cisco Live!

Let's go

#CiscoLiveAPJC

The bridge to possible

Extended Detection with Cisco XDR

Security analytics across the enterprise

Matt Robertson
Distinguished Engineer

BRKSEC-2178

Agenda

Objective:
Understand Cisco XDR Analytics

1 HOUR

Agenda:
- Intro to Cisco XDR
- Data, Analytics and Detection
- Extended Detection
- Summary

Cisco Webex App

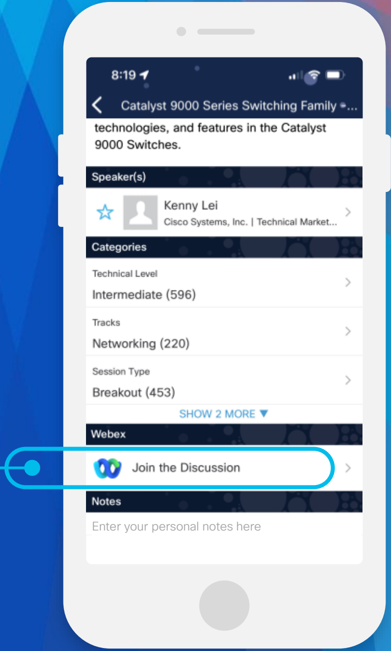
Questions?

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 December 22, 2023.



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

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

About Me

Matt Robertson

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

Public Service Announcement

Darrin Miller: Beer Thief

Alex Burger: Probably not a beer thief

Not currently in Melbourne

What is Cisco XDR?

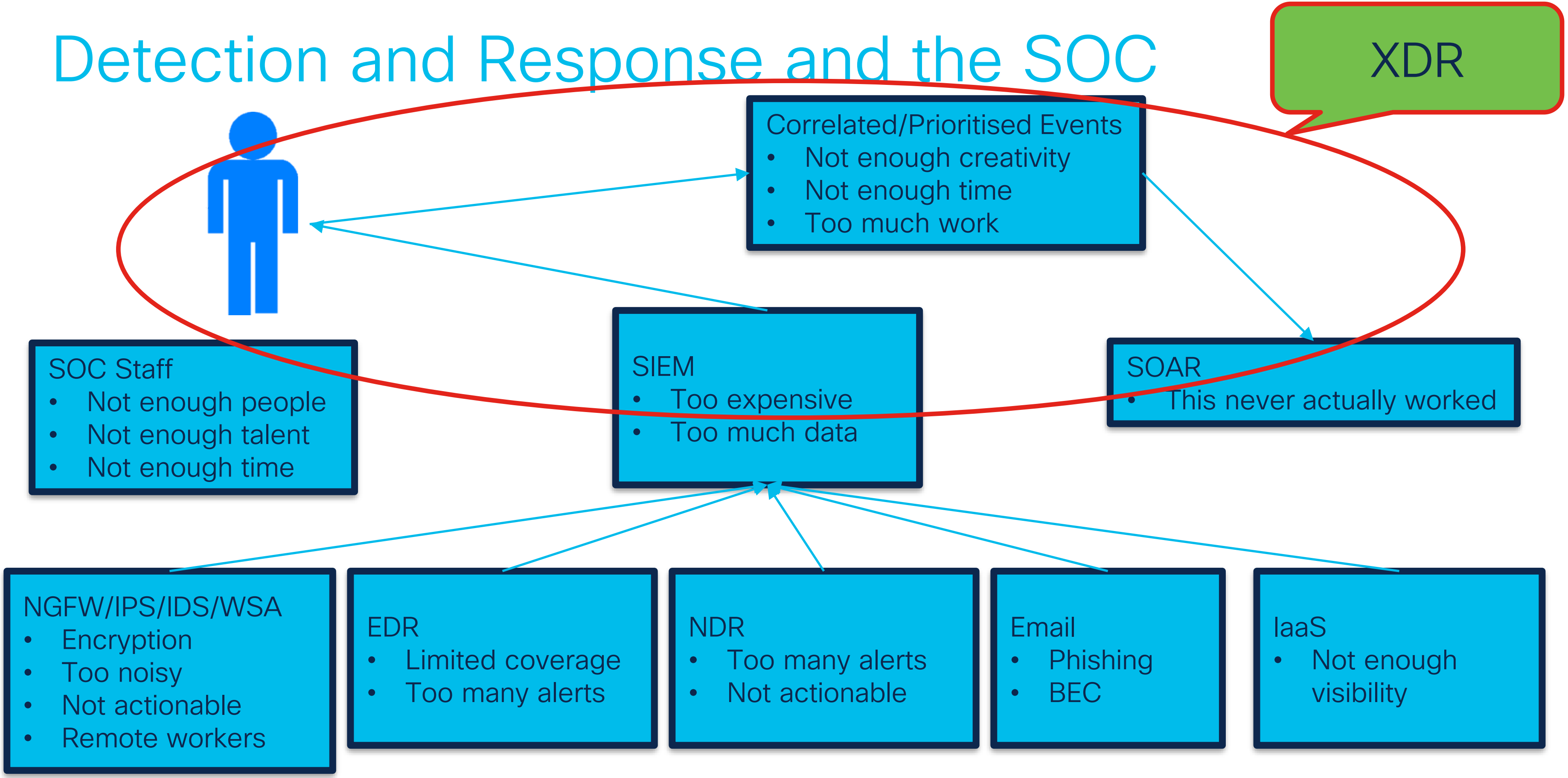
What is Extended Detection and Response?

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

Detection and Response and the SOC



XDR

Correlated/Prioritised Events
- Not enough creativity
- Not enough time
- Too much work

SOC Staff
- Not enough people
- Not enough talent
- Not enough time

SIEM
- Too expensive
- Too much data

SOAR
- This never actually worked

NGFW/IPS/IDS/WSA
- Encryption
- Too noisy
- Not actionable
- Remote workers

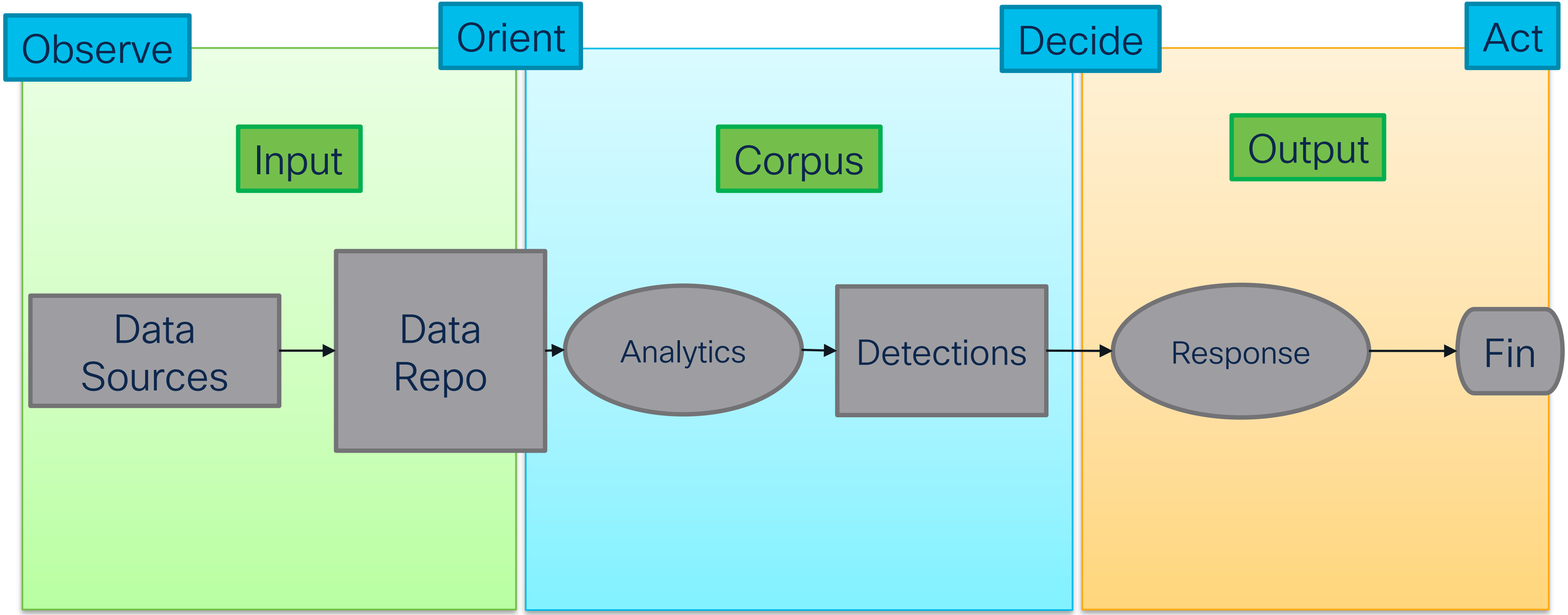
EDR
- Limited coverage
- Too many alerts

NDR
- Too many alerts
- Not actionable

Email
- Phishing
- BEC

IaaS
- Not enough visibility

An XDR speeds up the OODA Loop



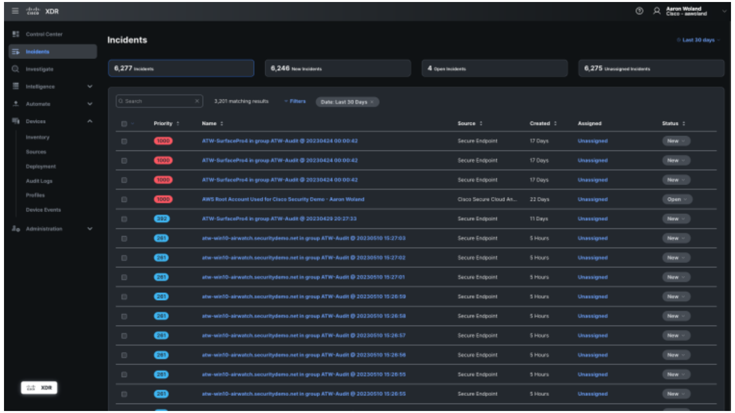
Cisco XDR: A new product offer

Data collection
Analytics
Detection

Incident framework
Enrichment
Response

Evolved Into

Cisco XDR



Incidents

Last 30 days

6,277 Incidents | 6,246 New Incidents | 4 Open Incidents | 6,275 Unassigned Incidents

Search | 3,201 matching results | Filters | Date: Last 30 Days

Priority	Name	Source	Created	Assigned	Status
1000	ATW-SurfacePro4 in group ATW-Audit @ 20230424 00:00:42	Secure Endpoint	17 Days	Unassigned	New
1000	ATW-SurfacePro4 in group ATW-Audit @ 20230424 00:00:42	Secure Endpoint	17 Days	Unassigned	New
1000	ATW-SurfacePro4 in group ATW-Audit @ 20230424 00:00:42	Secure Endpoint	17 Days	Unassigned	New
1000	AWS Root Account Used for Cisco Security Demo - Aaron Woland	Cisco Secure Cloud An...	22 Days	Unassigned	Open
202	ATW-SurfacePro4 in group ATW-Audit @ 20230429 20:27:33	Secure Endpoint	11 Days	Unassigned	New
261	atw-win10-airwatch.securitydemo.net in group ATW-Audit @ 20230510 15:27:03	Secure Endpoint	5 Hours	Unassigned	New
261	atw-win10-airwatch.securitydemo.net in group ATW-Audit @ 20230510 15:27:02	Secure Endpoint	5 Hours	Unassigned	New
261	atw-win10-airwatch.securitydemo.net in group ATW-Audit @ 20230510 15:27:01	Secure Endpoint	5 Hours	Unassigned	New
261	atw-win10-airwatch.securitydemo.net in group ATW-Audit @ 20230510 15:26:59	Secure Endpoint	5 Hours	Unassigned	New
261	atw-win10-airwatch.securitydemo.net in group ATW-Audit @ 20230510 15:26:58	Secure Endpoint	5 Hours	Unassigned	New
261	atw-win10-airwatch.securitydemo.net in group ATW-Audit @ 20230510 15:26:57	Secure Endpoint	5 Hours	Unassigned	New
261	atw-win10-airwatch.securitydemo.net in group ATW-Audit @ 20230510 15:26:56	Secure Endpoint	5 Hours	Unassigned	New
261	atw-win10-airwatch.securitydemo.net in group ATW-Audit @ 20230510 15:26:55	Secure Endpoint	5 Hours	Unassigned	New
261	atw-win10-airwatch.securitydemo.net in group ATW-Audit @ 20230510 15:26:55	Secure Endpoint	5 Hours	Unassigned	New

Along with
Significant
Enhancements

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.

Current Integrations

Data Analytics and Correlation

Cisco

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

3rd Party

- Crowdstrike

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…

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

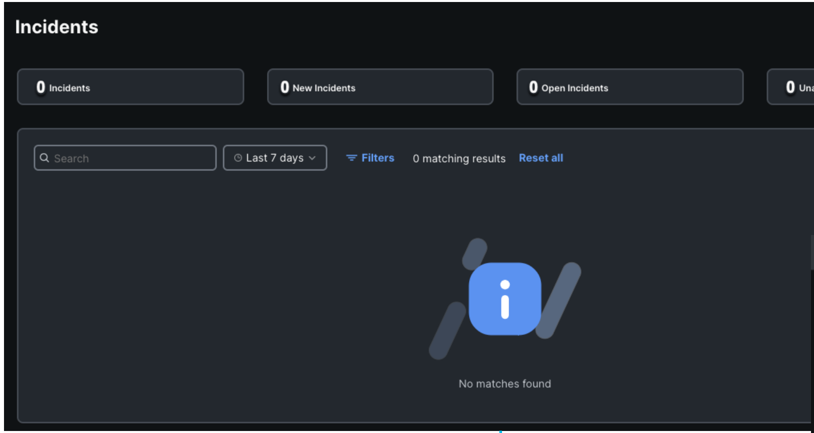
Cisco
- Adaptive Security Appliance
- Attack Surface Management
- Defense Orchestrator
- Identity Services Engine
- Meraki MX
- Orbital
- Secure Email and Web Manager
- Secure Email Gateway
- Secure Email Threat Defense
- Secure Endpoint
- Secure Firewall (FPR)
- Secure Malware Analytics
- Secure Network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



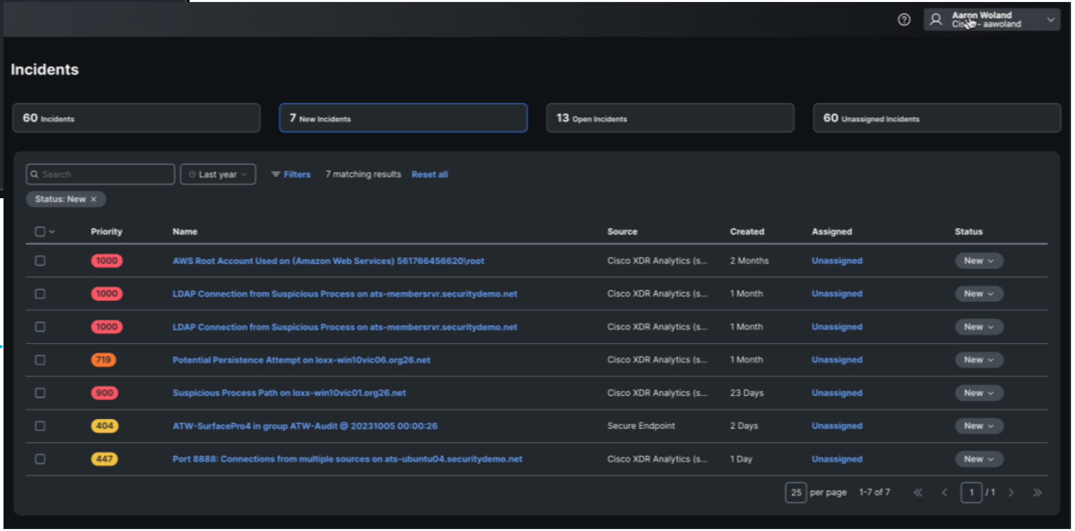
Incidents

0 Incidents | 0 New Incidents | 0 Open Incidents | 0 Unassigned Incidents

Search | Last 7 days | Filters | 0 matching results | Reset all

No matches found

How are incidents created from data sources?



Aaron Woland
Cisco - aawoland

Incidents

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

Search | Last year | Filters | 7 matching results | Reset all

Status: New ×

☐	Priority	Name	Source	Created	Assigned	Status
☐	1000	AWS Root Account Used on (Amazon Web Services) 561766456620\root	Cisco XDR Analytics (s...	2 Months	Unassigned	New
☐	1000	LDAP Connection from Suspicious Process on ats-membersrvr.securitydemo.net	Cisco XDR Analytics (s...	1 Month	Unassigned	New
☐	1000	LDAP Connection from Suspicious Process on ats-membersrvr.securitydemo.net	Cisco XDR Analytics (s...	1 Month	Unassigned	New
☐	719	Potential Persistence Attempt on loxx-win10vic06.org26.net	Cisco XDR Analytics (s...	1 Month	Unassigned	New
☐	900	Suspicious Process Path on loxx-win10vic01.org26.net	Cisco XDR Analytics (s...	23 Days	Unassigned	New
☐	404	ATW-SurfacePro4 in group ATW-Audit @ 20231005 00:00:26	Secure Endpoint	2 Days	Unassigned	New
☐	447	Port 8888: Connections from multiple sources on ats-ubuntu04.securitydemo.net	Cisco XDR Analytics (s...	1 Day	Unassigned	New

25 per page 1-7 of 7 | 1 / 1

Methods of Incident Creation: Current Status

XDR Analytics

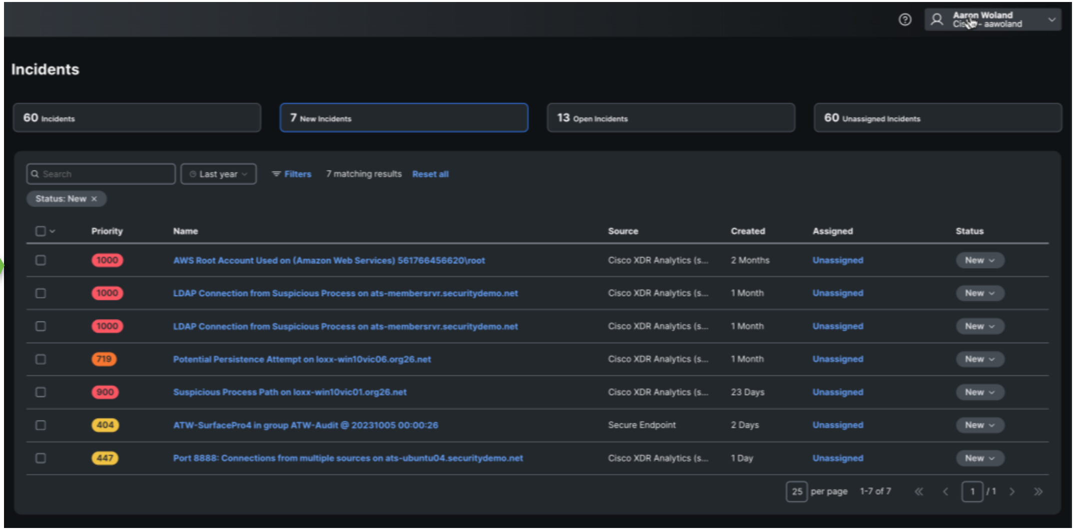
Individual and/or correlated alerts

API

For workflows and custom integrations

Cisco Secure Endpoint

- Critical and High Events automatically promoted
- this will evolve in the next quarter



Aaron Woland
Cisco - aawoland

Incidents

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

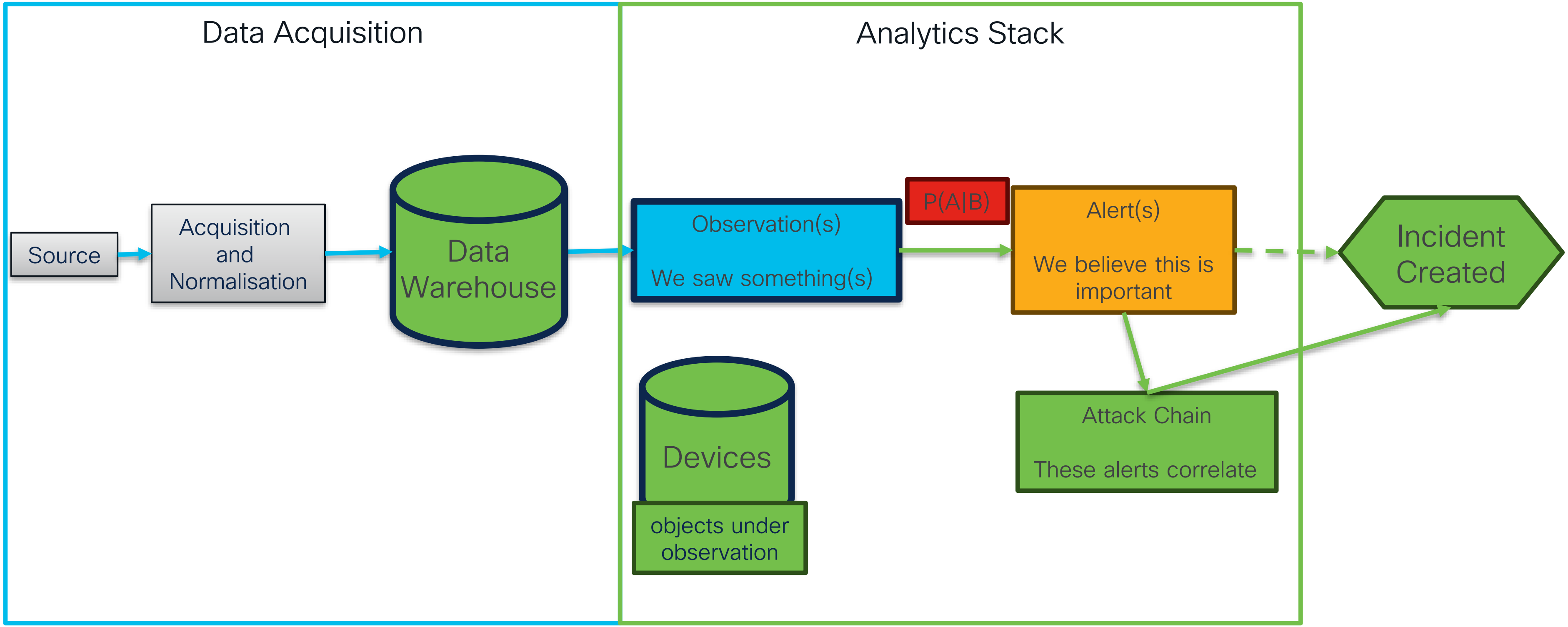
Search | Last year | Filters | 7 matching results | Reset all

Status: New ×

□	Priority	Name	Source	Created	Assigned	Status
□	1000	AWS Root Account Used on (Amazon Web Services) 561766456620\root	Cisco XDR Analytics (s...	2 Months	Unassigned	New
□	1000	LDAP Connection from Suspicious Process on ats-membersrvr.securitydemo.net	Cisco XDR Analytics (s...	1 Month	Unassigned	New
□	1000	LDAP Connection from Suspicious Process on ats-membersrvr.securitydemo.net	Cisco XDR Analytics (s...	1 Month	Unassigned	New
□	719	Potential Persistence Attempt on loxx-win10vic06.org26.net	Cisco XDR Analytics (s...	1 Month	Unassigned	New
□	900	Suspicious Process Path on loxx-win10vic01.org26.net	Cisco XDR Analytics (s...	23 Days	Unassigned	New
□	404	ATW-SurfacePro4 in group ATW-Audit @ 20231005 00:00:26	Secure Endpoint	2 Days	Unassigned	New
□	447	Port 8888: Connections from multiple sources on ats-ubuntu04.securitydemo.net	Cisco XDR Analytics (s...	1 Day	Unassigned	New

25 per page 1-7 of 7 « ‹ 1 / 1 › »

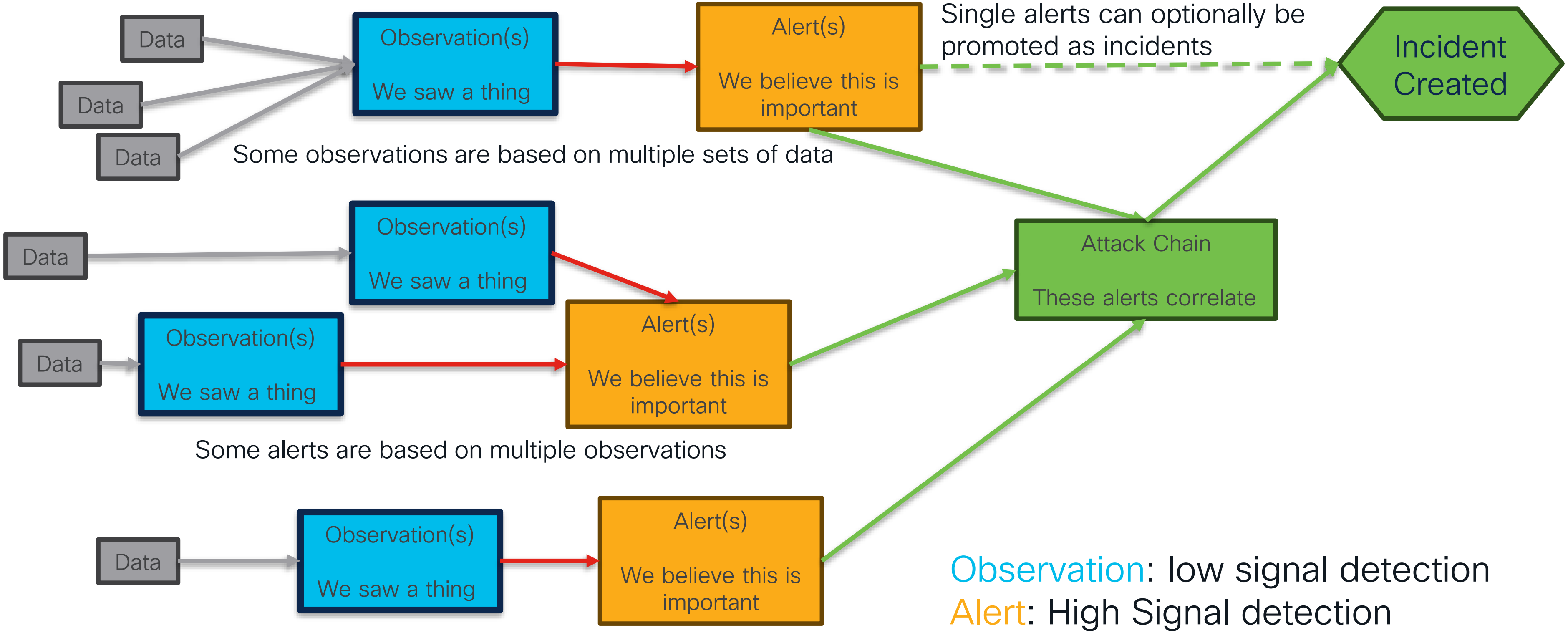
Data Analytics Pipeline



P(A|B)

There is an AI/ML model behind observation to alert

Detection and Correlation



Data

Data

Data

Observation(s)

We saw a thing

Alert(s)

We believe this is important

Single alerts can optionally be promoted as incidents

Incident Created

Some observations are based on multiple sets of data

Data

Observation(s)

We saw a thing

Attack Chain

These alerts correlate

Data

Observation(s)

We saw a thing

Alert(s)

We believe this is important

Some alerts are based on multiple observations

Data

Observation(s)

We saw a thing

Alert(s)

We believe this is important

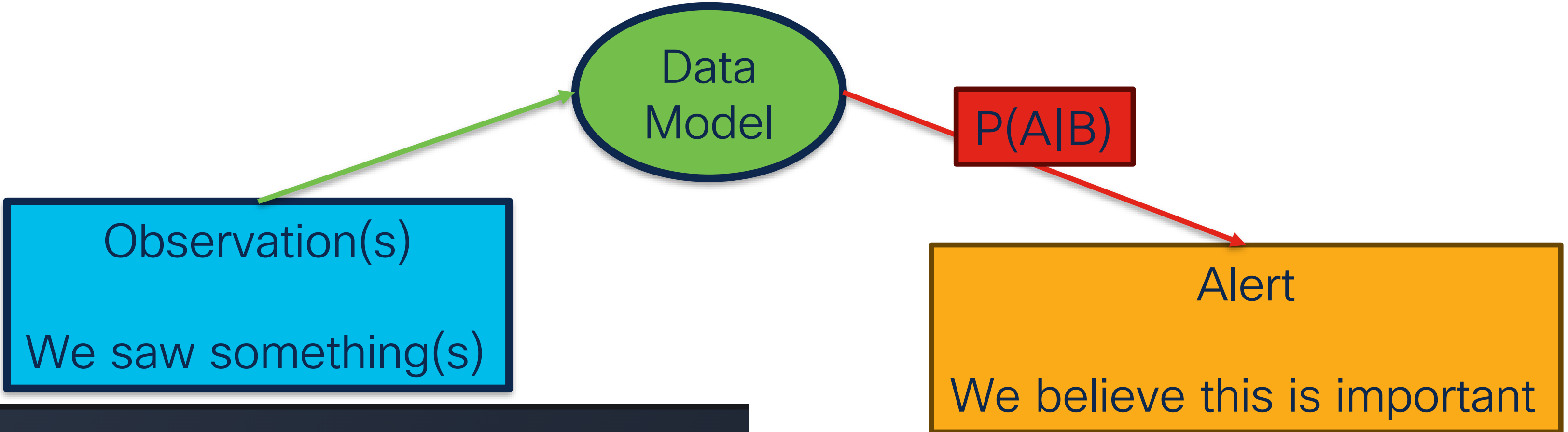
Some data sets can lead directly to an observation and alert

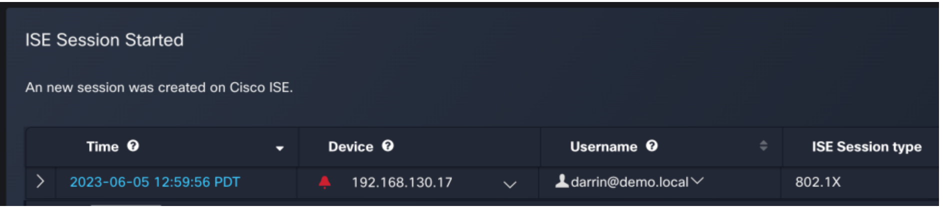
Observation: low signal detection

Alert: High Signal detection

Attack chain: Higher signal detection

Observations to Alert

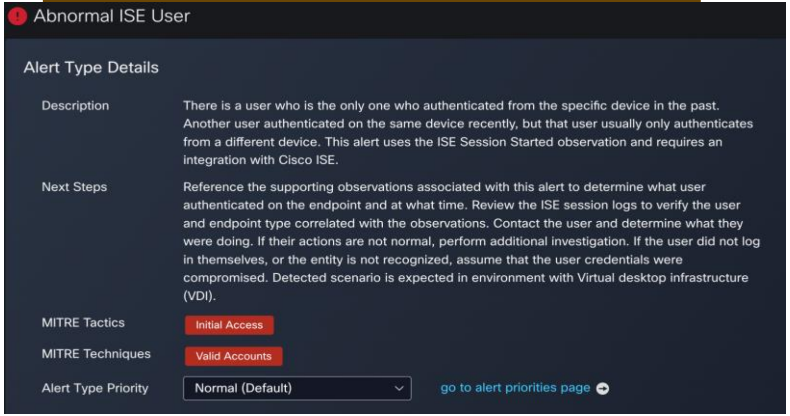




ISE Session Started

An new session was created on Cisco ISE.

Time	Device	Username	ISE Session type
2023-06-05 12:59:56 PDT	192.168.130.17	darrin@demo.local	802.1X



Abnormal ISE User

Alert Type Details

Description: 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. This alert uses the ISE Session Started observation and requires an integration with Cisco ISE.

Next Steps: Reference the supporting observations associated with this alert to determine what user authenticated on the endpoint and at what time. Review the ISE session logs to verify the user and endpoint type correlated with the observations. Contact the user and determine what they were doing. If their actions are not normal, perform additional investigation. If the user did not log in themselves, or the entity is not recognized, assume that the user credentials were compromised. Detected scenario is expected in environment with Virtual desktop infrastructure (VDI).

MITRE Tactics: Initial Access

MITRE Techniques: Valid Accounts

Alert Type Priority: Normal (Default)

A note about data science

$$\underset{\text{posterior}}{\boxed{P(A|B)}} = \underset{\text{prior}}{\boxed{P(A)}} \times \frac{\boxed{P(B|A)}\ \text{likelihood}}{\boxed{P(B)}\ \text{marginal}}$$

There is a complex AI/ML data model behind the alerting engine

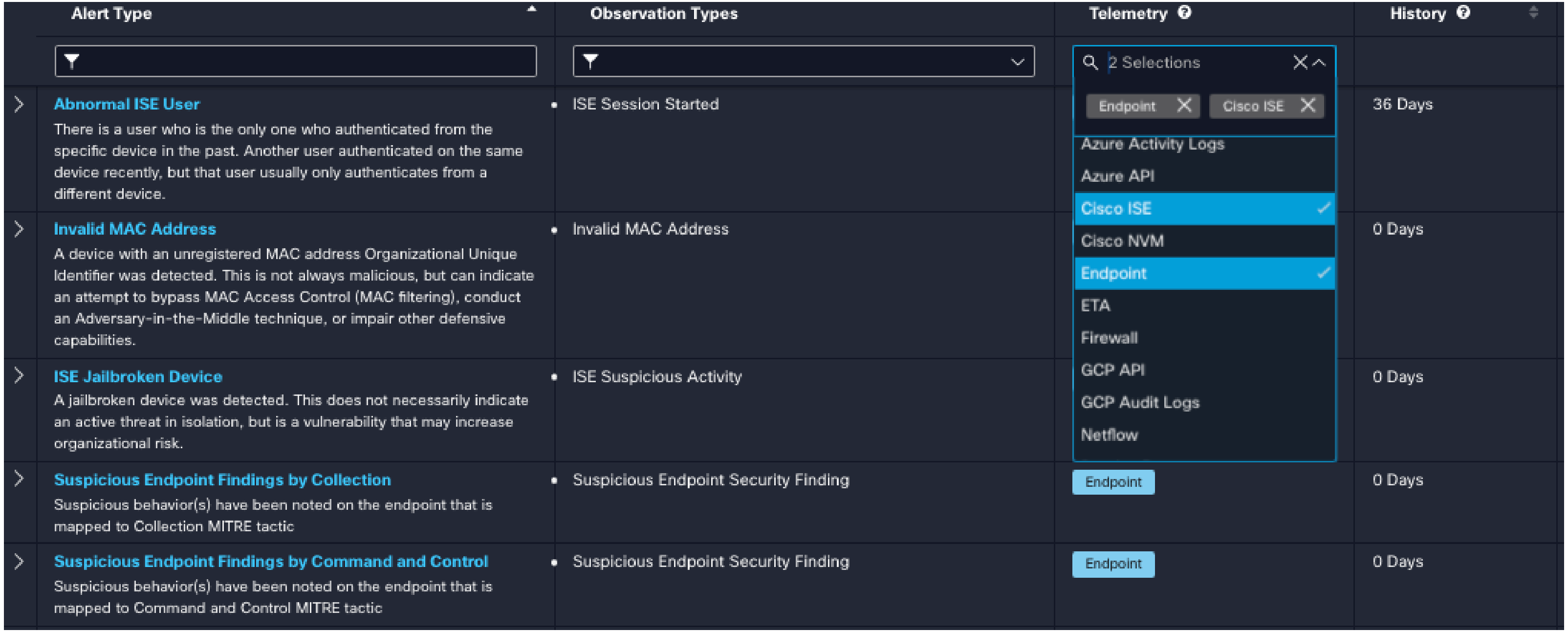
What moves a set of observations to an alert can be situational dependent for certain alert types

For some alerts predicting their future appearance in the UI is not always deterministic

Practical terms:

- Small labs are not ideal proof of concept scenarios
- Single test scenarios may also not present ideal results
- You might not get alerts (incidents) for some data sources

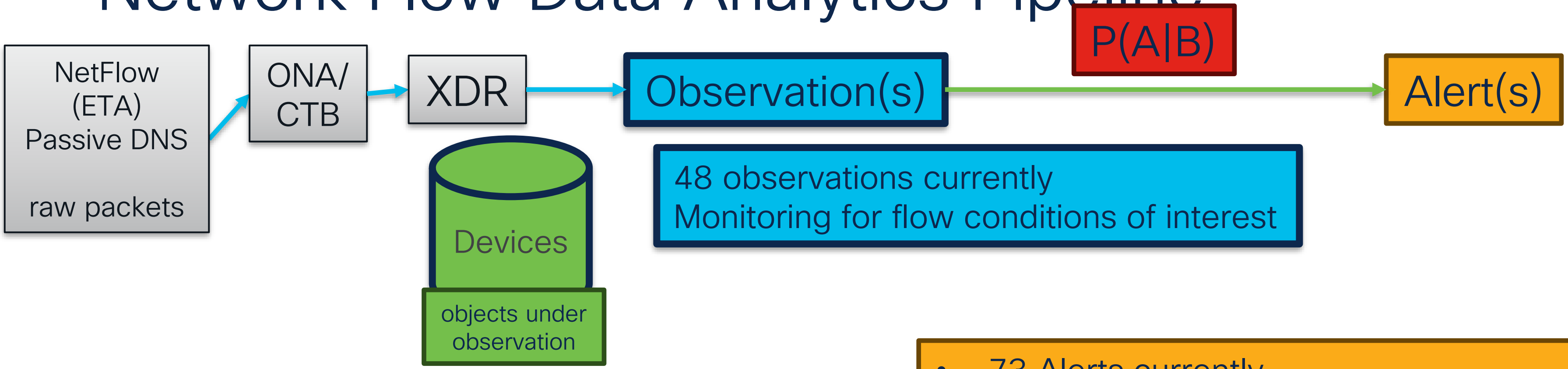
Alerts Require (Specific) Data



Alert Type	Observation Types	Telemetry	History
		2 Selections Endpoint ✕ Cisco ISE ✕ Azure Activity Logs Azure API Cisco ISE ✓ Cisco NVM Endpoint ✓ ETA Firewall GCP API GCP Audit Logs Netflow	
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

Network Flow Data Analytics Pipeline

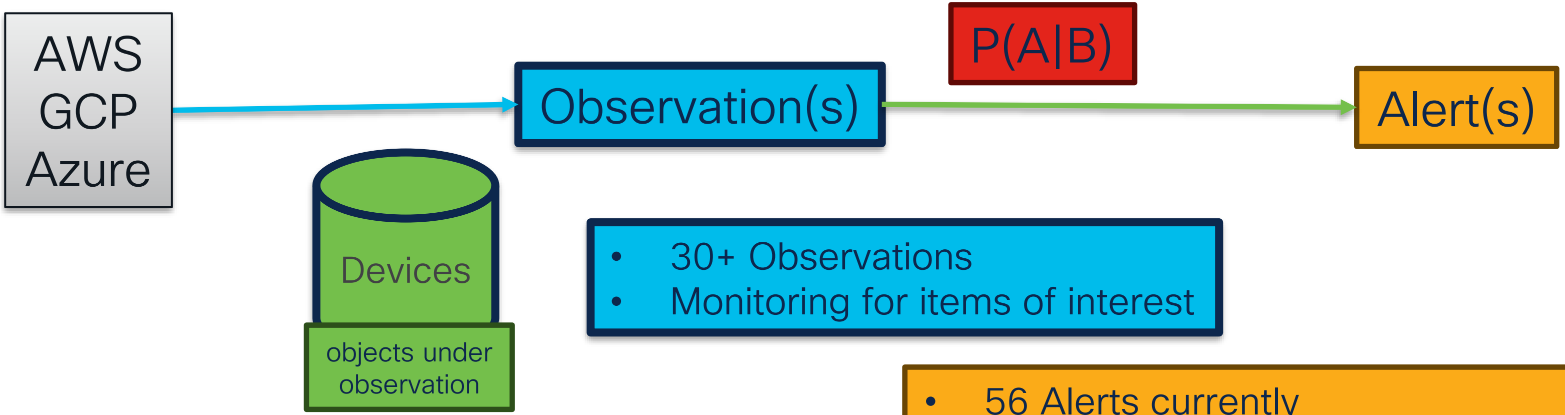


48 observations currently
Monitoring for flow conditions of interest

- 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 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

IAAS Data Analytics Pipeline

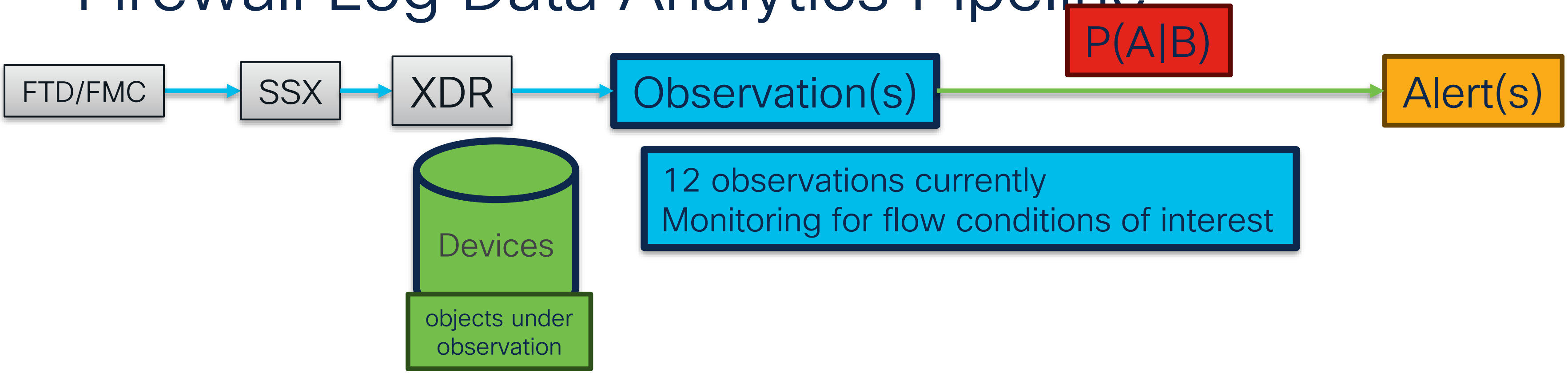


- 30+ Observations
- Monitoring for items of interest

- 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

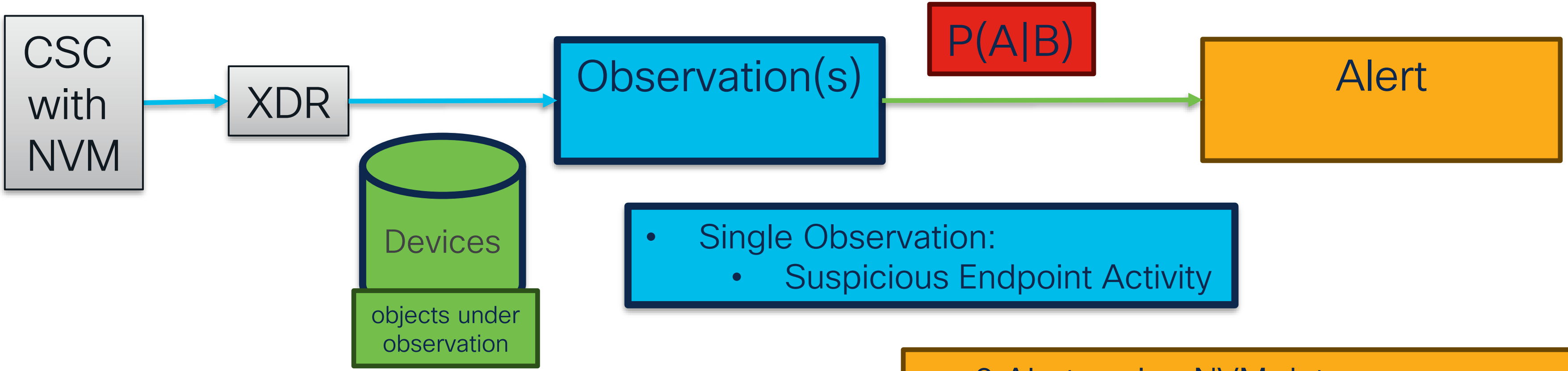


12 observations currently
Monitoring for flow conditions of interest

- 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

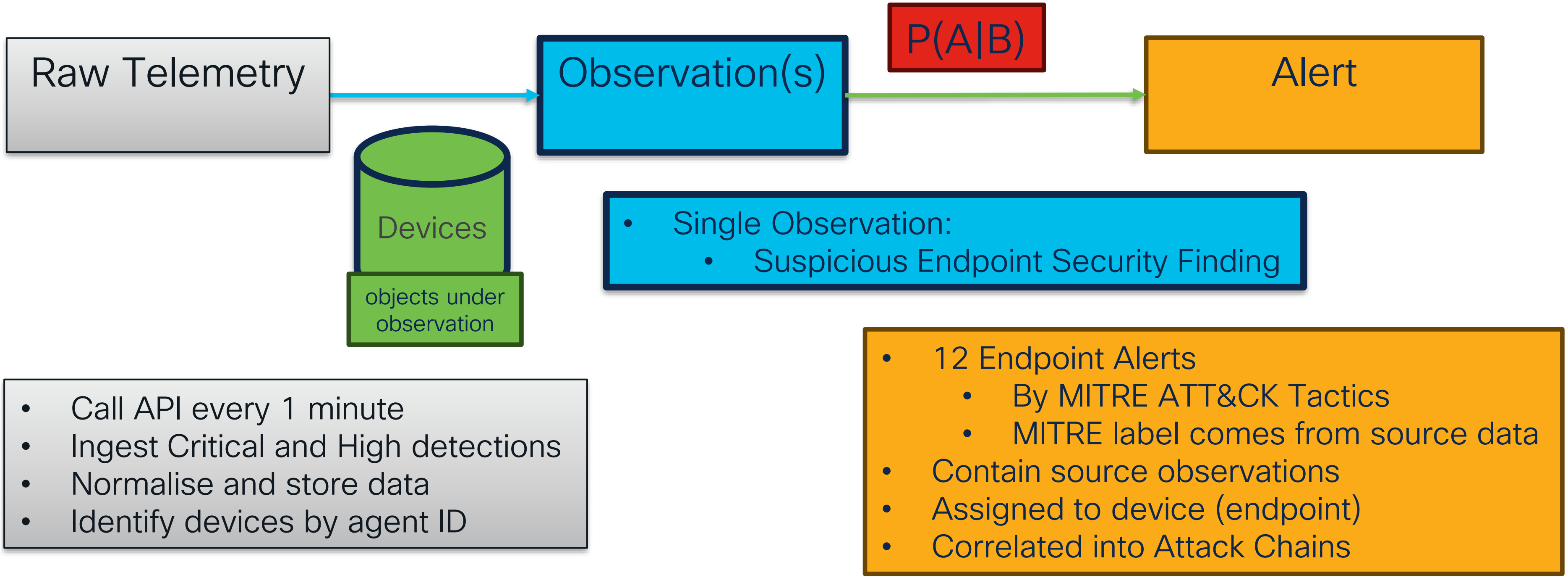


- Single Observation:
  - Suspicious Endpoint Activity

- 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

- 9 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 (ex.Crowdstrike)



Raw Telemetry

Observation(s)

P(A|B)

Alert

Devices

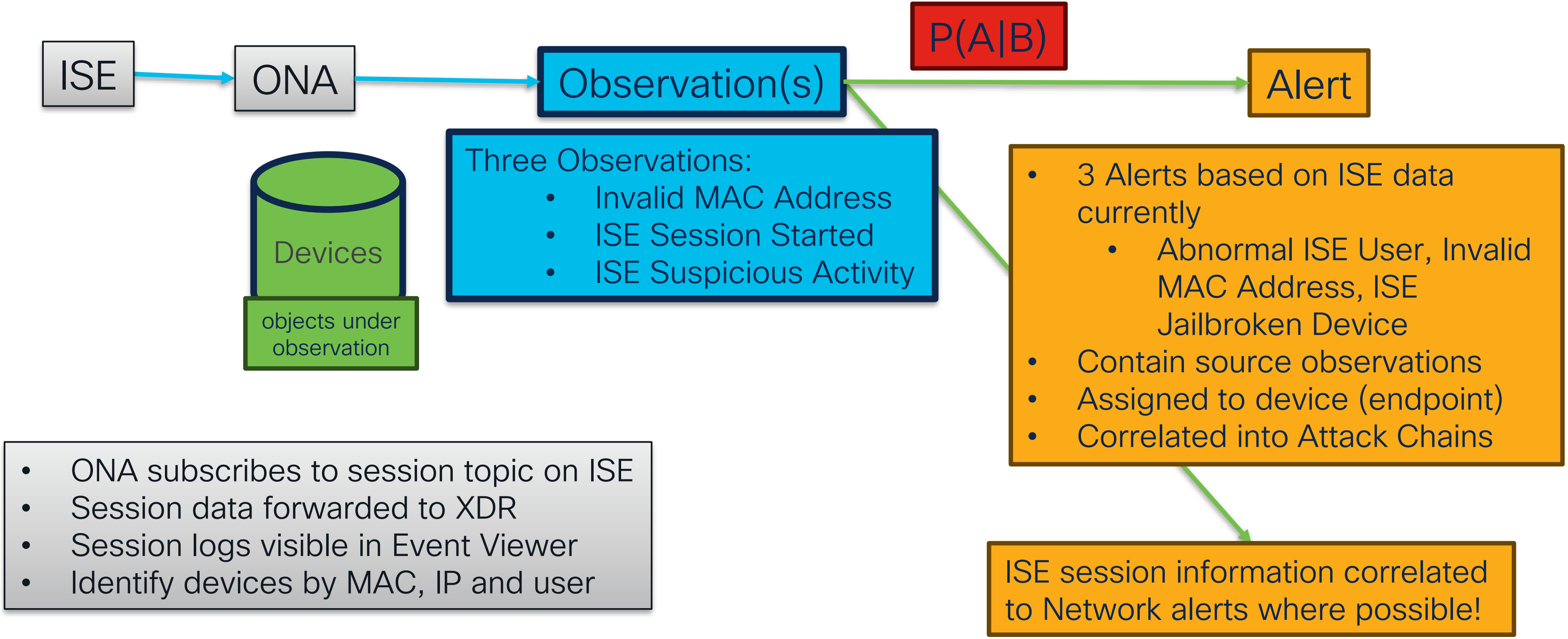
objects under observation

- Single Observation:
  - Suspicious Endpoint Security Finding

- Call API every 1 minute
- Ingest Critical and High detections
- Normalise and store data
- Identify devices by agent ID

- 12 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



Three Observations:

- Invalid MAC Address
- ISE Session Started
- ISE Suspicious Activity

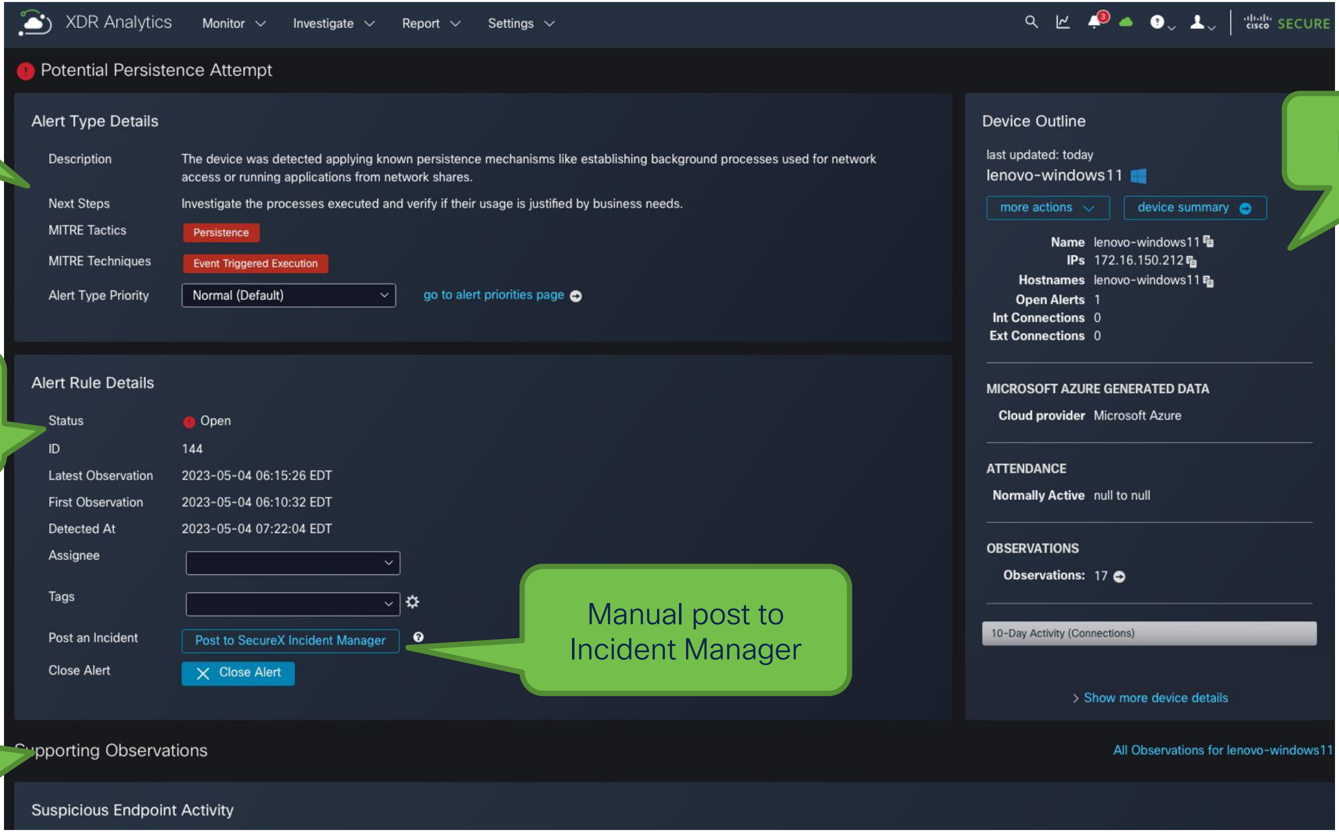
- 3 Alerts based on ISE data currently
  - Abnormal ISE User, Invalid MAC Address, ISE Jailbroken Device
- Contain source observations
- Assigned to device (endpoint)
- Correlated into Attack Chains

ISE session information correlated to Network alerts where possible!

- ONA subscribes to session topic on ISE
- Session data forwarded to XDR
- Session logs visible in Event Viewer
- Identify devices by MAC, IP and user

XDR Analytics Alert

New alerts are frequently published into production



Potential Persistence Attempt

Alert Type Details

Description: The device was detected applying known persistence mechanisms like establishing background processes used for network access or running applications from network shares.

Next Steps: Investigate the processes executed and verify if their usage is justified by business needs.

MITRE Tactics: Persistence

MITRE Techniques: Event Triggered Execution

Alert Type Priority: Normal (Default)

go to alert priorities page

Alert Rule Details

Status: Open

ID: 144

Latest Observation: 2023-05-04 06:15:26 EDT

First Observation: 2023-05-04 06:10:32 EDT

Detected At: 2023-05-04 07:22:04 EDT

Assignee:

Tags:

Post an Incident: Post to SecureX Incident Manager

Close Alert: Close Alert

Device Outline

last updated: today

lenovo-windows11

more actions | device summary

Name: lenovo-windows11

IPs: 172.16.150.212

Hostnames: lenovo-windows11

Open Alerts: 1

Int Connections: 0

Ext Connections: 0

MICROSOFT AZURE GENERATED DATA

Cloud provider: Microsoft Azure

ATTENDANCE

Normally Active: null to null

OBSERVATIONS

Observations: 17

10-Day Activity (Connections)

Show more device details

Supporting Observations

All Observations for lenovo-windows11

Suspicious Endpoint Activity

Alert Type Details

Alert Occurrence Details

Supporting Observations

Entity details

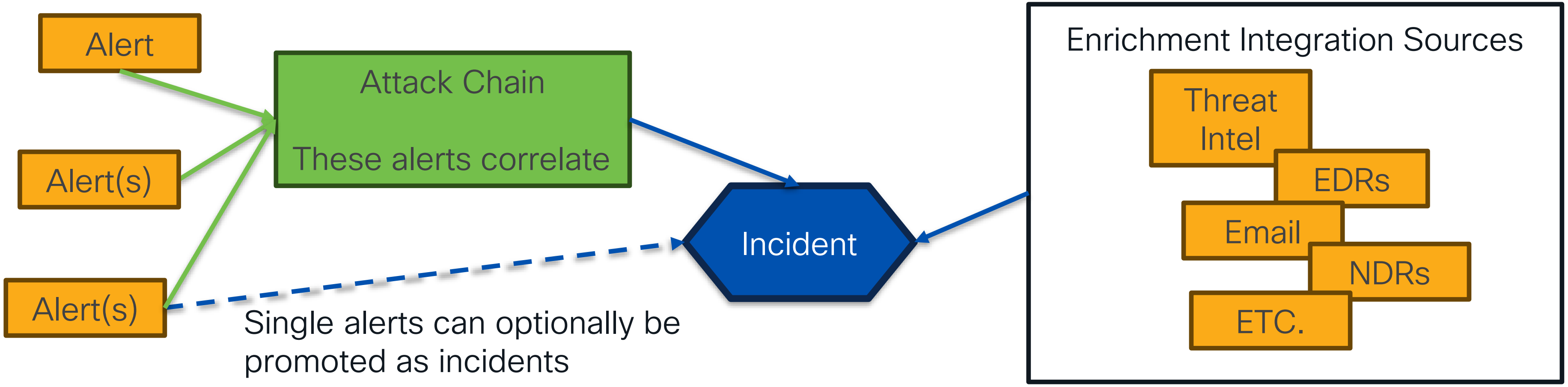
Manual post to Incident Manager

Alert Demo

Extended Detection

Important note:
Some XDR Analytics alerts contain data from multiple tools!

Extending a Detection



Alert

Alert(s)

Alert(s)

Attack Chain

These alerts correlate

Incident

Single alerts can optionally be promoted as incidents

Enrichment Integration Sources

Threat Intel

EDRs

Email

NDRs

ETC.

Correlation (pre-incident creation):

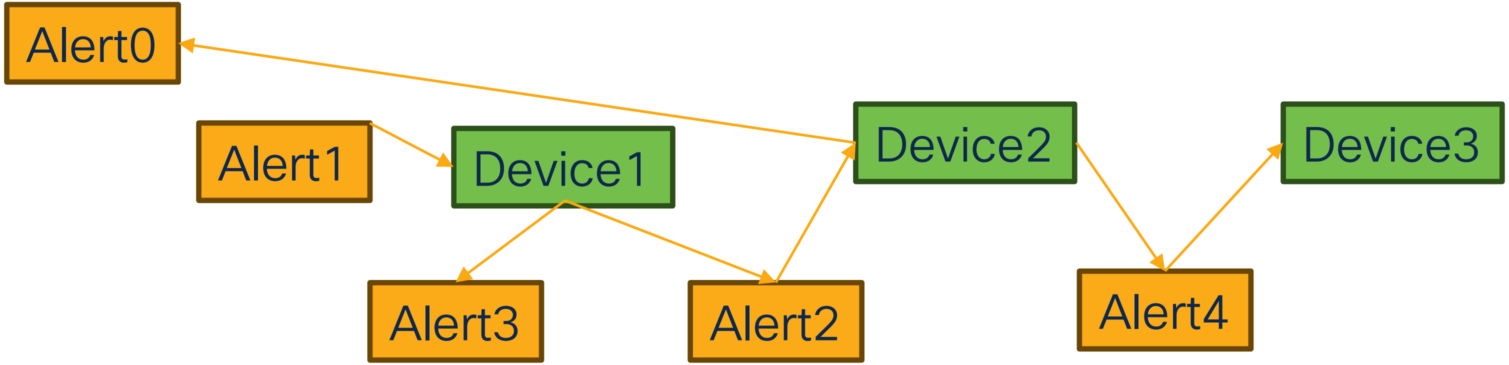
Data from multiple security tools is analysed to arrive at a detection of maliciousness

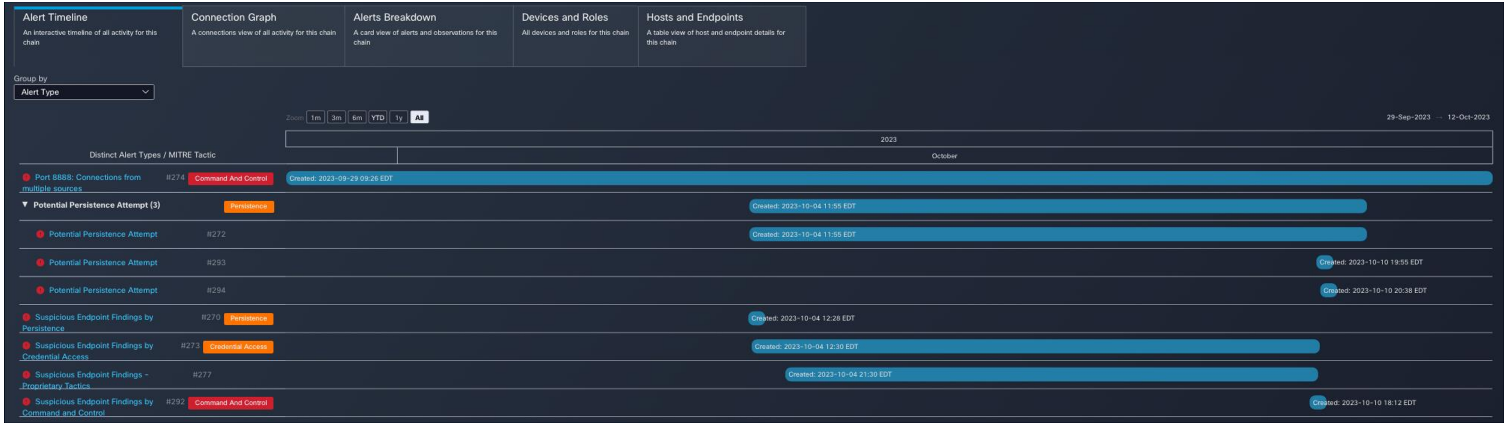
Enrichment (post-incident creation):

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

Attack Chains

Reconstructing the attack timeline





Alert Timeline
An interactive timeline of all activity for this chain

Connection Graph
A connections view of all activity for this chain

Alerts Breakdown
A card view of alerts and observations for this chain

Devices and Roles
All devices and roles for this chain

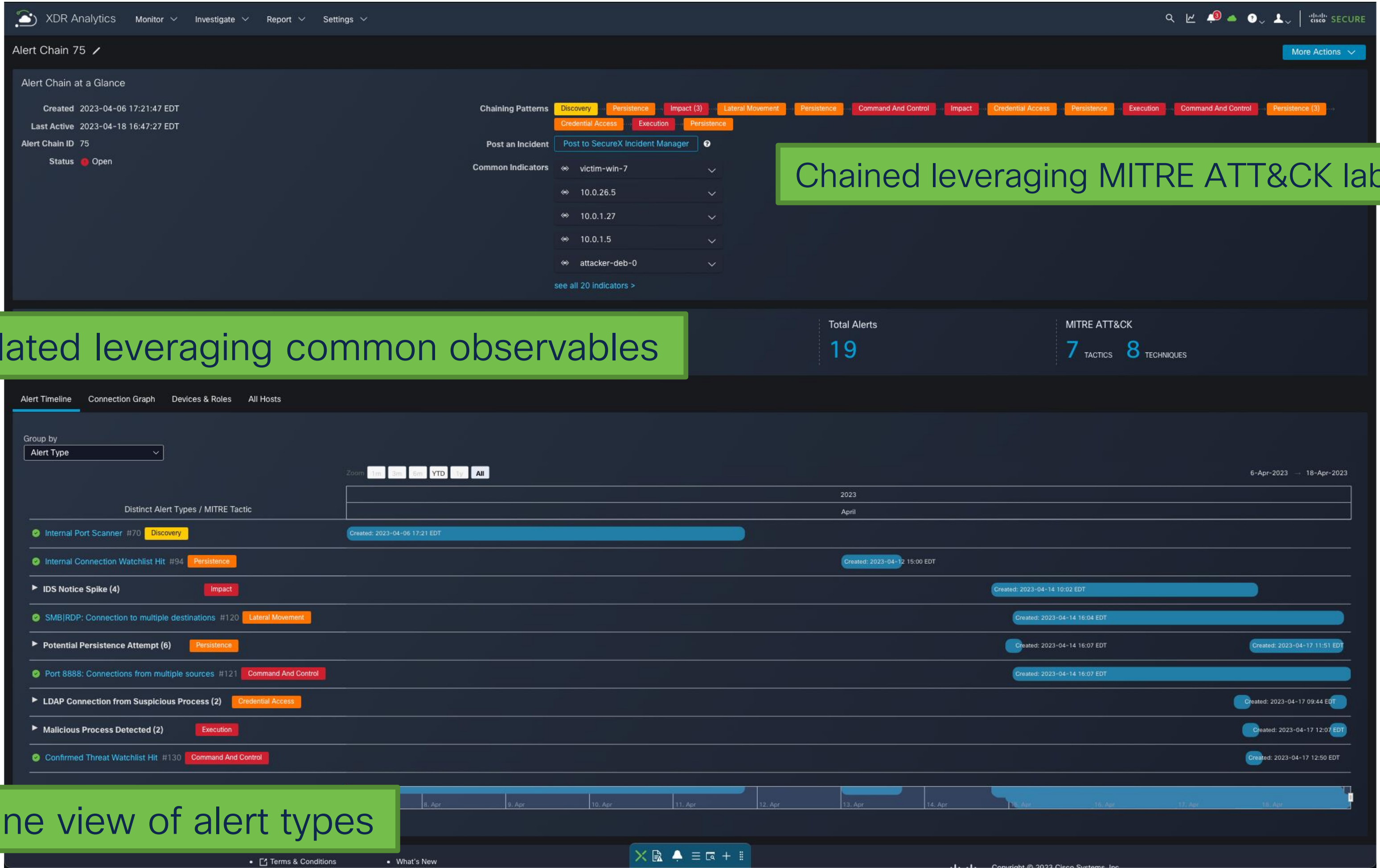
Hosts and Endpoints
A table view of host and endpoint details for this chain

Group by: Alert Type

Distinct Alert Types / MITRE Tactic			
Port 8888: Connections from multiple sources	#274	Command And Control	Created: 2023-09-29 09:26 EDT
▼ Potential Persistence Attempt (3)		Persistence	Created: 2023-10-04 11:55 EDT
Potential Persistence Attempt	#272		Created: 2023-10-04 11:55 EDT
Potential Persistence Attempt	#293		Created: 2023-10-10 19:55 EDT
Potential Persistence Attempt	#294		Created: 2023-10-10 20:38 EDT
Suspicious Endpoint Findings by Persistence	#270	Persistence	Created: 2023-10-04 12:28 EDT
Suspicious Endpoint Findings by Credential Access	#273	Credential Access	Created: 2023-10-04 12:30 EDT
Suspicious Endpoint Findings - Proprietary Tactics	#277		Created: 2023-10-04 21:30 EDT
Suspicious Endpoint Findings by Command and Control	#292	Command And Control	Created: 2023-10-10 18:12 EDT

XDR Analytics: Attack Chain

Automatic correlation of related alerts



Alert Chain 75

Alert Chain at a Glance

Created	2023-04-06 17:21:47 EDT
Last Active	2023-04-18 16:47:27 EDT
Alert Chain ID	75
Status	● Open

Chaining Patterns: Discovery → Persistence → Impact (3) → Lateral Movement → Persistence → Command And Control → Impact → Credential Access → Persistence → Execution → Command And Control → Persistence (3) → Credential Access → Execution → Persistence

Post an Incident: Post to SecureX Incident Manager

Common Indicators:
- victim-win-7
- 10.0.26.5
- 10.0.1.27
- 10.0.1.5
- attacker-deb-0

see all 20 indicators >

Chained leveraging MITRE ATT&CK labels

Correlated leveraging common observables

Total Alerts 19

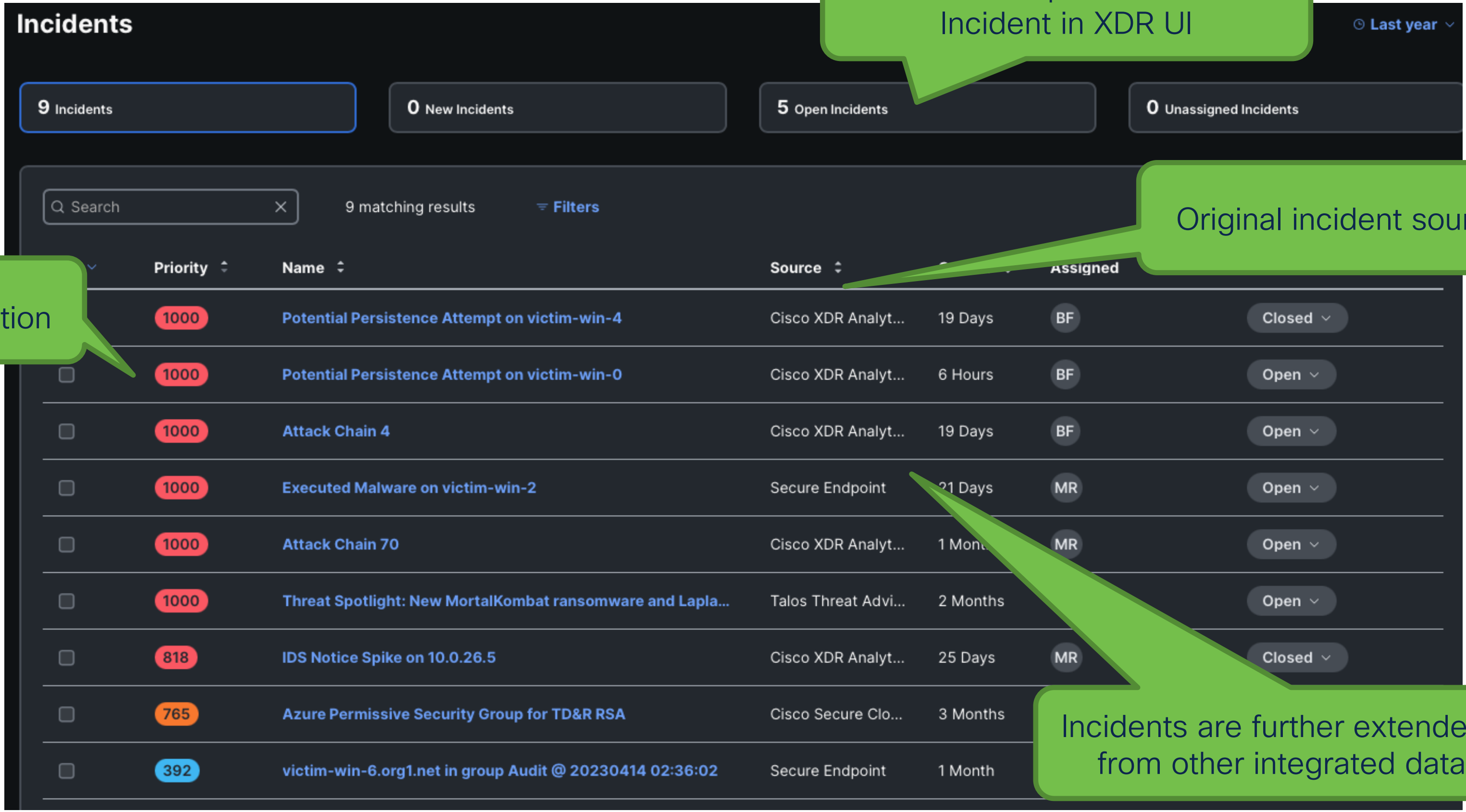
MITRE ATT&CK 7 TACTICS 8 TECHNIQUES

Group by: Alert Type

Distinct Alert Types / MITRE Tactic		
Internal Port Scanner #70	Discovery	Created: 2023-04-06 17:21 EDT
Internal Connection Watchlist Hit #94	Persistence	Created: 2023-04-12 15:00 EDT
▸ IDS Notice Spike (4)	Impact	Created: 2023-04-14 10:02 EDT
SMB|RDP: Connection to multiple destinations #120	Lateral Movement	Created: 2023-04-14 16:04 EDT
▸ Potential Persistence Attempt (6)	Persistence	Created: 2023-04-14 16:07 EDT Created: 2023-04-17 11:51 EDT
Port 8888: Connections from multiple sources #121	Command And Control	Created: 2023-04-14 16:07 EDT
▸ LDAP Connection from Suspicious Process (2)	Credential Access	Created: 2023-04-17 09:44 EDT
▸ Malicious Process Detected (2)	Execution	Created: 2023-04-17 12:07 EDT
Confirmed Threat Watchlist Hit #130	Command And Control	Created: 2023-04-17 12:50 EDT

Timeline view of alert types

XDR Incident Manager



Incidents

Last year

9 Incidents | 0 New Incidents | 5 Open Incidents | 0 Unassigned Incidents

Search

9 matching results

Filters

	Priority	Name	Source		Assigned	
	1000	Potential Persistence Attempt on victim-win-4	Cisco XDR Analyt...	19 Days	BF	Closed
□	1000	Potential Persistence Attempt on victim-win-0	Cisco XDR Analyt...	6 Hours	BF	Open
□	1000	Attack Chain 4	Cisco XDR Analyt...	19 Days	BF	Open
□	1000	Executed Malware on victim-win-2	Secure Endpoint	21 Days	MR	Open
□	1000	Attack Chain 70	Cisco XDR Analyt...	1 Mont	MR	Open
□	1000	Threat Spotlight: New MortalKombat ransomware and Lapla...	Talos Threat Advi...	2 Months		Open
□	818	IDS Notice Spike on 10.0.26.5	Cisco XDR Analyt...	25 Days	MR	Closed
□	765	Azure Permissive Security Group for TD&R RSA	Cisco Secure Clo...	3 Months		
□	392	victim-win-6.org1.net in group Audit @ 20230414 02:36:02	Secure Endpoint	1 Month		

Detections promoted into Incident in XDR UI

Original incident source

Prioritisation

Incidents are further extended with data from other integrated data sources

Prioritise by Impact

Incidents prioritized by business impact and asset value

742 | 92 Detection Risk | 8 Asset Value at Risk

Priority Score = Detection Risk x Asset Value

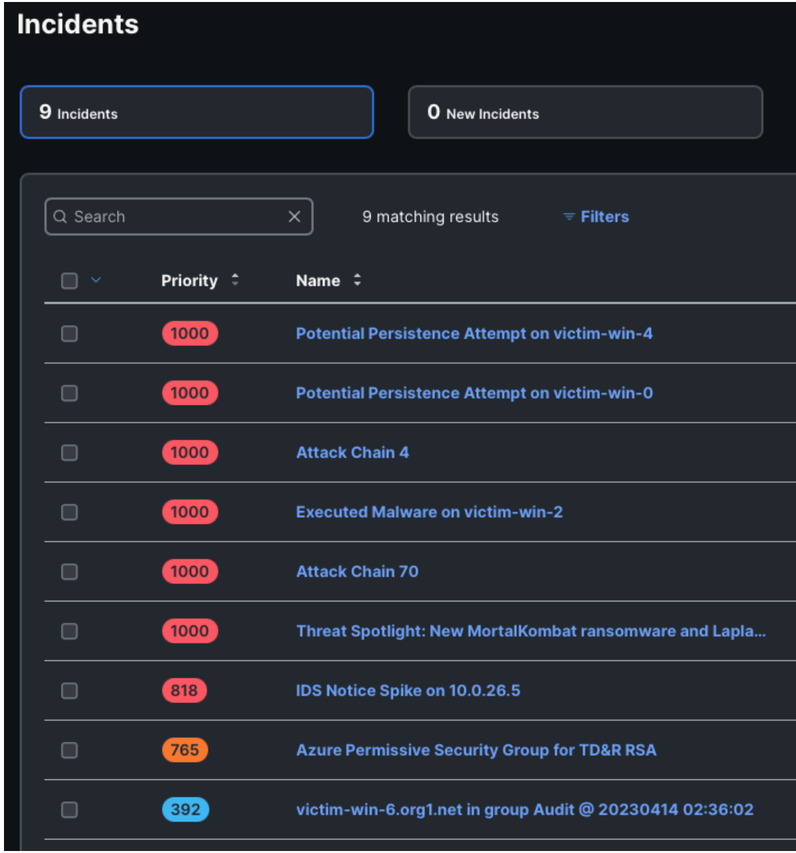
0-1000 | 0-100 | 0-10

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



Incidents

9 Incidents | 0 New Incidents

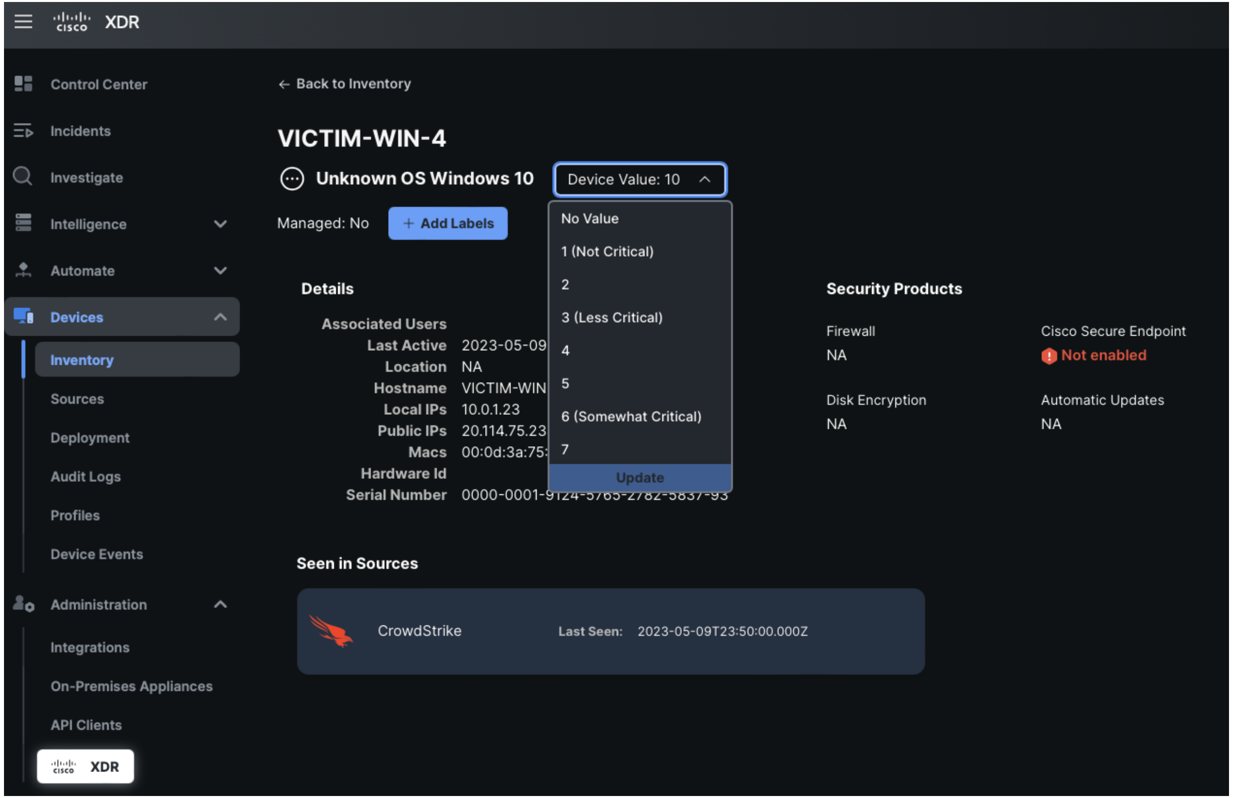
Search ✕ | 9 matching results | Filters

□	Priority	Name
□	1000	Potential Persistence Attempt on victim-win-4
□	1000	Potential Persistence Attempt on victim-win-0
□	1000	Attack Chain 4
□	1000	Executed Malware on victim-win-2
□	1000	Attack Chain 70
□	1000	Threat Spotlight: New MortalKombat ransomware and Lapla...
□	818	IDS Notice Spike on 10.0.26.5
□	765	Azure Permissive Security Group for TD&R RSA
□	392	victim-win-6.org1.net in group Audit @ 20230414 02:36:02

Aside: Asset Value Configuration

- Configured on device page
- Default is 10

Note:
Only devices known to Device Insights will appear here



VICTIM-WIN-4

Unknown OS Windows 10

Device Value: 10

Managed: No

Details

Associated Users
Last Active 2023-05-09
Location NA
Hostname VICTIM-WIN
Local IPs 10.0.1.23
Public IPs 20.114.75.23
Macs 00:0d:3a:75:
Hardware Id
Serial Number 0000-0001-9124-5765-2782-5837-93

Security Products

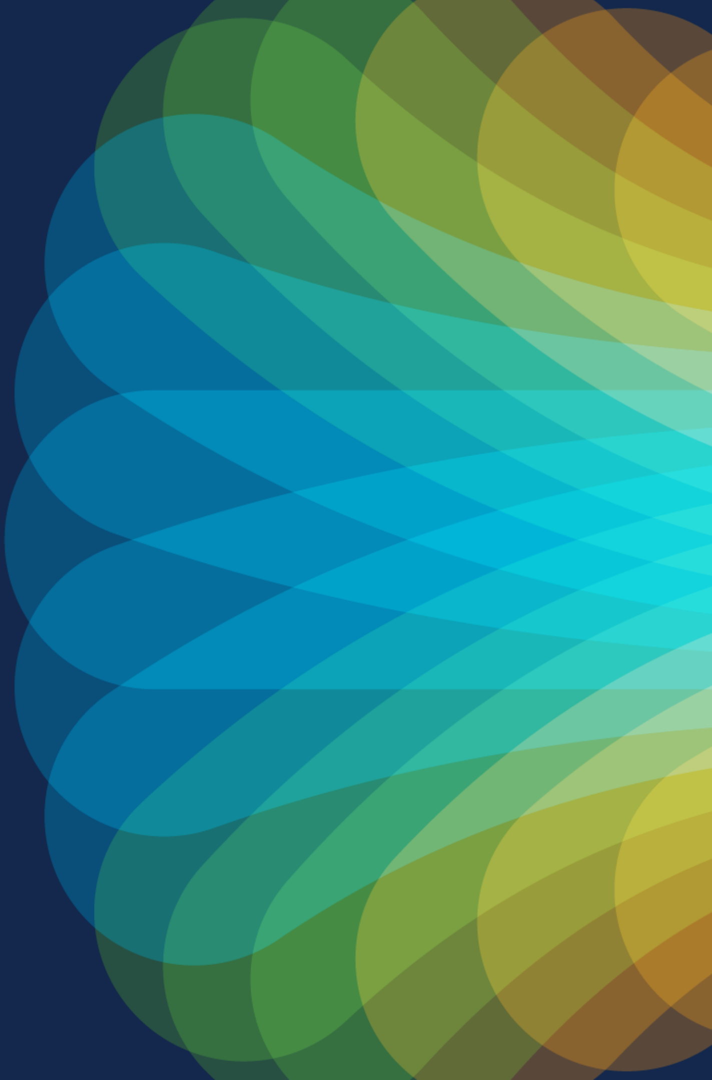
Firewall NA
Cisco Secure Endpoint: Not enabled
Disk Encryption NA
Automatic Updates NA

Seen in Sources

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

Demo

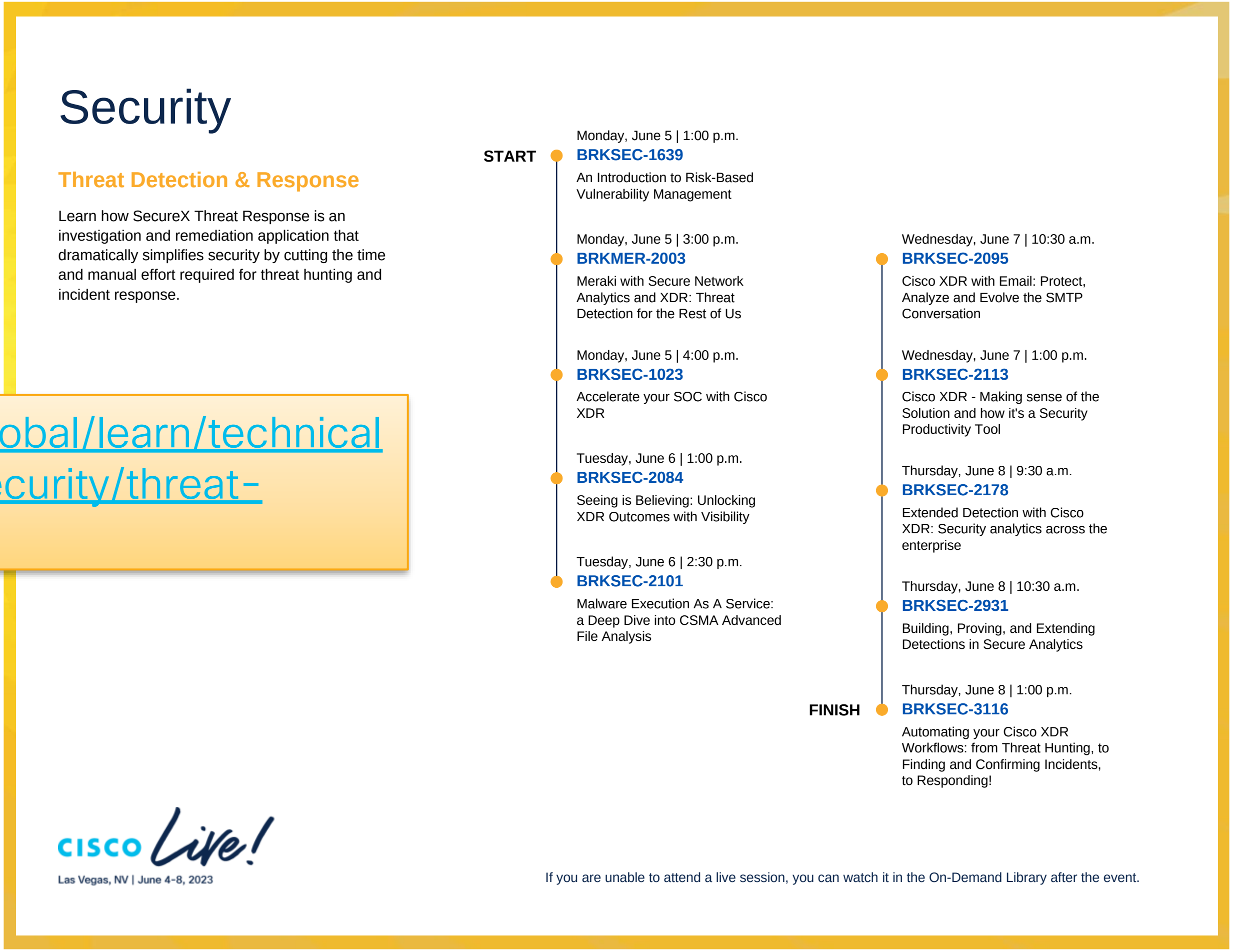
Summary



Continue your education

- Visit the Cisco Showcase 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

Learning Map



Security

Threat Detection & Response

Learn how SecureX Threat Response is an investigation and remediation application that dramatically simplifies security by cutting the time and manual effort required for threat hunting and incident response.

START

Monday, June 5 | 1:00 p.m.
BRKSEC-1639
An Introduction to Risk-Based Vulnerability Management

Monday, June 5 | 3:00 p.m.
BRKMER-2003
Meraki with Secure Network Analytics and XDR: Threat Detection for the Rest of Us

Monday, June 5 | 4:00 p.m.
BRKSEC-1023
Accelerate your SOC with Cisco XDR

Tuesday, June 6 | 1:00 p.m.
BRKSEC-2084
Seeing is Believing: Unlocking XDR Outcomes with Visibility

Tuesday, June 6 | 2:30 p.m.
BRKSEC-2101
Malware Execution As A Service: a Deep Dive into CSMA Advanced File Analysis

Wednesday, June 7 | 10:30 a.m.
BRKSEC-2095
Cisco XDR with Email: Protect, Analyze and Evolve the SMTP Conversation

Wednesday, June 7 | 1:00 p.m.
BRKSEC-2113
Cisco XDR - Making sense of the Solution and how it's a Security Productivity Tool

Thursday, June 8 | 9:30 a.m.
BRKSEC-2178
Extended Detection with Cisco XDR: Security analytics across the enterprise

Thursday, June 8 | 10:30 a.m.
BRKSEC-2931
Building, Proving, and Extending Detections in Secure Analytics

FINISH

Thursday, June 8 | 1:00 p.m.
BRKSEC-3116
Automating your Cisco XDR Workflows: from Threat Hunting, to Finding and Confirming Incidents, to Responding!

Las Vegas, NV | June 4-8, 2023

If you are unable to attend a live session, you can watch it in the On-Demand Library after the event.

https://www.ciscolive.com/global/learn/technical-education/learning-maps/security/threat-detection-response.html

Related Sessions

Session ID	Title	When
BRKSEC-2113	Cisco XDR – Making sense of the Solution and how it's a Security Productivity Tool	Friday Dec 8 1:30-3:00 PM
BRKSEC-1023	Accelerate your SOC with Cisco XDR	Wed Dec 6 2:4-3:40 PM
DEVWKS-1732	Getting started with Cisco XDR Automate workflows and atomics	Thursday Dec 7 2:30-3:15 PM
BRKMER-2234	A Common Policy for Network Agility and Security: The Unified Meraki Approach	Wed Dec 6 1:00-2:30 PM

Parting Thoughts

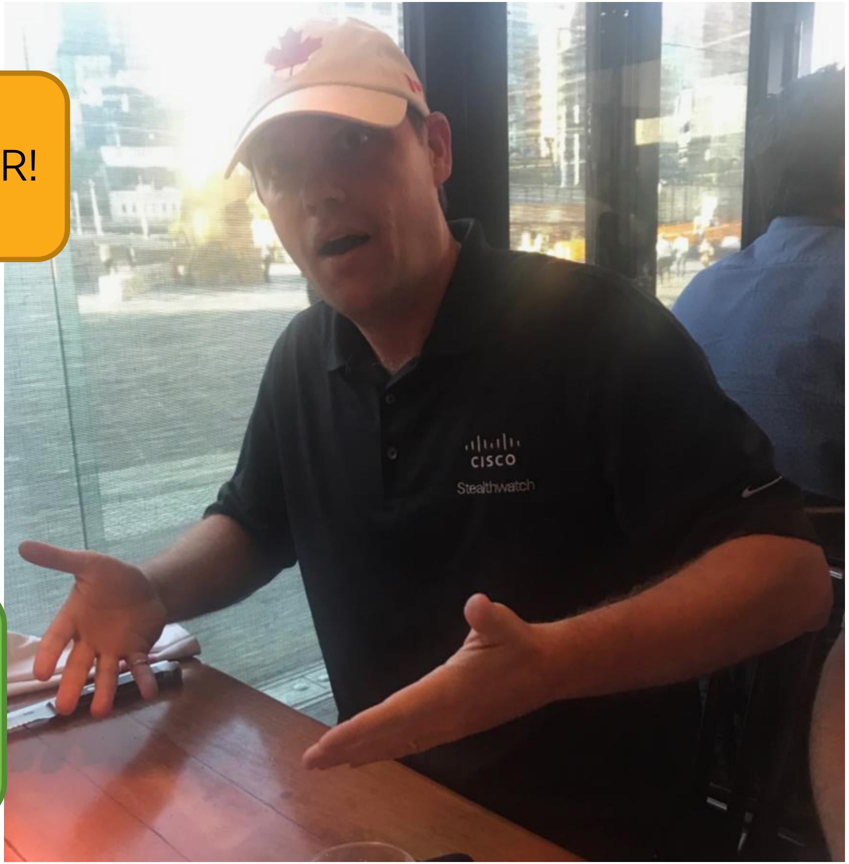
Simplify your security operations with Cisco XDR!

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

Keep your eyes open

and

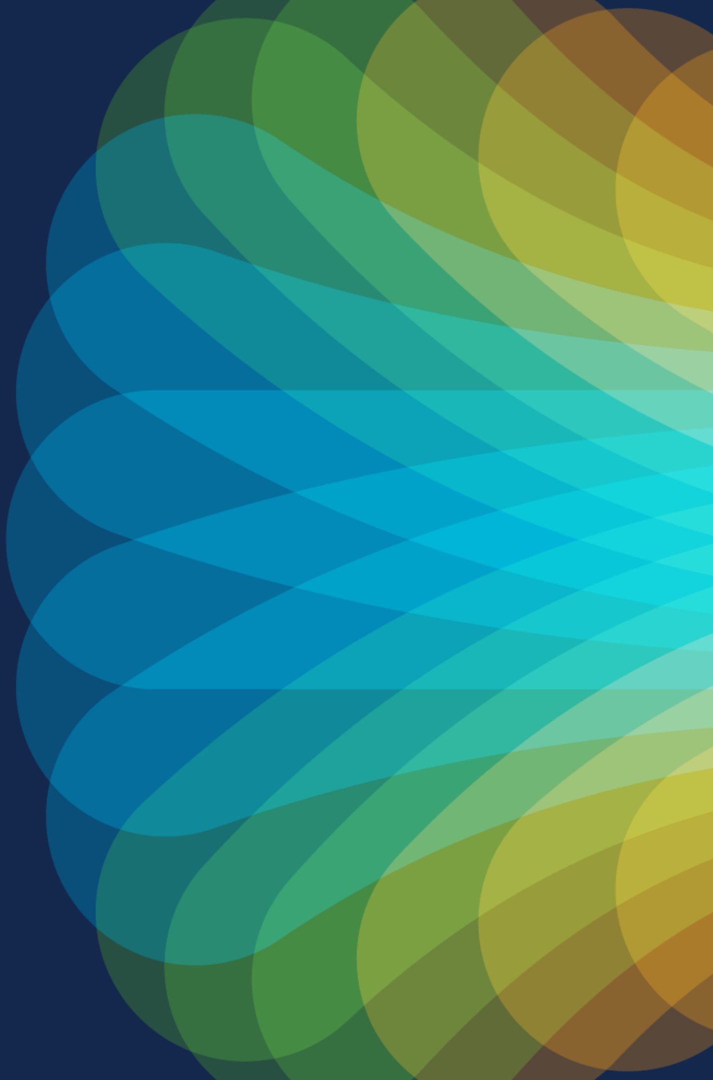
don't have your beer stolen.



THE BOATBUILDERS YARD

The bridge to possible

Thank you



cisco Live!

Let’s go

#CiscoLiveAPJC