The bridge to possible

The SNOC is a Real Thing

Meraki, Security Analytics and XDR

Alex Burger, PTME, Cisco Meraki
Matt Robertson, DTME Cisco Security

BRKENT-2033

Cisco Webex App

Questions?

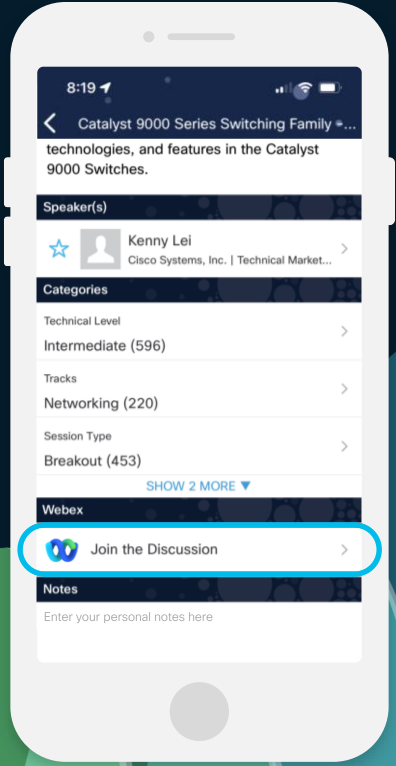
Use Cisco Webex App to chat
with the speaker after the session

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.

https://ciscolive.ciscoevents.com/
ciscolivebot/#BRKENT-2033



8:19

Catalyst 9000 Series Switching Family -...

technologies, and features in the Catalyst 9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

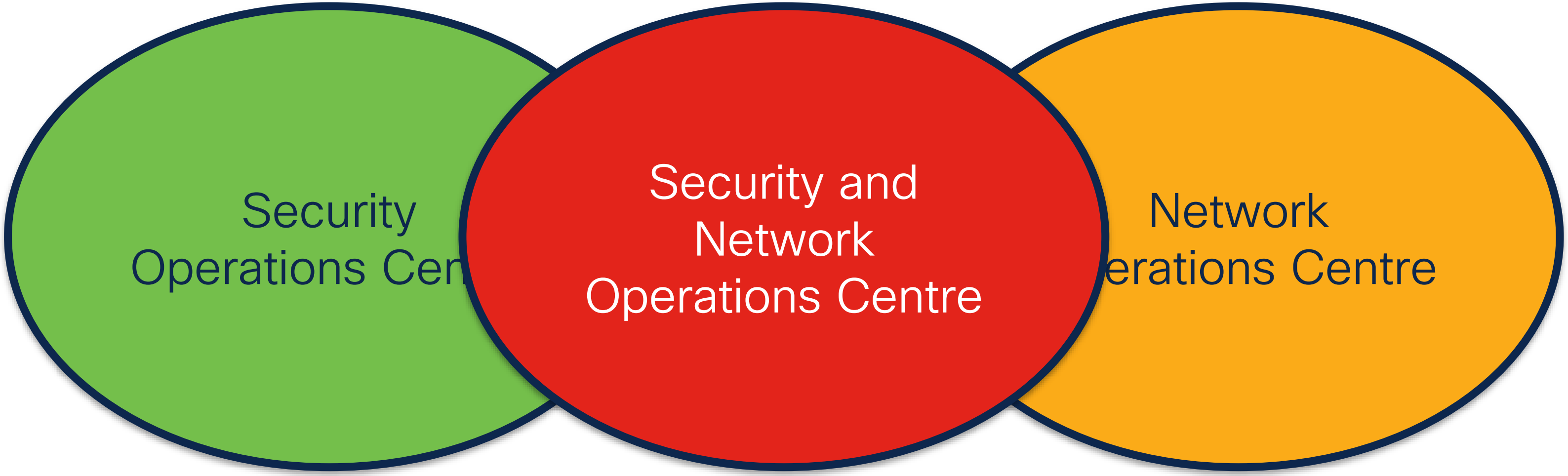
Join the Discussion

Notes

Enter your personal notes here

Exactly what is a SNOC?

Get SNOC'd!


Security
Operations Cen
Security and
Network
Operations Centre
Network
erations Centre

Agenda

- Introduction
- Secure Network Analytics and XDR
- Telemetry from the Meraki Network
- Threat Detection and Response
- Conclusion

Watch out for this guy!

About Us

Matt Robertson
Distinguished Engineer

cisco SECURE

Alex Burger
Principal Engineer

cisco Meraki

Secure Network Analytics and Cisco XDR

NDR & XDR

Network Detection and Response

- Analyze north/south and east/west traffic flows in near-real time
- Model network traffic and highlight suspicious traffic and offer behavioral techniques (non-signature) to detect anomalies
- Aggregate individual alerts in structured incidents to facilitate investigation
- Provide automatic or manual response capabilities

Extended Detection and Response

- Collection of telemetry from multiple security tools
- Application of analytics to the collected and homogenized data to arrive at a detection of maliciousness
- Response and remediation of that maliciousness

NDR & XDR

Network Detection and Response

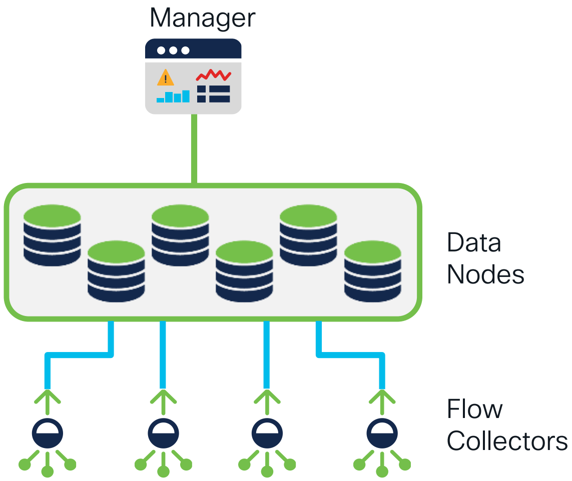
Extended Detection and Response

Cisco Secure Network Analytics

Cisco XDR

Cisco Secure Network Analytics

(Stealthwatch Enterprise)



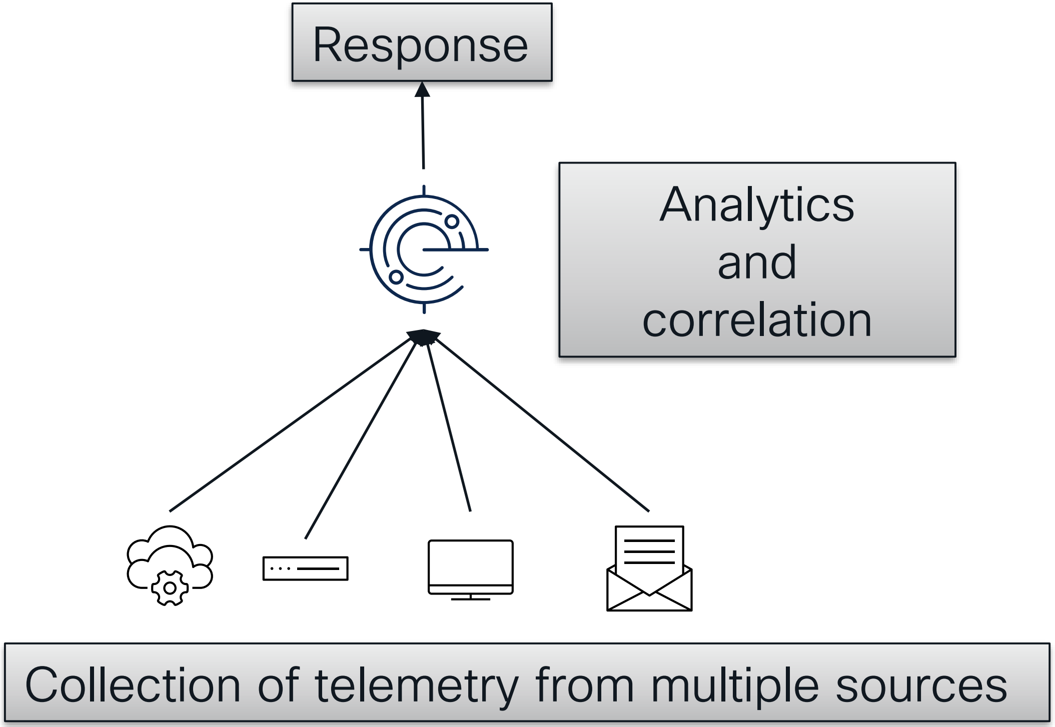
BRKSEC-2248 – Design, Deploy Cisco Network Detection and Response with Cisco Breach Suite
– Hanna Jabbour, Wednesday Jun 5 @ 2:30 pm

BRKSEC-3019 – Visibility, Detection and Response with Cisco Secure Network Analytics
– Matt Robertson, Monday Jun 3 @ 3:00 pm

Secure Network Analytics is a collector and aggregator of network telemetry for the purposes of security analysis and monitoring

Comprehensive East-West network visibility and analytics

Cisco XDR



Response

Analytics and correlation

Collection of telemetry from multiple sources

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

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.

Meraki and XDR Integrations

Data Analytics and Correlation

Flow logs ingested for network detections

Threat Hunting and Investigation

API enrichment for incidents

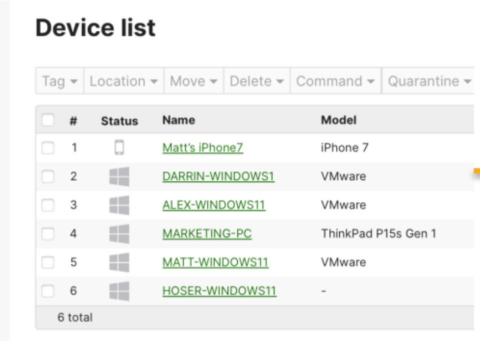
Asset Insights and Context

Systems Manager assets ingested to Asset Insights

Automation and Response

Response workflows available

Meraki Systems Manager & XDR Asset Insights

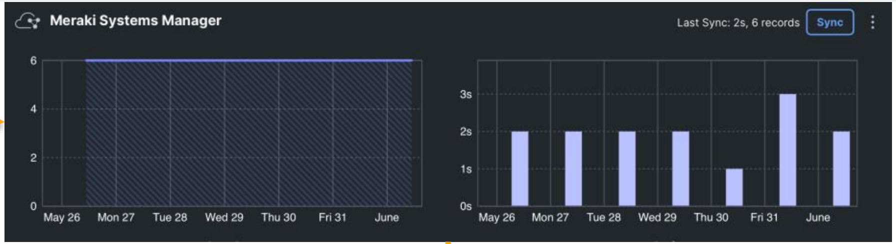


Device list

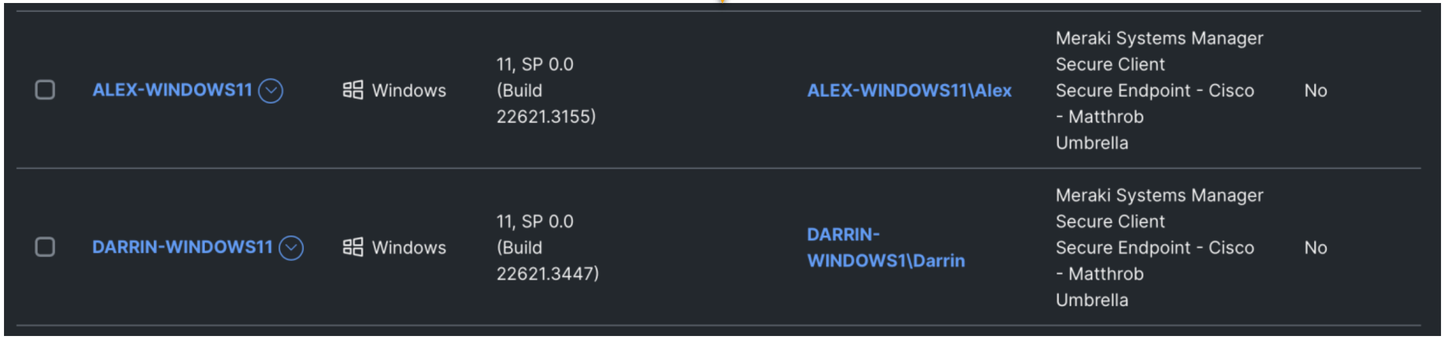
#	Status	Name	Model
1		Matt's iPhone7	iPhone 7
2		DARRIN-WINDOWS1	VMware
3		ALEX-WINDOWS11	VMware
4		MARKETING-PC	ThinkPad P15s Gen 1
5		MATT-WINDOWS11	VMware
6		HOSER-WINDOWS11	-

6 total

System Manager devices and details via API

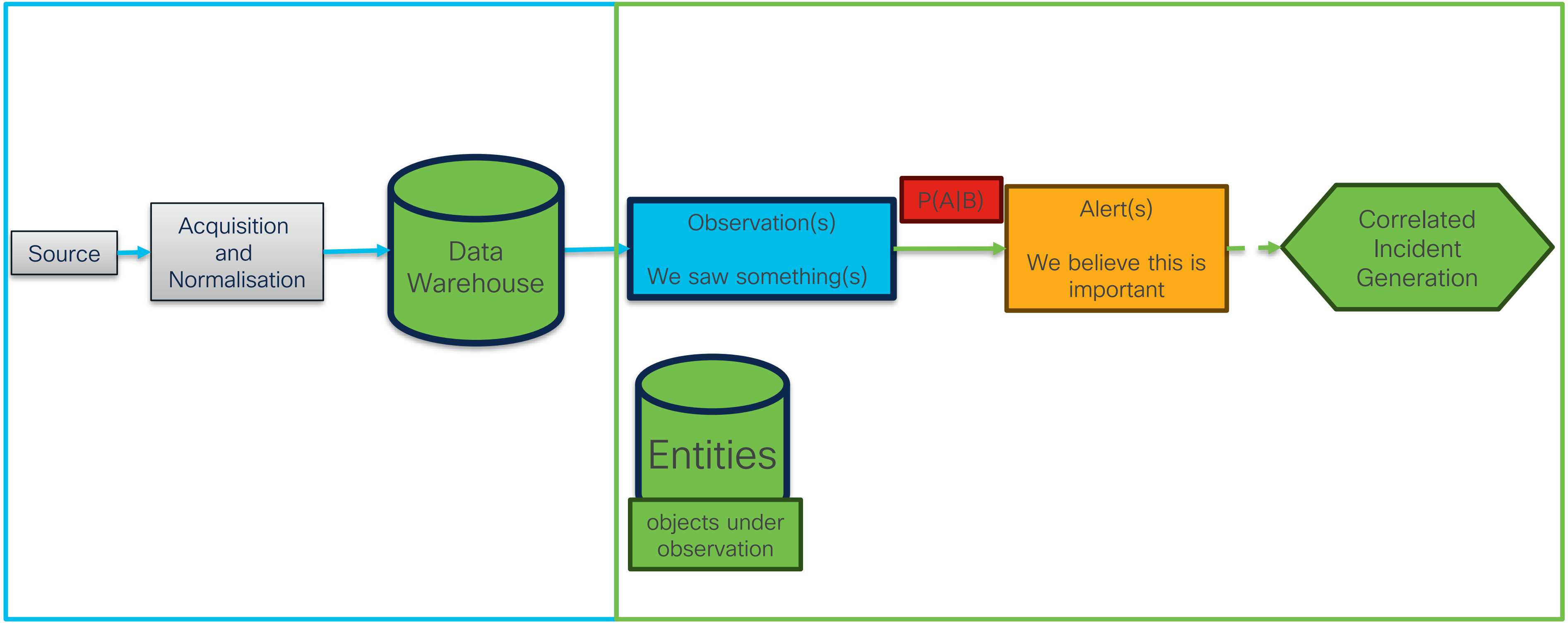


Details consolidated into Asset Inventory

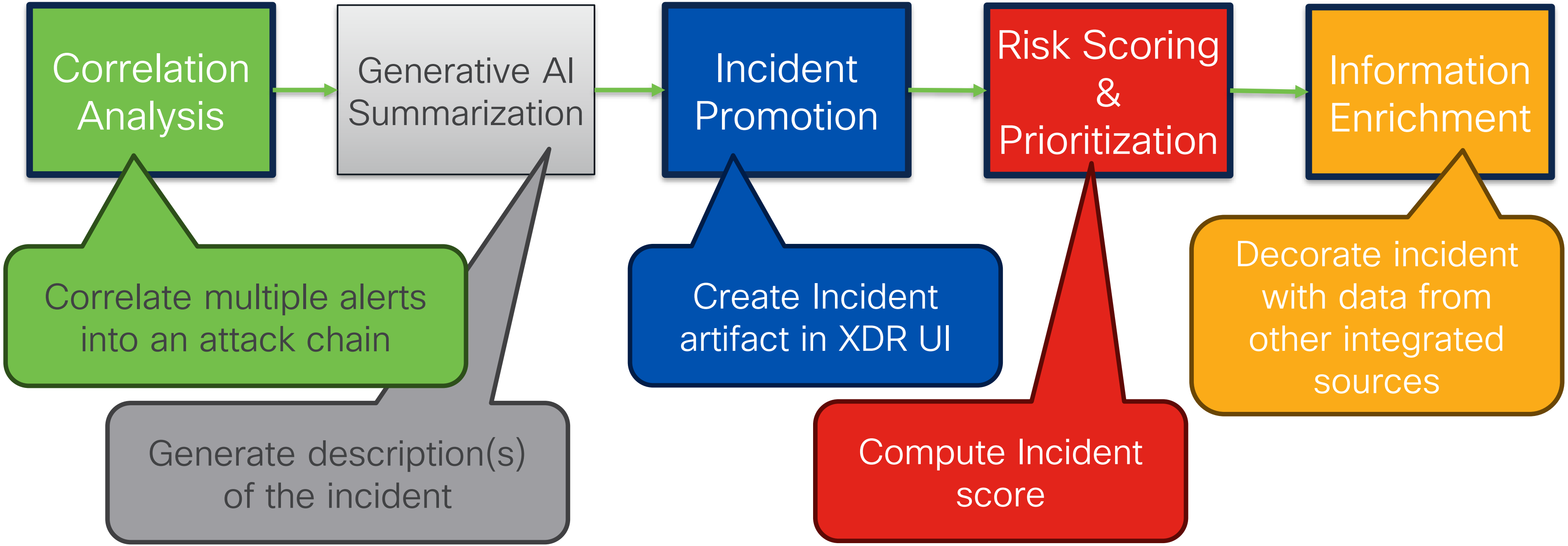


□	ALEX-WINDOWS11	Windows	11, SP 0.0 (Build 22621.3155)	ALEX-WINDOWS11\Alex	Meraki Systems Manager Secure Client Secure Endpoint - Cisco - Matthrob Umbrella	No
□	DARRIN-WINDOWS11	Windows	11, SP 0.0 (Build 22621.3447)	DARRIN-WINDOWS1\Darrin	Meraki Systems Manager Secure Client Secure Endpoint - Cisco - Matthrob Umbrella	No

XDR Data Analytics Pipeline


Source
Acquisition and Normalisation
Data Warehouse
Observation(s)
We saw something(s)
P(A|B)
Alert(s)
We believe this is important
Correlated Incident Generation
Entities
objects under observation

Correlated Incident Generation



Correlation Analysis → Generative AI Summarization → Incident Promotion → Risk Scoring & Prioritization → Information Enrichment

Correlate multiple alerts into an attack chain

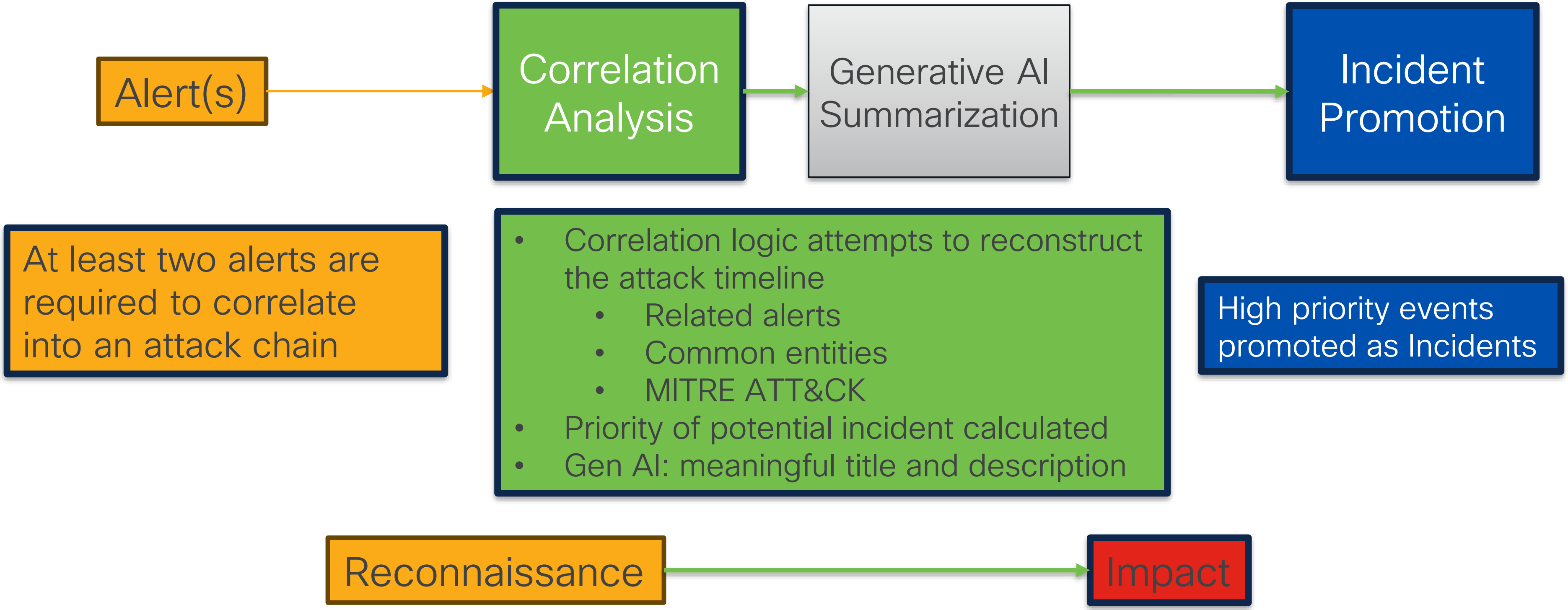
Generate description(s) of the incident

Create Incident artifact in XDR UI

Compute Incident score

Decorate incident with data from other integrated sources

Correlation Analysis: Attack Chains



Alert(s)

Correlation Analysis

Generative AI Summarization

Incident Promotion

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

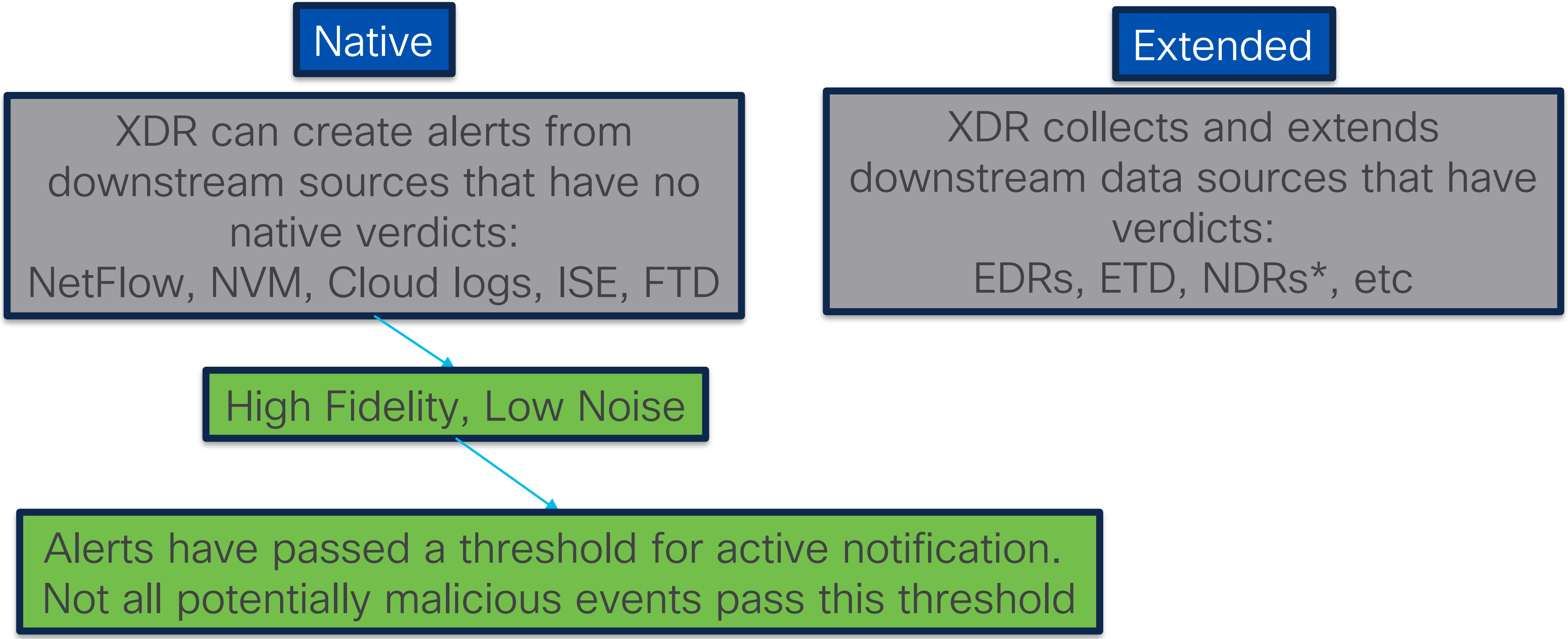
- Correlation logic attempts to reconstruct the attack timeline
  - Related alerts
  - Common entities
  - MITRE ATT&CK
- Priority of potential incident calculated
- Gen AI: meaningful title and description

High priority events promoted as Incidents

Reconnaissance

Impact

Native Detection vs Extended Detection



Native

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

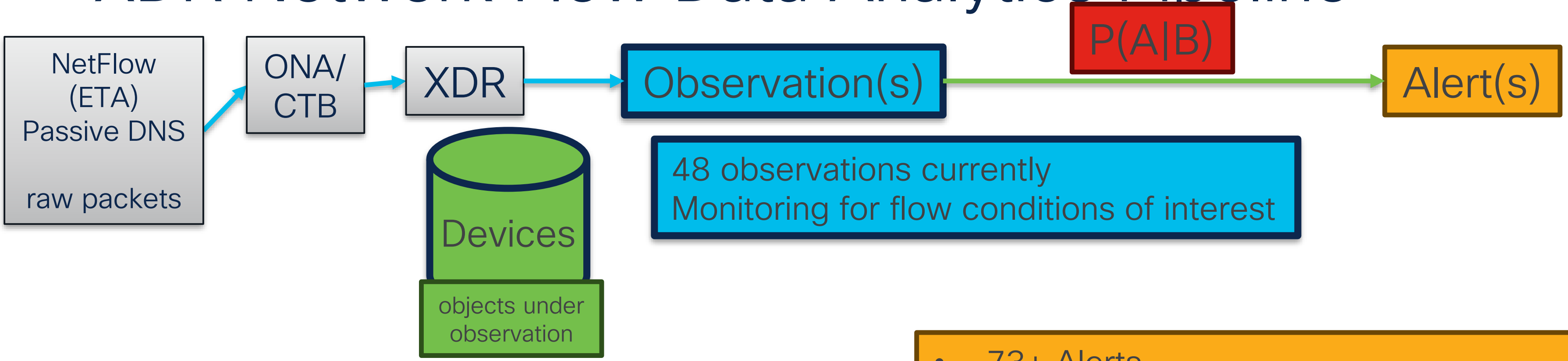
High Fidelity, Low Noise

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

XDR Network Flow Data Analytics Pipeline



NetFlow (ETA) Passive DNS

raw packets

ONA/ CTB

XDR

Devices

objects under observation

Observation(s)

P(A|B)

Alert(s)

48 observations currently
Monitoring for flow conditions of interest

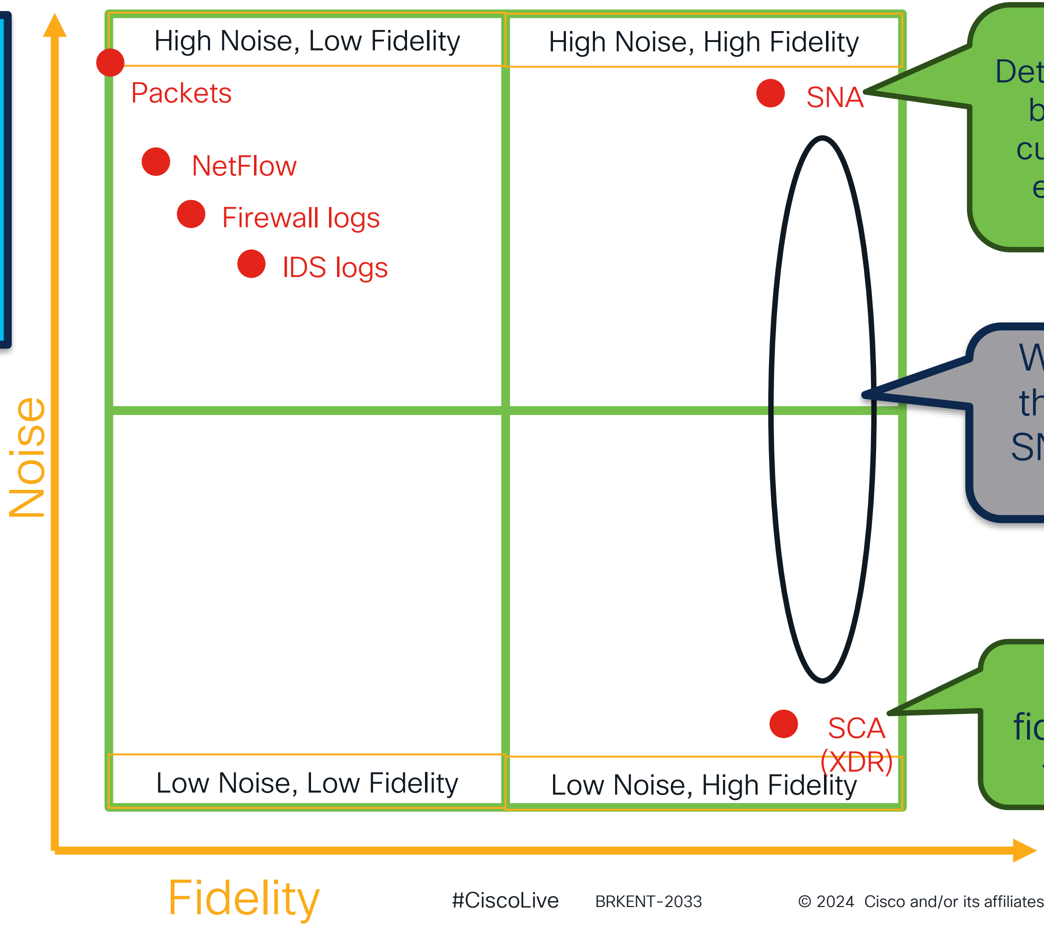
- NetFlow (incl. ETA), Passive DNS, Raw packets sent to:
  - Observable Network Appliance (ONA)
  - Cisco Telemetry Broker (CTB)
- Metadata extracted and sent to XDR
- Flow logs visible in Event Viewer
- Identify devices by IP Address, Hostname

- 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

NDR: Extracting security value from Network Data

Network telemetry is by nature high volume of data sets with minimal direct security outcomes associated

NDR's apply analytics to network to telemetry to ascertain security outcomes (i.e. create fidelity)



Detect as much as possible, broad alarm set, tuning, customisation required to extract maximum value

Whitespace: possible things to detect. (i.e. SNA detects more but tuning is required)

Alarm only for high fidelity events. minimal to no tuning options

Integrating Meraki with XDR and SNA

Dashboard Managed NetFlow Exporters

Meraki MX

NetFlow v9

Meraki MS390 & C9300-M

IPFIX enriched with Application and ETA

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

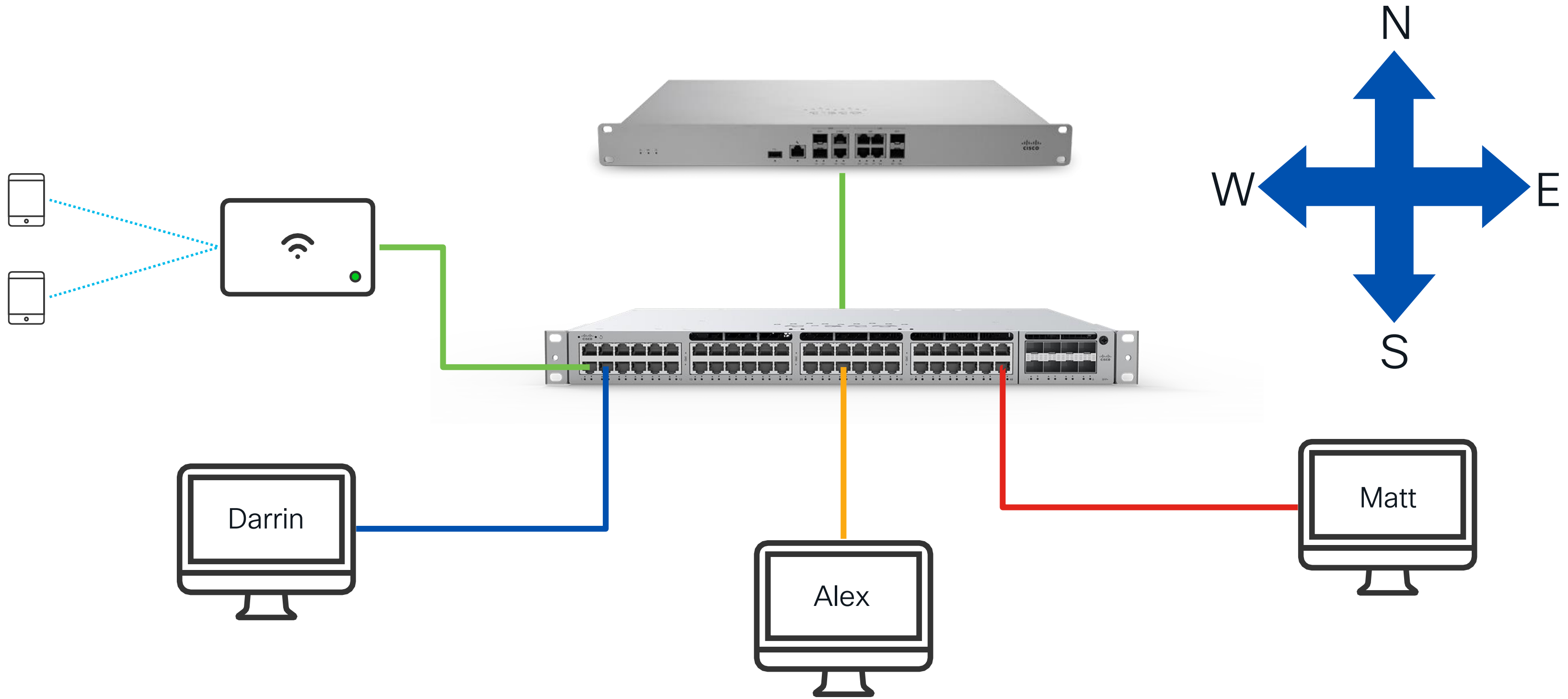
Security Policy:

Analyse network behaviour to design, implement and validate security policy

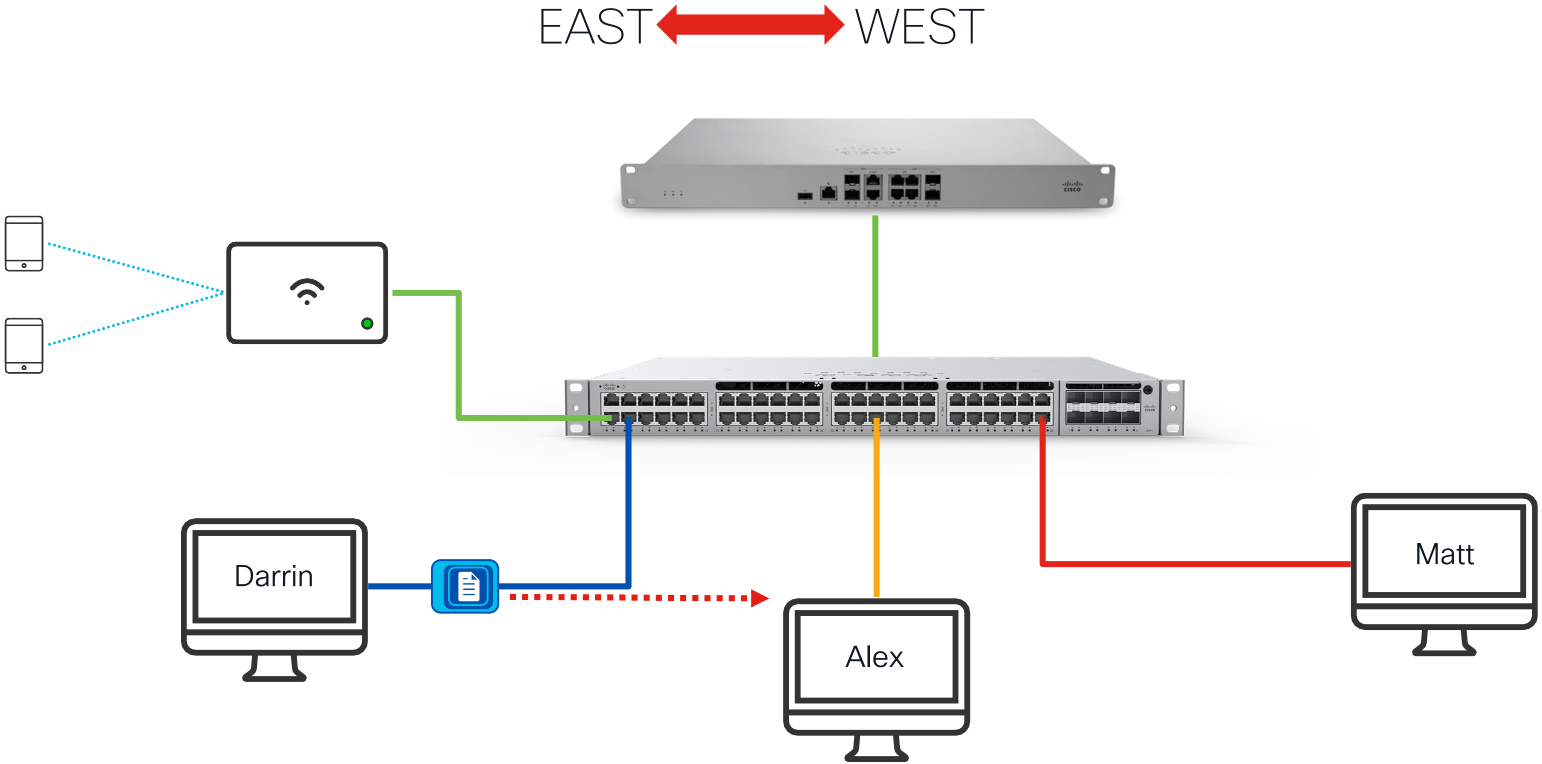
Threat **Detection:**

Analyse network behaviour to infer the presence of a threat actor

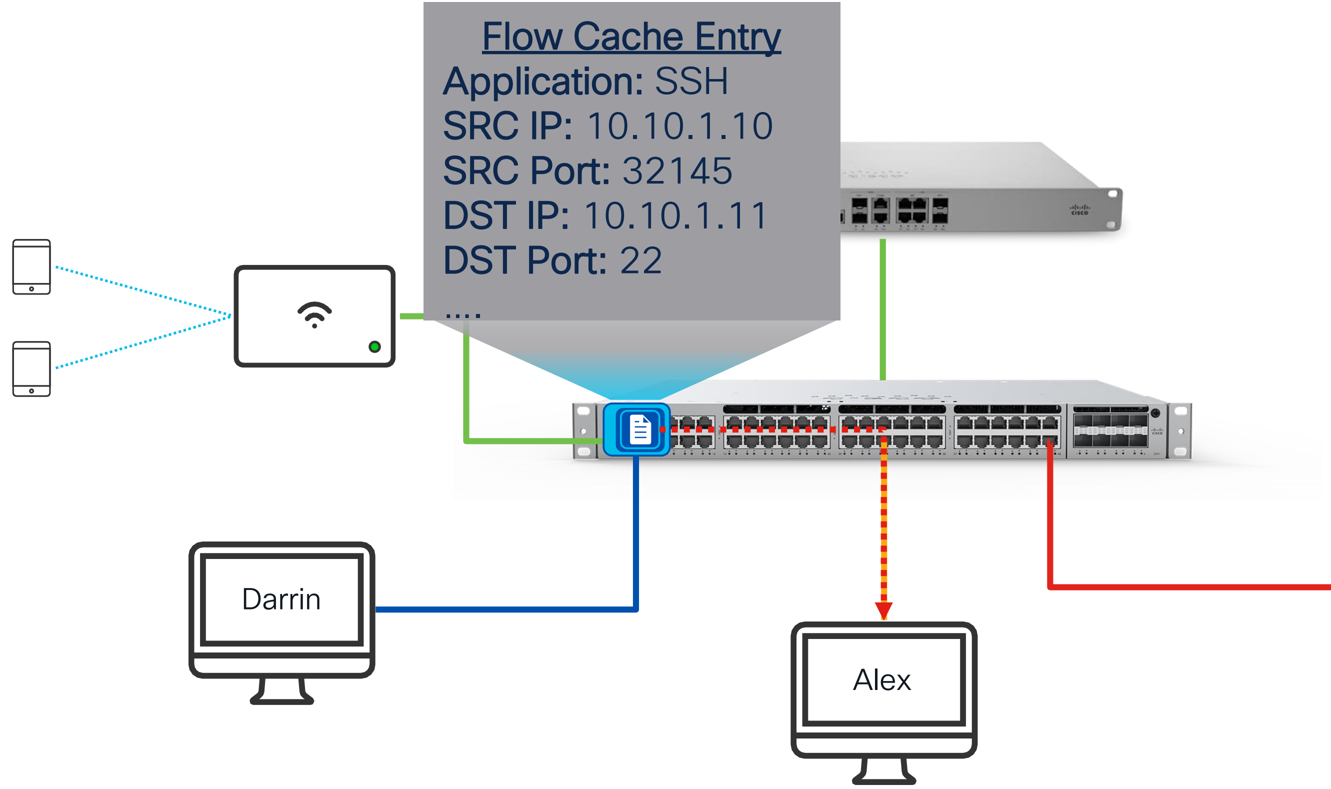
Where should you capture flows in a network?



Where should you capture flows in a network?



Where should you capture flows in a network?



Flow Cache Entry

Application: SSH

SRC IP: 10.10.1.10

SRC Port: 32145

DST IP: 10.10.1.11

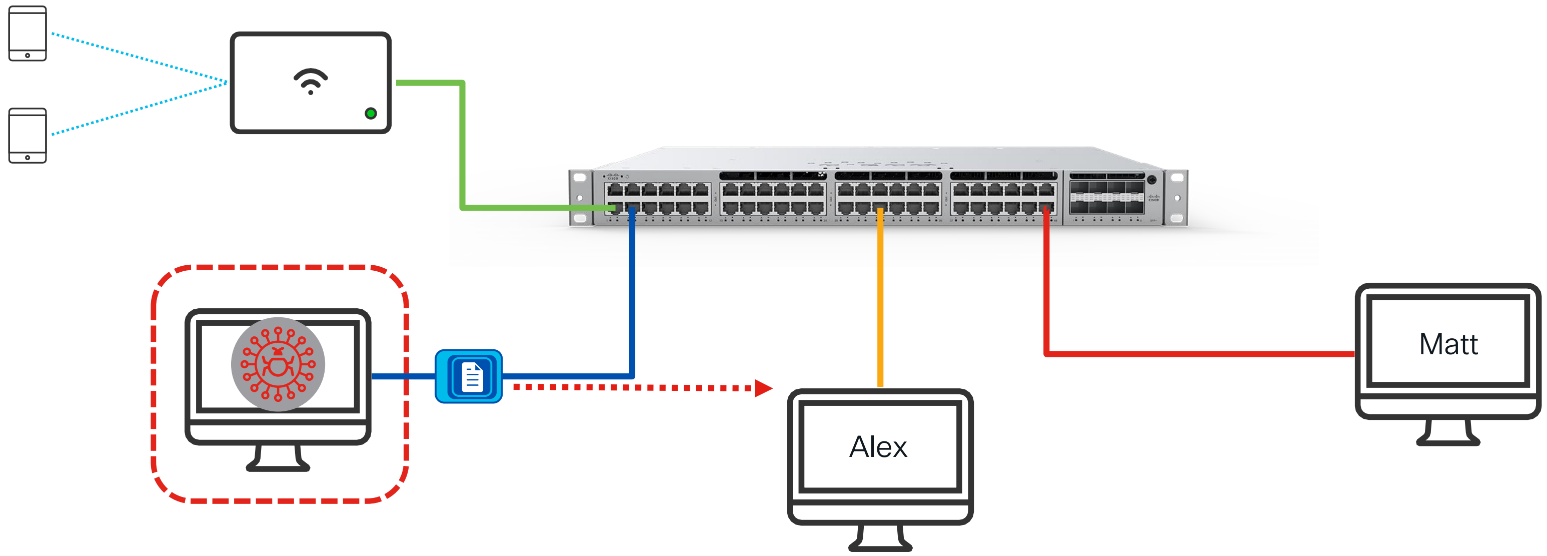
DST Port: 22

....

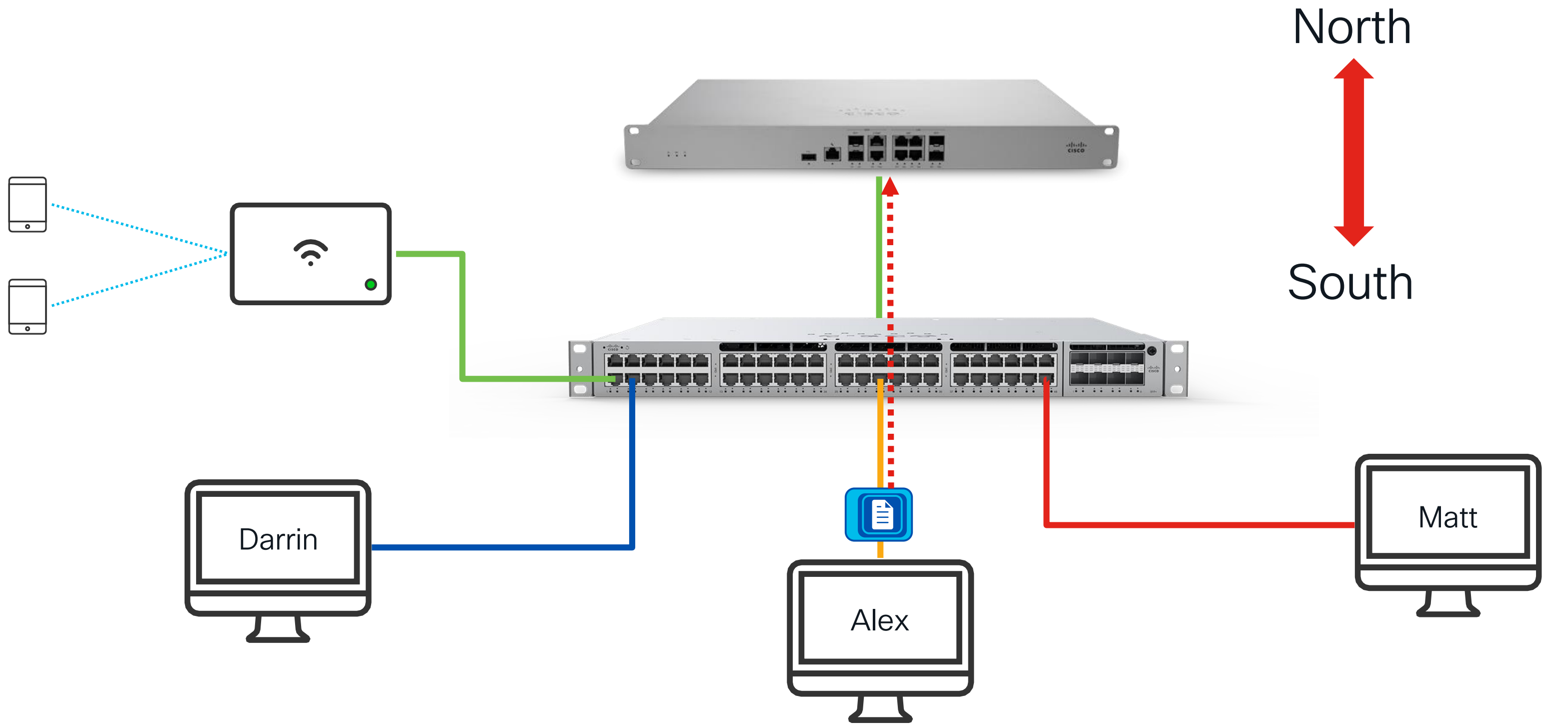
Why capture east-west traffic?

Visibility into

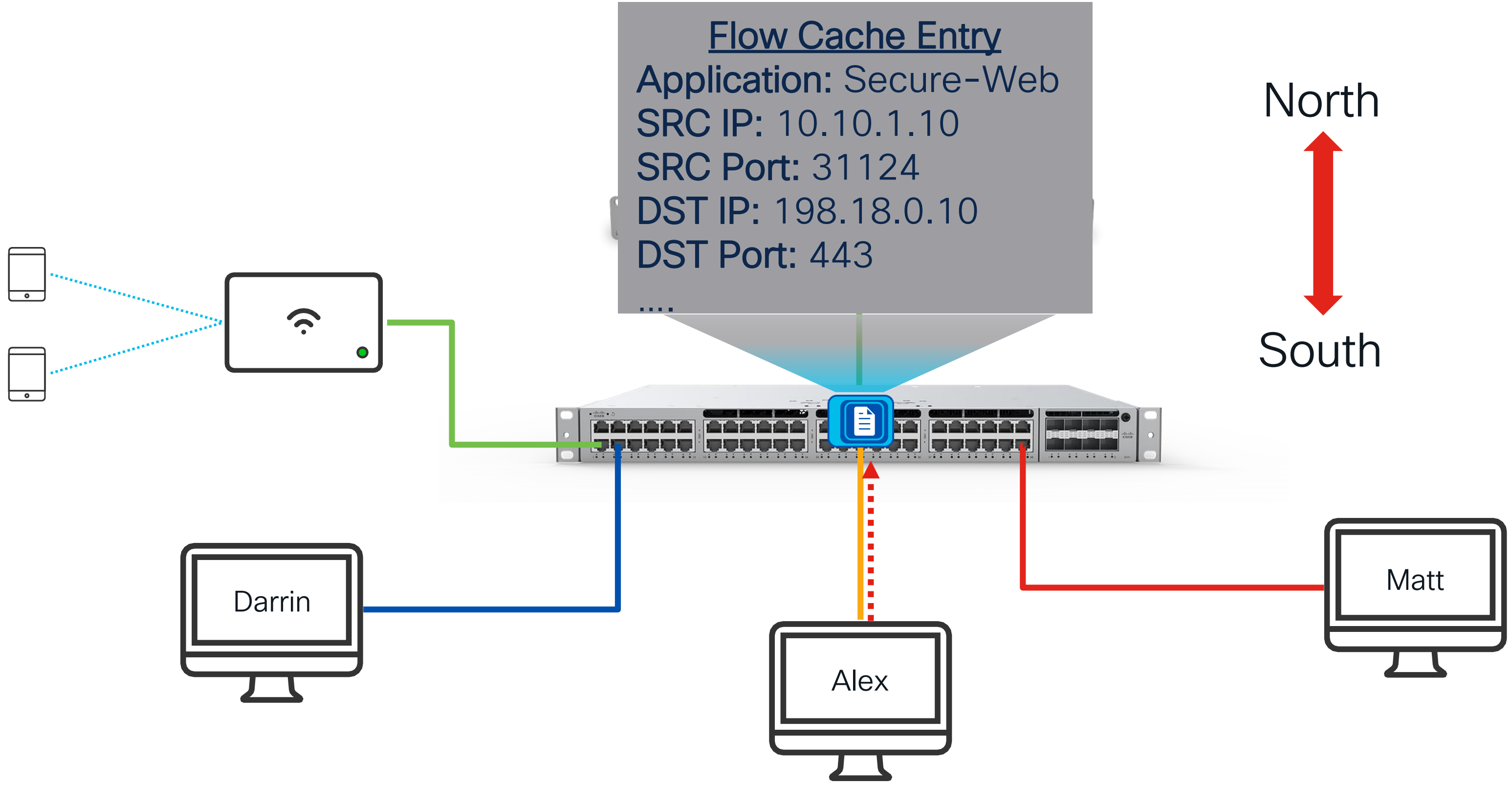
Vulnerability scanning
Lateral movement
Malicious package distribution
Valid communications for policy building



Where should you capture flows in a network?



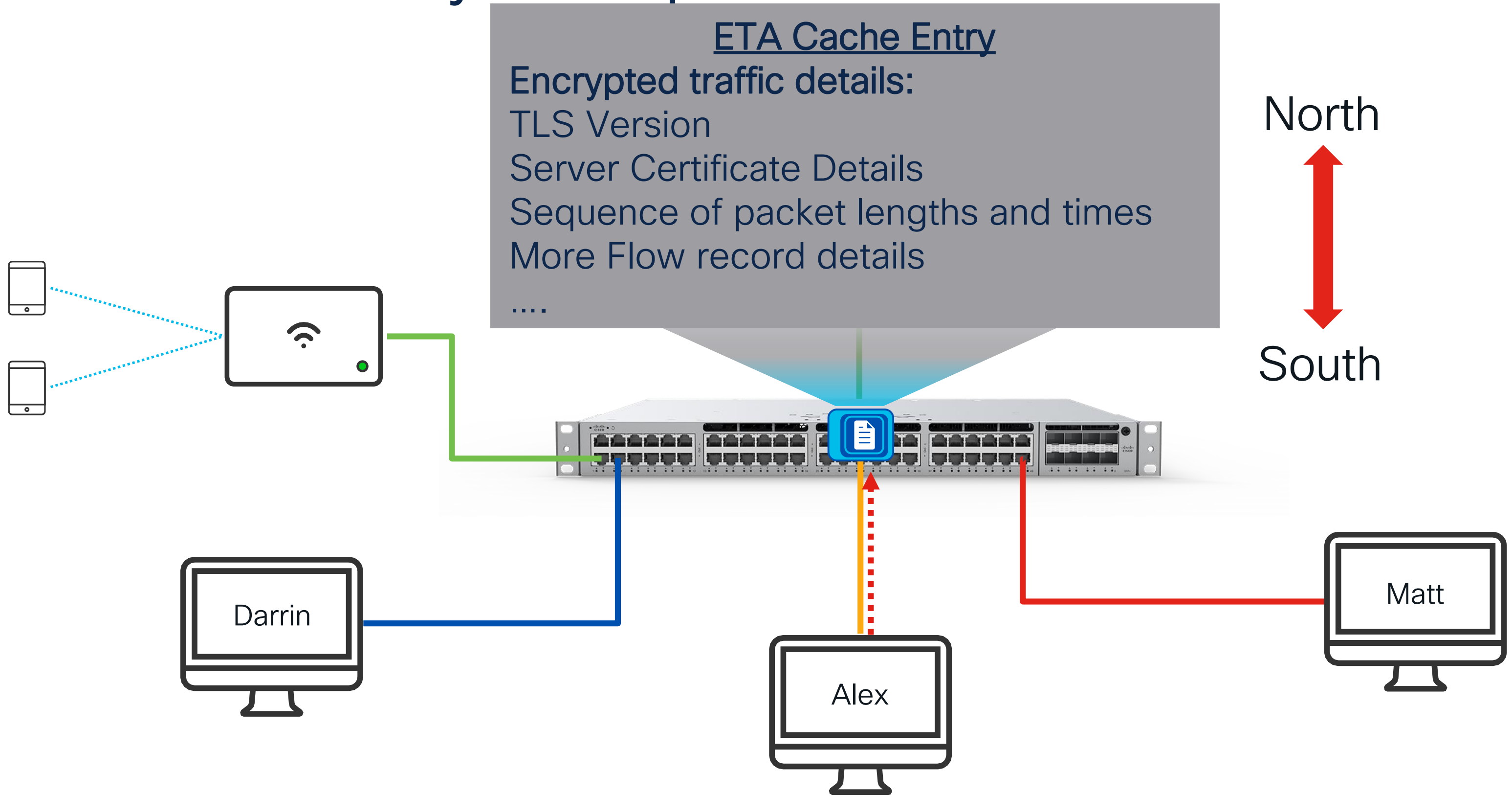
Where should you capture flows in a network?



Flow Cache Entry

Application: Secure-Web
SRC IP: 10.10.1.10
SRC Port: 31124
DST IP: 198.18.0.10
DST Port: 443
....

Where should you capture flows in a network?



ETA Cache Entry

Encrypted traffic details:

TLS Version

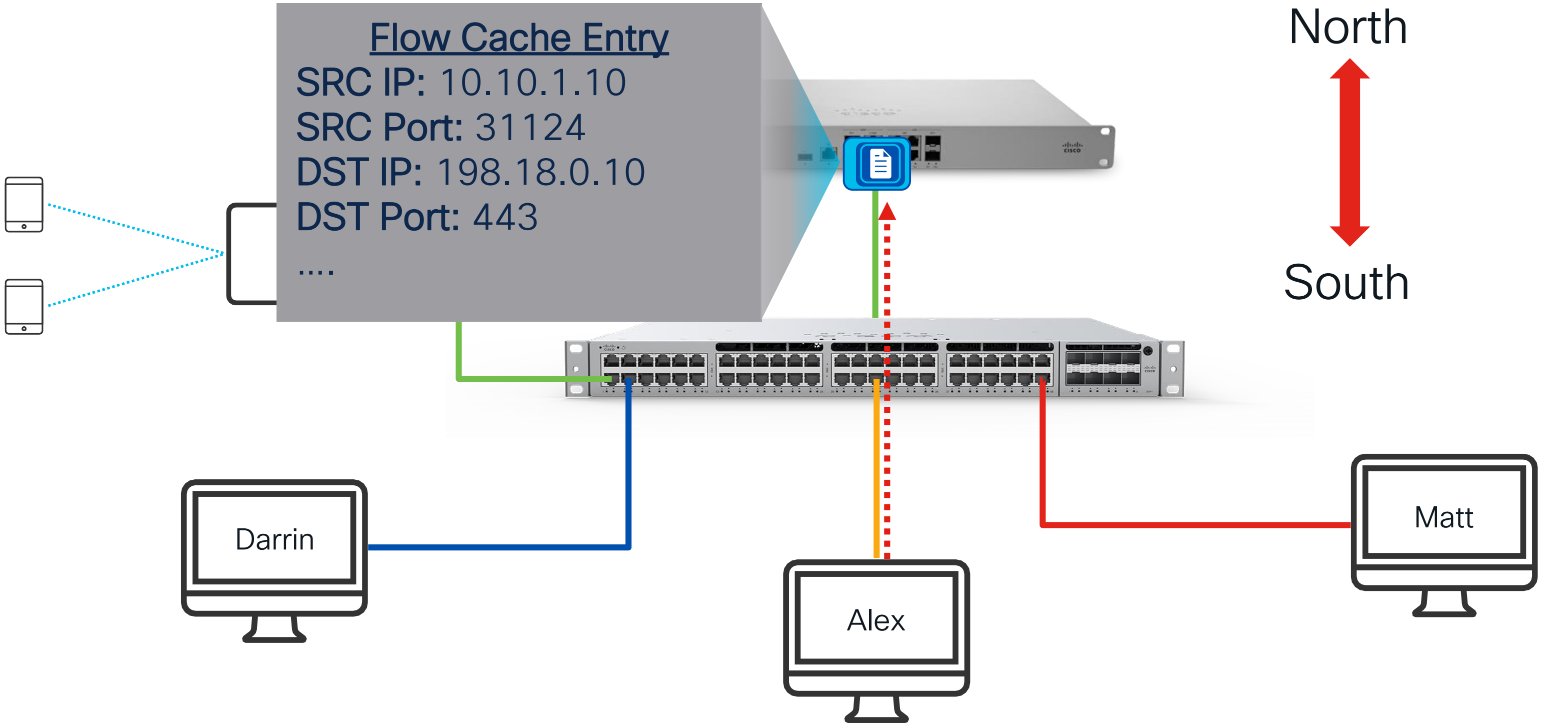
Server Certificate Details

Sequence of packet lengths and times

More Flow record details

....

Where should you capture flows in a network?



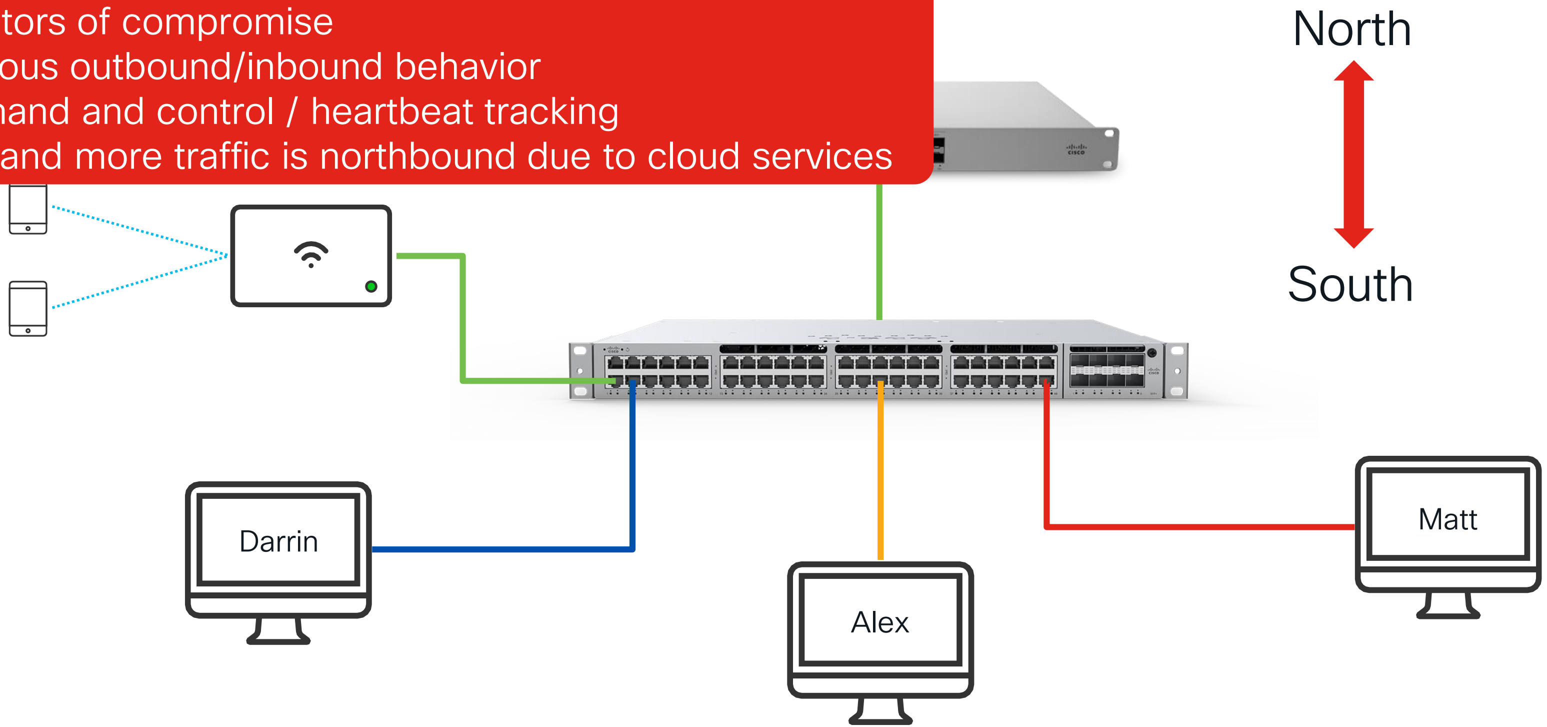
Flow Cache Entry

SRC IP: 10.10.1.10
SRC Port: 31124
DST IP: 198.18.0.10
DST Port: 443
....

Why capture north-south traffic?

Visibility into

- Indicators of compromise
- malicious outbound/inbound behavior
- command and control / heartbeat tracking
- More and more traffic is northbound due to cloud services



NetFlow and ETA details on the MS390/9300-M

CS NetFlow & Encrypted Traffic Analytics

Supported on all MS390/9300/X/L-M

AVC NetFlow

IPv4 and v6 records built for Cisco Secure Analytics

All East-West Traffic

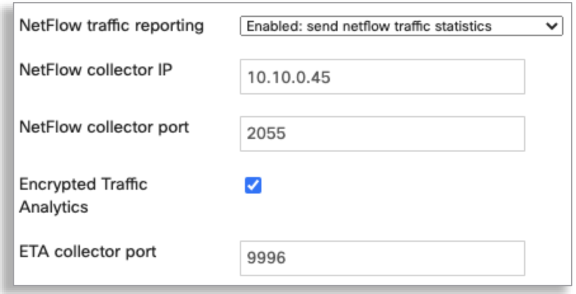
capturing flows on every client facing port on all supported switches in the network

Encrypted Traffic Analytics

for in-depth analysis of traffic without MiTM decryption

Adaptive Policy

Export of Source Security Group Tags (SGTs)

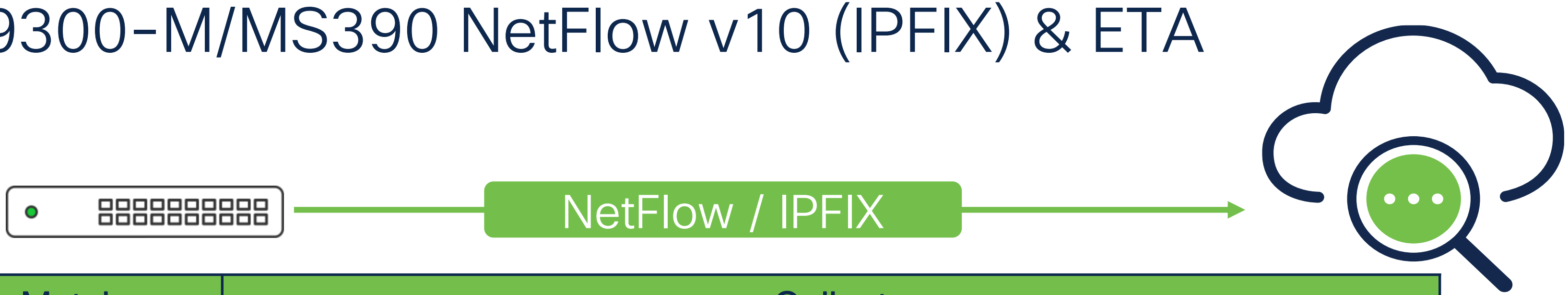


NetFlow traffic reporting	Enabled: send netflow traffic statistics
NetFlow collector IP	10.10.0.45
NetFlow collector port	2055
Encrypted Traffic Analytics	☑
ETA collector port	9996

Requires Advanced Licensing

https://documentation.meraki.com/MS/Monitoring_and_Reporting/MS_NetFlow_and_Encrypted_Traffic_Analytics

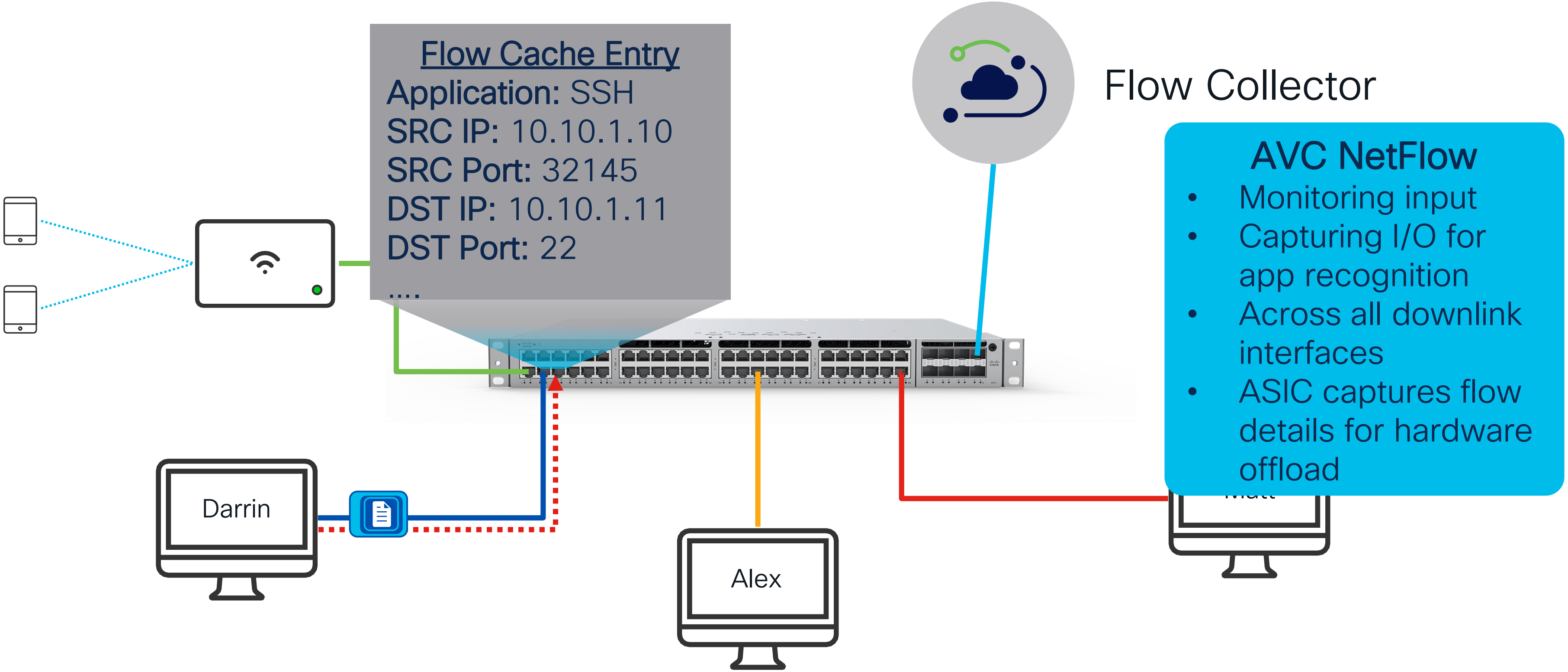
C9300-M/MS390 NetFlow v10 (IPFIX) & ETA



Match	Collect
Application	Security Group Tag
SRC/DST IP	Connection Client Location (IP, Port, Direction, VLAN, Observation Point)
SRC Interface	Connection Client Counters (Bytes, Packets, Timestamps, TCP flags)
SRC / DST Port	Connection State (Server, Source Port, Dest Port, Initiator)
Protocol	

Encrypted Traffic Analytics
Initial Data Packet
Sequence of Packets Lengths and Times
Byte Distribution

Flow Capture on CS (390/9300)



Flow Cache Entry

Application: SSH
SRC IP: 10.10.1.10
SRC Port: 32145
DST IP: 10.10.1.11
DST Port: 22
....

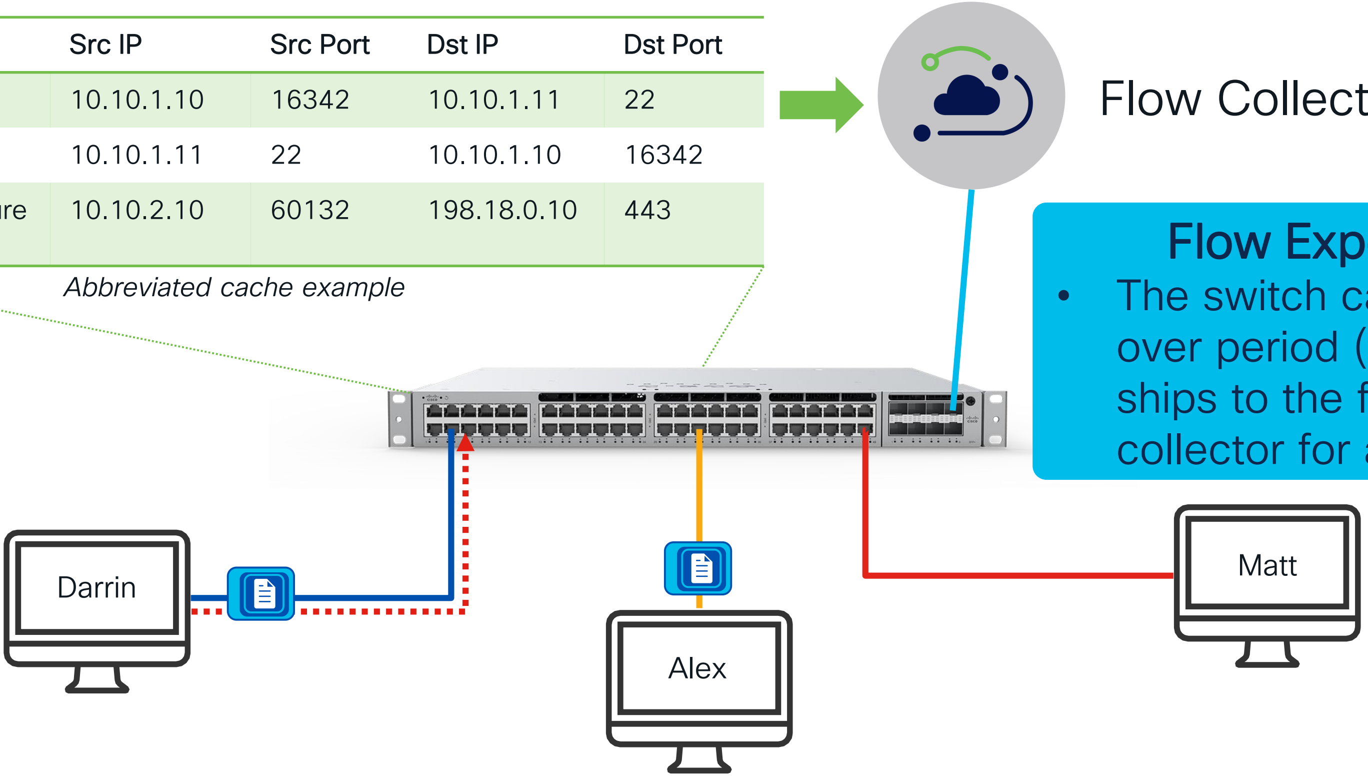
AVC NetFlow

- Monitoring input
- Capturing I/O for app recognition
- Across all downlink interfaces
- ASIC captures flow details for hardware offload

Flow Export on CS (390/9300)

Src Port	App	Src IP	Src Port	Dst IP	Dst Port
Port 4	SSH	10.10.1.10	16342	10.10.1.11	22
Port 36	SSH	10.10.1.11	22	10.10.1.10	16342
Port 48	Secure Web	10.10.2.10	60132	198.18.0.10	443

Abbreviated cache example

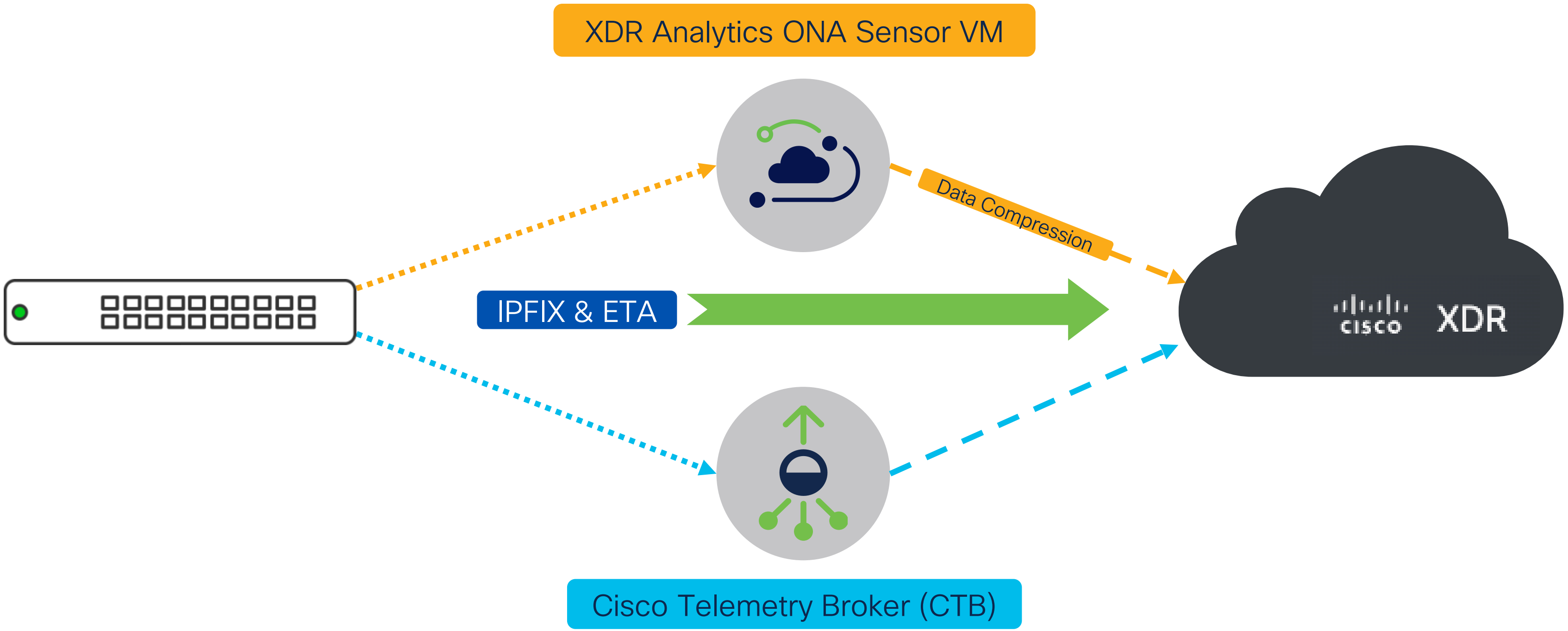


Flow Exporting

- The switch caches flows over period (60s) and ships to the flow collector for analysis

How do we get this telemetry into XDR?

Getting Flows into XDR from MS390/9300


XDR Analytics ONA Sensor VM

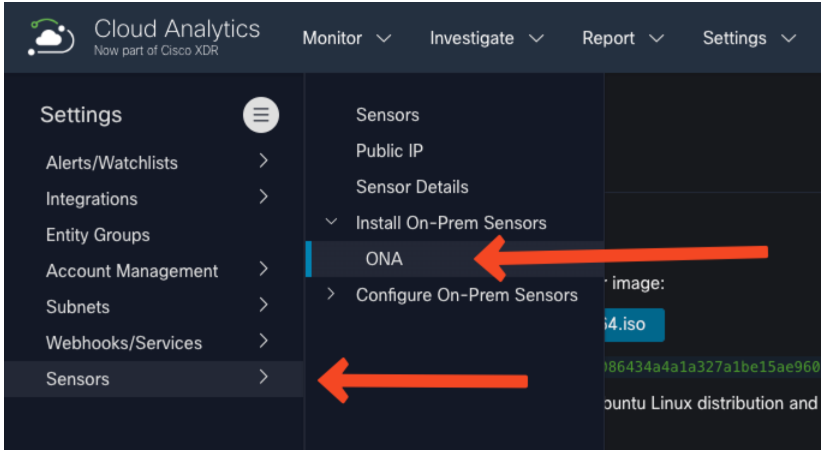
Cisco Telemetry Broker (CTB)

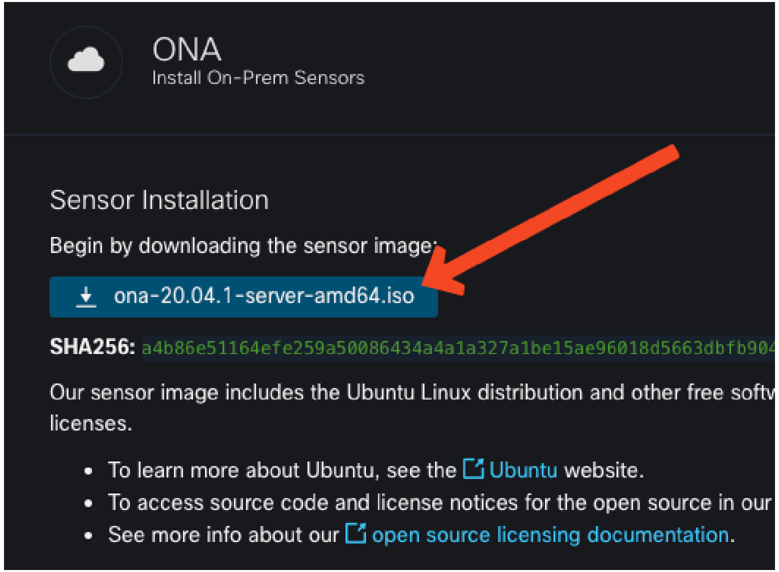
XDR Secure Cloud Analytics ONA Sensor Install

1. Log into XDR Analytics (SCA) and navigate to sensors
2. Download the ONA Sensor Appliance ISO
3. Install in virtual environment and set a static IP address
4. Validate connectivity in XDR dashboard
5. Program the IPFIX/NetFlow/ETA port configurations in XDR Analytics for the sensor

Login to XDR Analytics Download the ISO

Secure Cloud Analytics Web Interface




ONA
Install On-Prem Sensors

Sensor Installation

Begin by downloading the sensor image:

ona-20.04.1-server-amd64.iso

SHA256: a4b86e51164efe259a50086434a4a1a327a1be15ae96018d5663dbfb904

Our sensor image includes the Ubuntu Linux distribution and other free softw licenses.

- To learn more about Ubuntu, see the Ubuntu website.
- To access source code and license notices for the open source in our
- See more info about our open source licensing documentation.

Install in a virtual environment

ONA server appliance = Ubuntu 22.04 + Fancy Packages

PROXMOX

XCP-ng

VMware vSphere®

Microsoft Hyper-V

KVM

VirtualBox ORACLE

CPUs : 2+

Memory : 2GB+

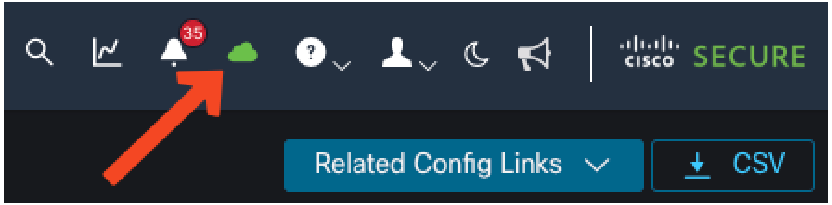
Storage : 32GB+

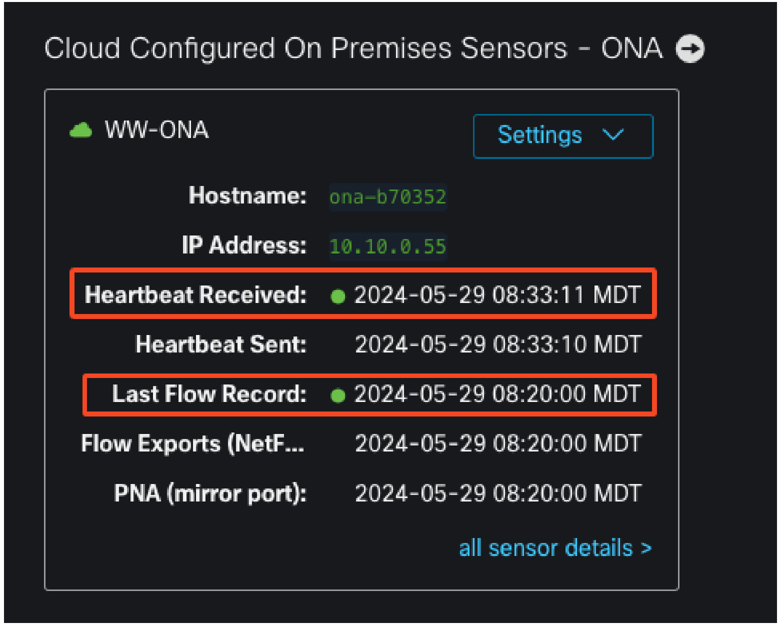
Network :
1x interface if only collecting flows
2x if using SPAN for raw traffic analysis

https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/cloud/deployment/Sensor_Installation_Guide_DV_1_3.pdf

Validate Sensor Connectivity to XDR

Secure Cloud Analytics Web Interface




Cloud Configured On Premises Sensors - ONA

WW-ONA

Hostname: ona-b70352

IP Address: 10.10.0.55

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

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

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

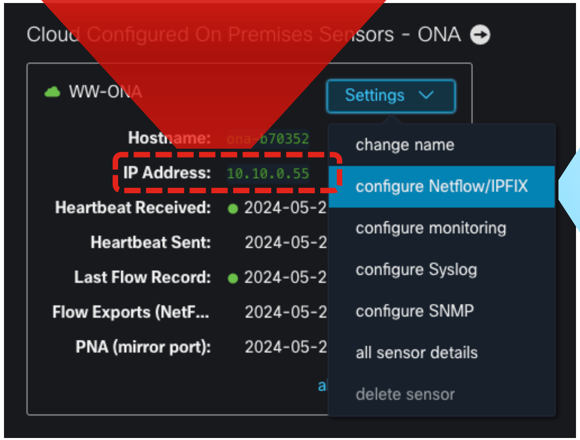
Flow Exports (NetF... 2024-05-29 08:20:00 MDT

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

all sensor details >

Configure IPFIX/ETA/NetFlow

Sensor IP address



Cloud Configured On Premises Sensors - ONA

WW-ONA

Hostname: ona-b70352

IP Address: 10.10.0.55

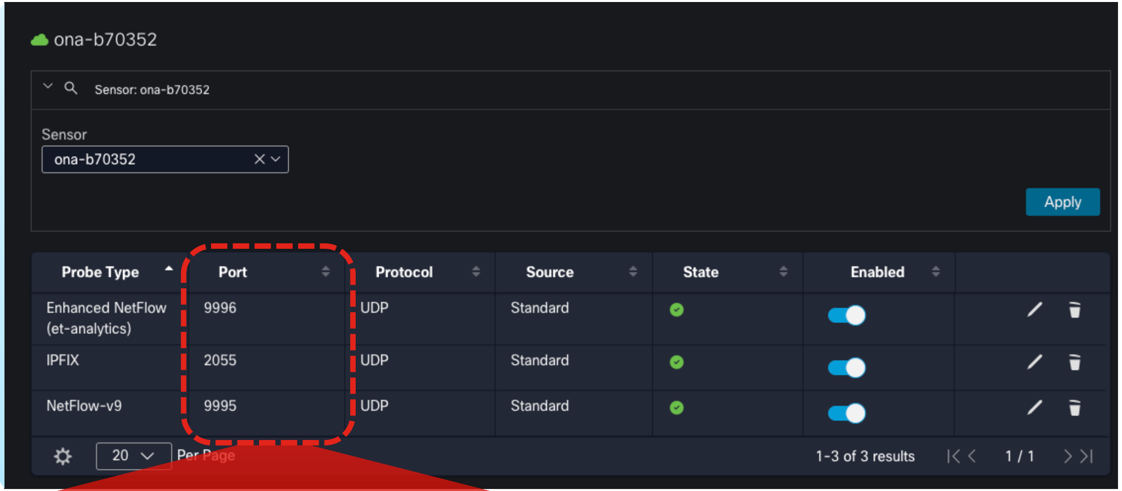
Heartbeat Received: ● 2024-05-2

Heartbeat Sent: 2024-05-2

Last Flow Record: ● 2024-05-2

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

PNA (mirror port): 2024-05-2



ona-b70352

Sensor: ona-b70352

Sensor: ona-b70352

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

20 Per Page   1-3 of 3 results   1 / 1

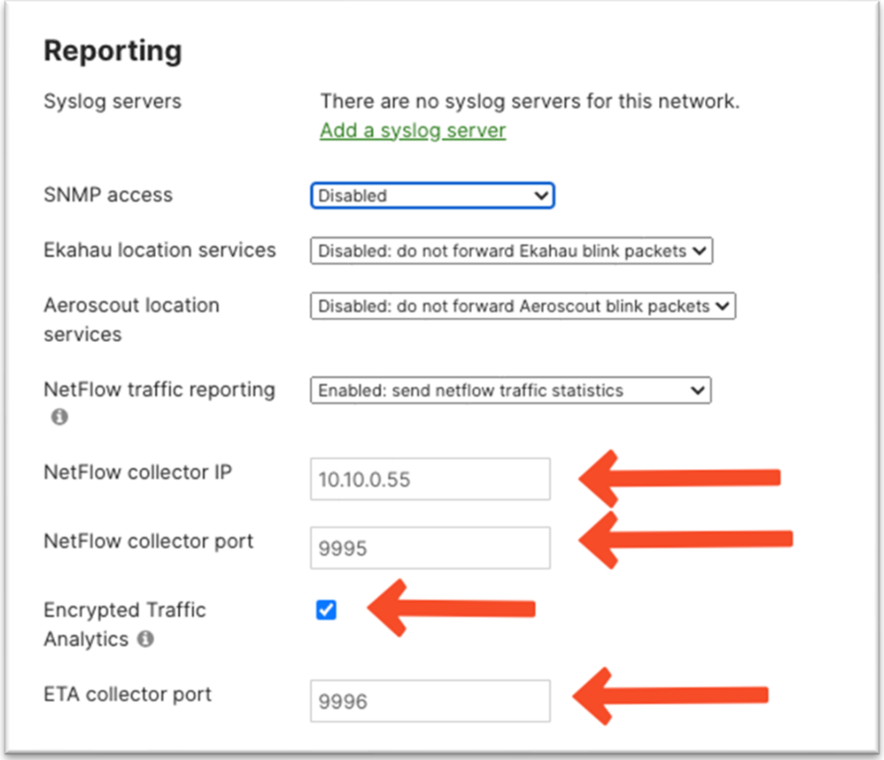
Port/s to use for flow export configuration in dashboard

Configuring NetFlow / ETA Exporting in Dashboard

Network-wide > General > Reporting

CS Enablement
Network Wide Enablement on all supported switches with an SVI configured

MX Enablement
MX in the network will ship flows from LAN to WAN



Reporting

Syslog servers: There are no syslog servers for this network. Add a syslog server

SNMP access: Disabled

Ekahau location services: Disabled: do not forward Ekahau blink packets

Aeroscout location services: Disabled: do not forward Aeroscout blink packets

NetFlow traffic reporting: Enabled: send netflow traffic statistics

NetFlow collector IP: 10.10.0.55

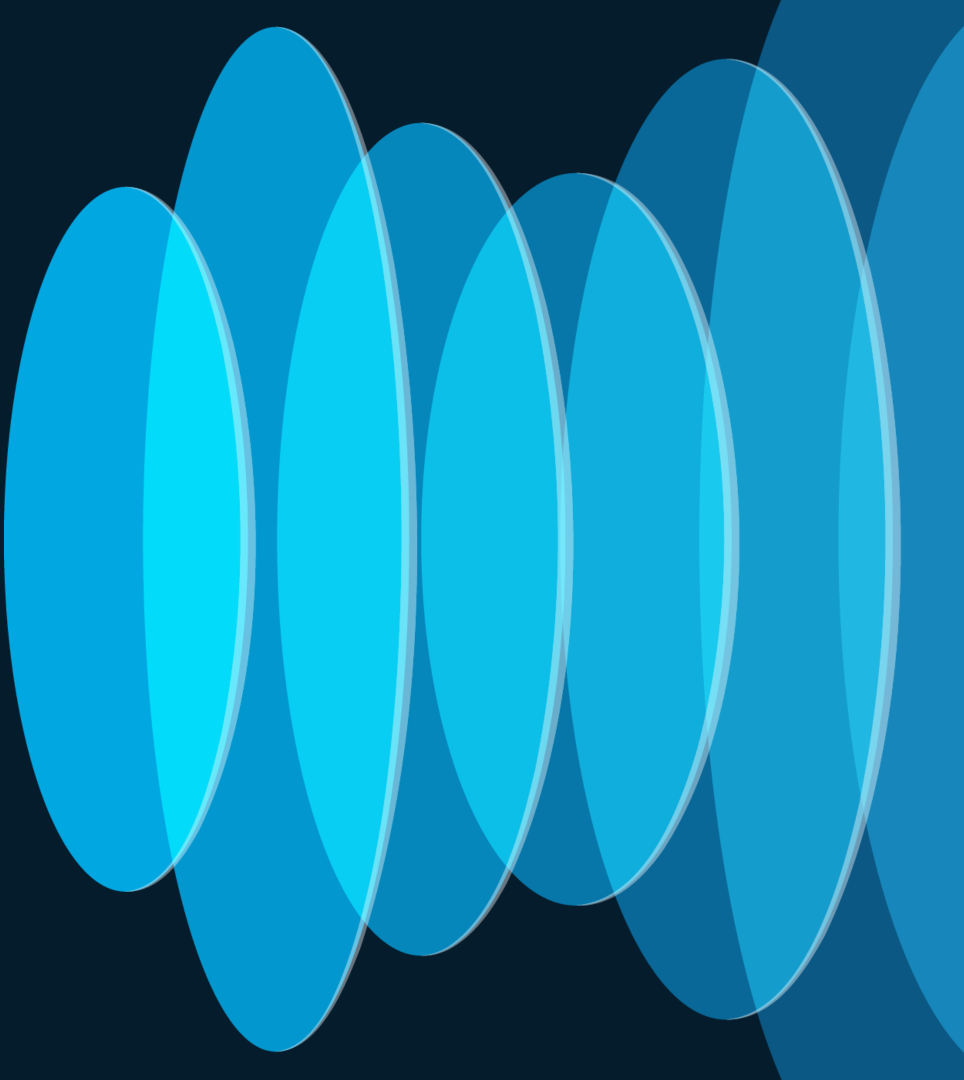
NetFlow collector port: 9995

Encrypted Traffic Analytics: ☑

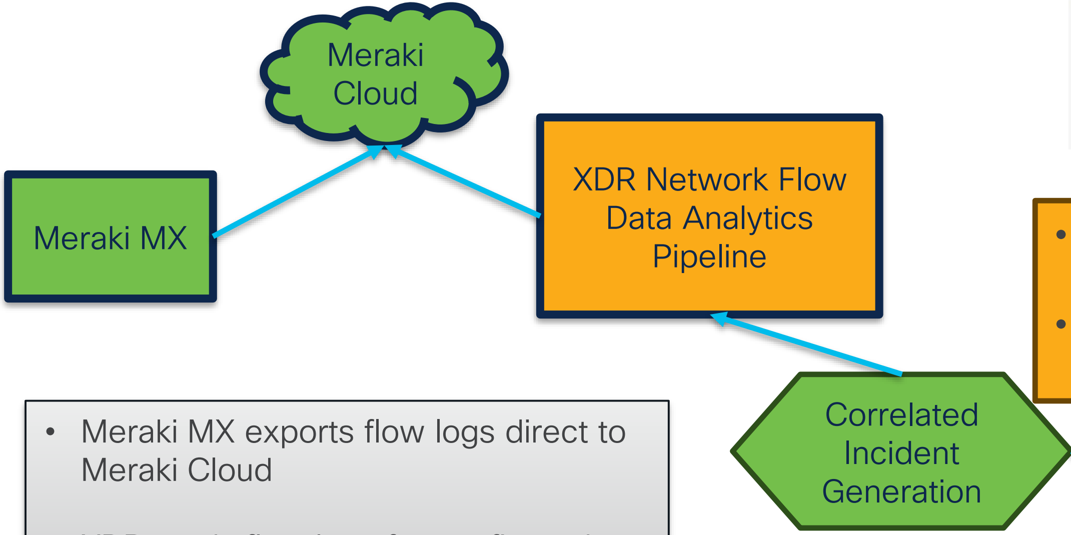
ETA collector port: 9996

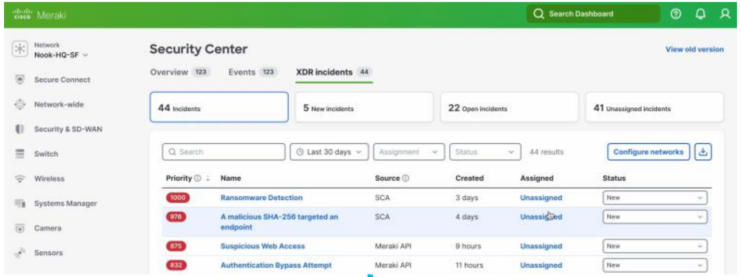
Demo

Introducing something new!



Coming Soon: Meraki MX!


Meraki Cloud
Meraki MX
XDR Network Flow Data Analytics Pipeline
Correlated Incident Generation



Security Center

View old version

Overview 123 | Events 123 | XDR incidents 44

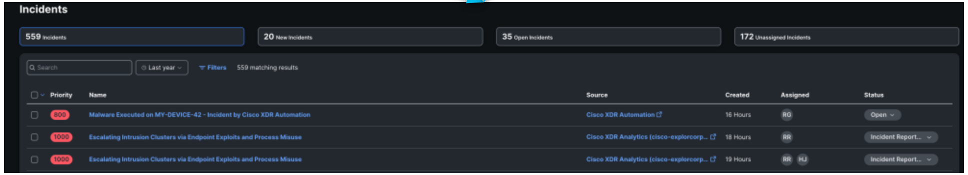
44 Incidents | 5 New incidents | 22 Open incidents | 41 Unassigned incidents

Search | Last 30 days | Assignment | Status | 44 results | Configure networks

Priority	Name	Source	Created	Assigned	Status
1000	Ransomware Detection	SCA	3 days	Unassigned	New
978	A malicious SHA-256 targeted an endpoint	SCA	4 days	Unassigned	New
875	Suspicious Web Access	Meraki API	9 hours	Unassigned	New
832	Authentication Bypass Attempt	Meraki API	11 hours	Unassigned	New

- 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



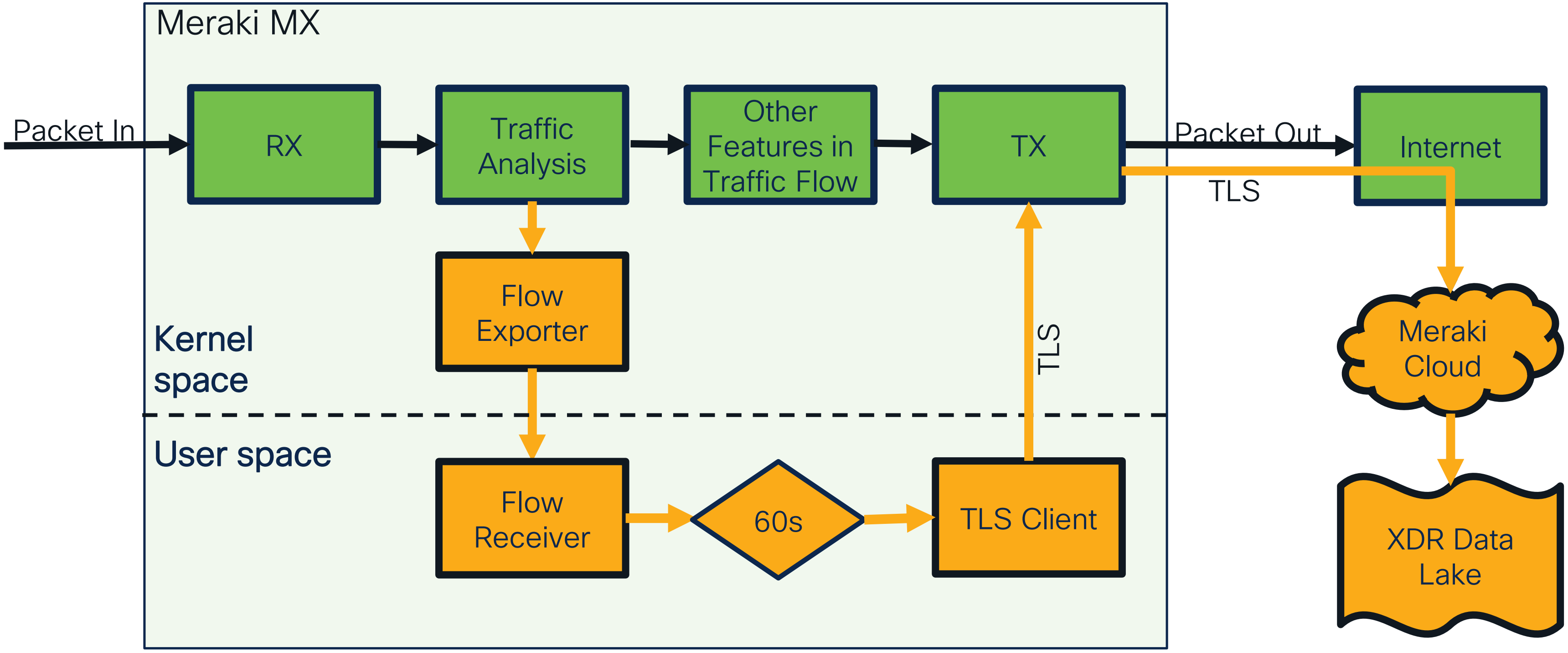
Incidents

559 Incidents | 20 New Incidents | 35 Open Incidents | 172 Unassigned Incidents

Search | Last year | Filters | 559 matching results

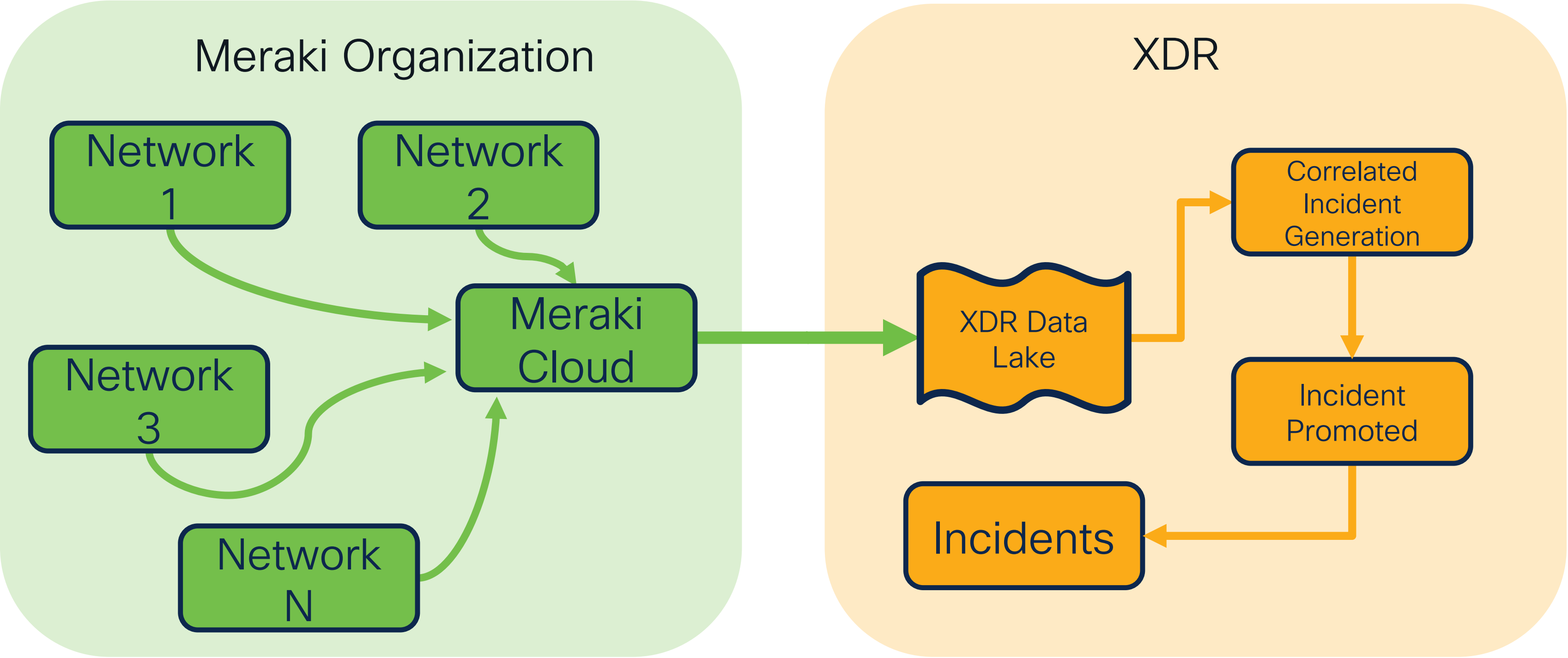
Priority	Name	Source	Created	Assigned	Status
800	Malware Executed on MY-DEVICE-42 - Incident by Cisco XDR Automation	Cisco XDR Automation	16 Hours	RG	Open
1000	Escalating Intrusion Clusters via Endpoint Exploits and Process Misuse	Cisco XDR Analytics (cisco-explorcorp...	18 Hours	RR	Incident Report...
1000	Escalating Intrusion Clusters via Endpoint Exploits and Process Misuse	Cisco XDR Analytics (cisco-explorcorp...	19 Hours	RR HJ	Incident Report...

Close Up: MX Telemetry Packet Flow



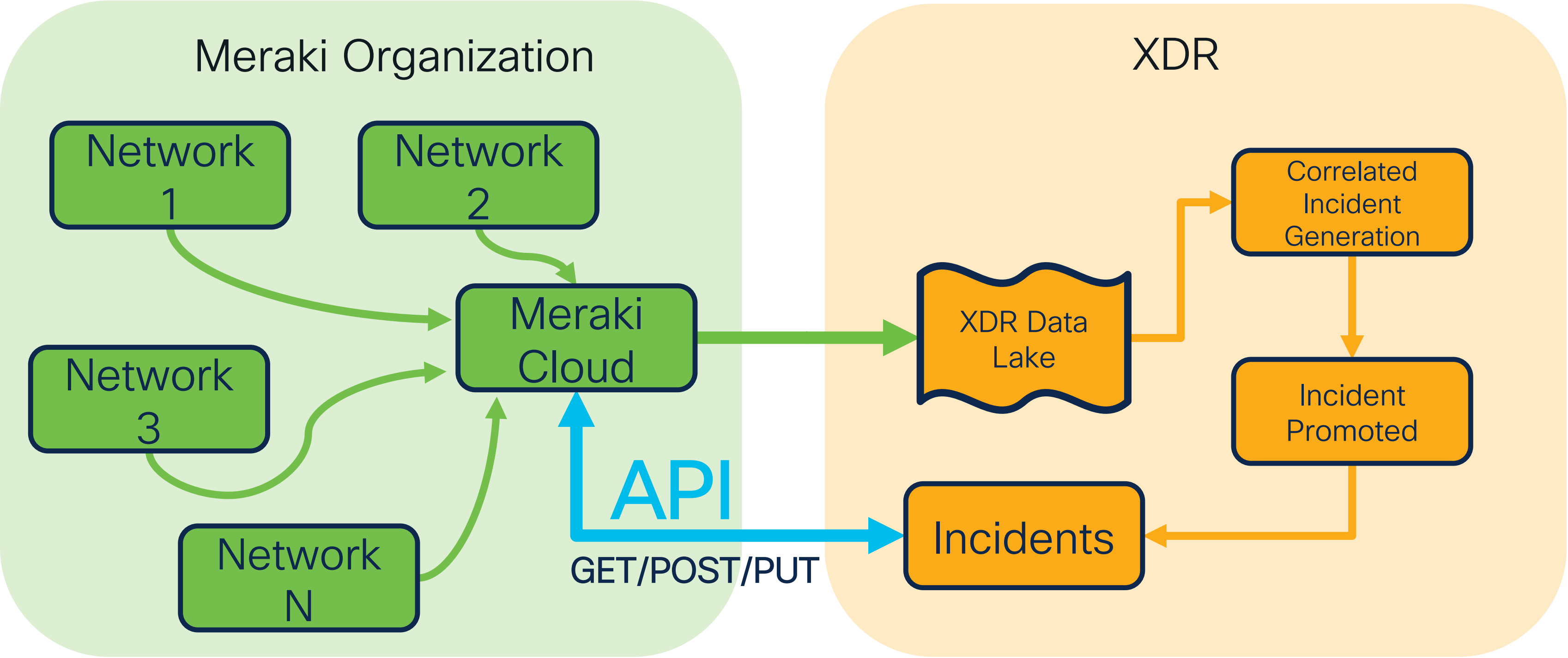
MX & XDR Integration

High-level Overview

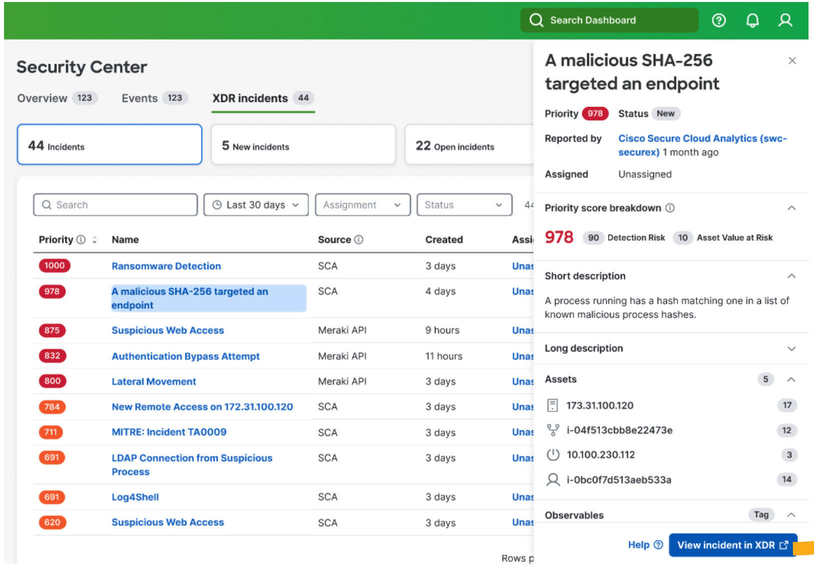


MX & XDR Integration

High-level Overview: API



Bringing the SOC to the Meraki Dashboard



Security Center

Overview 123 | Events 123 | XDR incidents 44

44 Incidents | 5 New incidents | 22 Open incidents

Search | Last 30 days | Assignment | Status | 44

Priority	Name	Source	Created	Assi
1000	Ransomware Detection	SCA	3 days	Unas
978	A malicious SHA-256 targeted an endpoint	SCA	4 days	Unas
875	Suspicious Web Access	Meraki API	9 hours	Unas
832	Authentication Bypass Attempt	Meraki API	11 hours	Unas
800	Lateral Movement	Meraki API	3 days	Unas
784	New Remote Access on 172.31.100.120	SCA	3 days	Unas
711	MITRE: Incident TA0009	SCA	3 days	Unas
691	LDAP Connection from Suspicious Process	SCA	3 days	Unas
691	Log4Shell	SCA	3 days	Unas
620	Suspicious Web Access	SCA	3 days	Unas

Rows p

A malicious SHA-256 targeted an endpoint

Priority 978 Status New

Reported by Cisco Secure Cloud Analytics (swc-securex) 1 month ago

Assigned Unassigned

Priority score breakdown

978 90 Detection Risk 10 Asset Value at Risk

Short description

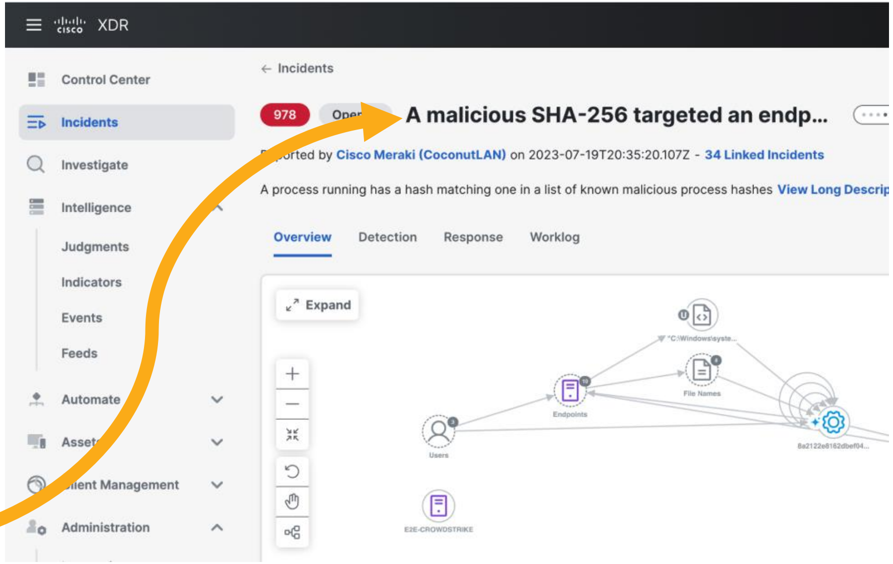
A process running has a hash matching one in a list of known malicious process hashes.

Long description

Assets 5

Asset	
173.31.100.120	17
i-04f513cbb8e22473e	12
10.100.230.112	3
i-0bc0f7d513aeb533a	14

Observables Tag

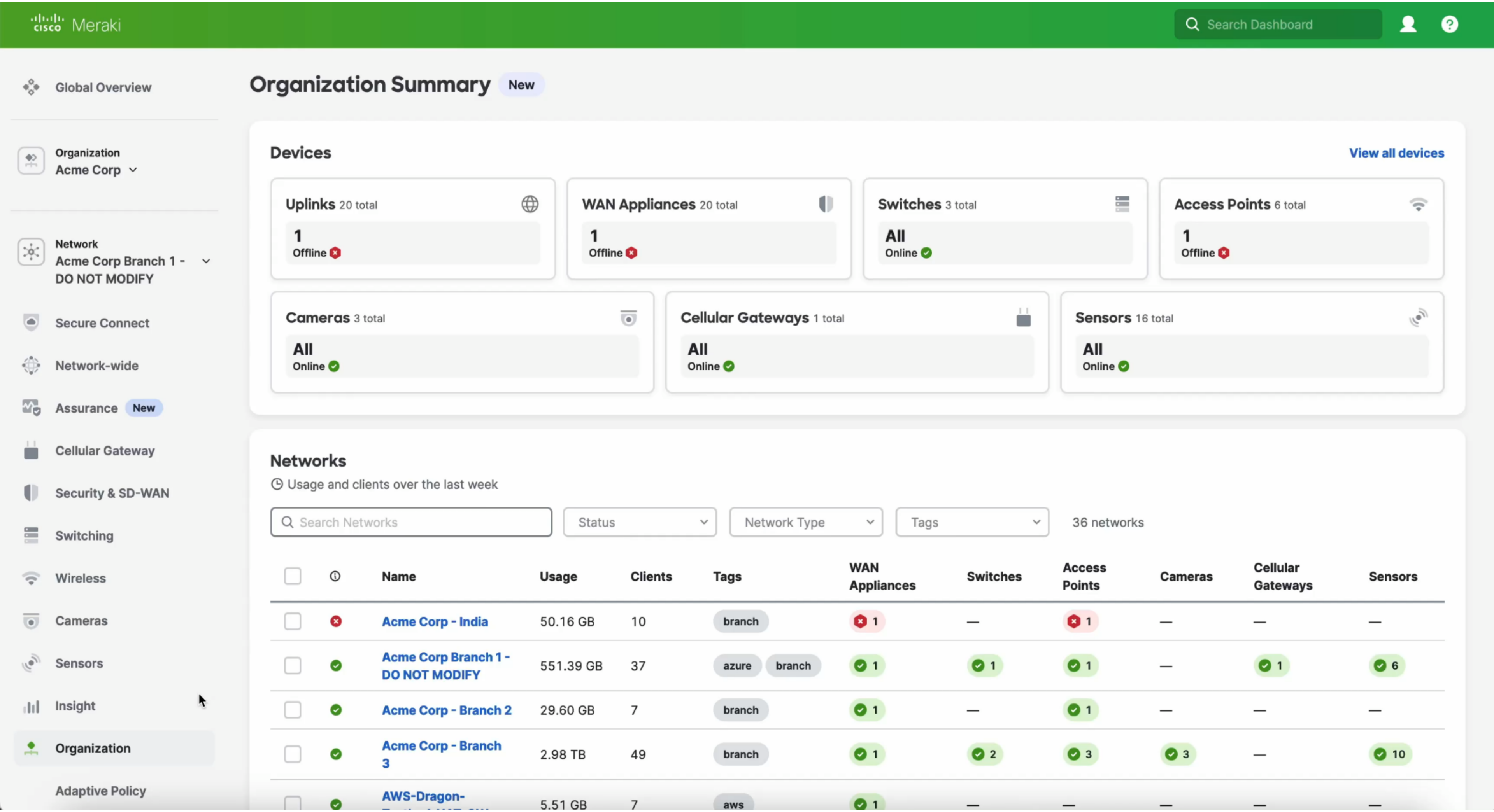


← Incidents

978 Open **A malicious SHA-256 targeted an endp...**

...orted by Cisco Meraki (CoconutLAN) on 2023-07-19T20:35:20.107Z - 34 Linked Incidents

A process running has a hash matching one in a list of known malicious process hashes View Long Descrip



Organization Summary New

Devices

View all devices

Uplinks 20 total
1
Offline ✗

WAN Appliances 20 total
1
Offline ✗

Switches 3 total
All
Online ✓

Access Points 6 total
1
Offline ✗

Cameras 3 total
All
Online ✓

Cellular Gateways 1 total
All
Online ✓

Sensors 16 total
All
Online ✓

Networks

Usage and clients over the last week

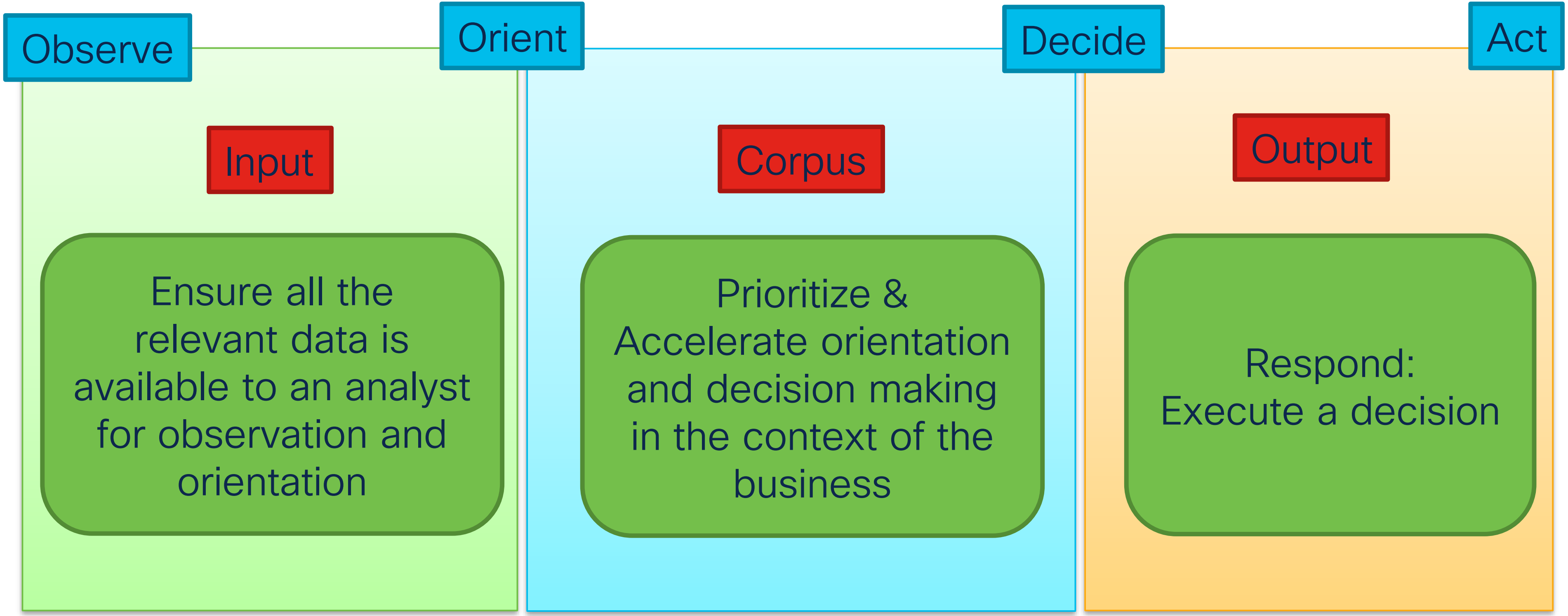
Search Networks | Status | Network Type | Tags | 36 networks

□	ⓘ	Name	Usage	Clients	Tags	WAN Appliances	Switches	Access Points	Cameras	Cellular Gateways	Sensors
□	✗	Acme Corp - India	50.16 GB	10	branch	✗ 1	—	✗ 1	—	—	—
□	✓	Acme Corp Branch 1 - DO NOT MODIFY	551.39 GB	37	azure branch	✓ 1	✓ 1	✓ 1	—	✓ 1	✓ 6
□	✓	Acme Corp - Branch 2	29.60 GB	7	branch	✓ 1	—	✓ 1	—	—	—
□	✓	Acme Corp - Branch 3	2.98 TB	49	branch	✓ 1	✓ 2	✓ 3	✓ 3	—	✓ 10
□	✓	AWS-Dragon-	5.51 GB	7	aws	✓ 1	—	—	—	—	—

What does this mean for a full stack Meraki and XDR customer?

Threat Detection

Security Operations: Data to Response



Observe

Orient

Decide

Act

Input

Ensure all the relevant data is available to an analyst for observation and orientation

Corpus

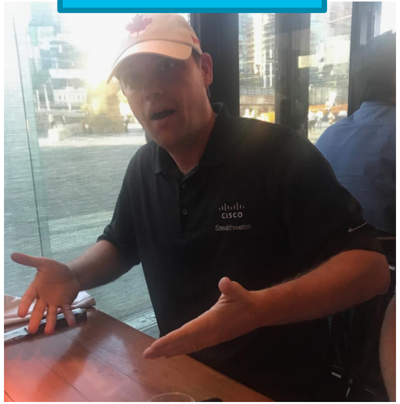
Prioritize & Accelerate orientation and decision making in the context of the business

Output

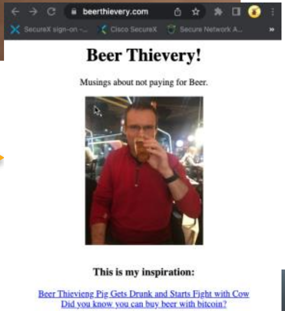
Respond:
Execute a decision

Threat Detection and Response with OODA

Observation: Missing Beer



Orient: Gather data



beerthievery.com

Beer Thievery!

Musings about not paying for Beer.

This is my inspiration:

Beer Thievieng Pig Gets Drunk and Starts Fight with Cow
Did you know you can buy beer with bitcoin?

Orient: Convict

Darrin Miller: Beer Thief

Decide

Act

Demo

Response Actions with Adaptive Network Control

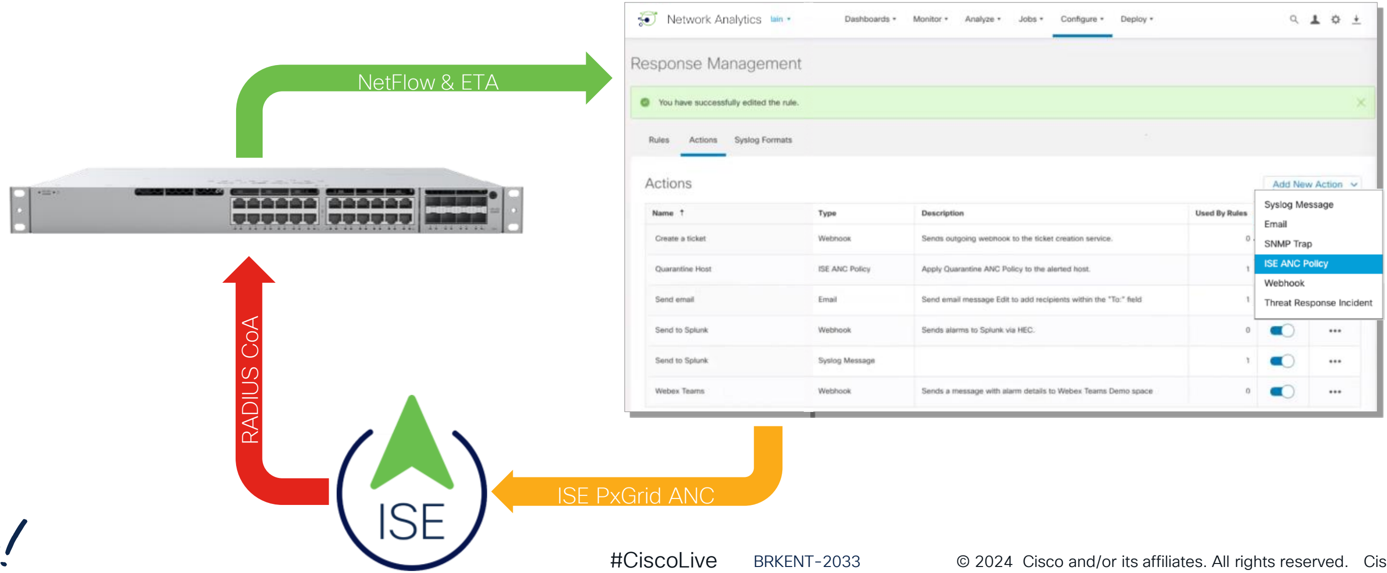
MS390/C9300-M with Secure Network Analytics & ISE

Automated threat response and alerting

Telemetry provided by MS390 to SNA / XDR

Flexible outcomes: Policy Violation

Trigger CoA via ISE



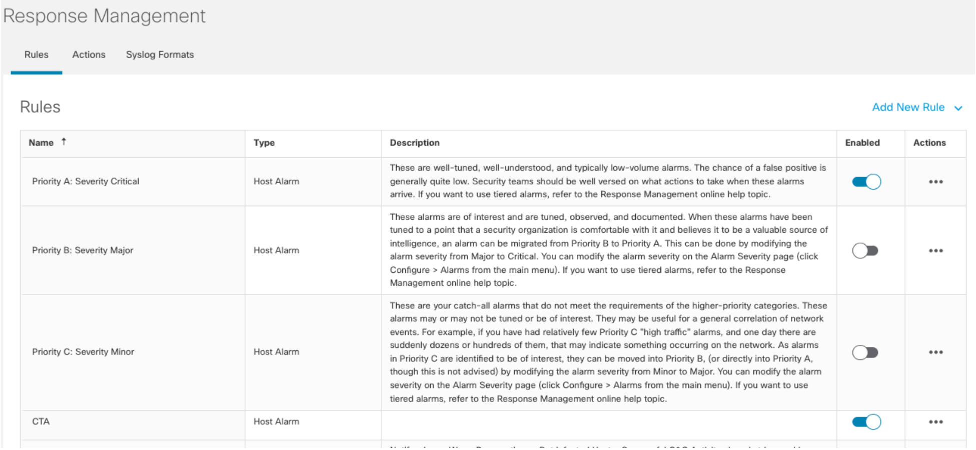
Response Management

You have successfully edited the rule.

Actions

Name ↑	Type	Description	Used By Rules		
Create a ticket	Webhook	Sends outgoing webhook to the ticket creation service.	0		
Quarantine Host	ISE ANC Policy	Apply Quarantine ANC Policy to the alerted host.	1		
Send email	Email	Send email message Edit to add recipients within the "To:" field	1		
Send to Splunk	Webhook	Sends alarms to Splunk via HEC.	0		•••
Send to Splunk	Syslog Message		1		•••
Webex Teams	Webhook	Sends a message with alarm details to Webex Teams Demo space	0		•••

SNA: alarm response rules & actions



Response Management

Rules | Actions | Syslog Formats

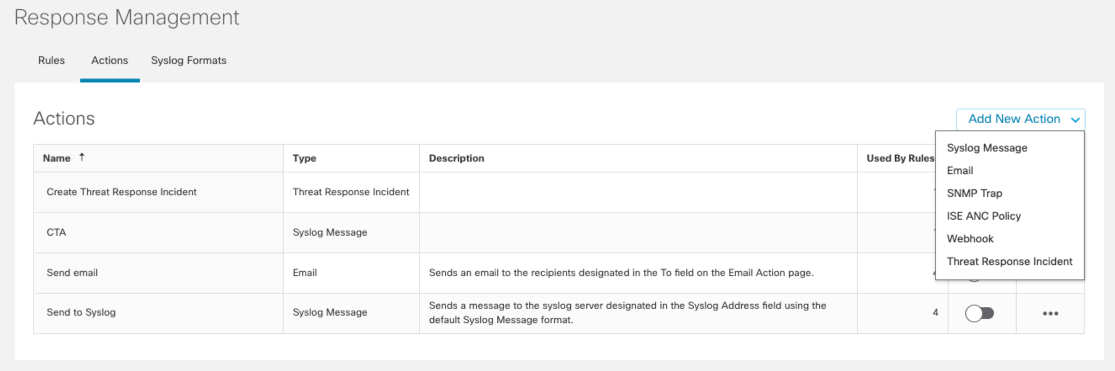
Rules

Add New Rule

Name ↑	Type	Description	Enabled	Actions
Priority A: Severity Critical	Host Alarm	These are well-tuned, well-understood, and typically low-volume alarms. The chance of a false positive is generally quite low. Security teams should be well versed on what actions to take when these alarms arrive. If you want to use tiered alarms, refer to the Response Management online help topic.	●	•••
Priority B: Severity Major	Host Alarm	These alarms are of interest and are tuned, observed, and documented. When these alarms have been tuned to a point that a security organization is comfortable with it and believes it to be a valuable source of intelligence, an alarm can be migrated from Priority B to Priority A. This can be done by modifying the alarm severity from Major to Critical. You can modify the alarm severity on the Alarm Severity page (click Configure > Alarms from the main menu). If you want to use tiered alarms, refer to the Response Management online help topic.	○	•••
Priority C: Severity Minor	Host Alarm	These are your catch-all alarms that do not meet the requirements of the higher-priority categories. These alarms may or may not be tuned or be of interest. They may be useful for a general correlation of network events. For example, if you have had relatively few Priority C "high traffic" alarms, and one day there are suddenly dozens or hundreds of them, that may indicate something occurring on the network. As alarms in Priority C are identified to be of interest, they can be moved into Priority B, (or directly into Priority A, though this is not advised) by modifying the alarm severity from Minor to Major. You can modify the alarm severity on the Alarm Severity page (click Configure > Alarms from the main menu). If you want to use tiered alarms, refer to the Response Management online help topic.	○	•••
CTA	Host Alarm		●	•••

- Create rules to automate response/export on occurrence of an alarm
- Leverage built-in Tiered Alarm Severity rules

- Define automated actions when alarm rule is hit: ISE ANC, syslog, etc.
- Create SecureX Threat Response incident



Response Management

Rules | Actions | Syslog Formats

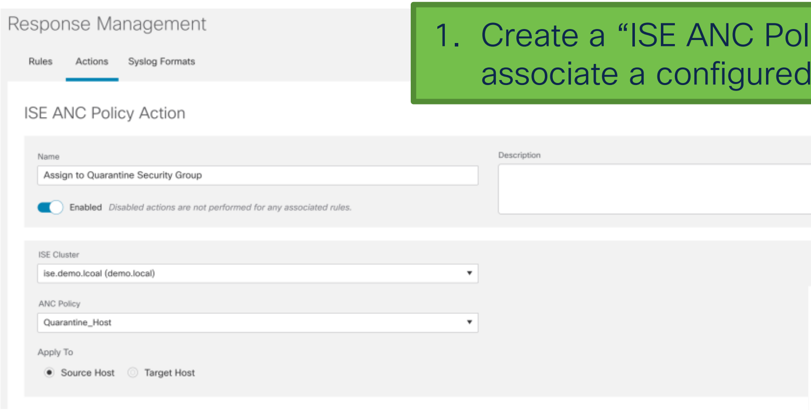
Actions

Add New Action

Name ↑	Type	Description	Used By Rules		
Create Threat Response Incident	Threat Response Incident		1		
CTA	Syslog Message		1		
Send email	Email	Sends an email to the recipients designated in the To field on the Email Action page.	4		
Send to Syslog	Syslog Message	Sends a message to the syslog server designated in the Syslog Address field using the default Syslog Message format.	4	○	•••

SNA: Remediating Action with ISE

1. Create a “ISE ANC Policy” Action rule and associate a configured ISE cluster.



ISE ANC Policy Action

Name: Assign to Quarantine Security Group

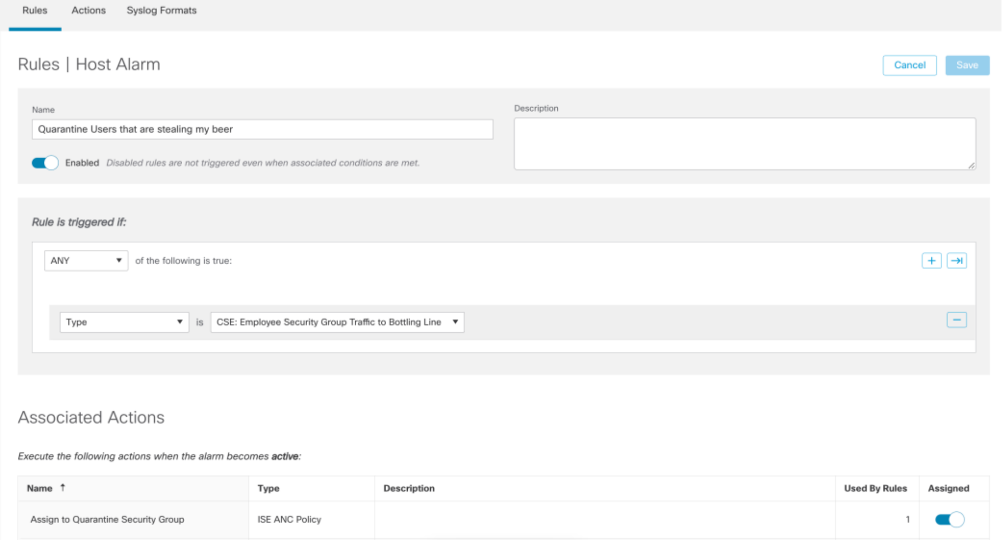
Description:

Enabled *Disabled actions are not performed for any associated rules.*

ISE Cluster: ise.demo.lcoal (demo.local)

ANC Policy: Quarantine_Host

Apply To: ● Source Host ○ Target Host



Rules | Host Alarm

Name: Quarantine Users that are stealing my beer

Description:

Enabled *Disabled rules are not triggered even when associated conditions are met.*

Rule is triggered if:

ANY of the following is true:

Type is CSE: Employee Security Group Traffic to Bottling Line

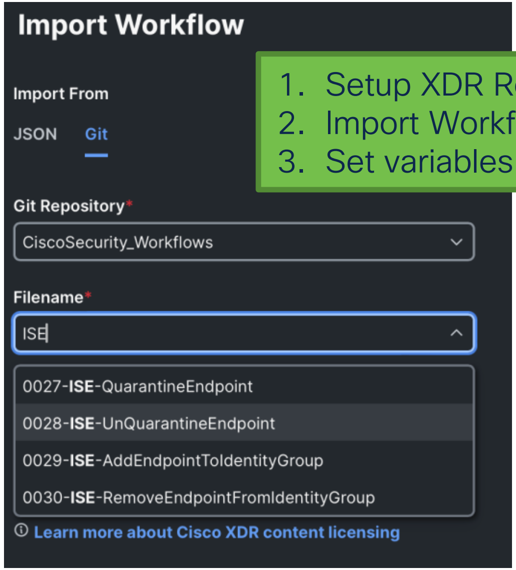
Associated Actions

*Execute the following actions when the alarm becomes **active**:*

Name ↑	Type	Description	Used By Rules	Assigned
Assign to Quarantine Security Group	ISE ANC Policy		1	●

2. Define a response Rule that invokes the defined Action

XDR: Remediating Action with ISE



Import Workflow

Import From

JSON Git

Git Repository*

CiscoSecurity_Workflows

Filename*

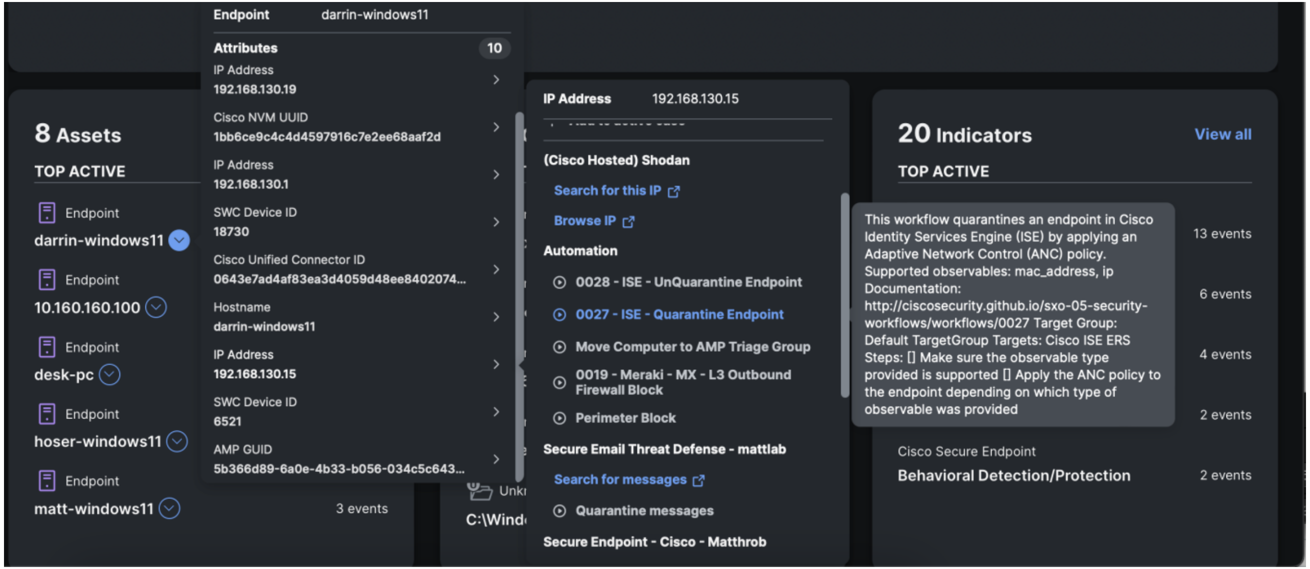
ISE

- 0027-**ISE**-QuarantineEndpoint
- 0028-**ISE**-UnQuarantineEndpoint
- 0029-**ISE**-AddEndpointToIdentityGroup
- 0030-**ISE**-RemoveEndpointFromIdentityGroup

ⓘ Learn more about Cisco XDR content licensing

1. Setup XDR Remote
2. Import Workflows
3. Set variables

1. Execute Actions!



Endpoint darrin-windows11

Attributes 10

IP Address
192.168.130.19

Cisco NVM UUID
1bb6ce9c4c4d4597916c7e2ee68aaf2d

IP Address
192.168.130.1

SWC Device ID
18730

Cisco Unified Connector ID
0643e7ad4af83ea3d4059d48ee8402074...

Hostname
darrin-windows11

IP Address
192.168.130.15

SWC Device ID
6521

AMP GUID
5b366d89-6a0e-4b33-b056-034c5c643...

8 Assets

TOP ACTIVE

Endpoint
darrin-windows11

Endpoint
10.160.160.100

Endpoint
desk-pc

Endpoint
hoser-windows11

Endpoint
matt-windows11 3 events

IP Address 192.168.130.15

(Cisco Hosted) Shodan

Search for this IP

Browse IP

Automation

- 0028 - ISE - UnQuarantine Endpoint
- 0027 - ISE - Quarantine Endpoint
- Move Computer to AMP Triage Group
- 0019 - Meraki - MX - L3 Outbound Firewall Block
- Perimeter Block

Secure Email Threat Defense - mattlab

Search for messages

- Quarantine messages

Secure Endpoint - Cisco - Matthrob

20 Indicators View all

TOP ACTIVE

This workflow quarantines an endpoint in Cisco Identity Services Engine (ISE) by applying an Adaptive Network Control (ANC) policy. Supported observables: mac_address, ip Documentation: http://ciscosecurity.github.io/sxo-05-security-workflows/workflows/0027 Target Group: Default TargetGroup Targets: Cisco ISE ERS Steps: [] Make sure the observable type provided is supported [] Apply the ANC policy to the endpoint depending on which type of observable was provided

13 events

6 events

4 events

2 events

Cisco Secure Endpoint
Behavioral Detection/Protection 2 events

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

Session ID	Title	When
BRKSEC-2178	Extended Detection with Cisco XDR: Security Analytics across the enterprise	Thursday 11:00 AM
BRKSEC-3019	Visibility, Detection and Response with Cisco Secure Network Analytics	Monday 3:00 PM
BRKSEC-2248	Design and Deploy Cisco Network Detection and Response with Cisco Breach Suite	Wednesday 2:30 PM
BRKSEC-2227	Evaluating and Improving Defenses with MITRE ATT&CK	Thursday 1:00 PM

Parting Thoughts

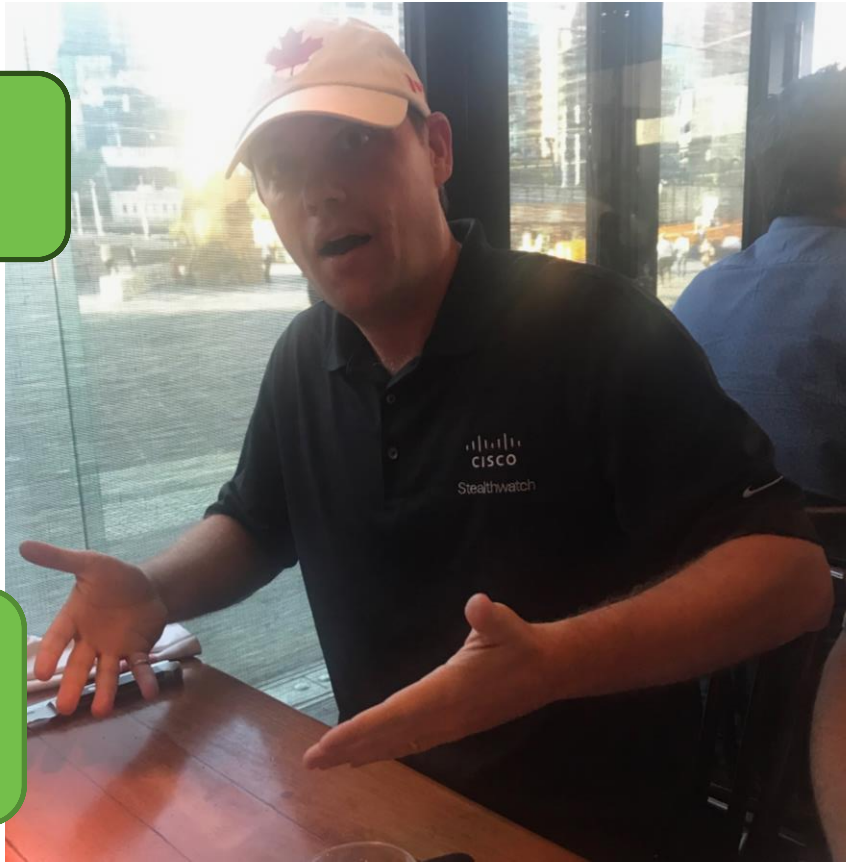
The SNOC is real!

Security Operations can be simplified with Meraki and XDR

Keep your eyes open

and

don’t have your beer stolen.



cisco The bridge to possible

Thank you

cisco Live!

#CiscoLive