cisco
You make possible

Security Analytics with Stealthwatch

Operationalising Visibility and Machine Learning

Matt Robertson, Principal Engineer
@mattrobertson25

BRKSEC-3014

cisco Live!
Barcelona | January 27-31, 2020

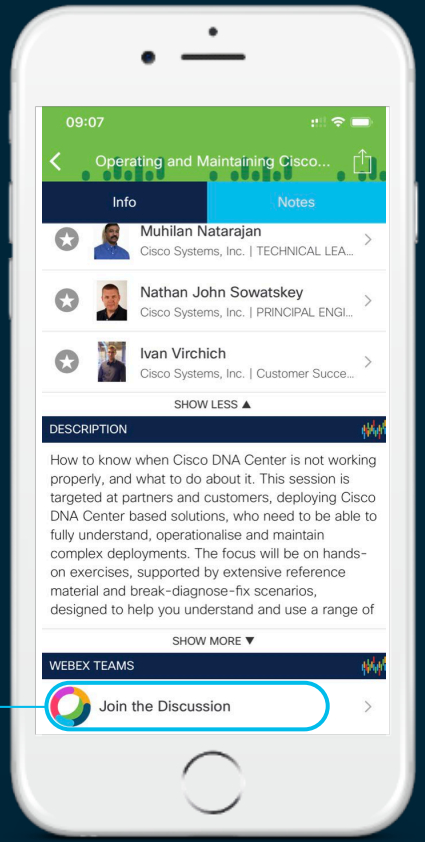
Cisco Webex Teams

Questions?

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

How

1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

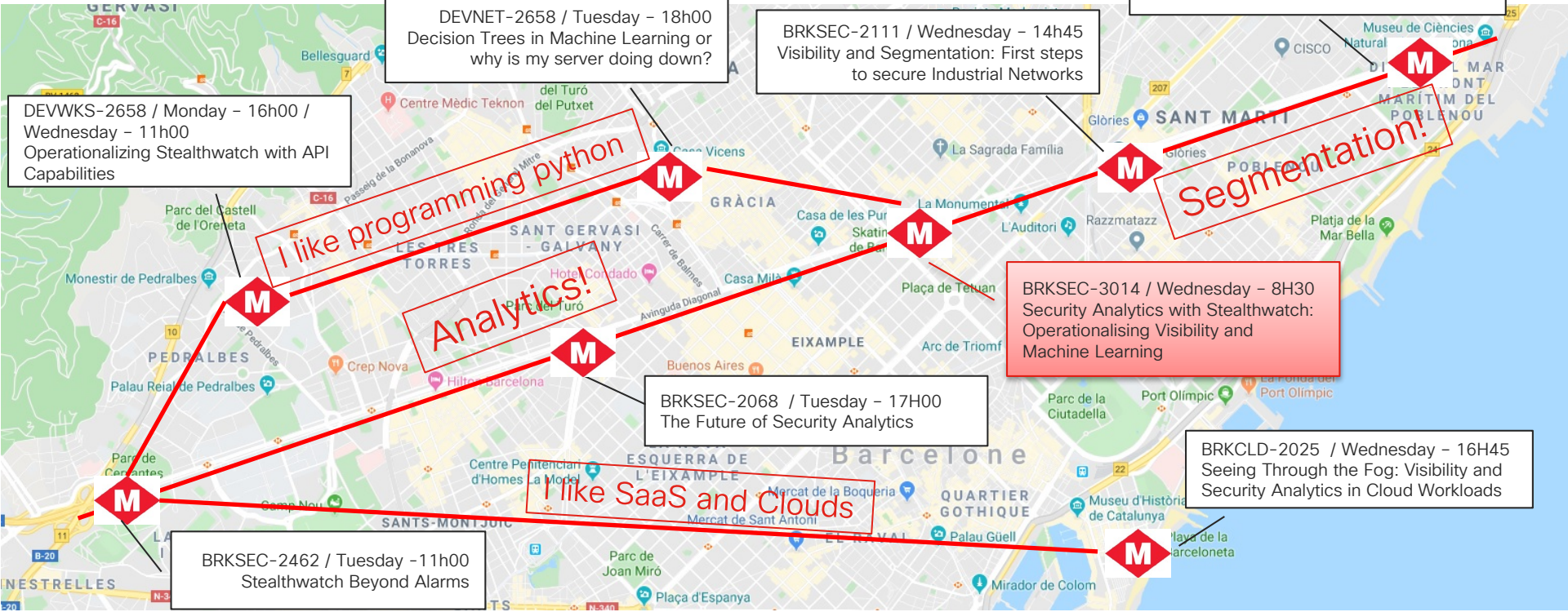
About this Session: Operationalizing Stealthwatch

Operationalizing visibility:
- Understanding the data
- Generating outcomes

Operationalizing security analytics:
- How Stealthwatch analytics work
- Making them relevant and actionable

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Security Analytics Learning Map



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

- Introduction
- Enabling Visibility and Analytics with Telemetry
- Understanding Security Analytics
- Operationalising Stealthwatch Analytic Engines
- Investigating an Alarm
- Summary

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

About Me

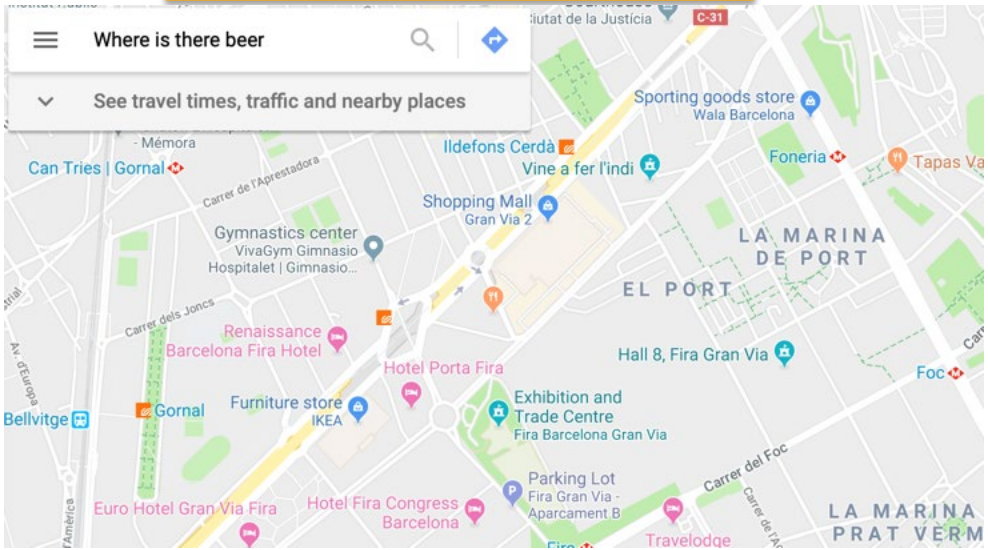
Matt Robertson

- Principal Technical Marketing Engineer
- Security Analytics and Advanced Threat
- Cisco Live Distinguished Speaker
- 11.5 years at Cisco: Development, TME, Lancope
- Canadian eh
- Known beer hoser: http://www.beerhoser.ca

cisco Live!

Before we Begin....

Operationalising Visibility



Operationalising Analytics

Empowering Security Operations

Automating Security Operations

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

- Introduction
- Enabling Visibility and Analytics with Telemetry

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Stealthwatch System

Stealthwatch is a collector and aggregator of telemetry for the purposes of security analysis and monitoring

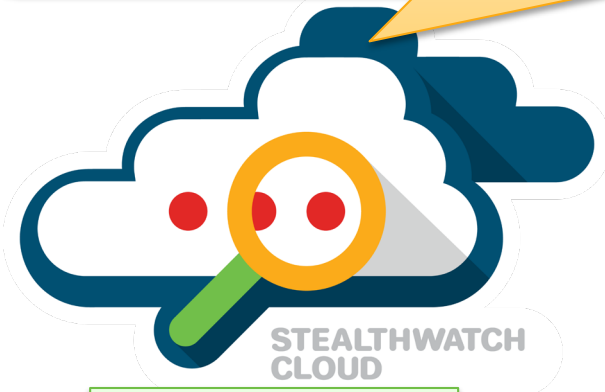
Stealthwatch Enterprise

- On-premises appliances
- On-premises telemetry collection, storage and analytics
- (Optional) Cloud Analytics Engine

Focus of this Session

Stealthwatch Cloud

- Cloud hosted (SaaS) telemetry collection, storage and analytics
- Public cloud (IaaS) monitoring
- On-prem visibility and analytics



BRKCLD-2025

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Stealthwatch Value Use Case Menu

This limited collection of use cases highlights the capabilities of Stealthwatch

Threat Detection

- Detecting Beaconing
- Detecting Bogon Traffic
- Detecting Command and Control Traffic Using the Threat Intelligence License
- Detecting Fake Applications
- Detecting Fileless Malware—PowerShell Attacks
- Detecting Internal Brute Force Attacks
- Detecting Lateral Movement
- Detecting Man in the Middle Attacks
- Detecting Password Spray Attacks
- Detecting Rogue DHCP Servers
- Detecting Tor Traffic
- Detecting Rogue DNS Traffic
- Detecting Fragmentation Attacks
- Detecting Targeted Attacks
- Detecting ATM Attacks
- Detecting WannaCry Malware
- Reducing Mean Time To Know
- Detecting Browser-Based Attacks
- Detecting Cryptomining Attacks
- Using Cognitive Intelligence
- Using Cognitive Intelligence and AMP for Network Security
- Detecting Malware in Encrypted Traffic

Compliance

- Identifying Medical Asset Types on the Network
- Managing Stealthwatch Users
- Monitoring Trusted Third Parties
- Using Bi-Directional Policies
- Using the ETA Cryptographic Audit Application
- Using the Visibility Assessment Application
- Verifying Change Control Management
- Detecting Obsolete Encryption Protocols
- Detecting Insecure Protocols
- Detecting Torrent or File Sharing Traffic
- Monitoring Vendor Activity
- Monitoring High Priority Host Groups
- Detecting Fake Applications
- Detecting Rogue and New Devices
- Defining Business Applications
- Detecting Application Access Policy Violation
- Identifying Applications on the Network
- Monitoring Remote Access Users
- Using Custom Security Events to Monitor Firewalls
- Using Encryption Auditing

Incident Response

- Determining if a User Violated Access Policies
- Detecting Users Not Traversing the Web Proxy
- Detecting Unauthorized Hosts in a Bypass VLAN
- Determining if Internet Hosts are Connecting to Internal Servers
- Monitoring Corporate Email
- Using the SMC Web UI for Threat Investigation
- Detecting Top Alarming Hosts on the Network

Network Visibility

- Identifying a Virtual Machine Generating Excessive Traffic
- Investigating NTP Reflection DDoS
- Investigating Unidirectional Traffic
- Using the Host Classifier Application
- Using the Interface Status Report in the SMC Web UI for Network Operations
- Using the SMC Web UI for Network Usage Accounting
- Using Stealthwatch for Network Segmentation and Policy Development

Stealthwatch Cloud

- Investigating IP and Port Scans Using Stealthwatch Cloud
- Investigating Potential Data Exfiltration Using Stealthwatch Cloud
- Investigating Potential Threats Using Stealthwatch Cloud
- Monitoring Cloud Resources Using Stealthwatch Cloud
- Detecting Endpoint Deviations Using Stealthwatch Cloud

Forensic Investigation

- Reporting Internet URL Access
- Using the Interface Status Report for Security Operations
- Using the Security Event Workflow
- Using Top Reports
- Obtaining Historical Conversations for Unauthorized Data Transfer

Alarm Categories

- Alarm Category: Command and Control
- Alarm Category: Anomaly
- Alarm Category: Recon
- Alarm Category: High Concern and High Target Index
- Alarm Category: Data Exfiltration
- Alarm Category: Policy Violation
- Alarm Category: Data Hoarding
- Alarm Category: DDoS
- Alarm Category: Exploitation

© 2018 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.

Stealthwatch:
A use case approach to solving crucial network security gaps

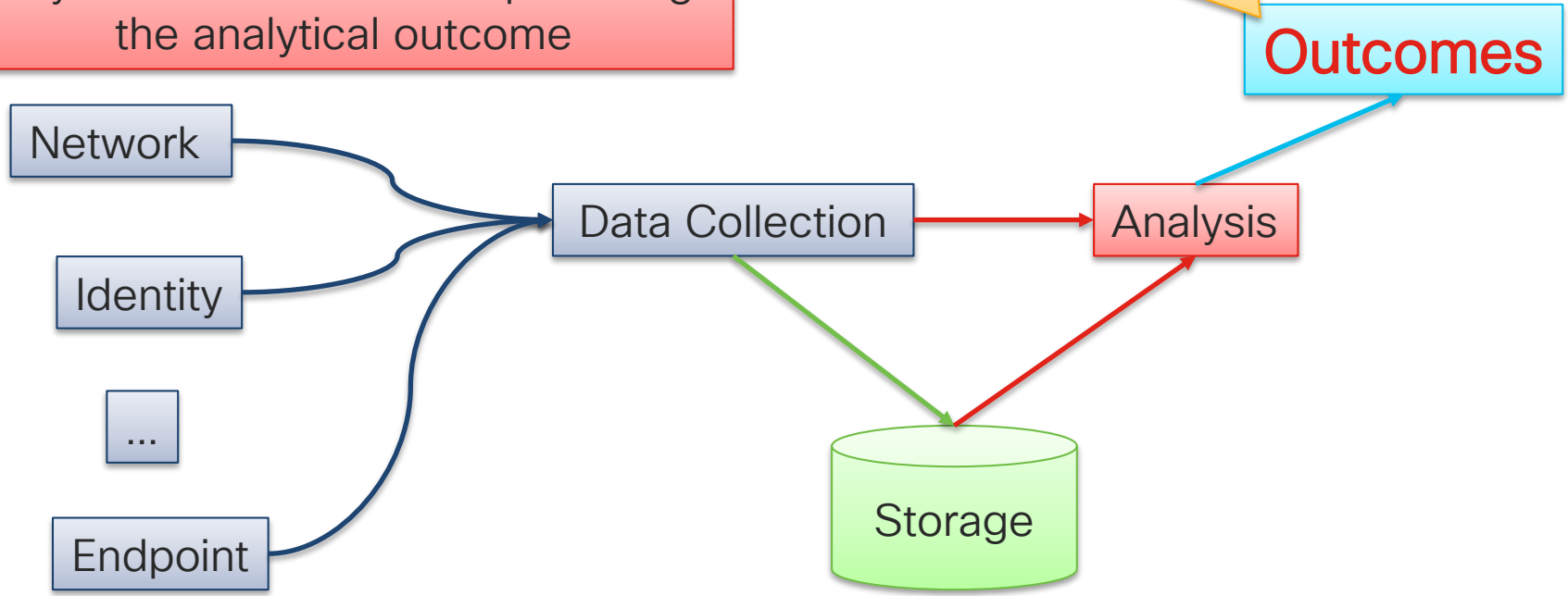
Find the use case docs at:

cs.co/StealthwatchValueUseCaseMenu

Powering Visibility & Analytics with Telemetry

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

This is what's important.

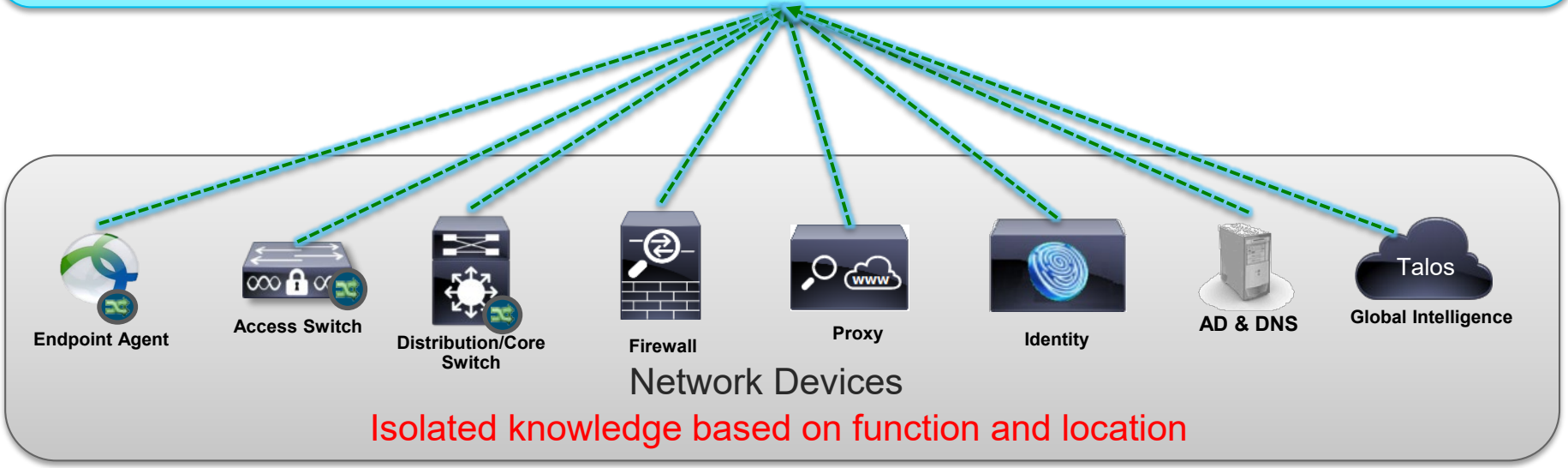


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Network Telemetry

Telemetry: an automated communications process by which measurements and other data are collected at remote or inaccessible points and transmitted to receiving equipment for monitoring.

https://en.wikipedia.org/wiki/Telemetry



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Stealthwatch Objective: Modelling The Network

Modelling Entities (Nouns)

Modelling Transactions (Verbs)

Host Attributes:

- Role in transaction
- Role in organization
- Device Type
- Username
- Reverse DNS
- …
- Etc.

Transaction Attributes:

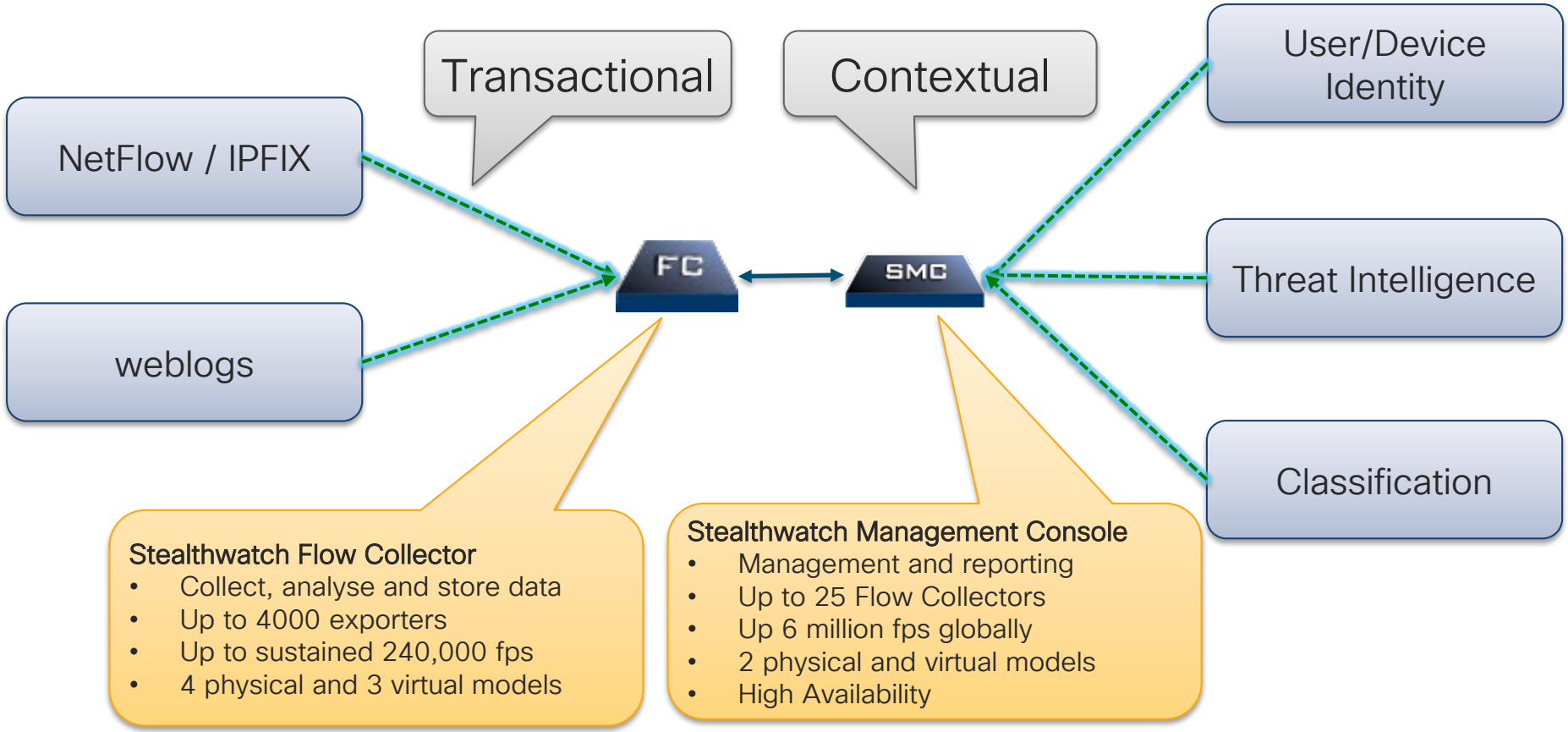
- Time
- Byte, packet counts
- Protocols & ports
- Application
- Application Content
- Process Name
- Network Devices
  - Interfaces
  - Decisions
- …
- Etc.

Host Attributes:

- Role in transaction
- Role in organization
- Device Type
- Username
- Reverse DNS
- …
- Etc.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

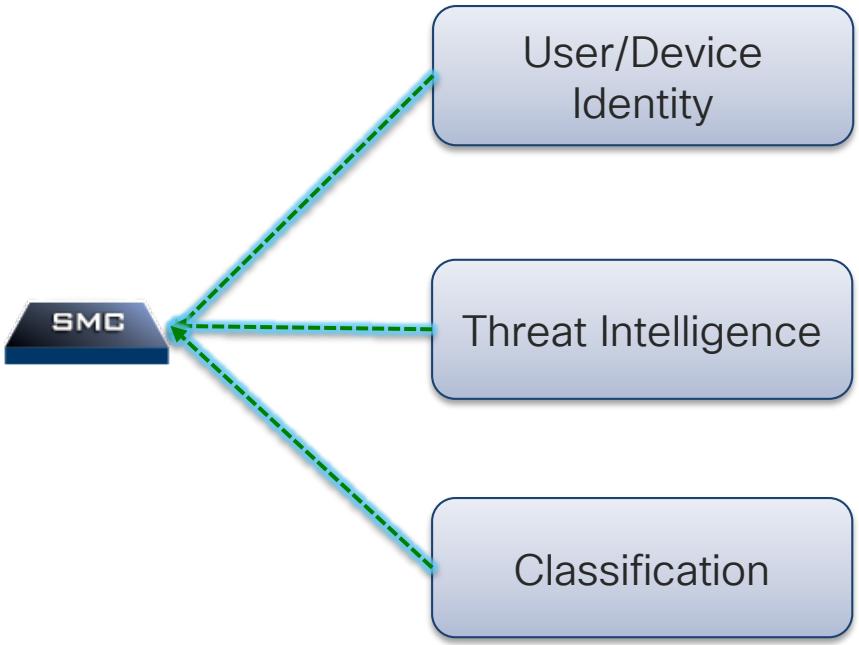
Stealthwatch: Building the “General Ledger”



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Contextual Telemetry

Labelling the IP Space



Identity Services Engine pxGrid Topics:

- Session
- TrustSec Group Members (SXP)

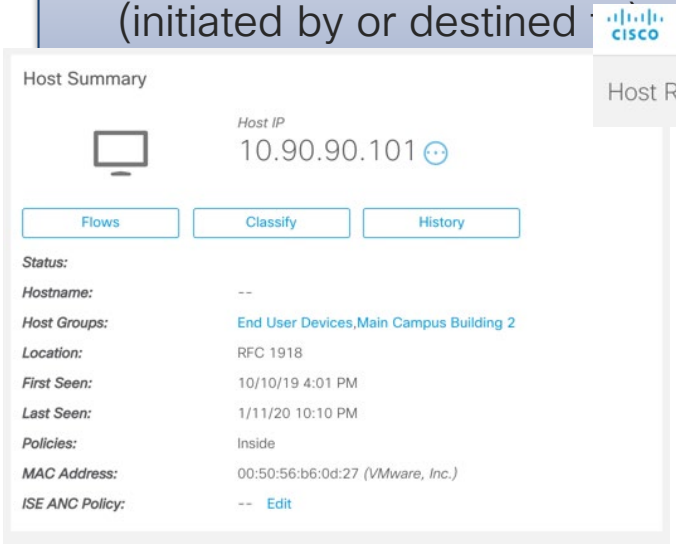
Host Groups:
Configured, Imported and/or Automated

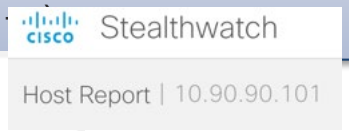
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Key Concepts!

Host:

- Single IP Address
- Stealthwatch identifies and monitors all hosts for which traffic was observed (initiated by or destined



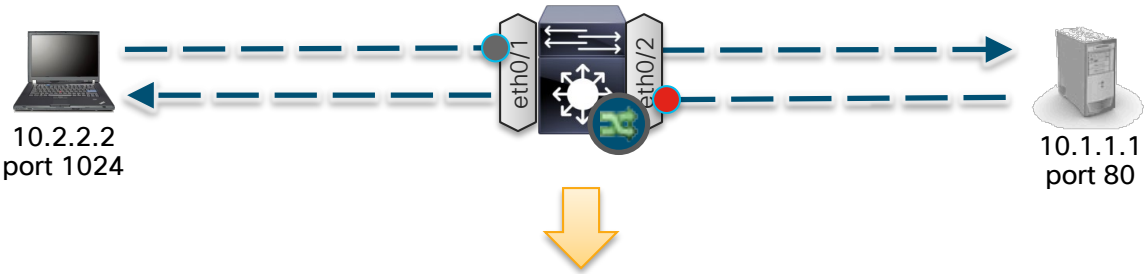


Host Group:

- Software label on one or more IP Addresses

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Transactional Telemetry with NetFlow

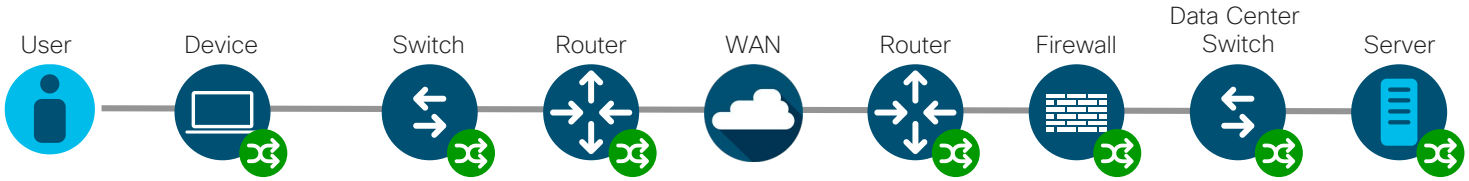


Start Time	Interface	Src IP	Src Port	Dest IP	Dest Port	Proto	Pkts Sent	Bytes Sent	SGT	DGT	TCP Flags
10:20:12.221	eth0/1	10.2.2.2	1024	10.1.1.1	80	TCP	5	1025	100	1010	SYN,ACK,PSH
10:20:12.871	eth0/2	10.1.1.1	80	10.2.2.2	1024	TCP	17	28712	1010	100	SYN,ACK,FIN

NetFlow is a Layer 7 protocol. The **Metadata** is what's important.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Example NetFlow Exporters



NetFlow/sFlow Export is available across the Cisco portfolio

Switch
- Catalyst 2960-X (v9/IPFIX)
- Catalyst 3650/3850 (v9/IPFIX)
- Catalyst 4500E (v9/IPFIX)
- Catalyst 6500E (v9/IPFIX)
- Catalyst 6800 (v9/IPFIX)
- Catalyst 9200 (v9/IPFIX)
- Catalyst 9300/9400 (v9/IPFIX ETA)
- Catalyst 9500 (v9/IPFIX ETA)
- Catalyst 9600 (v9/IPFIX ETA)
- IE3000 (v9/IPFIX)
- IE4000 (v9/IPFIX)
- IE5000 (v9/IPFIX)

Router
- Cisco ISR 4000 (v9/IPFIX ETA)
- Cisco CSR 1000v (v9/IPFIX ETA)
- Cisco ASR 1000 (v9/IPFIX ETA)
- Cisco ASR 9000 (v9/IPFIX)
- Cisco WLC 5520, 8510, 8540 (v9 Fixed)
- Catalyst 9800 (v9/IPFIX ETA)

Firewall
- ASA 5500-X (NSEL)
- FTD (NSEL)
- Meraki MX/Z1 (v9 Fixed)

Data Center Switch
- Nexus 1000v (v9/IPFIX)
- Nexus 3000 (sFlow)
- Nexus 7000 (M Series I/O modules – (v9/IPFIX)
- Nexus 7000 (F Series I/O modules – (v9/IPFIX sampled)
- Nexus 9000 Series (sFlow)
- Nexus 9000 Series EX/FX (v9)

Servers, Software and Appliances
- Cisco Stealthwatch Flow Sensor (v9/IPFIX ETA)
- Cisco UCS VIC (v9/IPFIX)
- Cisco AnyConnect Client (IPFIX)

The above is a non-exhaustive list of Cisco exporters.
For individual platform features, reference the Cisco Feature Navigator: http://cfn.cloudapps.cisco.com/ITDIT/CFN/jsp/index.jsp

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Versions of NetFlow

Version 5
Fixed Format
18 Defined Entities

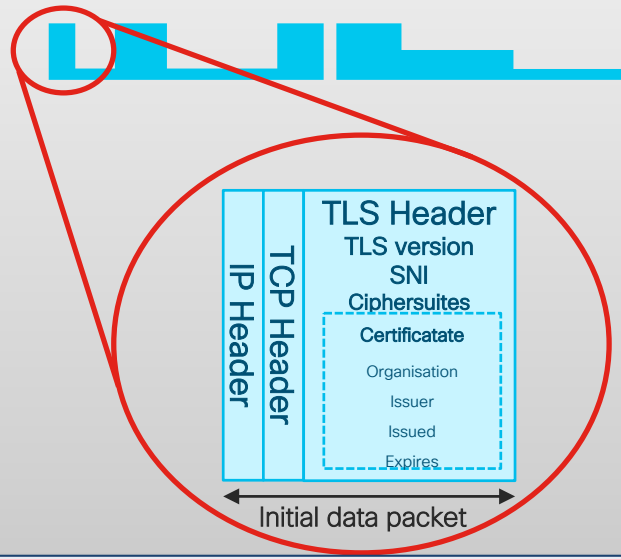
Version 9
Template Based
108+ Defined Entities

IPFIX
Standardized
Template Based
Variable Length Fields
450+ Defined Entities

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Enhanced Telemetry for Encrypted Traffic Analytics

Initial Data Packet



First application layer message.

In **TLS** this is the **Client Hello** and **Server Hello**

Sequence of Packet Lengths and Time (SPLT)

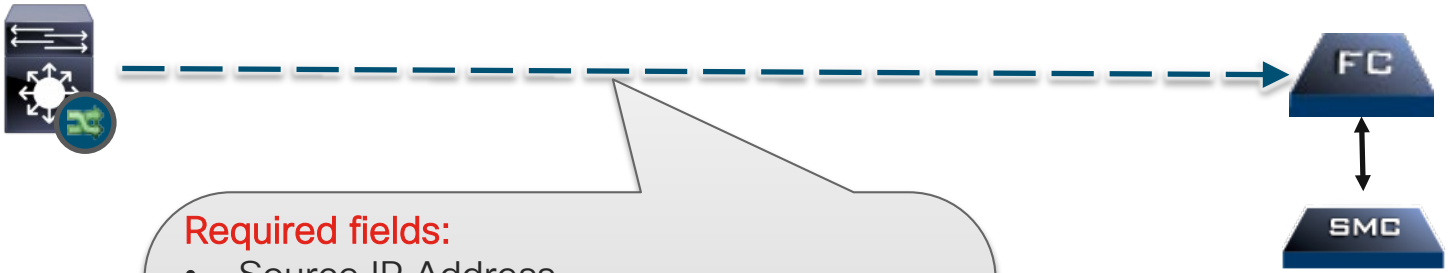
Size and timing of the first packets of a flow

Useful in identifying application, data types and characterising the source

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Stealthwatch: What defines a Flow

Stealthwatch requires certain fields to make a database entry:



Required fields:

- Source IP Address
- Source Port
- Destination IP Address
- Destination Port
- IP Protocol
- Byte count
- Packet count
- Start time (first switched)
- End time (last switched)
- Input Interface (*recommended*)

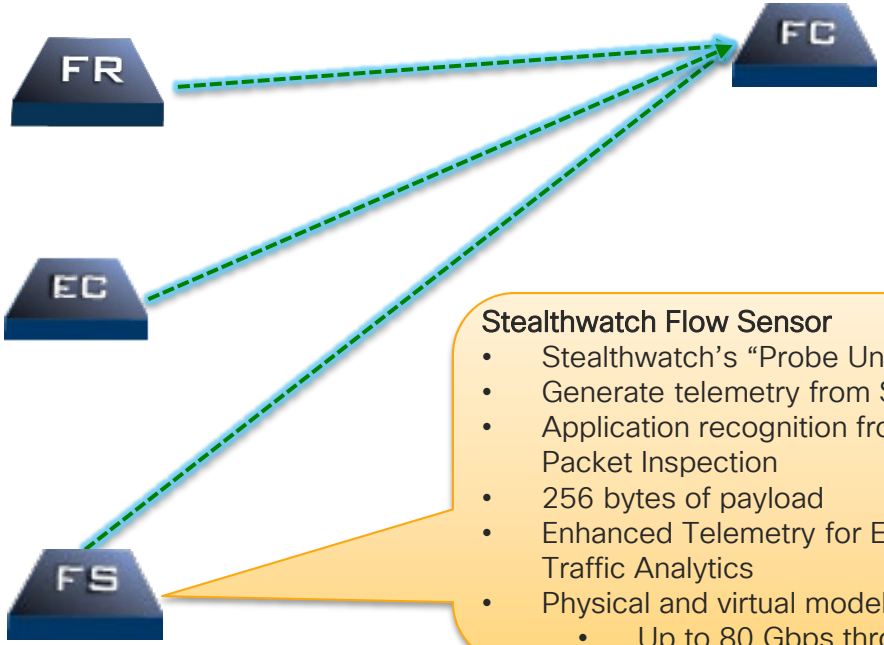
Other fields are additional meta data to enable additional analytics

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Expanding a Stealthwatch Deployment

Optional methods of increasing and enriching the dataset

UDP Director
- UDP Packet copier
- Forward to multiple destinations
- High Availability
- 2 physical and virtual models



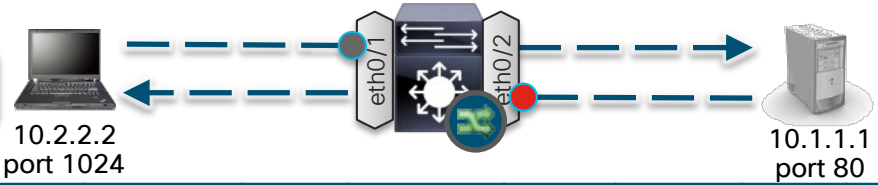
Endpoint License Concentrator
- Collect AnyConnect Network Visibility Module IPFIX export, synthesize and forward to Flow Collector
- Virtual Appliance

Stealthwatch Flow Sensor
- Stealthwatch's "Probe Unit"
- Generate telemetry from SPAN/TAP
- Application recognition from Deep Packet Inspection
- 256 bytes of payload
- Enhanced Telemetry for Encrypted Traffic Analytics
- Physical and virtual models
  - Up to 80 Gbps throughput

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Telemetry Processing: Sessionizing the Data

Uni-directional flow records



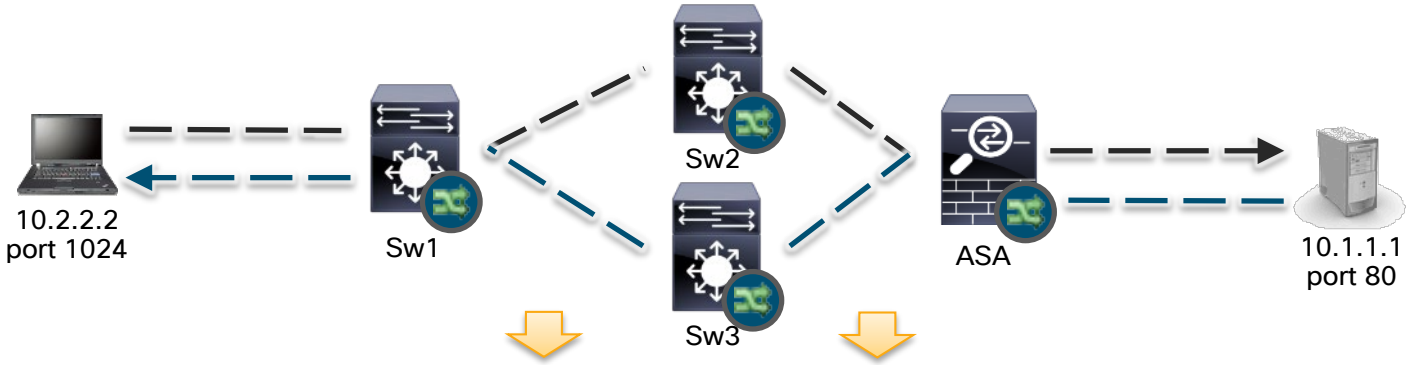
Start Time	Interface	Src IP	Src Port	Dest IP	Dest Port	Proto	Pkts Sent	Bytes Sent	SGT	DGT
10:20:12.221	eth0/1	10.2.2.2	1024	10.1.1.1	80	TCP	5	1025	100	1010
10:20:12.871	eth0/2	10.1.1.1	80	10.2.2.2	1024	TCP	17	28712	1010	100

Start Time	Client IP	Client Port	Server IP	Server Port	Proto	Client Bytes	Client Pkts	Server Bytes	Server Pkts	Client SGT	Server SGT	Interfaces
10:20:12.221	10.2.2.2	1024	10.1.1.1	80	TCP	1025	5	28712	17	100	1010	eth0/1 eth0/2

Bi-directional:
- Conversation flow record
- Allows easy visualisation and analysis

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

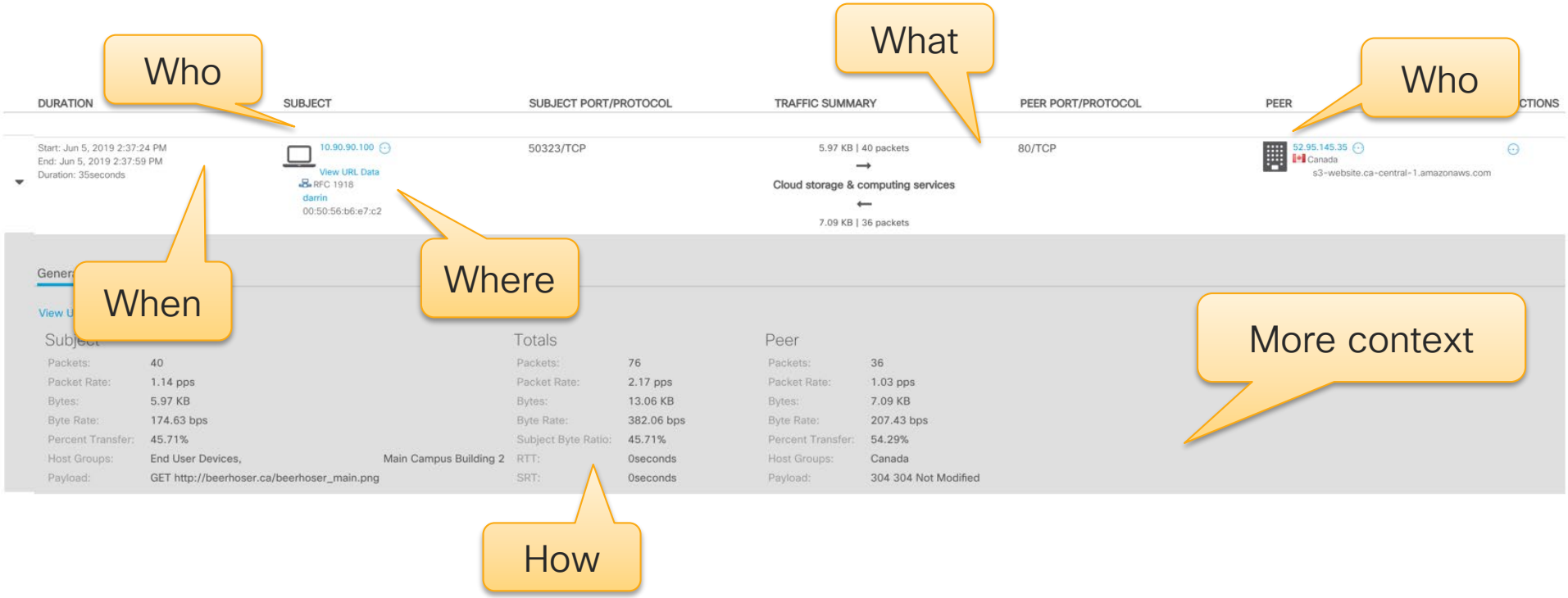
Telemetry Processing: End-to-End Sessionization



Start Time	Client IP	Client Port	Server IP	Server Port	Proto	Client Bytes	Client Pkts	Server Bytes	Server Pkts	App	Client SGT	Server SGT	Exporter, Interface, Direction, Action
10:20:12.221	10.2.2.2	1024	10.1.1.1	80	TCP	1025	5	28712	17	HTTP	100	1010	Sw1, eth0, in Sw1, eth1, out Sw2, eth0, in Sw2, eth1, out ASA, eth1, in ASA, eth0, out, Permitted ASA eth0, in, Permitted ASA, eth1, out Sw3, eth1, in Sw3, eth0, out Sw1, eth1, in Sw1, eth0, out

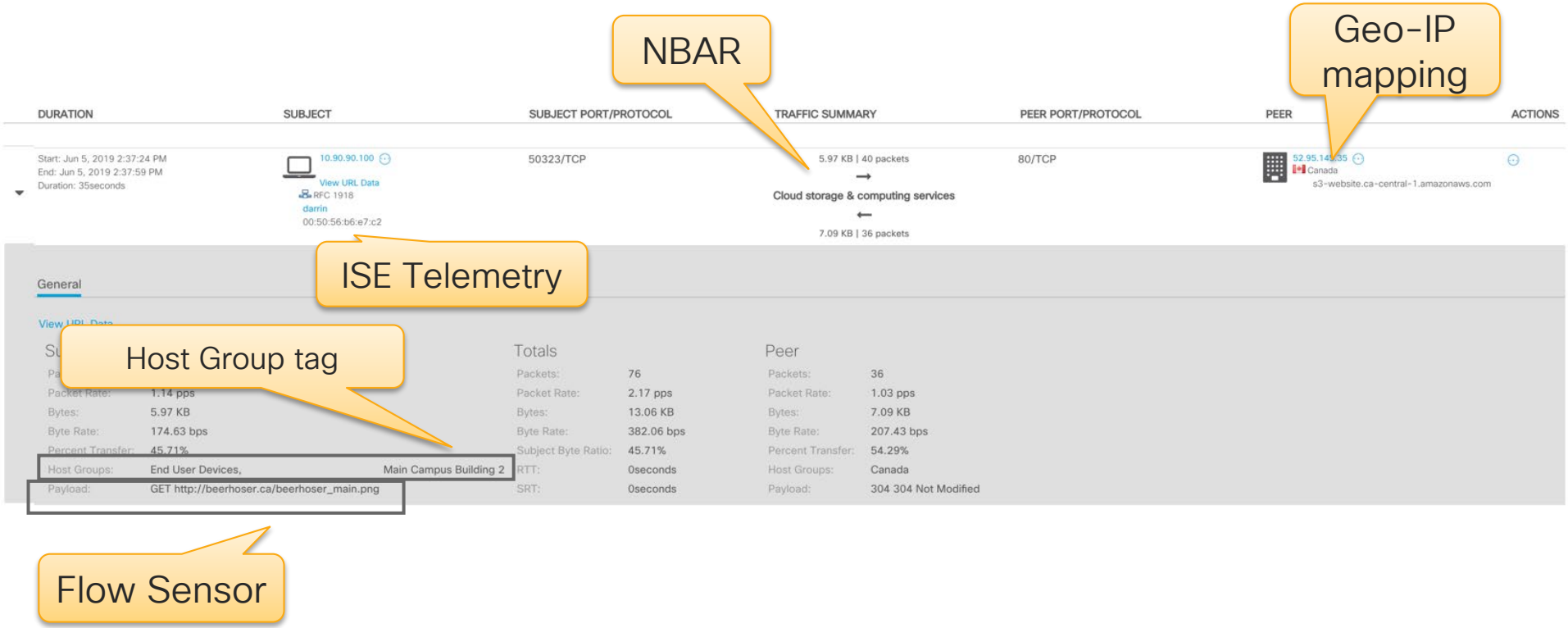
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Conversational Flow Record



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

“Decorated” Conversational Flow Record



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Operationalising Visibility

Empowering Security Operations

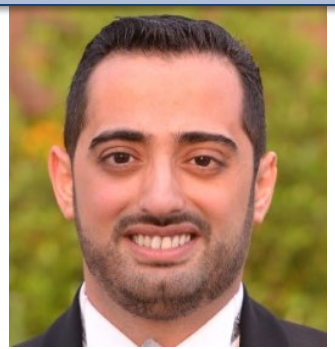
Hunting:
Finding something of interest in the wild

Analysing:
Determine what the data is telling you

Investigating:
Piecing together the story from a piece of data

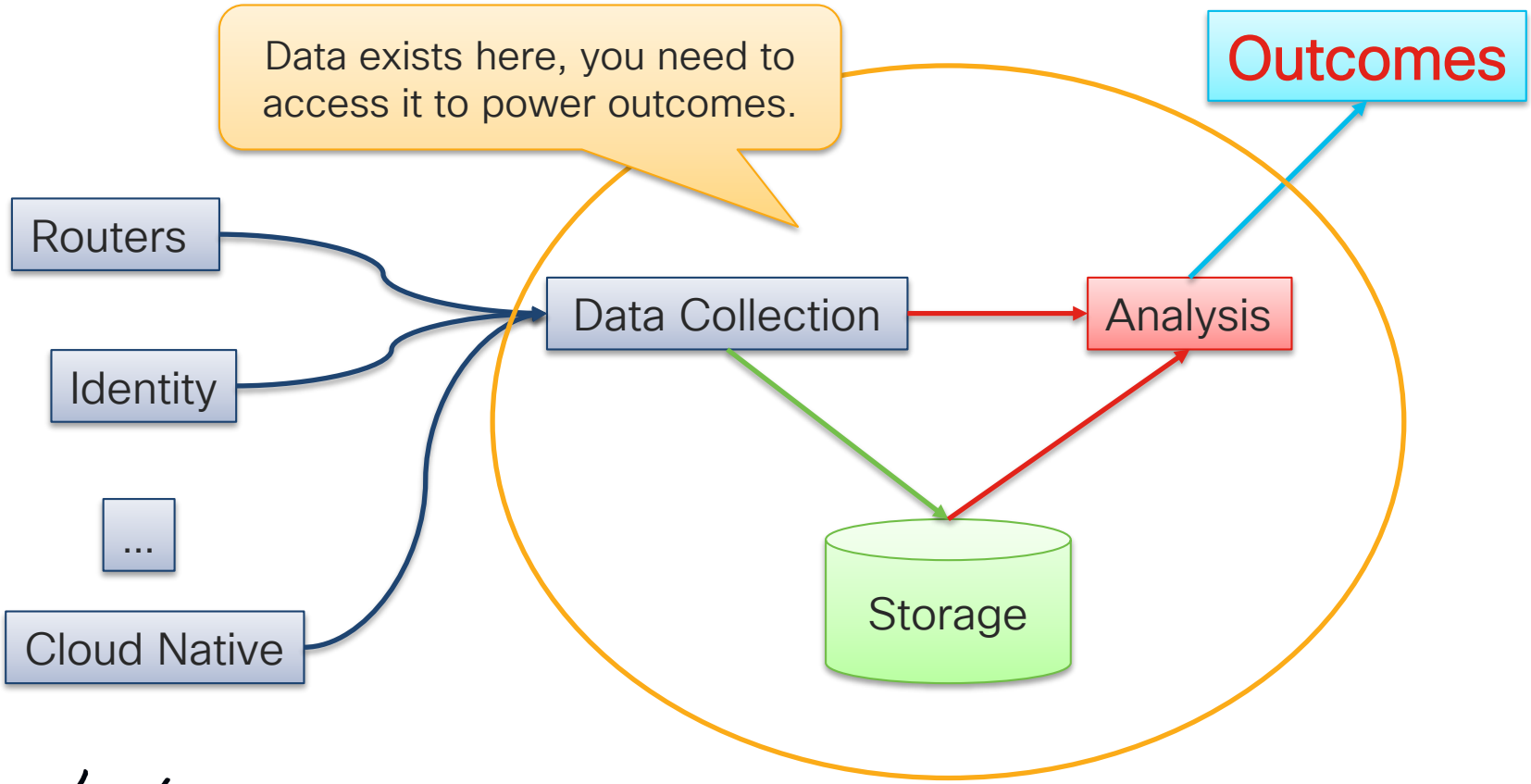
Creating outcomes from the data

BRKSEC-2462 – Stealthwatch Beyond Alarms – Hanna Jabbour – Tuesday, January 28, 11:00 AM – 1:00 PM



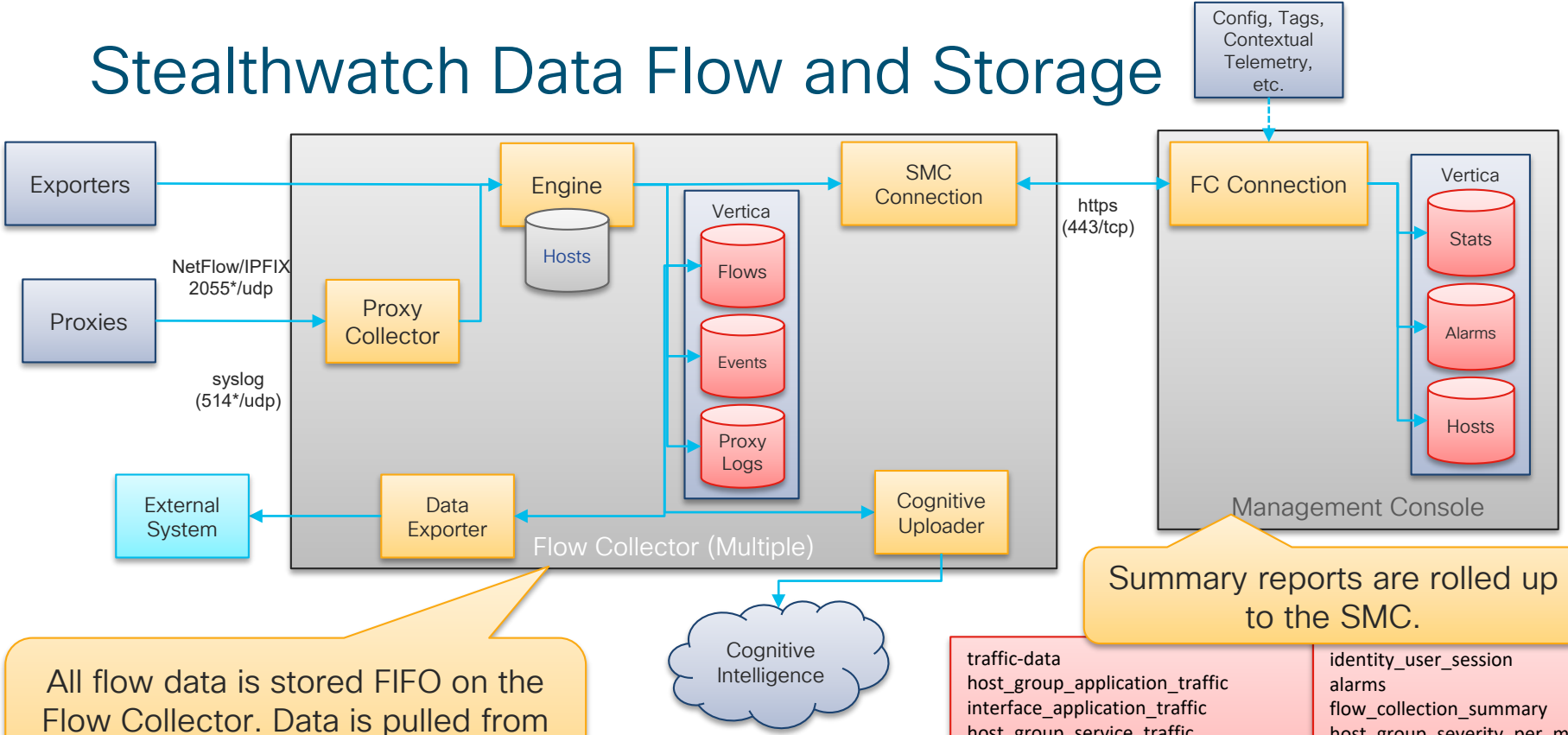
 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Powering Outcomes with Data



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Stealthwatch Data Flow and Storage



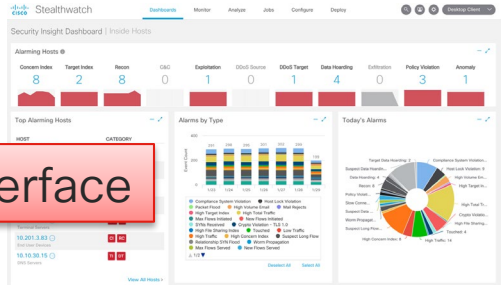
All flow data is stored FIFO on the Flow Collector. Data is pulled from Flow Collector(s) at query time.

Summary reports are rolled up to the SMC.

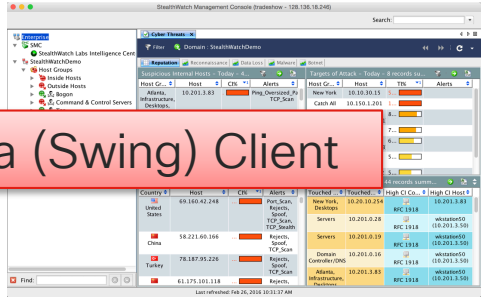
traffic-data	identity_user_session
host_group_application_traffic	alarms
interface_application_traffic	flow_collection_summary
host_group_service_traffic	host_group_severity_per_minute
as_traffic	host_group_pair_info
host_group_pair_service_traffic	host_group_pair_status
interface_traffic	host_hourly_byte
system_traffic	flow_collection_trend
dscp_traffic	host_info
host_group_traffic	host_group_info
host_group_pair_application_traffic	

cisco Live!

Accessing the Data: User Interfaces

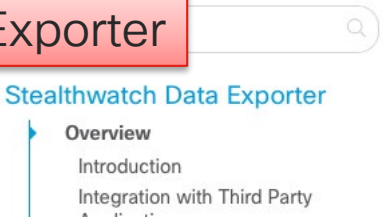


Web Interface



Java (Swing) Client

REST APIs



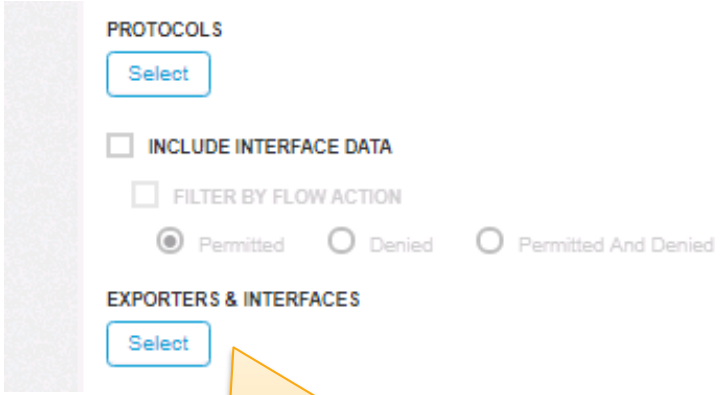
Data Exporter

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Best Practices: Working with the Data

Structure the data by using Host Groups (more on this later)

- Define your objective: What are you looking for?
- Leverage pre-built reports on the SMC
  - Host Groups Reports
    - Top Reports
  - Host Report
  - Analytic Observations (more on this later)
  - Use Stealthwatch Apps
- Use Flow Summary Reports first when looking for flows over long periods of time
  - Flow Traffic, Top Hosts, Top Conversations
  - Drill down to the flow data



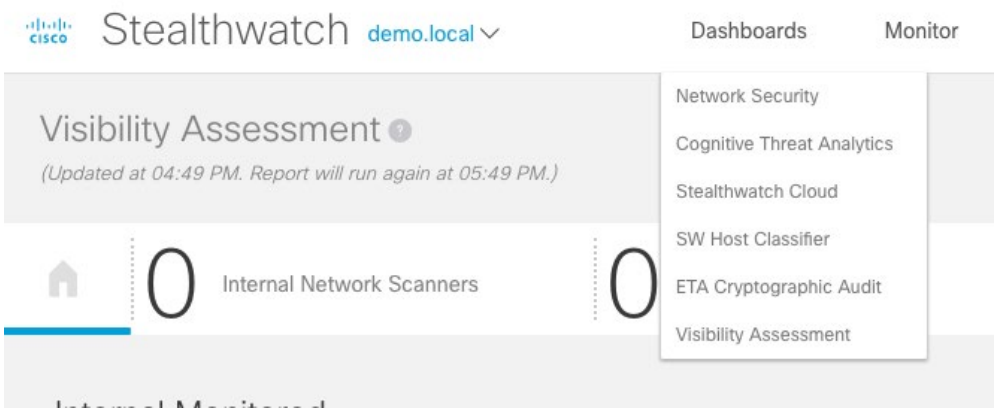
Leave “Include interface data” unchecked if you don’t need it when performing a flow search. Searches return faster.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Stealthwatch Apps

Stealthwatch Apps

- Scheduled reports/analytic
- Independent of product release cycle
- New in 7.0



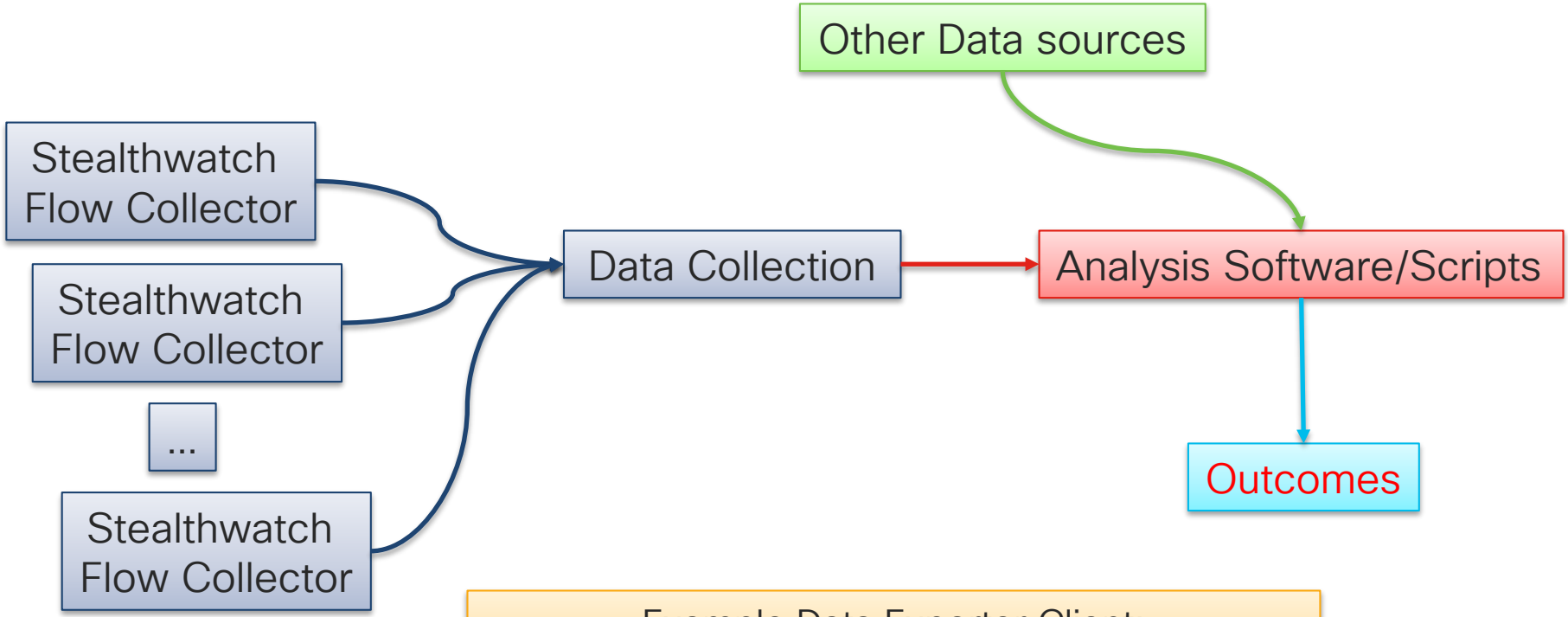
Current Stealthwatch Apps

- Visibility Assessment
  - Scheduled report
- Host Classifier
  - Rule-based Classification
- ETA Cryptographic Audit
  - By Host Group Report
- Network Diagrams
  - Maps!

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Flow Query Demo

Data Export and analysis



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

- Introduction
- Enabling Visibility and Analytics with Telemetry
- Understanding Security Analytics

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Why Machine Learning

Evolving Security Landscape:

- Pattern matching insufficient
- Dark Data
- Direct Inspection expensive
- Internet of things

Etc.

Evolving Security

The security domain is always evolving,
has a large amount of variability,
and is not well-understood

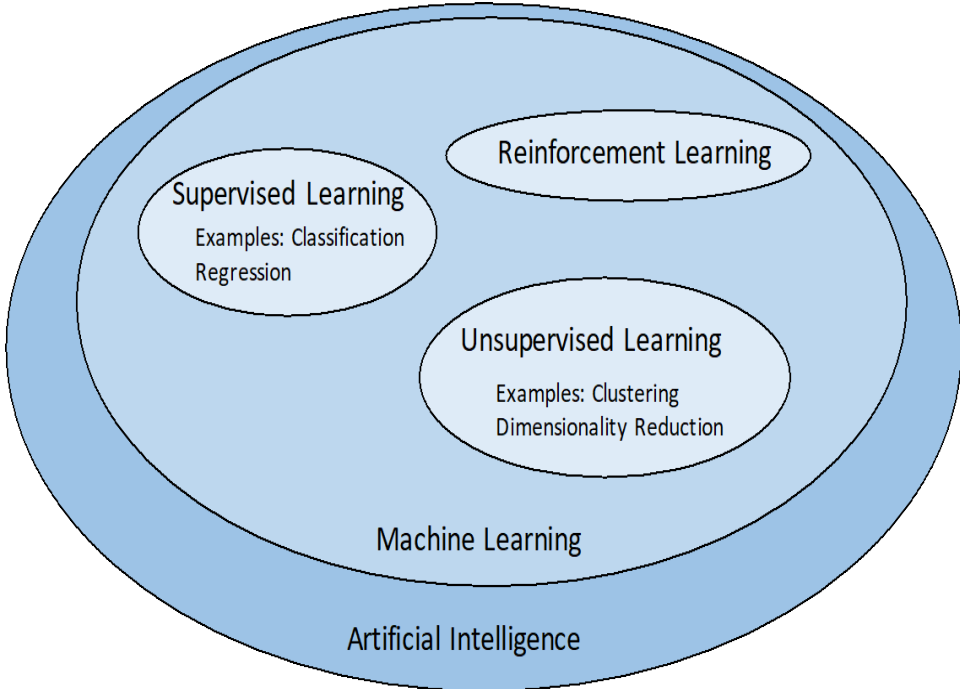
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Machine Learning

Designing algorithms directed at achieving some outcome.

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

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



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Supervised Learning

Supervised:
Used when you know the question you are trying to answer and have examples of it being answered correctly.

Training Data (Ground Truth)

This is Matt

Is this Matt?

Ground Truth:
"we know this is right, learn a way to answer more questions of this type"

Success depends on the accuracy of the ground truth.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Unsupervised Learning

Unsupervised:
Less structured. You don't know the answers and may not fully understand the question. Useful in understanding how members of a set relate.

These seem similar…

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Security Analytics: Outcomes

Automating Security Operations

Automating or Augmenting these functions:

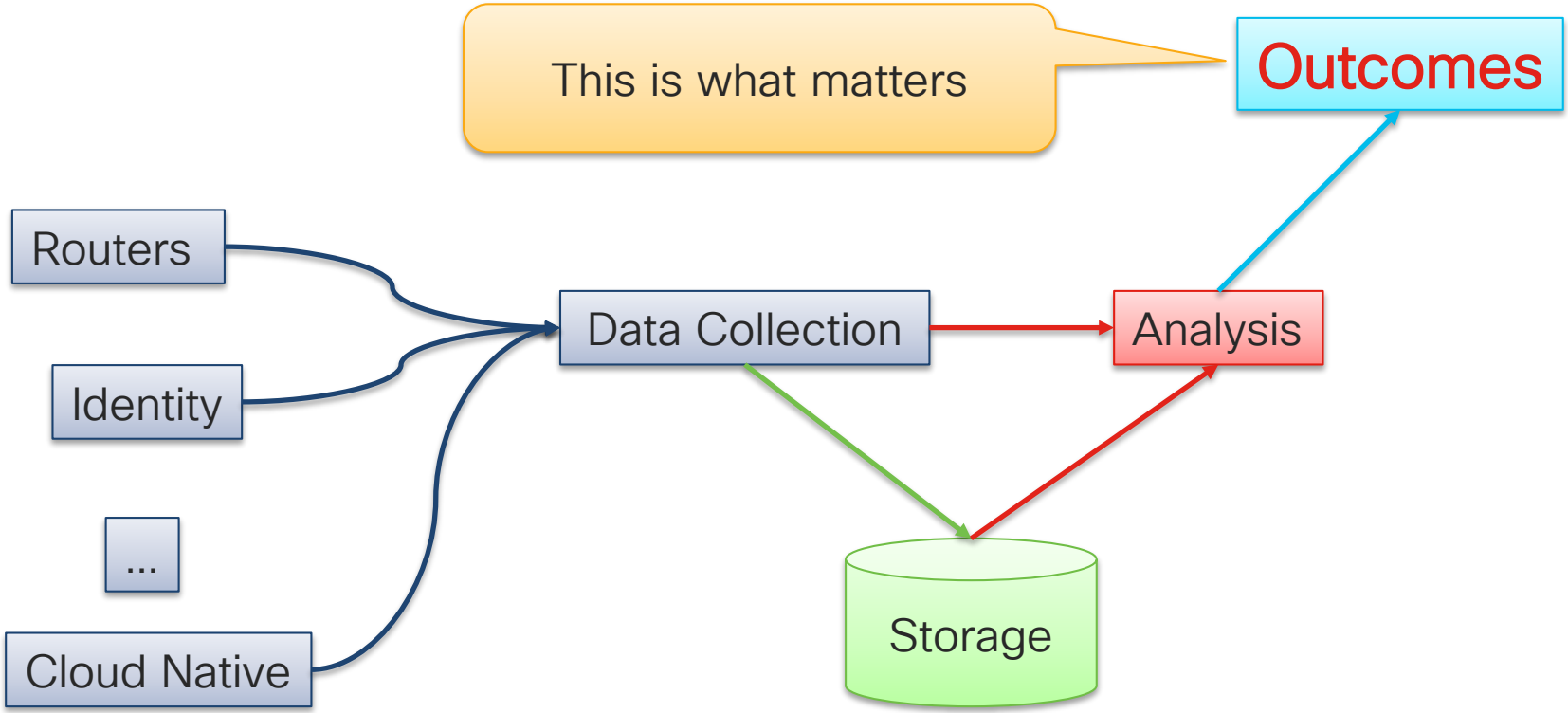
- Incident Responder
- Security Analyst
- Security Operations
- Threat Hunter
- Compliance and Policy
- Business Continuity
- Cybercrime fighting
- Etc.

Automating implies an algorithmic approach, which could be a diverse set of methods to accomplish the outcome:

- Entity Modelling
- Statistical Analysis
- Predictive Analysis
- Machine Learning
- Unsupervised Learning
- Supervised Learning
- Reinforced Learning
- Artificial Intelligence
- Etc.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

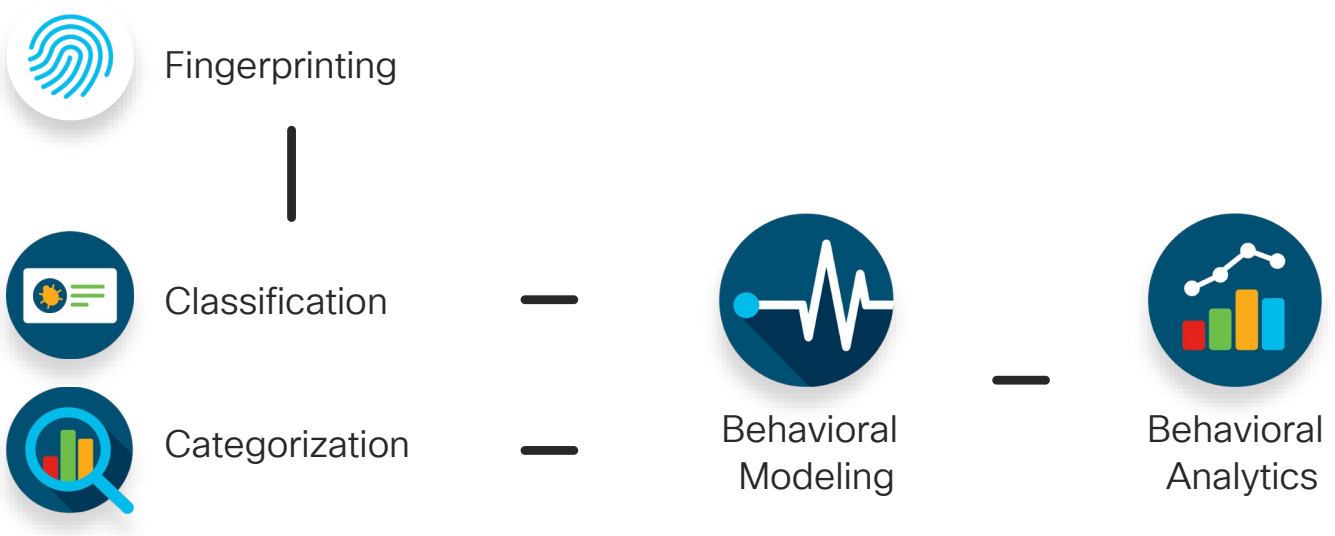
Creating Outcomes with Analytics



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

The Security Analytical Pipeline

BRKSEC-2068 – The Future of Security Analytics – TK Keanini – Tuesday, January 28, 5:00 PM – 6:30 PM



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

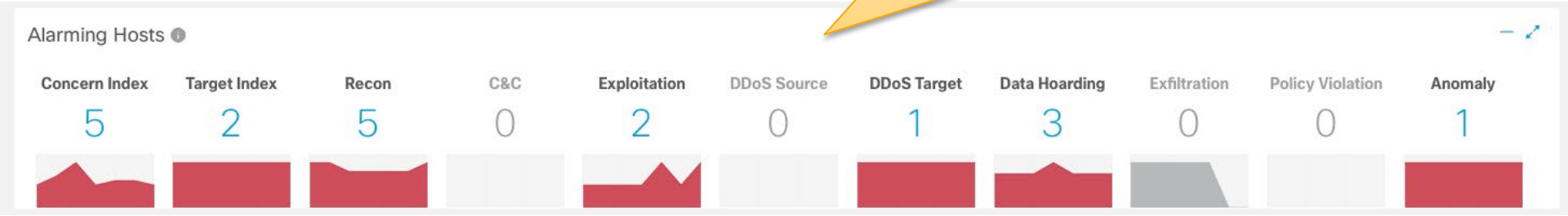
- Introduction
- Enabling Visibility and Analytics with Telemetry
- Understanding Security Analytics
- Operationalising Stealthwatch Analytic Engines

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Operationalising Stealthwatch Analytics

Automating Security Operations

Creating outcomes from Analytical Outputs



Analysing:

Making the observations actionable and relevant to the business

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Operationalising Stealthwatch Analytics

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_Stealthwatch_Six_Phased_Approach_to_Tuning.pdf

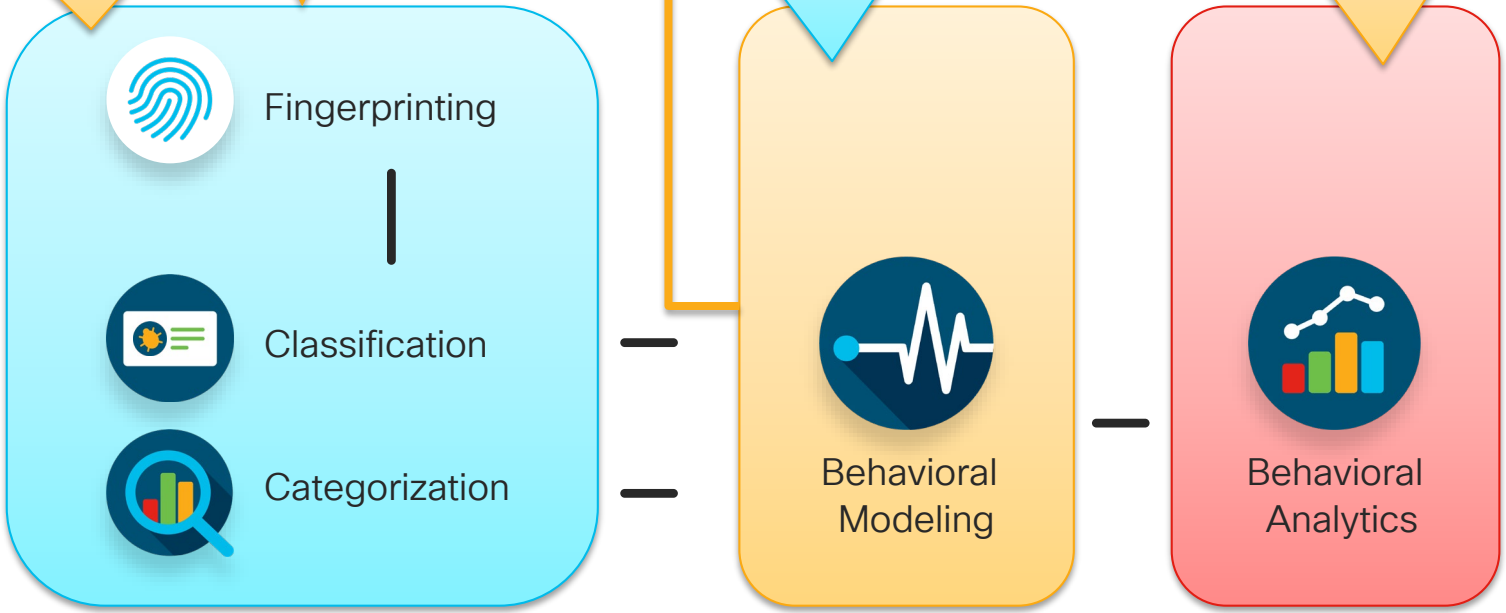
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Security Analytics Pipeline with Stealthwatch

- Discover Hosts,
- Classify into Host Groups

- Analyze observables
- Establish baseline
- Make observations

Use the Behaviour model to generate detections (outcomes)



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Discover and Classify Assets

- Discover Hosts,
- Classify into Host Groups

Fingerprinting

Classification

Categorization

Define the entities to perform analytics on

Behavioural Modelling

CREATING HOST GROUPS

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Types of Host Groups

- **Inside Hosts:**
  - All Hosts specifically defined as part of the network
  - By Default – "Catch All"
- **Outside Hosts**
  - All Hosts not specifically defined as part of the network
  - Countries – GEO-IP
- **Threat Intelligence Created**
  - Bogon
  - Command & Control Servers
  - Tor

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

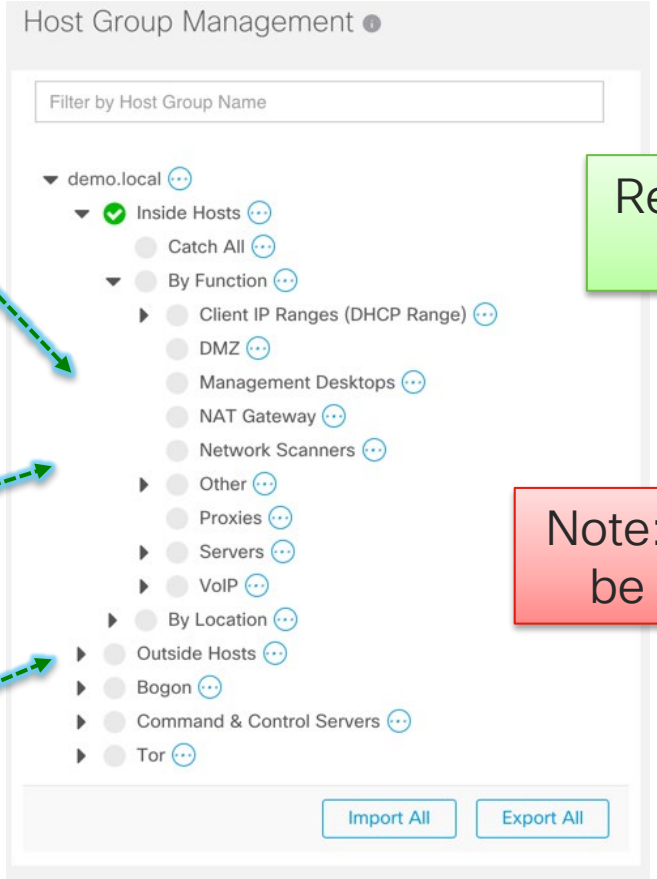
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Building Groups

Group Definitions as Telemetry via API:
- IPAM
- Threat Intelligence
- Etc.

Manual:
- Data Entry
- Search

Automatic:
- Host Classifier



Remember to stay focused on desired Outcomes!

Note: not everything needs to be classified immediately.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Host Group Automation via API

Tetration Analytics

IPAM

Threat Intel

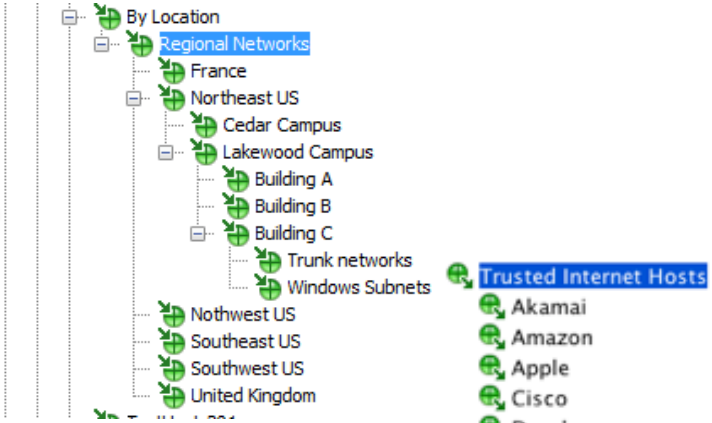
ASN:IP Databases

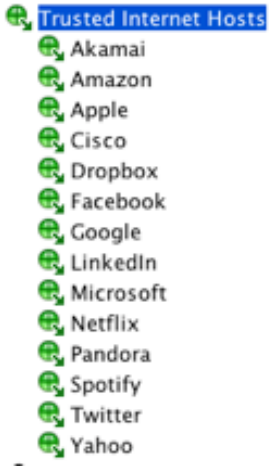
Etc.

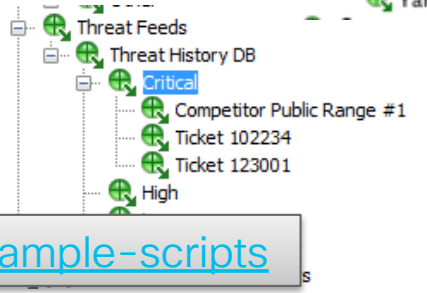
Contextual IP Definitions

SMC

Scripted conversion to host groups





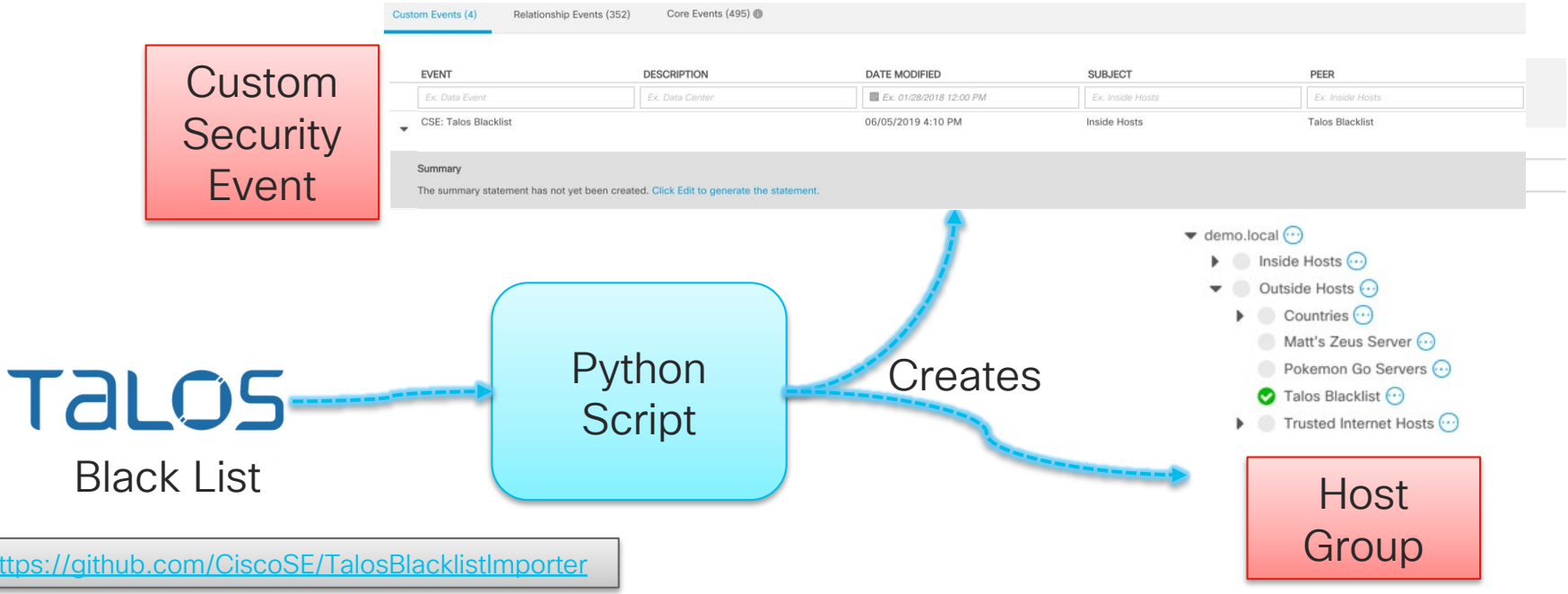


https://github.com/CiscoDevNet/stealthwatch-sample-scripts

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Example: Talos Blacklist Import

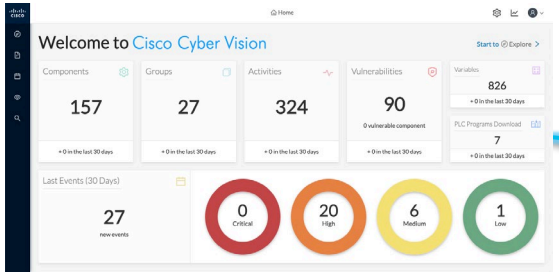
DEVWKS-1545 – DevNet Workshop – Operationalizing Stealthwatch with API Capabilities – Kyle Winters, Benjamin Mcinnis – Monday, January 27, 4:00 PM – 4:45 AM ; Wednesday January 29, 11:00 AM – 11:45 AM



https://github.com/CiscoSE/TalosBlacklistImporter

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Example: Cyber Vision

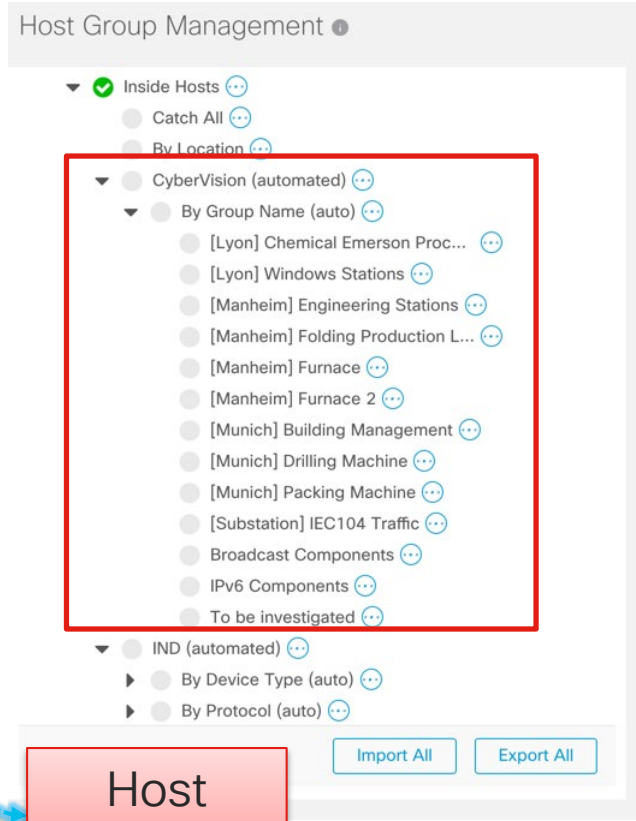


Cisco Cyber Vision

REST API

Python Script

Creates

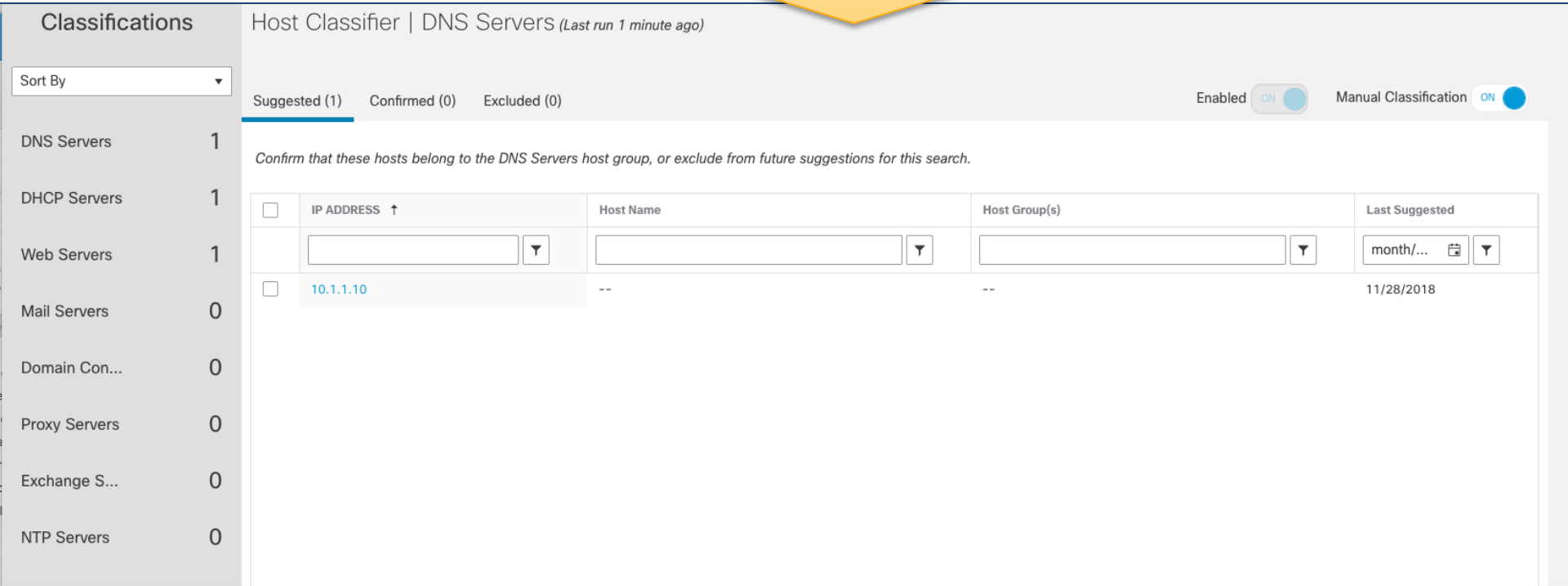


Host Groups

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Stealthwatch 7.0: Stealthwatch Host Classifier

- Make suggestions for unclassified hosts into host groups
- User can review and confirm, reject or exclude suggestions



Host Group Tactics: Best Practices

Outside Hosts

- Trusted Internet Hosts
  - Partners/Trusted Entities
- Monitored Internet Hosts
  - Specific hosts of interest. Ex. Cloud Service Providers
- Suspect Fat finger
  - Investigation acceleration
- Talos Blacklist
  - Talos published list of known bad IP's

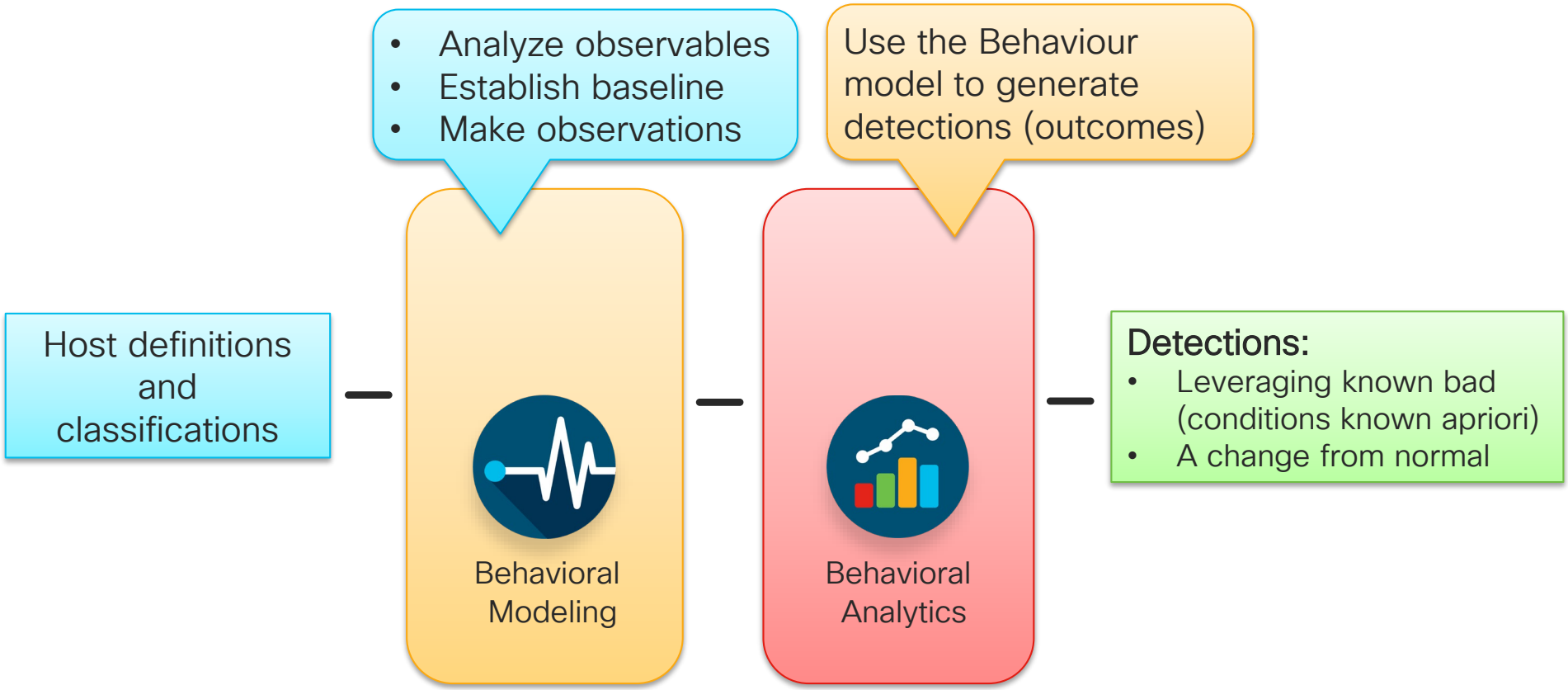
Inside Hosts

- Catch All
  - Unclassified Space
- By Location
  - for reference and trust boundaries
- By Function
  - for security policy and reporting
  - Limit policy to this group
- By Application
  - for investigation

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Host Classification Demo

Behavioural Modelling and Detection



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Leveraging Known Bad

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

A Change from Normal

Wine?!

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Stealthwatch Layers of Detection

Cognitive Intelligence

- Cloud Hosted
- Multi-layer Machine Learning
- Anomaly detection
- Supervised Learning Engine
- Malware classification

Custom Security Events

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

Relationship Events

- Interaction between host groups that violate a policy setting
- Derived from relationships created in network diagram

Core Events

- Unsupervised learning engine
- 98+ behavioural algorithms:
  - Statistical anomaly detection
  - Policy based detection
- Threat Intelligence powered alarms

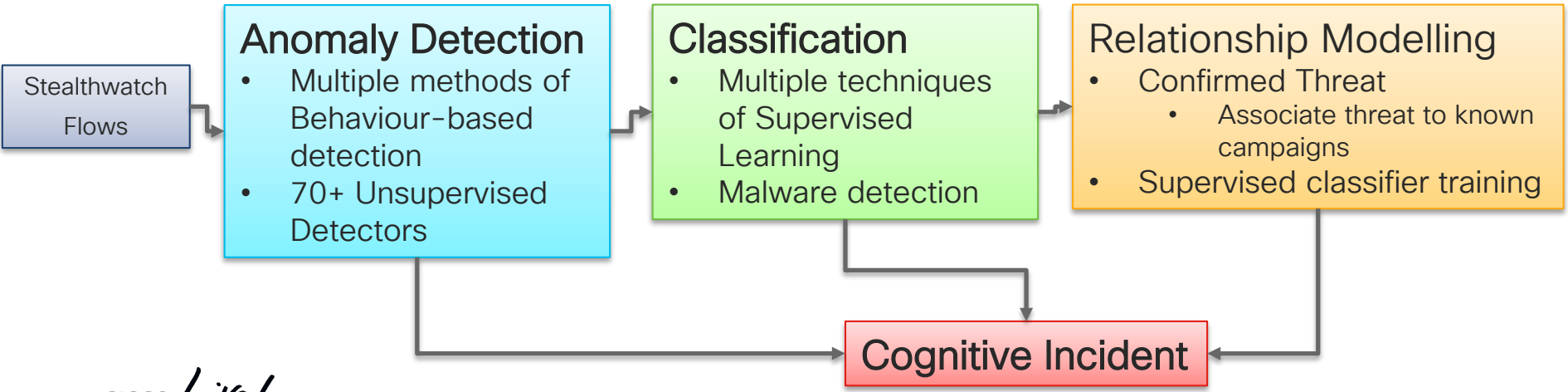
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cognitive Intelligence

Cognitive Intelligence

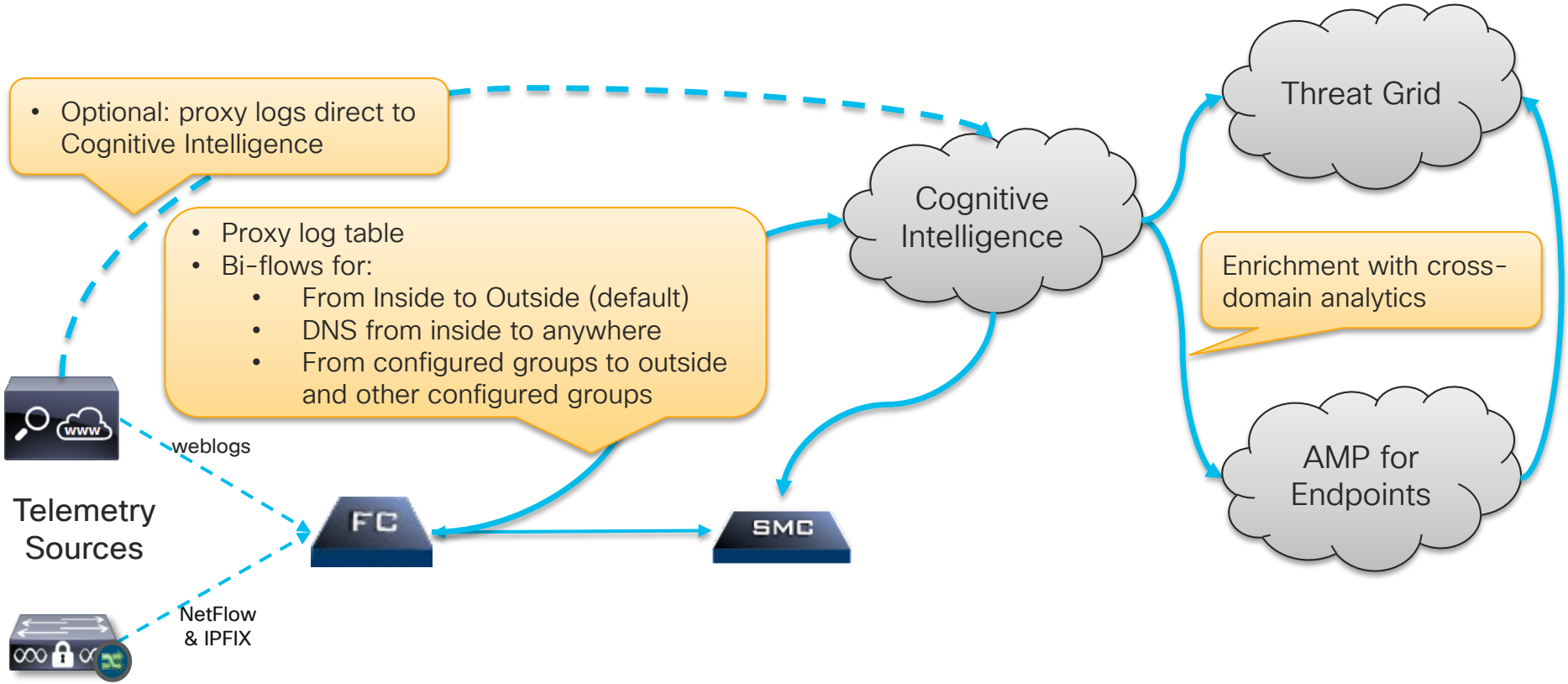
- Cloud Hosted
- Multi-layer Machine Learning
- Anomaly detection
- Supervised Learning Engine
- Malware classification

Added to Stealthwatch in v6.9.1



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Powering Cognitive Intelligence with Telemetry



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

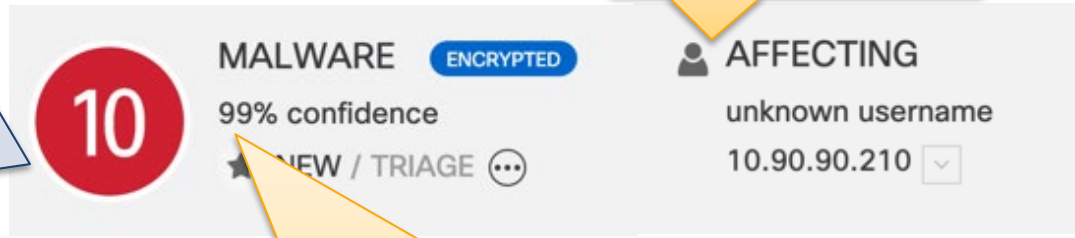
Cognitive Incident

Detection generated from the behavioural analysis of a host or user on the netwo

Risk Rating:

- Critical (10)
  - Likely compromised with an advanced threat with a behavior that may be damaging to the business has been observed.
- High (8,9)
  - Likely compromised with an advanced threat.
- Medium (6,7)
  - Likely contains malware that can be cleaned with endpoint cleaning tools
- Low (1-5)
  - May or may not be infected.

Affected user/host



Confidence Rating:

- How confident Cognitive is in the classification
- Three Levels:
  - High (95%-100%)
  - Medium (85%-94%)
  - Low (0%-84%)

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Example Incidents

Anomaly Incident

Odd Behaviour

- Anomalous Periodic Communication
- Anomalous Traffic
- Anomalous Destination
- Inconsistent User Time Activity
- Persistent Anomalous Traffic
- Unexpected User Destination
- 70+ More

Detected Incident

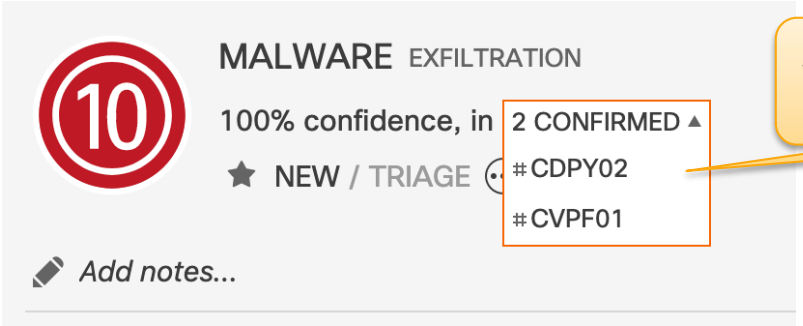
Labelled Behaviour

- Banking Trojan
- Cryptowall
- Ramnit
- Sality
- Botnet
- C&C
- Cryptocurrency Miner
- Potentially Unwanted Application
- SMB Service Discovery
- Phishing
- TOR
- 400+ More Classifiers

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cognitive Intelligence: Confirmed Threat

Anomaly Detection + Behavioural Detection + Global Feature Cache



Specific instance (campaign)

Confirmed incidents

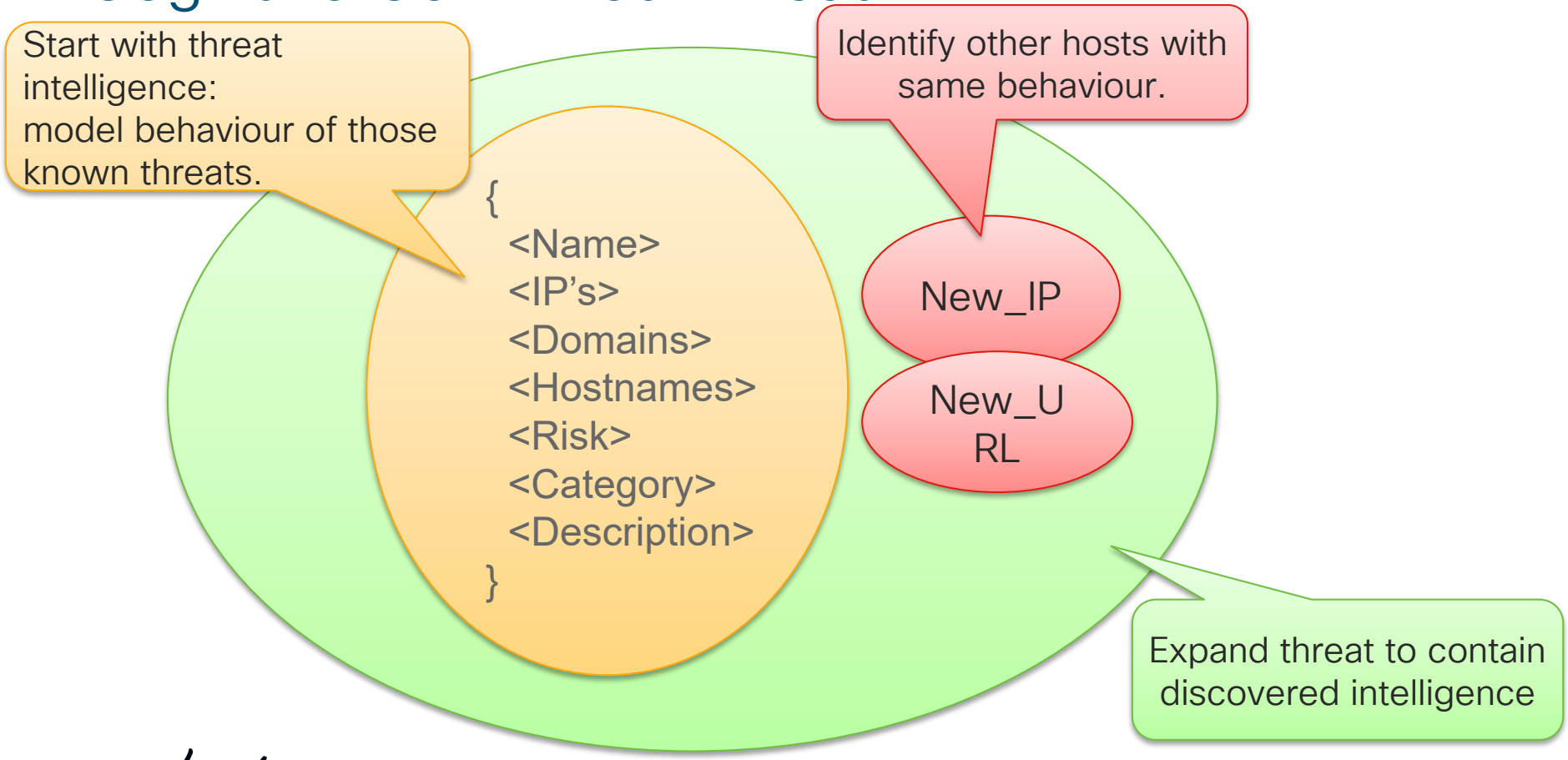
Confirmed incidents have a 100% confidence.

Confirmed incidents do not require much investigation time but rather fast action.

In addition to the general response instructions, the confirmed incident contains a threat-specific description and remediation instructions that can be found in CONFIRMED section to allow for more targeted remediation.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cognitive Confirmed Threat

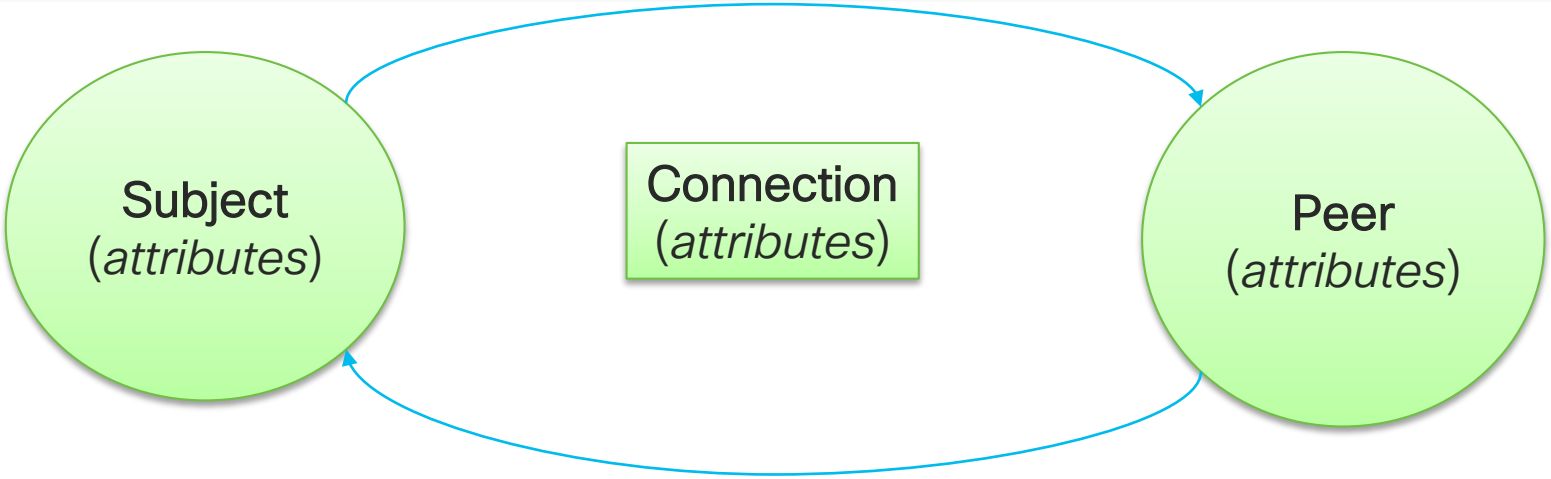


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cognitive Incident Demo

Stealthwatch Custom Security Event

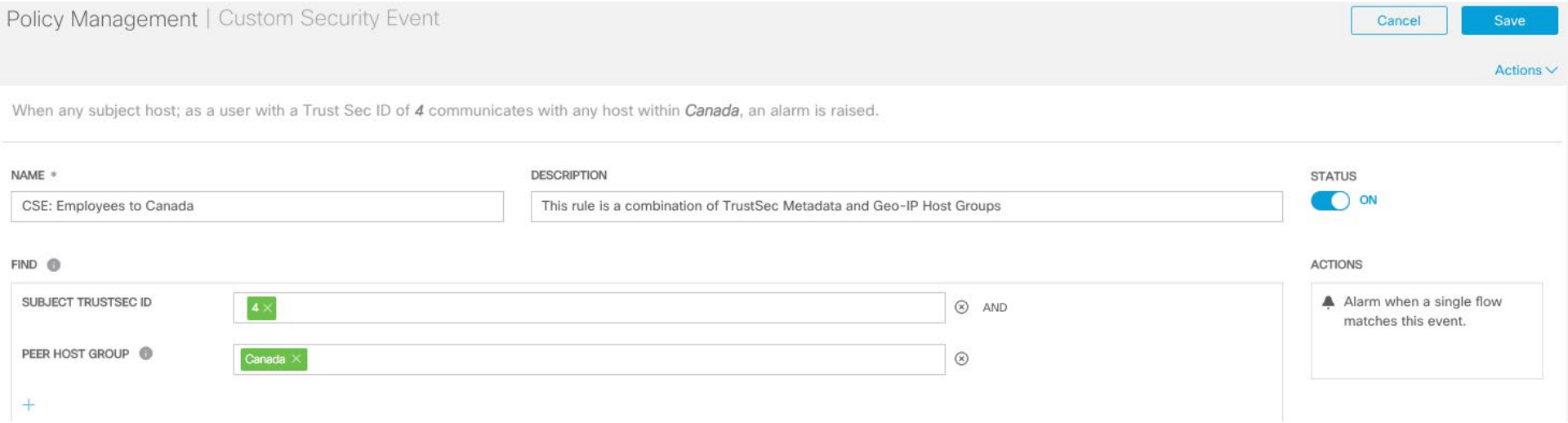
Generate an action when a single flow matches the selected conditions



Allows for the effective modelling and monitoring of policy

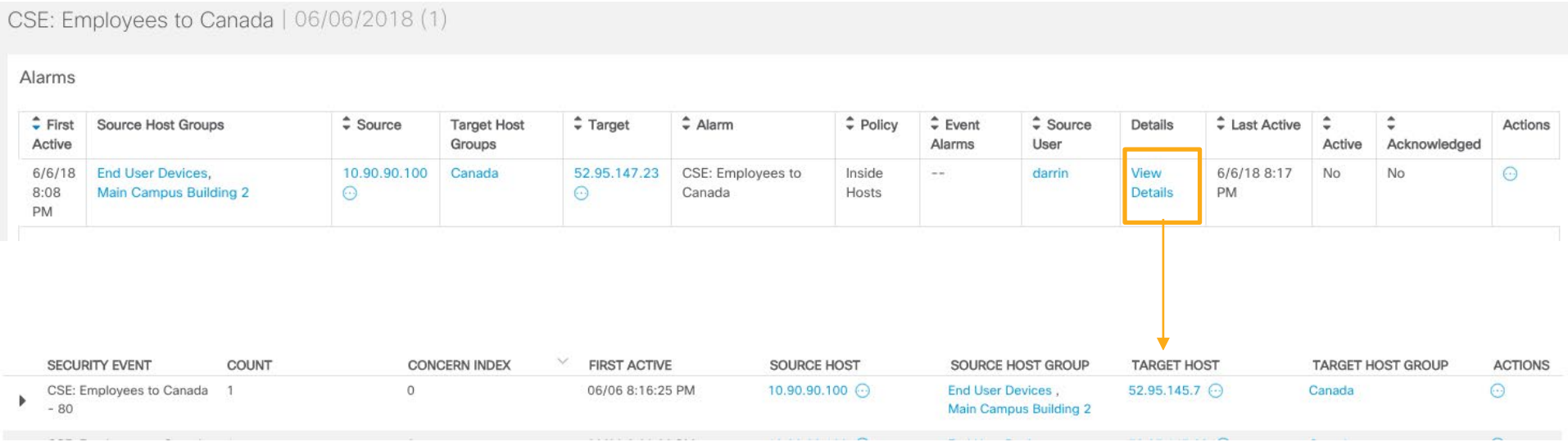
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

CSE using TrustSec/SD Access and Geo-IP Attributes



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

CSE using TrustSec/SD Access Meta Data: Occurrence



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Flow Details of TrustSec/SD Access & Geo-IP CSE

START	SUBJECT IP A...	SUBJECT HO...	SUBJECT USER	SUBJECT PRO...	SUBJECT TRU...	SUBJECT TRU...	APPLICATION	PEER IP ADDR...	PEER HOST G...	PEER TRUSTS...	PEER TRUSTS...
Ex. 06/09/2	Ex. 10.10.10.1	Ex. "catch All"	Ex. john	Ex. chrome.ex	Ex. 7	Ex. jsmith	Ex. "Corporate	Ex. 10.255.25:	Ex. "Catch All"	Ex. 7	Ex. jsmith
Jun 6, 2018 8:13:52 PM (42s ago)	10.90.90.100	End User Devices, Main Campus Building 2	darrin	chrome.exe	4	Employees	HTTP (unclassified)	52.95.145.7	Canada	--	--

General

View URL Data

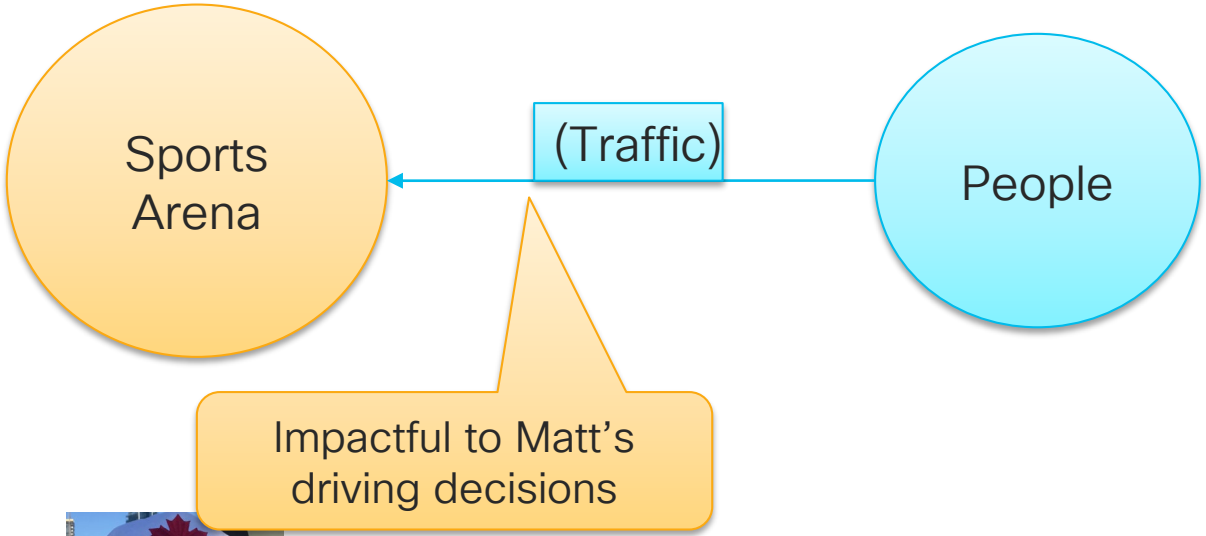
Subject		Totals		Peer	
Packets:	14	Packets:	22	Packets:	8
Packet Rate:	2 pps	Packet Rate:	3.14 pps	Packet Rate:	1.14 pps
Bytes:	980 B	Bytes:	1.72 KB	Bytes:	782 B
Byte Rate:	140 bps	Byte Rate:	251.71 bps	Byte Rate:	111.71 bps
Percent Transfer:	55.62%	Subject Byte Ratio:	55.62%	Percent Transfer:	44.38%
Host Groups:	End User Devices, Main Campus Building 2	RTT:	0seconds	Host Groups:	Canada
Payload:	GET http://beerhoser.ca/	SRT:	0seconds	Payload:	304 304 Not Modified

?

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Custom Security Event Demo

Relationship Events



Stealthwatch Relationship Events

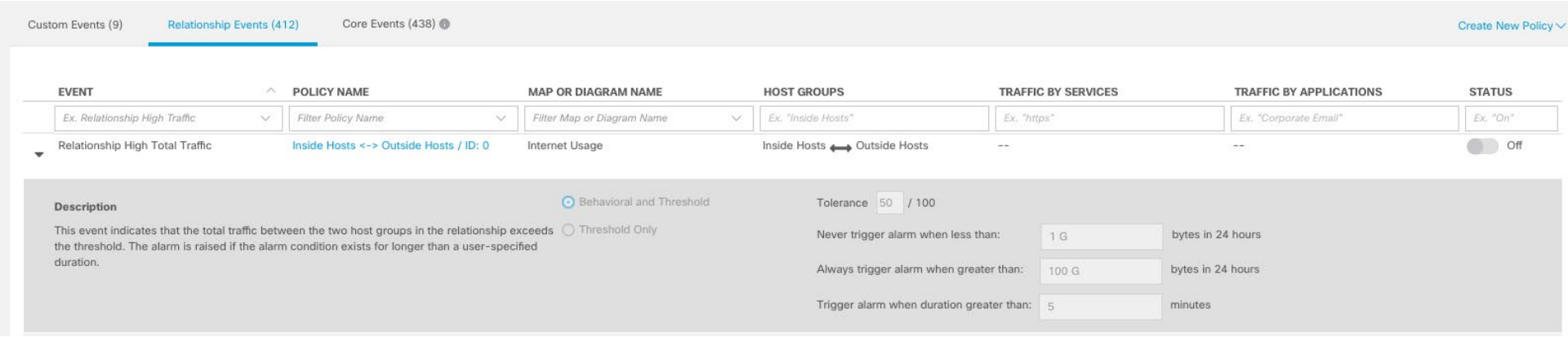
- Interaction between host groups that violate a policy setting

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Stealthwatch Relationship Events

Relationship Events

- Interaction between host groups that violate a policy setting
- Derived from relationships created in network diagram

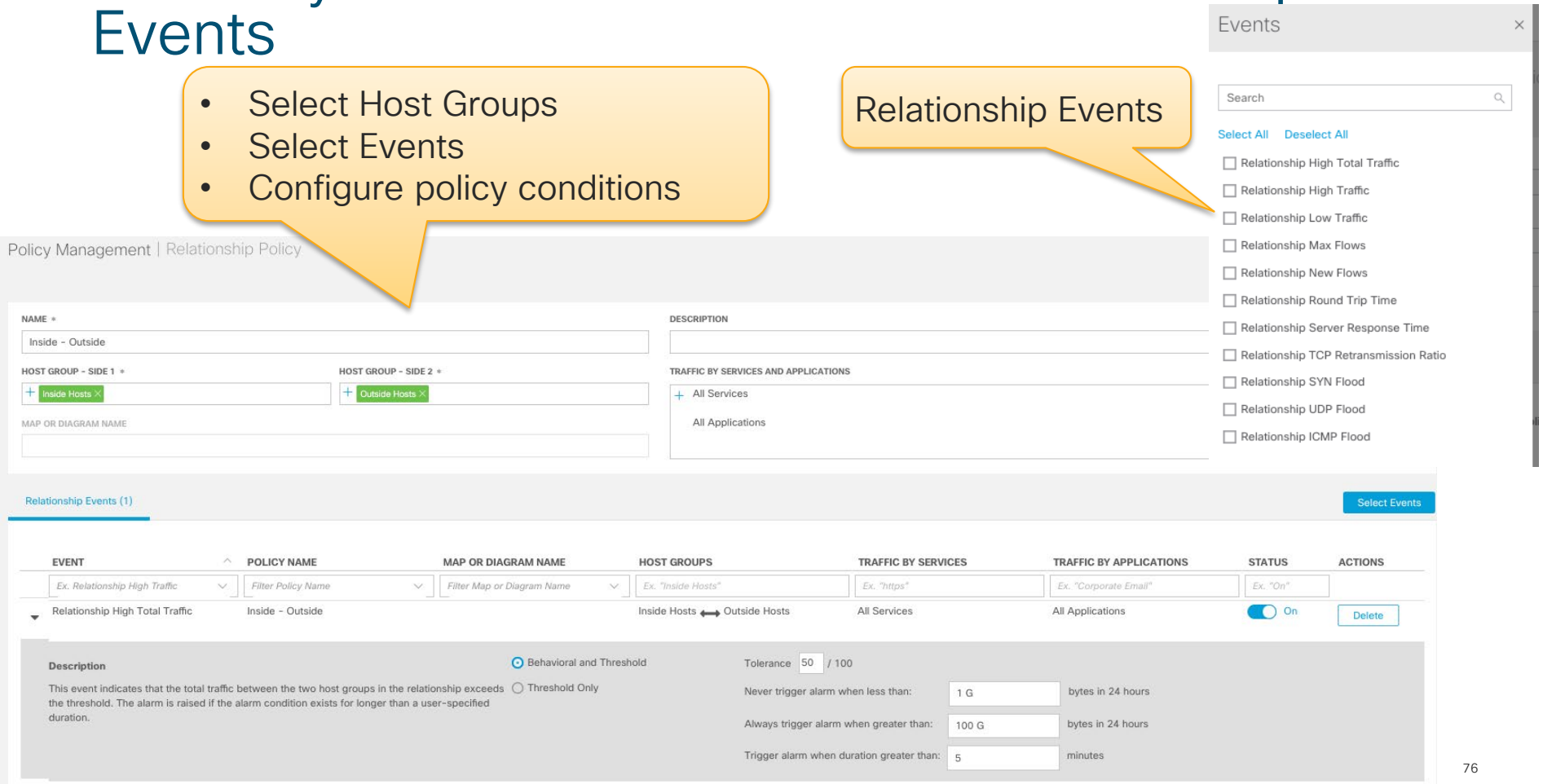


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Manually Created Stealthwatch Relationship Events

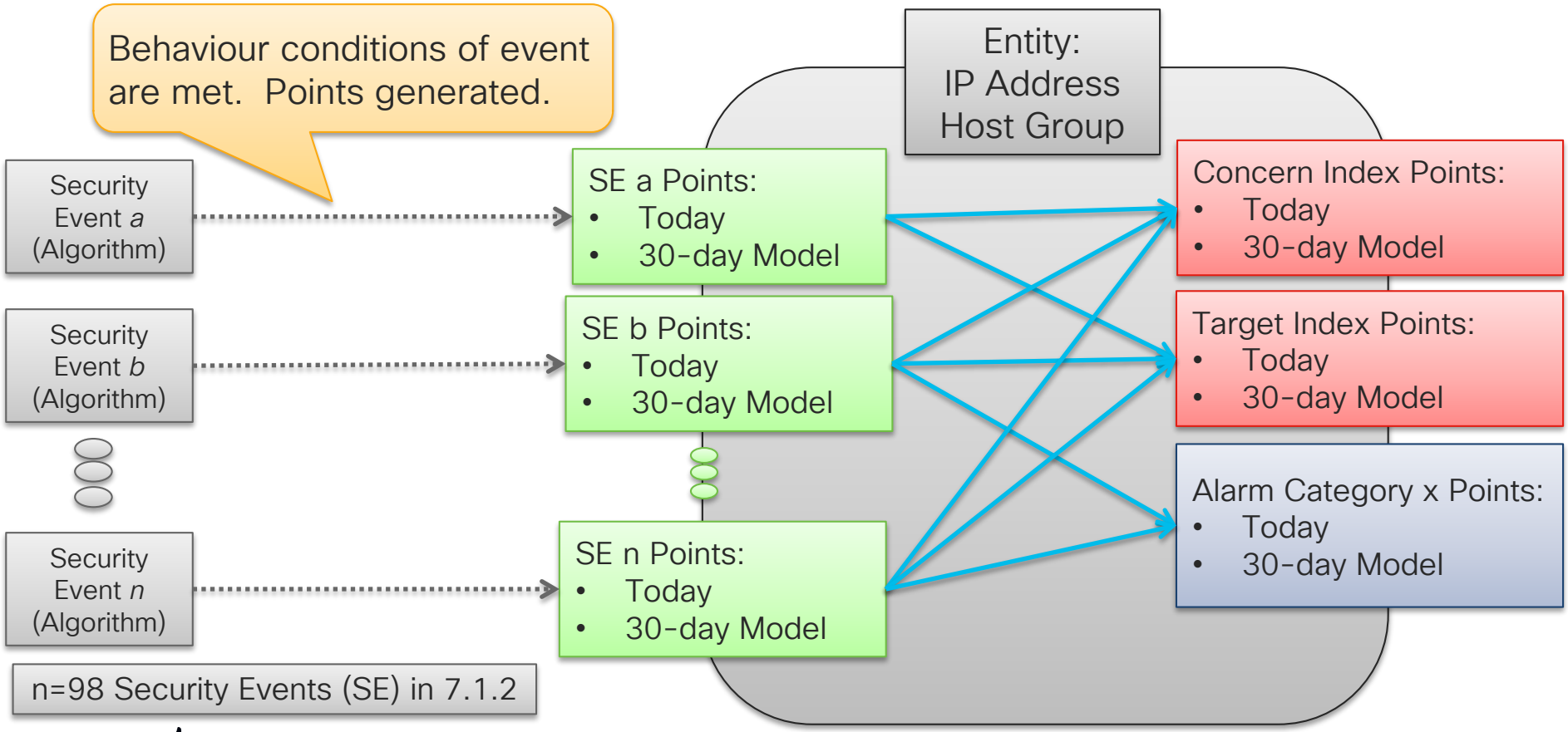
- Select Host Groups
- Select Events
- Configure policy conditions

Relationship Events



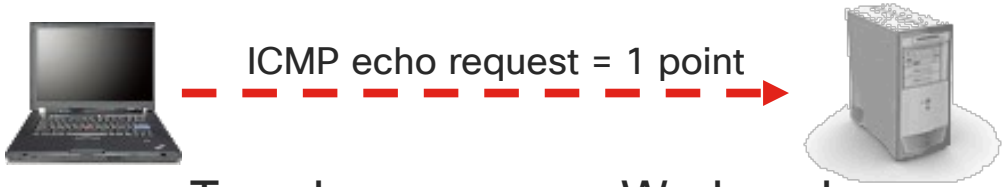
Relationship Events Demo

Stealthwatch Core Events



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

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.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Core Events and Alarm Categories

Cisco Stealthwatch

Security Events and Alarm Categories 7.1

https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/management_console/securit_events_alarm_categories/SW_7_1_Security_Events_and_Alarm_Categories_DV_1_0.pdf

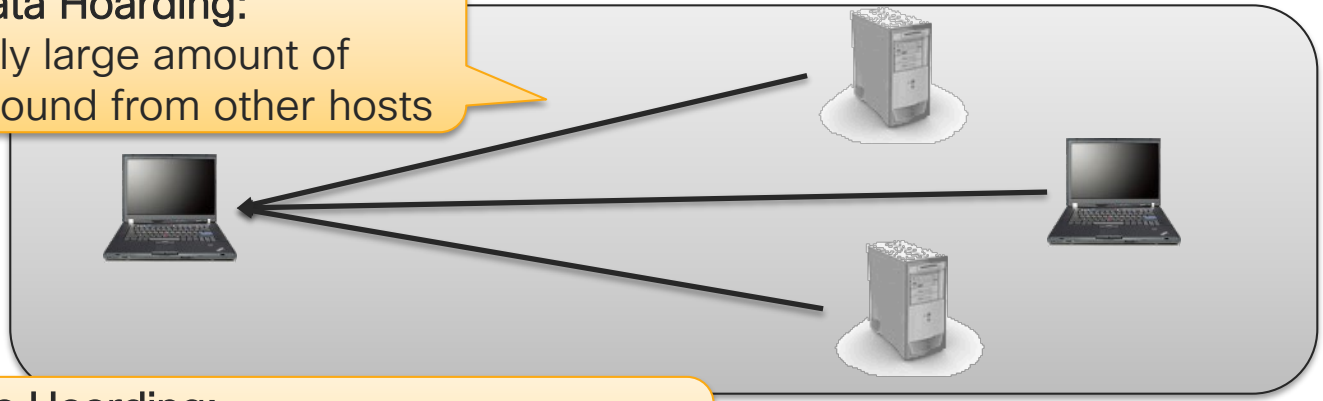
In Stealthwatch 7.1.2:

- 11 High Level Alarm Categories
- 98 Security Events

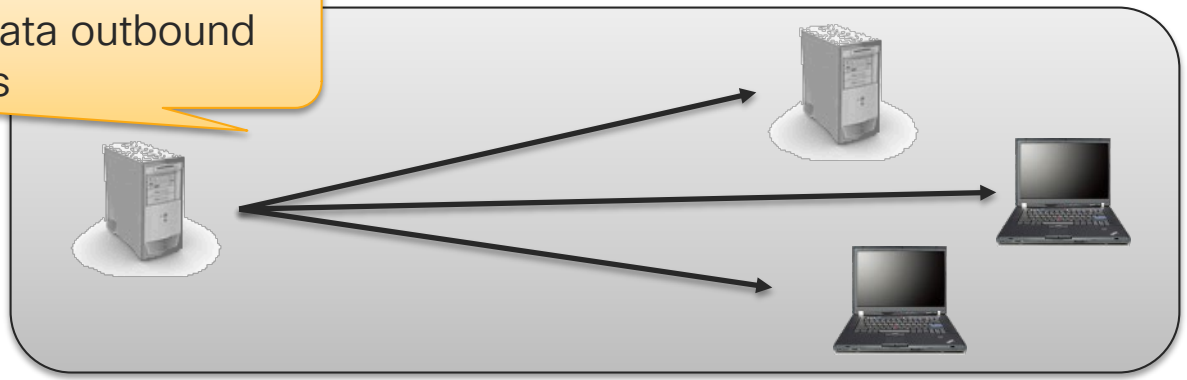
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Example Algorithm: Data Hoarding

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

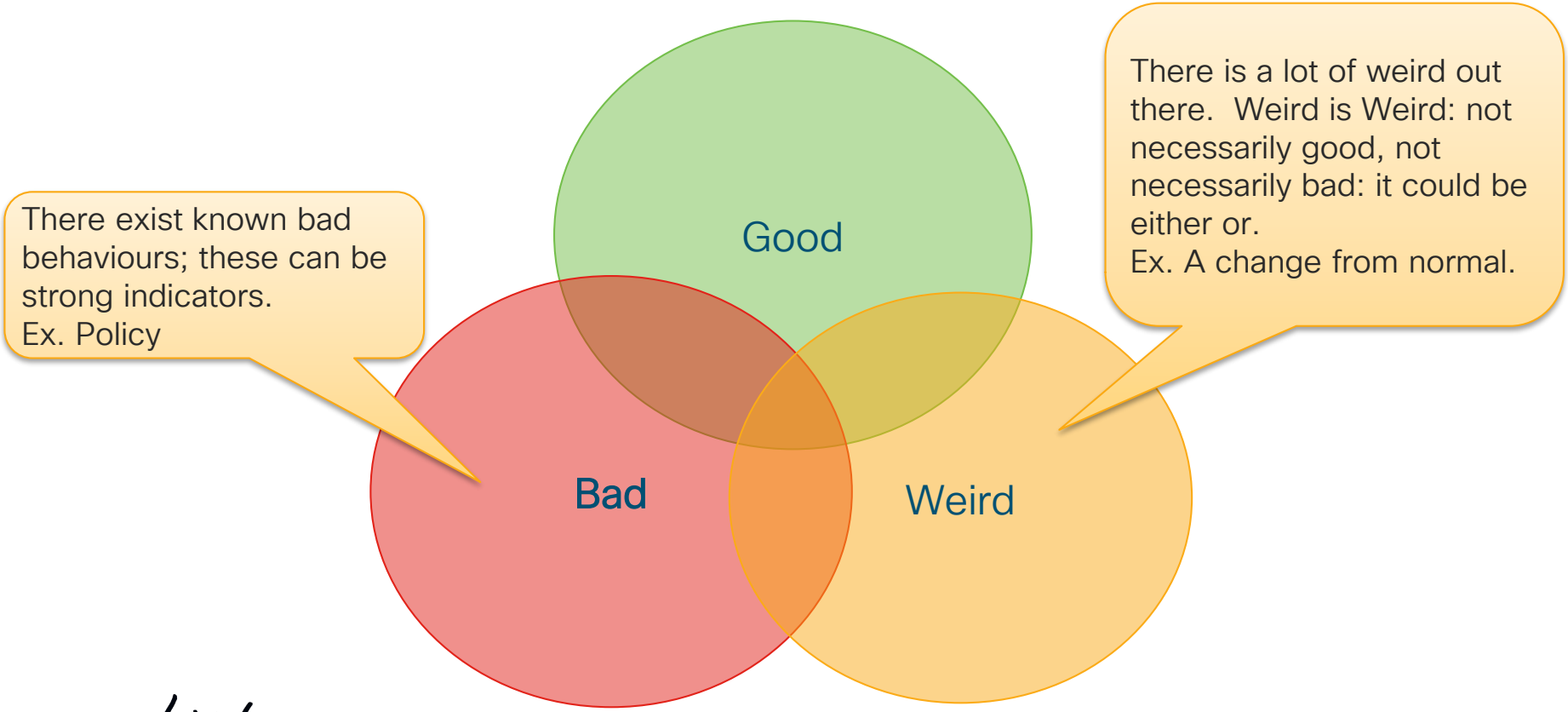


Target Data Hoarding:
- Unusually large amount of data outbound from a host to multiple hosts



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

The Thing about Behaviour



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Data Hoarding Example

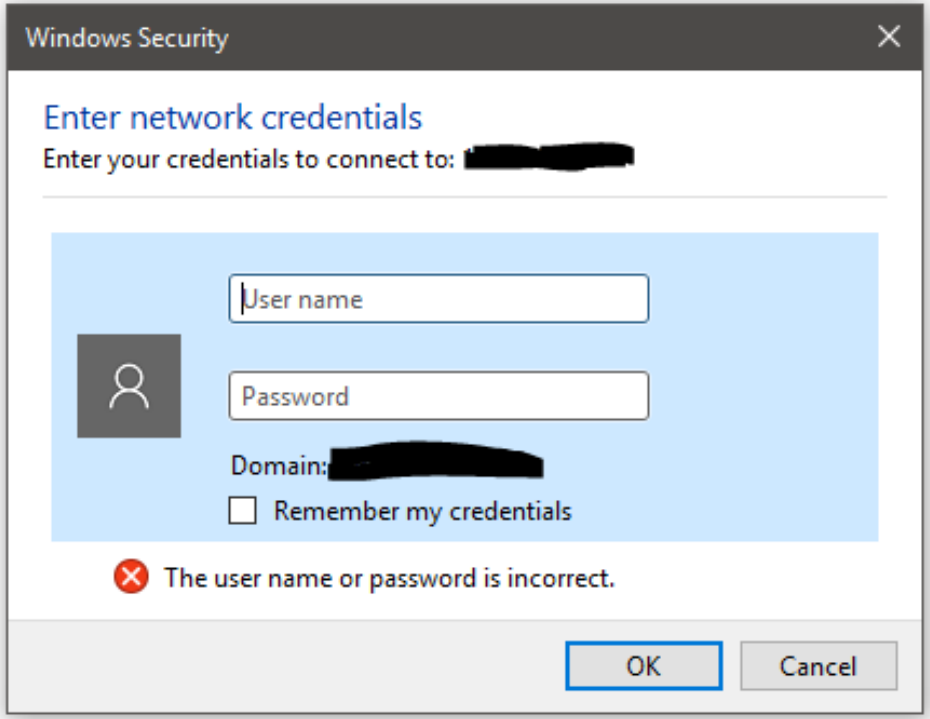
Target Data Hoarding event observed.

Number of east-west flows with this suspiciously familiar size

START	DURATION	SUBJECT IP ADD...	SUBJECT PORT/P...	SUBJECT	APPLICATION	PEER IP ADDRESS	PEER PORT/PRO...	ACTIONS
Ex. 06/09/2017	Ex. <=50min40s	Ex. 10.10.10.10	Ex. 57100/UDP	Ex. <=50	Ex. "Corporate Ema	Ex. 10.255.255.25:	Ex. 2055/UDP	
Jan 30, 2019 11:23:16 AM (31min ago)	22min 1s	10.201.3.20	50999/TCP	4.7G	SMB (unclassified)	10.201.3.2	445/TCP	

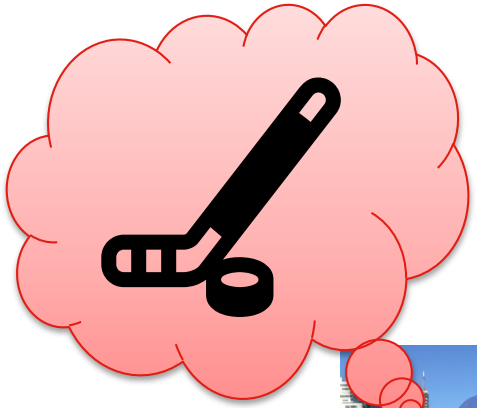
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Connecting to the Host Revealed:



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Making the Alarms Business Relevant

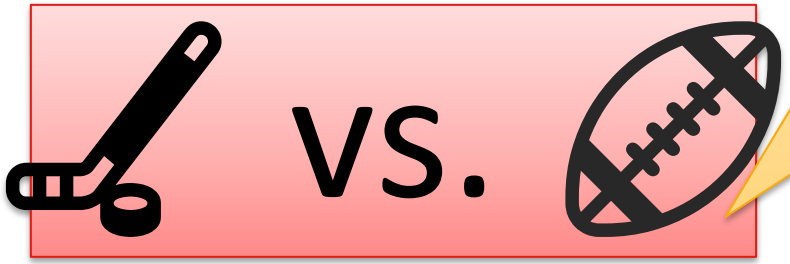


!

37 to 20

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Making the Alarms Business Relevant



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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

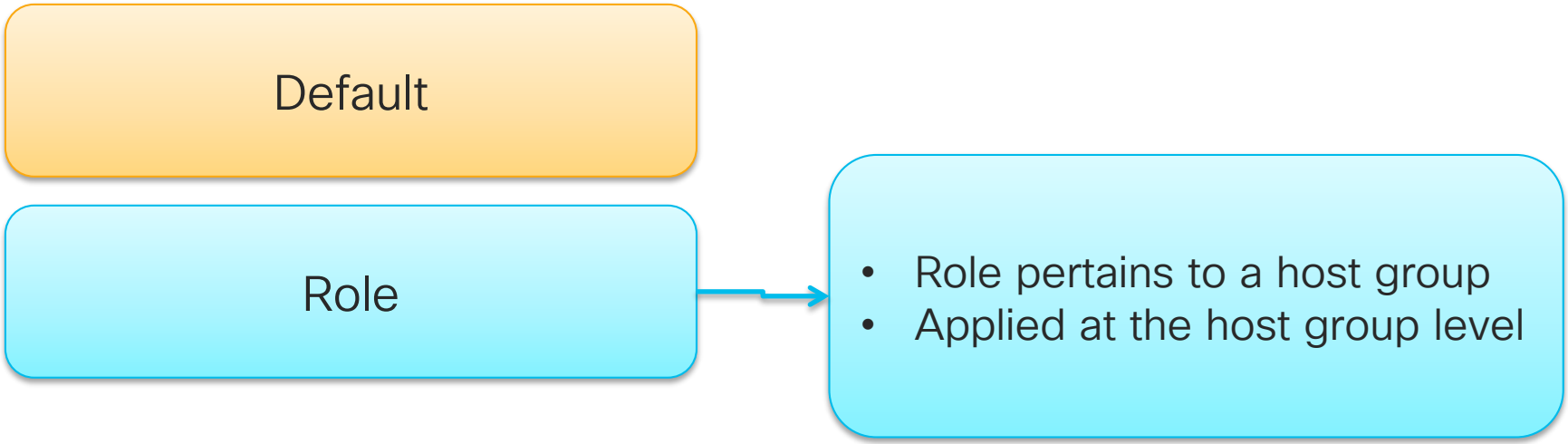
Three Types of Polices

Default

- Default pertains to all Inside and Outside hosts
- Default polices apply when there are no role or host policies assigned
- There are two default policies that have been pre-defined:
  - Inside Hosts host group
  - Outside Hosts host group

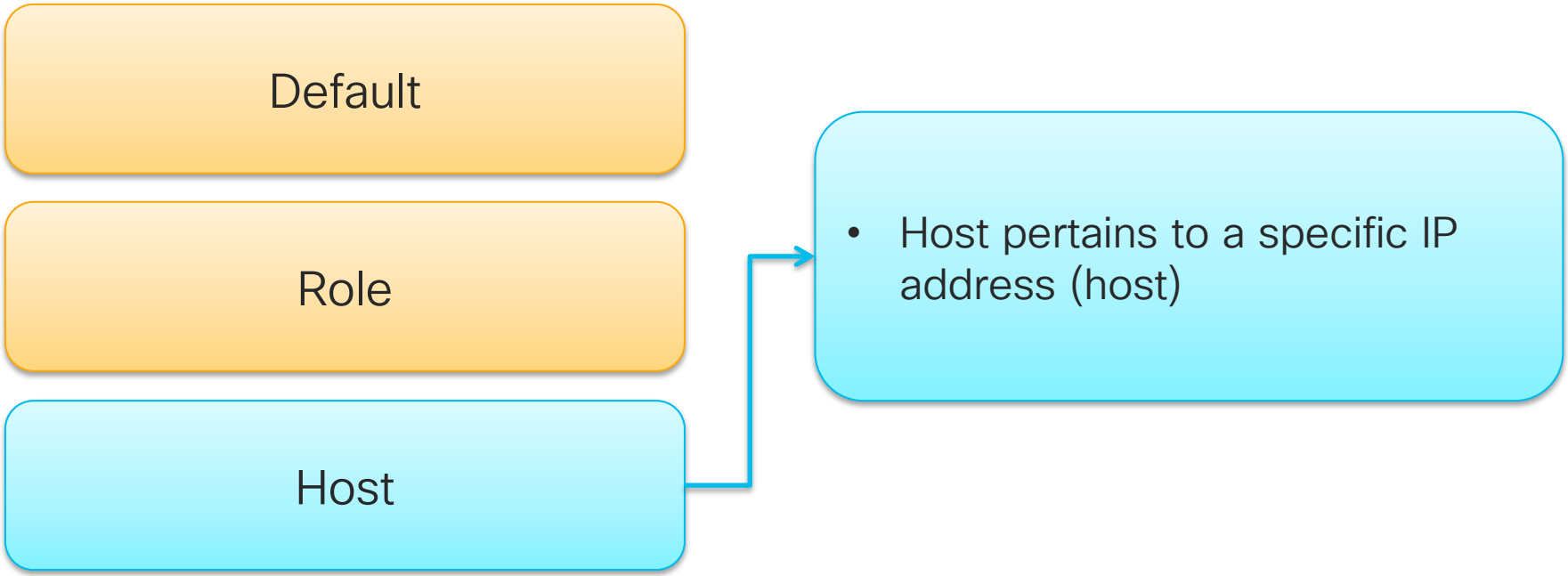
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Three Types of Policies



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Three Types of Policies



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

How Policies are Applied

Default

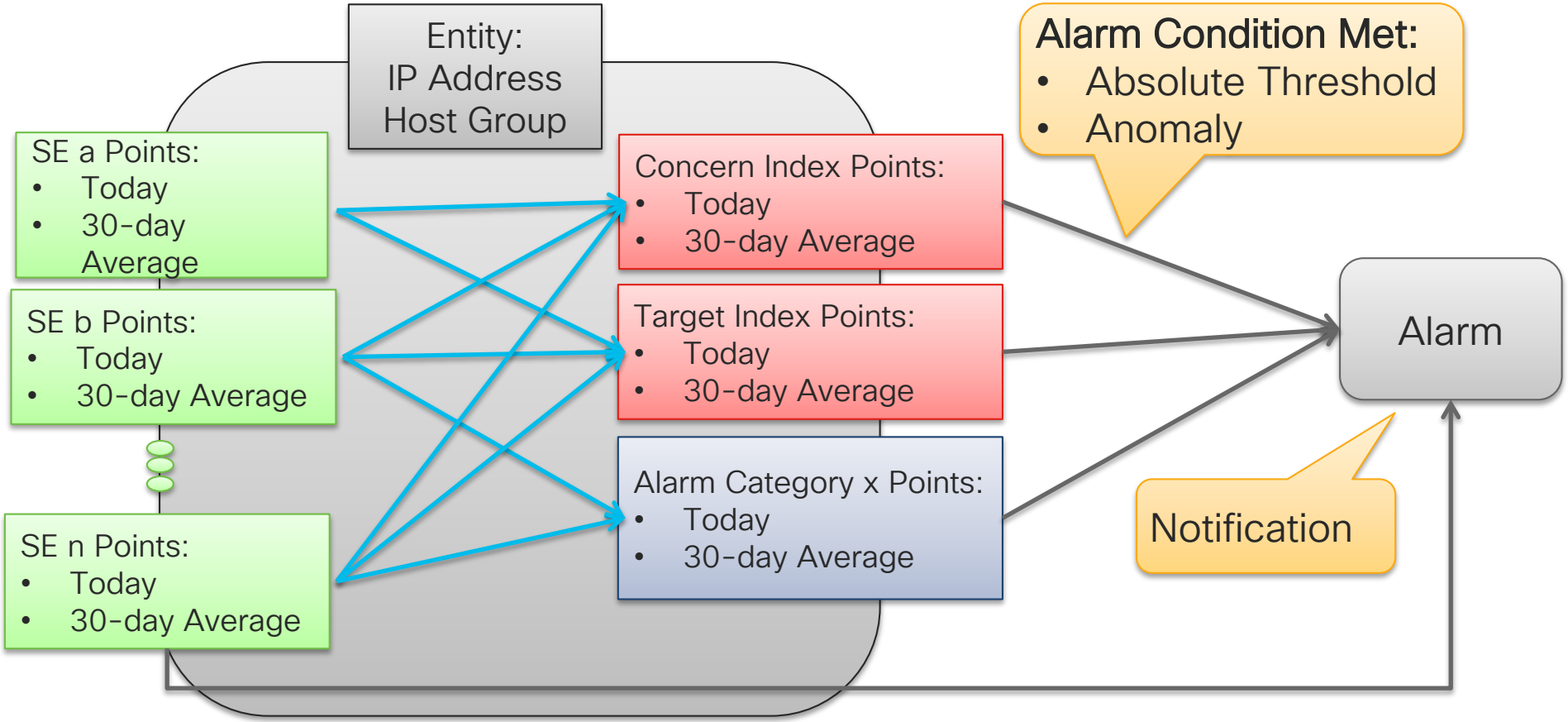
Role

Host

- 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

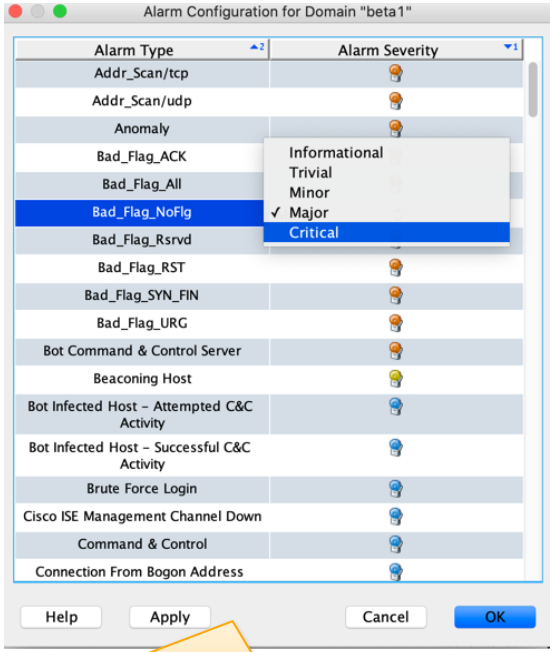
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Stealthwatch Alarming (Notification)

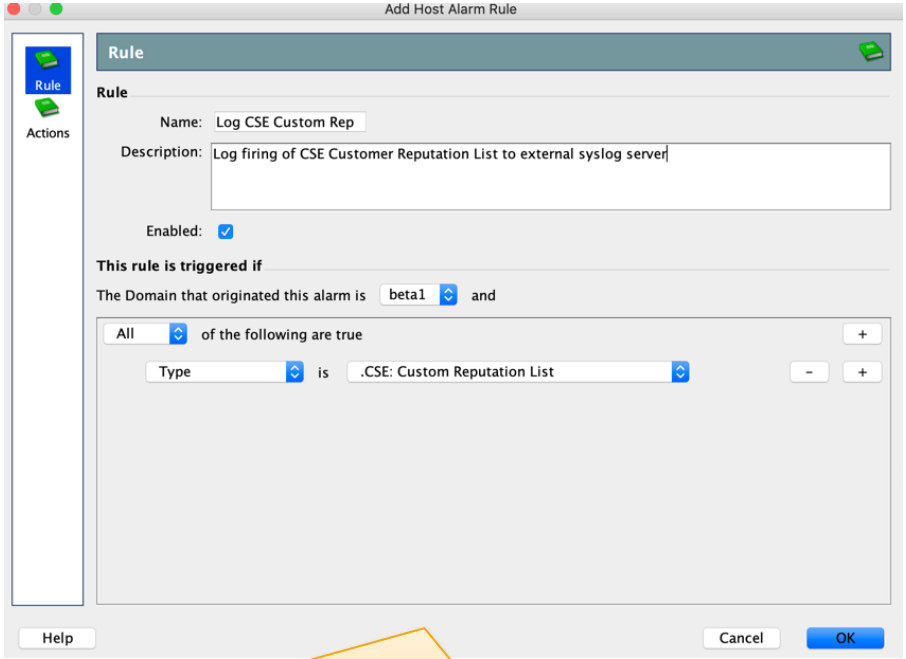


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Alarm Severity and Response Management



Severity of alarm can be set to four levels



Response management setting dictate how an alarm is handled after it is triggered.
Ex. Syslog to an external server

Coming to the WebUI soon!

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

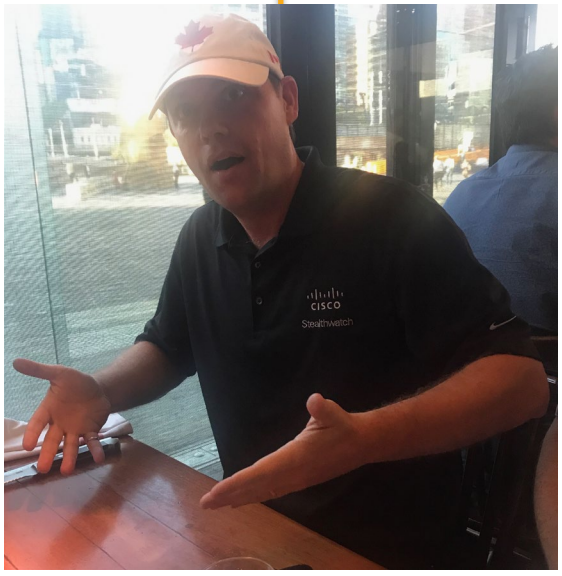
Policy Demos

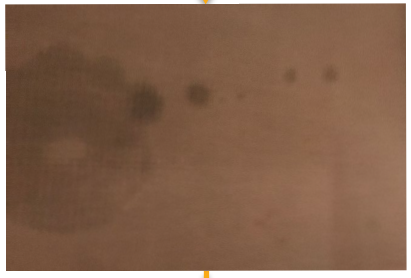
Agenda

- Introduction
- Enabling Visibility and Analytics with Telemetry
- Understanding Security Analytics
- Operationalising Stealthwatch Analytic Engines
- Investigating an Alarm

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Investigating

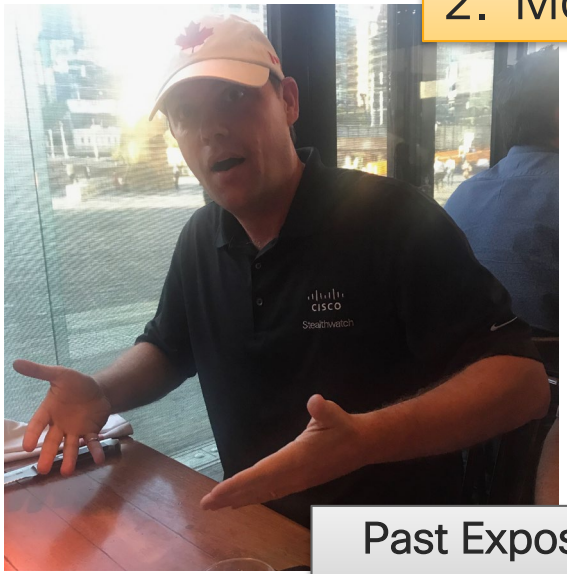




 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Investigating a Breach

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



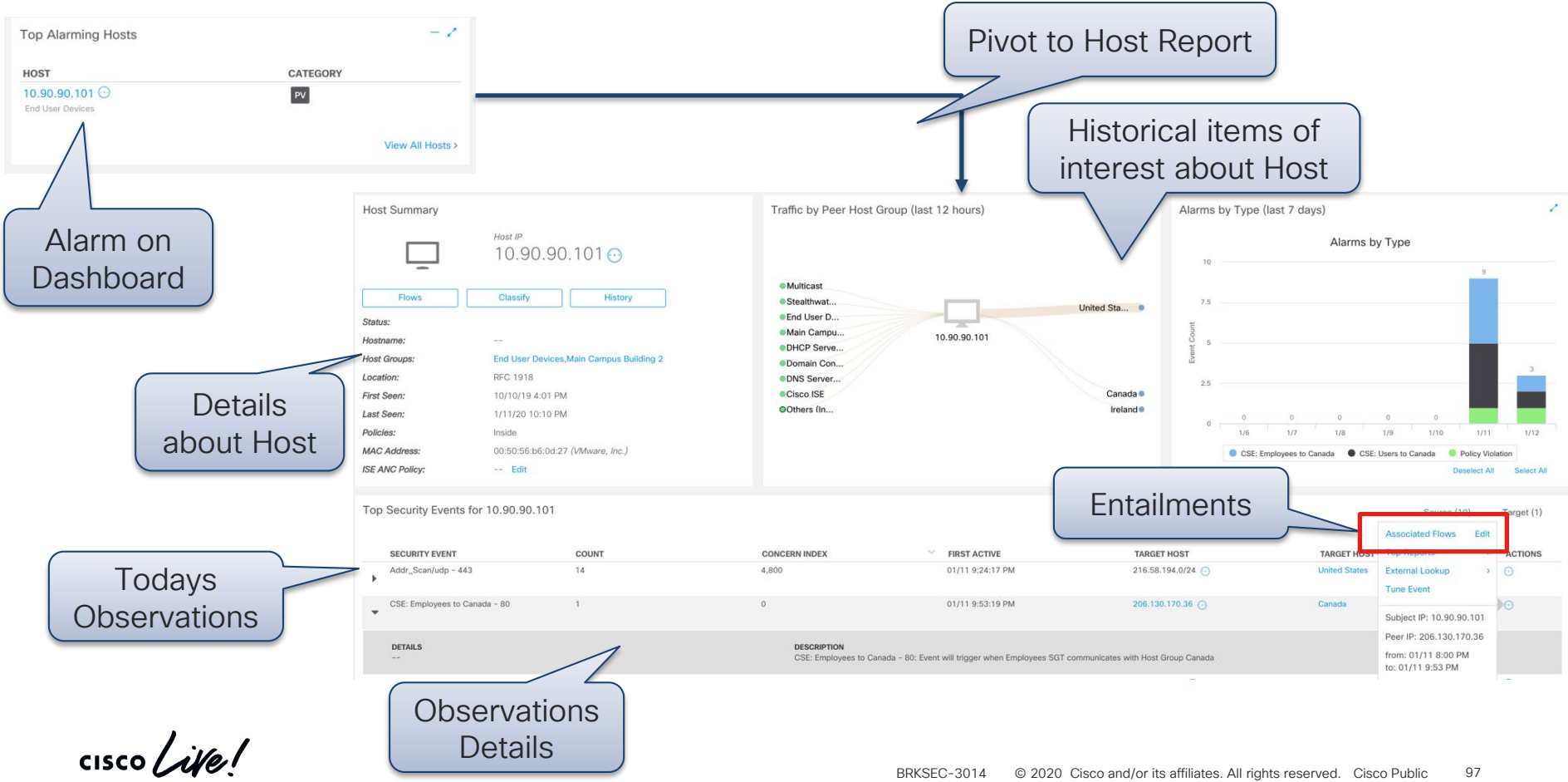
Past Exposure:
I don't have a beer

Darrin Miller:
Beer Thief

Ongoing Exposure:
Prevent Darrin from taking my beer.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

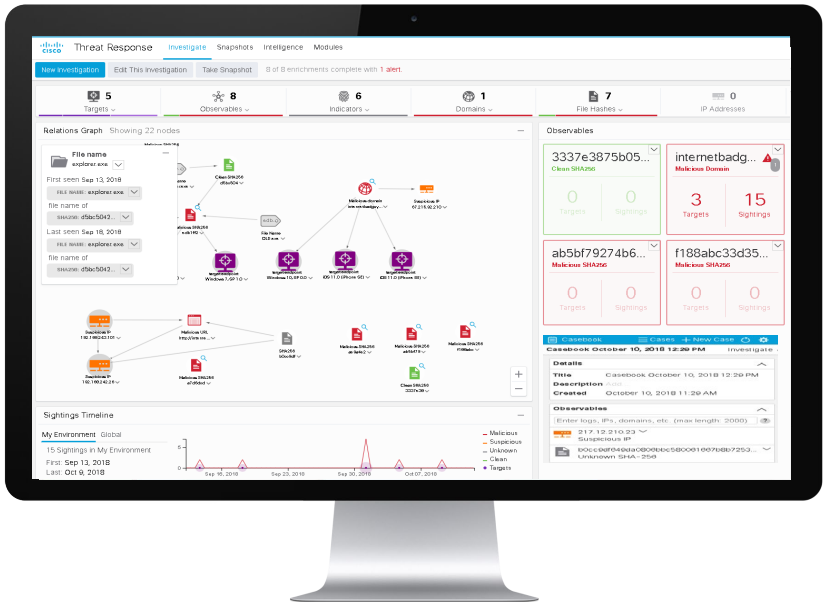
Investigating a Stealthwatch Alarm



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Threat Response (CTR)

BRKSEC-2433 – Threat Hunting and Incident Response with Cisco Threat Response – Ben Greenbaum – Thursday, January 30, 8:30 AM – 10:30 AM



- Automates integrations across Cisco security products
- Reduces the time and effort spent on key security operations functions:
  - Detection
  - Investigation
  - Remediation
- Included as part of Cisco Security product licenses

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Hunting workflow

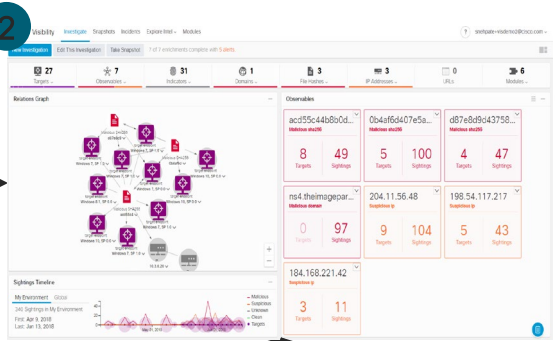
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Hunting workflow

1

Talos or other intel sources

2



- Automatically queries integrated products via APIs to enrich investigation
- User can pivot into each integrated product to get more specific as needed for investigation

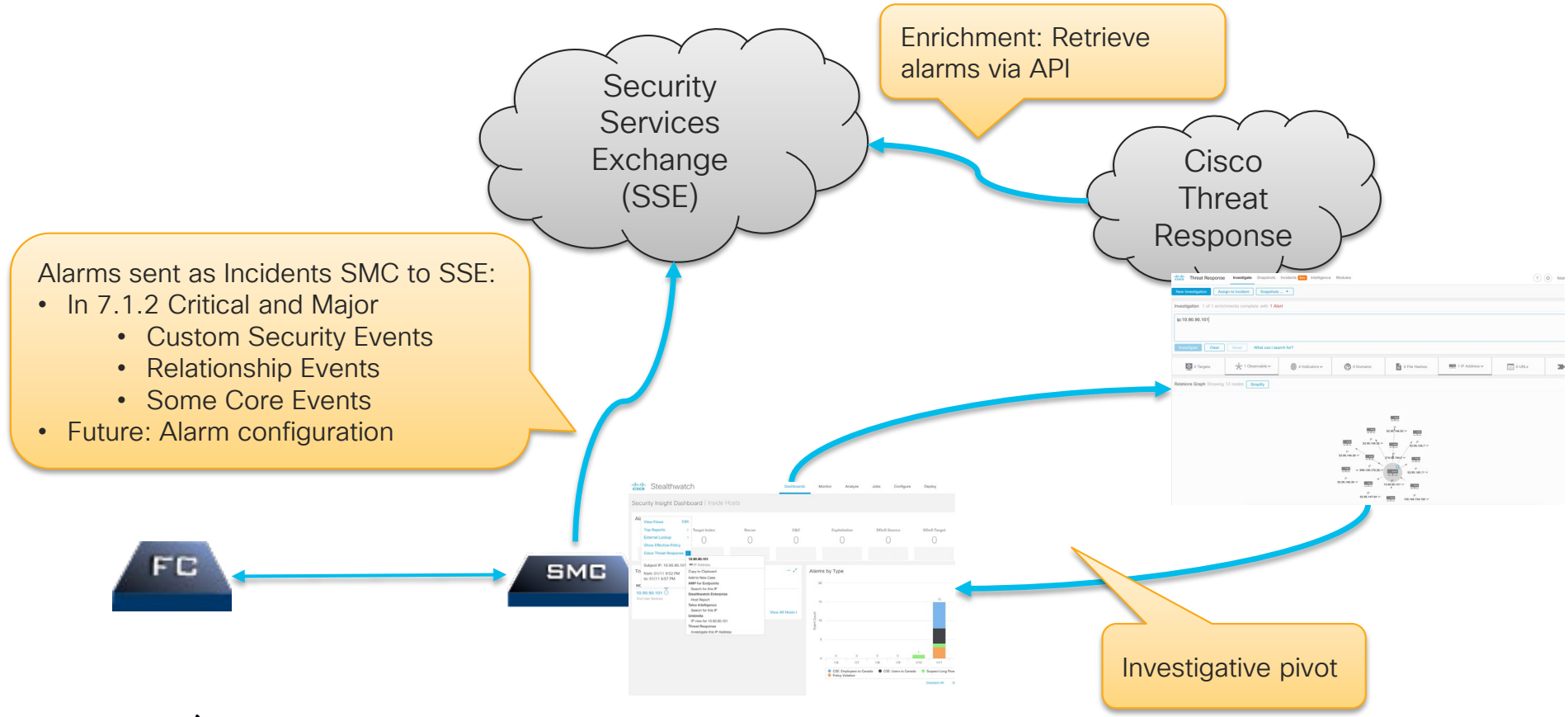
- What do you know about these (IP, Hash, URL, etc.) observables?

- Have we seen these observables?
- Which end-points reached out to the URL?
- Etc.

Virus Total | TALOS | ThreatGrid | ●●● | AMP | Umbrella | Stealthwatch | FTD | More ..

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Stealthwatch and Cisco Threat Response



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

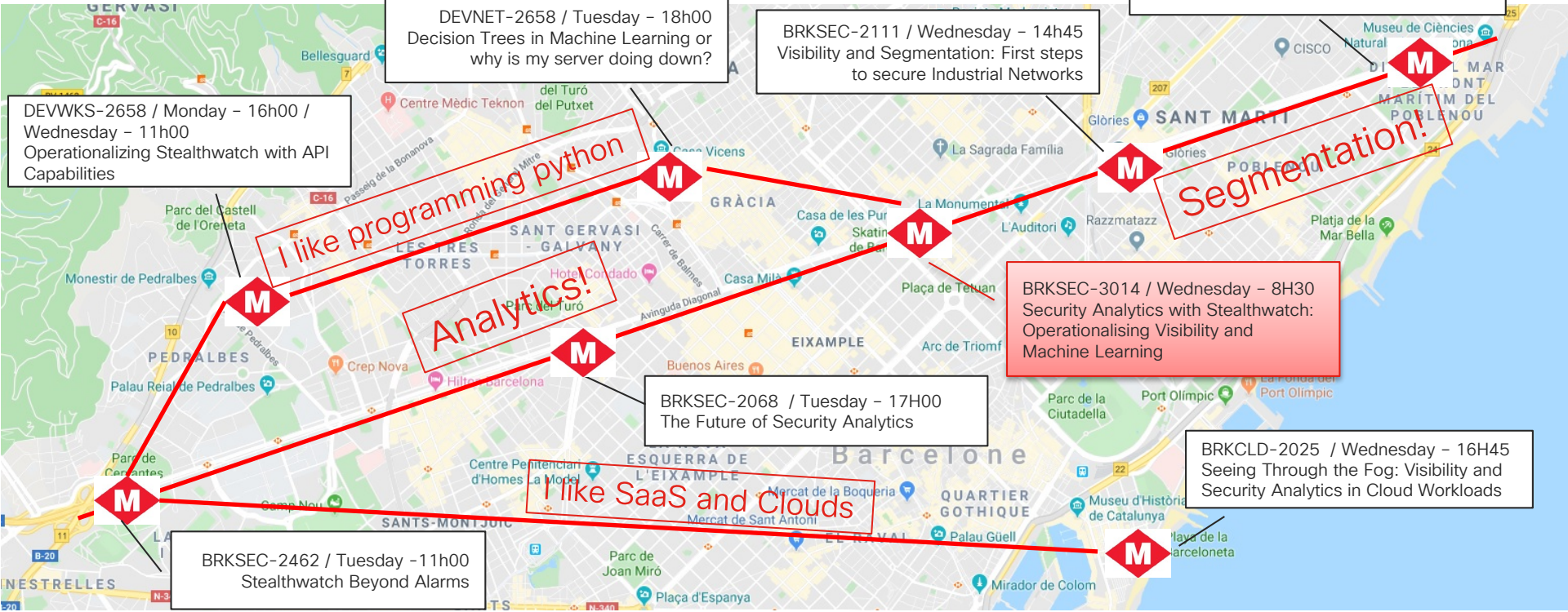
Stealthwatch and CTR Demo

Agenda

- Introduction
- Enabling Visibility and Analytics with Telemetry
- Understanding Security Analytics
- Operationalising Stealthwatch Analytic Engines
- Investigating an Alarm
- Summary

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Security Analytics Learning Map



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Related Sessions

- BRKSEC-3014 – Security Analytics with Stealthwatch: Operationalising Visibility and Machine Learning – Matt Robertson – Wednesday, January 29, 8:30 AM – 10:30 AM
- BRKCLD-2025 – Seeing Through the Fog: Visibility and Security Analytics in Cloud Workloads – Matt Robertson – Wednesday, January 29, 4:45 PM – 6:15 PM
- BRKSEC-2462 – Stealthwatch Beyond Alarms – Hanna Jabbour – Tuesday, January 28, 11:00 AM – 1:00 PM
- BRKSEC-2068 – The Future of Security Analytics – TK Keanini – Tuesday, January 28, 5:00 PM – 6:30 PM
- BRKSEC-2111 – Visibility and Segmentation: First Steps to Secure Industrial Networks – Francesca Martucci – Wednesday, January 29, 2:45 PM - 4:15 PM
- BRKSEC-2433 – Threat Hunting and Incident Response with Cisco Threat Response – Ben Greenbaum – Thursday, January 30, 8:30 AM – 10:30 AM
- LABSEC-1674 – Beat the Encrypted Traffic with Cisco Stealthwatch ETA – Sebju Varghese, Krishna Mall – Walk in Lab
- DEVWKS-1545 – DevNet Workshop – Operationalizing Stealthwatch with API Capabilities – Kyle Winters, Benjamin Mcinnis - Monday, January 27, 4:00 PM – 4:45 AM ; Wednesday January 29, 11:00 AM – 11:45 AM
- DEVNET-2658 – Decision Trees in Machine Learning or why is my server going down? – Alicia Garcia – Tuesday January 28, 6:00 PM - 6:45 PM

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Stealthwatch Value Use Case Menu

This limited collection of use cases highlights the capabilities of Stealthwatch

Threat Detection

- Detecting Beaconing
- Detecting Bogon Traffic
- Detecting Command and Control Traffic Using the Threat Intelligence License
- Detecting Fake Applications
- Detecting Fileless Malware—PowerShell Attacks
- Detecting Internal Brute Force Attacks
- Detecting Lateral Movement
- Detecting Man in the Middle Attacks
- Detecting Password Spray Attacks
- Detecting Rogue DHCP Servers
- Detecting Tor Traffic
- Detecting Rogue DNS Traffic
- Detecting Fragmentation Attacks
- Detecting Targeted Attacks
- Detecting ATM Attacks
- Detecting WannaCry Malware
- Reducing Mean Time To Know
- Detecting Browser-Based Attacks
- Detecting Cryptomining Attacks
- Using Cognitive Intelligence
- Using Cognitive Intelligence and AMP for Network Security
- Detecting Malware in Encrypted Traffic

Compliance

- Identifying Medical Asset Types on the Network
- Managing Stealthwatch Users
- Monitoring Trusted Third Parties
- Using Bi-Directional Policies
- Using the ETA Cryptographic Audit Application
- Using the Visibility Assessment Application
- Verifying Change Control Management
- Detecting Obsolete Encryption Protocols
- Detecting Insecure Protocols
- Detecting Torrent or File Sharing Traffic
- Monitoring Vendor Activity
- Monitoring High Priority Host Groups
- Detecting Fake Applications
- Detecting Rogue and New Devices
- Defining Business Applications
- Detecting Application Access Policy Violation
- Identifying Applications on the Network
- Monitoring Remote Access Users
- Using Custom Security Events to Monitor Firewalls
- Using Encryption Auditing

Incident Response

- Determining if a User Violated Access Policies
- Detecting Users Not Traversing the Web Proxy
- Detecting Unauthorized Hosts in a Bypass VLAN
- Determining if Internet Hosts are Connecting to Internal Servers
- Monitoring Corporate Email
- Using the SMC Web UI for Threat Investigation
- Detecting Top Alarming Hosts on the Network

Network Visibility

- Identifying a Virtual Machine Generating Excessive Traffic
- Investigating NTP Reflection DDoS
- Investigating Unidirectional Traffic
- Using the Host Classifier Application
- Using the Interface Status Report in the SMC Web UI for Network Operations
- Using the SMC Web UI for Network Usage Accounting
- Using Stealthwatch for Network Segmentation and Policy Development

Stealthwatch Cloud

- Investigating IP and Port Scans Using Stealthwatch Cloud
- Investigating Potential Data Exfiltration Using Stealthwatch Cloud
- Investigating Potential Threats Using Stealthwatch Cloud
- Monitoring Cloud Resources Using Stealthwatch Cloud
- Detecting Endpoint Deviations Using Stealthwatch Cloud

Forensic Investigation

- Reporting Internet URL Access
- Using the Interface Status Report for Security Operations
- Using the Security Event Workflow
- Using Top Reports
- Obtaining Historical Conversations for Unauthorized Data Transfer

Alarm Categories

- Alarm Category: Command and Control
- Alarm Category: Anomaly
- Alarm Category: Recon
- Alarm Category: High Concern and High Target Index
- Alarm Category: Data Exfiltration
- Alarm Category: Policy Violation
- Alarm Category: Data Hoarding
- Alarm Category: DDoS
- Alarm Category: Exploitation

© 2018 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.

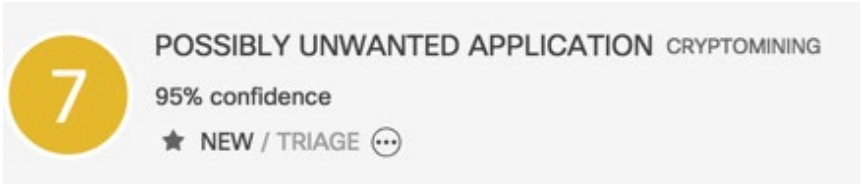
Stealthwatch:
A use case approach to solving crucial network security gaps

Find the use case docs at:

cs.co/StealthwatchValueUseCaseMenu

Key Takeaways

The Cisco Stealthwatch System provides visibility and actionable security intelligence



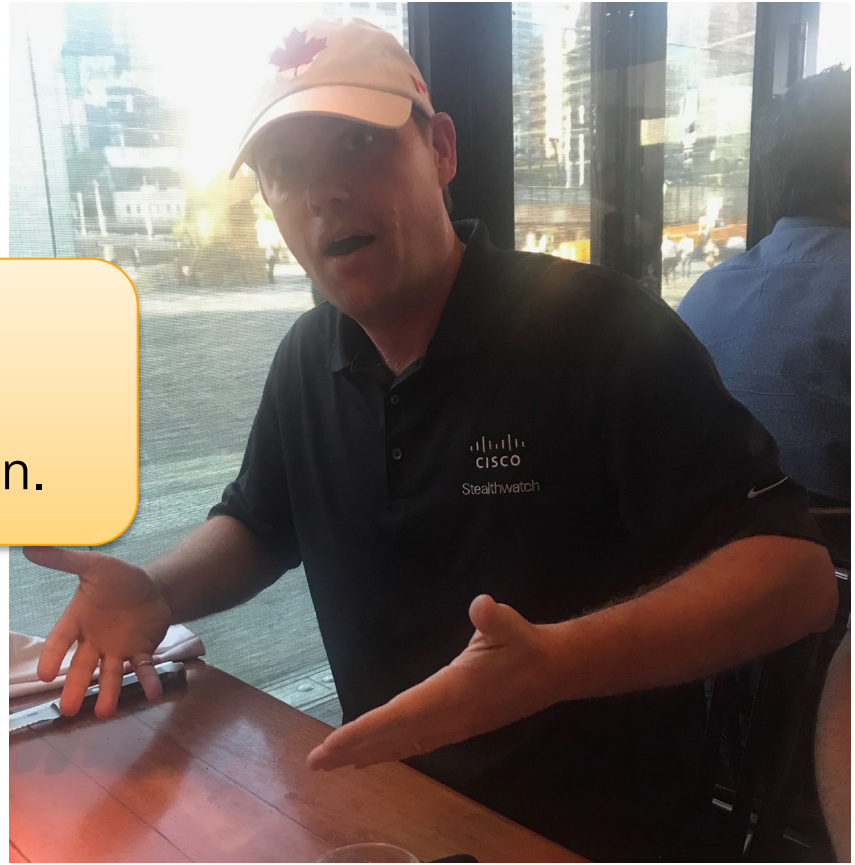
Behaviour analytics are necessary in securing today's networks

Operationalisation of Behavioural observations is context dependent

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Key Takeaways

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



http://www.beerhoser.ca

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Continue your education

Demos in the Cisco Showcase

Walk-In Labs

Meet the Engineer 1:1 meetings

Related sessions

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Complete your online 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 (starting on 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 Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

cisco Live!

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Thank you

cisco Live!

You make **possible**

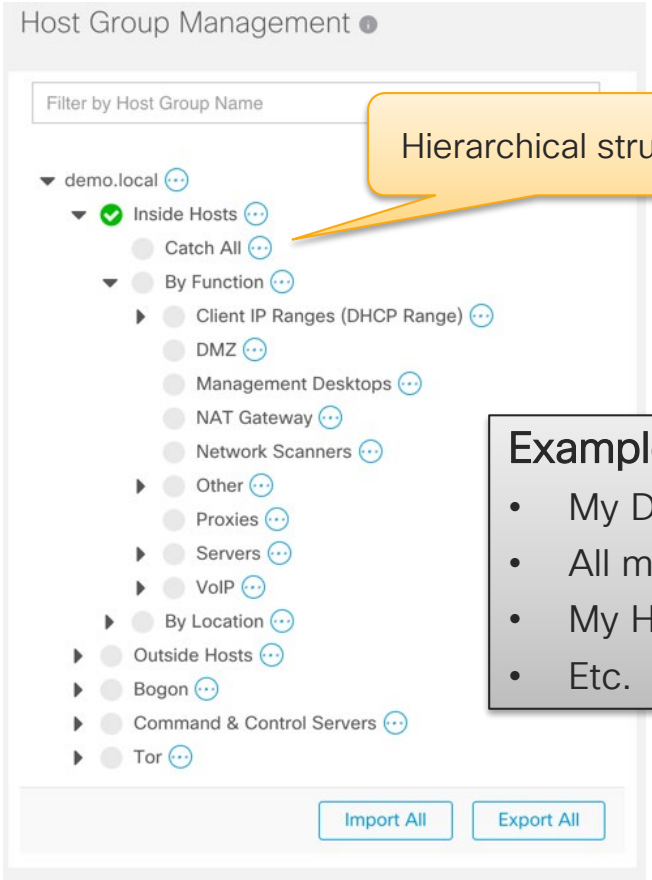
Before we Begin ...

“The world is full of obvious things which nobody by any chance observes.”
Sherlock Holmes, *The Hound of the Baskervilles*

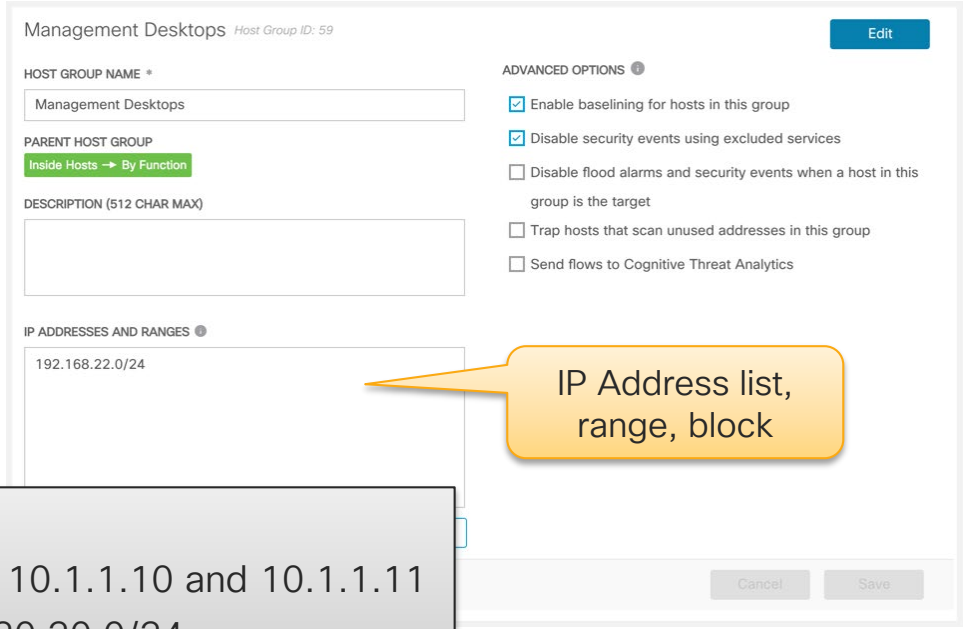
Smart.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Classifying the Network



Hierarchical structure



IP Address list, range, block

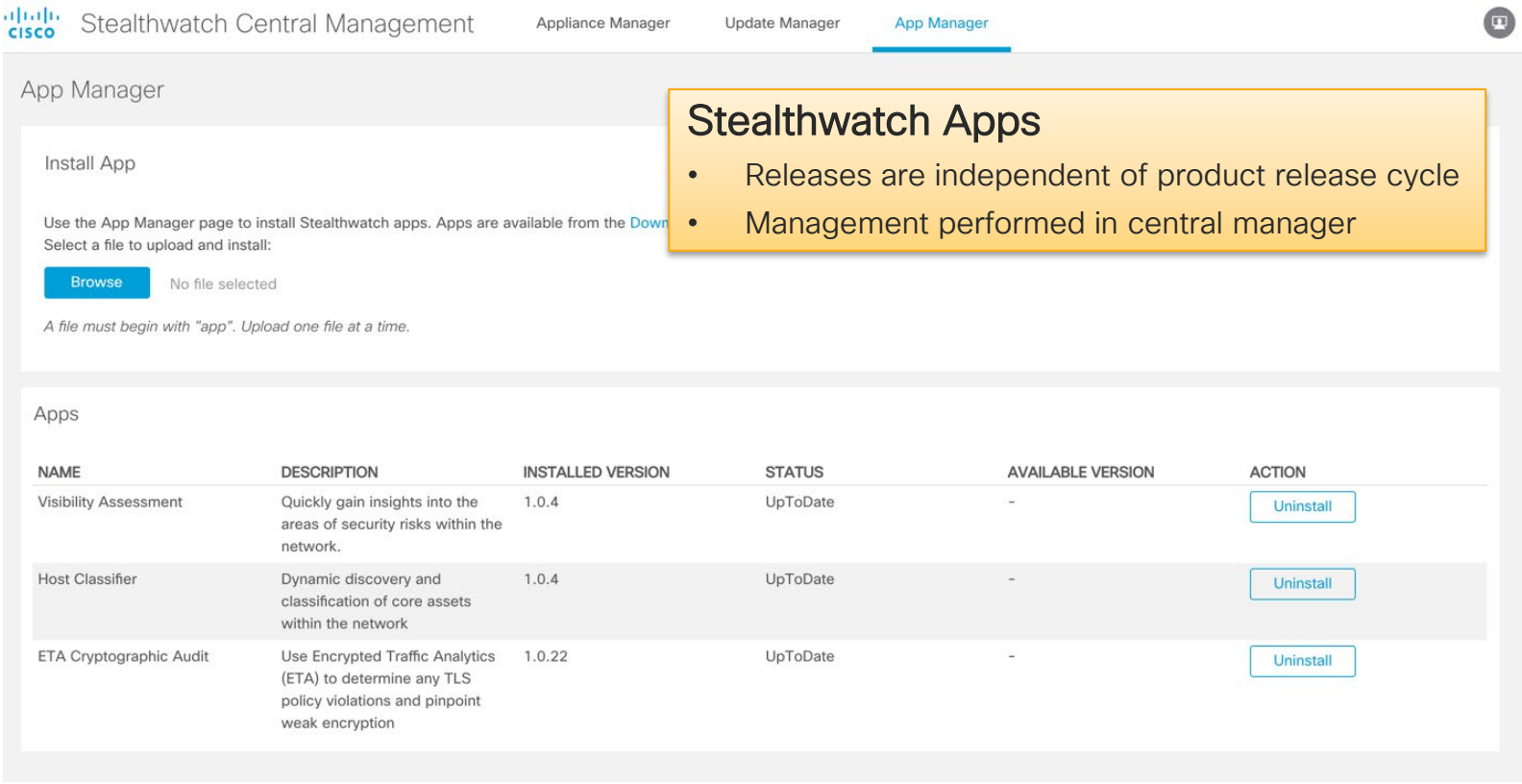
Examples:

- My DNS Servers are 10.1.1.10 and 10.1.1.11
- All my POSs are 10.20.20.0/24
- My 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

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Stealthwatch Apps Management



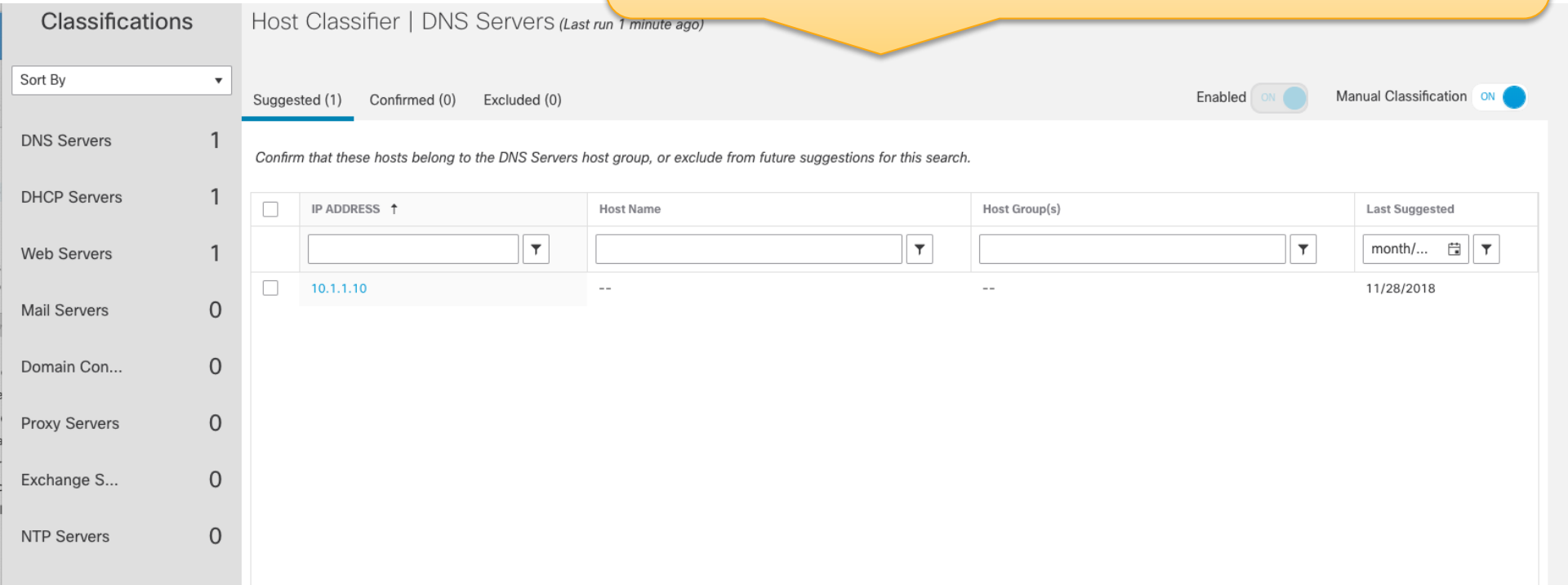
Stealthwatch Apps

- Releases are independent of product release cycle
- Management performed in central manager

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

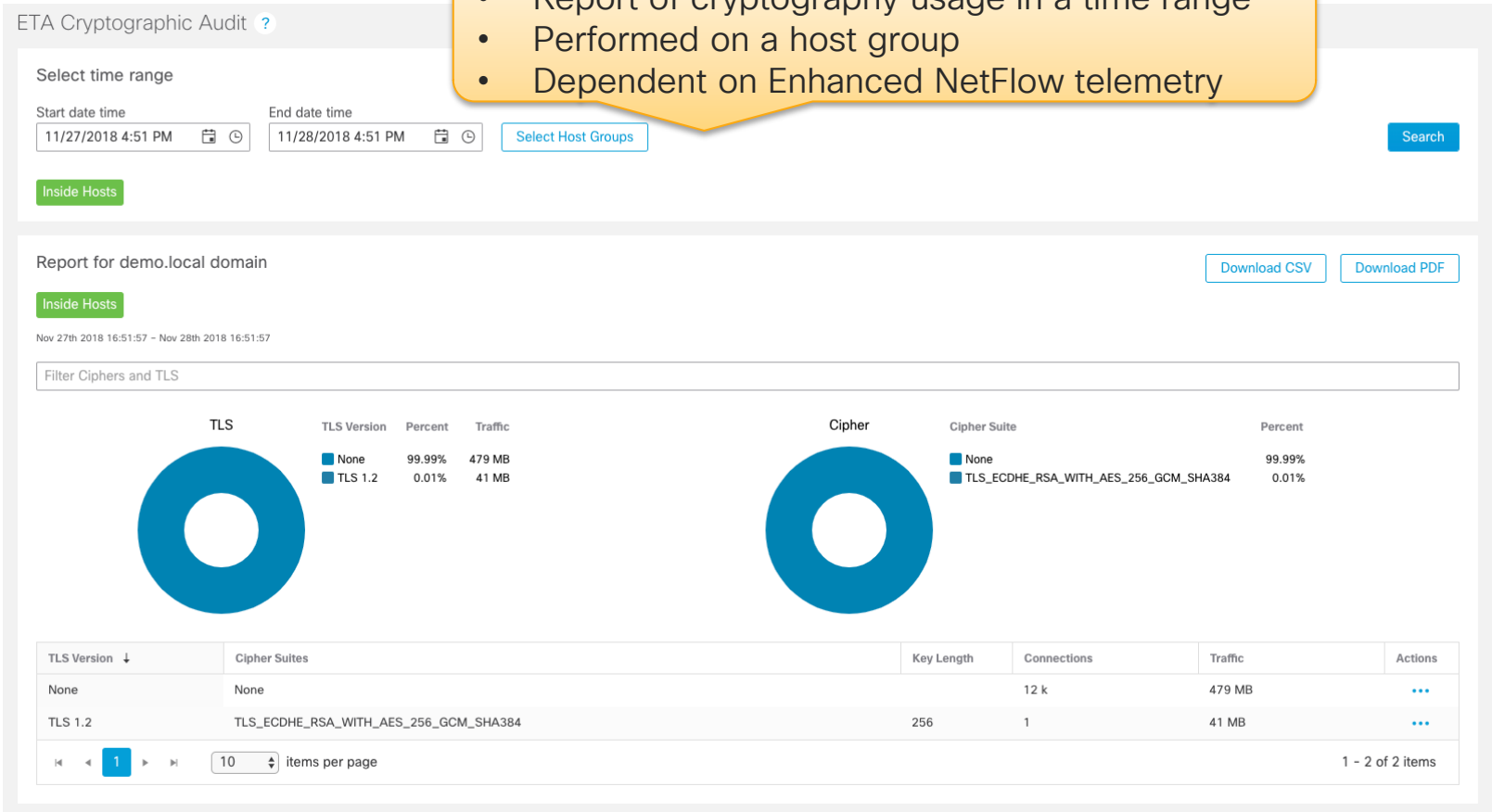
Stealthwatch 7.0: Stealthwatch Host Classifier

- Make suggestions for unclassified hosts into host groups
- User can review and confirm, reject or exclude suggestions



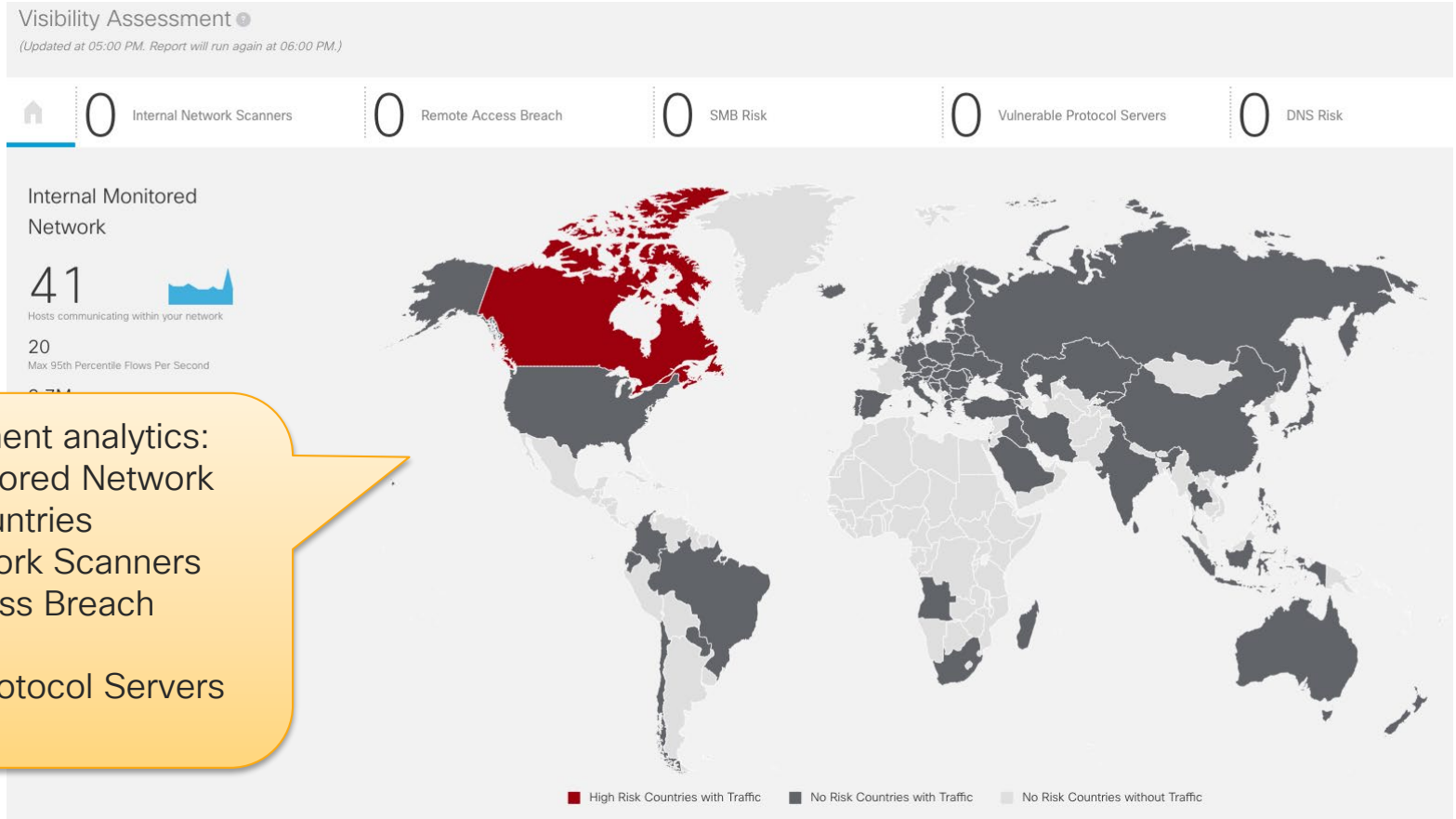
ETA Cryptographic Audit Report

- Report of cryptography usage in a time range
- Performed on a host group
- Dependent on Enhanced NetFlow telemetry



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Visibility Assessment

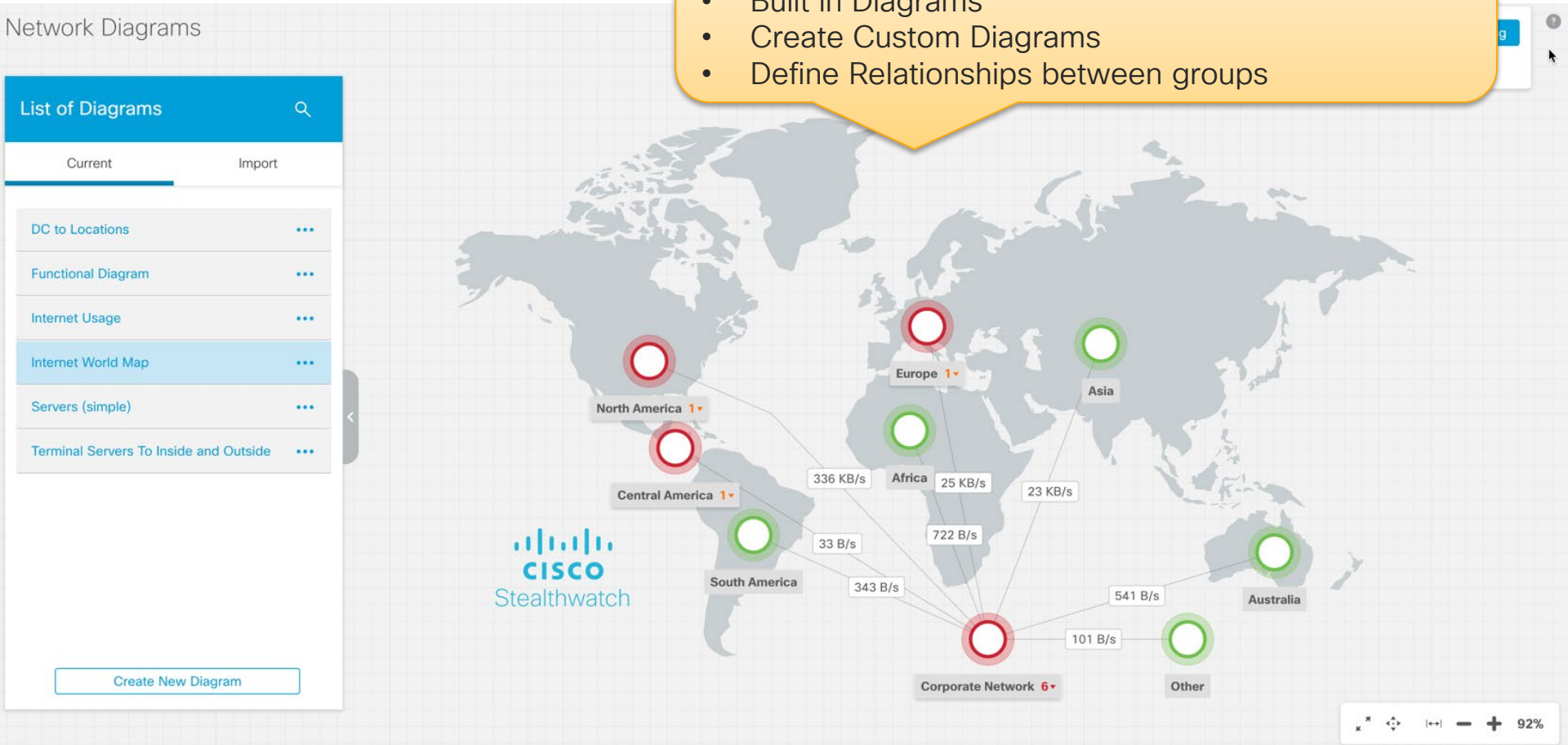


Visibility assessment analytics:

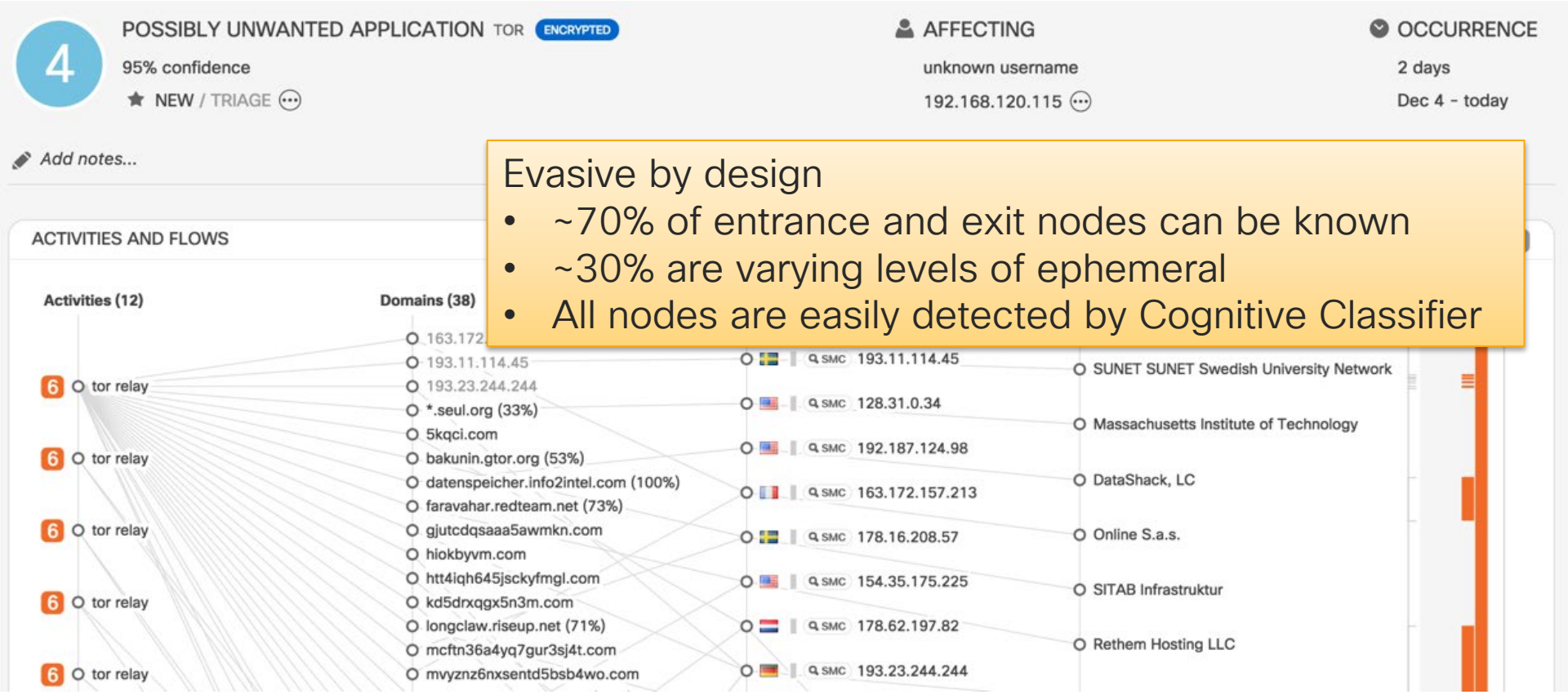
- Internal Monitored Network
- High Risk Countries
- Internal Network Scanners
- Remote Access Breach
- SMB Risk
- Vulnerable Protocol Servers
- DNS Risk

Network Diagrams

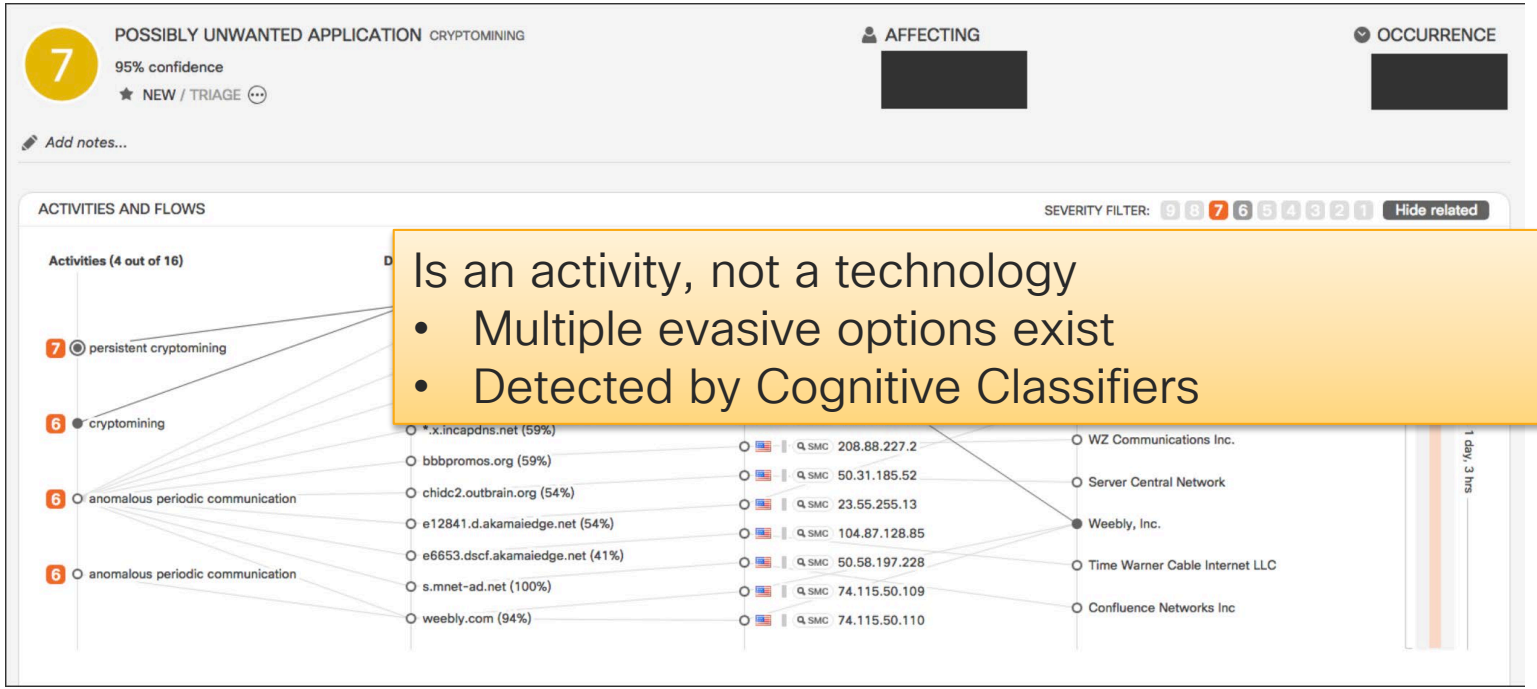
- MAPS!
- Easy visualize communications in your environment
- Built in Diagrams
- Create Custom Diagrams
- Define Relationships between groups



Example: TOR


4
POSSIBLY UNWANTED APPLICATION TOR ENCRYPTED
95% confidence
NEW / TRIAGE
AFFECTING
unknown username
192.168.120.115
OCCURRENCE
2 days
Dec 4 - today
Add notes...
Evasive by design
• ~70% of entrance and exit nodes can be known
• ~30% are varying levels of ephemeral
• All nodes are easily detected by Cognitive Classifier
ACTIVITIES AND FLOWS
Activities (12)
Domains (38)
6 tor relay
6 tor relay
6 tor relay
6 tor relay
6 tor relay
193.11.114.45
193.23.244.244
*.seul.org (33%)
5kqci.com
bakunin.gtor.org (53%)
datenspeicher.info2intel.com (100%)
faravahar.redteam.net (73%)
gjutcdqsaaa5awmkn.com
hiokbyvm.com
htt4iqh645jsckyfmgl.com
kd5drxqgx5n3m.com
longclaw.riseup.net (71%)
mcftn36a4yq7gur3sj4t.com
mvyznz6nxsentd5bsb4wo.com
SMC 193.11.114.45
SMC 128.31.0.34
SMC 192.187.124.98
SMC 163.172.157.213
SMC 178.16.208.57
SMC 154.35.175.225
SMC 178.62.197.82
SMC 193.23.244.244
SUNET SUNET Swedish University Network
Massachusetts Institute of Technology
DataShack, LC
Online S.a.s.
SITAB Infrastruktur
Rethem Hosting LLC

Example: Cryptomining



Is an activity, not a technology

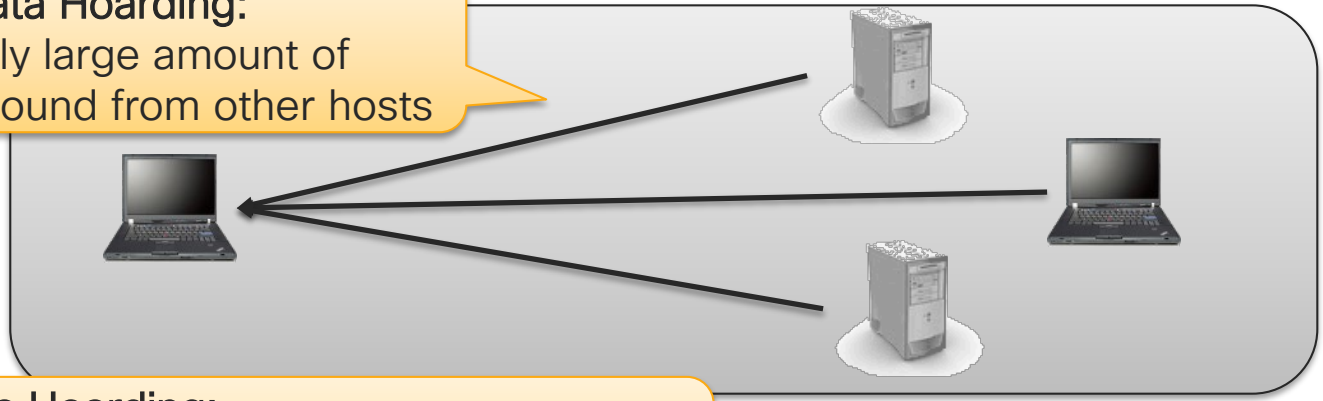
- Multiple evasive options exist
- Detected by Cognitive Classifiers

Example: This incident shows communication to an exotic cryptomining pool. The IP address 74.115.50.111 is strongly associated with cryptomining but is not a commonly used cryptomining pool. The IP address is also associated with a C&C channel for malware. This activity was discovered as a result of an autoupdate to the cryptomining classifier.

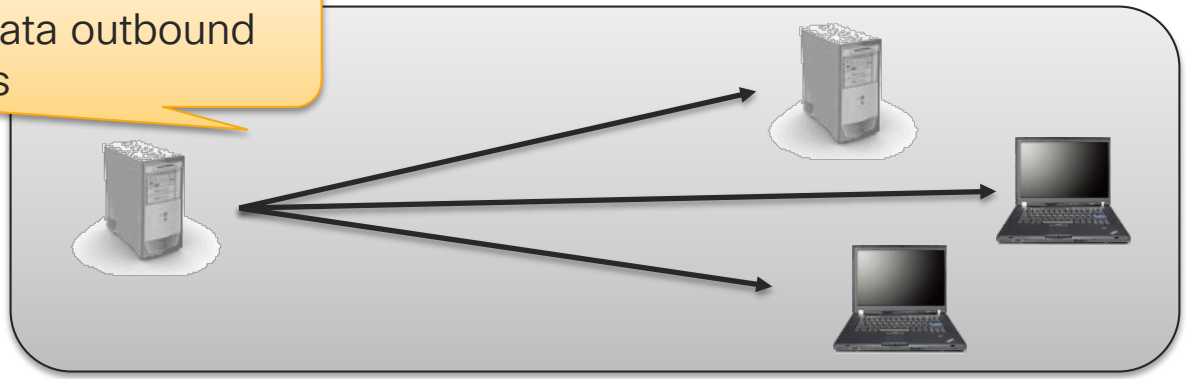
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

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



 © 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Data Hoarding Example

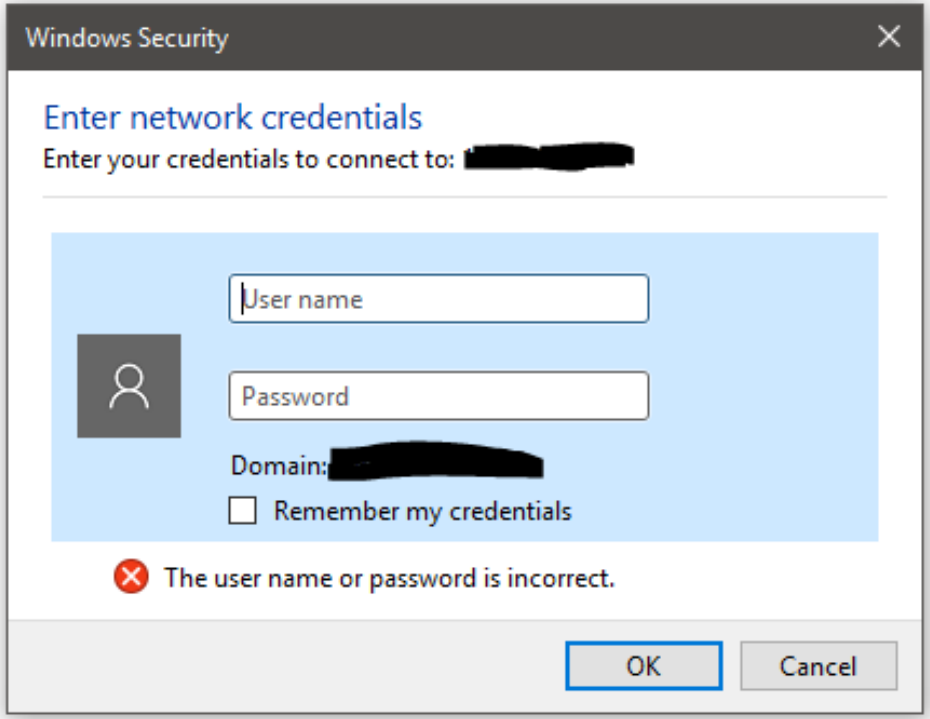
Target Data Hoarding event observed.

Number of east-west flows with this suspiciously familiar size

START	DURATION	SUBJECT IP ADD...	SUBJECT PORT/P...	SUBJECT	APPLICATION	PEER IP ADDRESS	PEER PORT/PRO...	ACTIONS
Ex. 06/09/2017	Ex. <=50min40s	Ex. 10.10.10.10	Ex. 57100/UDP	Ex. <=50	Ex. "Corporate Ema	Ex. 10.255.255.25:	Ex. 2055/UDP	
Jan 30, 2019 11:23:16 AM (31min ago)	22min 1s	10.201.3.20	50999/TCP	4.7G	SMB (unclassified)	10.201.3.2	445/TCP	

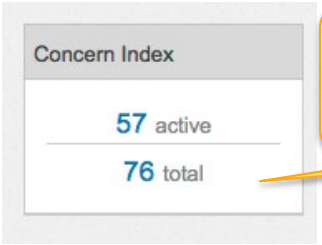
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Connecting to the Host Revealed:

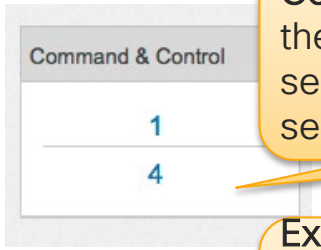


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

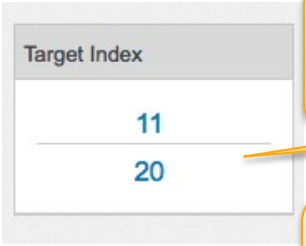
Alarm Categories



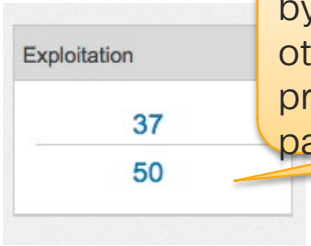
Concern Index: Tracks hosts that appear to be compromising network integrity.



Command and Control: Indicates the existence of bot-infected servers or hosts contacting a C&C servers

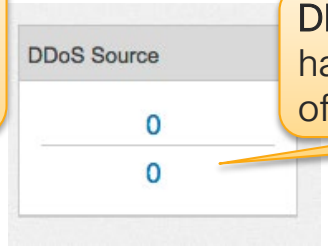


Target Index: Tracks hosts that appear to be victims of other hosts.



Exploitation: Tracks direct attempts by hosts to compromise each other, such as through worm propagation and brute force password cracking.

Recon: Indicates the presence of unauthorised and potentially malicious scanning activity



DDoS Source: Indicates that a host has been identified as the source of a DDoS attack.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Alarm Categories

DDoS Target
0
1

DDoS Target: Indicates that a host as been identified as a the target of a DDoS attack.

Policy Violation
1
45

Policy Violation: The subject is exhibiting behaviour that violates normal network policies.

Data Hoarding
1
5

Data Hoarding: Indicates that a source or target host within a network has downloaded an unusual amount of data from one or more hosts.

Anomaly
0
0

Anomaly: Tracks events that indicate that hosts are behaving abnormally or generating traffic that is unusual but is not consistent with another category of activity.

Exfiltration
0
4

Exfiltration: Tracks inside and outside hosts to which an abnormal amount of data has been transferred.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Best Practice Approach to Tuning Policy

Step 1: Define the Monitored Network
- Build Host Groups

Step 2: Create Custom Events
- These are the “Known Bad”
- Leverage “By Function” Host Groups
- BRKSEC-2026 for more on security policy

Step 3: Create Role Policy Framework
- Ensure policies are tied to functional groups
- Recommended order:
  - Network scanners
  - Server types
  - Cloud Providers
- Leverage Host Classifier or Roles (Cloud)

Step 4: Classify Undefined Services/Applications
- Custom services & Applications

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

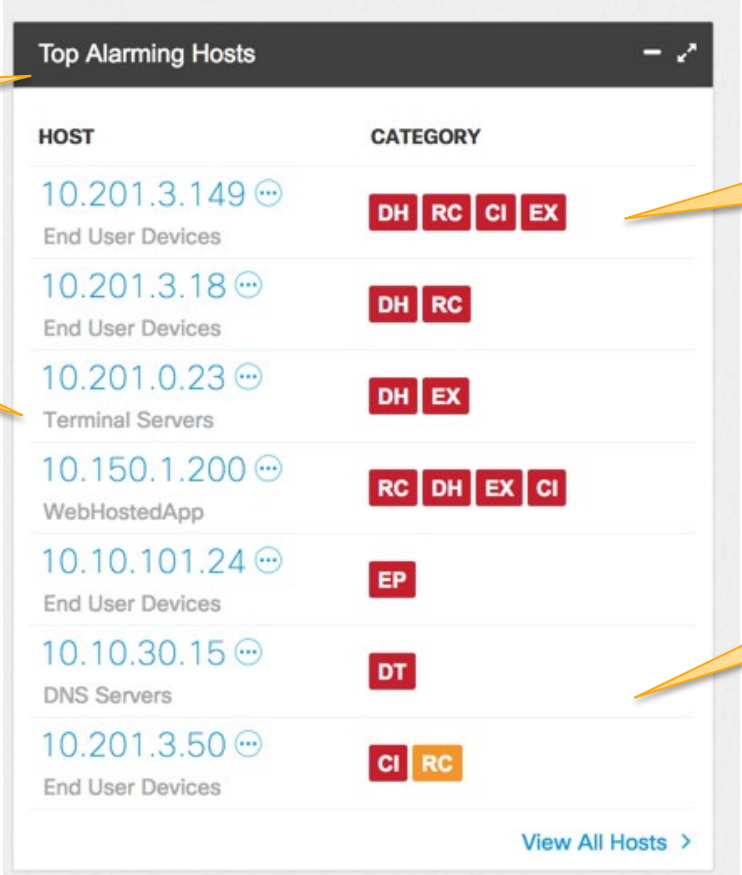
Operationalising Anomaly Detections

Stack Ranked

Leverage classification!

This host is the MOST different/interesting

Work down the list



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public