



The bridge to possible

Visibility, Detection and Response with Cisco Secure Network Analytics

Matt Robertson, Distinguished Engineer

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 as 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

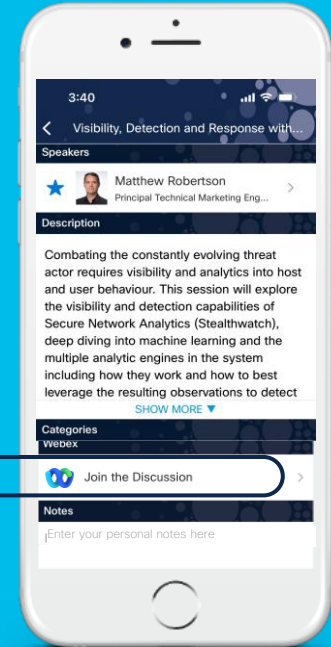
Questions?

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?

Machine Learning:

“Field of study that gives computers the ability to learn without being explicitly programmed.”

– Arthur Samuel, 1959



Designing algorithms directed at achieving some outcome.

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

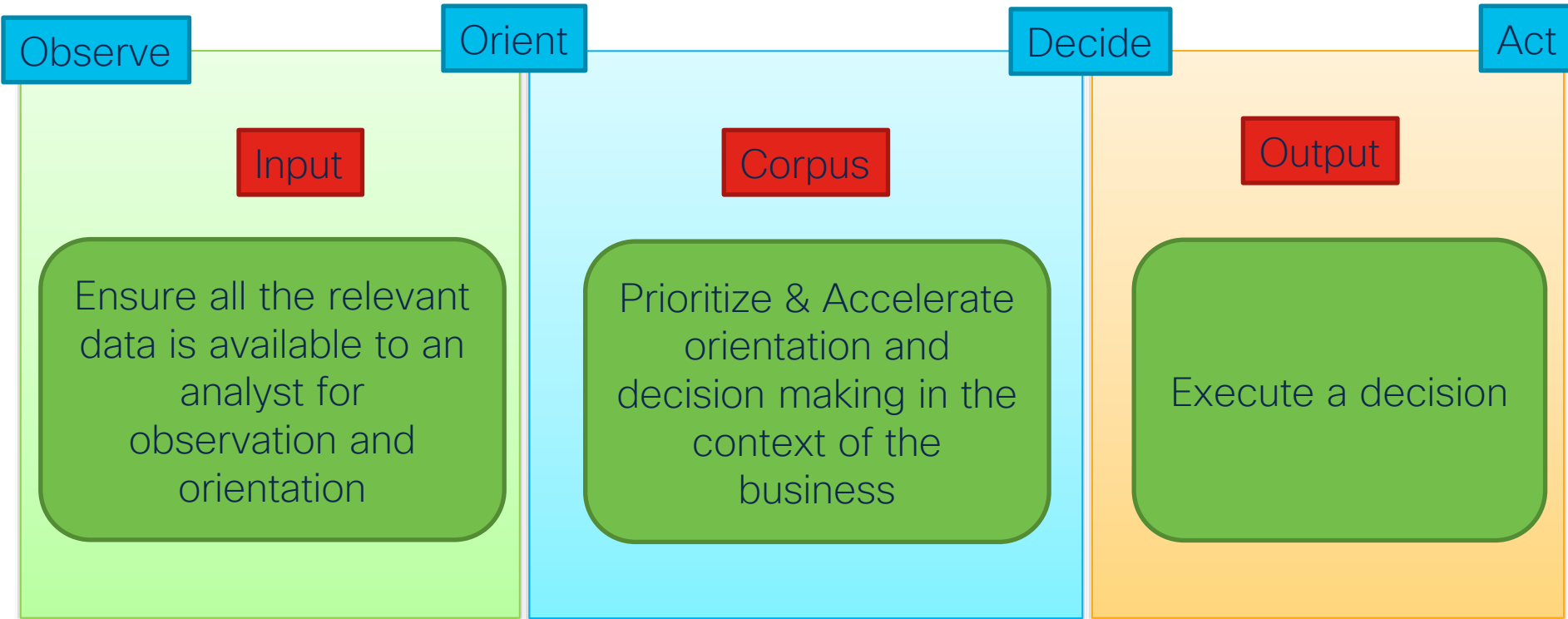
Key idea!
Analytics are not magic.



Two popular ML approaches:

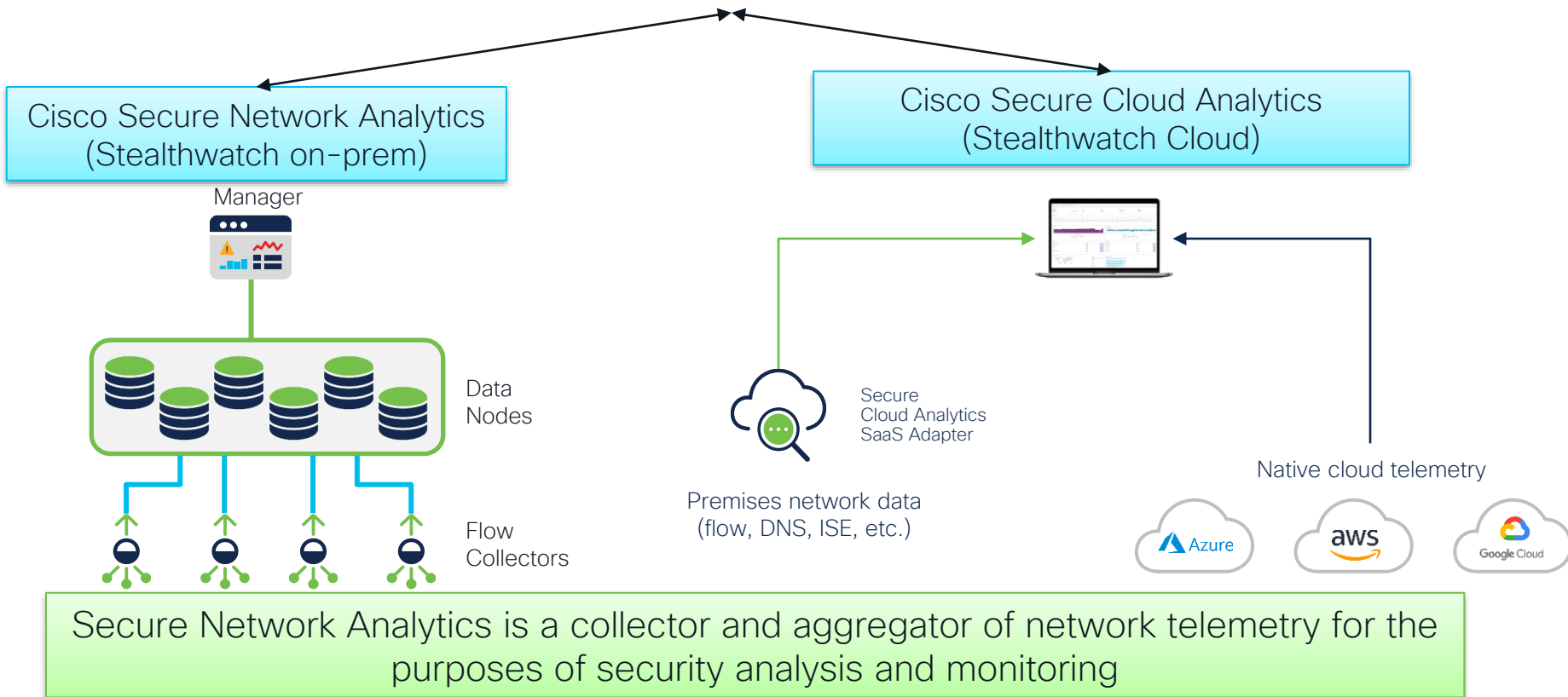
- Supervised
- Unsupervised

Accelerating the SOC's OODA Loop



Cisco Secure Network Analytics Portfolio

SecureX



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.

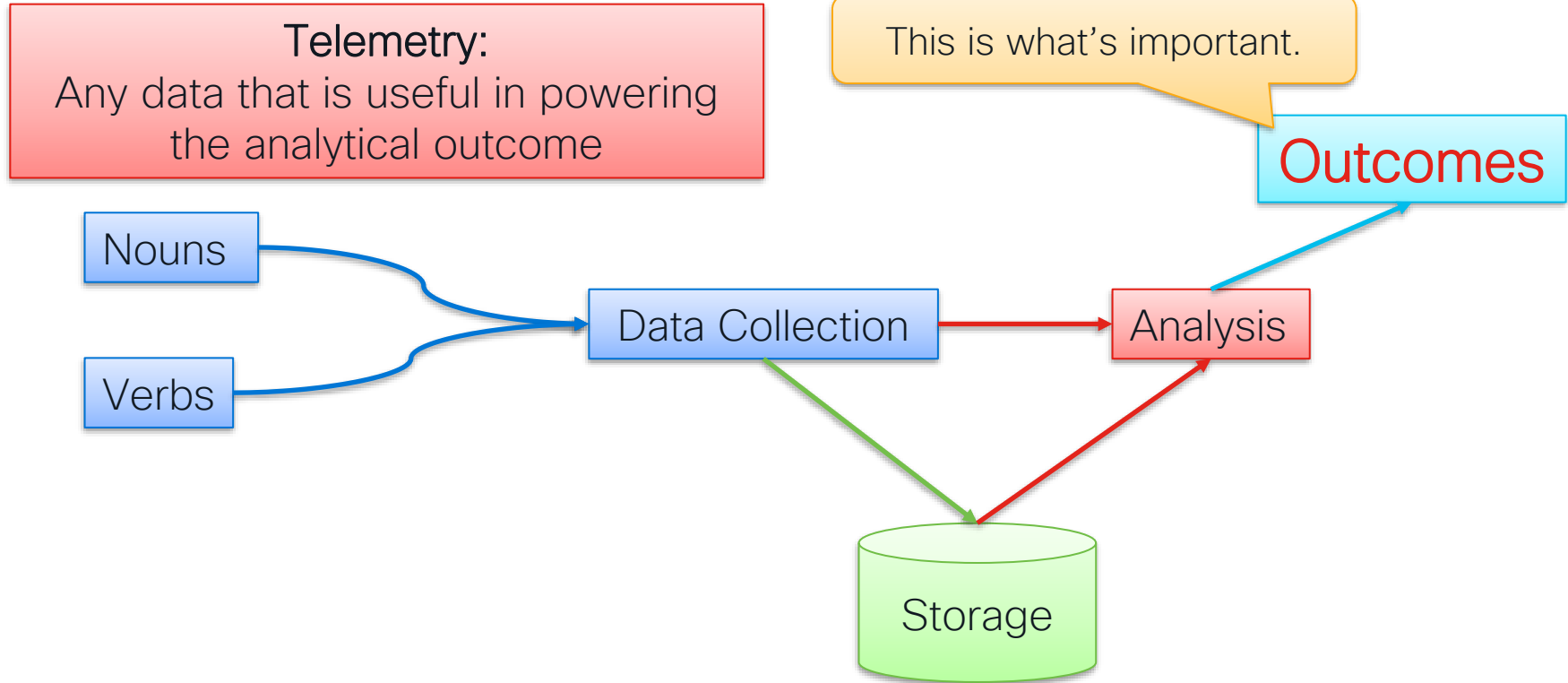


Host Attributes:

IP Address, Hostname, Username, Role, etc.

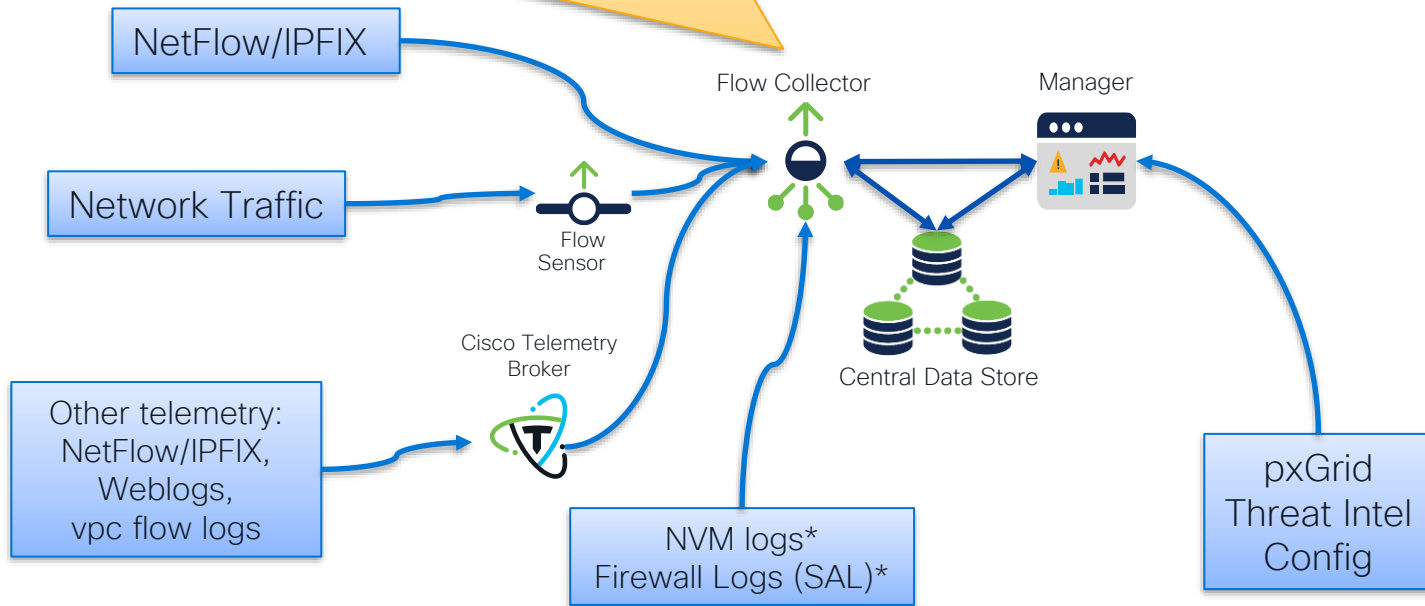


Powering Visibility & Analytics with Telemetry






Telemetry in SNA

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



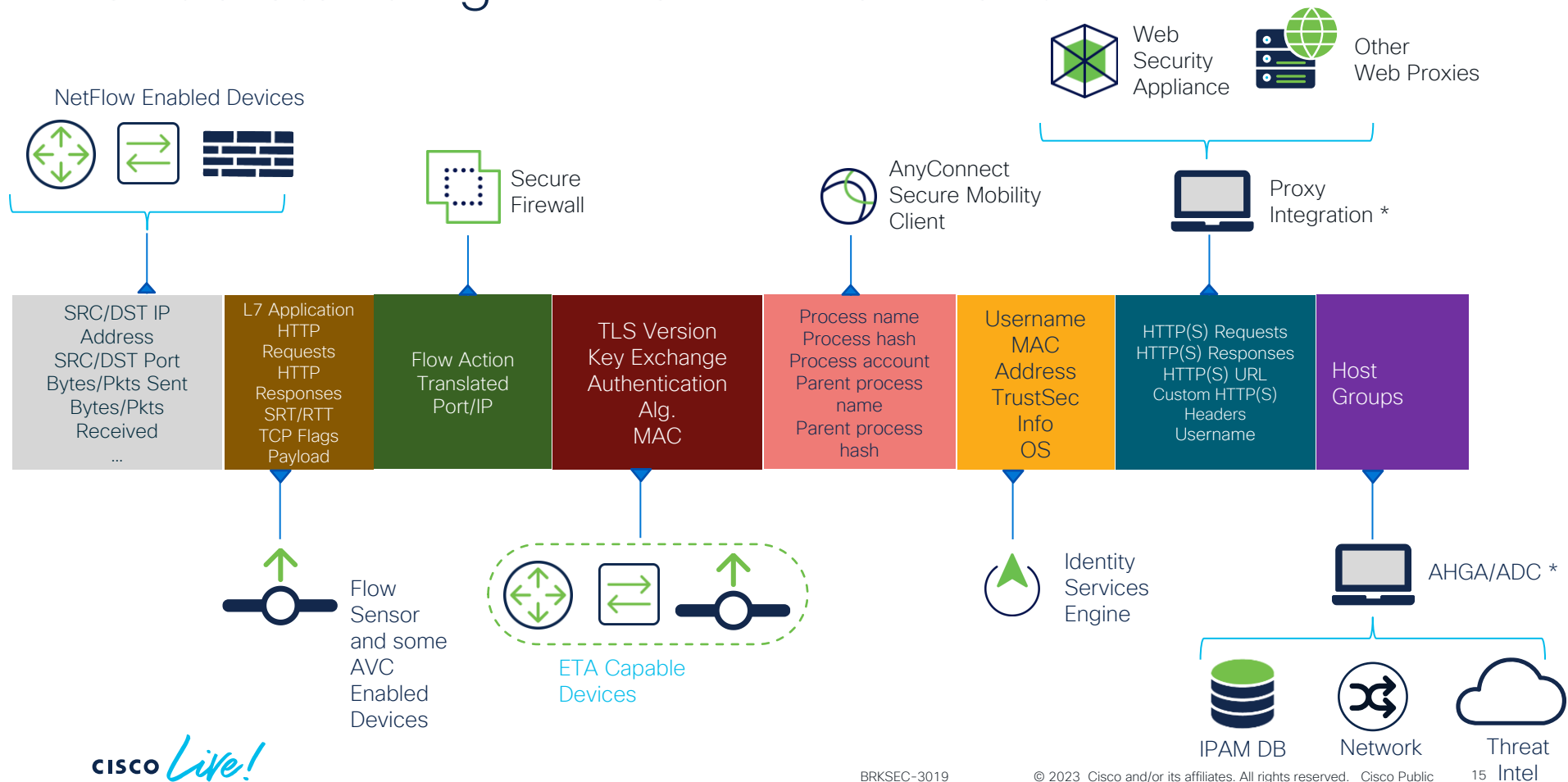
The “Bi-Flow”

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).

DURATION	SUBJECT	SUBJECT PORT/PROTOCOL	TRAFFIC SUMMARY	PEER PORT/PROTOCOL	PEER	ACTIONS
Start: Jun 5, 2019 2:37:24 PM End: Jun 5, 2019 2:37:59 PM Duration: 35seconds	 10.90.90.100 View URL Data RFC 1918 darrin 00:50:56:b6:e7:c2	50323/TCP	5.97 KB 40 packets → Cloud storage & computing services ← 7.09 KB 36 packets	80/TCP	 52.95.145.35 Canada s3-website.ca-central-1.amazonaws.com	
General						
View URL Data						
Subject		Totals	Peer			
Packets:	40	Packets:	76	Packets:	36	
Packet Rate:	1.14 pps	Packet Rate:	2.17 pps	Packet Rate:	1.03 pps	
Bytes:	5.97 KB	Bytes:	13.06 KB	Bytes:	7.09 KB	
Byte Rate:	174.63 bps	Byte Rate:	382.06 bps	Byte Rate:	207.43 bps	
Percent Transfer:	45.71%	Subject Byte Ratio:	45.71%	Percent Transfer:	54.29%	
Host Groups:	End User Devices, Main Campus Building 2	RTT:	0seconds	Host Groups:	Canada	
Payload:	GET http://beerhoser.ca/beerhoser_main.png	SRT:	0seconds	Payload:	304 304 Not Modified	

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

Duration	Subject IP Address	Subject Proces...	Application	Application (NBAR)	Total Bytes	Encryption TLS...	Encryption Key...	Encryption Aut...	Encryption Alg...	Encryption MAC	Peer IP Address	Peer Port/Prot...
Ex. <=50min4t	Ex. 10.10.10.10	chrome x	Ex. "Corporate	Ex. netbios	Ex. <=50M	Ex. 1.0	Ex. ECDH	Ex. ECDSA	Ex. AES_256_	Ex. SHA384	Ex. 10.255.25	Ex. 2055/UDP
▶ 1min 48s	10.90.90.201 ...	chrome.exe	HTTPS	ssl	9.33 K	TLS 1.2	RSA	RSA	AES_128_GCM/128	SHA256	146.112.61.110 ...	443/TCP
▶ 6min 9s	10.90.90.201 ...	chrome.exe	Web	google-services	47.21 K	TLS 1.3	PSK_ECDHE	--	AES_128_GCM/128	SHA256	142.251.41.67 ...	443/TCP

Application (NBAR) data

ETA "Encryption fields"

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?

Transaction Attributes:

Time, ports, protocols, applications, etc.

Host Attributes:

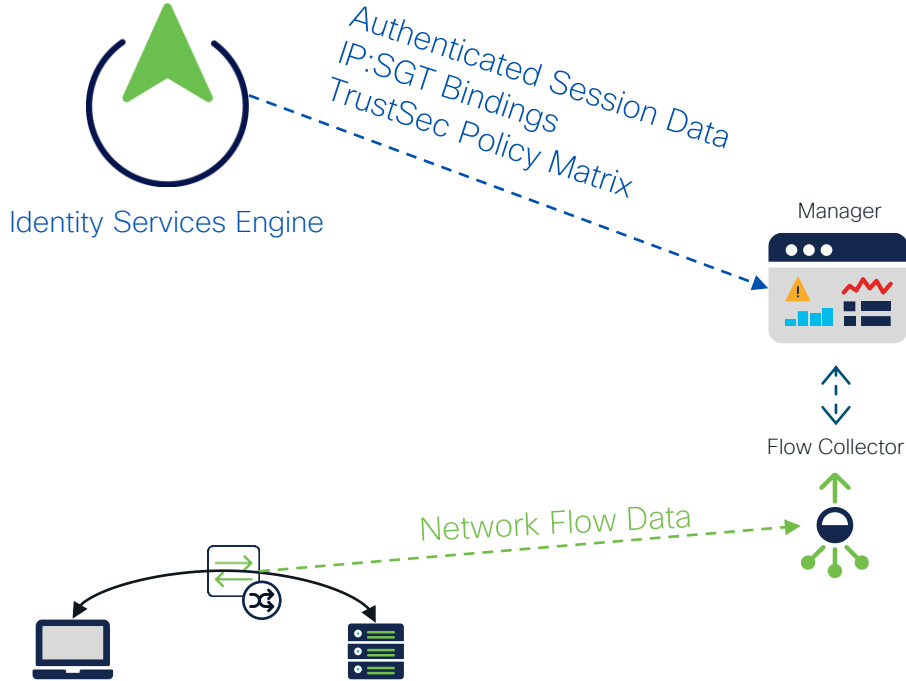
IP Address, Hostname, Username, Role, etc.



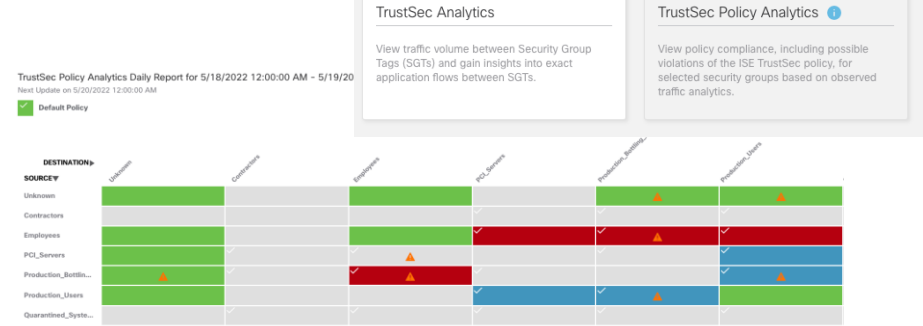
Host Attributes:

IP Address, Hostname, Username, Role, etc.

Policy Analytics with Secure Network Analytics



1. TrustSec Analytics Reports



2. Direct flow analysis leveraging SGT & DGT in Flow Table

3. Custom Security Events

Search filters: 5/18/2022 12:00 AM - 5/19/2022 12:00 AM, 1000 Mbps, 100% Complete, Delete Search

Subject: [Production_Users] [Other Applications]

Connection: [Production_Users] [Other Applications]

Peer: [Production_Users]

Start	Duration	Subject IP Address	Subject Port/Protocol	Subject Bytes	Subject TrustSec Name	Application	Total Bytes	Encryption TLS...	Peer IP Address	Peer Port/Protocol	Peer Bytes	Peer TrustSec Name	Actions
May 18, 2022 11:55:14 AM (210K 10min 5s ago)	12s	10.80.90.100	50884/TCP	10.57 K	Production_Users	HTTPS	25.5 K	TLS 1.0	10.70.70.100	443/TCP	12.93 K	PCI_Servers	

TrustSec Policy Analytics

Two report types introduced in Secure Network Analytics v7.3.1

TrustSec Analytics

View traffic volume between Security Group Tags (SGTs) and gain insights into exact application flows between SGTs.

Multiple Reports of this type allowed

TrustSec Policy Analytics ⓘ

View policy compliance, including possible violations of the ISE TrustSec policy, for selected security groups based on observed traffic analytics.

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?

TrustSec Analytics Dashboard

Next Update on 5/20/2022 12:00:00 AM

7 SGTs [Manage Columns](#) [Export](#)

☒ Default Policy

DESTINATION ►	Unknown	Contractors	Employees	PCI_Servers	Production_Bottlin...	Production_Users	Quarantined_Systems
SOURCE ▼							
Unknown							
Contractors							
Employees							
PCI_Servers							
Production_Bottlin...							
Production_Users							
Quarantined_Syste...							

☐ No Traffic
 ☒ Traffic
 ☐ Denied Traffic
 ☐ Traffic with Custom Policy
 ☐ Policy Monitor Mode
 ☐ Policy Disabled
 ☒ Policy Enabled

- 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

TrustSec Policy Analysis Report
Next Update on 5/20/2023 10:00 AM

✓ Default Policy

DESTINATION ▶	Unknown	Contractors	Employees	PCI_Servers	Production	Production	Quarantined
SOURCE ▼							
Unknown							
Contractors							
Employees							
PCI_Servers							
Production_Bottlin...							
Production_Users							
Quarantined_Syste...							

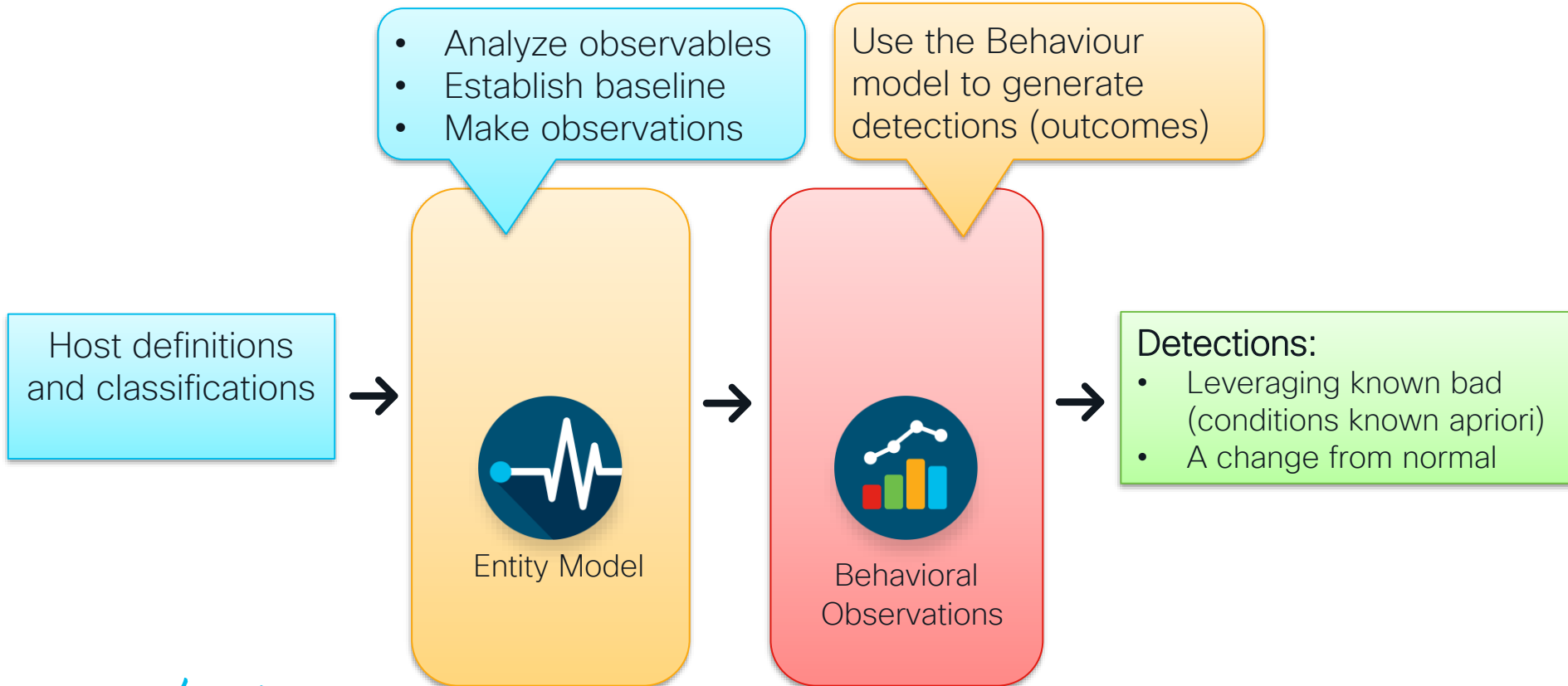
No Traffic Traffic Denied Traffic Traffic with Custom Policy Offending Traffic Unsupported policy Policy Analysis Pending Policy Monitor Mode Policy Disabled Policy Enabled

- 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

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

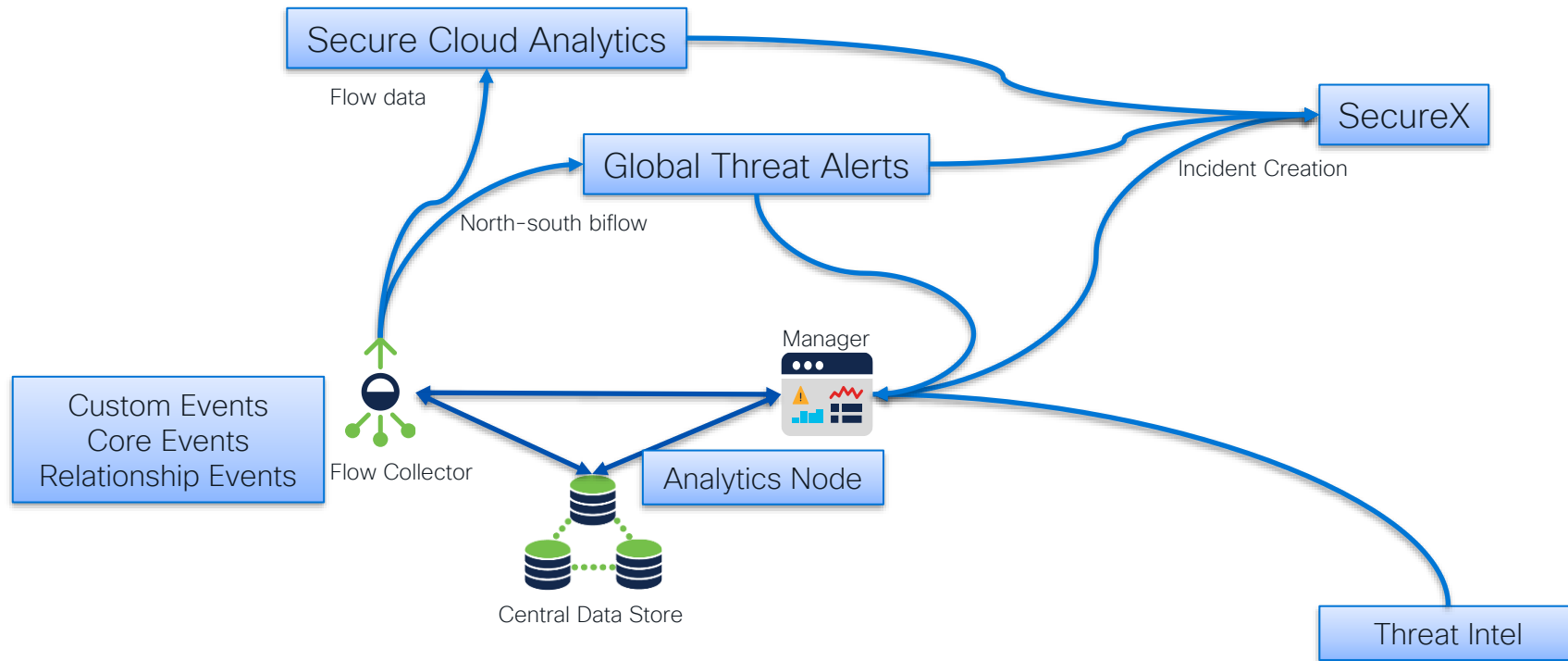
Global Threat Alerts (Cognitive Intelligence)

- 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

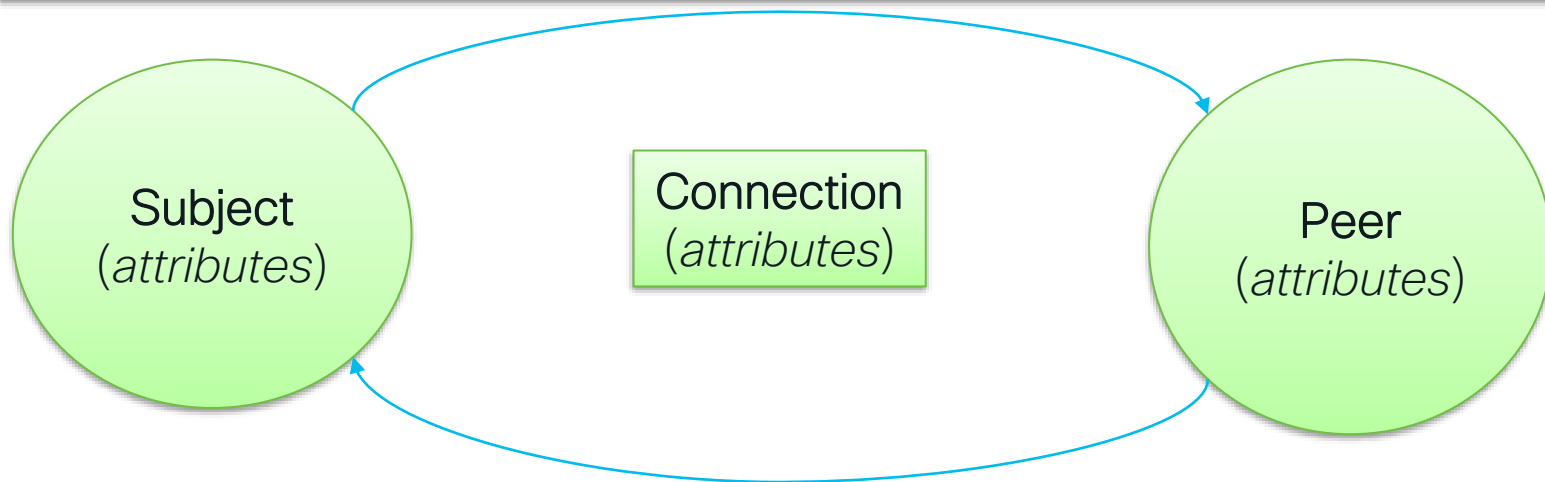
Custom Security Events

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

Matt's Note:

When implemented these are often the most immediately actionable events

Generate an action when a single flow matches the selected conditions



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

Policy Management | Custom Security Event

Cancel

Save

Actions ▾

When any subject host; as a user with a Trust Sec ID of **4** communicates with any host within *Canada*, an alarm is raised.

NAME *

DESCRIPTION

STATUS

CSE: Employees to Canada

This rule is a combination of TrustSec Metadata and Geo-IP Host Groups

☒ ON

FIND ⓘ

ACTIONS

SUBJECT TRUSTSEC ID

4 ✕

✕ AND

PEER HOST GROUP ⓘ

Canada ✕

✕

🔔 Alarm when a single flow matches this event.

Example CSE using Endpoint Attributes from CSC NVM Module

Policy Management | Custom Security Event

CancelSave

Actions

Name *

CSE: Forbidden Application: tor.exe

Description

A device is using the forbidden application tor.exe

Status

☒ On

When any *subject host*, using the process *tor.exe* communicates with any *peer host*, an alarm is raised.

Find ⓘ

Subject Process Names

tor.exe

×

+

Actions

🔔

Alarm when a single flow matches this event.

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

Custom Events (9) Relationship Events (412) Core Events (438) [Create New Policy](#)

EVENT	POLICY NAME	MAP OR DIAGRAM NAME	HOST GROUPS	TRAFFIC BY SERVICES	TRAFFIC BY APPLICATIONS	STATUS
Ex. Relationship High Traffic	Filter Policy Name	Filter Map or Diagram Name	Ex. "Inside Hosts"	Ex. "https"	Ex. "Corporate Email"	Ex. "On"
Relationship High Total Traffic	Inside Hosts <-> Outside Hosts / ID: 0	Internet Usage	Inside Hosts ↔ Outside Hosts	--	--	<input type="checkbox"/> Off

Description

This event indicates that the total traffic between the two host groups in the relationship exceeds the threshold. The alarm is raised if the alarm condition exists for longer than a user-specified duration.

☒ Behavioral and Threshold ☐ Threshold Only

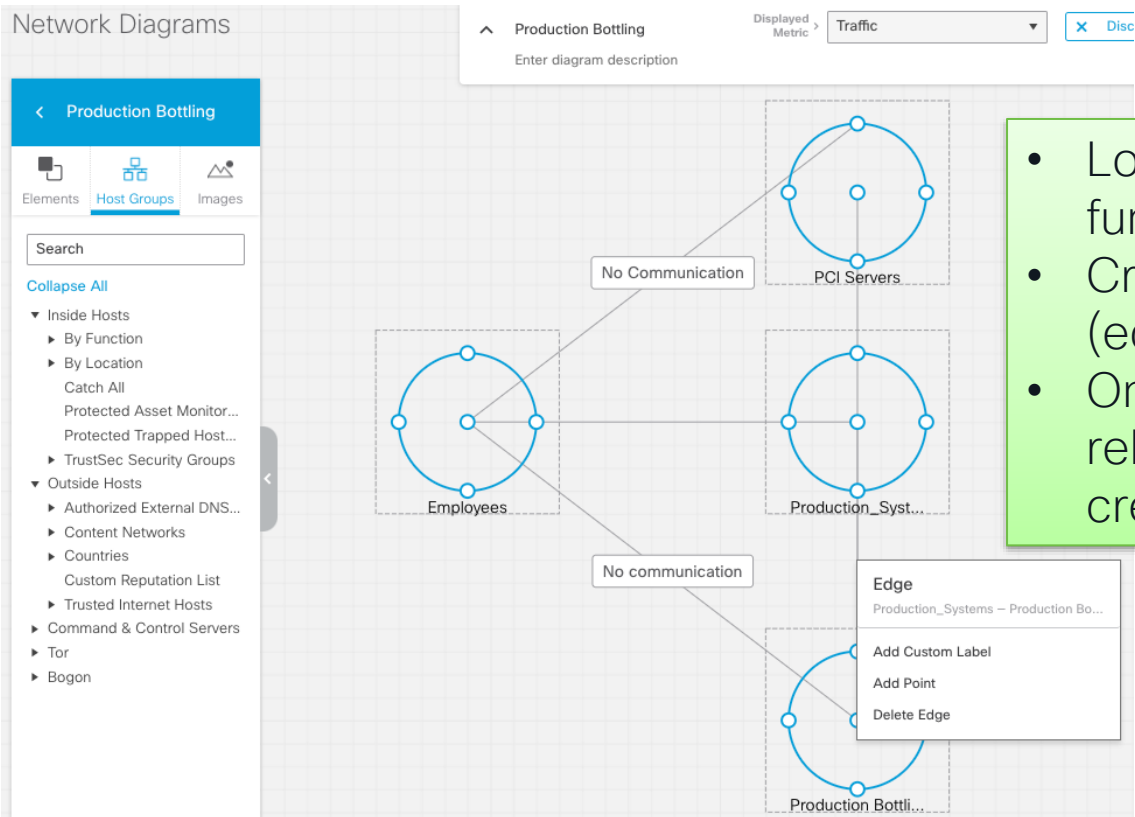
Tolerance 50 / 100

Never trigger alarm when less than: 1 G bytes in 24 hours

Always trigger alarm when greater than: 100 G bytes in 24 hours

Trigger alarm when duration greater than: 5 minutes

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

Policy Management | Relationship Policy

Events

Search

Select All Deselect All

- ☐ Relationship High Total Traffic
- ☐ Relationship High Traffic
- ☐ Relationship Low Traffic
- ☐ Relationship Max Flows
- ☐ Relationship New Flows
- ☐ Relationship Round Trip Time
- ☐ Relationship Server Response Time
- ☐ Relationship TCP Retransmission Ratio
- ☐ Relationship SYN Flood
- ☐ Relationship UDP Flood
- ☐ Relationship ICMP Flood

NAME *

Inside - Outside

DESCRIPTION

HOST GROUP - SIDE 1 *

+ Inside Hosts x

HOST GROUP - SIDE 2 *

+ Outside Hosts x

TRAFFIC BY SERVICES AND APPLICATIONS

+ All Services

All Applications

MAP OR DIAGRAM NAME

Relationship Events (1)

Select Events

EVENT	POLICY NAME	MAP OR DIAGRAM NAME	HOST GROUPS	TRAFFIC BY SERVICES	TRAFFIC BY APPLICATIONS	STATUS	ACTIONS
Ex. Relationship High Traffic	Filter Policy Name	Filter Map or Diagram Name	Ex. "Inside Hosts"	Ex. "https"	Ex. "Corporate Email"	Ex. "On"	
Relationship High Total Traffic	Inside - Outside		Inside Hosts ↔ Outside Hosts	All Services	All Applications	<input checked="" type="checkbox"/> On	Delete

Description

This event indicates that the total traffic between the two host groups in the relationship exceeds the threshold. The alarm is raised if the alarm condition exists for longer than a user-specified duration.

☒ Behavioral and Threshold

☐ Threshold Only

Tolerance 50 / 100

Never trigger alarm when less than: 1 G bytes in 24 hours

Always trigger alarm when greater than: 100 G bytes in 24 hours

Trigger alarm when duration greater than: 5 minutes

Core Events

Core Events

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

Matt's Note:

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

Entity
(IP Address,
Host Group)

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

Event	Event Type	Policy Name	Policy Type	Hosts	When Host Is Source	When Host Is Target
Suspect Data Hoarding	Ex. C...	Inside Hosts	Ex. Role	Ex. Network Scanners	Ex. On + Alarm	Ex. On + Alarm
Suspect Data Hoarding	Security	Inside Hosts	Default	Inside Hosts	On	On

Description

The source host has downloaded an unusual amount of data from one or more hosts.

☒ Behavioral and Threshold

☐ Threshold Only

Tolerance / 100

Never trigger alarm when less than: downloaded payload bytes in 24 hrs

Always trigger alarm when greater than: downloaded payload bytes in 24 hrs

Example (Very Simple) Core Event: ICMP_ECHO_REQUEST



ICMP echo request = 1 point



Monday

Tuesday

Wednesday

Thursday

ICMP Points:

- Today: 10
- 30-day Model: 10

ICMP Points:

- Today: 20
- 30-day Model: 15

ICMP Points:

- Today: 15
- 30-day Model: 15

ICMP Points:

- Today: **1000**
- 30-day Model: 15

Anomaly condition for algorithm met. Observation generated.

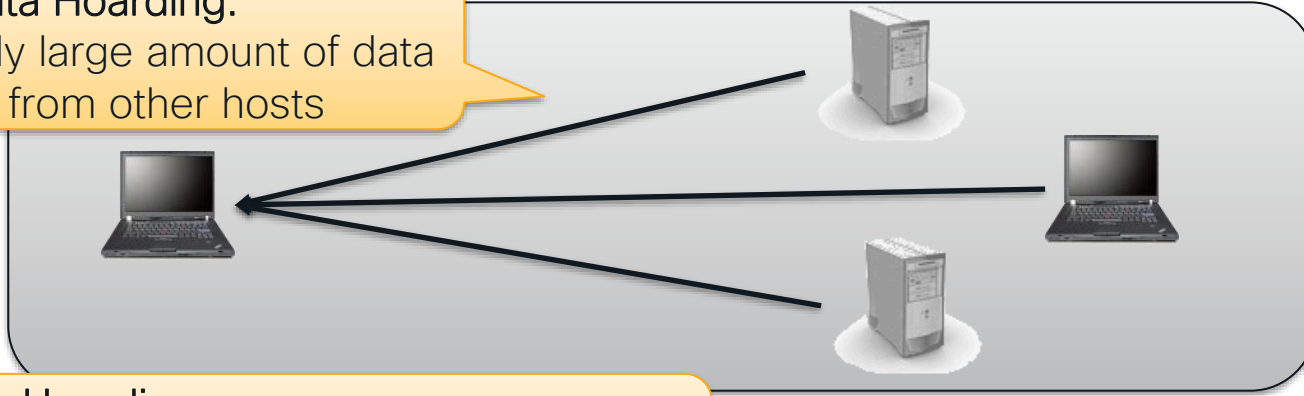
Note 1: Anomaly condition requires 7 days of traffic baseline in real life.

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

Example Algorithm: Data Hoarding

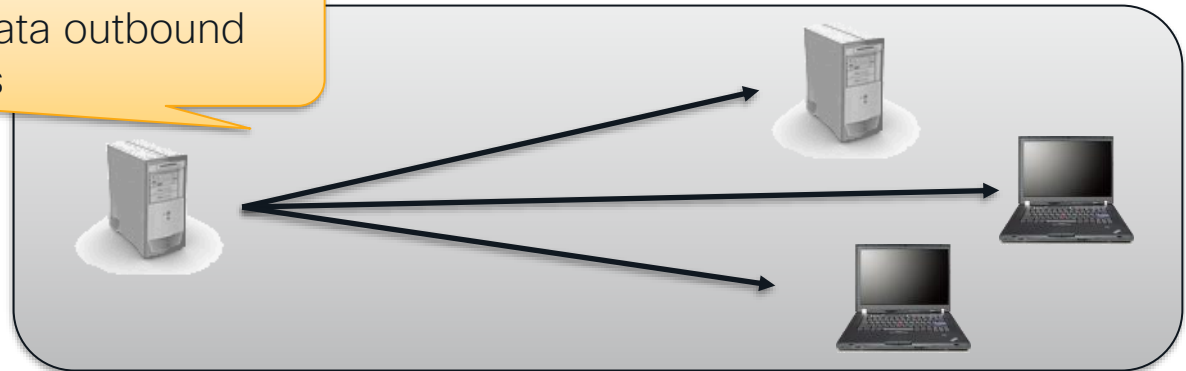
Suspect Data Hoarding:

- Unusually large amount of data inbound from other hosts

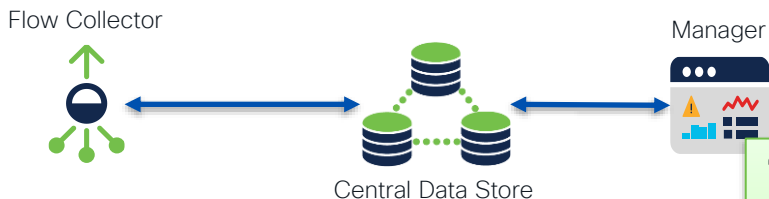


Target Data Hoarding:

- Unusually large amount of data outbound from a host to multiple hosts



Analytics Node (on box)

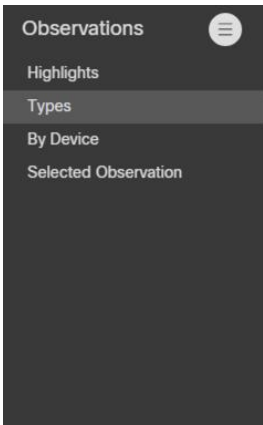


Matt's Note:

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



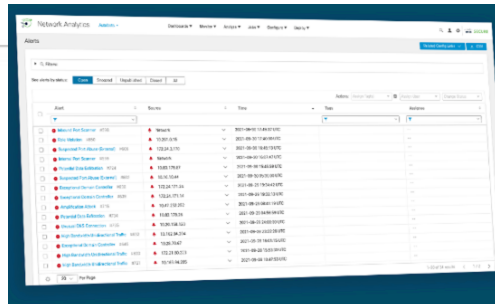
Types Observations

Anomalous Profile Observation (0) ⌵

Device(s) used a profile for the first time which differs from typical behaviors seen in the network (e.g., an abnormally high number of devices using the profile for the first time, sending anomalous traffic)

Telemetry: **Netflow**

Bad Protocol Observation (0) ⌵



Welcome to Analytics

Analytics provides additional detection and modeling capabilities as well as new interface features that enable you to review, prioritize, and address any security concerns.

Beginning with v7.3.2, Analytics provides:

- Automated role detection
- Additional alerting capabilities
- Experimental alert dashboard
- Supporting device report

Threat Intelligence 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

Matt's Note:

These are often immediately actionable events

Host Group Management

Filter by Host Group Name

- ▼ demo.local ...
 - ▶ Inside Hosts ...
 - ▶ Outside Hosts ...
 - ▼ Bogon ...
 - ◉ Bogon Subnets ...
 - ▶ ✓ Command & Control Servers ...
 - ▼ Tor ...
 - ◉ Tor Entrance ...
 - ◉ Tor Exit ...

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

Detected Threats

Threats that we detected on your network

Malicious file execution

Execution of file with malicious name or other characteristics

Last seen: 6 hours ago
Affected Assets: 1
Alerts: 1
Category: Attack Pattern - unknown

High Severity

Threat Detail

DoS attack

This may indicate a Denial-of-service (DoS) attack or non-stealthy scanning activity

Last seen: 21 days ago
Affected Assets: 1
Alerts: 1
Category: Attack Pattern - unknown

High Severity

Threat Detail

Cryptocurrency miner

Software that uses your computing resources to mine cryptocurrencies

Last seen: 6 hours ago
Affected Assets: 3
Alerts: 2
Category: Tool - crypto miner

High Severity

Threat Detail

Tor

Free software and network for enabling anonymous communication

Last seen: 14 hours ago
Affected Assets: 5
Alerts: 3
Category: Tool - anonymization

Medium Severity

Threat Detail

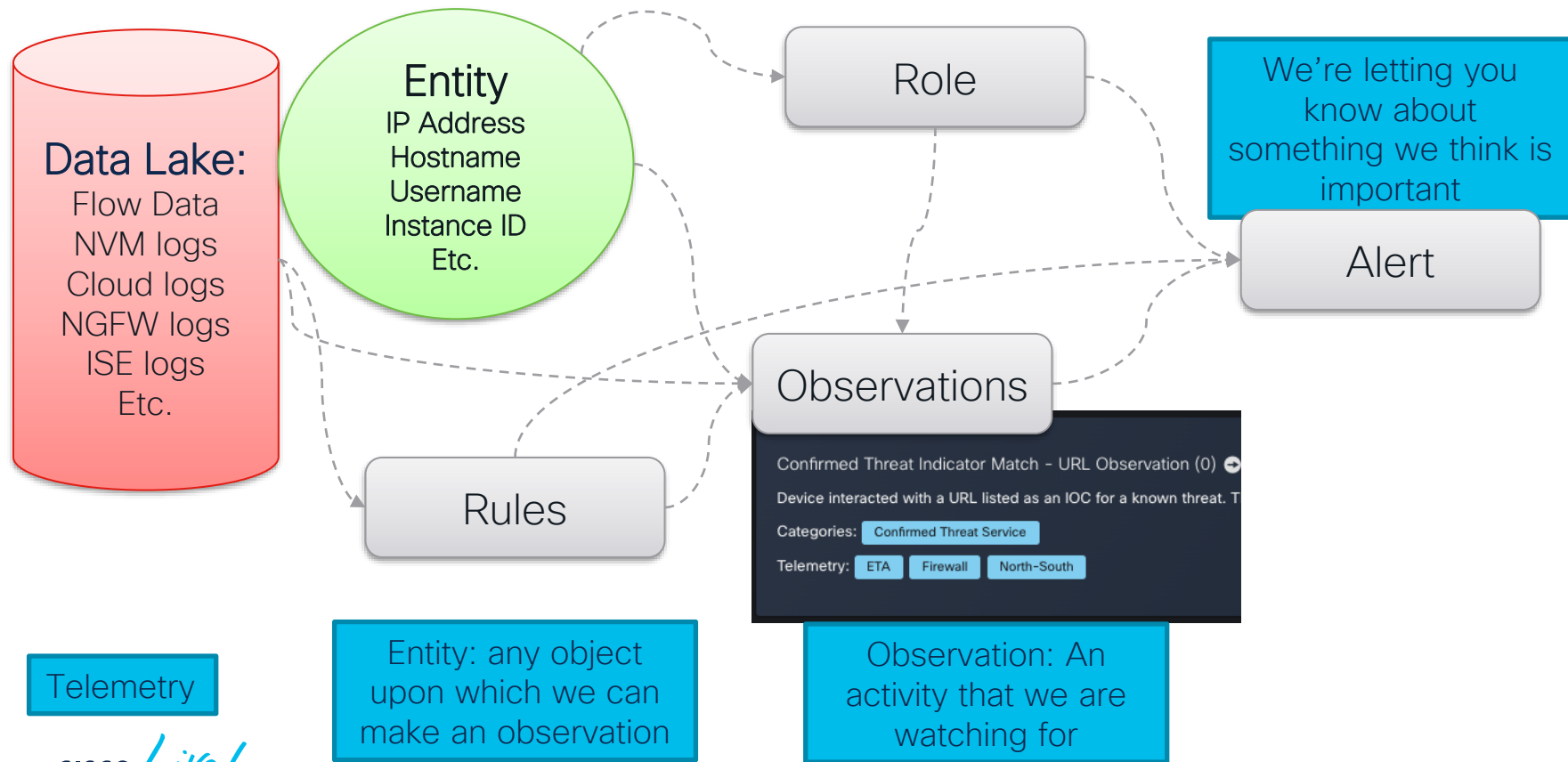
Global Threat Alerts

The screenshot displays the Cisco Global Threat Alerts dashboard. The left sidebar contains navigation links for Detections, Alerts (with sub-links for New, Open, Closed, Threat Catalog, Detected, Suppressed, All, Asset Groups, Affected, Suppressed, and Settings), and a menu icon. The main content area is titled 'New Alerts' and shows 'Alerts pointing to risks on your network'. It includes filters for 'Active from' (October 22nd to December 6th), 'Risk level' (Critical, High, Medium, Low), and a search bar. A table of alerts is shown, with the first alert being a 'High Risk' alert for a 'Network Denial Of Service (T1498)' threat, affecting the 'Stealthwatch System' asset group. The alert was detected on December 5th and modified 8 hours ago. The IP address 10.1.1.110 is listed. At the bottom right of the alert card are buttons for 'Open', 'Close', and 'Alert Detail'.

Adjust threat severity and asset value to prioritise alerts

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

Secure Cloud Analytics



SCA Alert

Cloud Analytics Monitor Investigate Report Settings

Metasploit Executed

Alert Type Details

Description: Execution of Metasploit exploits has been detected in endpoint via endpoint telemetry.

Next Steps: Isolate the endpoint and investigate the exploits and payloads that got executed on the endpoint.

MITRE Tactics: **Execution**

MITRE Techniques: **User Execution**

Alert Type Priority: **High** [go to alert priorities page](#)

Alert Rule Details

Status: **Open**

ID: 1411

Latest Observation: 2023-02-01 10:50:05 PST

First Observation: 2023-02-01 10:05:02 PST

Detected At: 2023-02-01 11:20:28 PST

IPs at the time of alert: 10.90.90.201

Assignee:

Tags:

Post an Incident: [Post to SecureX Incident Manager](#)

Close Alert: [Close Alert](#)

Device Outline

last updated: today
10.90.90.201

[more actions](#) [device summary](#)

Name: 10.90.90.201

IPs: 10.90.90.201

Roles: Cisco AMP Client

Subnets: 10.90.90.0/24 (Employee Wired)

Entity Groups: Employees

Open Alerts: 4

Int Connections: 187

Ext Connections: 8

Sensors: ona-9abc6e

Sensor Types: ONA,SAL

Exporters: FTD

ATTENDANCE

Normally Active: 0:03:30 to 23:41:37

OBSERVATIONS

Observations: 5545

10-Day Activity (Connections)

[Show more device details](#)

Supporting Observations

[All Observations for 10.90.90.201](#)

SCA Alert: Was this alert helpful?

Cloud Analytics Monitor Investigate Report

Metasploit Executed

Alert Type Details

Description: Execution of Metasploit exploits has been detected in end...

Next Steps: Isolate the endpoint and investigate the exploits and payl...

MITRE Tactics: **Execution**

MITRE Techniques: **User Execution**

Alert Type Priority: **High** [go to alert pri...](#)

Alert Rule Details

Status: **Open**

ID: 1411

Latest Observation: 2023-02-01 10:50:05 PST

First Observation: 2023-02-01 10:05:02 PST

Detected At: 2023-02-01 11:20:28 PST

IPs at the time of alert: 10.90.90.201

Assignee:

Tags:

Post an Incident: [Post to SecureX Incident Manager](#)

Close Alert: [Close Alert](#)

Close Alert

Was this alert helpful? [?](#)

Snooze this alert(s)?

Alert(s):

Type	Scope	Value
Metasploit Executed	Source	10.90.90.201

Don't show the alert matching the above criteria for a period of:

Device Outline

last updated: today

10.90.90.201

[more actions](#) [device summary](#)

Name: 10.90.90.201

IPs: 10.90.90.201

Roles: Cisco AMP Client

Subnets: 10.90.90.0/24 (Employee Wired)

Entity Groups: Employees

Open Alerts: 4

Int Connections: 187

Ext Connections: 8

Sensors: ona-9abc6e

Sensor Types: ONA,SAL

Exporters: FTD

ATTENDANCE

Normally Active: 0:03:30 to 23:41:37

OBSERVATIONS

Observations: 5545

10-Day Activity (Connections)

[Show more device details](#)

Supporting Observations

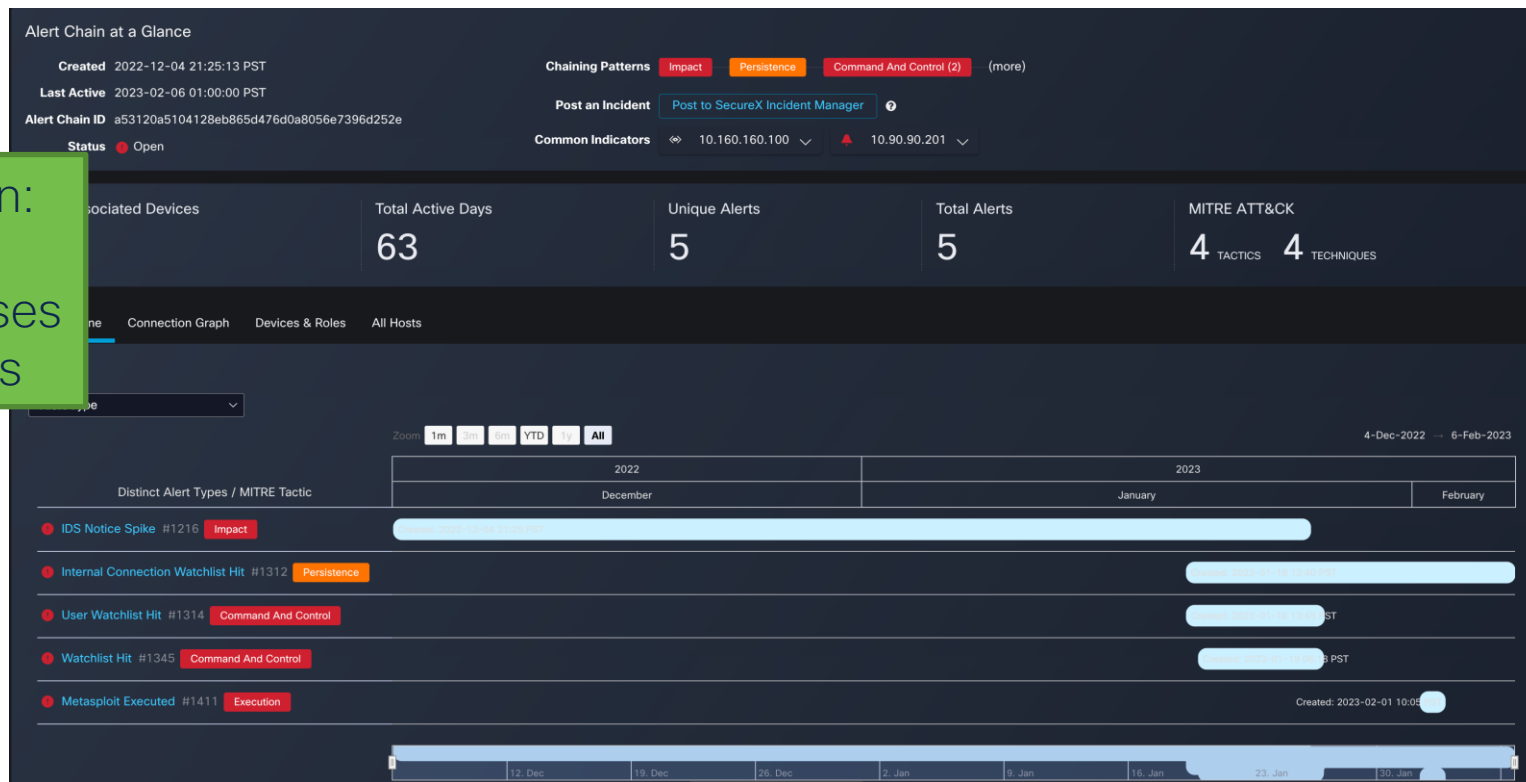
All Observations for 10.90.90.201

Alert Chaining (Beta)

Automatic correlation of related alerts

Correlation on:

- Devices
- IP Addresses
- Usernames



Demo



Extended Detection and Response

The Thing about Behaviour

There exist conditions that make the observation malicious



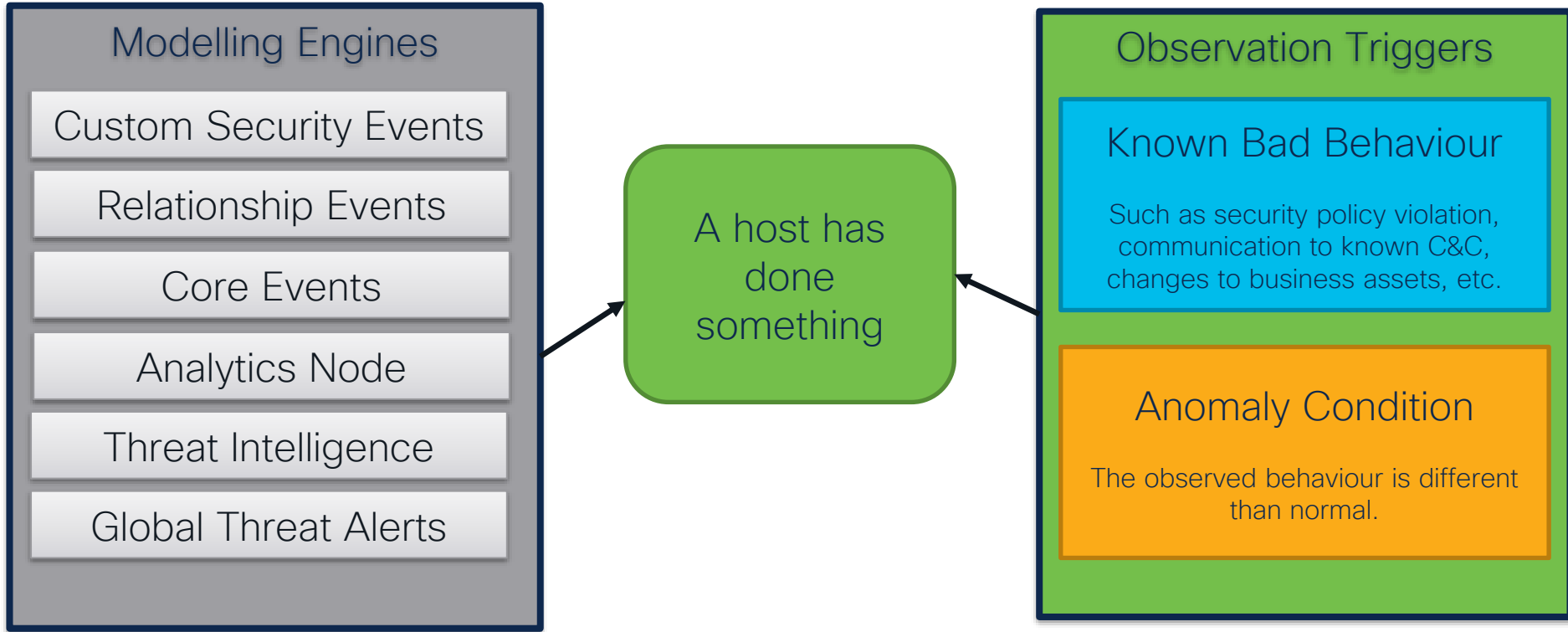
Observation:
This man drinks beer

Some observations are just
“different than normal”

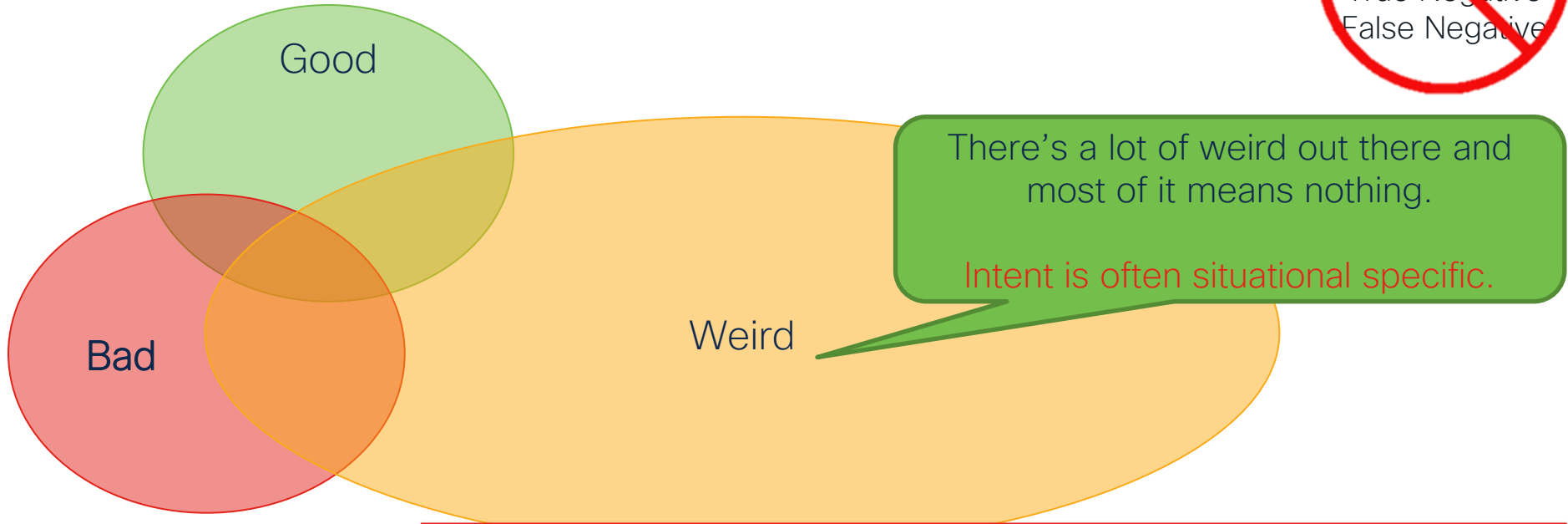


Key Idea:
Behaviour events are an observation

Behaviour events are an observation

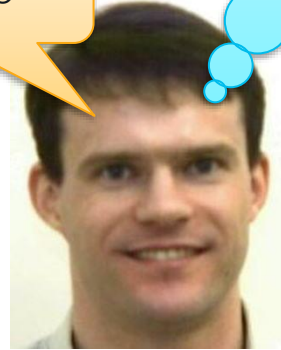
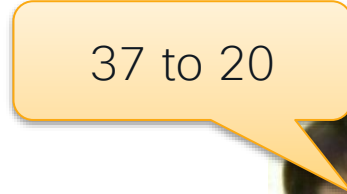
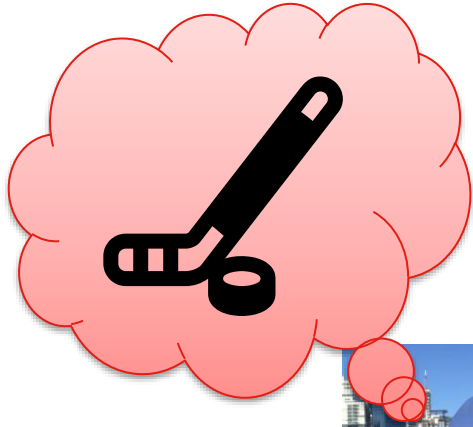


The Thing about Behaviour



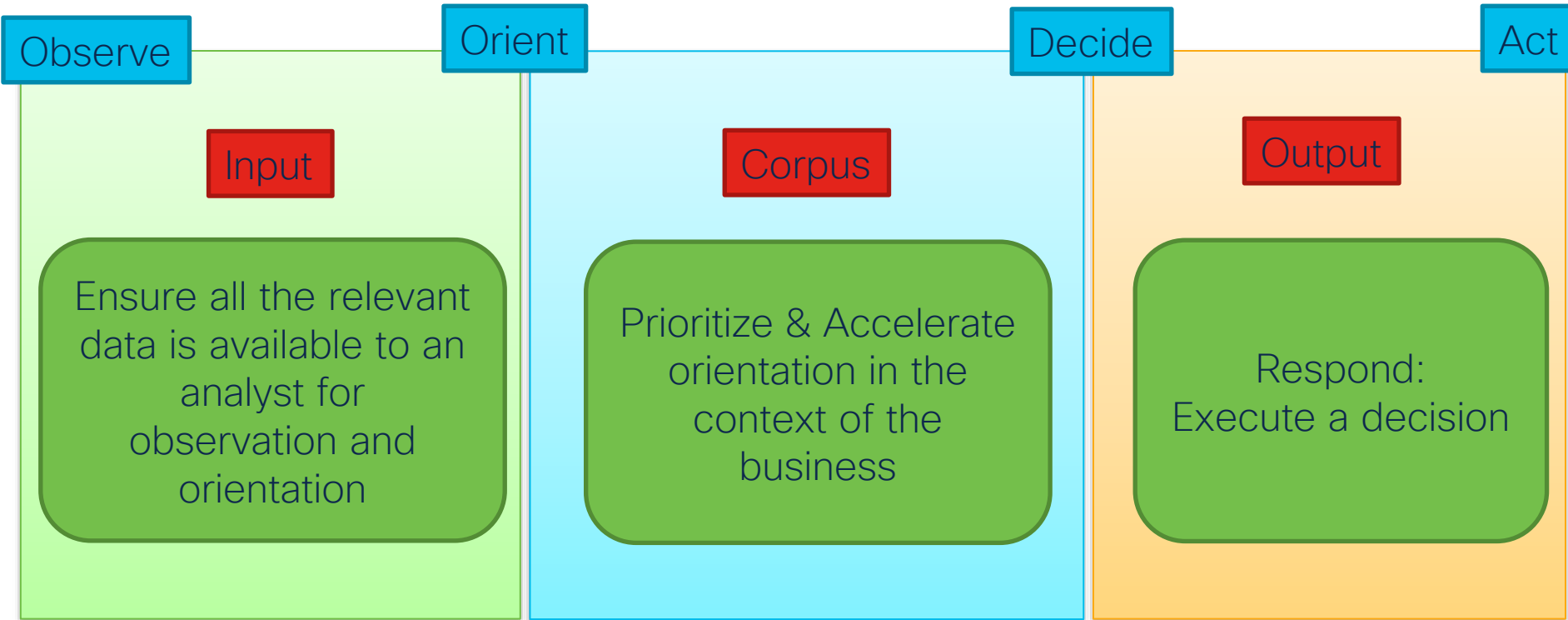
Intent requires business relevant language:
10.10.10.10 just uploaded a large amount of data to 128.107.78.10
versus
The PCI server just uploaded a large amount of data to an external server

Making the Alarms Business Relevant

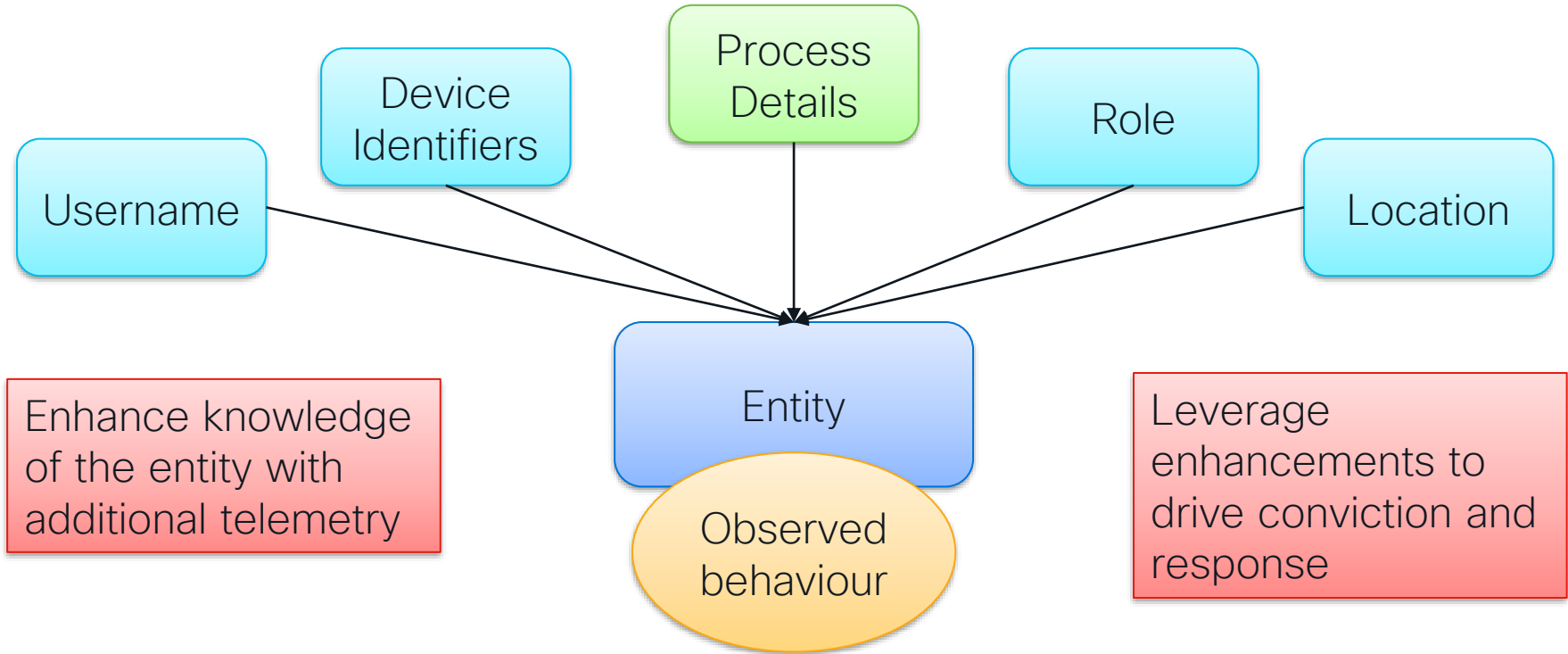


What matters to one organization might not matter to another

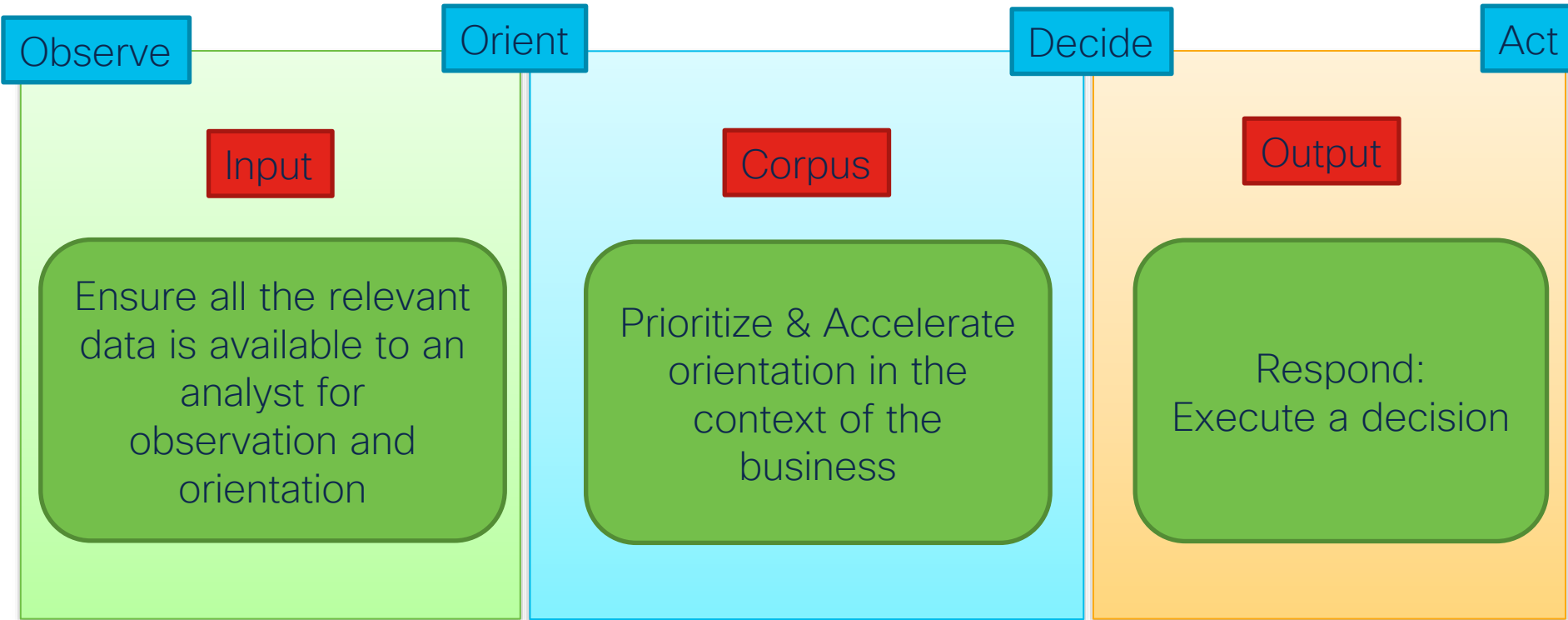
Making the Alarms Business Relevant



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

Event	Event Type	Policy Name	Policy Type	Hosts	When Host Is Source	When Host Is Target
Suspect Data Hoarding	Ex. C...	Inside Hosts	Default	Ex. Network Scanners	Ex. On + Alarm	Ex. On + Alarm
Suspect Data Hoarding	Security	Inside Hosts	Default	Inside Hosts	On Off On On + Alarm	On
Description The source host has downloaded an unusual amount of data from one or more hosts.						
<input checked="" type="radio"/> Behavioral and Threshold			Tolerance <input type="text" value="92"/> / 100			
<input type="radio"/> Threshold Only			Never trigger alarm when less than: <input type="text" value="500 M"/> downloaded payload bytes in 24 hrs			
			Always trigger alarm when greater than: <input type="text" value="1 T"/> downloaded payload bytes in 24 hrs			

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

The screenshot shows the MITRE ATT&CK matrix with columns for Initial Access, Execution, Persistence, Privilege Escalation, Discovery, Lateral Movement, and Command and Control. Each cell contains a list of specific attack techniques and the products that detect them.

Secure Network Analytics MITRE Mappings

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

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

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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. 2163580 07/2020

To learn more about Stealthwatch, please visit [cisco.com/go/stealthwatch](https://www.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

Policy Management | Role Policy

CancelSave

Actions

Name *

Exclude DNS Servers

Description

Exclude traffic events for DNS servers

Host Groups

+Authorized External DNS ServersX

DNS ServersX

IP Address Or Range

Core Events (2)

Select Events

Event	Event Type	When Host Is Source	When Host Is Target	Actions
Ex. Anomaly	Ex. Category	Ex. On + Alarm	Ex. On + Alarm	
High Total Traffic	Security	Off	Off	Delete
High Traffic	Security	Off	Off	Delete

50

items per page

1 - 2 of 2 items < < 1 / 1 > >

Tuning the Corpus: Adjust Alarm Severity

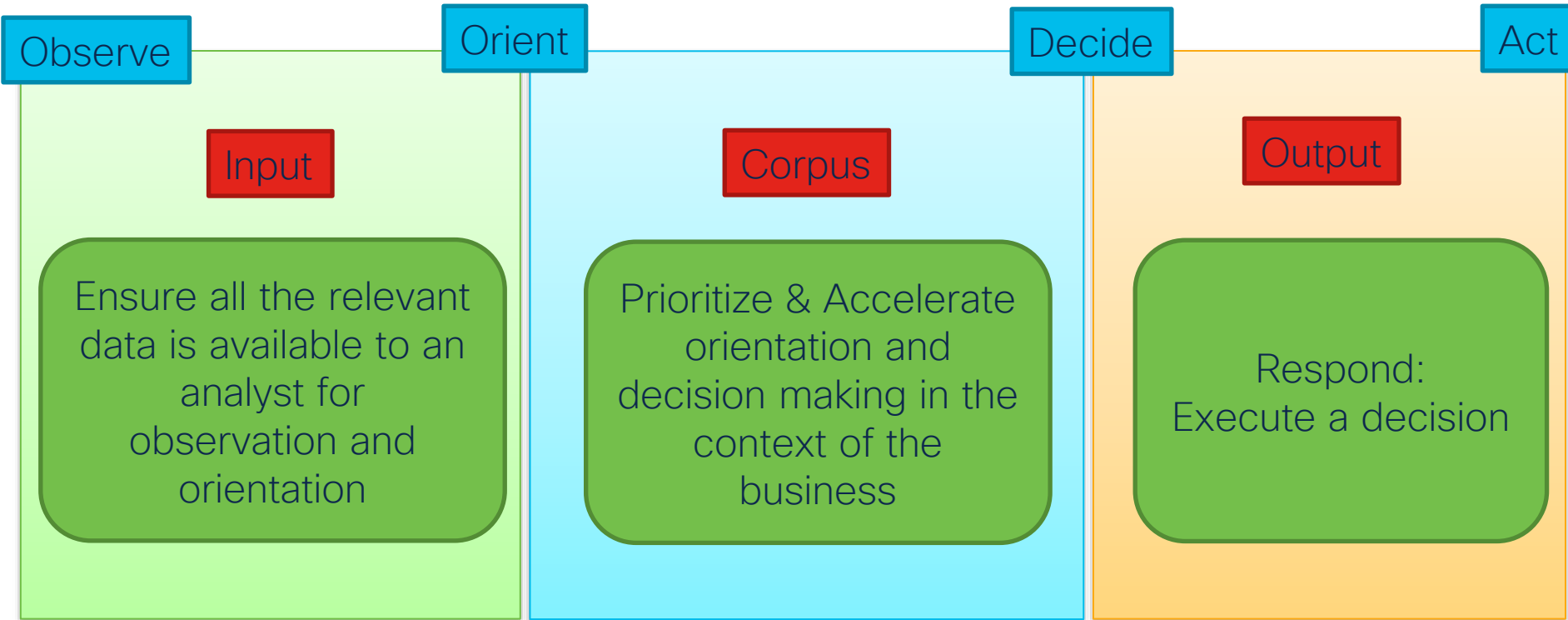
Alarm Severity

Alarm Type ↑	Alarm Severity
<input type="text"/>	<input type="text"/>
Suspect Data Hoarding	Major ▼
Suspect Data Loss	Critical
Suspect Long Flow	Major
Suspect Quiet Long Flow	Minor

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

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



Conviction:

- Who, what, when, where why, how

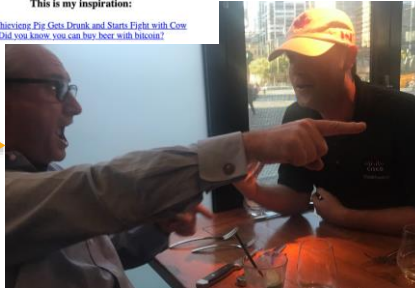
Investigating with OODA

Observation:
Missing Beer

Orient:
Gather data



This is my inspiration:
[Beer Thievery: Piv Gets Drunk and Starts Fight with Cow](#)
[Did you know you can buy beer with bitcoin?](#)



Orient:
Convict




Darrin Miller:
Beer Thief

Decide

Act

Observation to Action


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



Past Exposure:
Missing Beer

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

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.	<input checked="" type="checkbox"/>	...
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.	<input type="checkbox"/>	...
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.	<input type="checkbox"/>	...
CTA	Host Alarm		<input checked="" type="checkbox"/>	...

- 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				
CTA	Syslog Message				
Send email	Email	Sends an email to the recipients designated in the To field on the Email Action page.			
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	<input type="checkbox"/>	...

Syslog Message
Email
SNMP Trap
ISE ANC Policy
Webhook
Threat Response Incident

Export: 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.	<input checked="" type="checkbox"/>	...
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.	<input type="checkbox"/>	...
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.	<input type="checkbox"/>	...
CTA	Host Alarm		<input checked="" type="checkbox"/>	...

- 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				
CTA	Syslog Message				
Send email	Email	Sends an email to the recipients designated in the To field on the Email Action page.			
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	<input type="checkbox"/>	...

Syslog Message
Email
SNMP Trap
ISE ANC Policy
Webhook
Threat Response Incident

Remediating Action with ISE

Response Management

Rules Actions Syslog Formats

ISE ANC Policy Action

Cancel Save

Name
Assign to Quarantine Security Group

Description

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

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

ANC Policy
Quarantine_Host

Apply To
☒ Source Host ☐ Target Host

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

Rules Actions Syslog Formats

Rules | Host Alarm

Cancel Save

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	<input checked="" type="checkbox"/>

2. Define a response Rule that invokes the defined Action

XDR with SecureX and SNA/SCA

SECURE X

Workflow execution in Orchestration

Trigger actions via workflows

Create incidents automatically in Incident Manager as an alarm action

Incident Manager

Threat Response Investigation

Orchestration



Pull security events associated with observables during investigation enrichment

- ☒ Enable SecureX Security Ribbon and Pivot Menu ⓘ
- ☒ Enable SecureX Dashboard Tiles Service requests ⓘ
- ☒ Enable SecureX Threat Response enrichment requests ⓘ

Number of TOP Security Events

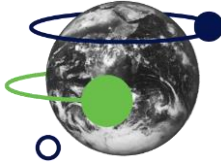
10

Period of time (days)

15

SNA alert promotion to SecureX

Secure
Network
Analytics



Create incidents automatically in
Incident Manager as an alarm action



Response Management

Rules Actions Syslog Formats

Threat Response Incident Action

Name: Description:

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

Incident Confidence Level:

☒ Create a new Target entity in SecureX Threat Response for alarms processed by this action.

- ☒ Create targets in Threat Response for internal hosts only.
- ☐ Create targets in Threat Response for internal and external hosts.

Use host details from the alarm data:

Incidents New Incident

Search...

> Assigned to me - Open (0)

> Assigned to me - New (0)

> Assigned to others - (5,300)

CSE: Employees to Bottling Line
Cisco Stealthwatch Enterprise Oct 07, 2021

CSE: Employees to Bottling Line
Cisco Stealthwatch Enterprise Oct 05, 2021

CSE: Employees to Bottling Line

Add short description...

New · Created By Cisco Stealthwatch Enterprise on 2021-10-07 04:00:01 UTC

Summary Observables Timeline Sightings Linked References (1)

Incident Title	CSE: Employees to Bottling Line
Confidence	High
Severity	High
Start Active Time	2021-10-07T04:00:01Z
Device ID	smc-01

SCA alert promotion to SecureX

Secure
Cloud
Analytics



Create incidents automatically in Incident Manager 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 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.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Default: Enabled	Normal Default Priority: Normal
Amplification Attack 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.	<input type="checkbox"/>	<input type="checkbox"/> Default: Disabled	Normal Default Priority: Normal
Anomalous AWS Workspace 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.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Default: Enabled	Normal Default Priority: Normal
Anomalous Mac Workstation An Apple Mac Workstation used a new anomalous behavioral profile (e.g., the host connected to many devices over BitTorrent). This alert uses the	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Default: Enabled	Normal Default Priority: Normal

Configure severity and publication settings in Secure Cloud Analytics

Status: **Open**

Unusual External Server for Cisco

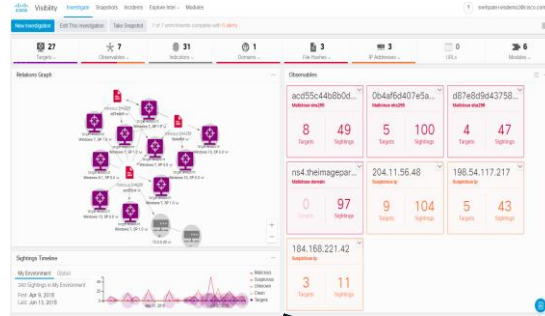
Created by [Cisco Secure Cloud Analytics](#) on 2022-03-22T08:47:56.000Z

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

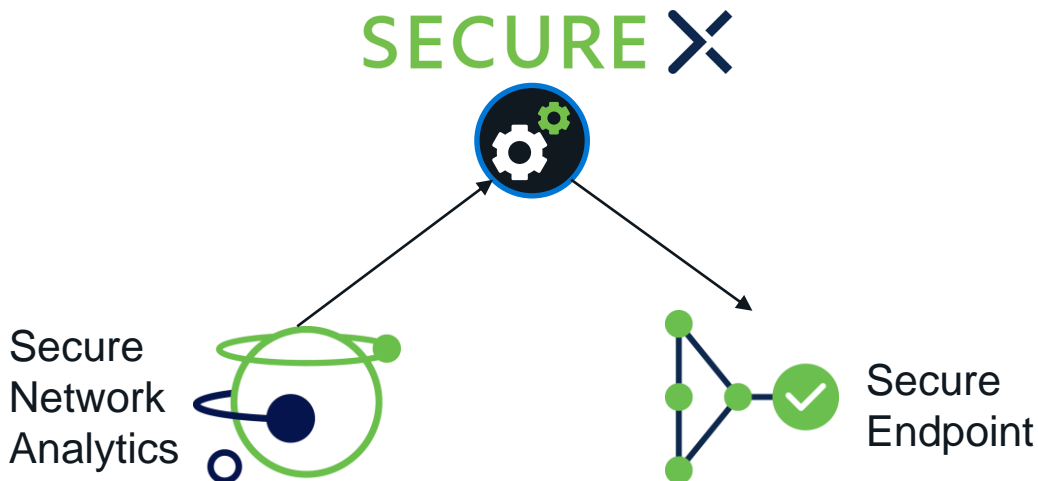
0034-SNA-GenerateCasebookWithTopHostsAndPe...

CISCO Live!

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 Sessions

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

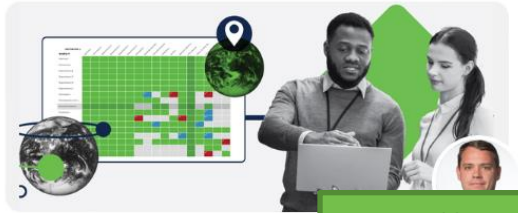


Security

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

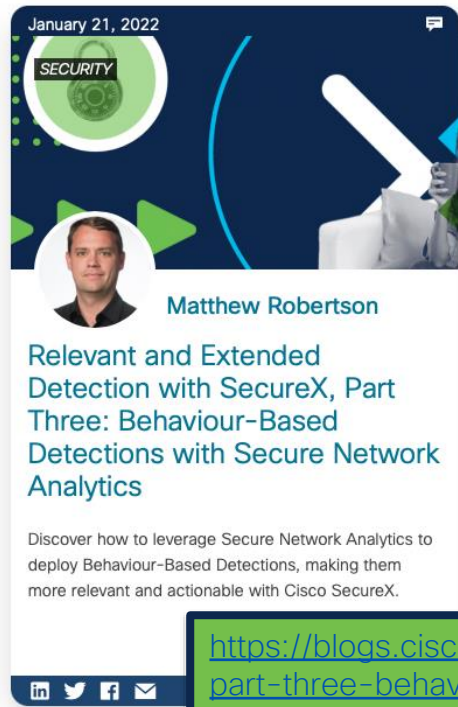
TrustSec Policy Analytics – Part Three: Policy Validation

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-three-behaviour-based-detections-with-secure-network-analytics>



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

Complete your Online Session Evaluation



Parting Thoughts

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



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.



The bridge to possible

Thank you

CISCO *Live!*

CISCO *Live!*

ALL IN