cisco Live!

Let's go

The bridge to possible

Visibility, Detection and Response

With Cisco Secure Network Analytics

Matthew Robertson, Distinguished Engineer

Agenda

Network Behaviour Analytics:
Understanding Secure Network Analytics Detections

Agenda:

- Introduction
- Visibility and Analytics
- TrustSec Policy Analytics
- SNA Detection Engines
- Detection Engineering
- Summary

About Me

Matt Robertson

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

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

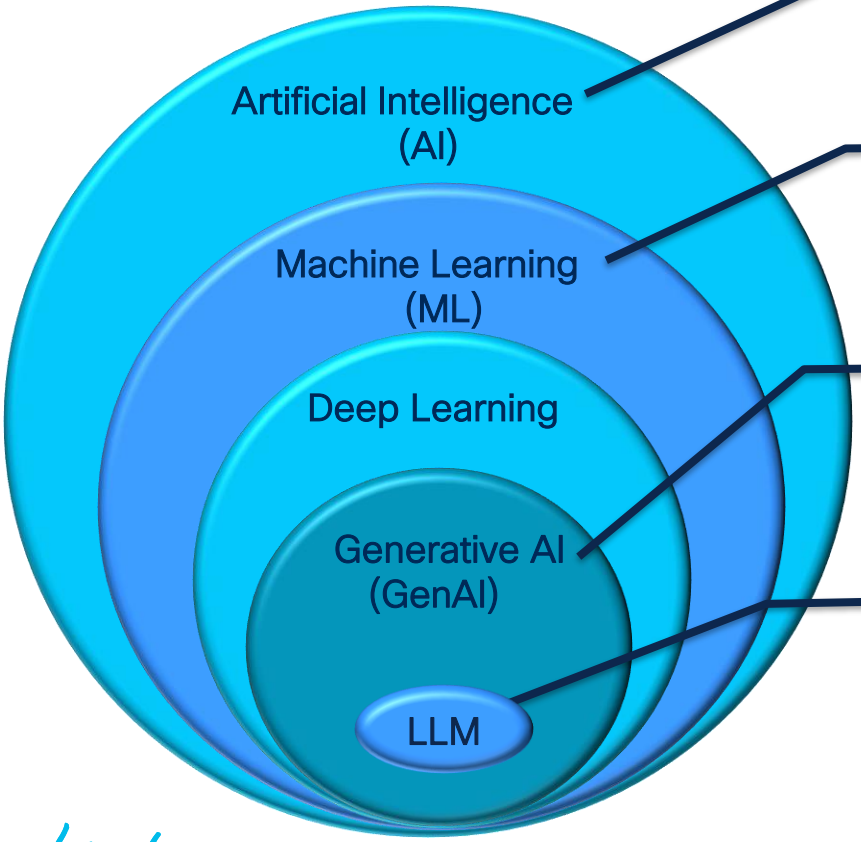
- Collection of telemetry from multiple security tools
- Application of analytics to the collected and homogenized data to arrive at a detection of maliciousness
- Response and remediation of that maliciousness

Analytics!

You Said Analytics!

Is that the AI/ML?

Artificial Intelligence Technology



Aims to mimic human behavior

Focuses on learning from data

Aims to generate new data or text that mirrors the input

Large Language Models (LLM) include GPT and ChatGPT specializing in understanding and generating human-like test

Analytics in Security Operations

Accelerating Decision Making

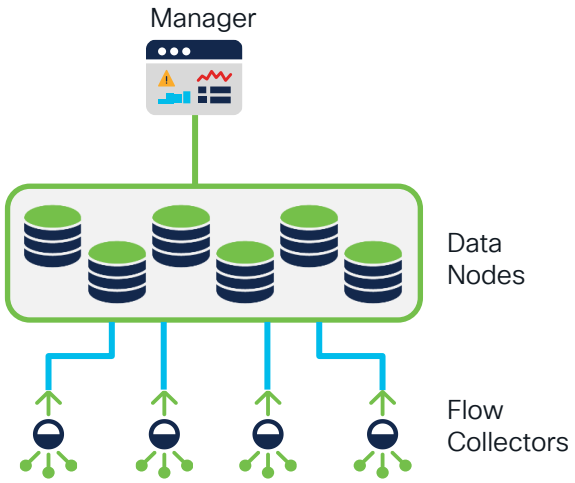
Observe	Orient	Decide	Act
Input	Corpus	Output	
Ensure all the relevant data is available to an analyst for observation and orientation	Prioritize & Accelerate orientation and decision making in the context of the business	Execute a decision	

AI is not magic

Algorithms directed at achieving a stated outcome

Cisco Secure Network Analytics Architecture

(Stealthwatch Enterprise)



BRKSEC-2248 – Design, Deploy and Troubleshoot Network Detection and Response
– Hanna Jabbour, Friday Feb 9 @ 11:00am

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

Naming FAQ

Is Secure Network Analytics and Stealthwatch the same thing?

Yes

What about Secure Cloud Analytics (Stealthwatch Cloud)?

Now Part of XDR

Network Visibility

Foundational Concept: Network Visibility

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

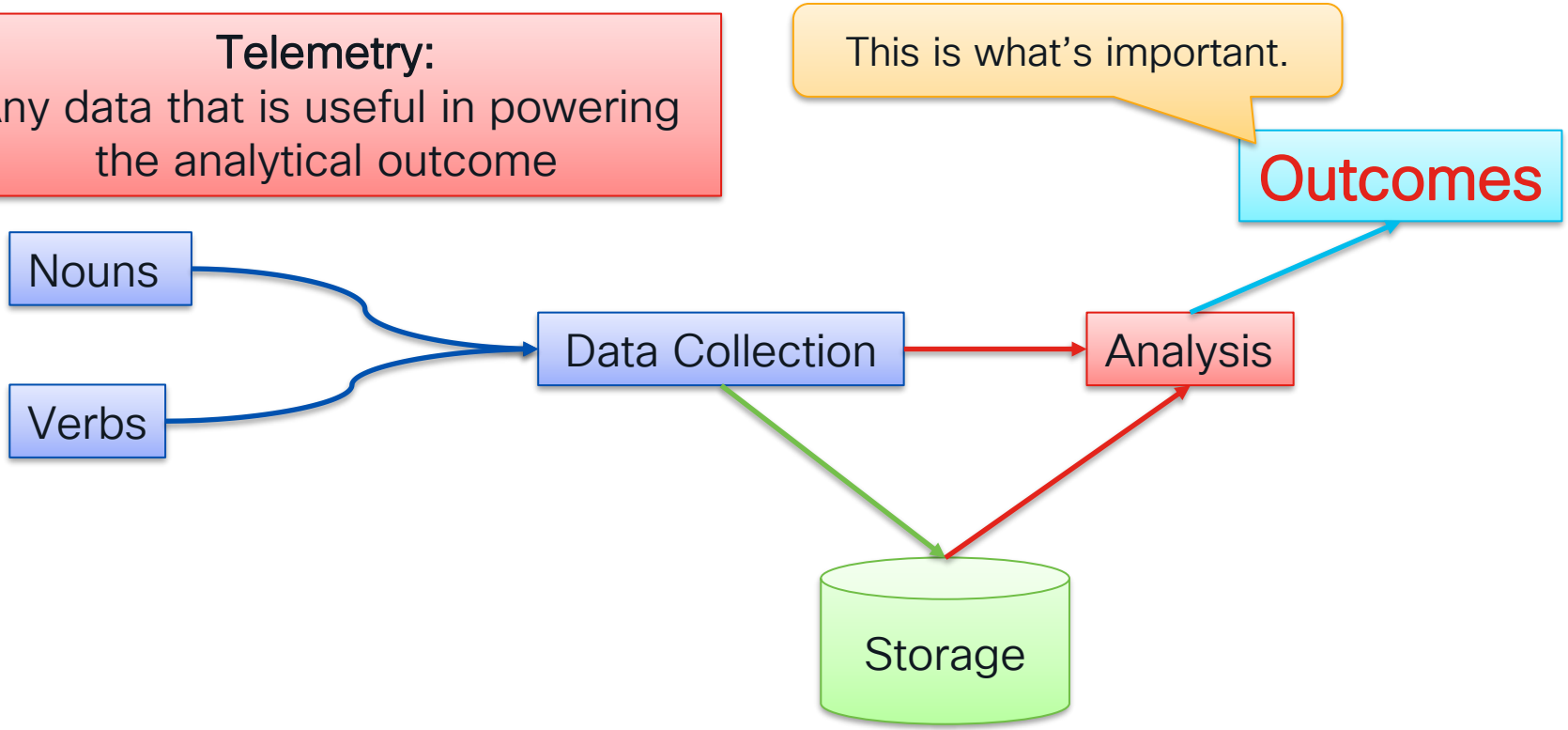
Transaction Attributes:
Time, ports, protocols, applications, etc.

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

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

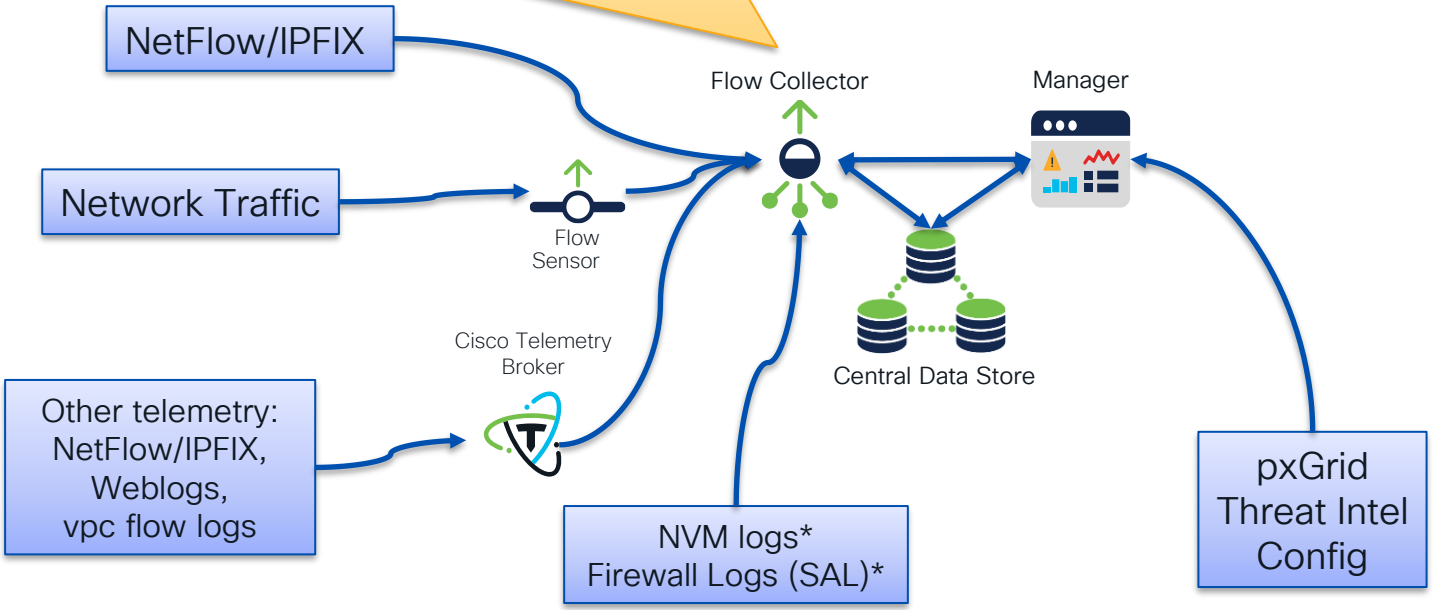
Powering Visibility & Analytics with Telemetry

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).

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

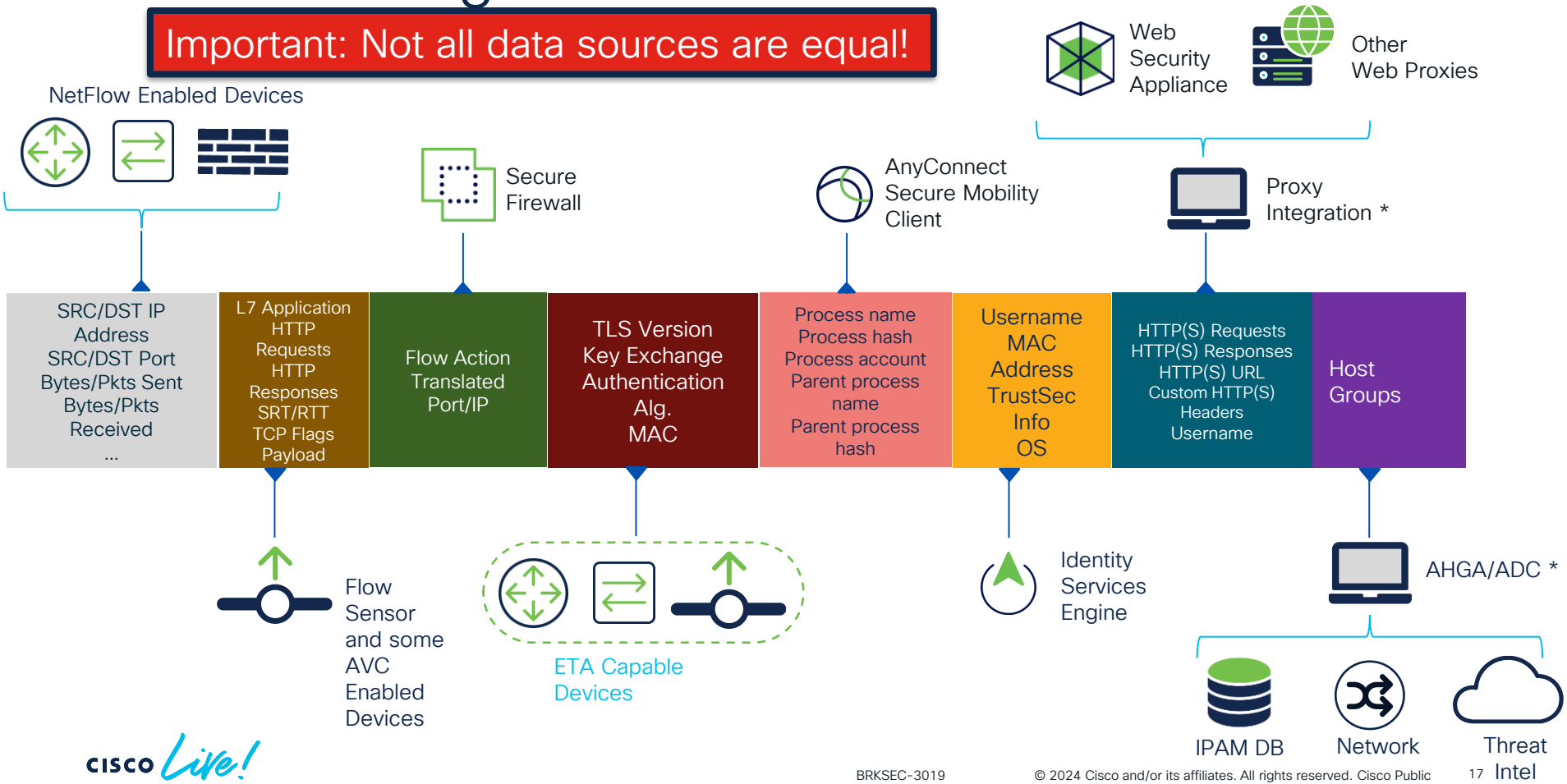
View URL Data

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

Important: Not all data sources are equal!



MS390 & C9300-M is an ideal SNA telemetry source

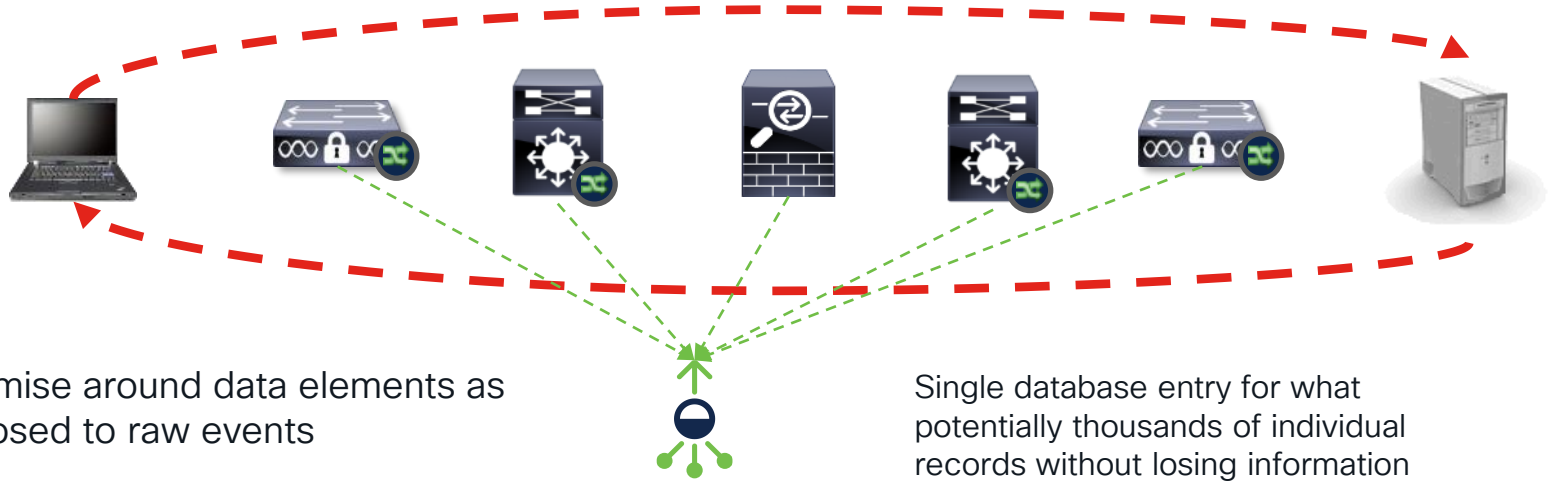
- Line rate, hardware supported telemetry
- Deep packet inspection enables application recognition
- Telemetry for advanced encrypted traffic analytics
- One click deployment to all devices

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. <=50min4	Ex. 10.10.10.10	chrome	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”

The magic of the bi-flow



Optimise around data elements as opposed to raw events

Single database entry for what potentially thousands of individual records without losing information

Cisco Stealthwatch and SIEM Optimization

Save time and money by integrating Stealthwatch with your SIEM deployment

Example Analytical Outcomes

We have data. So now what?

Security Policy:

Analyse network behaviour to design, implement and validate security policy

Threat Detection:

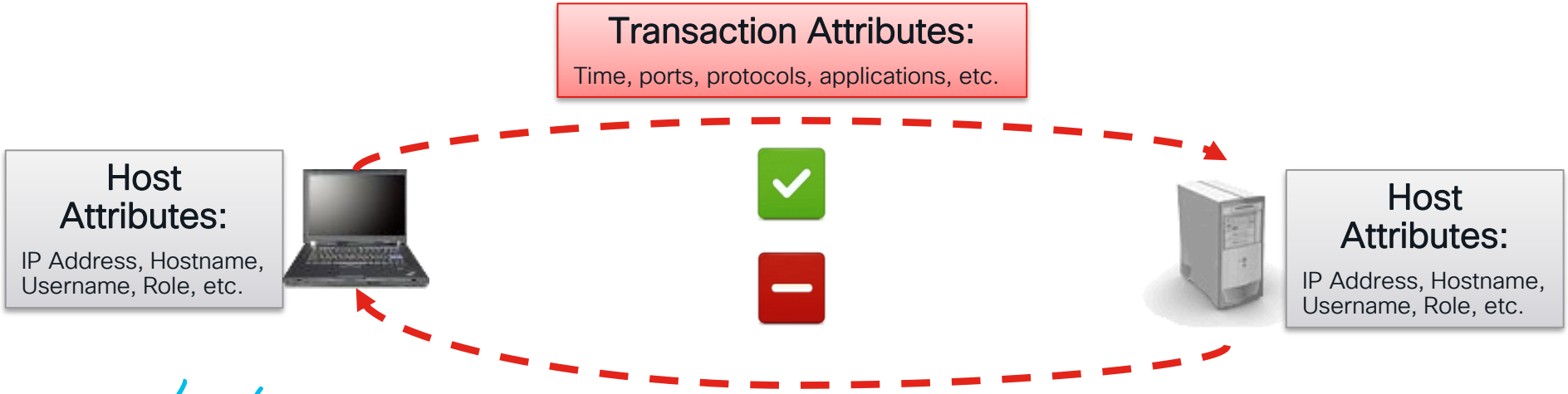
Analyse network behaviour to infer the presence of a threat actor

TrustSec Policy Analytics with SNA

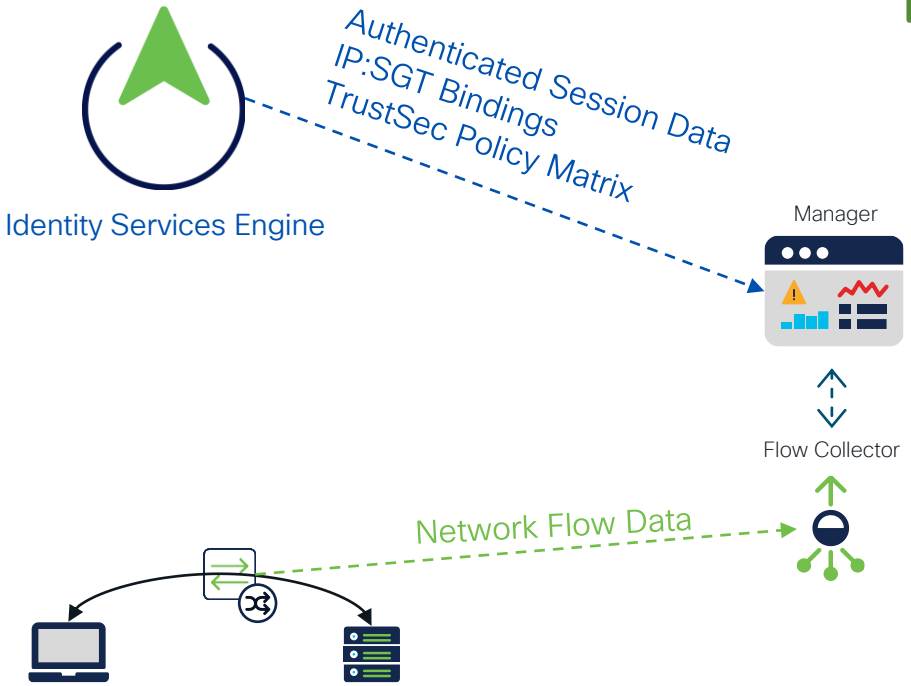
Policy Analytics

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?

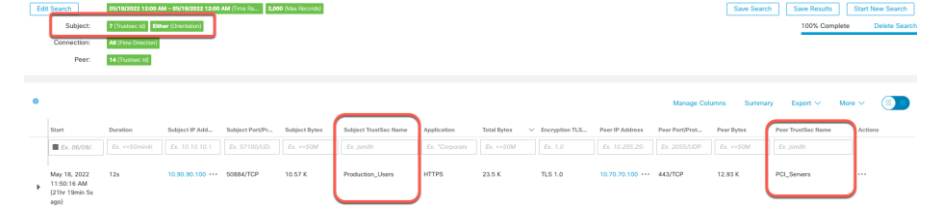


Policy Analytics with Secure Network Analytics



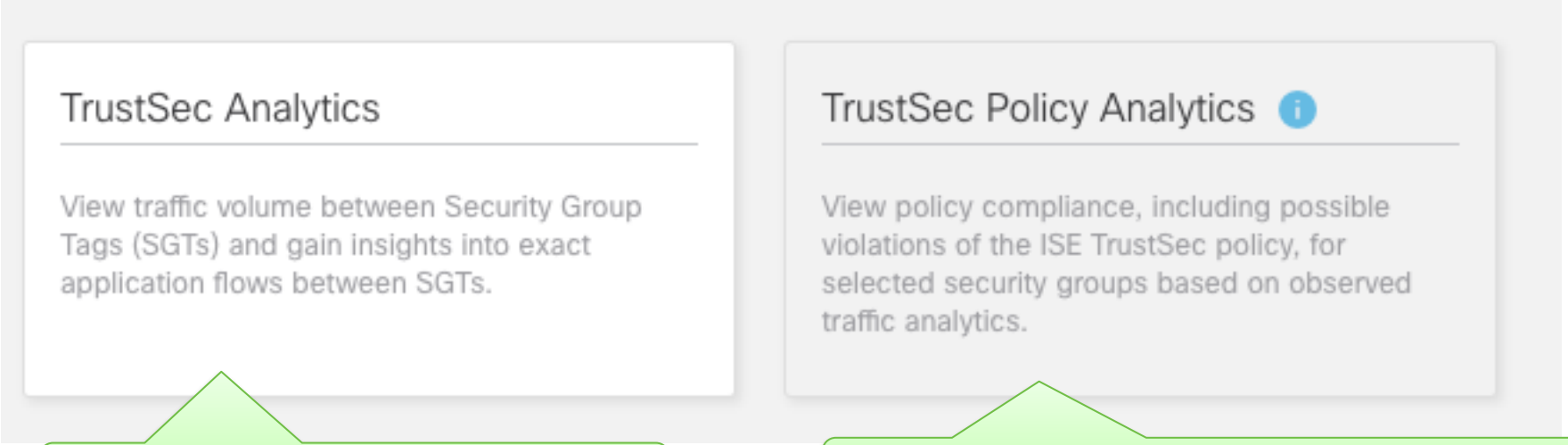
1. TrustSec Analytics Reports

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



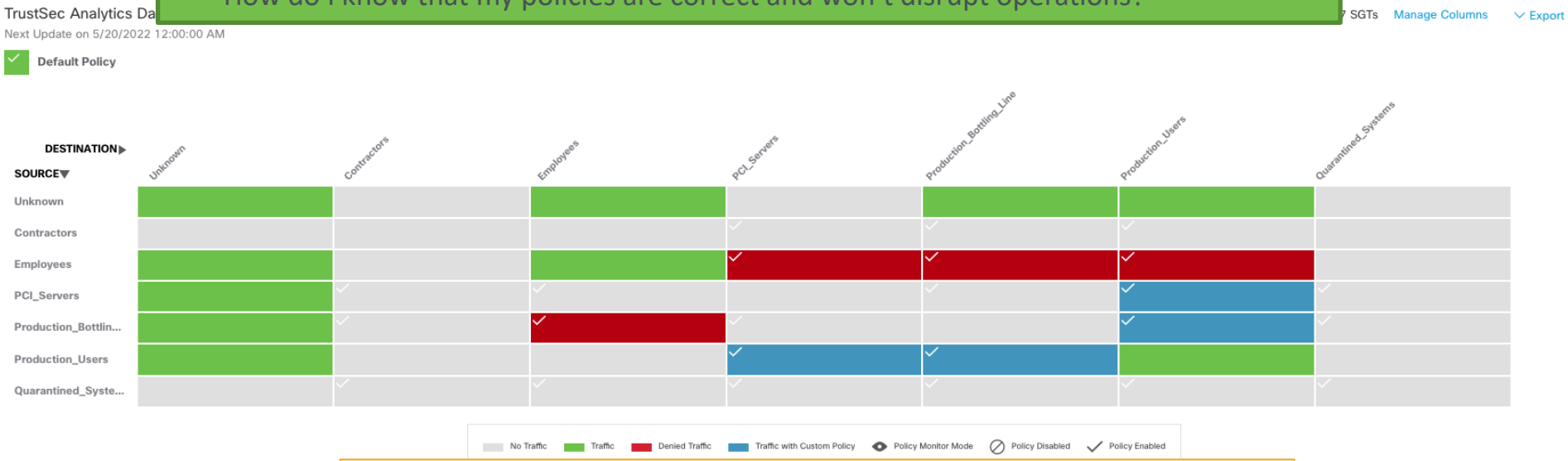
Multiple Reports of this type allowed

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

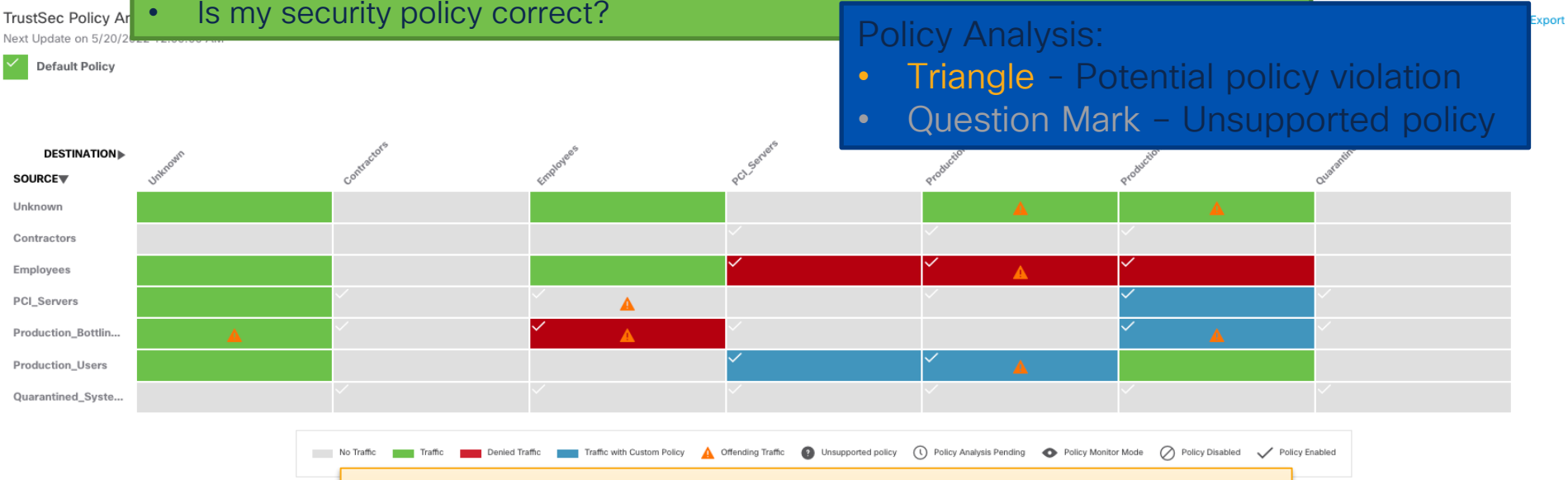
SNA: TrustSec Policy Analytics Report

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

Behavioural Modelling and Detection

- Analyze observables
- Establish baseline
- Make observations

Use the Behaviour model to generate detections (outcomes)

Host definitions and classifications

Entity Model

Behavioral Observations

Detections:

- Leveraging known bad (conditions known apriori)
- A change from normal

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

Central Analytics Node

- Runs on Manager, requires central data store
- CDS data => centralised Analytics
- Common network flow analytics with XDR
- Can promote alerts as XDR Incident

Cloud Enabled

Threat Intelligence

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

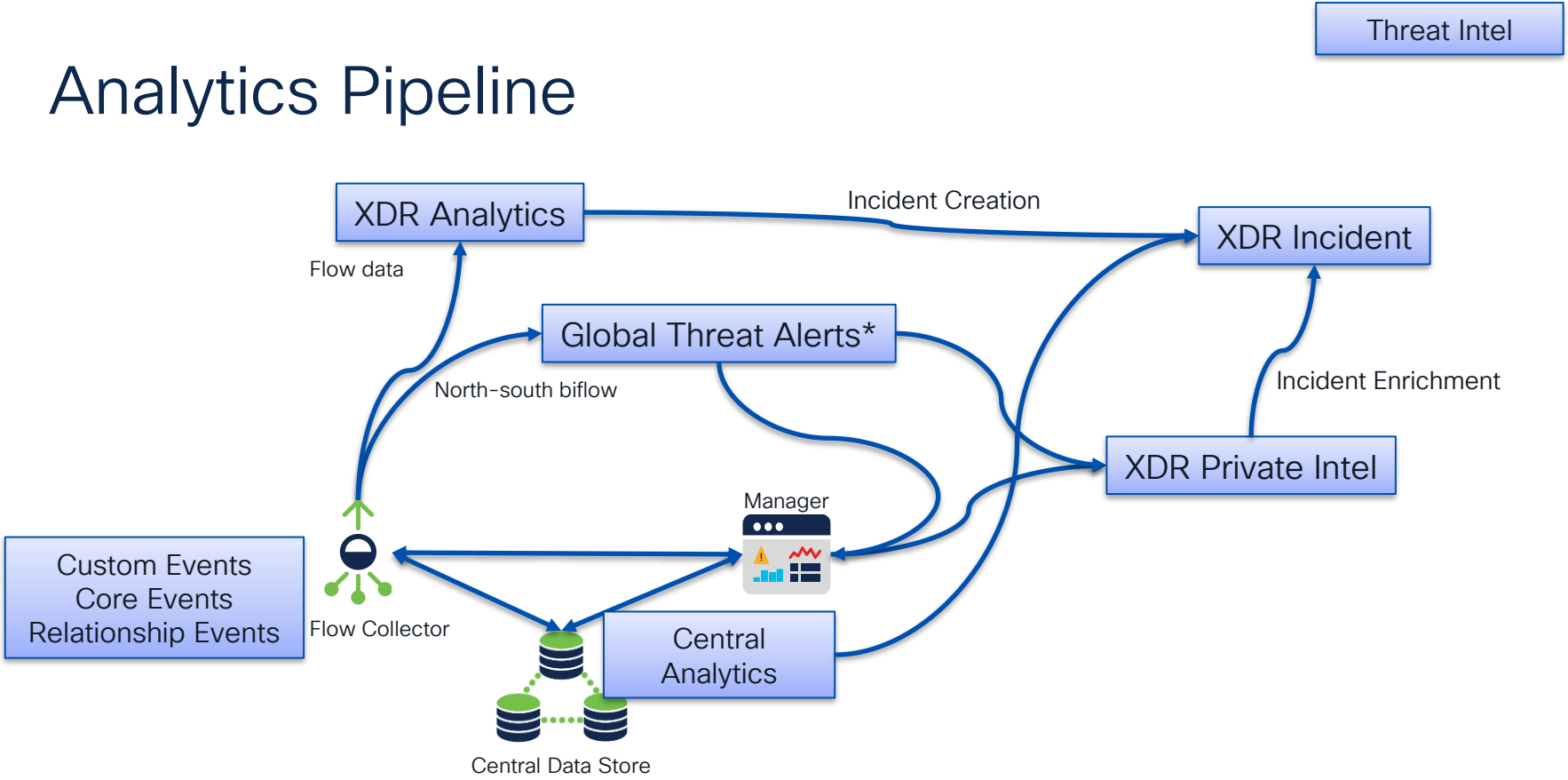
Global Threat Alerts (Cognitive Intelligence)

- Multi-layer Machine Learning
- Global malware campaign correlation to local incidents
- Merging into XDR Analytics

XDR Analytics

- Comprehensive entity modelling
- Detection and correlation across network, endpoint, email, Identity, IaaS data sets
- Attack Chaining
- XDR license required

Analytics Pipeline



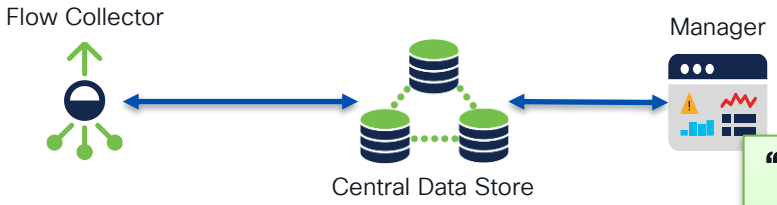
*GTA being decommissioned July 31, 2024

Central Analytics (on box)

Matt's Note:

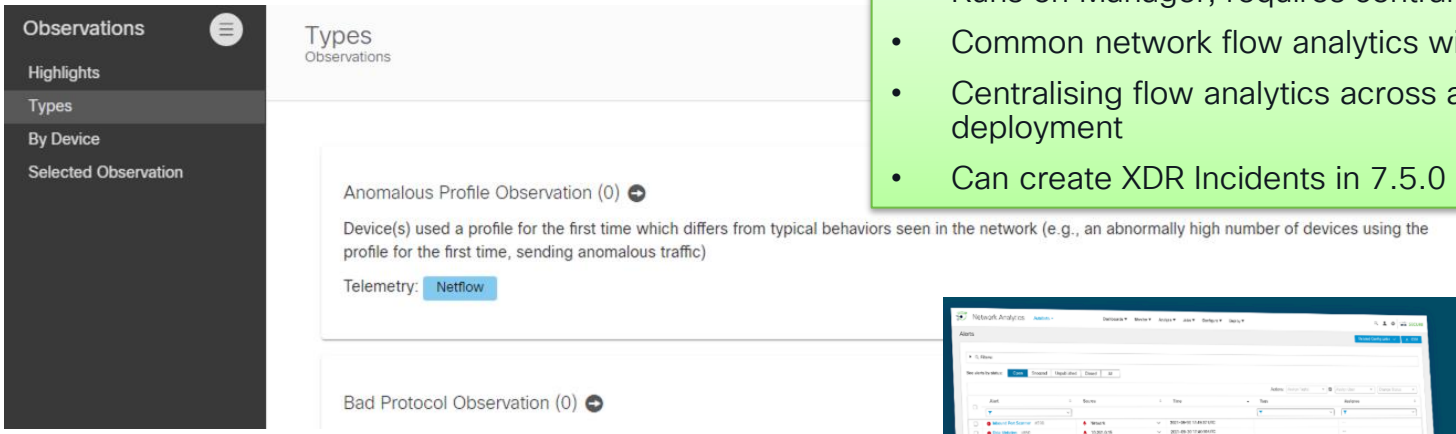
Minimal engineering required

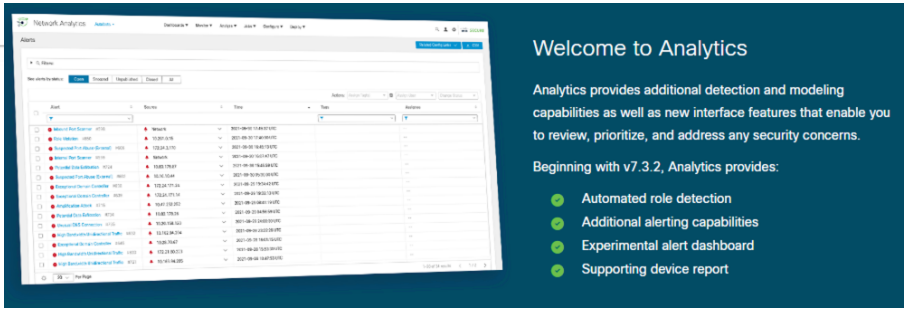
Simple out-of-box deployment



"Analytics" Node (New)

- Runs on Manager, requires central data store
- Common network flow analytics with XDR
- Centralising flow analytics across a multi-flow collector deployment
- Can create XDR Incidents in 7.5.0





Custom Security Events

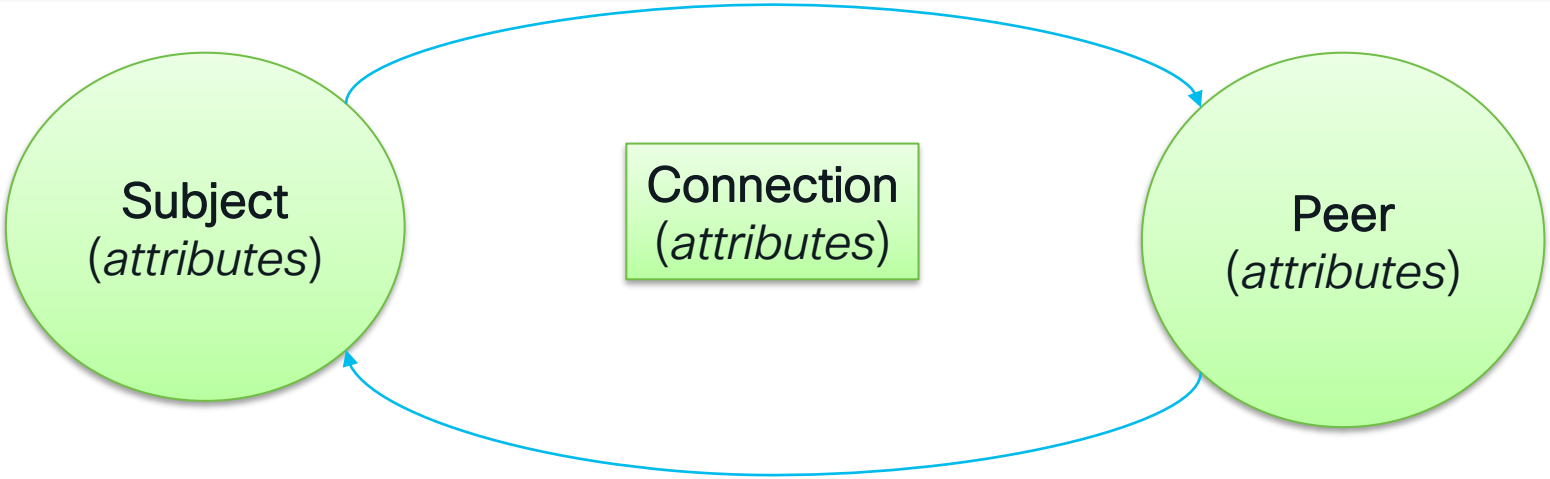
Matt's Note:

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

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 *

CSE: Employees to Canada

DESCRIPTION

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

STATUS

ON

FIND

SUBJECT TRUSTSEC ID: 4 AND

PEER HOST GROUP: Canada

+

ACTIONS

Alarm when a single flow matches this event.

Example CSE using Endpoint Attributes from CSC NVM Module

Policy Management | Custom Security Event

Cancel Save

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	--	--	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

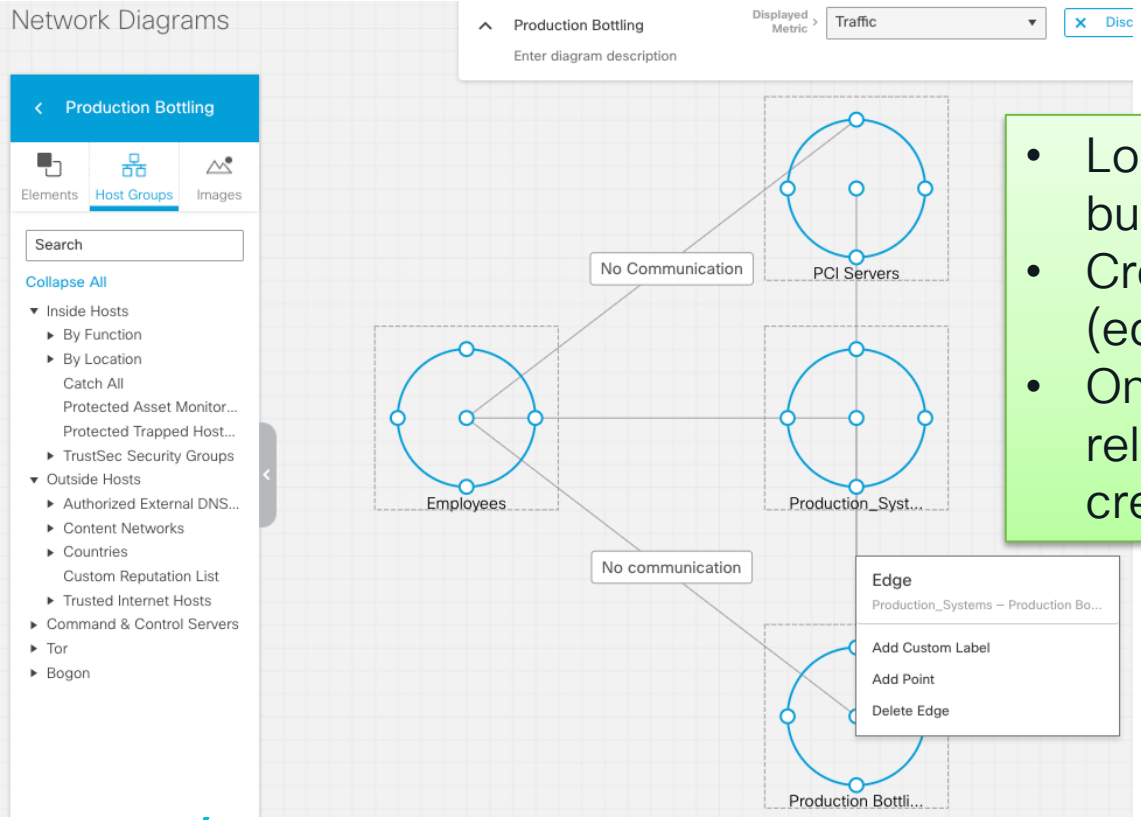
Tolerance 50 / 100

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

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

Policy Management | Relationship Policy

NAME *
Inside - Outside

DESCRIPTION

HOST GROUP - SIDE 1 *
Inside Hosts

HOST GROUP - SIDE 2 *
Outside Hosts

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	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

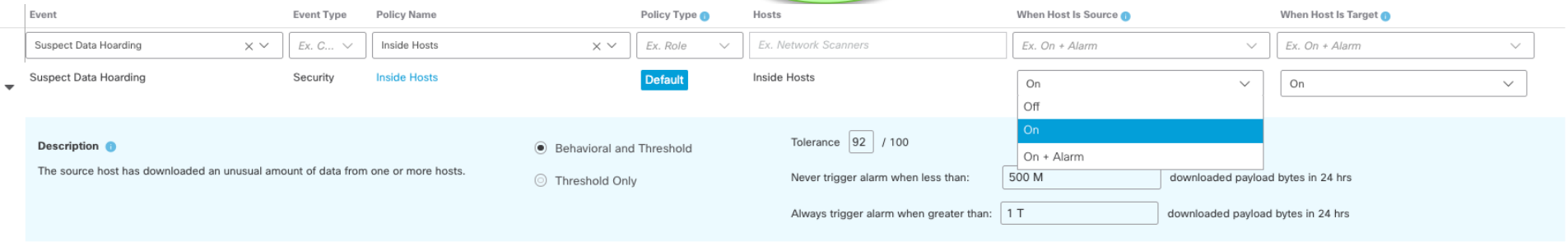
- Run on each flow collector
- 98+ tunable behavioural algorithms:
  - Statistical anomaly detection
  - Policy based detection

Entity
(IP Address, Host Group)

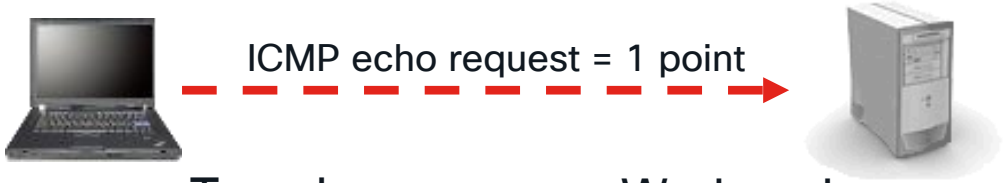
Matt's Note:

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: • 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.

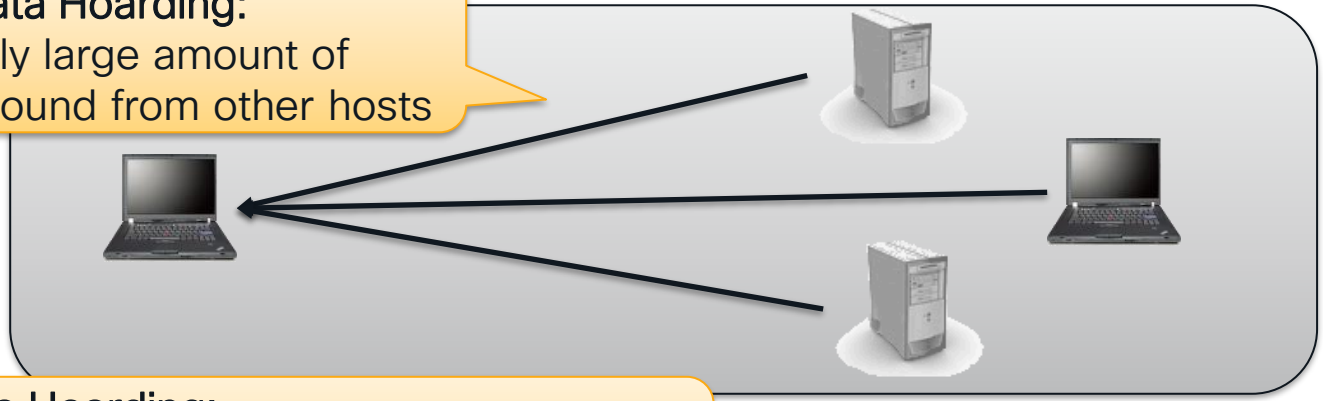
Note 1: Anomaly condition requires 7 days of traffic baseline in real life.

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

Example Algorithm: Data Hoarding

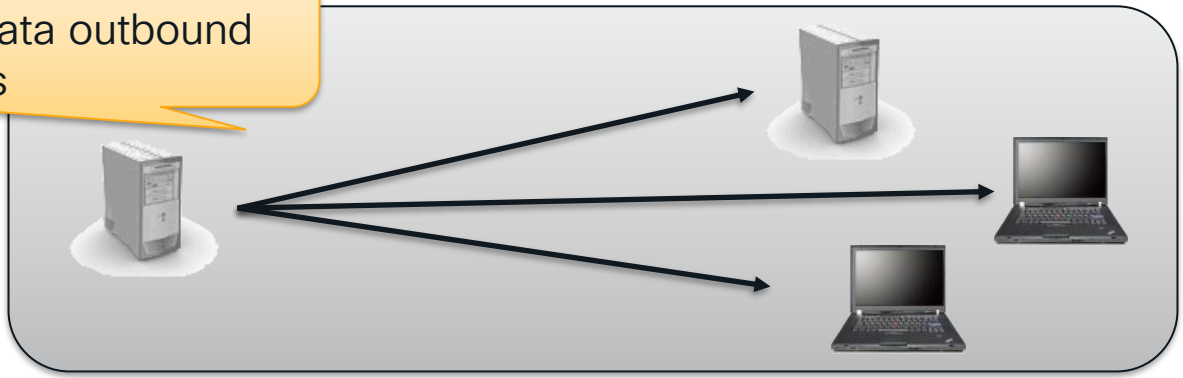
Suspect Data Hoarding:

- Unusually large amount of data inbound from other hosts



Target Data Hoarding:

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



Threat Intelligence Events

Matt's Note:

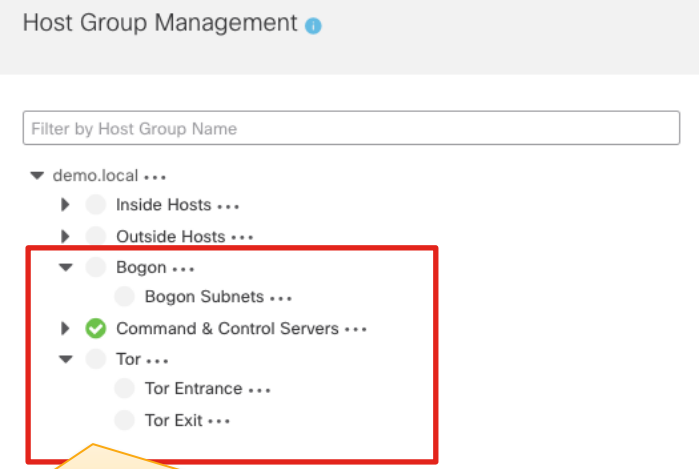
These are often immediately actionable events

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

i.e. detecting the unknown-knowns

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

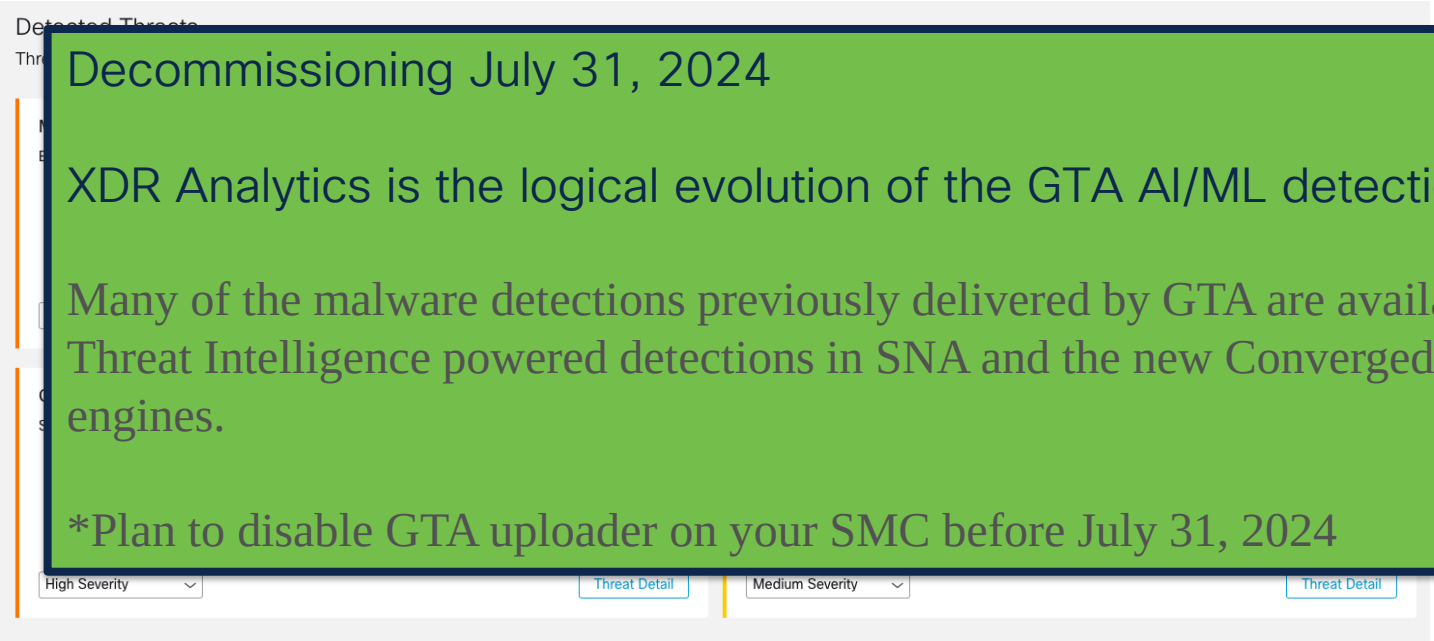
Last seen:	14 hours ago
Affected Assets:	5
Alerts:	3
Category:	Tool - anonymization

Medium Severity | Threat Detail

Global Threat Alerts (Cognitive Intelligence)

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

Global Threat Alerts



Decommissioning July 31, 2024

XDR Analytics is the logical evolution of the GTA AI/ML detection engines

Many of the malware detections previously delivered by GTA are available in the Threat Intelligence powered detections in SNA and the new Converged Analytics engines.

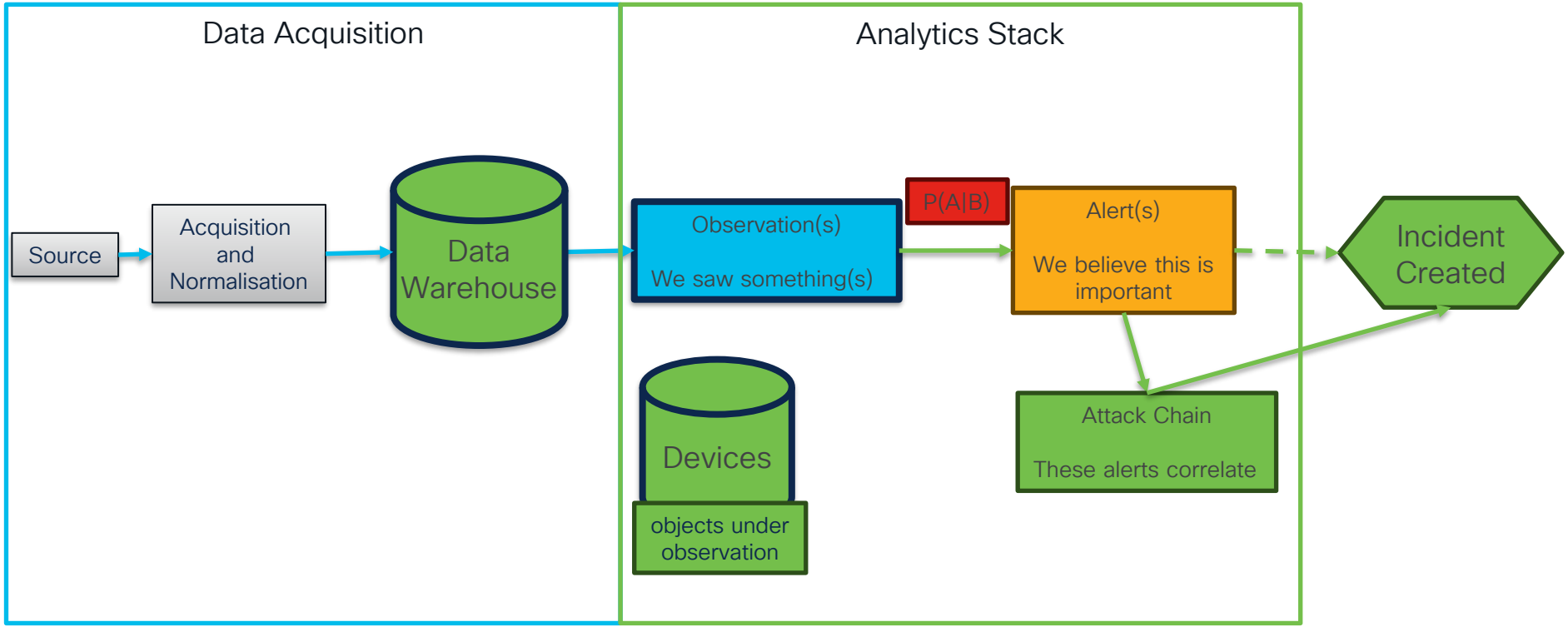
*Plan to disable GTA uploader on your SMC before July 31, 2024

Relevant CA Detections

Alert Type	Observation Types
	= Watchlist Interaction
Repeated Watchlist Communications Device has established periodic connections with any watchlisted IP (either in a user-defined or integrated watchlist). This alert uses the Watchlist Interaction and Heartbeat observations and may indicate a device is compromised.	• Heartbeat • Watchlist Interaction
Suspected Botnet Interaction Device exchanged traffic with IP addresses associated with botnets or attempted to resolve domain names associated with botnets using an integrated watchlist. This alert uses the Watchlist Interaction observation and may indicate a device is compromised.	• Watchlist Interaction
Suspected Cryptocurrency Activity Device exchanged a significant amount of traffic with multiple addresses known to be operating cryptocurrency nodes. This alert uses the Watchlist Interaction observation.	• Watchlist Interaction
Talos Intelligence Watchlist Hits Device exchanged a significant amount of traffic with multiple addresses on the integrated Cisco Talos IP Watchlist. This alert uses the Watchlist Interaction observation.	• Watchlist Interaction
Unusual External Server Device has repeatedly communicated with a new external server. This alert uses the New External Server and Persistent External Server observations and may indicate the presence of malware.	• New External Server • Persistent External Server • Watchlist Interaction

BRKSEC-2178 – Extended Detection with Cisco XDR
- Matt Robertson, Tuesday Feb 6 @ 2:00pm

XDR Analytics Pipeline



Attack Chaining

Automatic correlation of related alerts

Alert Chain at a Glance

Created 2022-12-04 21:25:13 PST
Last Active 2023-02-06 01:00:00 PST
Alert Chain ID a53120a5104128eb865d476d0a8056e7396d252e
Status Open

Chaining Patterns Impact Persistence Command And Control (2) (more)
Post an Incident Post to SecureX Incident Manager
Common Indicators 10.160.160.100 10.90.90.201

sociated Devices	Total Active Days	Unique Alerts	Total Alerts	MITRE ATT&CK
	63	5	5	4 TACTICS 4 TECHNIQUES

ne Connection Graph Devices & Roles All Hosts

Zoom 1m 3m 6m YTD 1y All
4-Dec-2022 → 6-Feb-2023

Distinct Alert Types / MITRE Tactic	2022 December	2023 January	2023 February
IDS Notice Spike #1216 Impact			
Internal Connection Watchlist Hit #1312 Persistence			
User Watchlist Hit #1314 Command And Control			
Watchlist Hit #1345 Command And Control			
Metasploit Executed #1411 Execution			Created: 2023-02-01 10:05

12. Dec 19. Dec 26. Dec 2. Jan 9. Jan 16. Jan 23. Jan 30. Jan

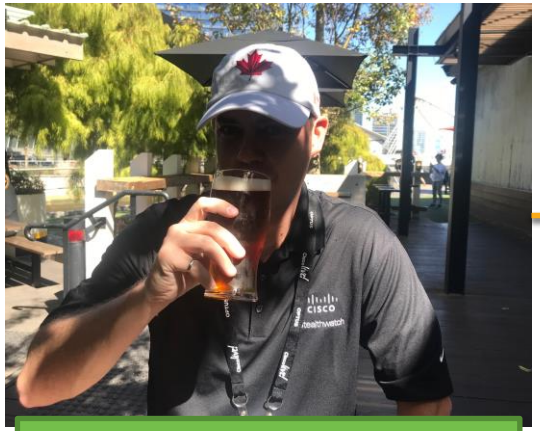
Correlation on:

- Devices
- IP Addresses
- Usernames

Timeline view of alert types

Detection Engineering with SNA

The Thing about Behaviour



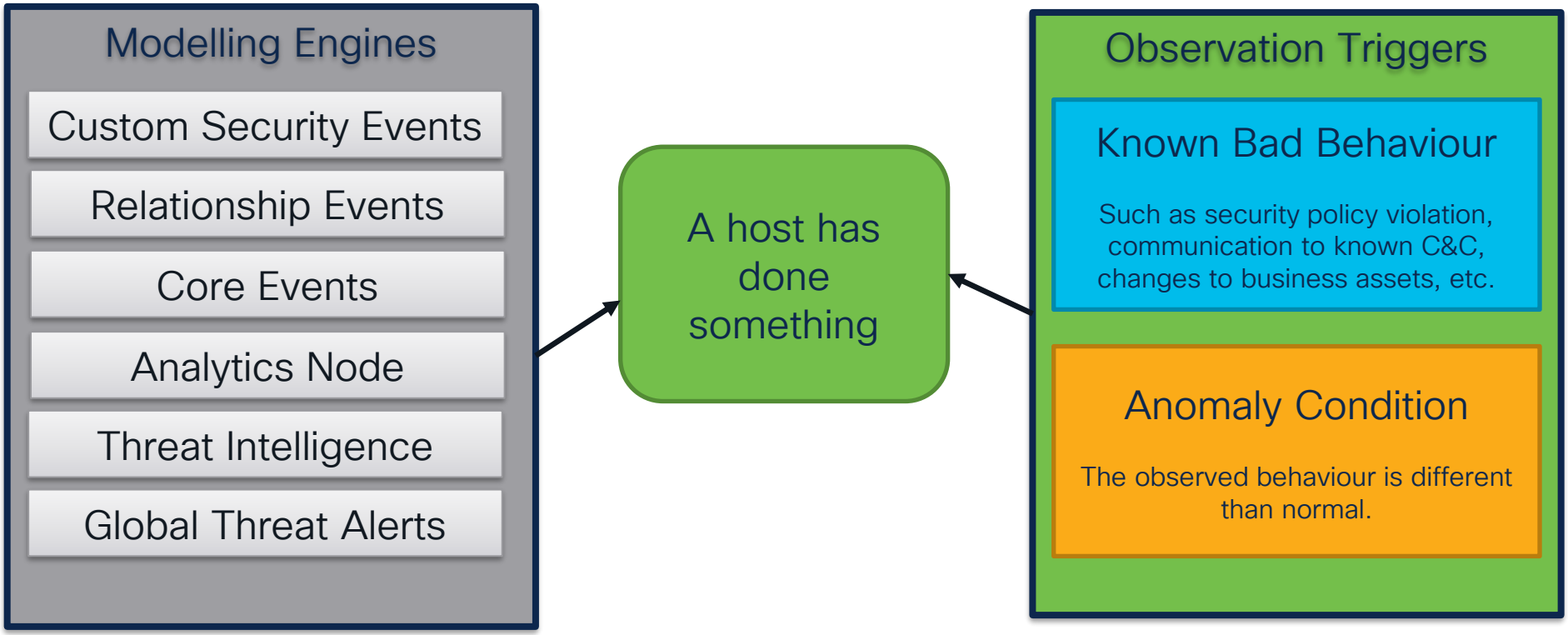
Observation:
This man drinks beer

There exist conditions that make the observation malicious

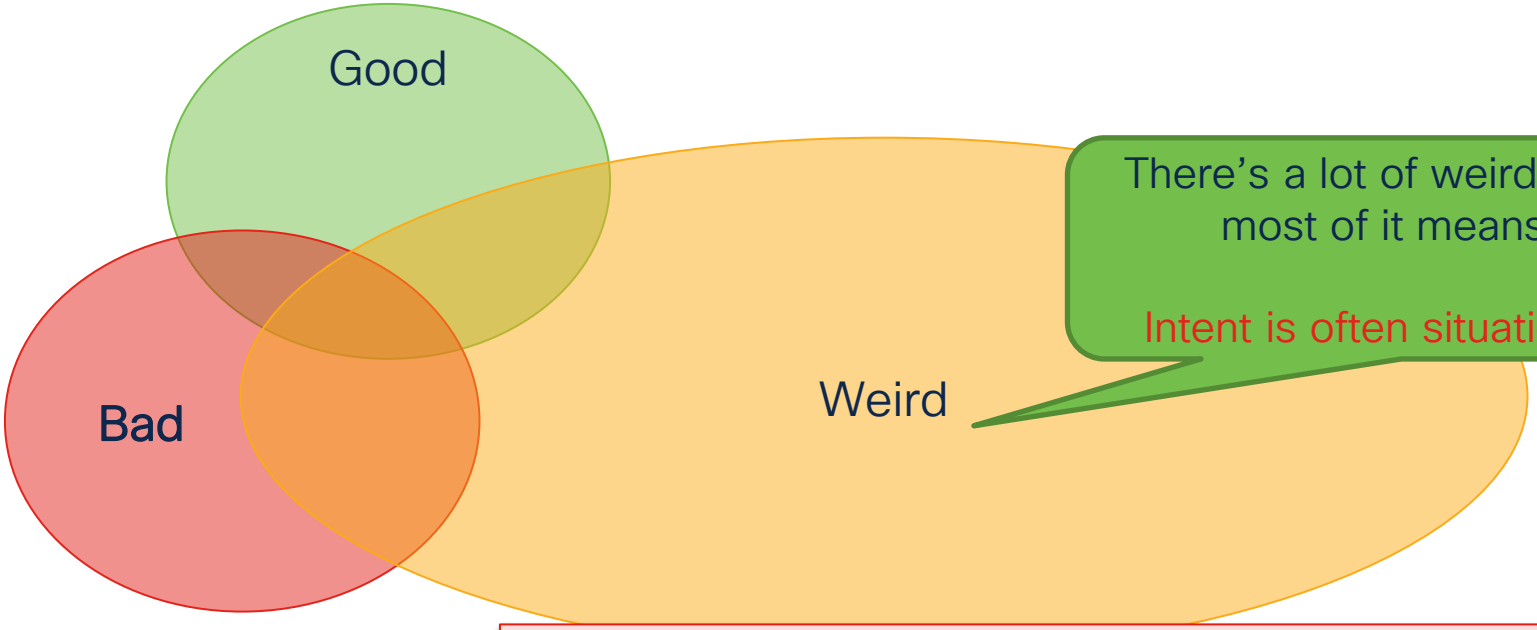
Some observations are just "different than normal"

Key Idea:
Behaviour events are an observation

Behaviour events are an observation



The Thing about Behaviour

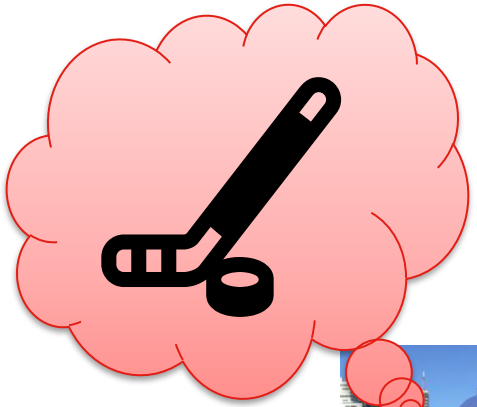


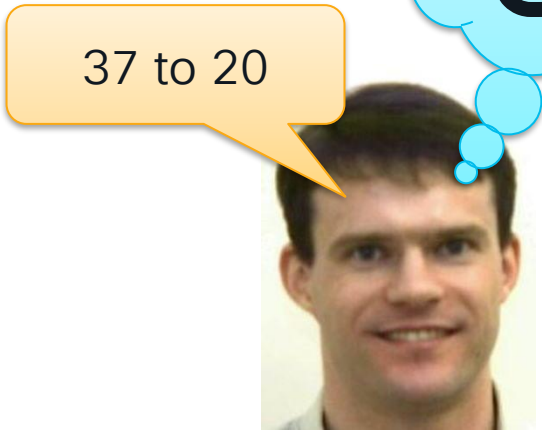
There's a lot of weird out there and most of it means nothing.

Intent is often situational specific.

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

Detection Engineering: Concept

Create detections for the edge cases not covered by your vendor's built-in detection logic

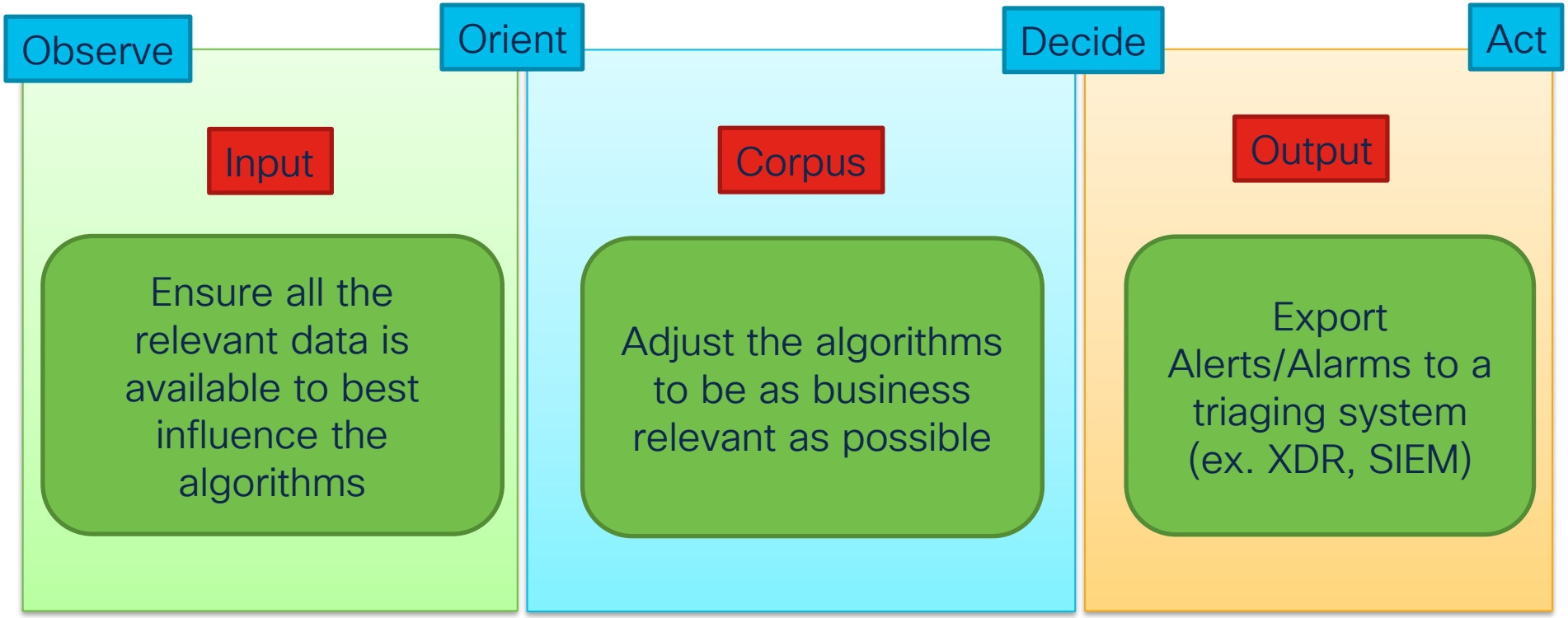
Identify Detection Requirements <Tactic, Technique>

Identify Data/tools Required

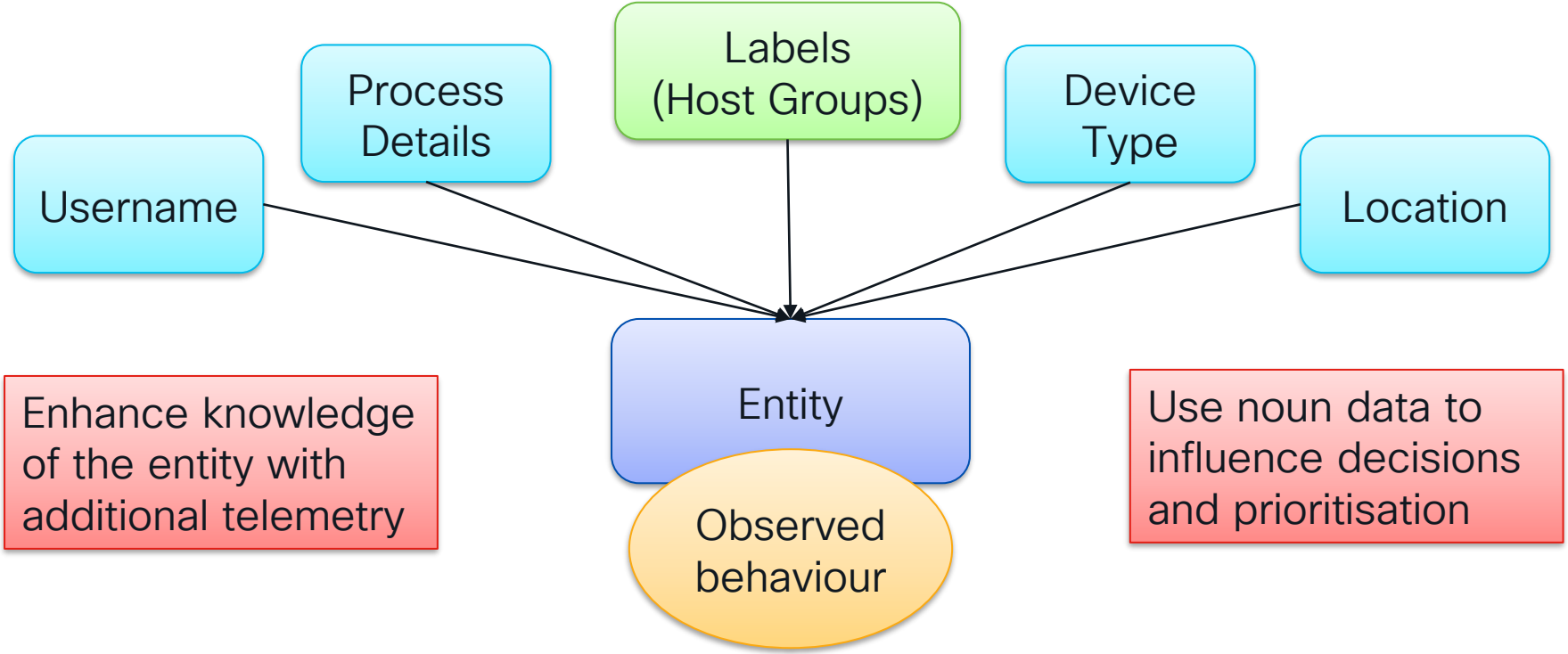
Define/write Detection Logic

Evaluate Detection

Detection Engineering with SNA



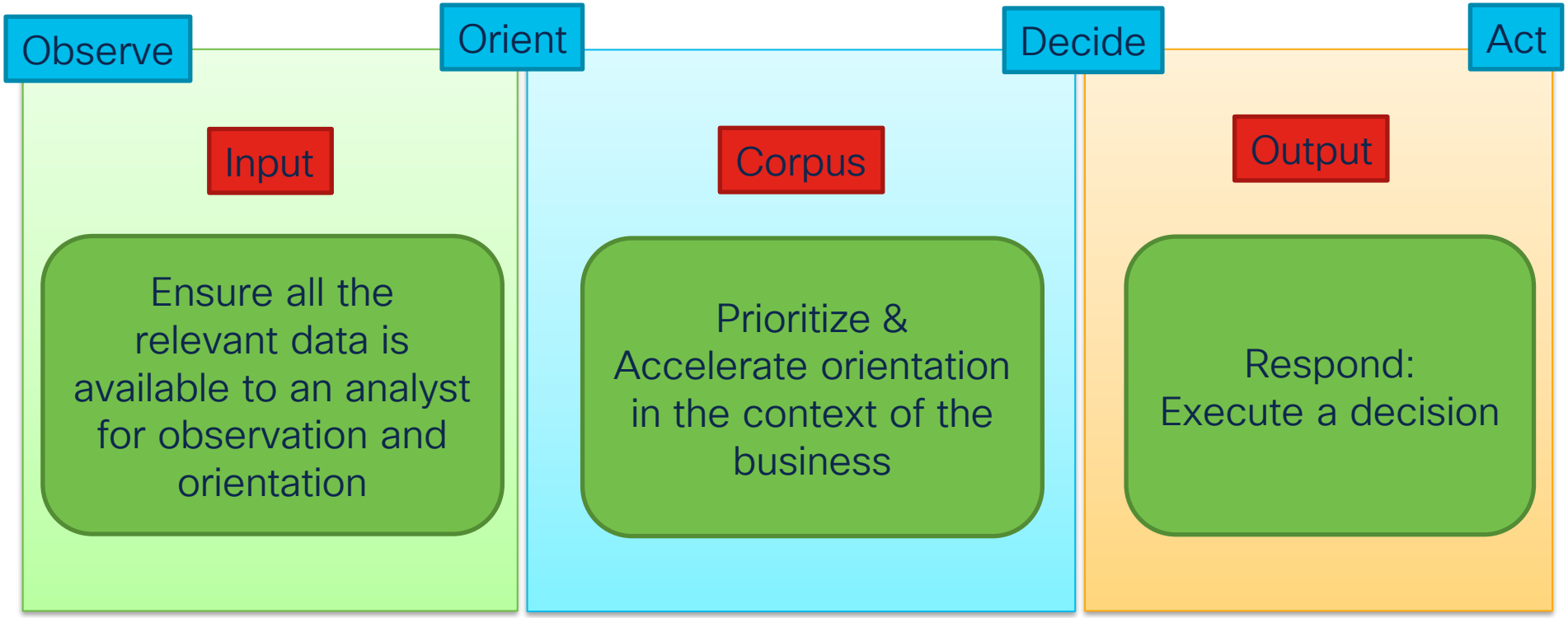
Input: Enhance the Detection



Enhance knowledge of the entity with additional telemetry

Use noun data to influence decisions and prioritisation

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

Detection Engineering with SNA

Greenfield 7.5.0 with datastore deployment

Step 0: Turn everything off
- Disable all default alarm/alert settings
  - Viable approach if you have clearly defined objectives

Step 1: Enable Central Analytics
- Quickest path to useful alerts/observations with no engineering

Step 2: Develop Custom Security Events
- High fidelity, policy driven monitoring
- May require some Host Group configuration

Step 3: Enable Core Engine
- Host Groups & tuning guidelines
- Objectives and creativity required

Step 4: Create relationship events
- Leverage host groups and network diagrams

Enable XDR:
- Enhance XDR with Network telemetry & insights

Aside: Disabling Everything 7.5.0

Manually change Core Events set to “On+Alarm” to either “On” or “Off”

Policy Management

Search for a host or select a host group | Search

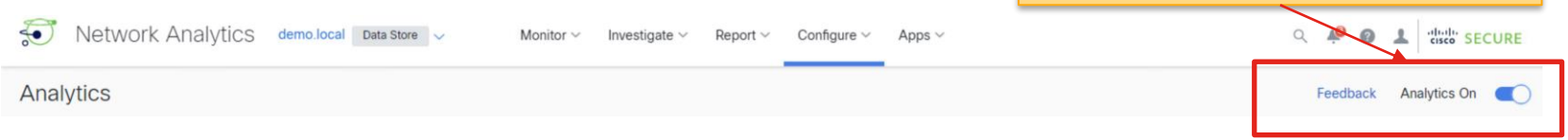
Custom Events (6) | Relationship Events (352) | Core Events (91) | Create New Policy

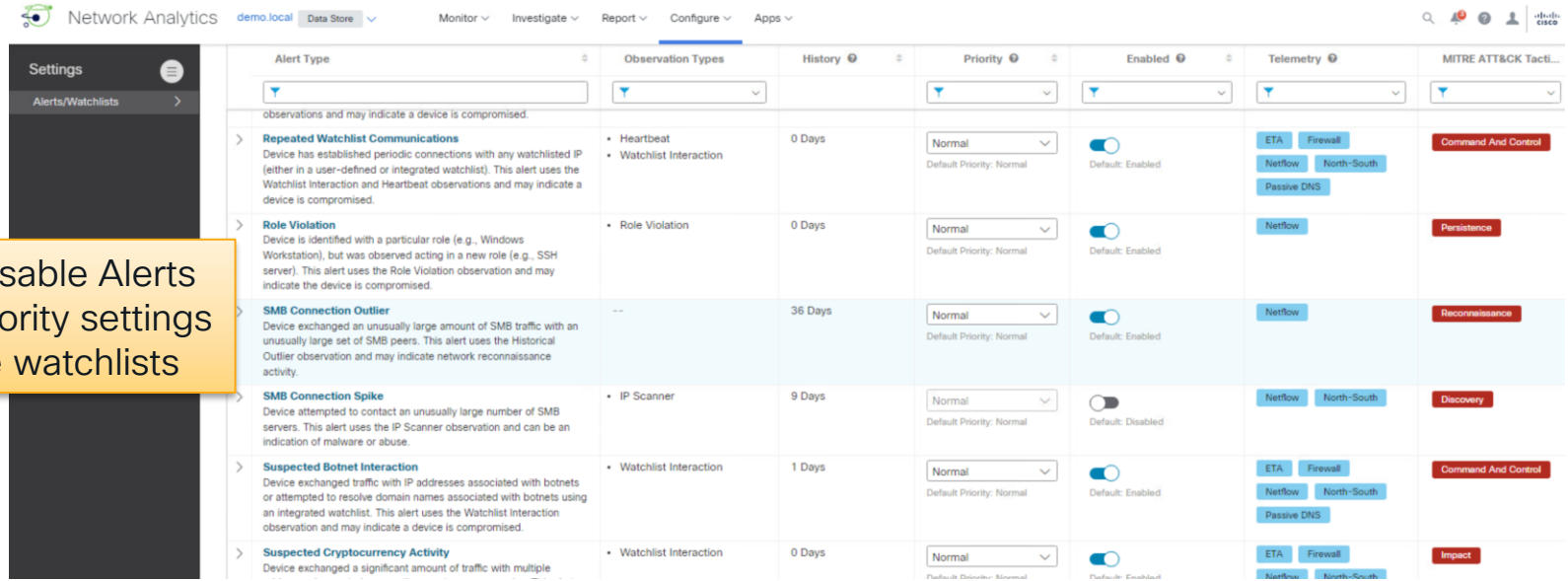
Event	Event Type	Policy Name	Policy Type	Hosts	When Host Is Source	When Host Is Target
Ex. Anomaly	Ex. Cat...	Ex. Outside Hosts	Ex. Role	Ex. Network Scanners	On + Alarm	Ex. On + Alarm
Addr_Scan/tcp	Security	Policy for Testing Security Events	Role	--	On + Alarm	On
Addr_Scan/udp	Security	Policy for Testing Security Events	Role	--	On + Alarm	On
Anomaly	Category	Outside Hosts	Default	Outside Hosts	On + Alarm	NA

“Alarm” is a notification setting
Algorithms will run against a host if set to “On”

Enable Central Analytics

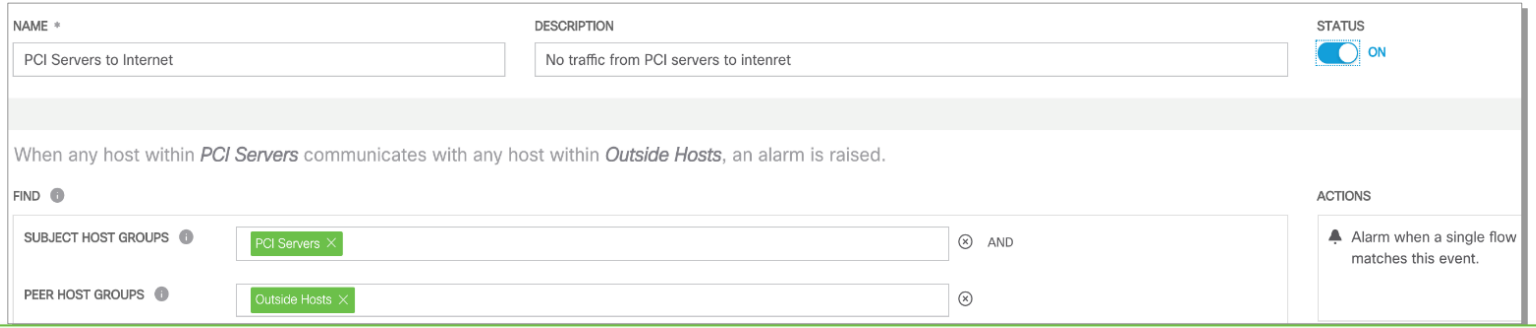
Turn it on: CA is off by default





- Enable/Disable Alerts
- Adjust priority settings
- Configure watchlists

Enable Custom Security Events



Tips for Building CSEs:

- Start with your critical assets
- Consider technical and administrative controls
- Model around the actual expected behavior
  - Segmentation policy, unauthorized traffic flows, security compliance, etc.
- Run a flow search first to avoid floods
- Start the name with “CSE:” or “.CSE:”
- Include a good description

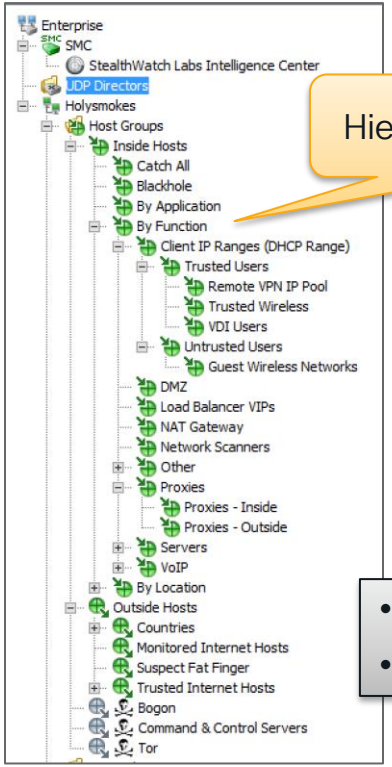
Enable Core Events

Detection Engineering at its finest

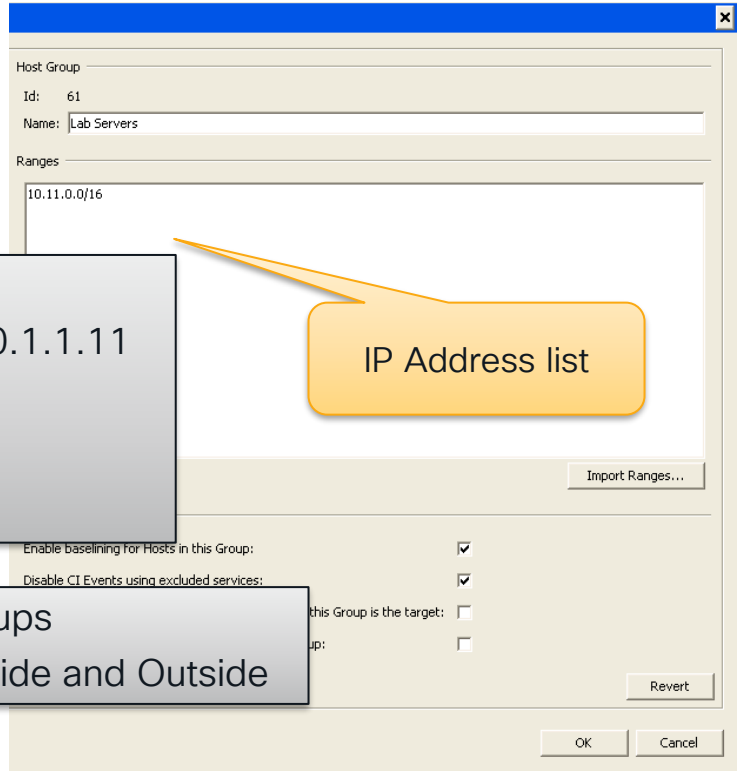
General Guidance:

- Define objectives
  - Ex. What do you want to detect?
- Use role-based functional logic
- Don't do everything at once
  - Ex. Choose a particular entity to monitor first
    - Ex. Domain Controller
- Create meaningful policies, used Tiered alarm framework
- Expect Alarms to be operationalised by SOC in a different UI
  - Ex. XDR, SIEM

Host Groups: Logical Labels on IP Space



Hierarchical structure



IP Address list

Examples:

- DNS Servers are 10.1.1.10 and 10.1.1.11
- All POSs are 10.20.20.0/24
- HQ is 10.0.0.0/8
- Etc.

- A host can exist in multiple Host Groups
- A Host can not be simultaneously Inside and Outside

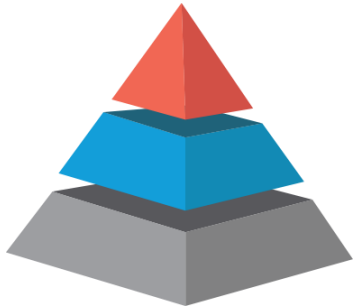
Host groups become basic building blocks for role-based detection engineering

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/

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	On

On
Off
On
On + Alarm

Description

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

Behavioral and Threshold

Threshold Only

Tolerance 92 / 100

Never trigger alarm when less than: 500 M downloaded payload bytes in 24 hrs

Always trigger alarm when greater than: 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

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

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

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

Cancel Save

Actions

Name *
Exclude DNS Servers

Description
Exclude traffic events for DNS servers

Host Groups
Authorized External DNS Servers DNS Servers

IP Address Or Range

Core Events (2)

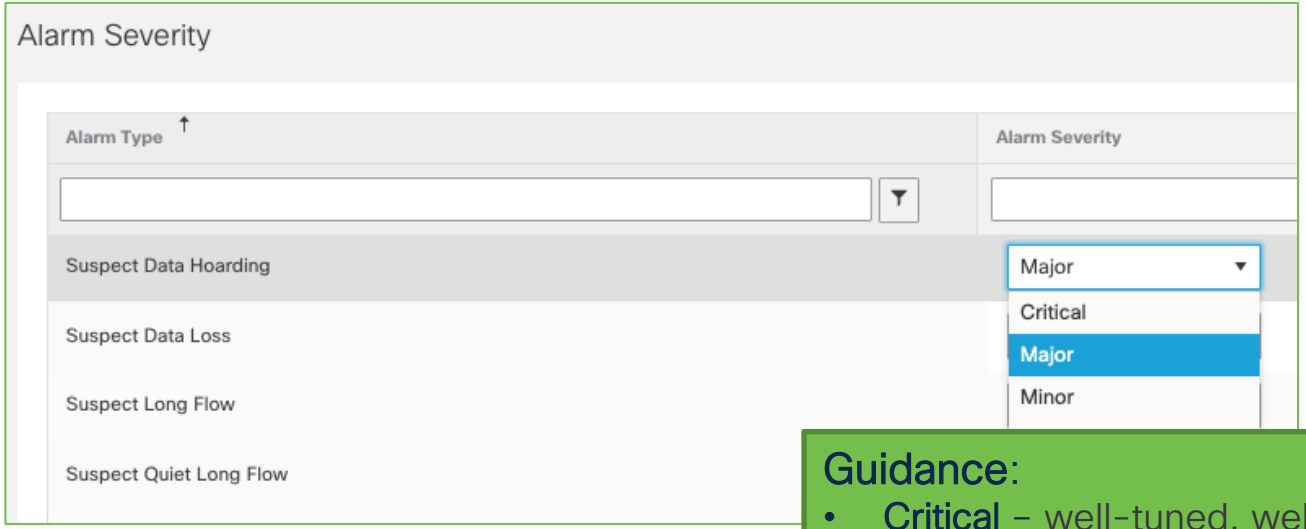
Select Events

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

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

Define Alarming Conditions

- Algorithm triggers are simply observations
- Alarming conditions indicate notification

Rules | Actions | Syslog Formats

Rules | Host Alarm

Cancel | Save

Name: Priority A: Severity Critical

Description: These are well-tuned, well-understood, and typically low-volume alarms. The chance of a false positive is generally quite low. Security teams should know what actions to take for

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

Rule is triggered if:

ALL of the following is true:

Severity is Critical or higher

Adjust alarm trigger conditions to ensure notification of only the things of import

Note: SNA alarms have a flat alarming structure; consider using an external system for additional prioritisation (ex. XDR, SIEM)

E2E Detection Engineering Example

Potential DCSync detection with Secure Network Analytics

1. Populate Domain Controller Host Group
2. Create Custom Security Events for terminal sessions
3. Create role policy for abnormal data movements
4. Create specific alarming conditions for DCSync

Example CSE for DCSync

Policy Management | Custom Security Event

Name *
Potential Credential Dumping event

Description
Remote terminal connection to Domain Controller

When any host within ***Inside Hosts*** communicates with any host within ***Domain Controllers***; through ***3389/tcp***, an alarm is raised.

Find

Subject Host Groups	Inside Hosts	AND
Peer Host Groups	Domain Controllers	AND
Peer Port/Protocols	3389/tcp	

Note: This is not a guarantee that it will work in all environments

Example Role Policy for DCSync

Name *
Domain Controller: Monitor for Credential Dumping Attacks

Description

Host Groups
Domain Controllers

IP Address Or Range

Core Events (3)

Select Events

Event	Event Type	When Host Is Source	When Host Is Target	Actions
Ex. Anomaly	Ex. Category	Ex. On + Alarm	Ex. On + Alarm	
Data Exfiltration	Category	On + Alarm	NA	Delete
Data Hoarding	Category	On + Alarm	NA	Delete
High Concern Index	Category	On + Alarm	NA	Delete

1 / 1 50 items per page

1 - 3 of 3 items

Note: This is not a guarantee that it will work in all environments

Example Alarming rule for DCSync

Rules | Host Alarm

Cancel Save

Name

Potential DCSync Attack

Description

Significant data loss from Domain Controllers; potentially indicating credential dumping attacks such as DCSync.

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

Rule is triggered if:

ALL of the following is true:

Host Group of Source Host is Domain Controllers

Type is Suspect Data Loss

Note: This is not a guarantee that it will work in all environments

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.	ON	•••
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.	OFF	•••
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.	OFF	•••
CTA	Host Alarm		ON	•••

- 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

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

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	•••

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.	ON	•••
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.	OFF	•••
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.	OFF	•••
CTA	Host Alarm		ON	•••

- 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

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

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	OFF	•••

Remediating Action with ISE

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

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.lcoal (demo.local)

ANC Policy: Quarantine_Host

Apply To: Source Host | Target Host

2. Define a response Rule that invokes the defined Action

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	

Demo

Summary

Related Sessions

XDR Learning Map:
https://www.ciscolive.com/emea/learn/technical-education/learning-maps/security/xdr.html

Session ID	Title	When
BRKSEC-2178	Extended Detection with Cisco XDR: Security Analytics across the enterprise	Thursday 4:45 PM
BRKSEC-2248	Design, Deploy and Troubleshoot Network Detection and Response	Friday 11:00 AM
BRKSEC-2227	Evaluating and Improving Defenses with MITRE ATT&CK	Thursday 4:30 PM

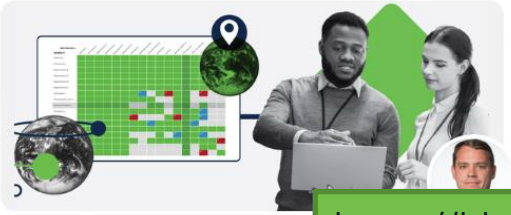
Reading: TrustSec Policy Analytics Blog Series

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

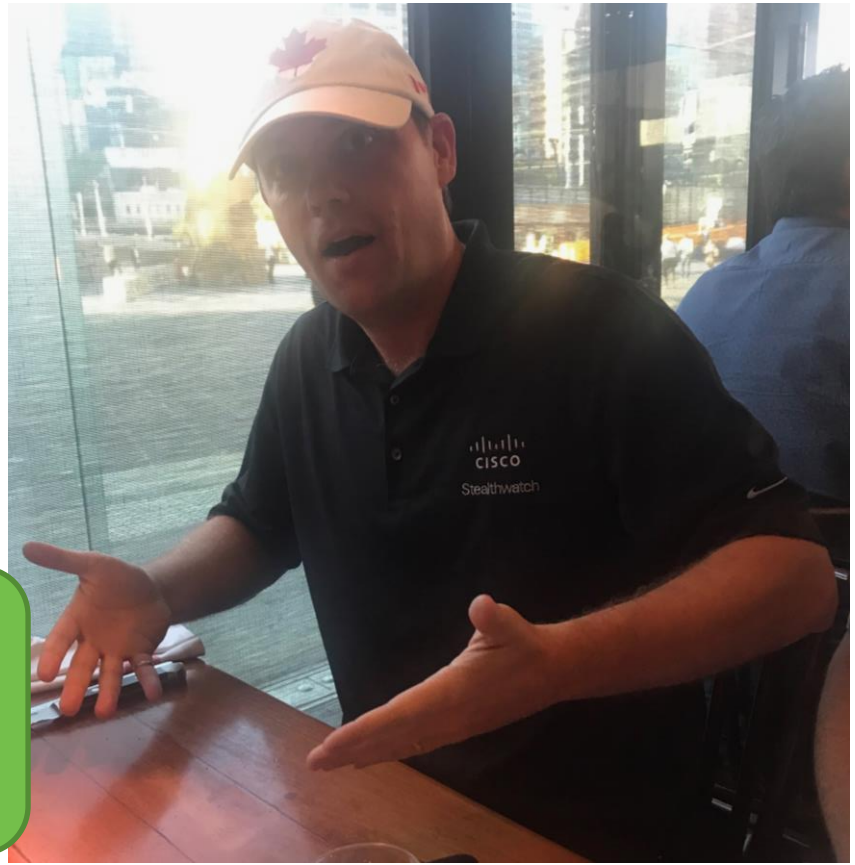
Parting Thoughts

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

Cisco XDR

Secure Network Analytics

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



The bridge to possible

Thank you

cisco Live!

cisco Live!

Let's go