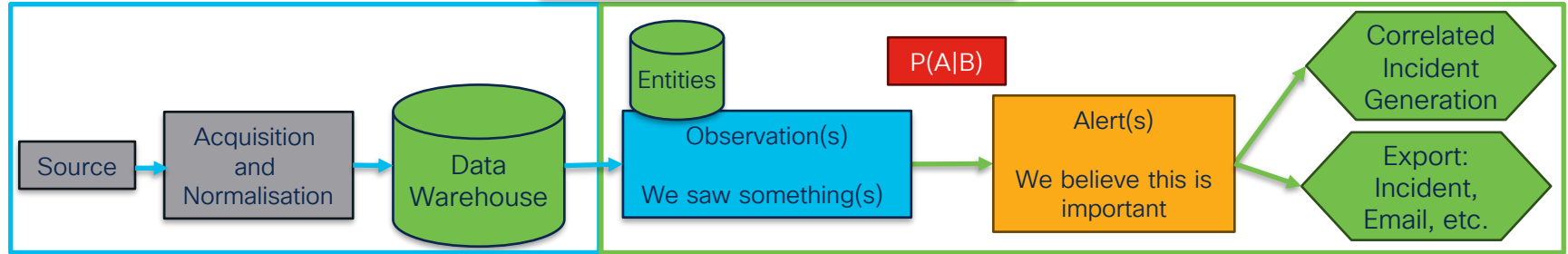
Native Detections



Native Detections

Detections XDR Analytics creates from telemetry that doesn't have a verdict

i.e. Creating a Verdict



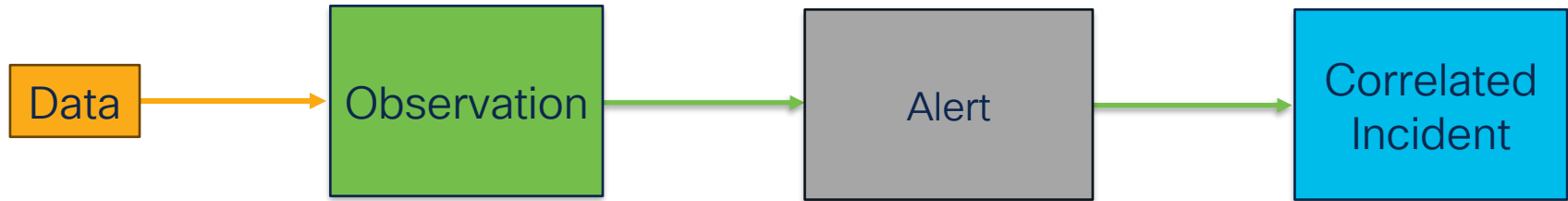
Time to Detect = Time to ingest and Normalise + time to analyse

Telemetry Sources:

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

$P(A|B)$: Probability model (i.e. probability that the (set of) observations is an Alert given what is known of the entity and the environment)

Creating Security Value from Data



Data powers observations, which power alerts

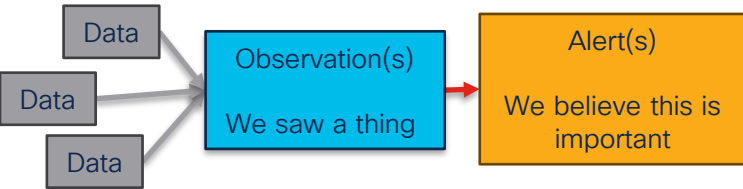
Alert Type	Observation Types	Telemetry	History
<div>▼</div>	<div>▼</div>	<div>Q 2 Selections X ^</div> <div>Endpoint X Cisco ISE X</div> <div>Azure Activity Logs</div> <div>Azure API</div> <div>Cisco ISE ✓</div> <div>Cisco NVM</div> <div>Endpoint ✓</div> <div>ETA</div> <div>Firewall</div> <div>GCP API</div> <div>GCP Audit Logs</div> <div>Netflow</div>	
> 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
> Invalid MAC Address 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.	• Invalid MAC Address		0 Days
> ISE Jailbroken Device A jailbroken device was detected. This does not necessarily indicate an active threat in isolation, but is a vulnerability that may increase organizational risk.	• ISE Suspicious Activity		0 Days
> Suspicious Endpoint Findings by Collection Suspicious behavior(s) have been noted on the endpoint that is mapped to Collection MITRE tactic	• Suspicious Endpoint Security Finding	Endpoint	0 Days
> Suspicious Endpoint Findings by Command and Control Suspicious behavior(s) have been noted on the endpoint that is mapped to Command and Control MITRE tactic	• Suspicious Endpoint Security Finding	Endpoint	0 Days

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

Creating Security Value from Data

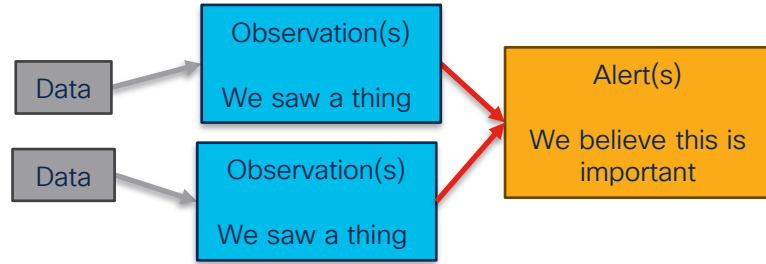
Observation: Low signal detection

Alert: High Signal detection



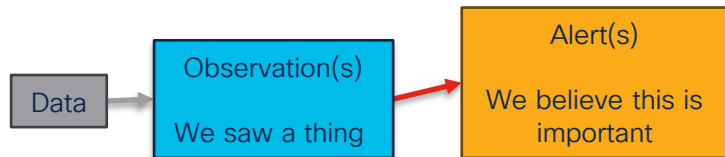
Alert Type	Observation Types	Telemetry ?	History ?
<div>Outbound Traffic</div> <div>Outbound Traffic Spike Device started sending a much larger amount of traffic to external destinations than before. This may indicate data exfiltration.</div>	<div></div> <div><ul style="list-style-type: none">New Large Connection (External)Record Profile OutlierRecord Metric Outlier</div>	<div>Netflow</div> <div>Netflow North-South</div>	14 Days

Some observations are based on lots of data



Alert Type	Observation Types	Telemetry ?	History ?
<div>IDS Emergent</div> <div>IDS Emergent Profile Device exhibits a new type of traffic at the same time it is flagged as suspicious by an IDS. This may indicate the device is compromised.</div>	<div></div> <div><ul style="list-style-type: none">Intrusion Detection System NoticeNew Profile</div>	<div>Firewall</div> <div>Netflow</div>	14 Days

Some alerts are based on multiple observations



Alert Type	Observation Types	Telemetry ?
<div>Powershell RDP</div> <div>Powershell RDP Connection The system utility Powershell was seen making connections over the RDP port, which is indicative of RDP connections.</div>	<div></div> <div><ul style="list-style-type: none">Suspicious Endpoint Activity</div>	<div>Cisco NVM</div>

Some data sets can lead directly to an observation and alert

Alerts can be a final data object

Alerts/Watchlists

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

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

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

Use discretion.

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.



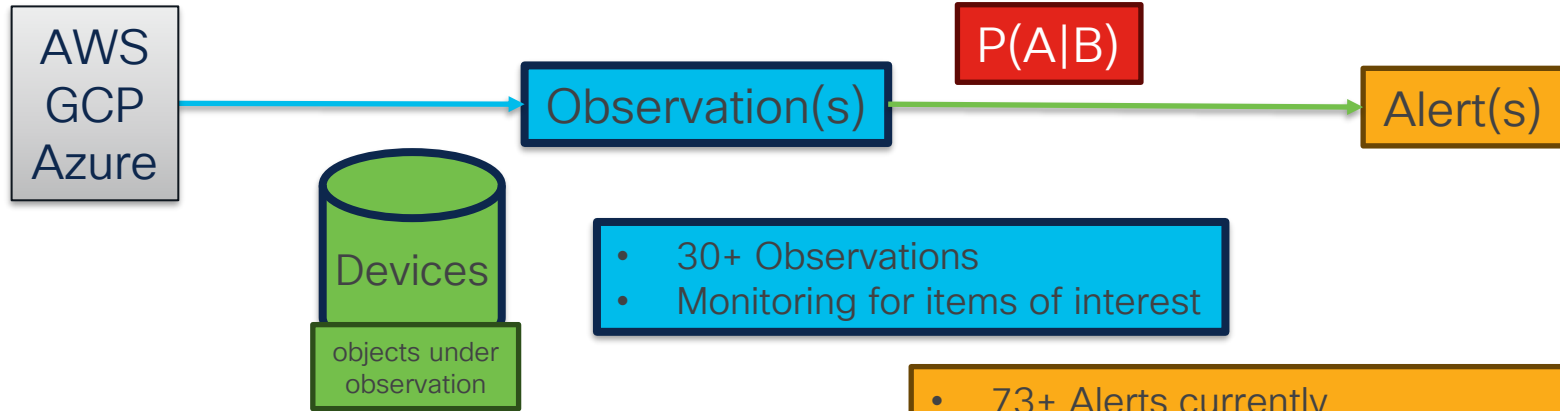
Webex Teams
Webhooks/Services

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.

IAAS Data Analytics Pipeline

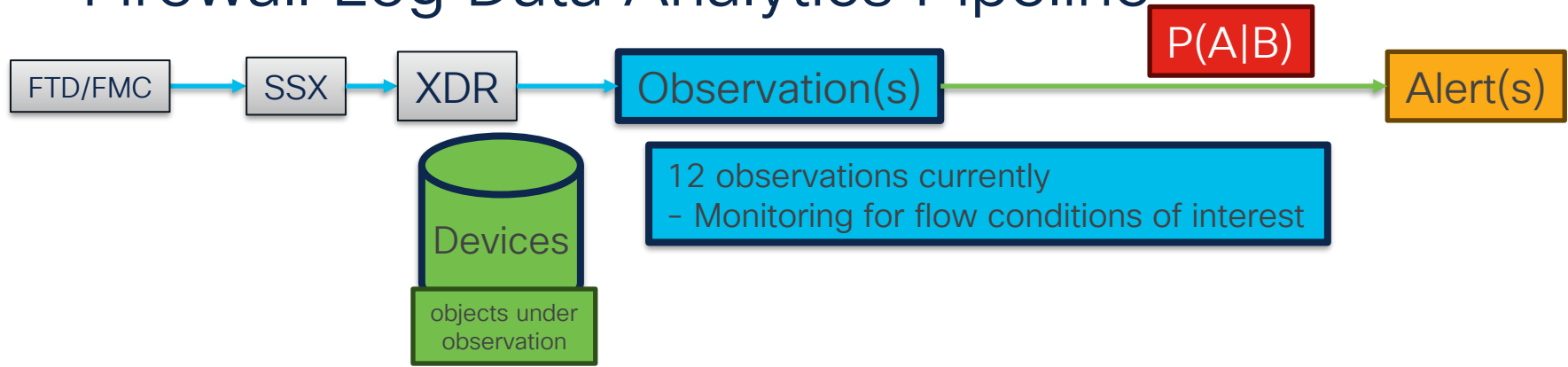


- Integrate on varying service options via API
- Normalise and store data
- Identify devices by numerous cloud objects (user, IP, instance-id, etc.)

- 30+ Observations
- Monitoring for items of interest

- 73+ Alerts currently
- Some alerts are composed of single observation(s)
- Some alerts are composed of multiple observation(s)
- Contain source observations, Assigned to device

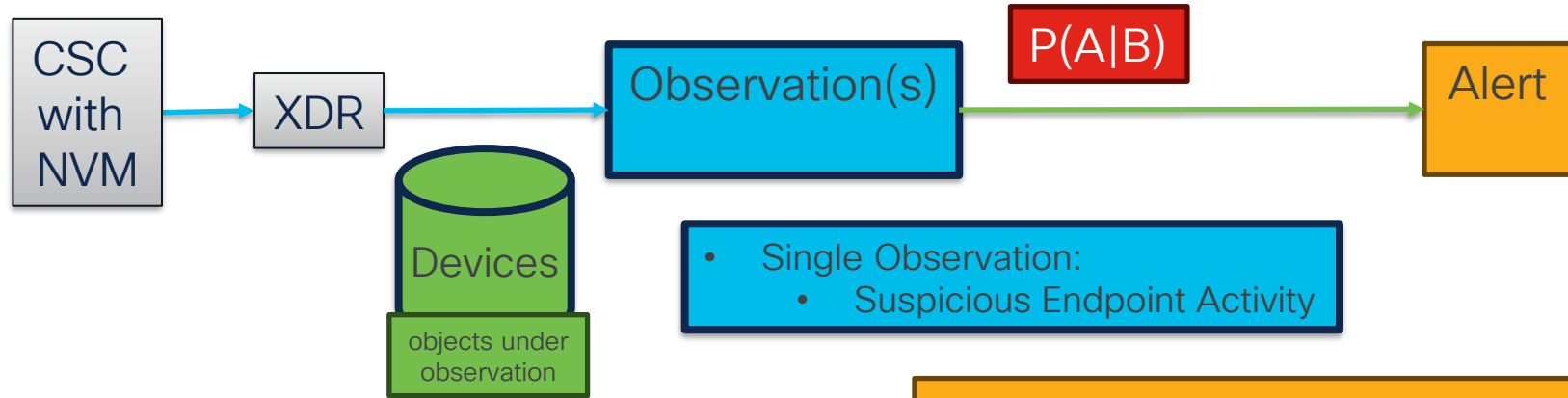
Firewall Log Data Analytics Pipeline



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

- 15+ Alerts currently
- Some alerts are composed of single observation(s)
- Some alerts are composed of multiple observation(s)
- Contain source observations, Assigned to device

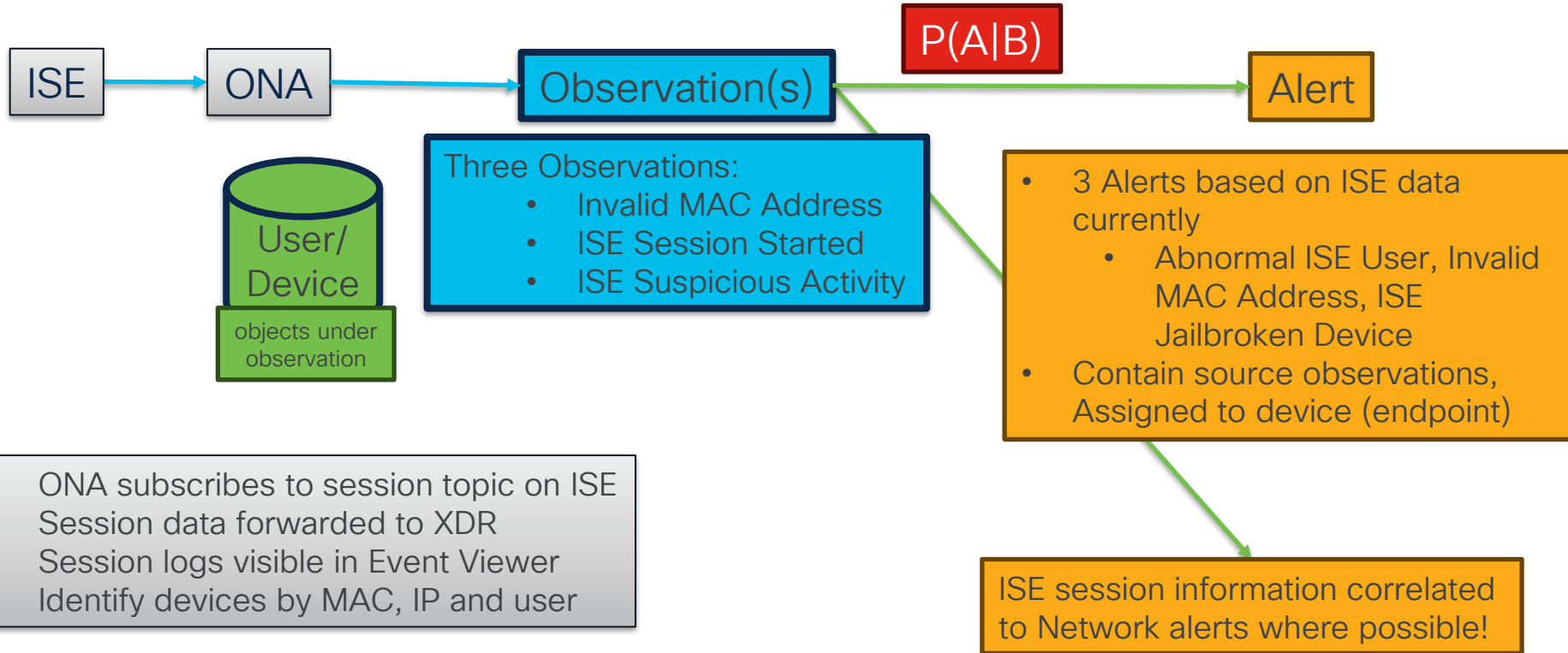
NVM Data Analytics Pipeline



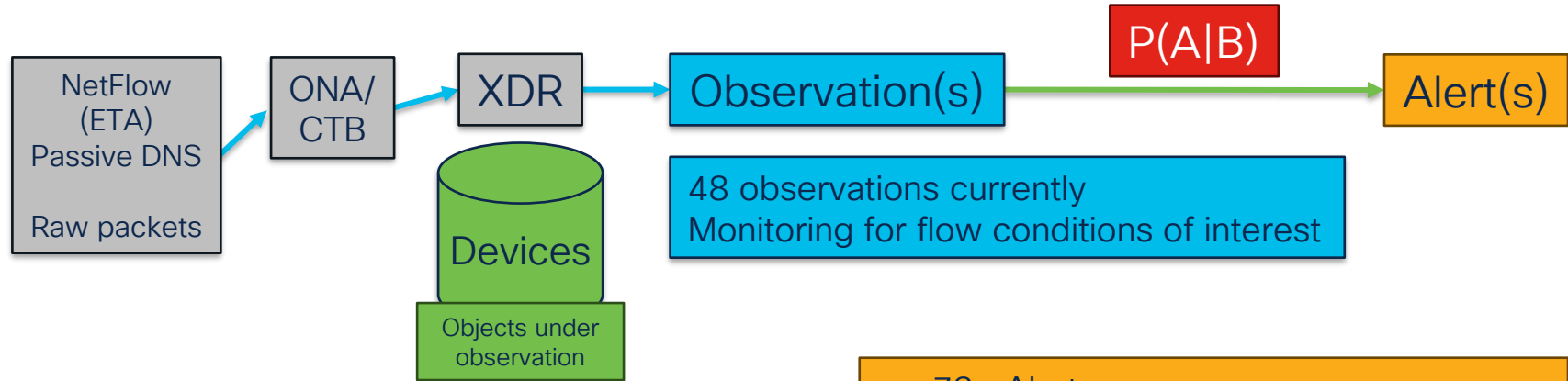
- NVM profile configured to send data direct to XDR cloud
- Normalise and store data
- NVM logs visible in Event Viewer
- Identify devices by agent ID

- 24+ Alerts using NVM data
 - Combination of network and endpoint data artifacts
- Contain source observations, Assigned to device (endpoint)

ISE Data Analytics Pipeline



Network Flow Data Analytics Pipeline

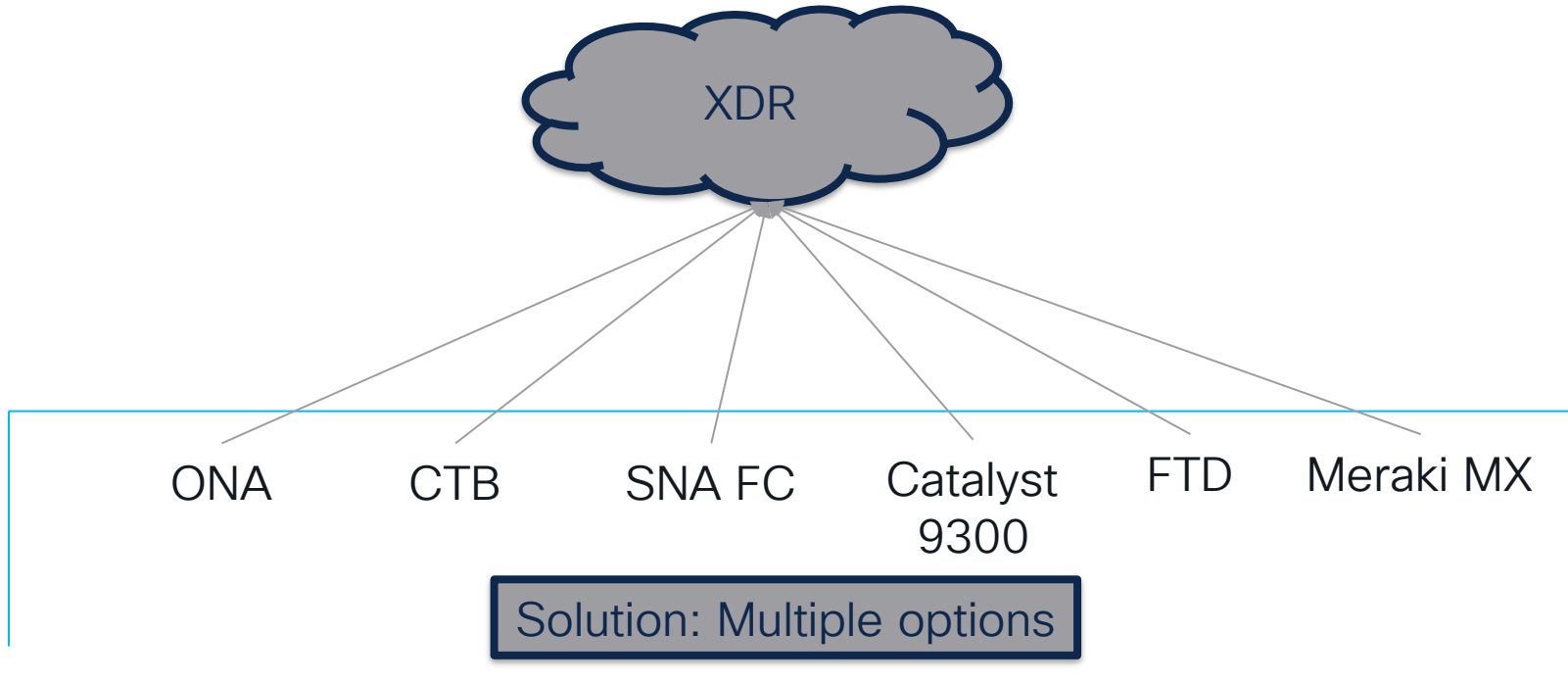


- NetFlow (incl. ETA), Passive DNS, Raw packets sent to:
 - Observable Network Appliance (ONA)
 - Cisco Telemetry Broker (CTB)
- Metadata extracted and sent to XDR
- Flow logs visible in Event Viewer
- Identify devices by IP Address, Hostname

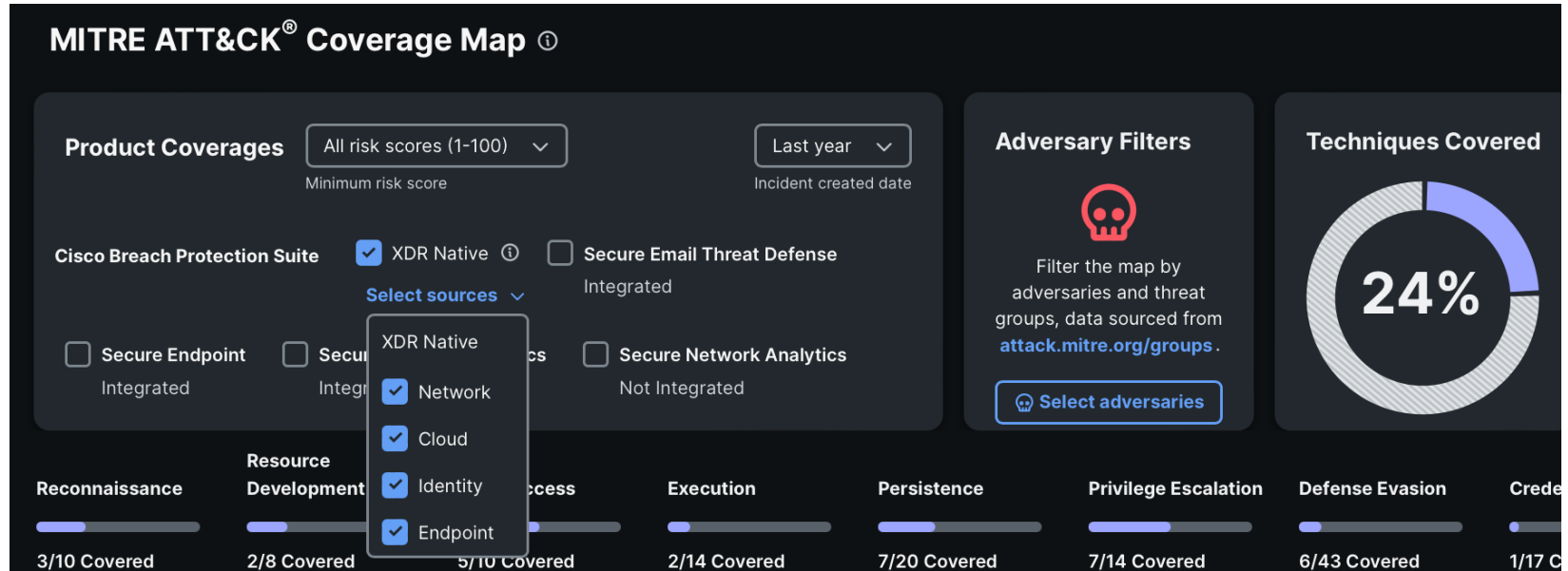
- 73+ Alerts
- Some alerts are composed of single observation(s)
- Some alerts are composed of multiple observation(s)
- Contain source observations
- Assigned to device
- Correlated into Attack Chains

XDR: Getting Network Data In

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

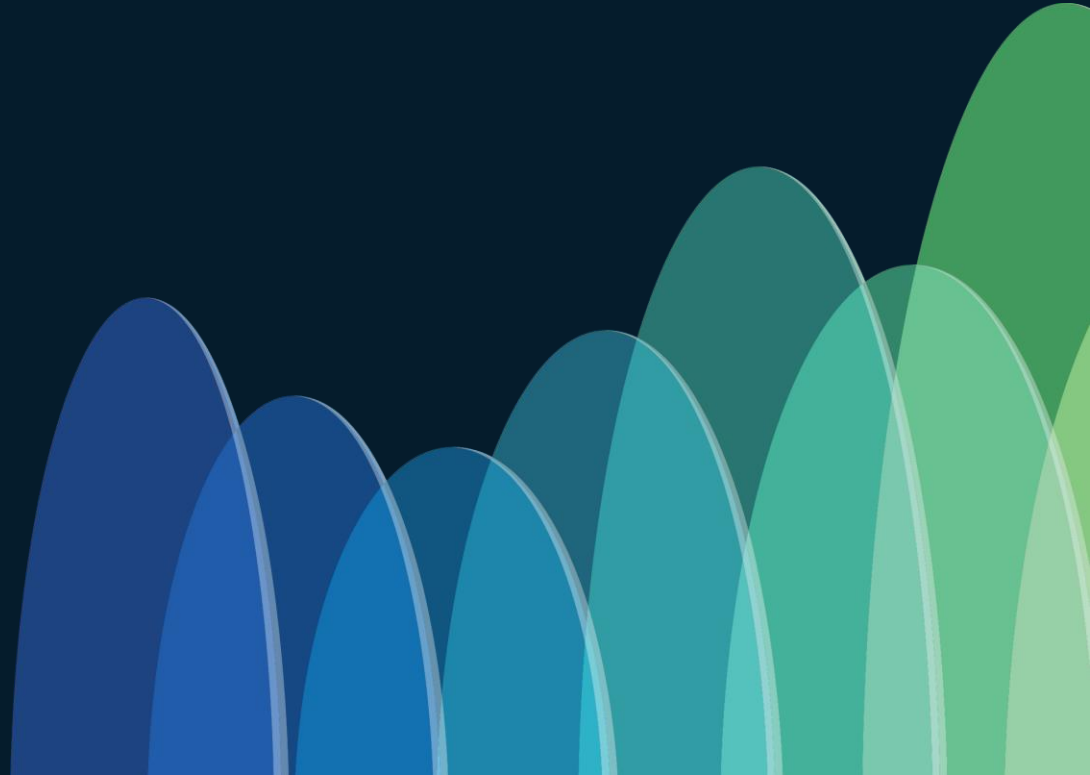


MITRE ATT&CK Coverage Map

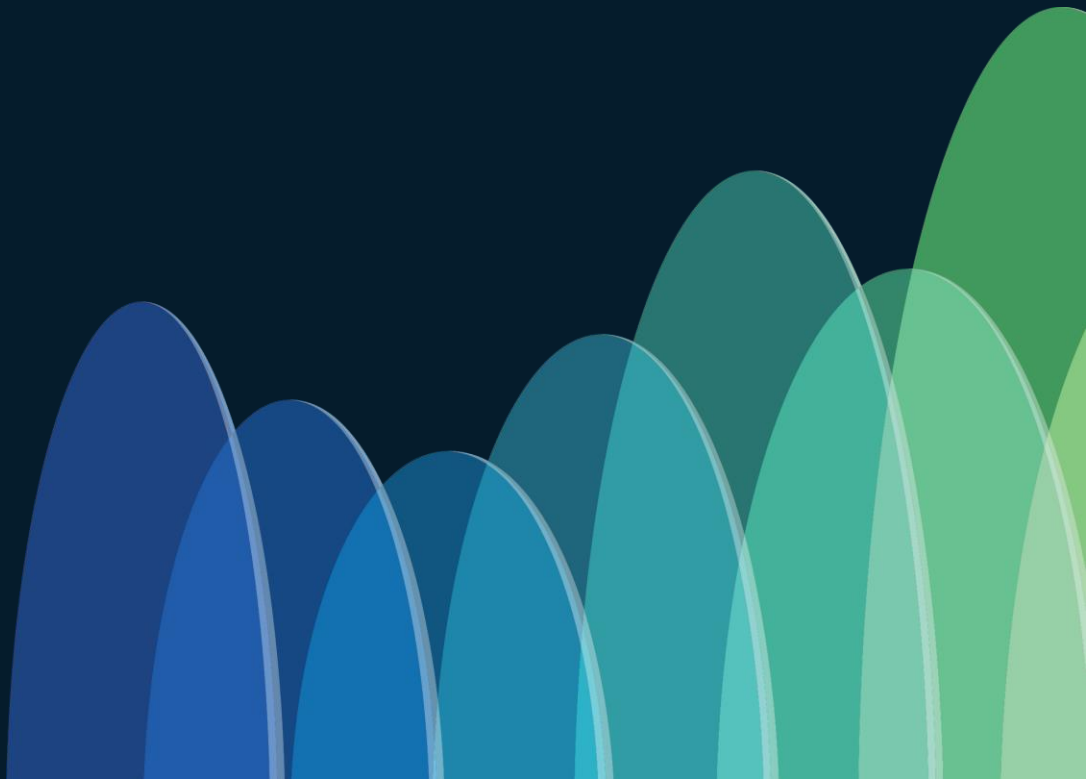


Understanding what coverage data sources can provide

Demo



Get SNOC'd



What is a SNOOC?



Get SNOC'd!



Network Operations = Security Operations = Lean Team

Simplified Operations, Fewer Consoles, Unified Policy, etc.

Get SNOC'd!

XDR & Meraki:
Security and
Network
Operations Centre

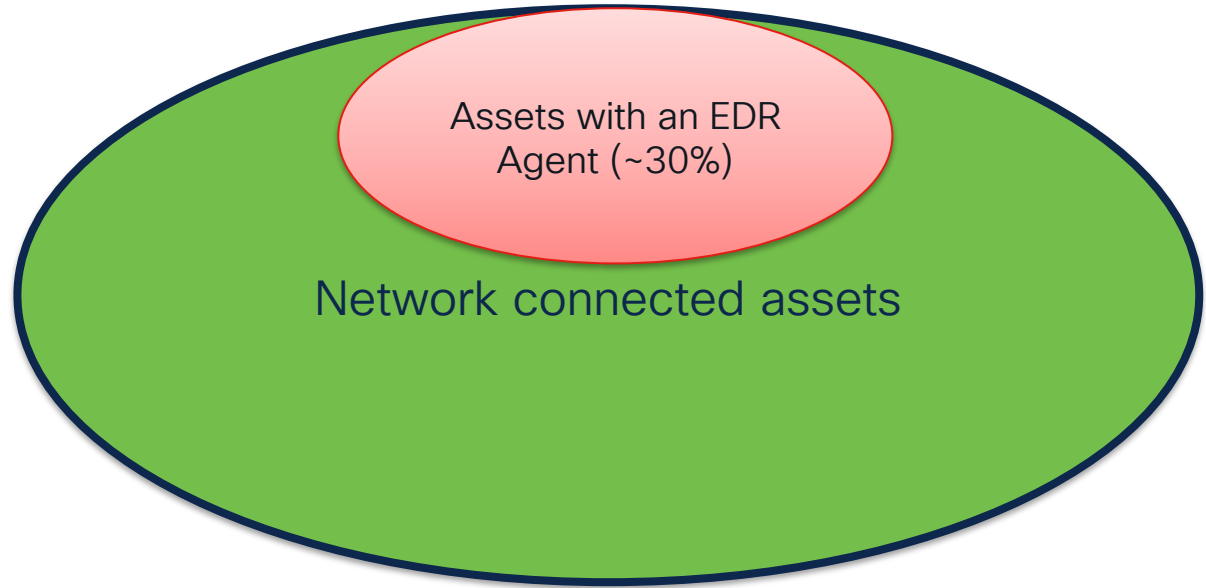
XDR:
Security
Operations Centre

Meraki:
Network
Operations Centre

Problem Statement: Visibility across my network

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.



The Value of Network Visibility

Gain insights into the devices, users and applications on your network and what they are up to.

Operational Outcomes

Ask questions of the data to make operational decisions.

Ex. How many users are bypassing my proxy.

Analytical Outcomes

Security Policy:

Analyse network behaviour to design, implement and validate security policy

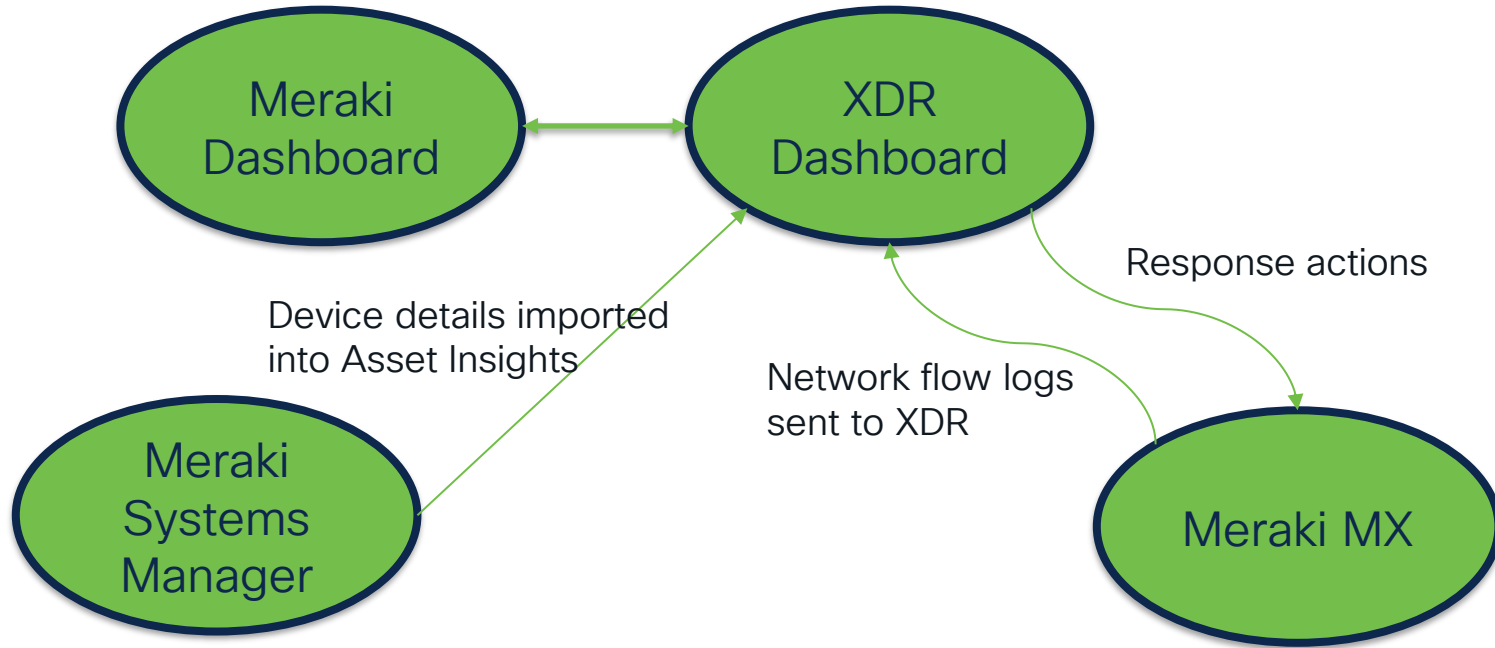
Threat Detection:

Analyse network behaviour to infer the presence of a threat actor

Example Network Threat Detection



High Level: Meraki-XDR Integration Today



Meraki and XDR Requirements

- Licensing

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

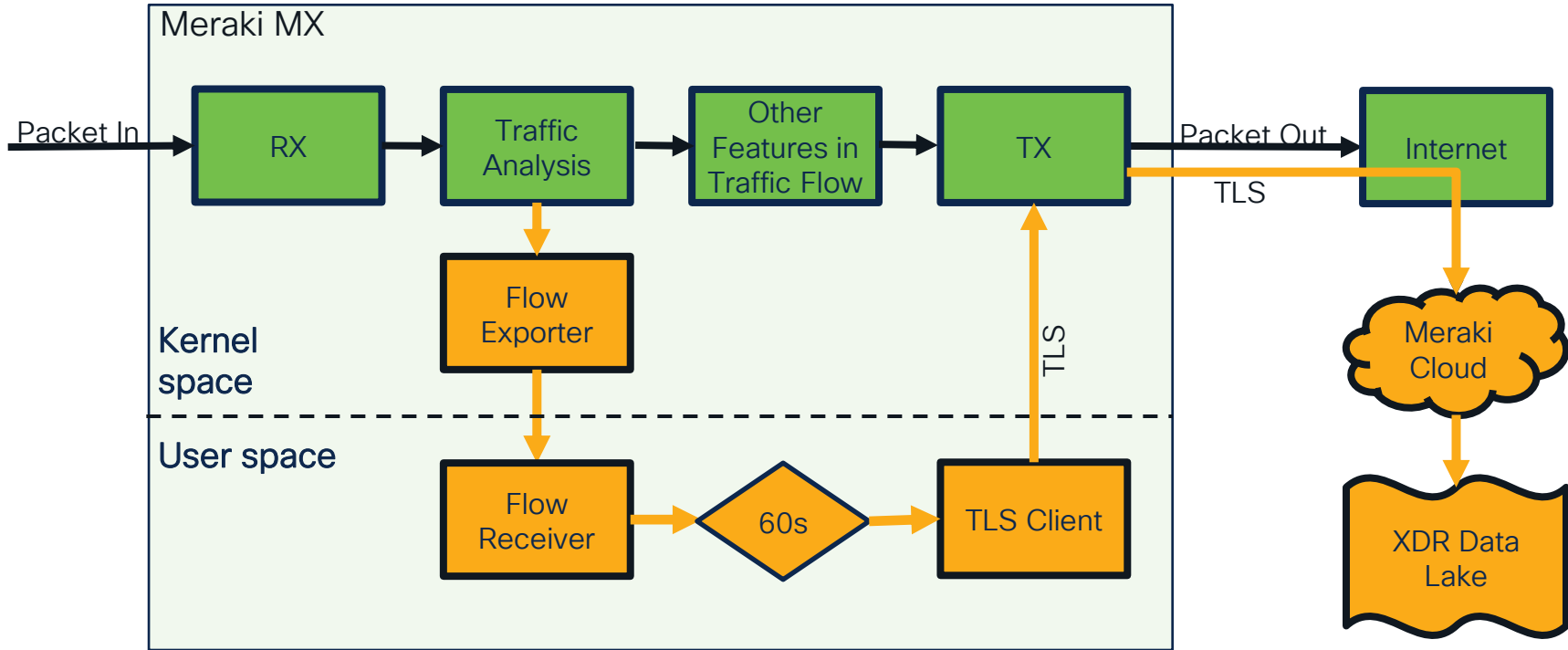
- Firmware

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

- Platforms

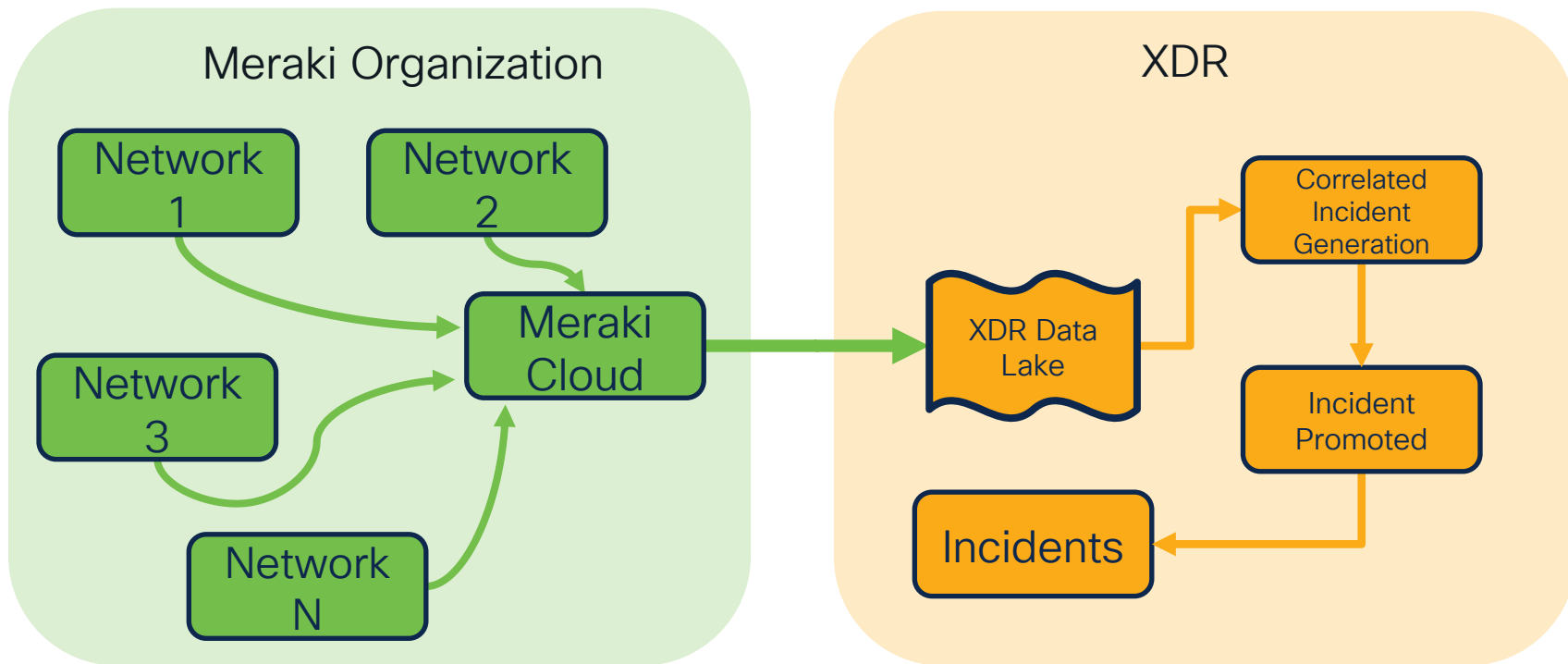
- Z3, Z4
- MX67, 68, 75, 85, 95, 105, 250, 450
- Virtual MX – S/M/L
- Not supported: vMX-XL, MX650, older platforms incompatible with 19.x such as the MX100, MX84, MX64

Close Up: MX Telemetry Packet Flow



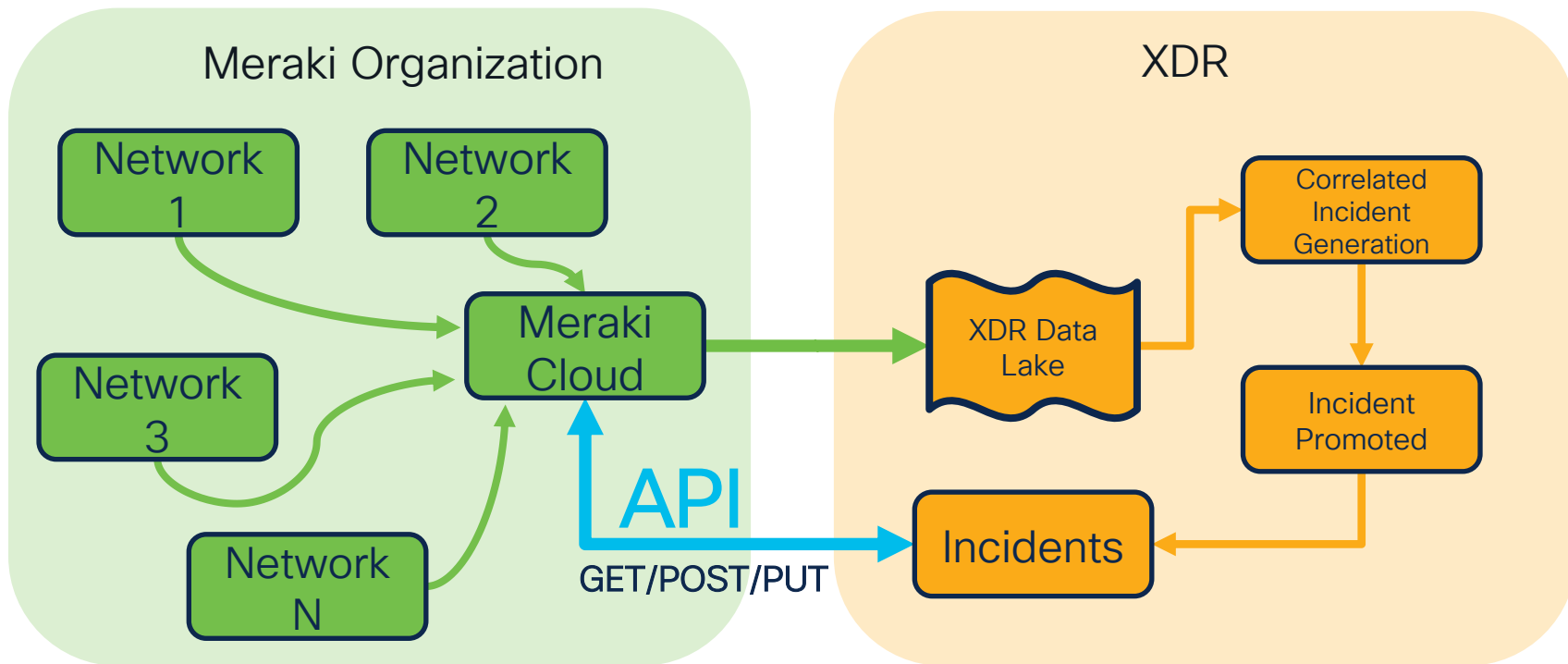
MX & XDR Integration

High-level Overview



MX & XDR Integration

High-level Overview: API



NDR: The problem of the overlapping IP

Alert:
192.168.128.100 is being bad!

Which 192.168.128.100?
Are they all the same, all different?
What gives?
Does this thing even work in this scenario?

Organisation wide NDR



Site 1:

192.168.128.0/24

Site 2:

192.168.128.0/24

Site 3:

192.168.128.0/24

Meraki, XDR and solving the problem of the Overlapping IP

Device Report | 10.1.1.111

Device Outline

Last updated: yesterday 2024-09-09
10.1.1.111

more actions

Name: 10.1.1.111
IPs: 10.1.1.111

Open Alerts: 0
Int Connections: 0
Ext Connections: 45

ATTENDANCE

Normally Active: 0:36:00 to 23:01:00

OBSERVATIONS

Observations: 13

10-Day Activity (Connections)

Profiles (AVG from 7 days ago to yesterday)

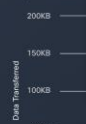
Alerts

Last updated: today 10:00:00

0 OPEN 0

History

Daily device metrics:



Challenge: Network telemetry identifies entities by IP

SCA tracks entities by a device ID:
- usually identified by a <namespace, ID> pair

Meraki telemetry includes <network-id, IP Address> pair

Overlapping IP Space (inside of a Meraki Organization) solved

Session Traffic ⓘ Cloud Posture ⓘ ISE ⓘ NVM Flow ⓘ

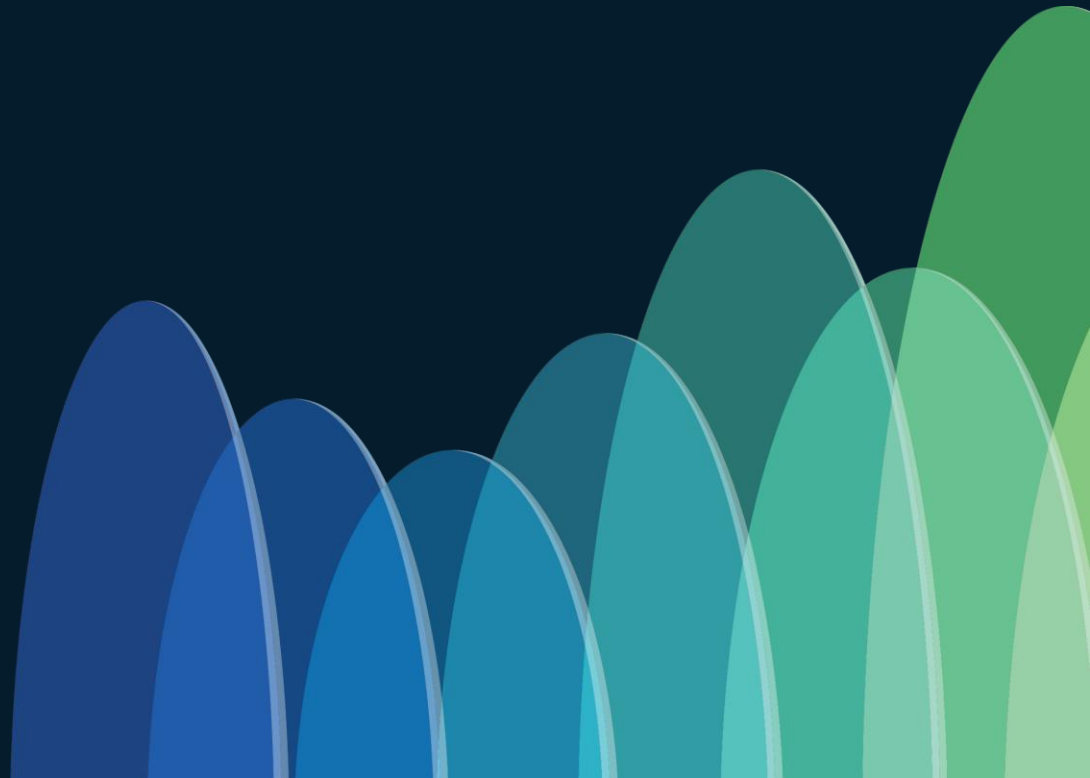
2024-09-10 07:58:22 PDT | 2024-09-10 08:58:22 PDT ▼

switch to query-mode above to

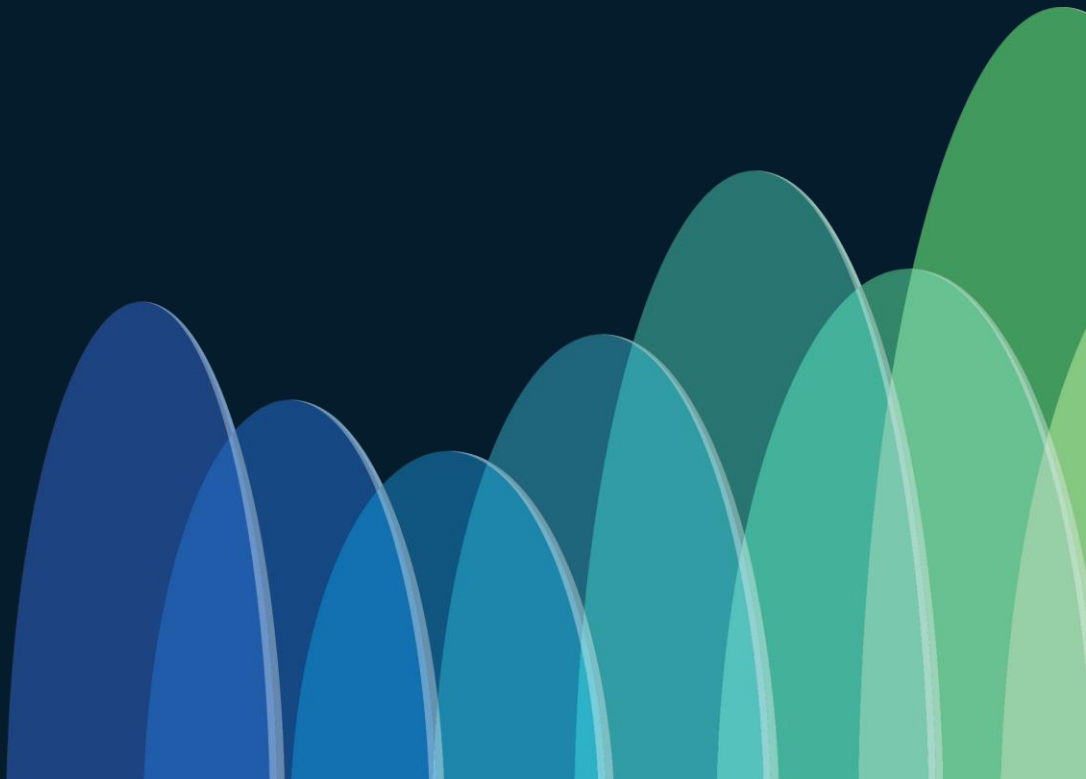
Applied filters: device_id: "35501" ✕ restore default filters

Time	Namespace ⓘ	IP
filter by custom range ...	▼	▼
2024-09-10 08:06:05 PDT	meraki:460175:N_573083052582919829:Q2YN-K76R-SLZU	10.1.1.111 ▼

Demo



Summary



Related Sessions

Session ID	Title	When
BRKSEC-2596	The In's and Out's of Cisco XDR's latest integrations	Tuesday 1:00 PM
DEVNET-2057	Building Incident Response Actions for Meraki using Cisco XDR Orchestration Workflows	Tuesday 12:00 PM
BRKSEC-2227	Evaluating and Improving Defenses with MITRE ATT&CK	Monday 3:15 PM
BRKSEC-2597	Securing Cloud Managed Networks: Delivering Zero Trust with Meraki and Cisco Security Technologies	Tuesday 8:30 AM
BRKSEC-2178	Extended Detection with Cisco XDR: Data, Analytics and Attack Chains	Tuesday 4:15 PM
DEVNET-1083	Security Automation: Developing with Cisco XDR	Monday 3:15-4:00 PM
DEVWKS-1190	Getting Started with Cisco XDR Automation workflows and atomics	Tuesday 4:00-4:45 PM

Keynote Deep Dives

Wednesday
10:30am – 11:30am



Experiences Amplified:
How AI Can Fuel Better Employee and Customer Experiences

Level 1
Room 106



Smart, Secure, Seamless:
Transforming Experiences with Next-Generation Networking

Level 2
Room 204



Harness a Bold New Era:
Transform Data Centre and Service Provider Connectivity

Level 2
Room 203



Securing User to Application and Everything in Between

Level 2
Melbourne Room 2



Unlocking Digital Resilience through Unified Observability

The HUB
Centre Stage

Complete Your Session Evaluations



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



Complete your surveys in the **Cisco Live mobile 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 DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: Meet The Engineer!

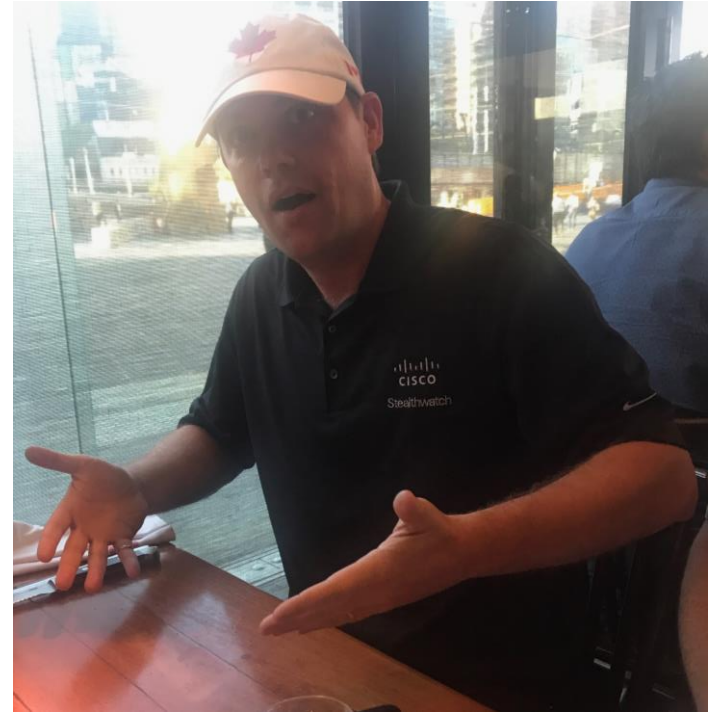
Parting Thoughts

Simplify your security operations with Cisco XDR!

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

Meraki and XDR integration is something truly special

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





Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC