The bridge to possible

# Visibility, Detection and Response

## with Cisco Secure Network Analytics

Matt Robertson, Distinguished Engineer

cisco Live!

BRKSEC-3019

# Abstract

Combating the constantly evolving threat actor requires visibility and analytics into host and user behaviour.

This session will explore the visibility and detection capabilities of Secure Network Analytics (Stealthwatch), deep diving into machine learning and the multiple analytic engines in the system including how they work and how to best leverage the resulting observations to detect and respond to suspicious and malicious activity in the network. Examples of threats detected using the system will be explored as well a how to leverage SecureX for investigation and response.

The target audience for this session are network and security administrators and analysts interested in learning how to best incorporate network detection and response technologies into their security operations centre.

# Agenda

**Network Behaviour Analytics:**
Understanding Secure Network Analytics Detections

**Agenda:**

- Introduction
- Visibility
- Threat Detection with SNA
- Extended Detection and Response
- Summary

Extended Detection and Response with SecureX

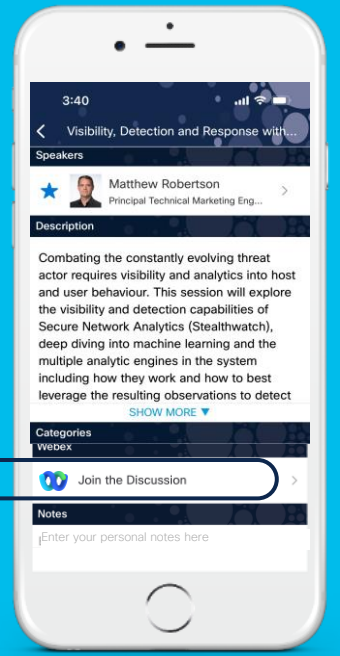
# Cisco Webex App

## 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

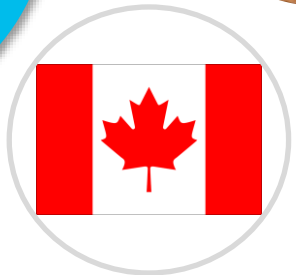



## Webex spaces will be moderated until February 24, 2023.

# About Me


## Matt Robertson

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



# 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

# So, What are Analytics?

Designing algorithms directed at achieving some outcome.

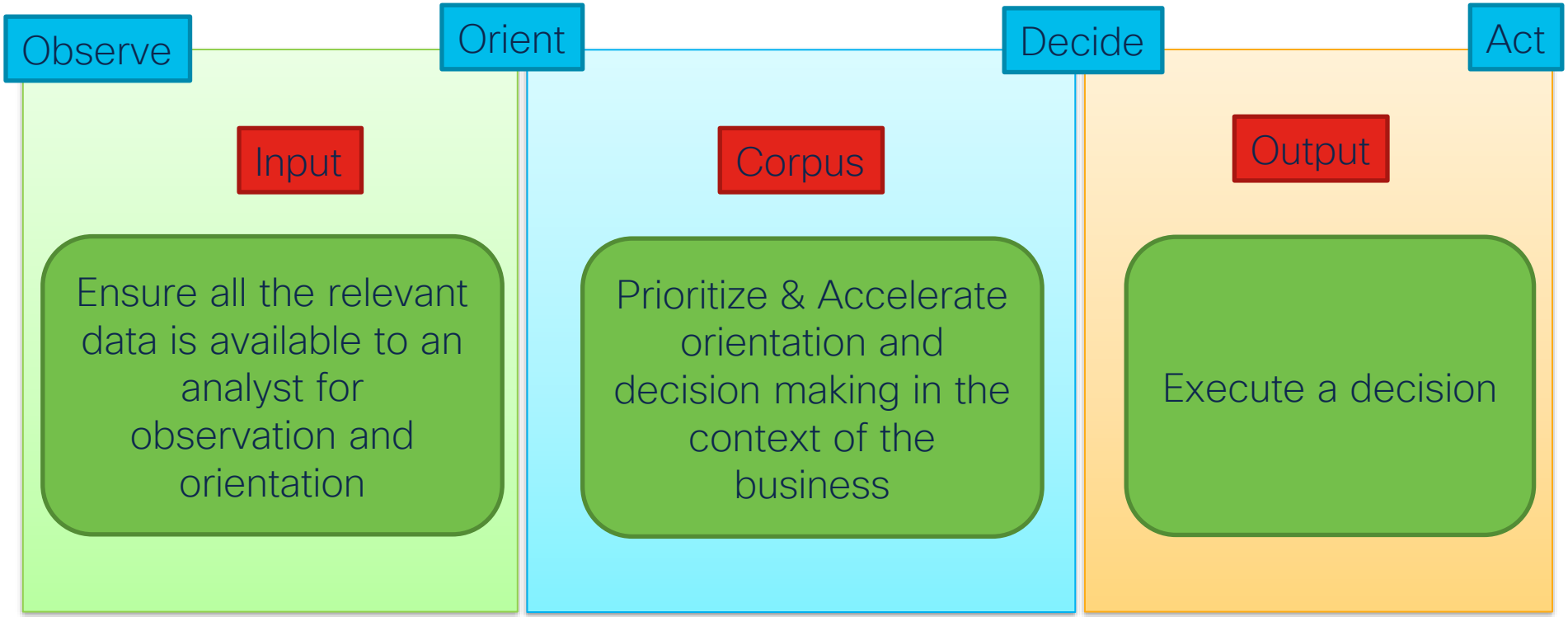
**Machine Learning:**
"Field of study that gives computers the ability to learn without being explicitly programmed."
- Arthur Samuel, 1959

Extremely useful in understanding domains that are constantly evolving with a large amount of variability

Key idea! Analytics are not magic.

Two popular ML approaches:
- Supervised
- Unsupervised

# Accelerating the SOC's OODA Loop

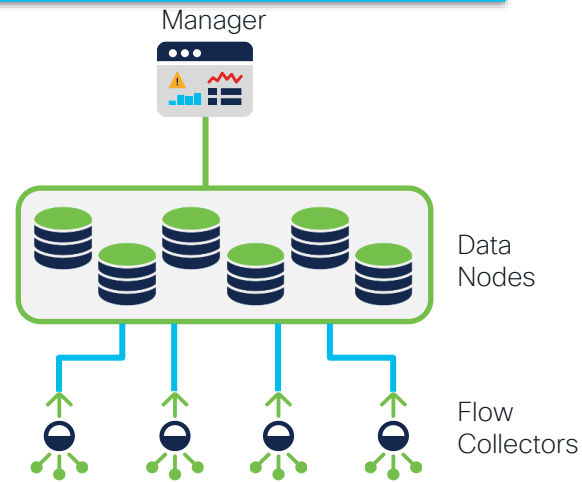


# Cisco Secure Network Analytics Portfolio

SecureX

Cisco Secure Network Analytics
(Stealthwatch on-prem)

Cisco Secure Cloud Analytics
(Stealthwatch Cloud)





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

# Network Visibility

# Network Visibility

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

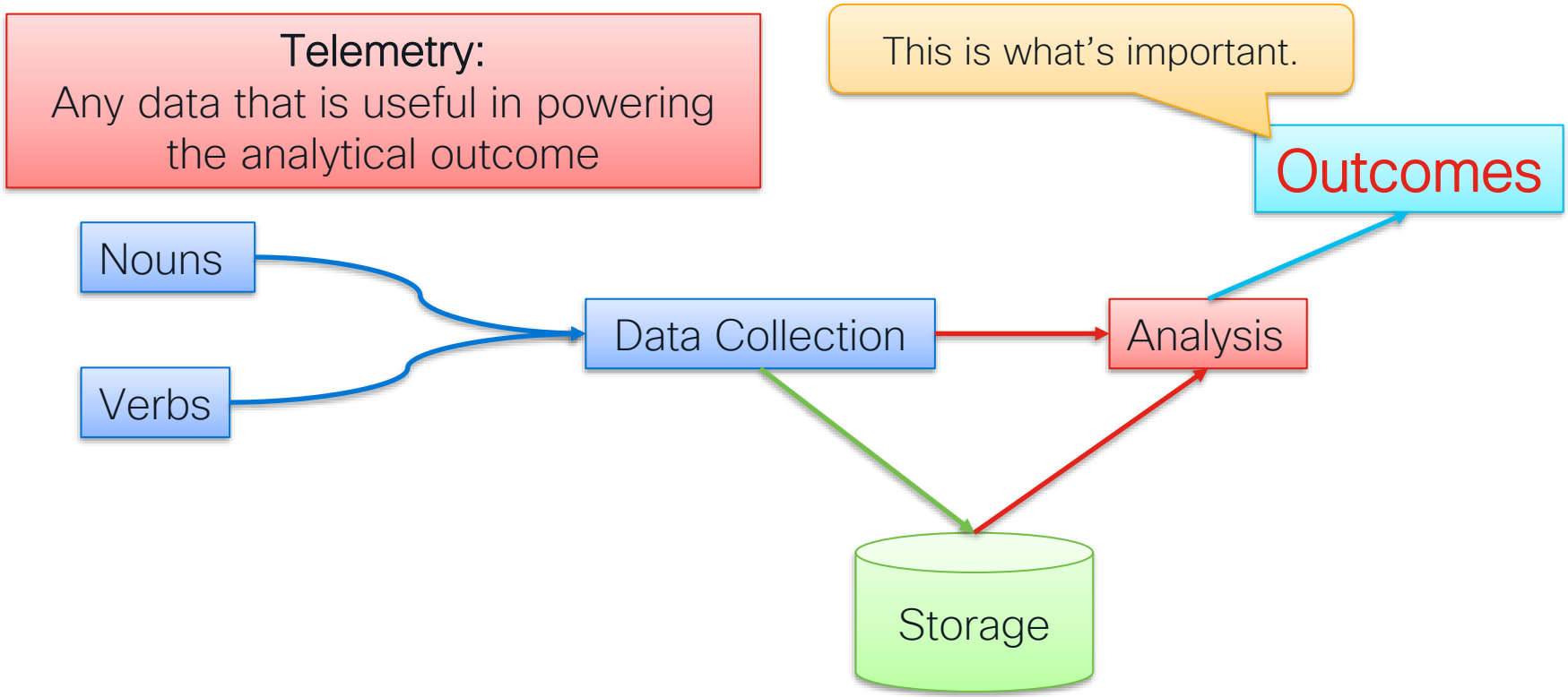
**Transaction Attributes:**
Time, ports, protocols, applications, etc.

**Host Attributes:**
IP Address, Hostname, Username, Role, etc.

**Host Attributes:**
IP Address, Hostname, Username, Role, etc.

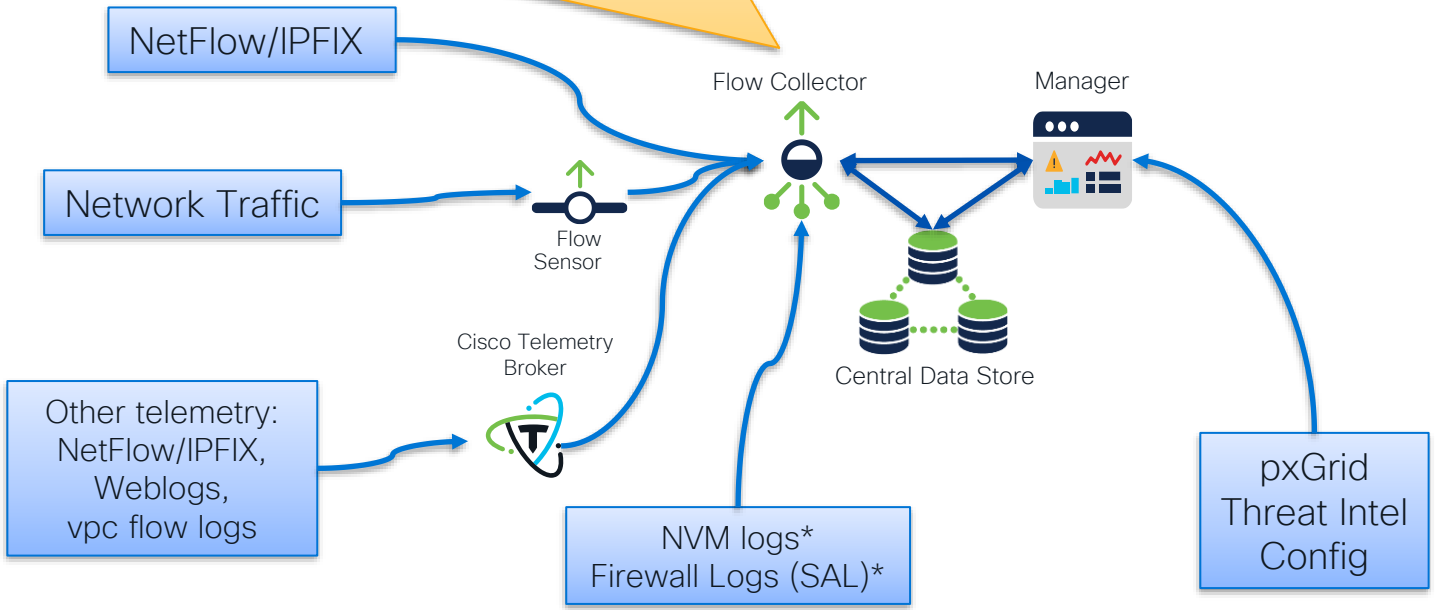
# Powering Visibility & Analytics with Telemetry

**Telemetry:**
Any data that is useful in powering the analytical outcome



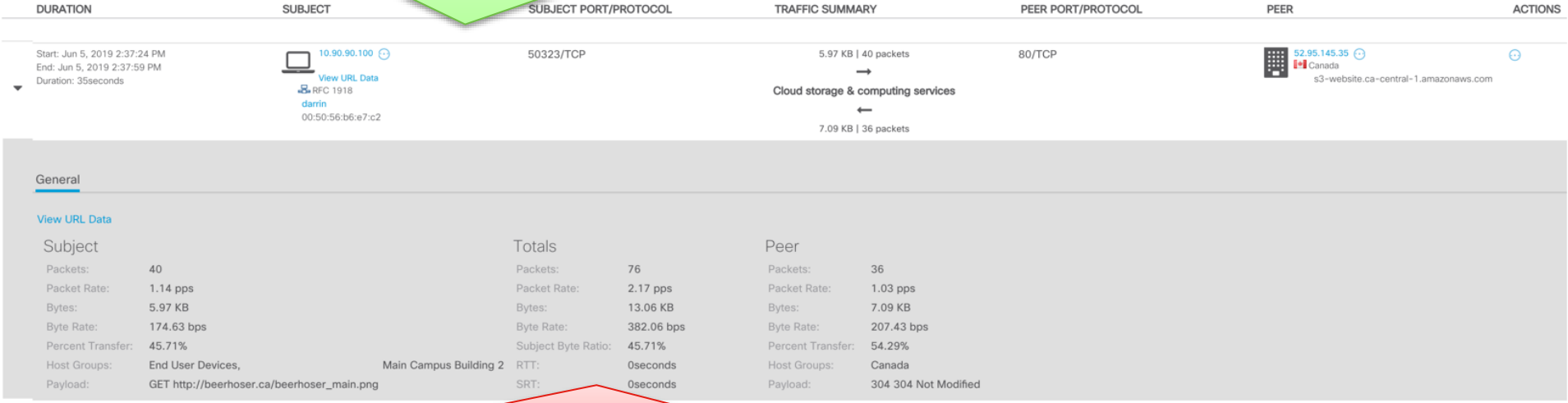
# Telemetry in SNA

Telemetry is collected, synthesized, correlated and stored in the “Flow Table”. Conceptual bi-directional conversation created. Known as the “bi-flow”.



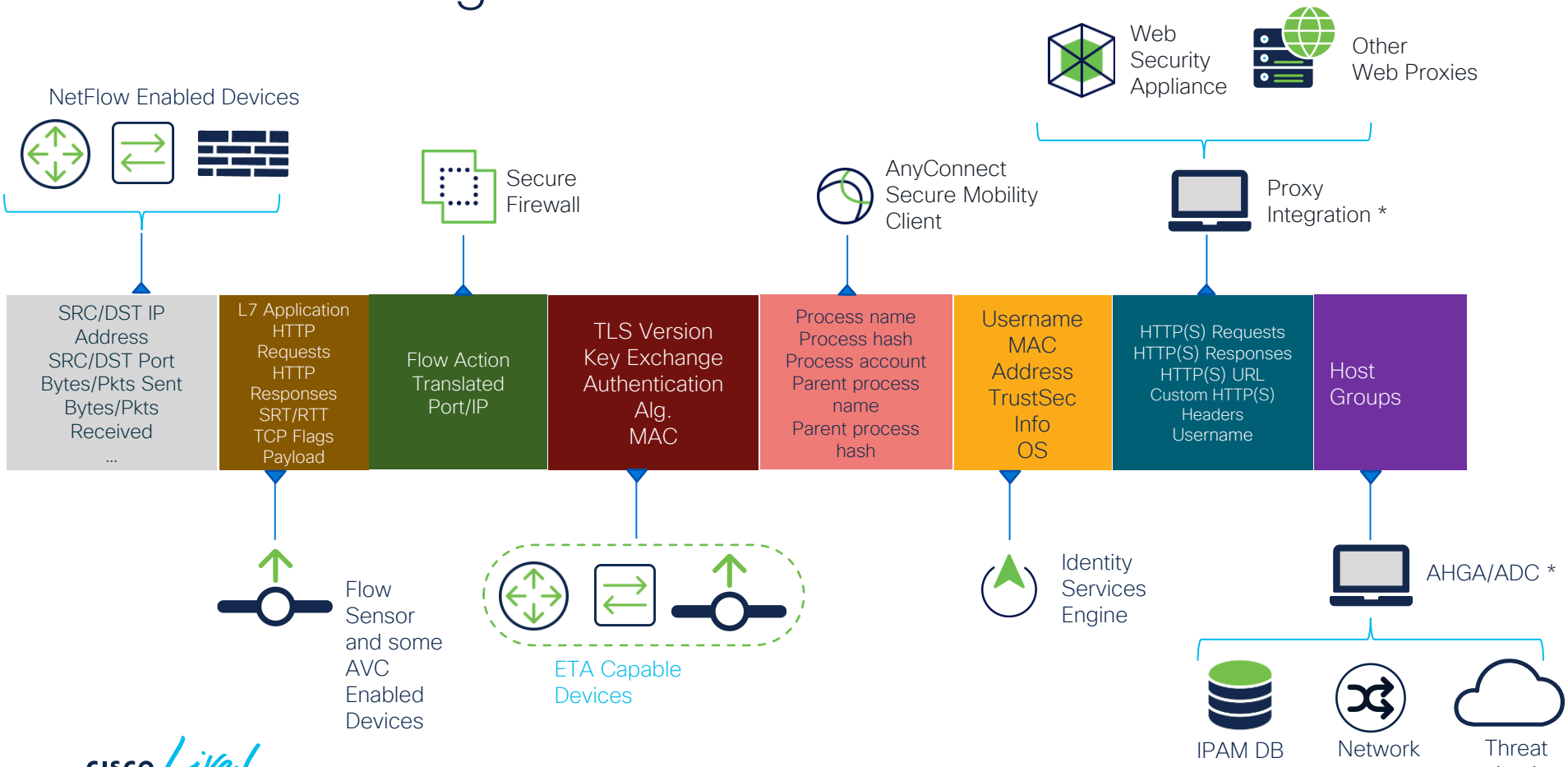
# The “Bi-Flow”

A single database row entry representing a logical bi-directional network flow between two network entities. Columns represent attributes of the connection and the two entities involved (Subject and Peer).




Telemetry from multiple sources synthesised and compressed into this single entry

# Understanding Bi-Flow Enrichment



# Meraki NetFlow Exporters

Meraki MX

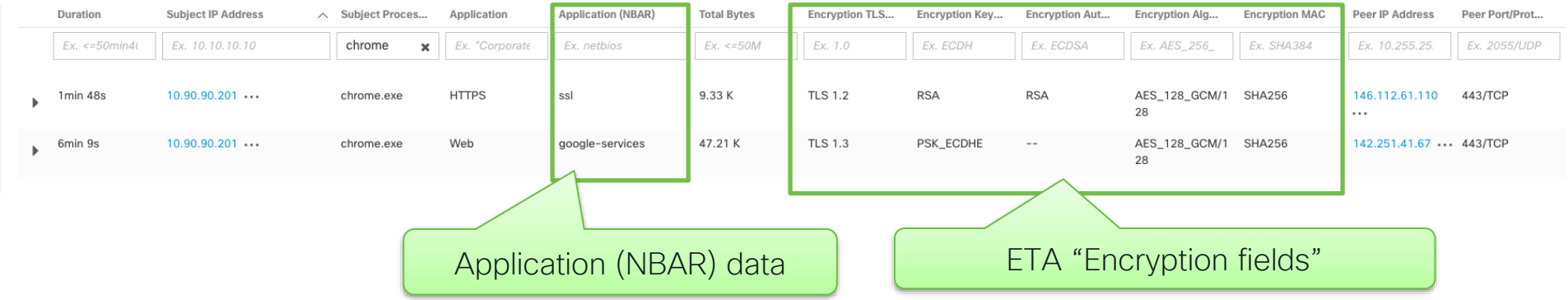
NetFlow v9

Meraki MS390 & C9300-M

IPFIX enriched with Application and ETA

# MS390 & C9300-M is an ideal SNA telemetry source

- Line rate, hardware supported telemetry
- Deep packet inspection enables application recognition
- Telemetry for advanced encrypted traffic analytics
- One click deployment to all devices



# Example Analytical Outcomes

We have data. So now what?

**Security Policy:**

Analyse network behaviour to design, implement and validate security policy

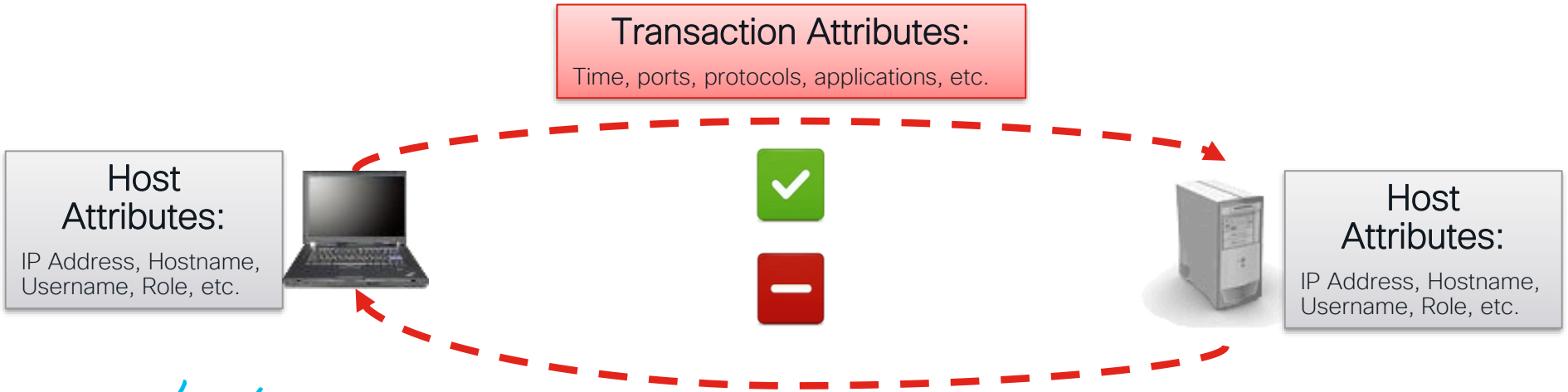
**Threat Detection:**

Analyse network behaviour to infer the presence of a threat actor

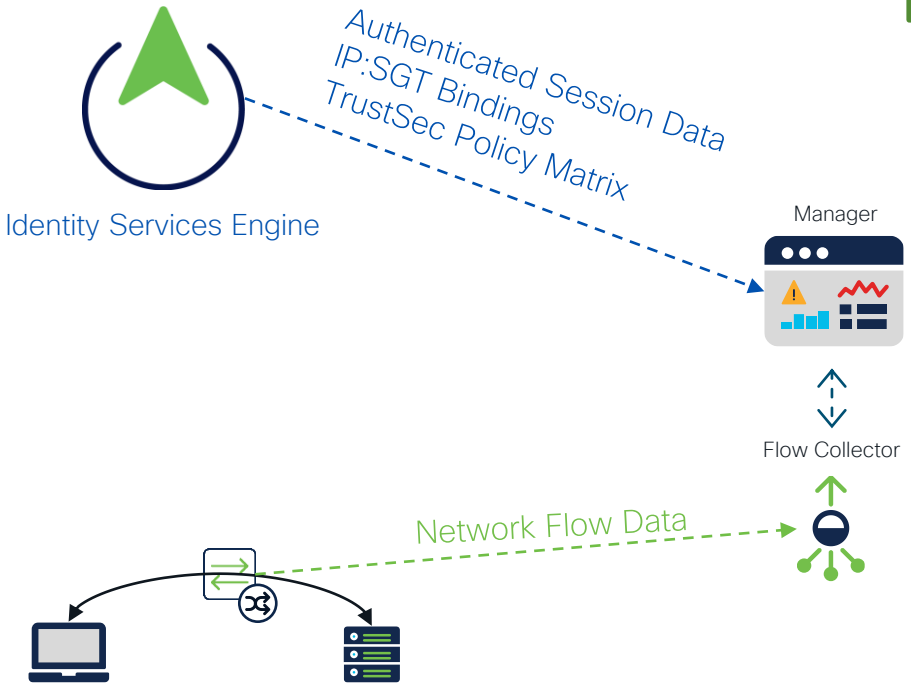
# Policy Analytics

**Validating Policy:**
How do I know that my policies are correct and won't disrupt operations?

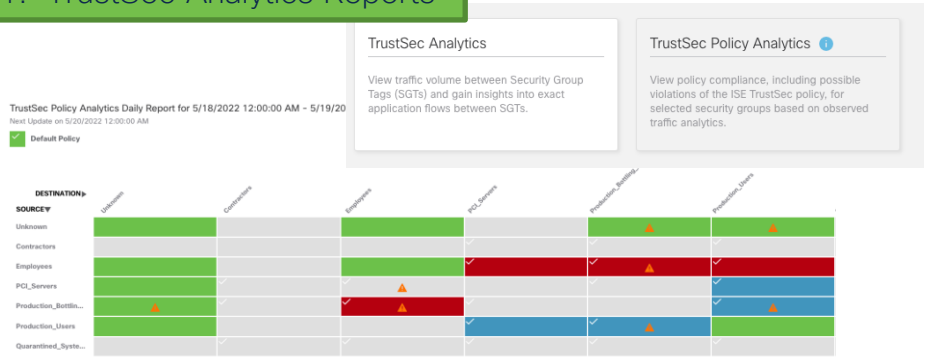
**Verifying Policy:**
How do I know that my policies are operating as intended?



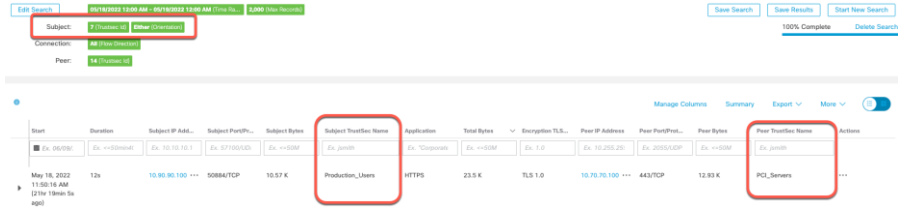
# Policy Analytics with Secure Network Analytics




1. TrustSec Analytics Reports

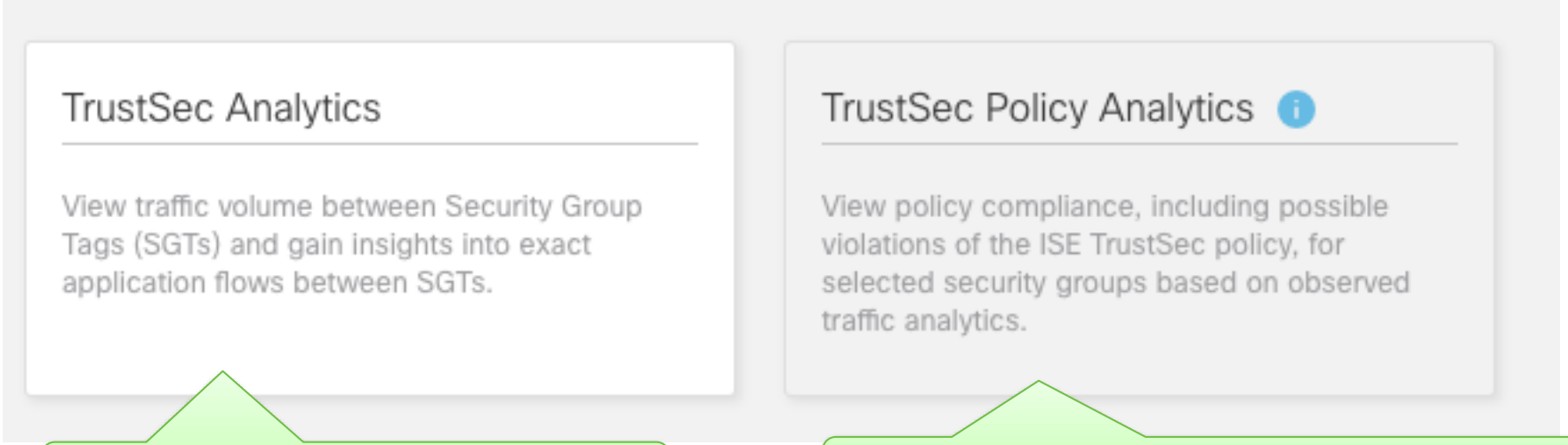



2. Direct flow analysis leveraging SGT & DGT in Flow Table
3. Custom Security Events



# TrustSec Policy Analytics

Two report types introduced in Secure Network Analytics v7.3.1



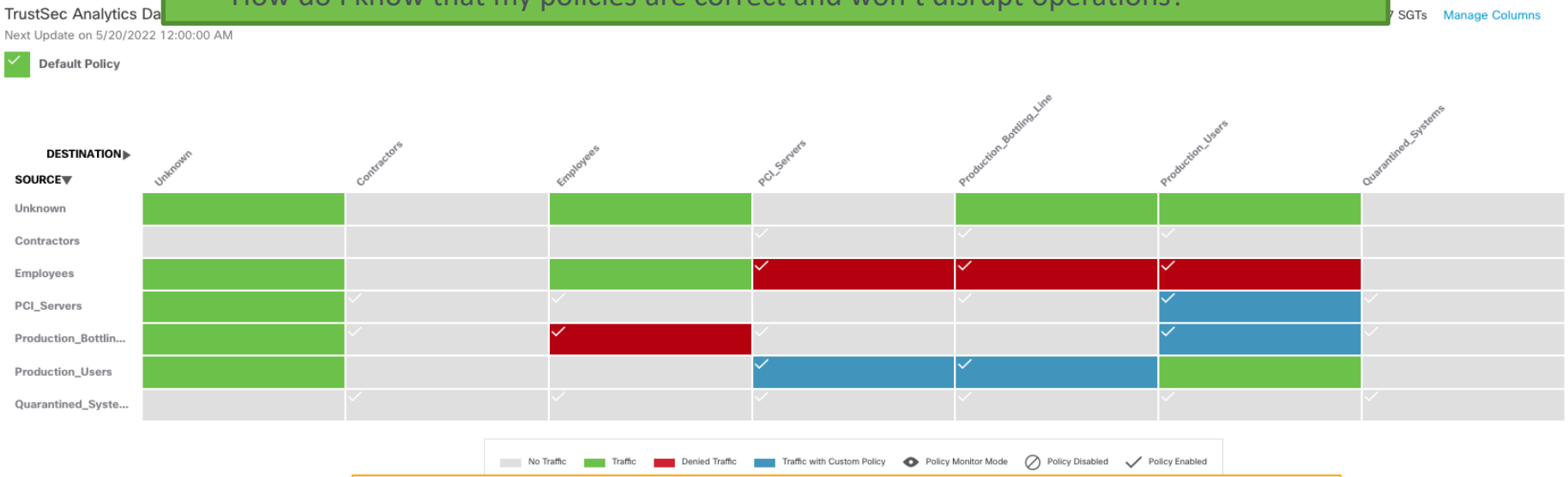

Multiple Reports of this type allowed

One report of this type allowed per deployment

# TrustSec Analytics Report

Designed to provide visibility into SGT traffic:

- How do I decide what policies should exist between my groups?
- How do I know that my policies are correct and won't disrupt operations?




- Gray – no traffic
- Green – there is traffic and a *permit IP* ACL exists
- Red – there is traffic and a *deny IP* ACL exists
- Blue – there is traffic and an ACL other than **permit** *IP* or **deny IP** exists

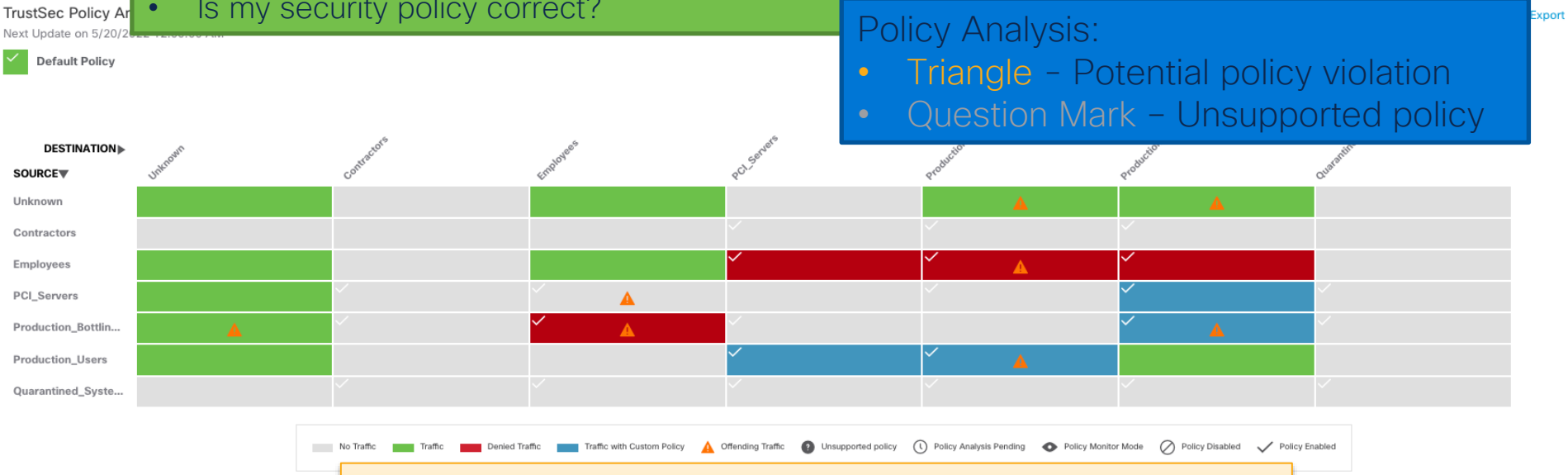
# SNA: TrustSec Policy Analytics Report

Designed to help verify correctness and adherence to TrustSec policy:

- Is my security policy being enforced as intended?
- Is my security policy correct?

Policy Analysis:

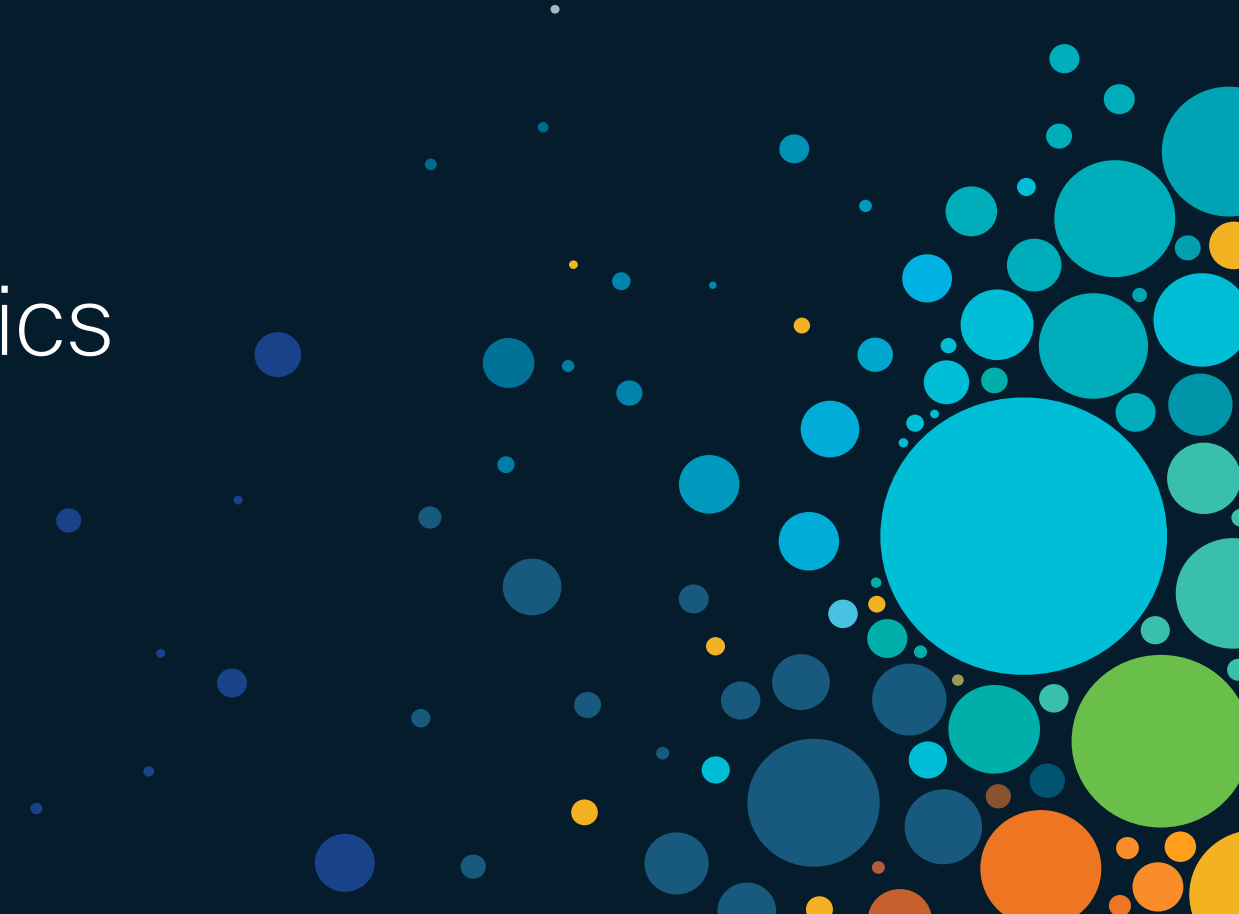
- Triangle – Potential policy violation
- Question Mark – Unsupported policy




- Gray – no traffic
- Green – there is traffic and a *permit IP* ACL exists
- Red – there is traffic and a *deny IP* ACL exists
- Blue – there is traffic and an ACL other than **permit** *IP* or **deny IP** exists

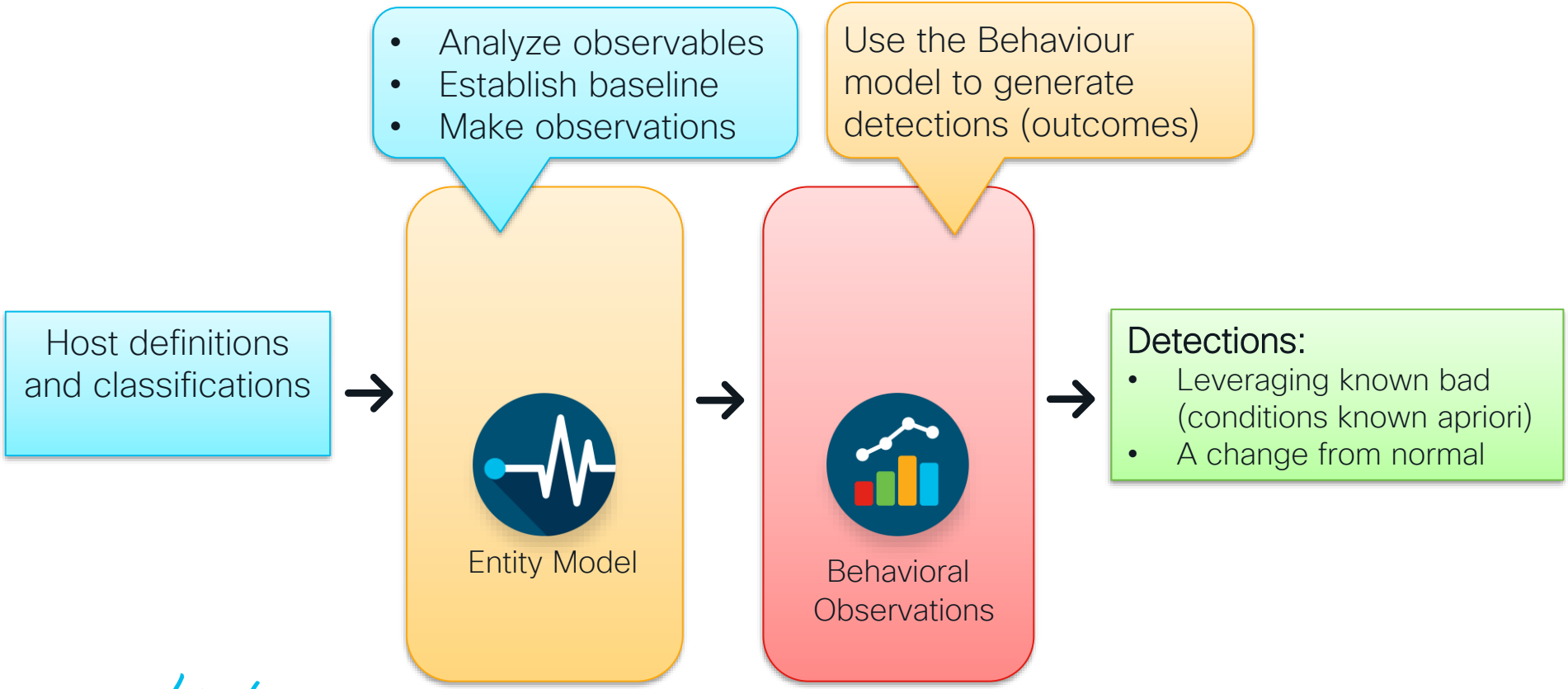
# Policy Analytics Demo

# Threat Analytics with SNA



cisco Live!

# Behavioural Modelling and Detection



# Layers of Detection in SNA

## On Box

### Custom Security Events

- User Defined Policy
- Generate an alarm based on flow attributes

### Core Events

- Run on each flow collector
- 98+ tunable behavioural algorithms:
  - Statistical anomaly detection
  - Policy based detection

### Relationship Events

- Interaction between host groups that violate a policy setting
- Directly created or automatically created from network diagram

### "Analytics" Node (New)

- Runs on Manager, requires central data store
- Common network flow analytics with Secure Cloud Analytics

## Cloud Enabled

### Threat Intelligence

- C&C, Bogon, Tor Entry/Exit Nodes
- Powered by Cisco Talos

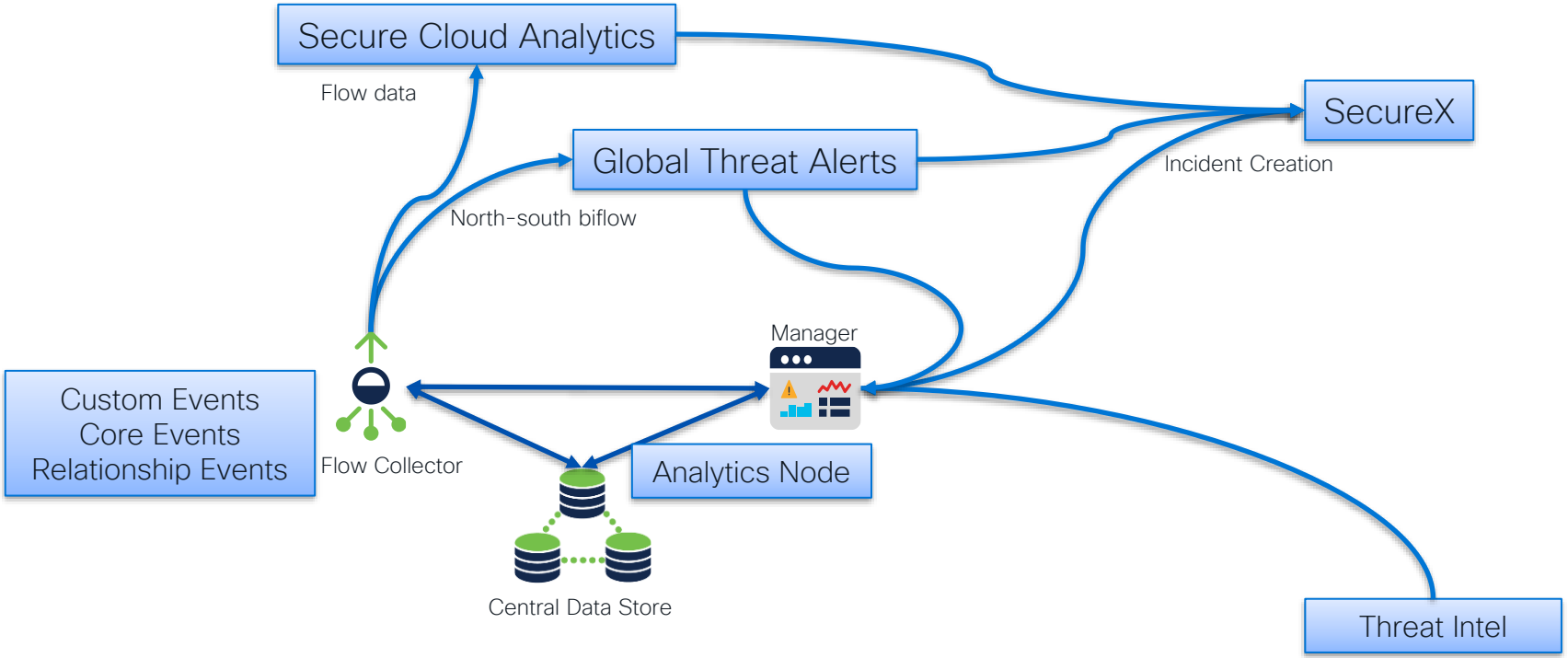
### Global Threat Alerts (Cognitive Intelligence)

- Multi-layer Machine Learning
- Malware classification in encrypted and un-encrypted traffic
- Global campaign correlation to local incidents

### Secure Cloud Analytics

- Comprehensive entity modelling
- 140+ (and growing) network and IaaS behaviour alarms
- Alert Chaining (beta)
- SCA license required

# Analytics Pipeline



# Custom Security Events

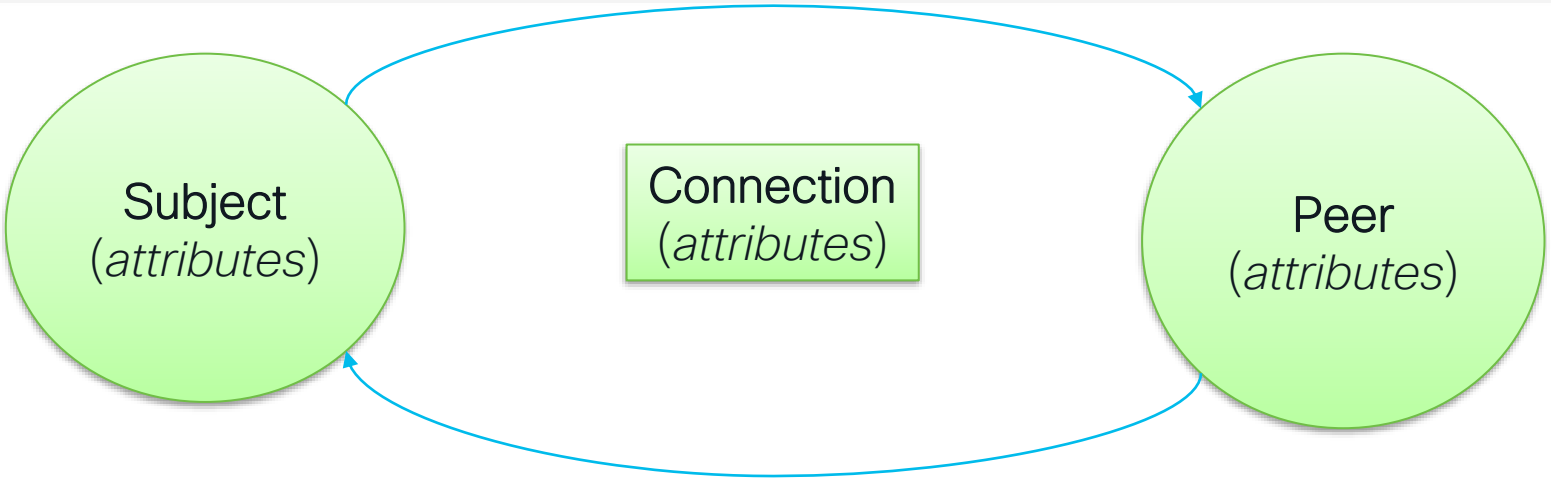
**Matt's Note:**

When implemented these are often the most immediately actionable events

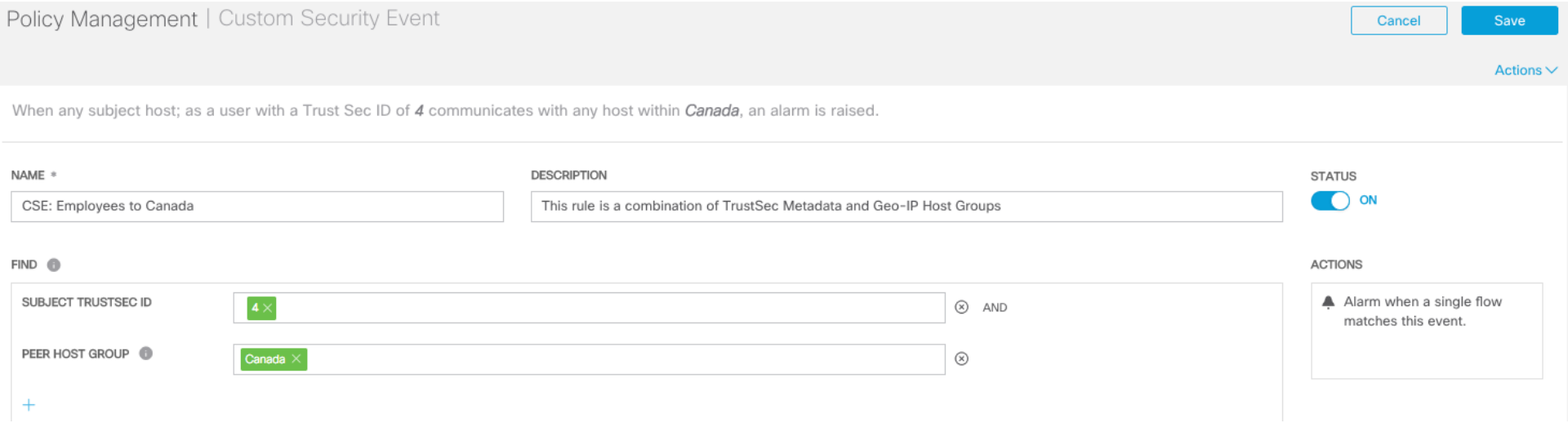
**Custom Security Events**

- User Defined Policy
- Generate an alarm based on flow attributes

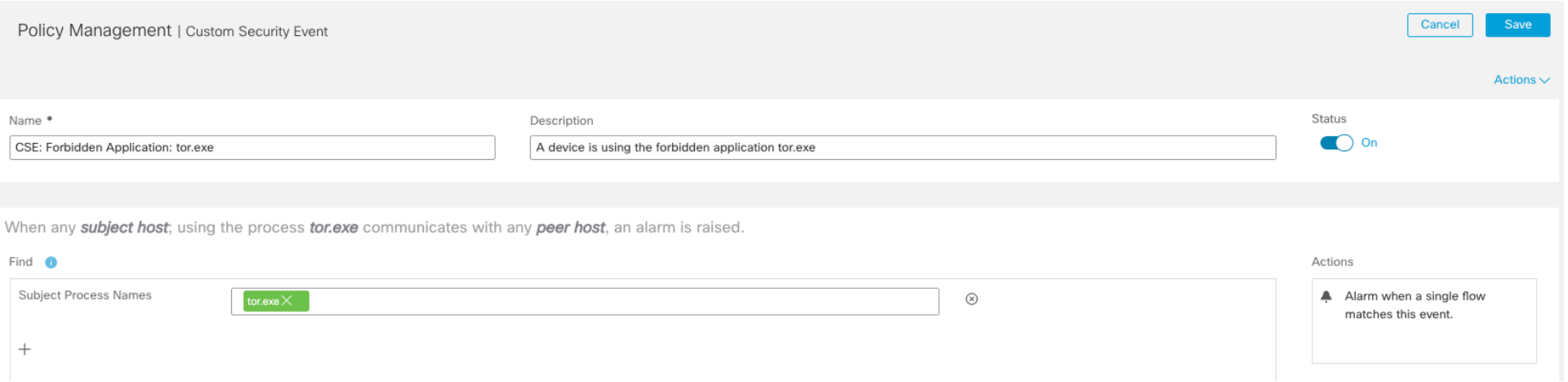
Generate an action when a single flow matches the selected conditions



# Example CSE using TrustSec/SD Access and Geo-IP Attributes



# Example CSE using Endpoint Attributes from CSC NVM Module

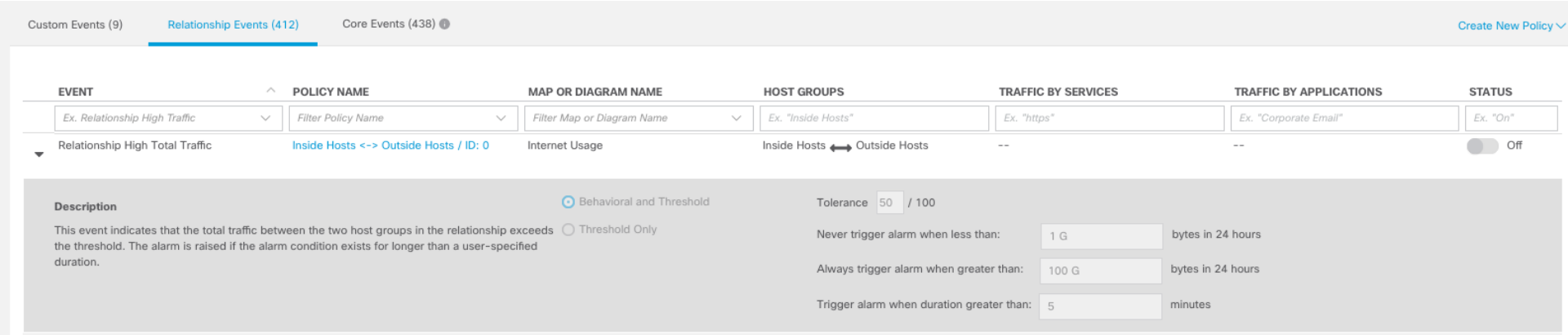


# Relationship Events

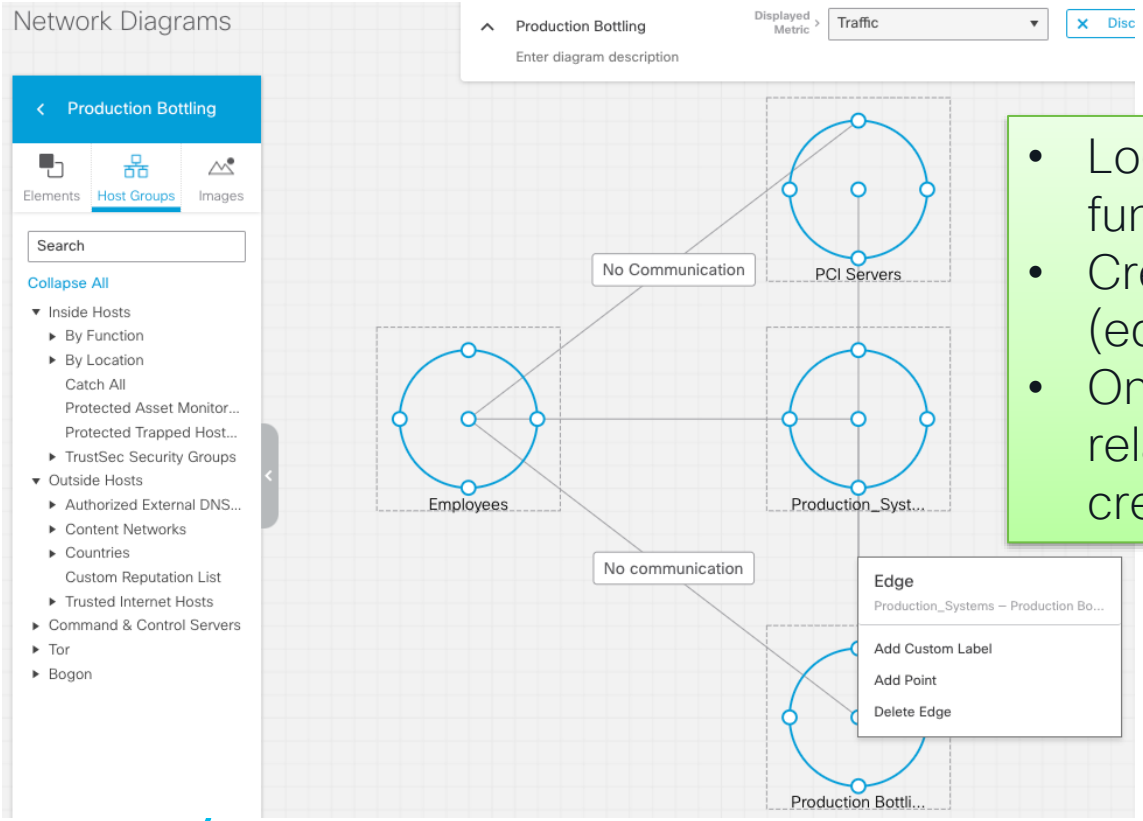
**Matt's Note:**

Can be useful for traffic presence/absent notifications

- Interaction between host groups that violate a policy setting
- Directly created or automatically created from network diagram



# Network Diagram

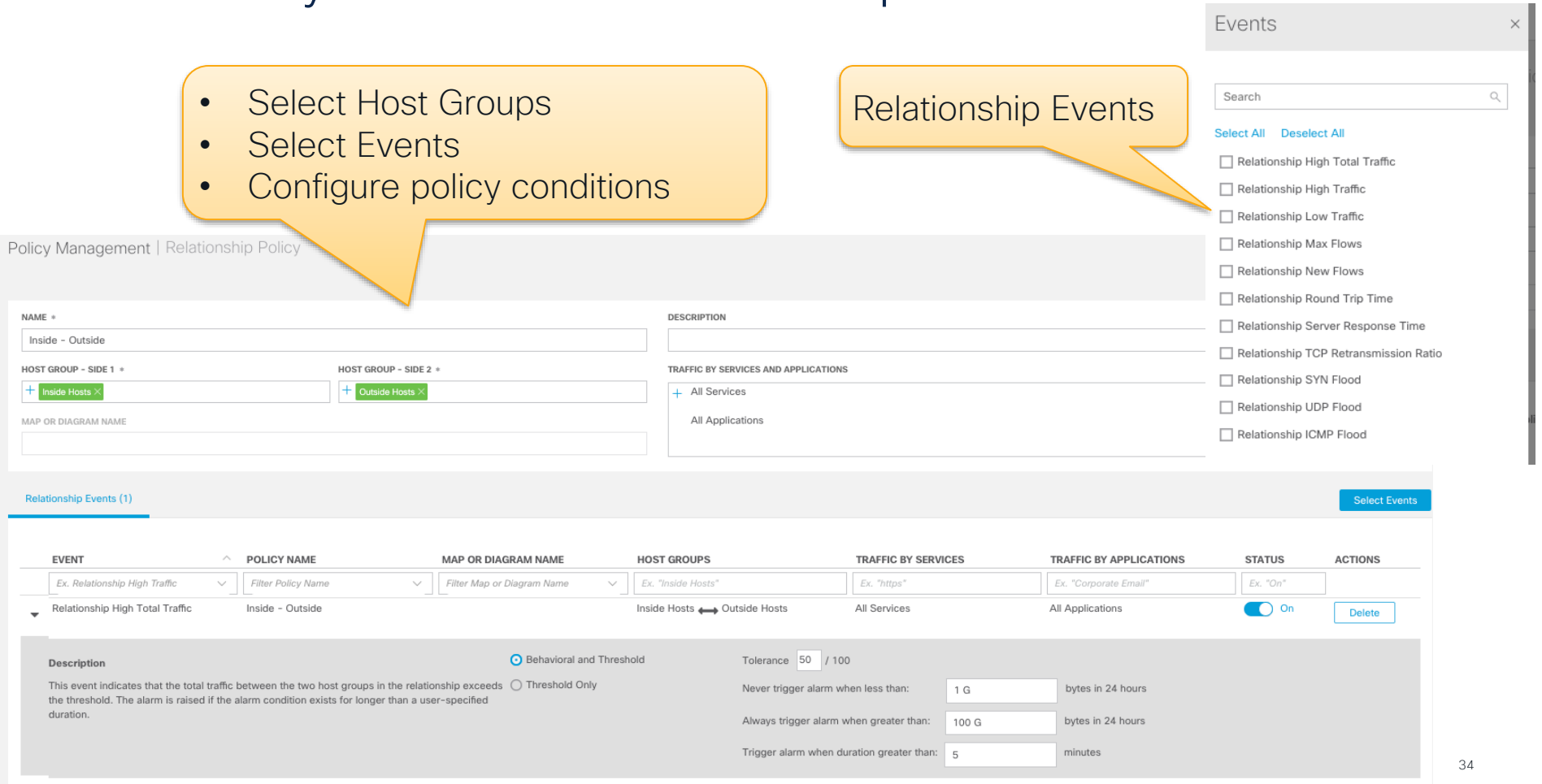



- Logical representation of business functions
- Created by defining relationships (edges) between host groups
- Once an edge is defined relationship policy is automatically created

# Manually Created Relationship Events

- Select Host Groups
- Select Events
- Configure policy conditions

Relationship Events



# Core Events

## Core Events

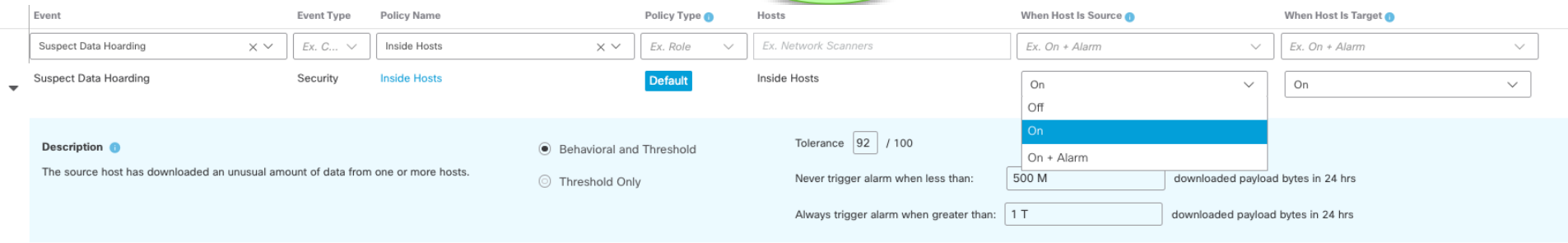
- Run on each flow collector
- 98+ tunable behavioural algorithms:
  - Statistical anomaly detection
  - Policy based detection

**Entity**
(IP Address, Host Group)

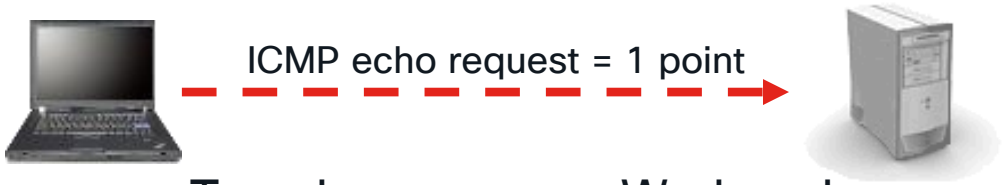
## Matt's Note:

Not every algorithm needs to be used. Operationalising can take some thought, tuning and use of host groups.

For every algorithm, maintain historical model of entity's behaviour. Generate an event when conditions are met.



# Example (Very Simple) Core Event: ICMP_ECHO_REQUEST




| Monday | Tuesday | Wednesday | Thursday |
|---|---|---|---|
| ICMP Points:<br>• Today: 10<br>• 30-day Model: 10 | ICMP Points:<br>• Today: 20<br>• 30-day Model: 15 | ICMP Points:<br>• Today: 15<br>• 30-day Model: 15 | ICMP Points:<br>• Today: 1000<br>• 30-day Model: 15 |

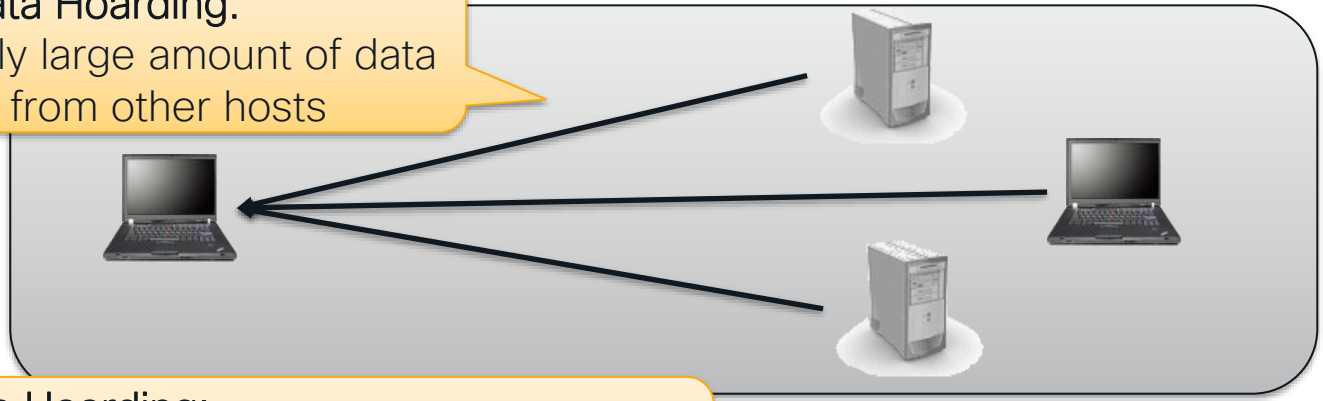
Anomaly condition for algorithm met. Observation generated.

Note 1: Anomaly condition requires 7 days of traffic baseline in real life.

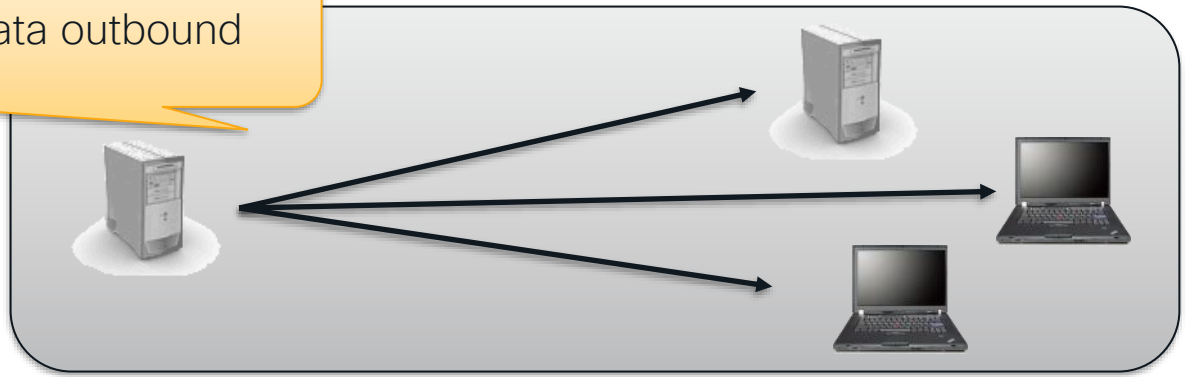
Note: 2: The Model is a little more complicated than a normal curve.

# Example Algorithm: Data Hoarding

Suspect Data Hoarding:
- Unusually large amount of data inbound from other hosts



Target Data Hoarding:
- Unusually large amount of data outbound from a host to multiple hosts



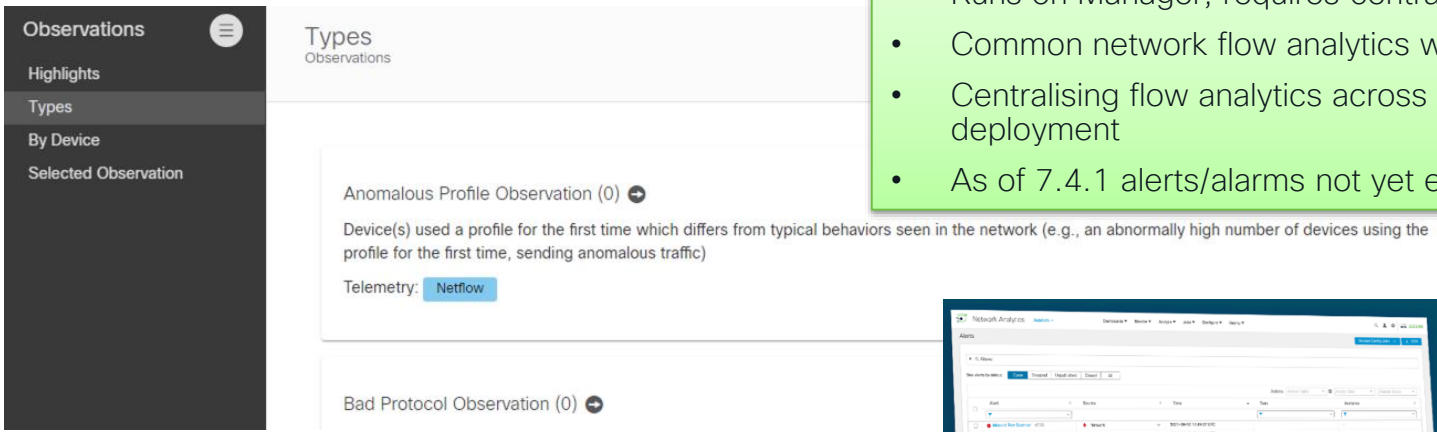
# Analytics Node (on box)

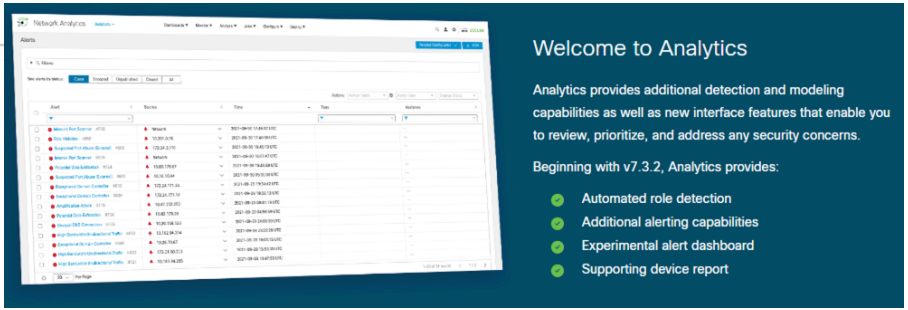

**Matt's Note:**

Relatively new, useful for context, still being explored for operationalising

## "Analytics" Node (New)

- Runs on Manager, requires central data store
- Common network flow analytics with Secure Cloud Analytics
- Centralising flow analytics across a multi-flow collector deployment
- As of 7.4.1 alerts/alarms not yet exportable



# Threat Intelligence Events

**Matt's Note:**

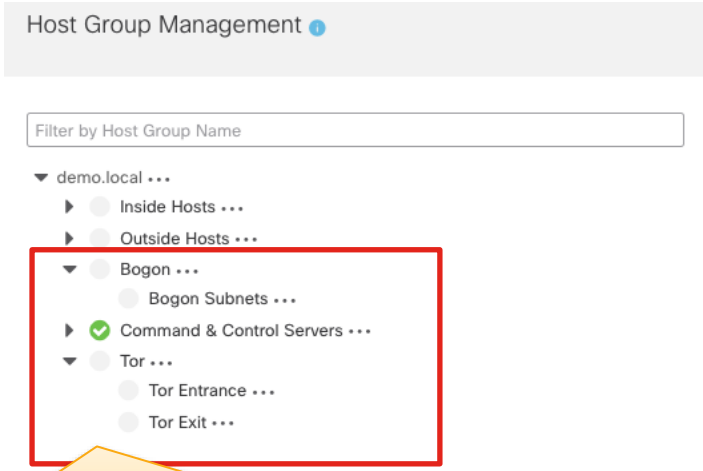
These are often immediately actionable events

## Threat Intelligence

- C&C, Bogon, Tor Entry/Exit Nodes
- Powered by Cisco Talos

## Alarms Include:

- Connection From Bogon Address Attempted
- Connection From Bogon Address Successful
- Connection From Tor Attempted
- Connection From Tor Successful
- Bot Command & Control Server
- Bot Infected Host- Attempted C&C
- Bot Infected Host – Successful C&C




Subscribing to threat intel will automatically create these host groups

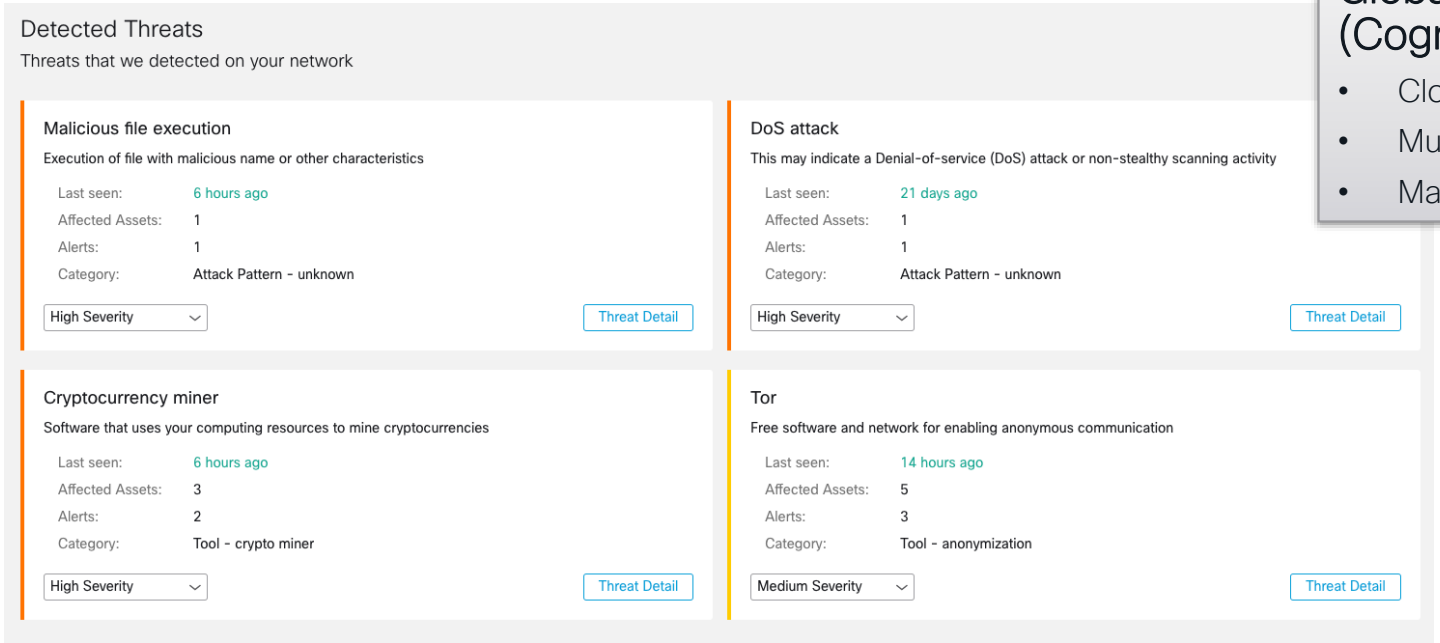
# Global Threat Alerts

**Matt's Note:**

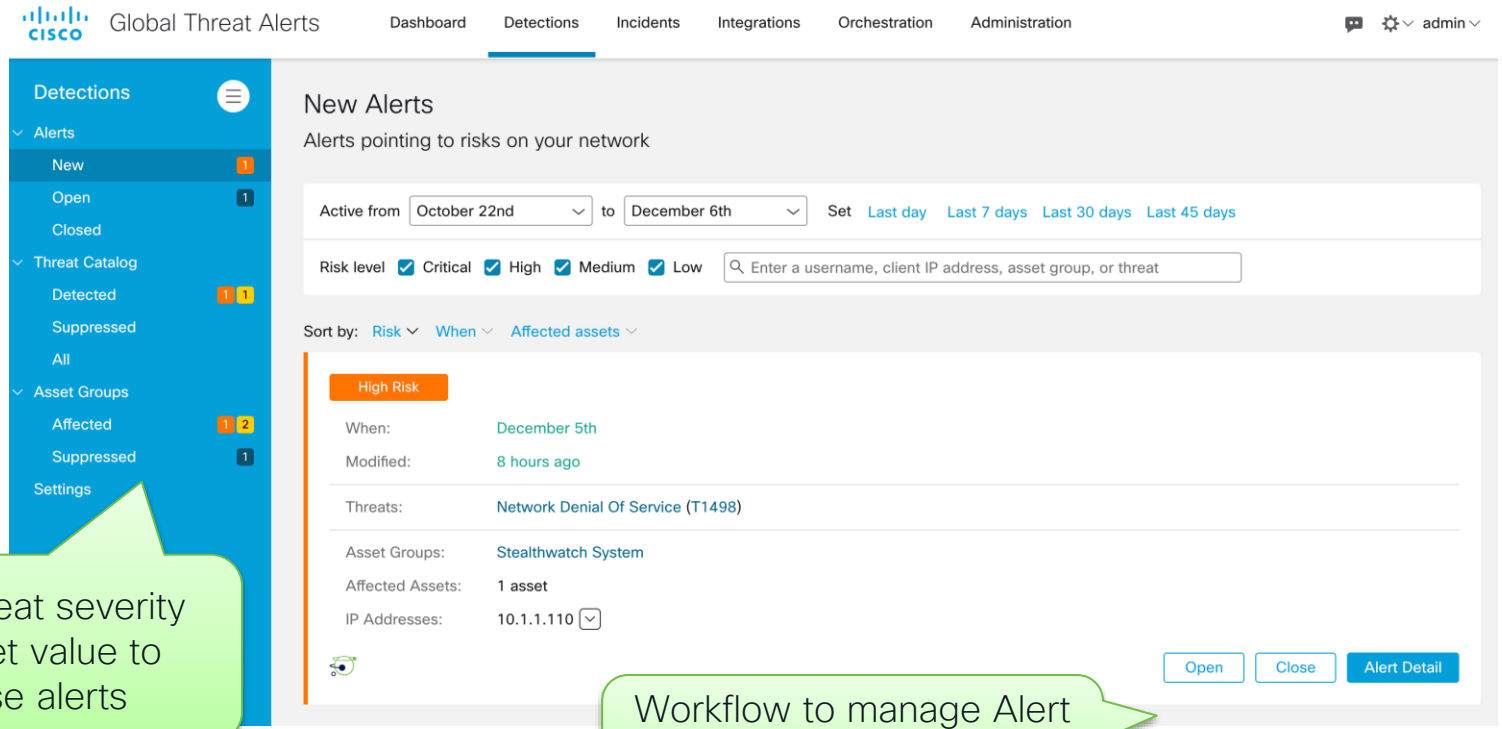
Useful in identifying presence of evasive threats

## Global Threat Alerts (Cognitive Intelligence)

- Cloud Hosted
- Multi-layer Machine Learning
- Malware classification



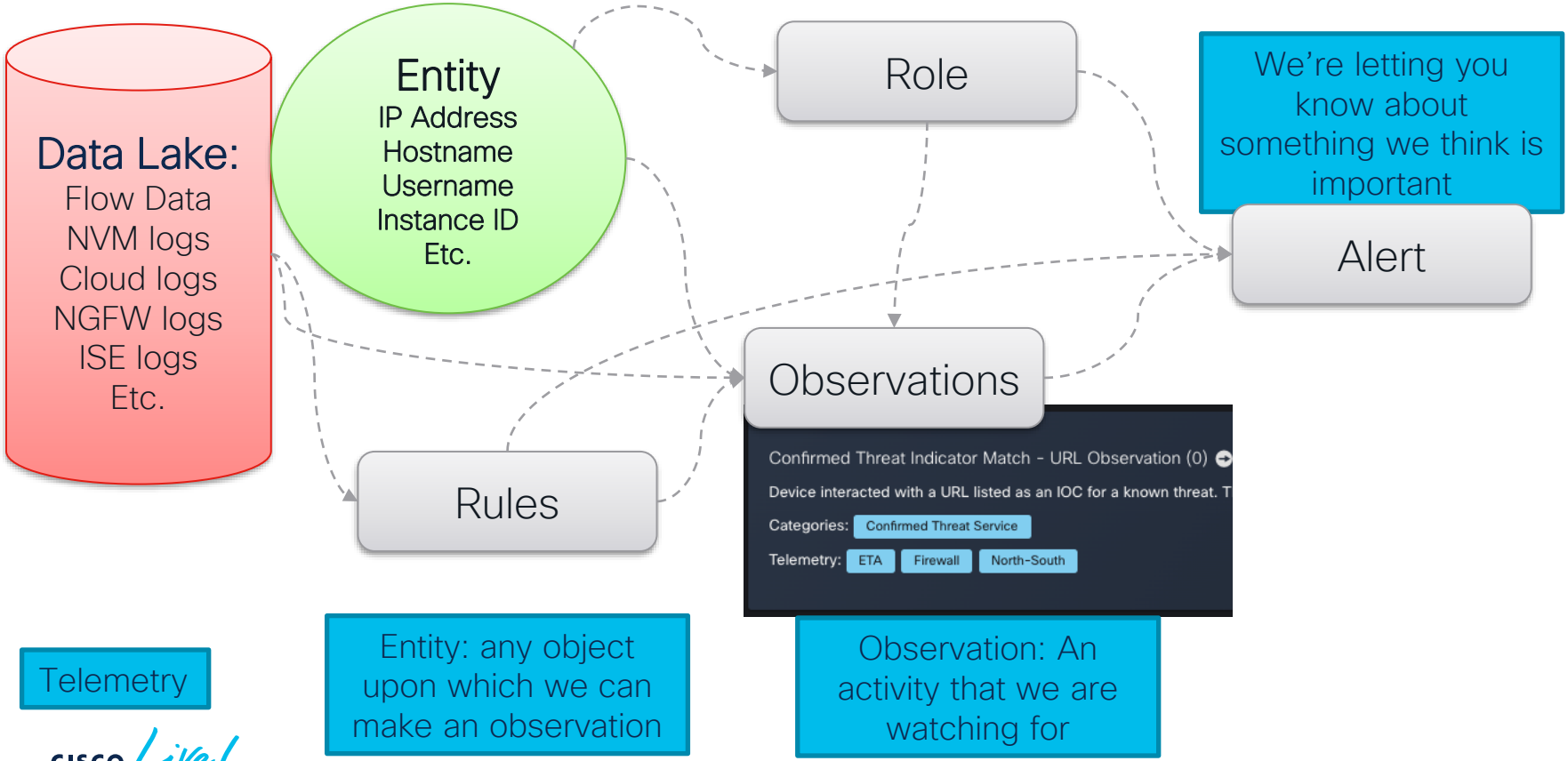
# Global Threat Alerts



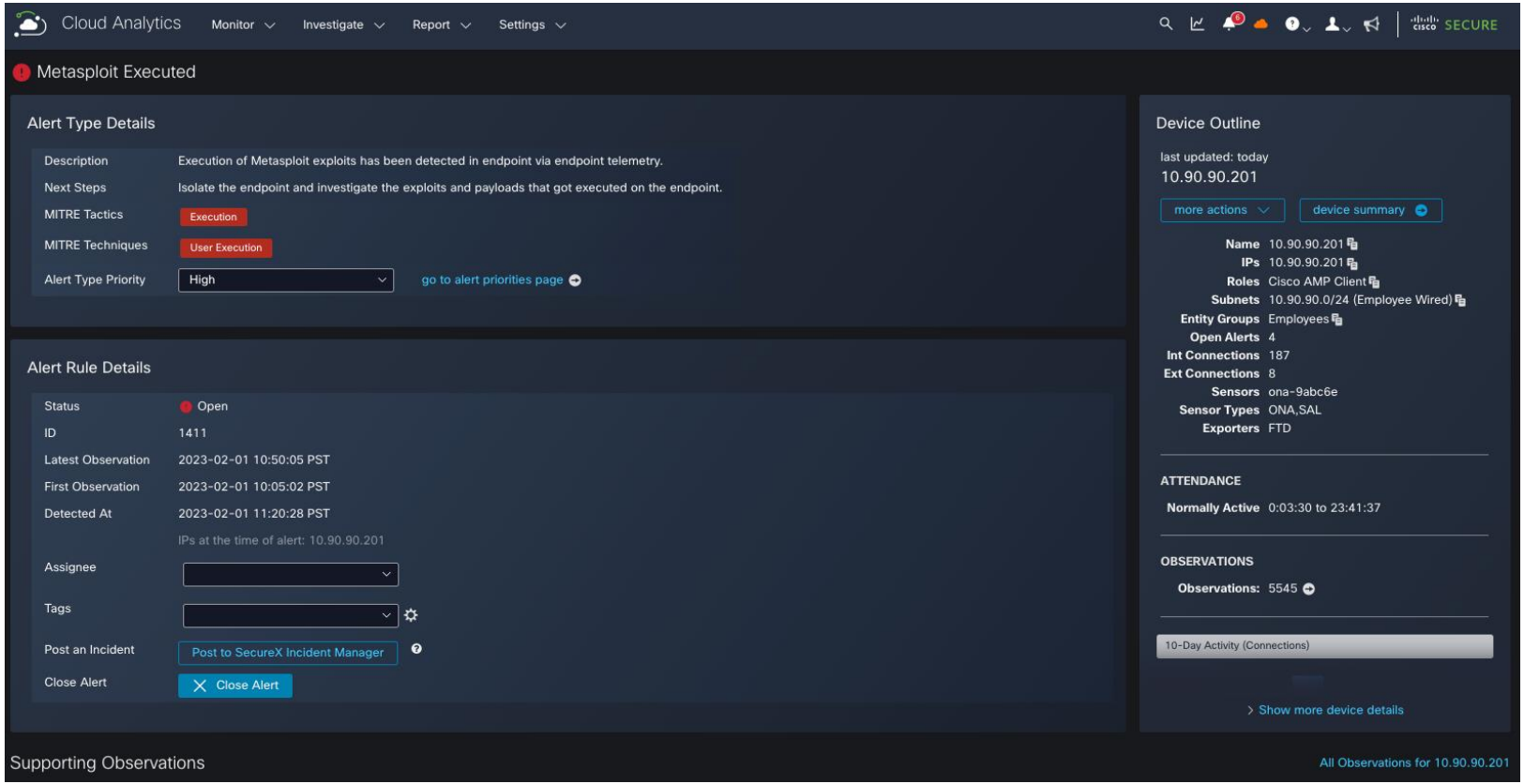

Adjust threat severity and asset value to prioritse alerts

Workflow to manage Alert – open, close, promote to SecureX, etc.

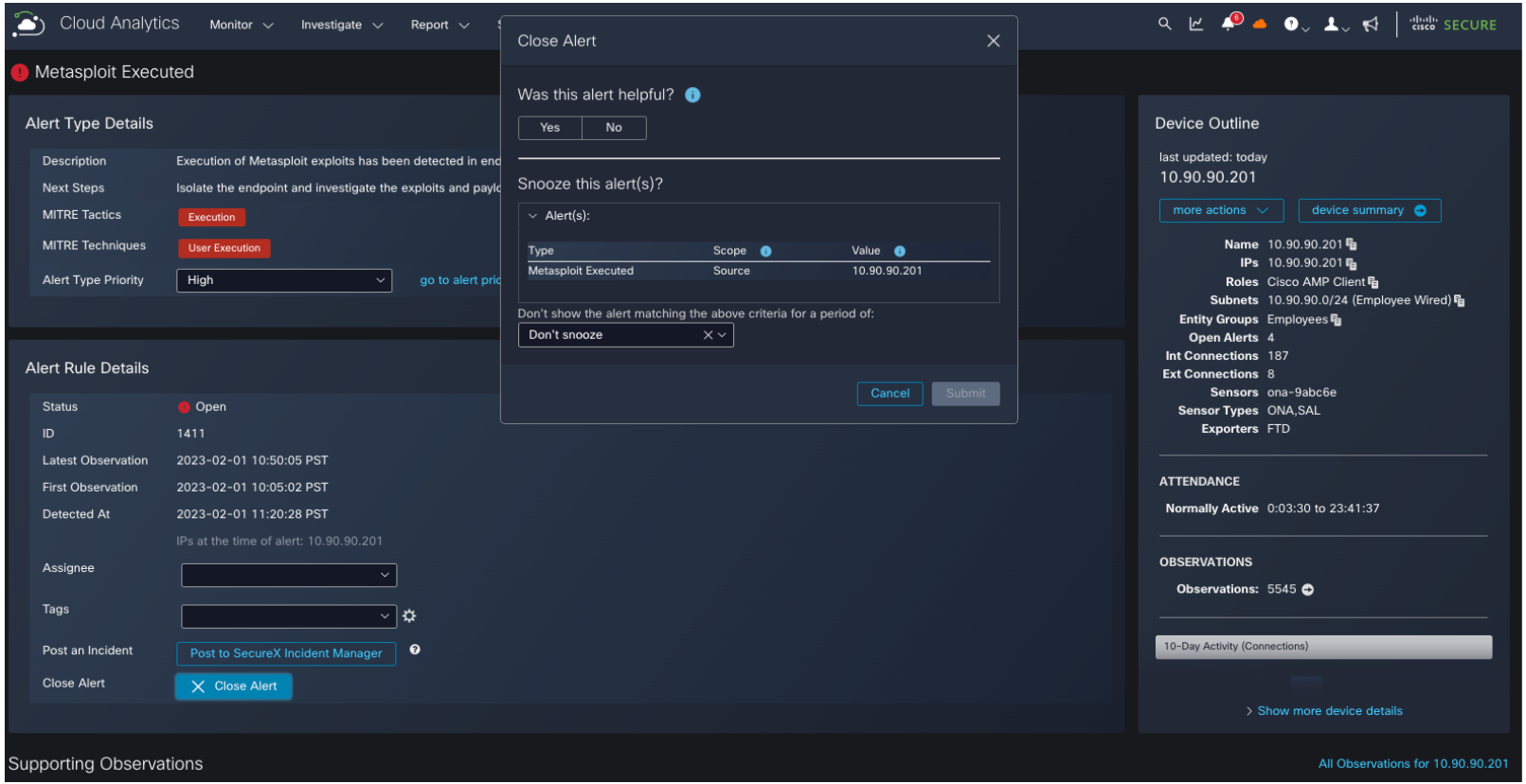
# Secure Cloud Analytics



# SCA Alert



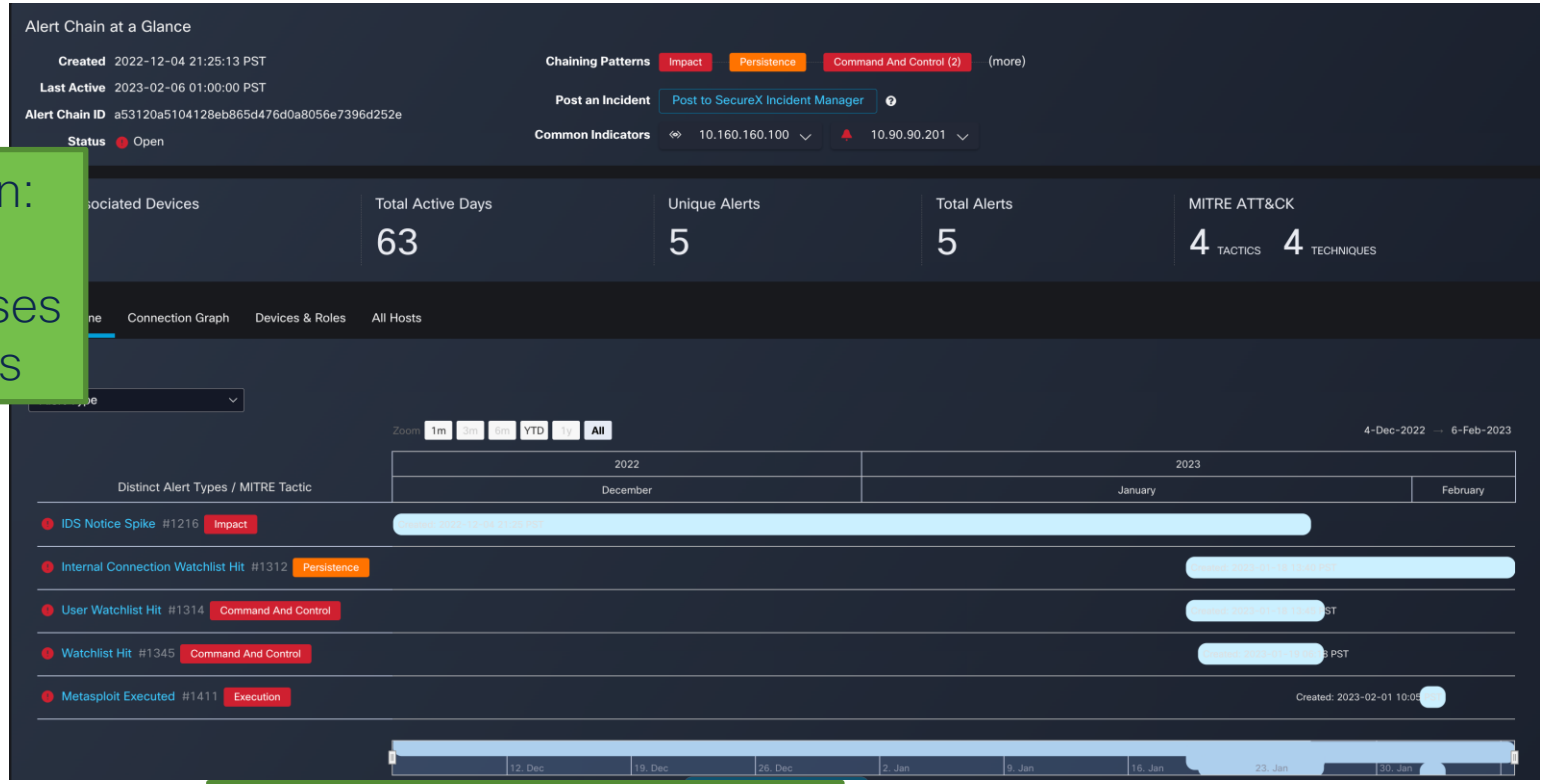
# SCA Alert: Was this alert helpful?



# Alert Chaining (Beta)

Automatic correlation of related alerts

Correlation on:
- Devices
- IP Addresses
- Usernames



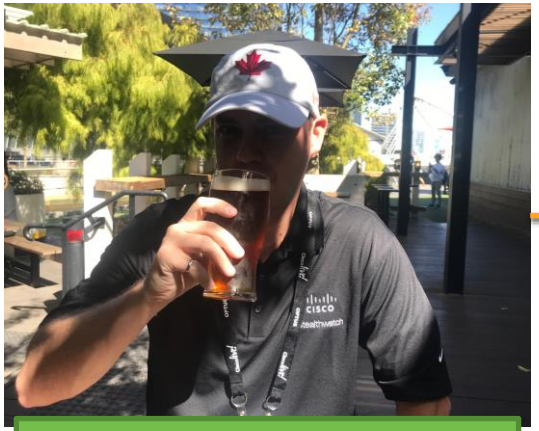

Timeline view of alert types

# Demo

# Extended Detection and Response

# The Thing about Behaviour

There exist conditions that make the observation malicious

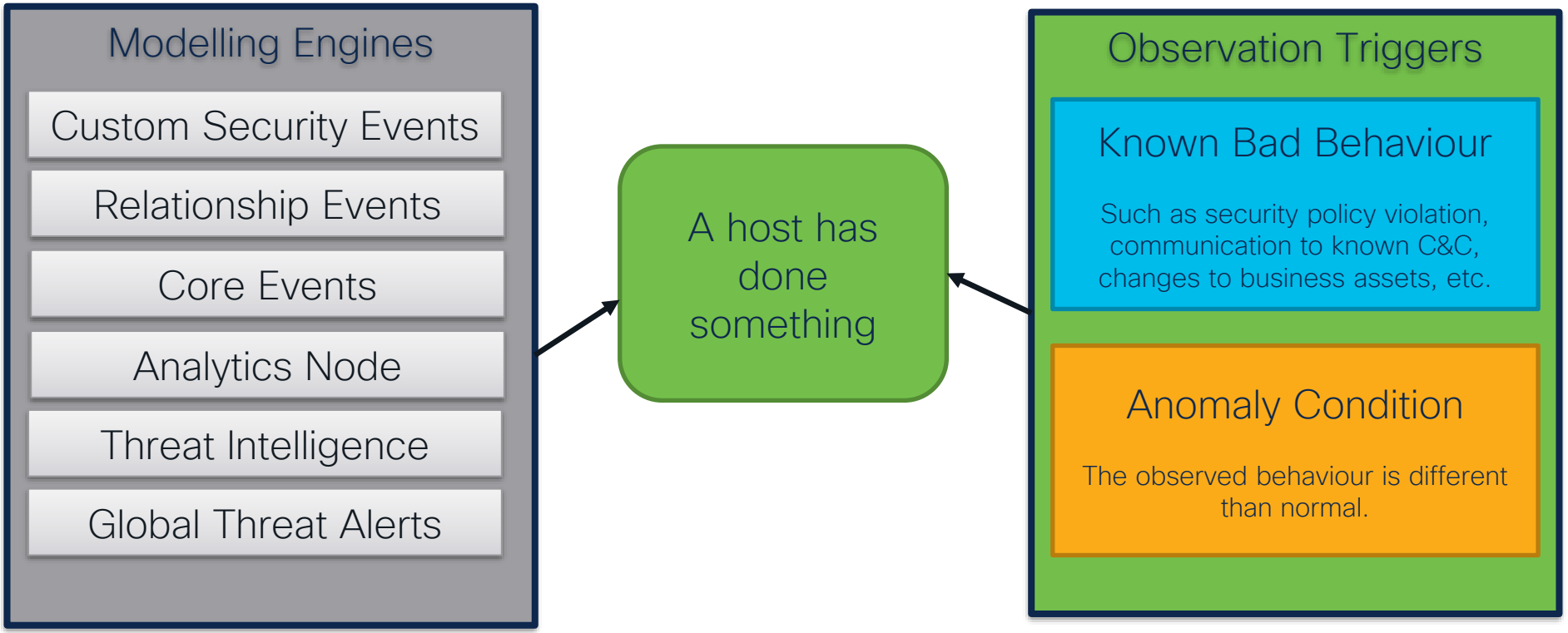



Observation:
This man drinks beer

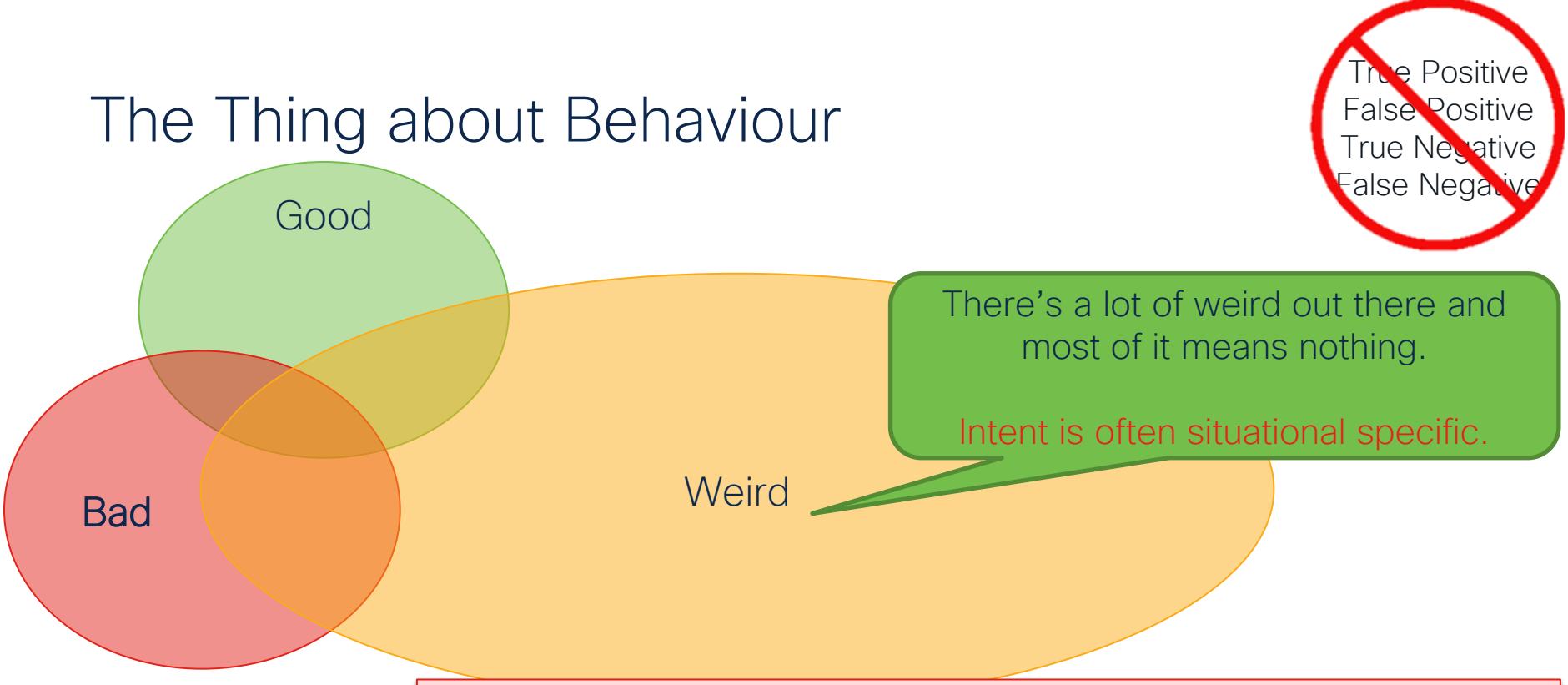
Some observations are just "different than normal"

Key Idea:
Behaviour events are an observation

# Behaviour events are an observation

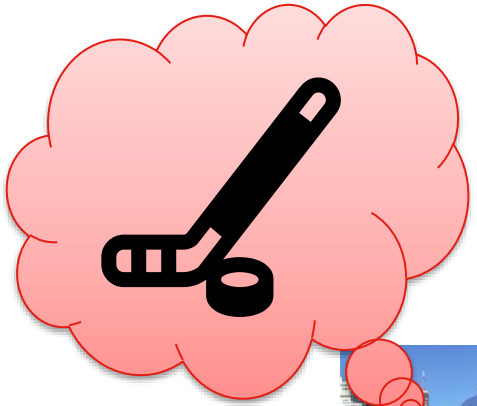


# The Thing about Behaviour




Intent requires business relevant language:
10.10.10.10 just uploaded a large amount of data to 128.107.78.10
versus
The PCI server just uploaded a large amount of data to an external server

# Making the Alarms Business Relevant

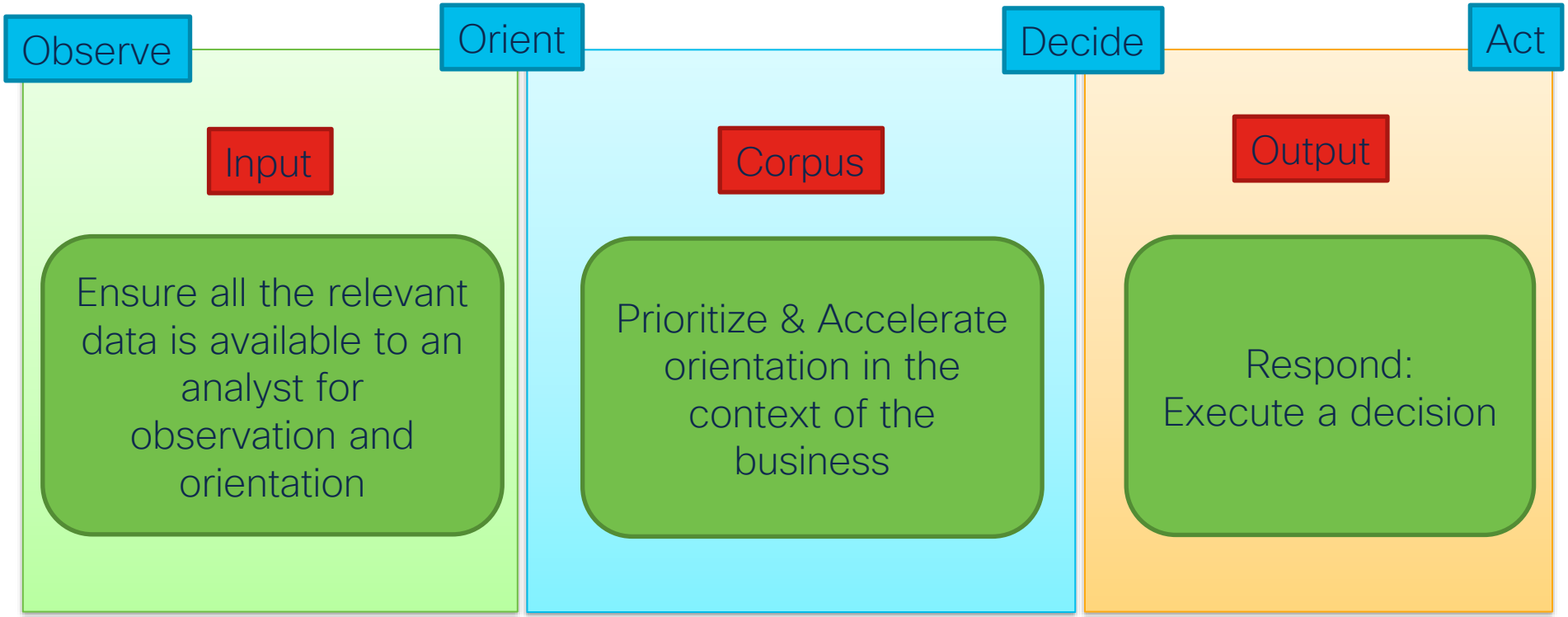


!

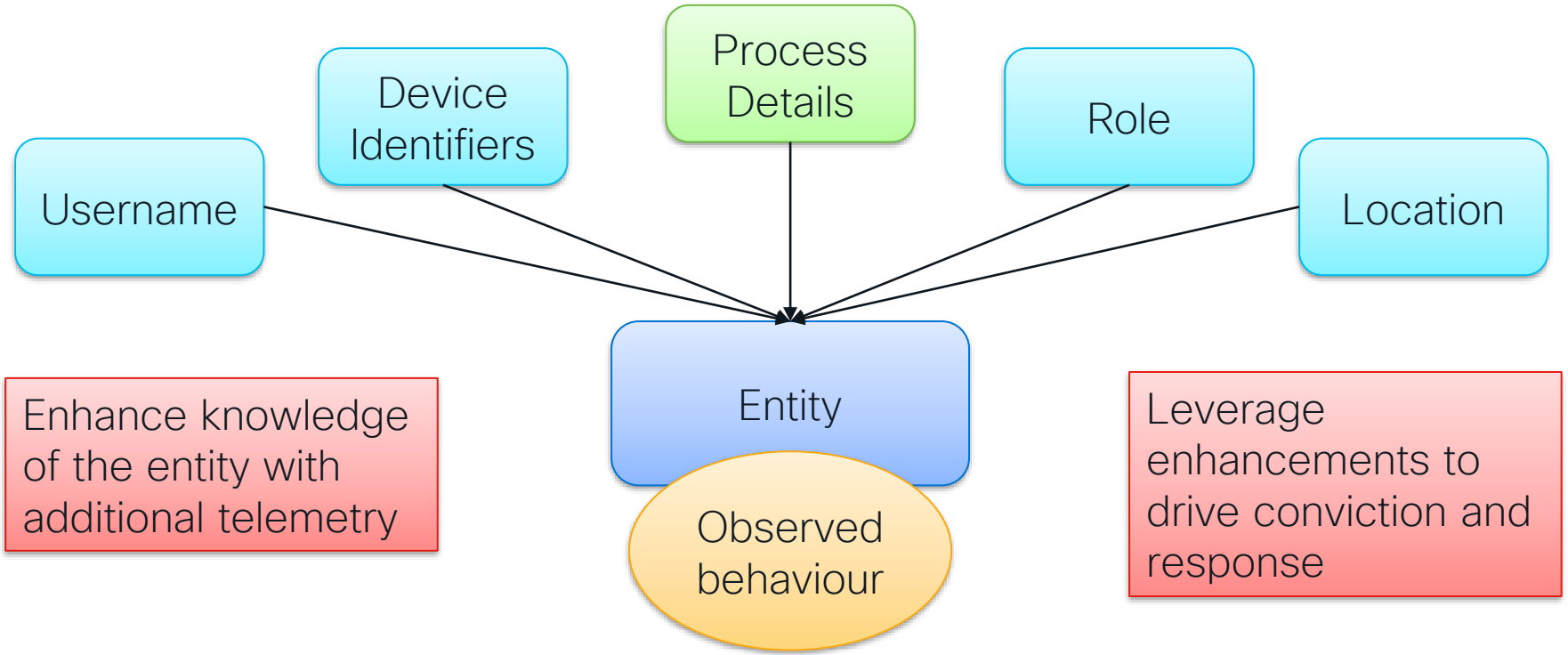
37 to 20

What matters to one organization might not matter to another

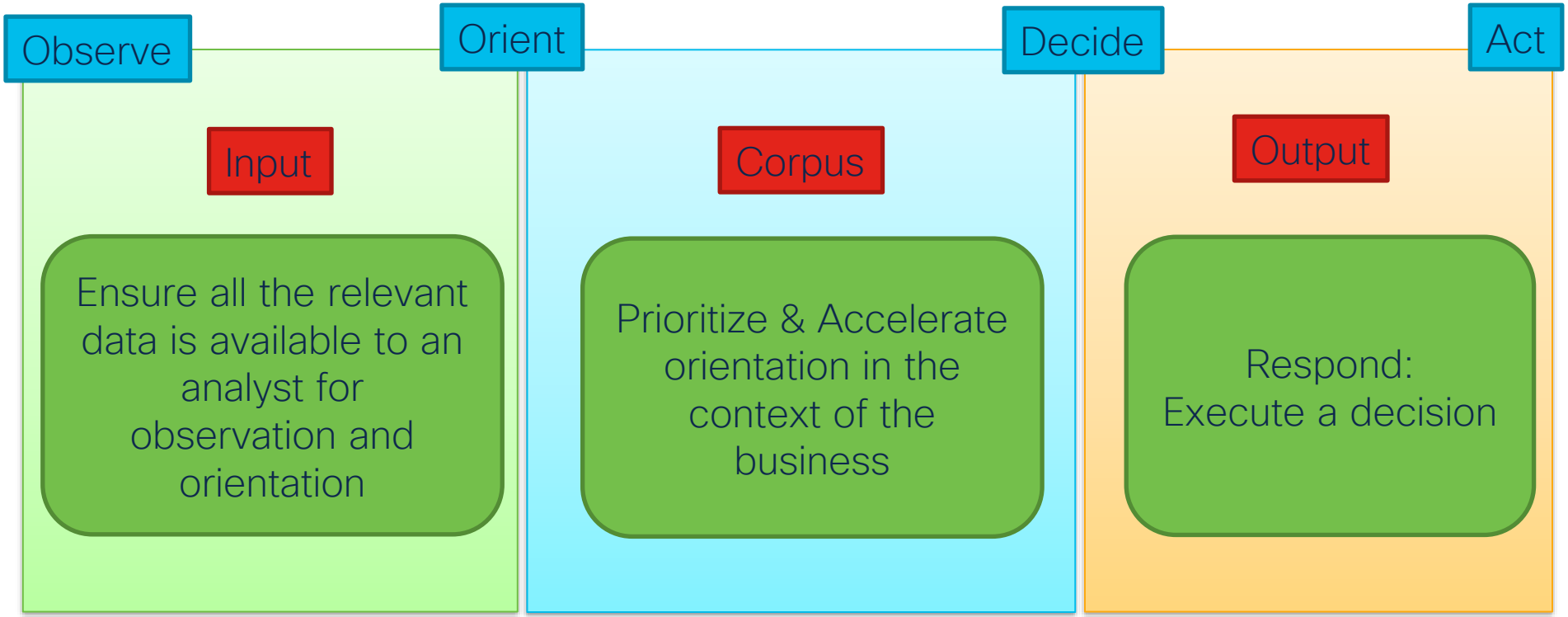
# Making the Alarms Business Relevant



# Input: Enhance the Detection



# Making the Alarms Business Relevant



# Read the Manual!

Understand what the observations mean!

## Cisco Secure Network Analytics

Security Events and Alarm Categories 7.4

https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/management_console/securit_events_alarm_categories/7_4_Security_Events_and_Alarm_Categories_DV_2_0.pdf

## Cisco Secure Network Analytics

Default Custom Security Event Setup Guide 7.4

https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/management_console/default_custom_security_event_setup_guide/7_4_Default_Custom_Security_Event_Setup_DV_1_0.pdf

## Cisco Secure Network Analytics

Analytics: Detections, Alerts, and Observations 7.4.1

https://www.cisco.com/c/dam/en/us/td/docs/security/Analytics/7_4_Analytics_DV_2_3.pdf

# Approaches to Tuning/Prioritisation

Six Phased Approach to Tuning:

1. Classify Inside: Bring RFC1918 and Public IP's Inside
2. Build Policy Groups Framework (Use By Function)
3. Classify Known Scanners
4. Classify Common Server Types
5. Classify Cloud Providers
6. Classify Undefined Applications

https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system_installation_configuration/Cisco_Secure_Network_Analytics_Six_Phased_Approach_to_Tuning_DV_3_0.pdf

Alarm prioritization with Tiered Alarms:

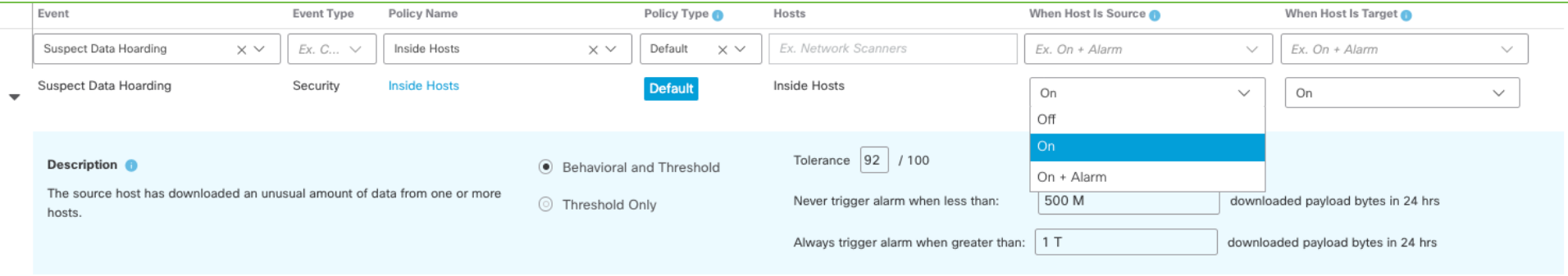
- Priority A: Severity Critical
- Priority B: Severity Major
- Priority C: Severity Minor

http://b2bcontact.com/cisco-stealthwatch/tiered_alarms/

# Tuning the Corpus

1. Create custom security events
2. Create Network Diagrams and Relationship Policies
3. Enable/Disable Alarms and thresholds by:
    1. Type – select the types of alarms you want
    2. Role – leverage role policies and alarm types
    3. Host – Some hosts are more valuable than others
4. Adjust Alarm Severity by Type (tiered alarms)

# Tuning the Corpus: Enable/Disable Algorithms/Alarms and Adjust Thresholds




Guidance

- Consider the alarm and its meaning
- Adjust thresholds
- Adjust Behavioural vs. threshold only
- Adjust Source/Target conditions
- Sometimes you just want to track the behaviour but not alarm

# Prioritizing Alarm Types with MITRE ATT&CK


MITRE Mappings are included in the alert details for Global Threat Alerts, Secure Cloud Analytics and the Analytics Node

## Secure Network Analytics MITRE Mappings

https://www.cisco.com/c/dam/en/us/products/collateral/security/stealthwatch/stealthwatch-mitre-use-case.pdf

**Initial Access**
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Spearphishing Attachment
- Spearphishing Link
- Trusted Relationship
- Valid Accounts

**Execution**
- Dynamic Data Exchange
- Exploitation for Client Execution
- PowerShell
- Scheduled Task
- Windows Management Instrumentation
- Windows Remote Management

**Exfiltration**
- Automated Exfiltration
- Data Compressed
- Data Encrypted
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over Command and Control Channel
- Exfiltration Over Other Network Medium
- Scheduled Transfer

**Privilege Escalation**
- Scheduled Task
- Valid Accounts

**Defense Evasion**
- BITS Jobs
- DCShadow
- Deobfuscate/Decode Files or Information
- Disabling Security Tools
- Port Knocking
- Redundant Access
- SIP and Trust Provider Hijacking
- Valid Accounts
- Web Service

**Credential Access**
- Account Manipulation
- Brute Force
- Forced Authentication
- LLMNR/NBT-NS Poisoning and Relay
- Network Sniffing

**Collection**
- Data Staged
- Data from Information Repositories
- Data from Network Shared Drive
- Email Collection

**Discovery**
- Account Discovery
- Application Window Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Remote System Discovery
- System Information Discovery
- System Network Connections Discovery
- System Service Discovery

**Lateral Movement**
- Application Deployment Software
- Exploitation of Remote Services
- Remote Desktop Protocol
- Remote File Copy
- Remote Services
- Windows Admin Shares
- Windows Remote Management

**Persistence**
- Account Manipulation
- BITS Jobs
- External Remote Services
- Port Knocking
- Redundant Access
- SIP and Trust Provider Hijacking
- Scheduled Task
- Valid Accounts

**Command and Control**
- Commonly Used Port
- Communication Through Removable Media
- Connection Proxy
- Custom Cryptographic Protocol
- Data Encoding
- Data Obfuscation
- Domain Fronting
- Domain Generation Algorithms
- Fallback Channels
- Multi-Stage Channels
- Multi-hop Proxy
- Multiband Communication
- Multilayer Encryption
- Port Knocking
- Remote Access Tools
- Remote File Copy
- Standard Application Layer Protocol
- Standard Cryptographic Protocol
- Standard Non-Application Layer Protocol
- Uncommonly Used Port
- Web Service

**Impact**
- Network Denial of Service
- Resource Hijacking

To learn more about Stealthwatch, please visit cisco.com/go/stealthwatch
Sign up for a free 2-week visibility assessment here

# Tuning the Corpus: Create Policies

**Policy:**
A set of allowed criteria that determines how the analytics engine reacts when behaviours violating the criteria are observed

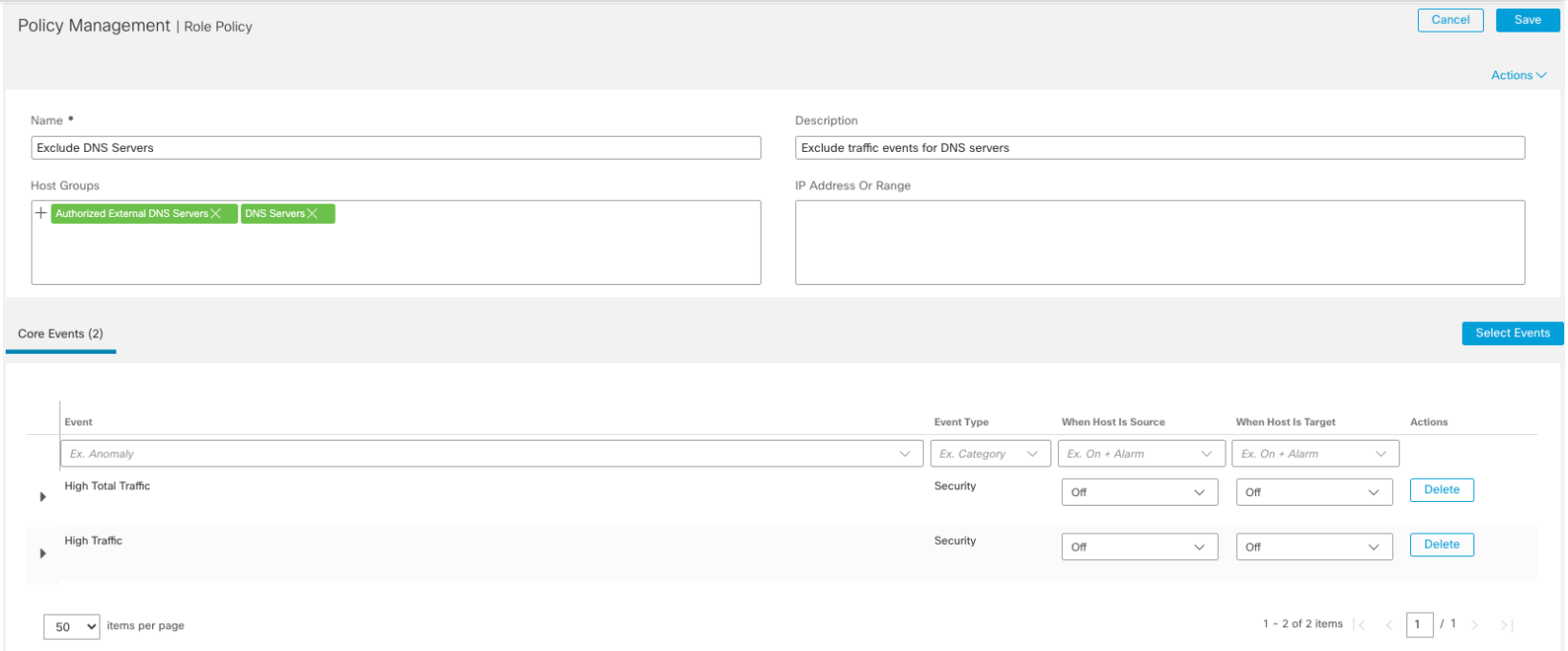
Three Types of Policy:

1. Default – Predefined for all Inside & Outside Host Groups
2. Role – Applied at a Host Group Level
3. Host – pertains to a specific IP address

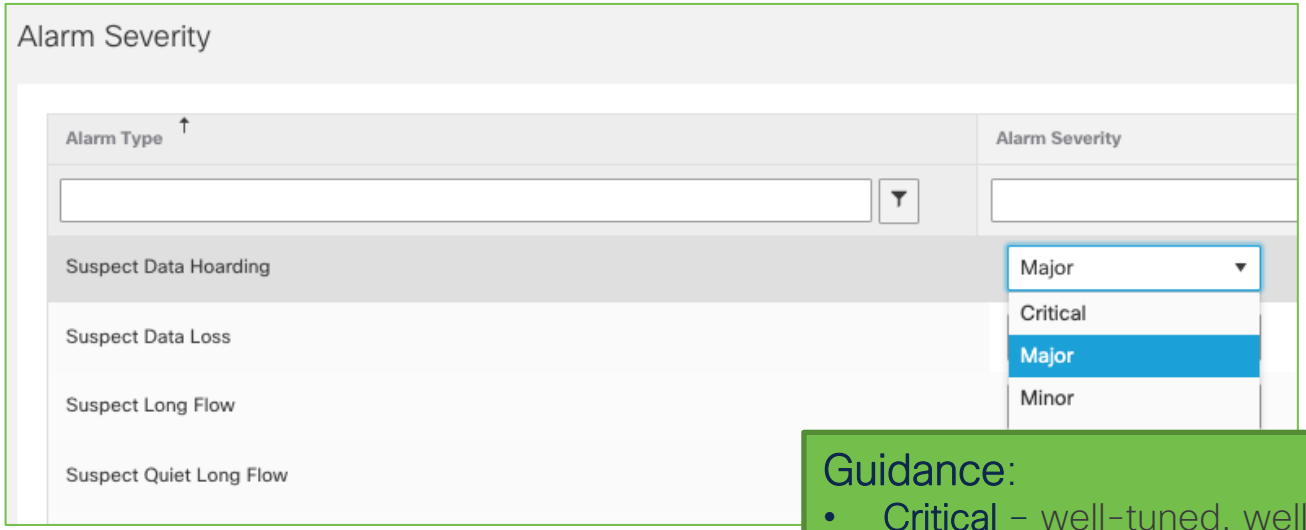
- If no tuning is performed, Default policies are in place
- A Role policy takes precedence over a Default Policy
- A Host policy takes precedence over all other policies

# Example Role Policy: Exclude DNS Servers

Challenge: Legit DNS traffic can result in High Traffic alarms for inside hosts
Solution: Exclude Authorised DNS servers from High Traffic Alarms



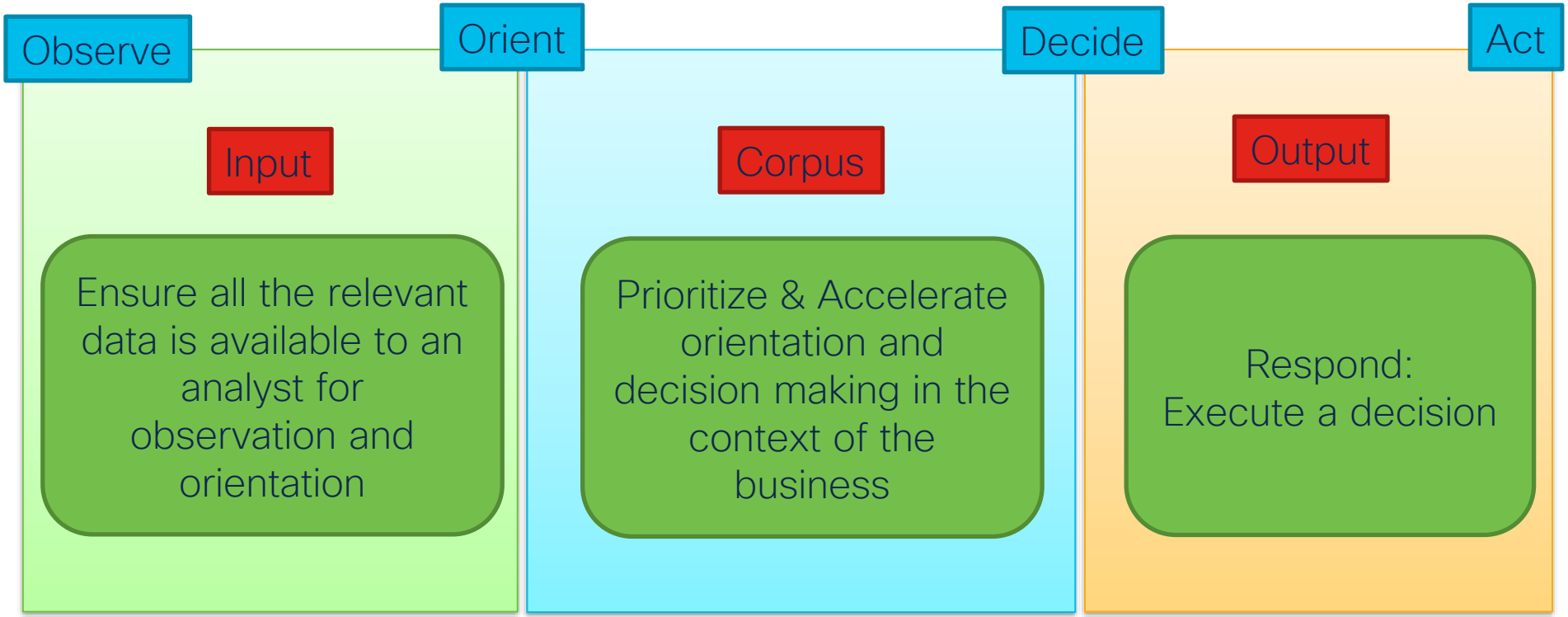
# Tuning the Corpus: Adjust Alarm Severity



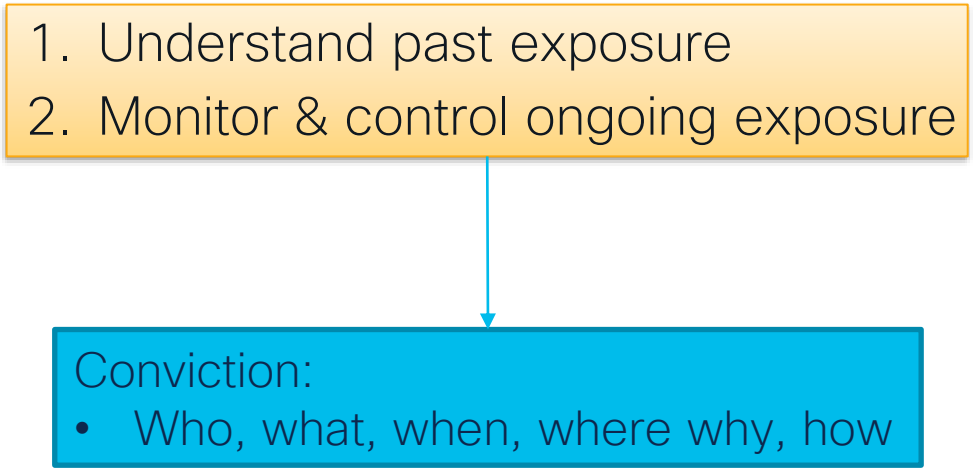

**Guidance:**

- **Critical** – well-tuned, well-understood, and typically low-volume alarms.
- **Major** – alarms are of interest and are tuned, observed, and documented.
- **Minor** – 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

# Making the Alarms Business Relevant

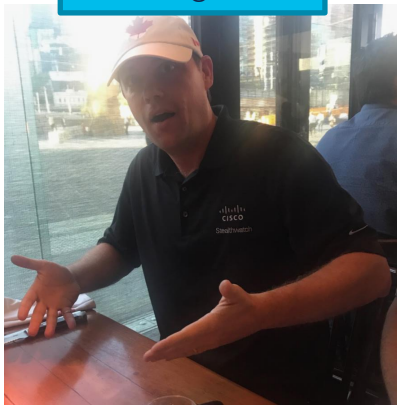


# Prioritised Observation to Action

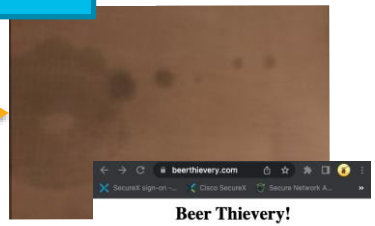


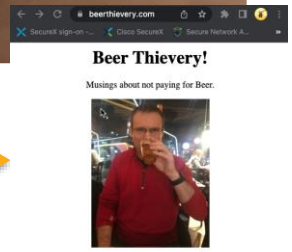
# Investigating with OODA

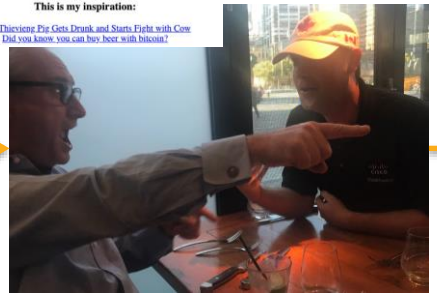
Observation: Missing Beer



Orient: Gather data





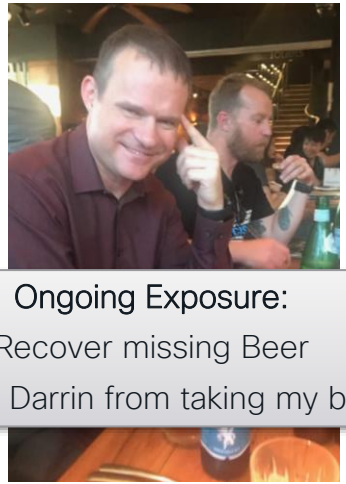
Orient: Convict


Decide → Act

# Observation to Action

1. Understand past exposure
2. Monitor & control ongoing exposure


Conviction:
- Who, what, when, where why, how



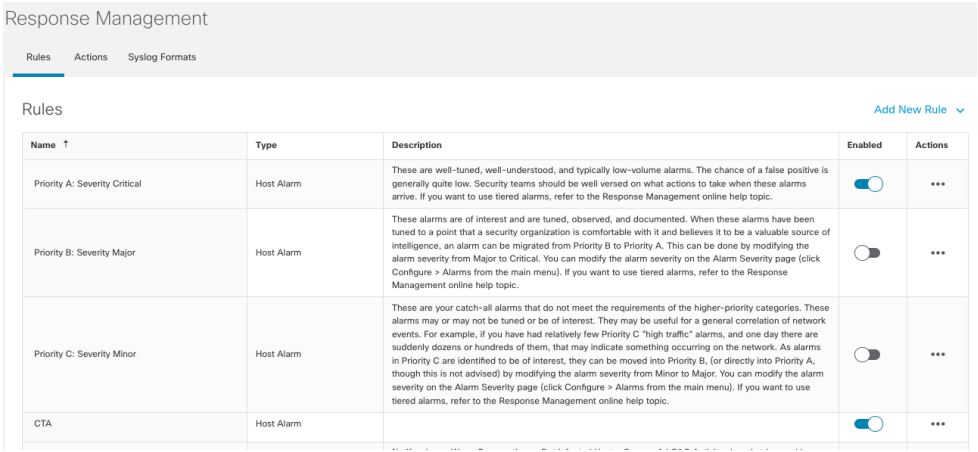
Ongoing Exposure:
Recover missing Beer
Prevent Darrin from taking my beer.

# Respond: Execute a Decision

**Notification**:
Export (prioritised) Alarms from SNA to another system

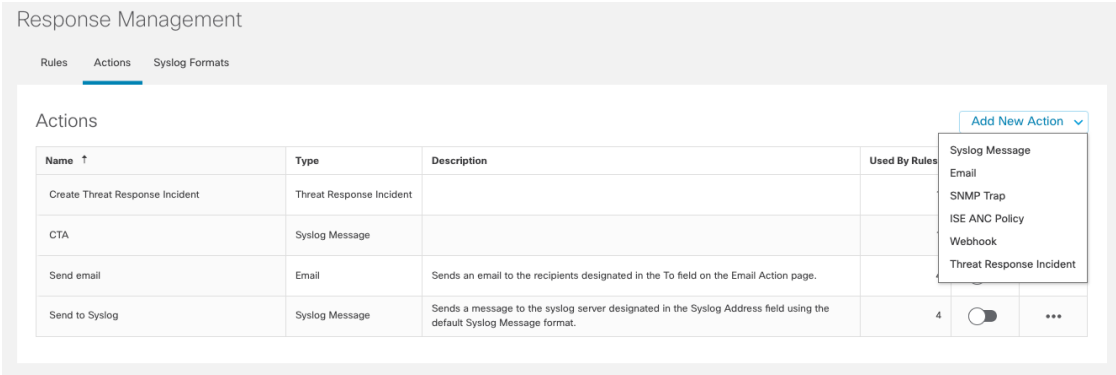
**Remediation**:
Leverage data from SNA (and other systems) to take remediating or corrective action

# Export: alarm response rules & actions

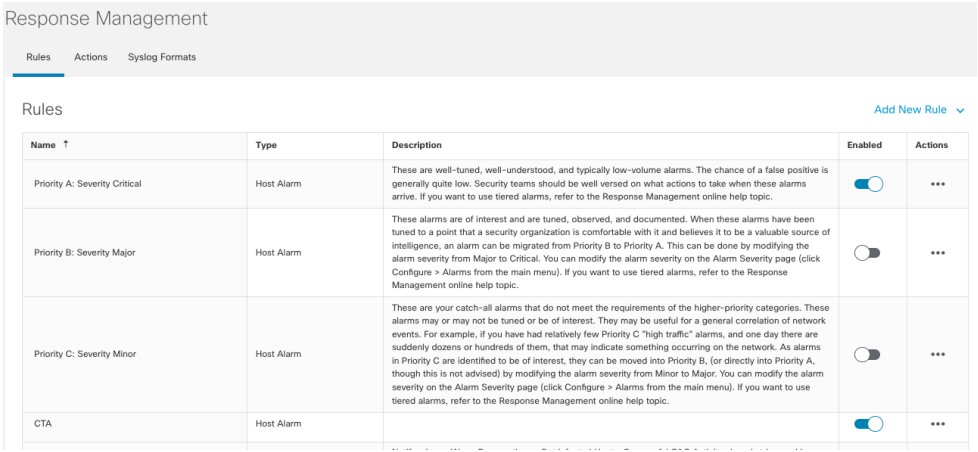



- Create rules to automate response/export on occurrence of an alarm
- Leverage built-in Tiered Alarm Severity rules

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

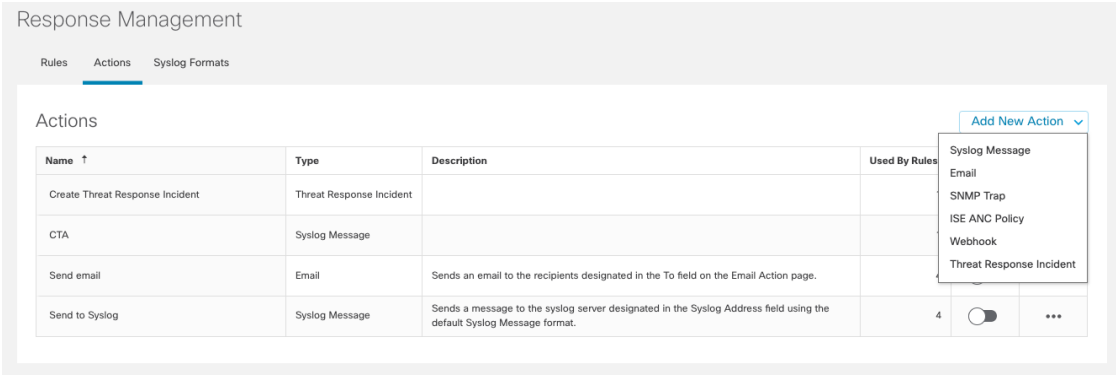


# Export: alarm response rules & actions



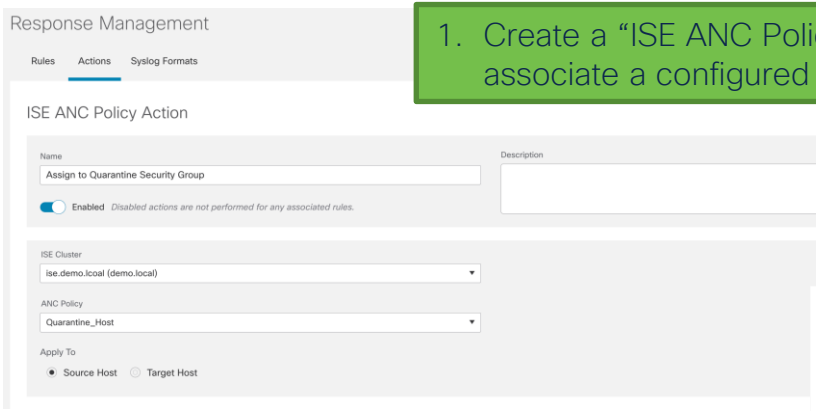

- Create rules to automate response/export on occurrence of an alarm
- Leverage built-in Tiered Alarm Severity rules

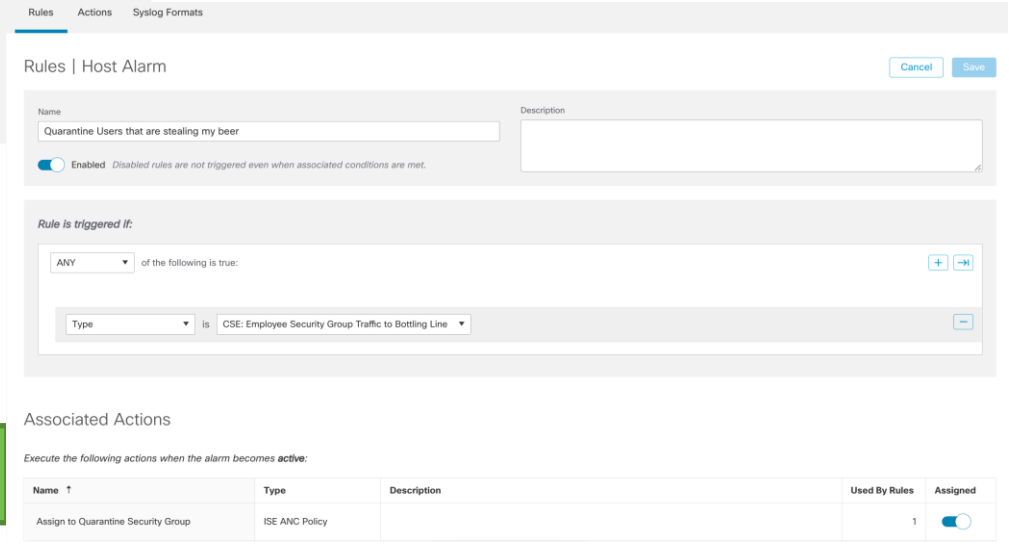
- Define automated actions when alarm rule is hit: ISE ANC, syslog, etc.
- Create SecureX Threat Response incident



# Remediating Action with ISE

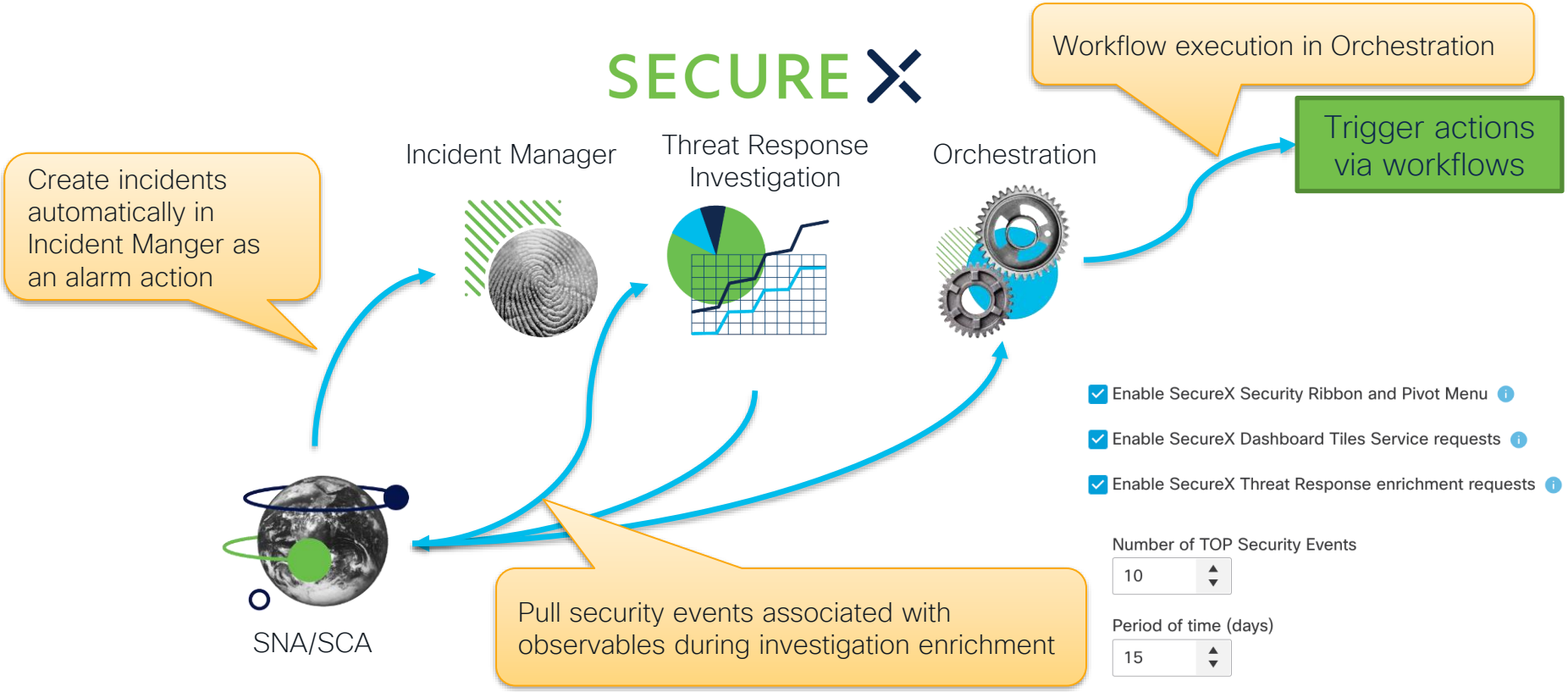
1. Create a “ISE ANC Policy” Action rule and associate a configured ISE cluster.



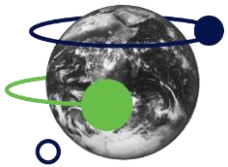

2. Define a response Rule that invokes the defined Action

# XDR with SecureX and SNA/SCA



# SNA alert promotion to SecureX

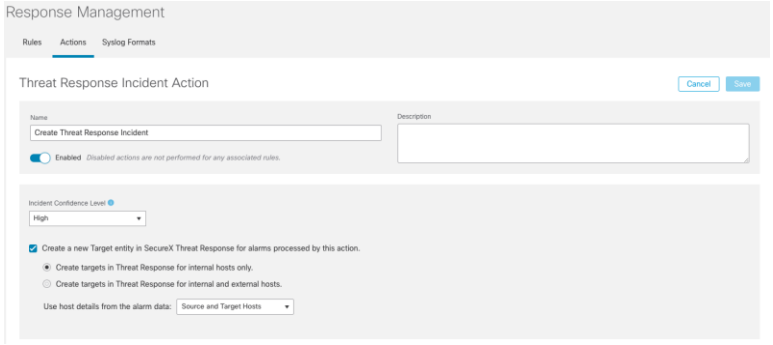
Secure Network Analytics

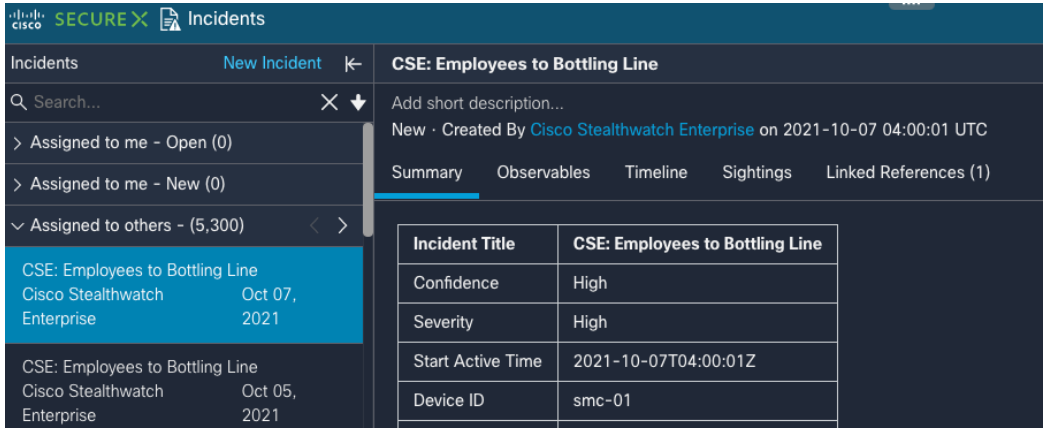


Create incidents automatically in Incident Manger as an alarm action

SECURE X

Incident Manager



# SCA alert promotion to SecureX

Secure Cloud Analytics

Create incidents automatically in Incident Manger as part of alert settings

Manually promote alerts as part of Secure Cloud Analytics alert workflow

SECURE X

Incident Manager

| Alert Type | Publish to SecureX | Enabled | Priority |
|---|---|---|---|
| **Abnormal User**<br>A user session was created on an endpoint that does not normally see sessions with this user. This alert uses the Session Opened observation and requires an integration with either AWS, Sumo Logic, or Active Directory. | | Default: Enabled | Normal<br>Default Priority: Normal |
| **Amplification Attack**<br>Device sent traffic with a profile that suggests participation in an amplification attack. This alert uses the Traffic Amplification observation and may indicate the device is part of a botnet. | | Default: Disabled | Normal<br>Default Priority: Normal |
| **Anomalous AWS Workspace**<br>An AWS Virtual Workspace used a new anomalous behavioral profile (e.g., the host connected to many devices over BitTorrent). This alert uses the Anomalous Profile observation and may be an indication of malware or misuse. | | Default: Enabled | Normal<br>Default Priority: Normal |
| **Anomalous Mac Workstation**<br>An Apple Mac Workstation used a new anomalous behavioral profile (e.g., the host connected to many devices over BitTorrent). This alert uses the | | Default: Enabled | Normal<br>Default Priority: Normal |

Configure severity and publication settings in Secure Cloud Analytics

Status: Open

## Unusual External Server for Cisco

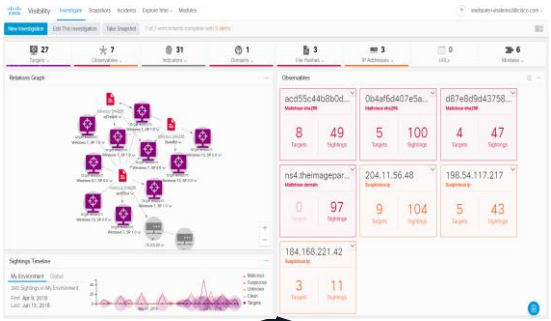
Created by Cisco Secure Cloud Analytics on 2022-03-22T08:47:56.000Z

Unusual External Server on 10.90.90.206

Description | Events | Observables | Timeline | Linked References (3)

| Alert | Unusual External Server - #421 |
|---|---|

# SecureX Threat Response



Threat Response automatically queries integrated products via APIs to enrich investigation

Collect everything integrated products knows about the queried observables in one place for faster investigation

Virus Total | TALOS | SMA | ●●● | Endpoint | Umbrella | SNA | FTD | More ..

# SNA/SCA Workflows

Import Workflow

Import From

Git | Browse

* Git Repository

CiscoSecurity_Workflows

Learn about Cisco-provided GitHub repositories

* Filename

Select

0005-SCA-GenerateCasebookWithFlowLinks
0006-SCA-QuarantineAWSInstancesFromAlerts
0007-SCA-HandleAWSSSHQuarantineApprovals

* Filename

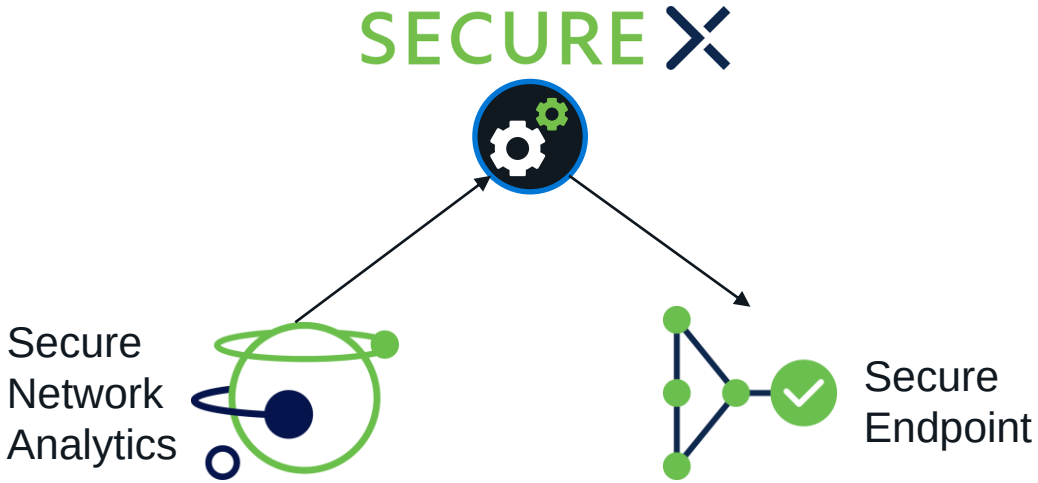
Select

0032-SNA-IsolateEndpointsAndBlockHashesFromAl...
0033-SNA-BlockExternalThreatsWithUmbrella
0034-SNA-GenerateCasebookWithTopHostsAndPe...

## Isolate Endpoints and Block Hashes from Alarms

WORKFLOW #0032

This workflow gets events from Cisco Secure Network Analytics (SNA) for the past 24 hours based on the event name provided. It then fetches associated flows and compiles information necessary to isolate related hosts and block file hashes in Cisco Secure Endpoint. At the end, a Webex message is sent with a summary.



# Demo

# Summary

# Complete your Session Survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.


- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard" at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

# Continue Your Education

Visit the Cisco Showcase for related demos.

Book your one-on-one Meet the Engineer meeting.

Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.

Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.

# Related Sesssions

XDR Learning Map:
(Anything SecureX)
https://events.rainfocus.com/widget/cisco/clemea23/sessioncatalogtest?search.learningmap=1614366204738006MRlo

| Session ID | Title | When |
|---|---|---|
| BRKSEC-2354 | Automating Security: Just Because You can, Doesn't Mean You Should | Tuesday 1:30 PM |
| BRKSEC-2227 | Evaluating and Improving Defenses with MITRE ATT&CK | Wed 8:45 AM |
| IBOSEC-2006 | Empty Threats – Building Your Own Cyber Threat Picture | Thursday 10:00 AM |
| BRKSEC-2931 | Building, Proving, and Extending Detections in Secure Analytics | Friday 11:15 AM |

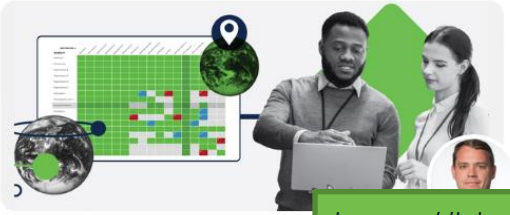
# Reading: TrustSec Policy Analytics Blog Series

Security

TrustSec Policy Analytics – Part One: What are policy analytics?

Samuel Brown

https://blogs.cisco.com/security/trustsec-policy-analytics-part-one-what-are-policy-analytics



Security

TrustSec Policy Analytics – Part Two: Policy Visualization

Matthew Robertson

https://blogs.cisco.com/security/trustsec-policy-analytics-part-two-policy-visualization

Security

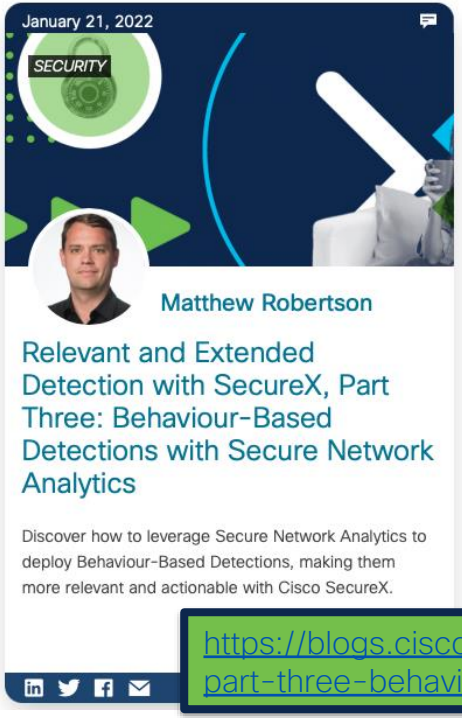
TrustSec Policy Analytics – Part Three: Policy Validation

Matthew Robertson

https://blogs.cisco.com/security/trustsec-policy-analytics-part-three-policy-validation

# Reading: Relevant and Extended Detection with SecureX Blog Series

https://blogs.cisco.com/tag/relevant-and-extended-detection-with-secureX





https://blogs.cisco.com/security/relevant-and-extended-detection-with-securex-part-four-secure-cloud-analytics-detections

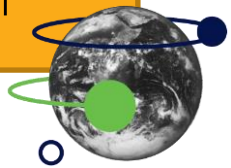
https://blogs.cisco.com/security/relevant-and-extended-detection-with-securex-part-three-behaviour-based-detections-with-secure-network-analytics

# Complete your Online Session Evaluation

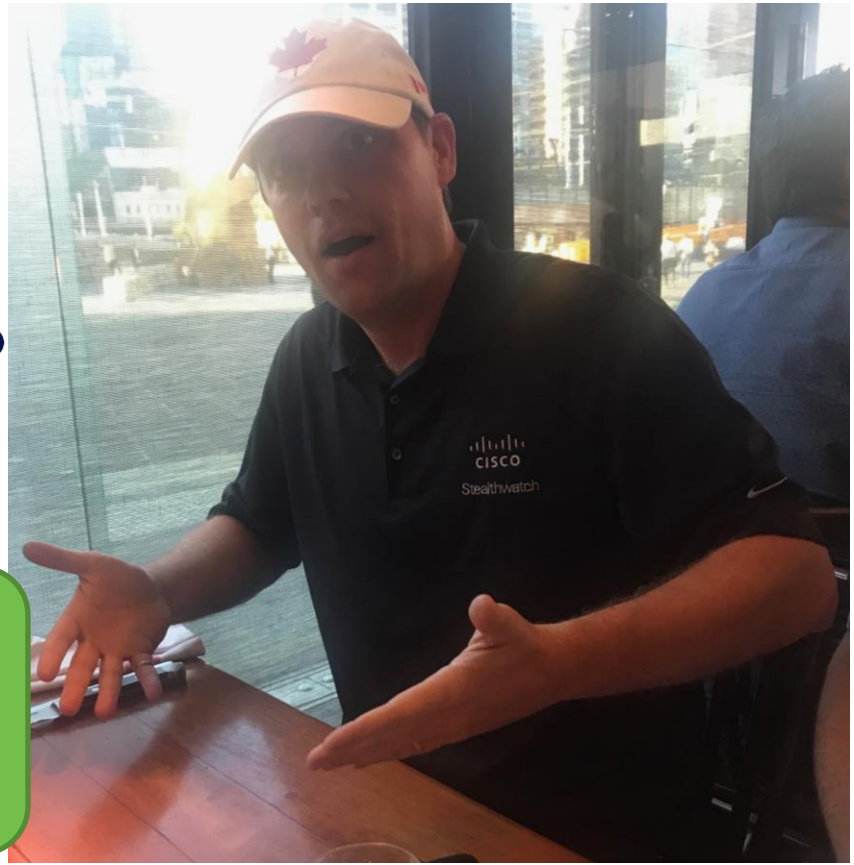
# Parting Thoughts

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

SECURE X



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



# Complete your Session Survey

- Please complete your session survey after each session. Your feedback is important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.


- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard" at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

# Continue Your Education

Visit the Cisco Showcase for related demos.

Book your one-on-one Meet the Engineer meeting.

Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.

Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.


cisco
The bridge to possible
Thank you
cisco Live!


CISCO Live!
ALL IN