

# Cisco Secure Network Analytics Visibility Detection Response

Redouane MEDDANE  
Author and Collaboration – Security Consultant

## Agenda:

1. Visibiltiy Overview
2. Cisco Secure Network Analytics architecture
3. Host Group and Layer Detection
4. Encrypted Traffic Analysis (ETA)
5. Integration with Cisco ISE
6. Global Threat Alerts



# Visibility Overview

## Why Network Visibility and analytics is important?

Network security is a constant war  
When defending against the enemy  
you must know your own territory  
and implement defense mechanisms in place.

# Why Network Visibility and analytics is important?

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

# Why Network Visibility and analytics is important?

Firewall is there to protect your inside network from threats in internet. But misconfiguration and mistake is possible, how to detect it?

If a policy rules on firewall or WSA are changed which causes some rules placed on the top. How to detect this?

If an authorized server is used with stolen credentials and the attacker performs scanning and reconnaissance attack. How to detect this?

If you have a huge volume of exfiltration data. How to detect this?

# Why Network Visibility and analytics is important?

If you are using DNS Layer security with Umbrella as the trusted DNS server, and users are using rogue DNS servers with risk of traffic redirection to malicious websites. How to detect this violation?

You want to build policy segmentation on firewalls and other security products but you dont want to disrupt critical business activities. How to to use policies without enforcing them?

You want to detect malware in encrypted traffic without decryption while maintaining Data Integrity. How to do this?

# Cisco Visibility Solution

Cisco Secure Network Analytics  
(Formerly Stealthwatch)

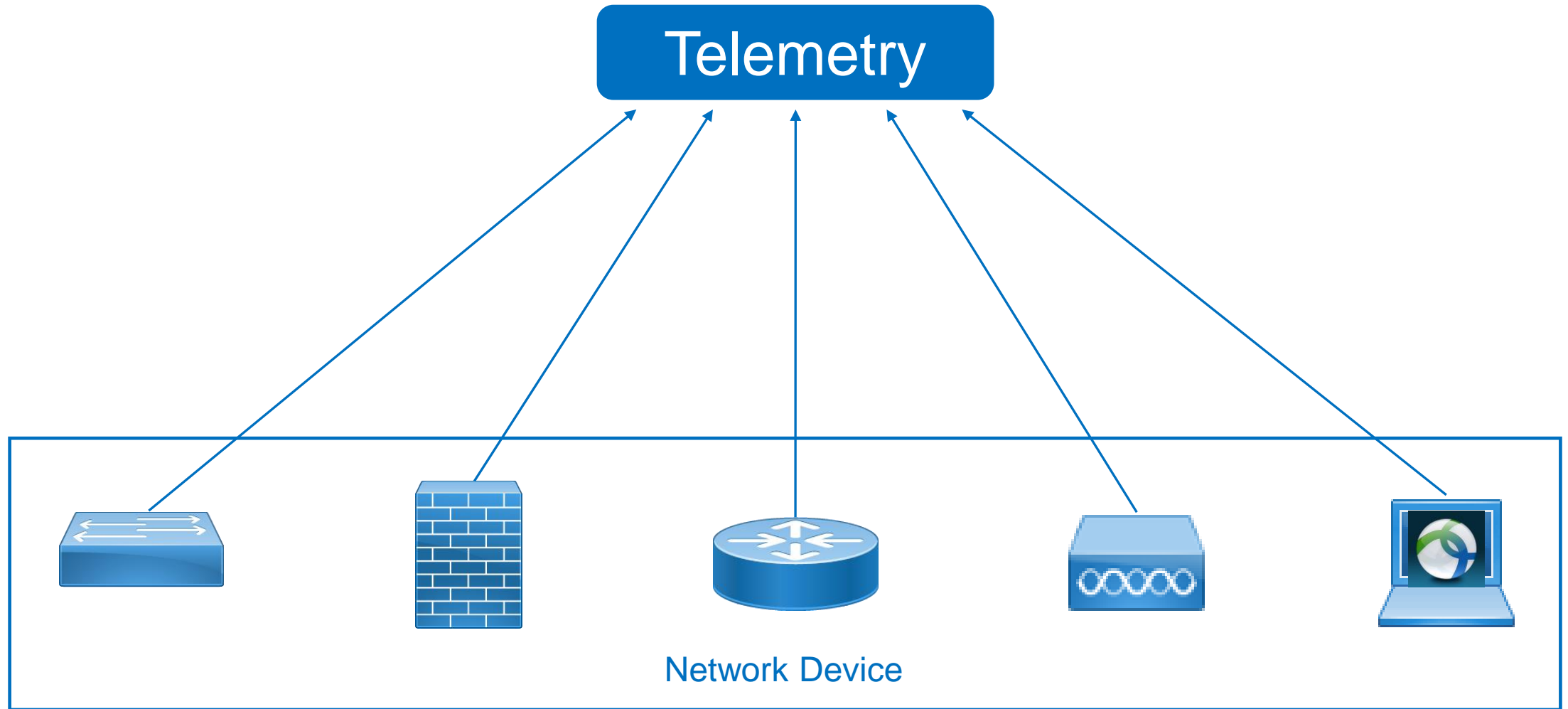


2015 – Acquisition of Lancope





# Telemetry with NetFlow

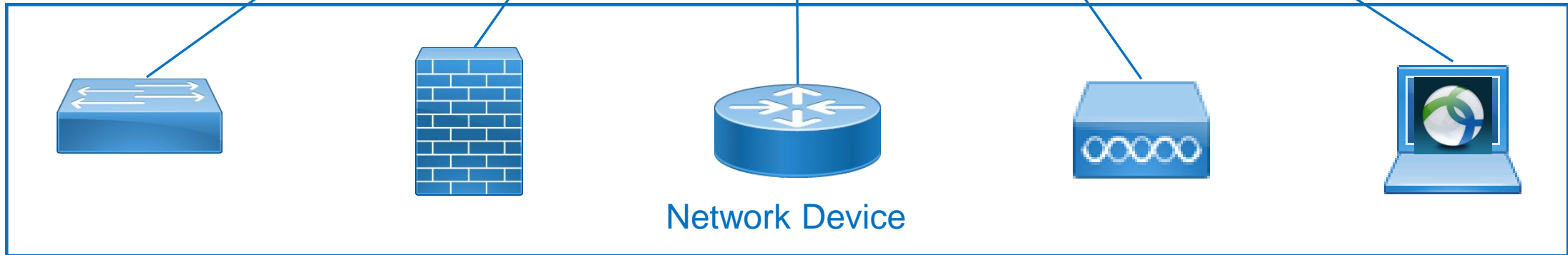


# Telemetry with NetFlow

Stealthwatch

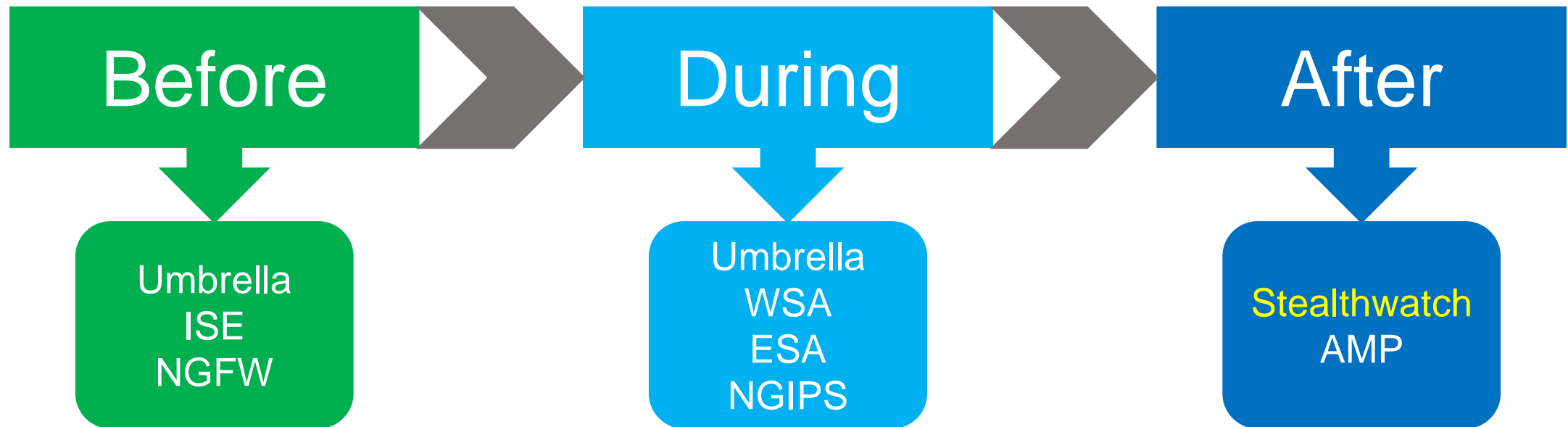


Telemetry



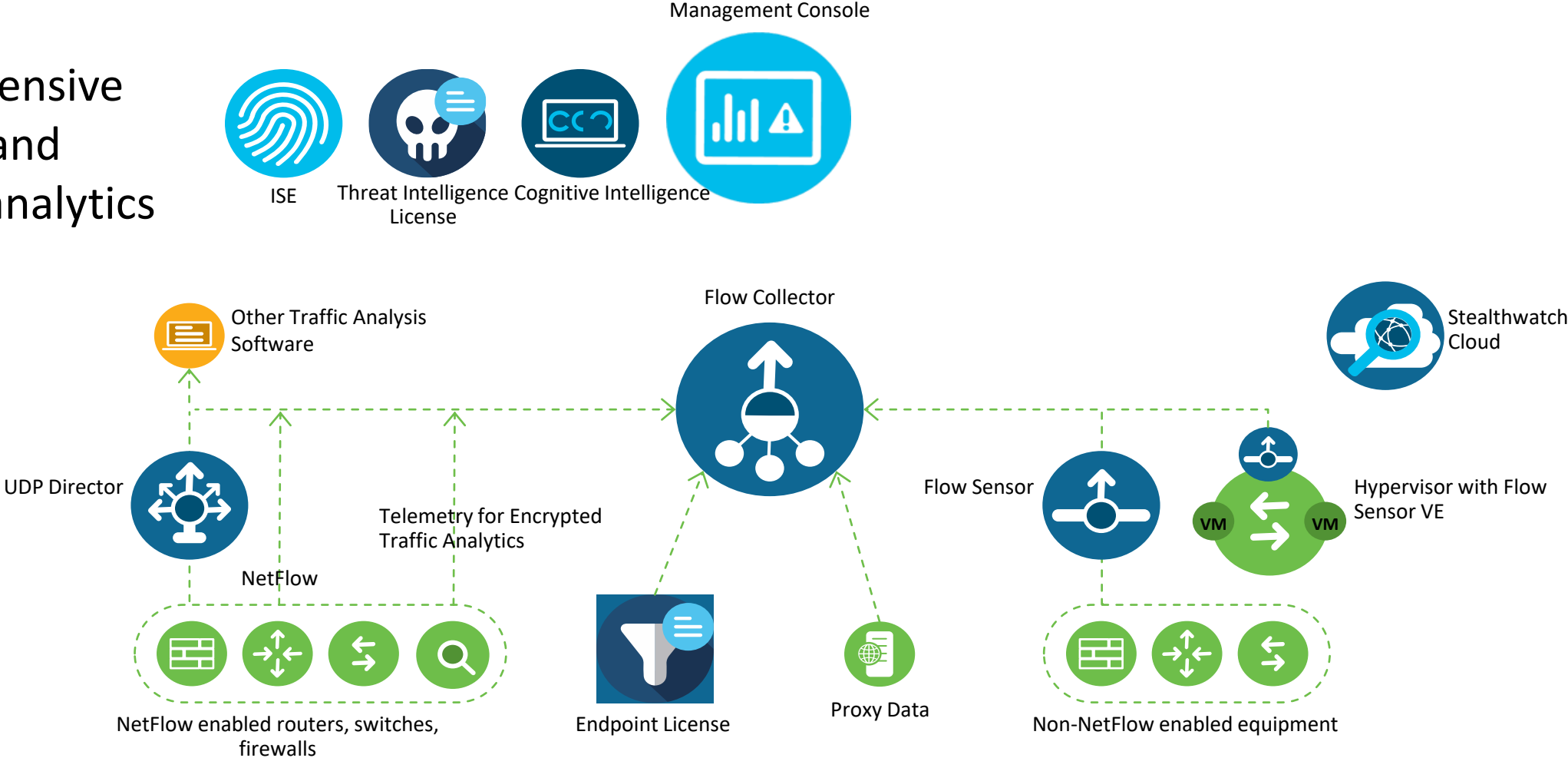
# Cisco SNA and Attack Continuum

## Cisco Security Products in the Attack Continuum

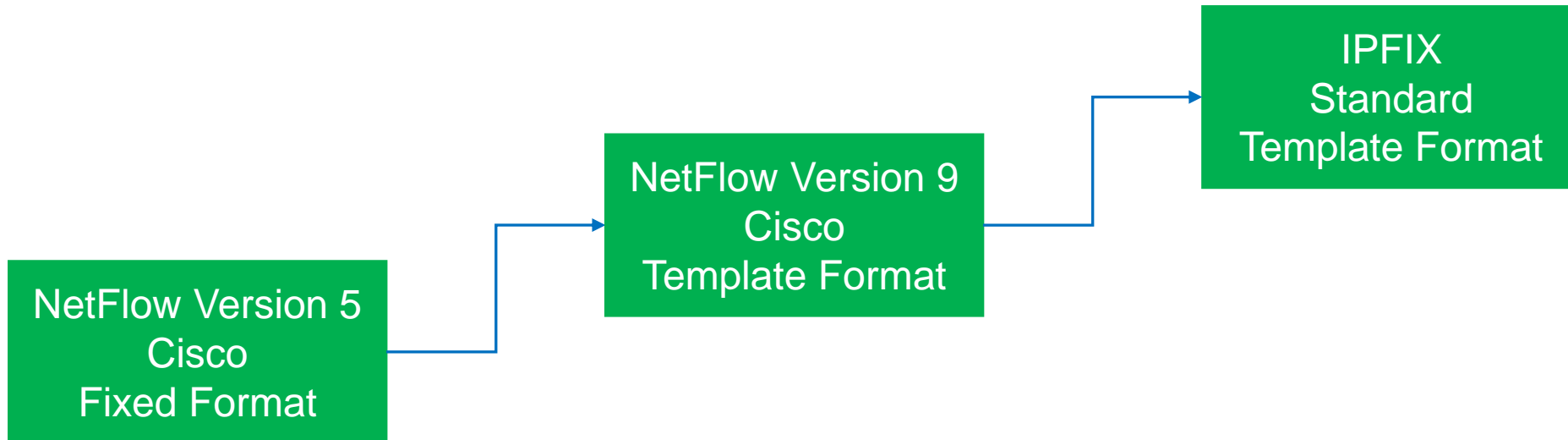


# Stealthwatch Enterprise architecture

Comprehensive visibility and security analytics



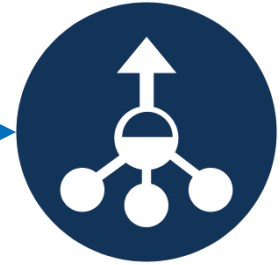
# Versions of NetFlow



## Guidelines

- Enable NetFlow on Access Layer. East-West and North-South (Internet) Visibility.
- Move NetFlow to the distribution layer if NetFlow is not supported in the access layer.
- Enable NetFlow on the WAN and Internet Edge routers.
- Enable NetFlow on Cisco Wireless LAN Controllers.
- Enable NBAR on routers and switchers to provide layer 7 informations.
- Integrate Cisco ISE to provide user identity.

# Stealthwatch: What defines a Flow



## Required fields:

- Source IP Address
- Source Port
- Destination IP Address
- Destination Port
- IP Protocol
- Byte count
- Packet count
- Start time
- End time
- Input Interface

# NetFlow in 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)

## Data Center Switch

Nexus 1000v (v9/IPFIX)  
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)

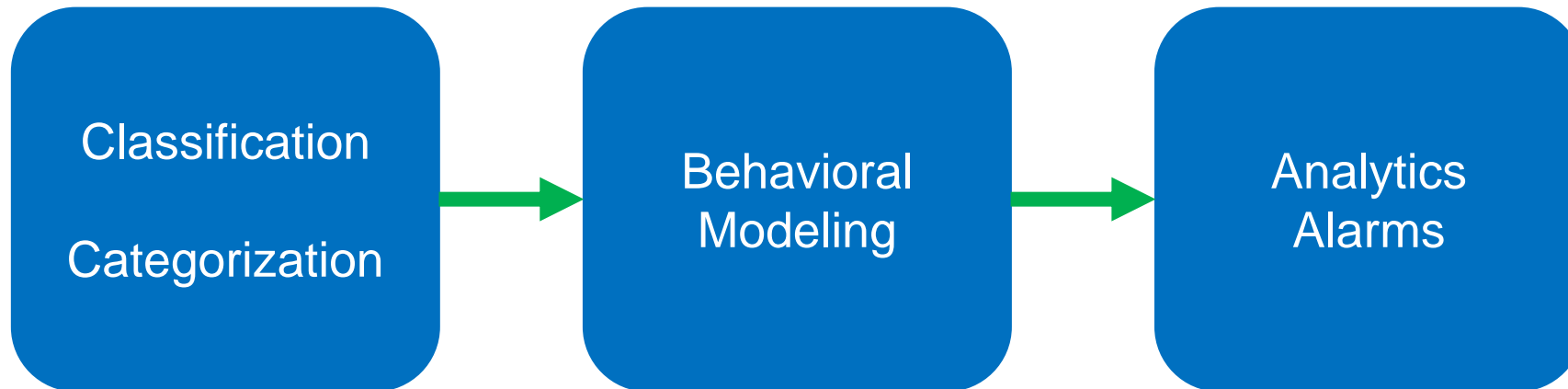
## Servers, Software and Appliances

Cisco Stealthwatch Flow Sensor (v9/IPFIX ETA)  
Cisco UCS VIC (v9/IPFIX)  
Cisco AnyConnect Client (IPFIX)

# Cisco Secure Network Analytics architecture

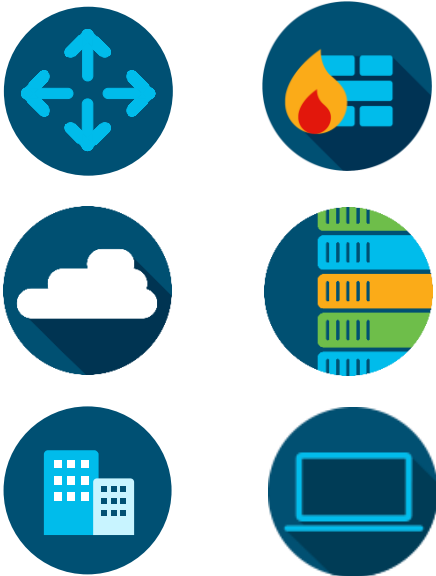


# Cisco Secure Network Analytics Pipeline



# Threat analytics detection and response

## Contextual network-wide visibility



Using existing network infrastructure

## Predictive threat analytics



Behavioral modeling

Machine learning

Global threat intelligence

## Automated detection and response



Unknown threats

Insider threat

Encrypted malware

Policy violations

# Cisco SNA Key Features

## Visibility everywhere

Analyses enterprise telemetry from any source (NetFlow, IPFIX, sFlow, other Layer 7 protocols) across the extended network

## Encrypted Traffic Analytics

Only product that can analyze encrypted traffic to detect malware and ensure policy compliance without decryption

## Rapid Threat Containment

Quarantine infected hosts easily using the Identity Services Engine (ISE) integration, collect and store network audit trails for deeper forensic investigations

## Unique threat detection

Combination of multi-layer machine learning and behavioral modeling provides the ability to detect inside as well as outside threats

## Smart segmentation

Create logical user groups that make sense for your business, monitor the effectiveness of segmentation policies through contextual alarms

# Deduplication and Stitching



Unidirectional Telemetry Records

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

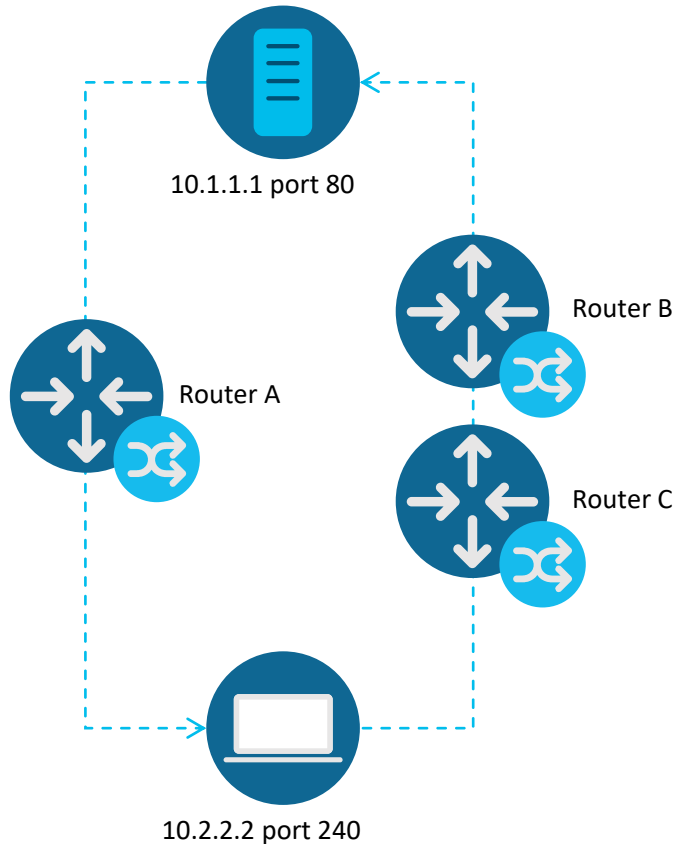
Bidirectional Telemetry Record

Conversation record

Easy visualization and analysis

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

# deduplication and stitching



Router A: 10.1.1.1:80 → 10.2.2.2:1024

Router B: 10.2.2.2:1024 → 10.1.1.1:80

Router C: 10.2.2.2:1024 → 10.1.1.1:80

Duplicates

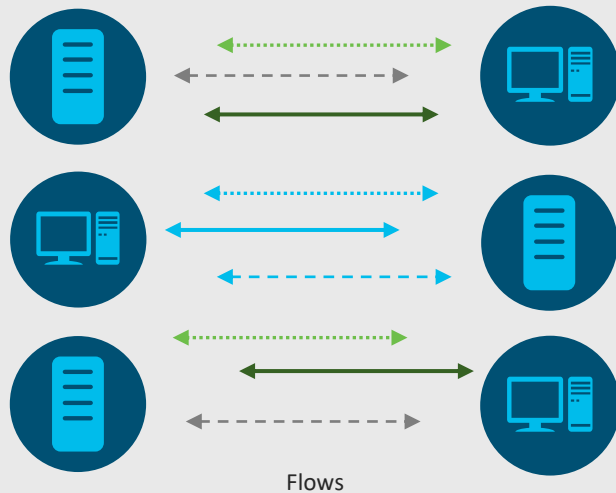
## Deduplication

- Avoid false positives and misreported traffic volume
- Enable efficient storage of telemetry data
- Necessary for accurate host-level reporting
- No data is discarded

# Anomaly detection using behavioral modeling

## Collect and analyze telemetry

Comprehensive data set optimized to remove redundancies



## Create a baseline of normal behavior

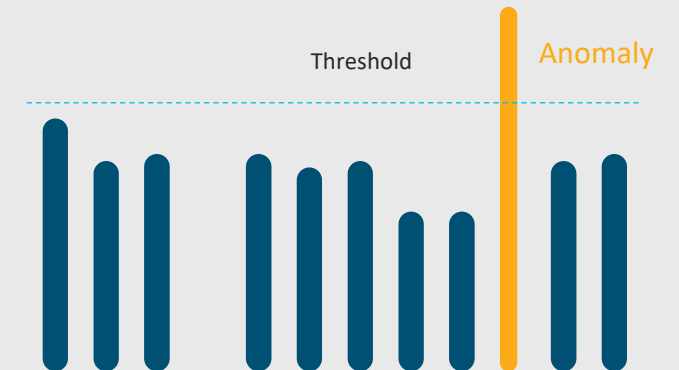
Security events to detect anomalies and known bad behavior

### Analysis of multiple threat behaviors

Number of concurrent flows	New flows created	Number of SYNs received
Packet per second	Number of SYNs sent	Rate of connection resets
Bits per second	Time of day	Duration of the flow

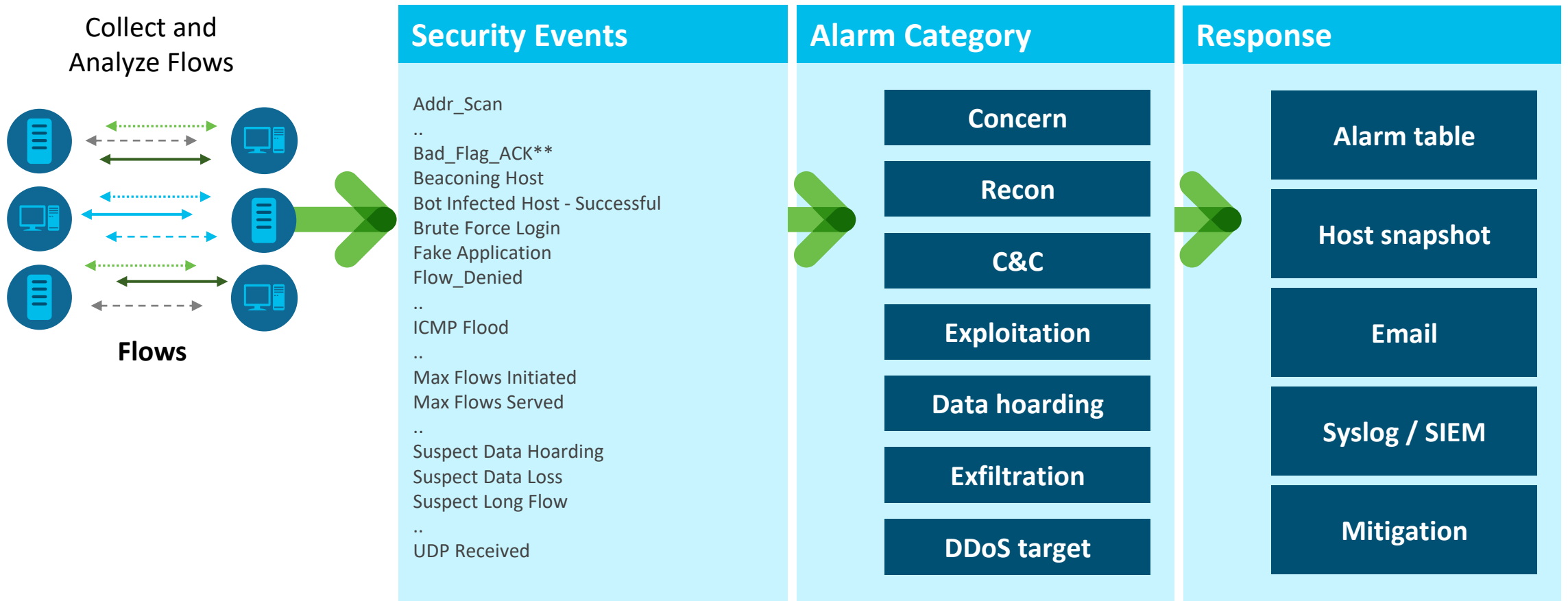
## Alarm on anomalies and behavioral changes

Alarm categories with threshold



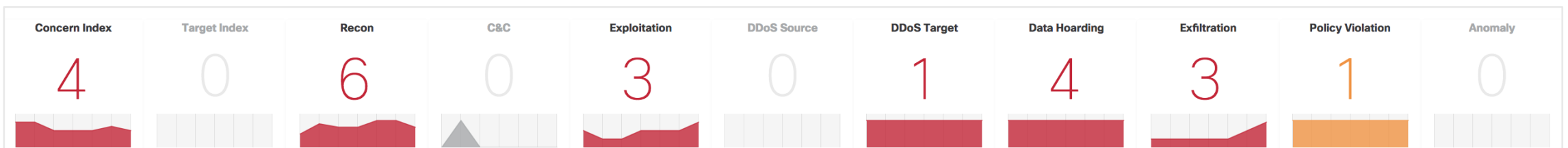
# Behavioral & Anomaly Detection Model

Note: Behavioral Algorithms are Applied to Build “Security Events”



# Logical alarms based on suspicious events

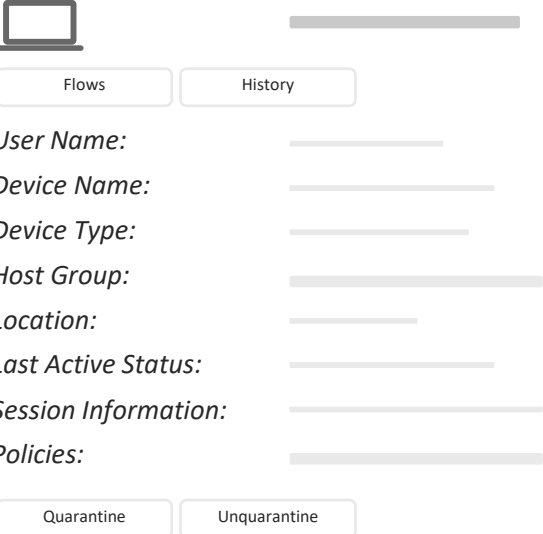
<b>Source or target of malicious behavior</b>	<b>Reconnaissance</b>	<b>Command and Control</b>	<b>DDoS Activity</b>	<b>Insider threats</b>
Scanning, excessive network activity such as file copying or transfer, policy violation, etc.	Port scanning for vulnerabilities or running services	Communication back to an external remote controlling server through malware	Sending or receiving SYN flood and other types of data floods	Data hoarding and data exfiltration





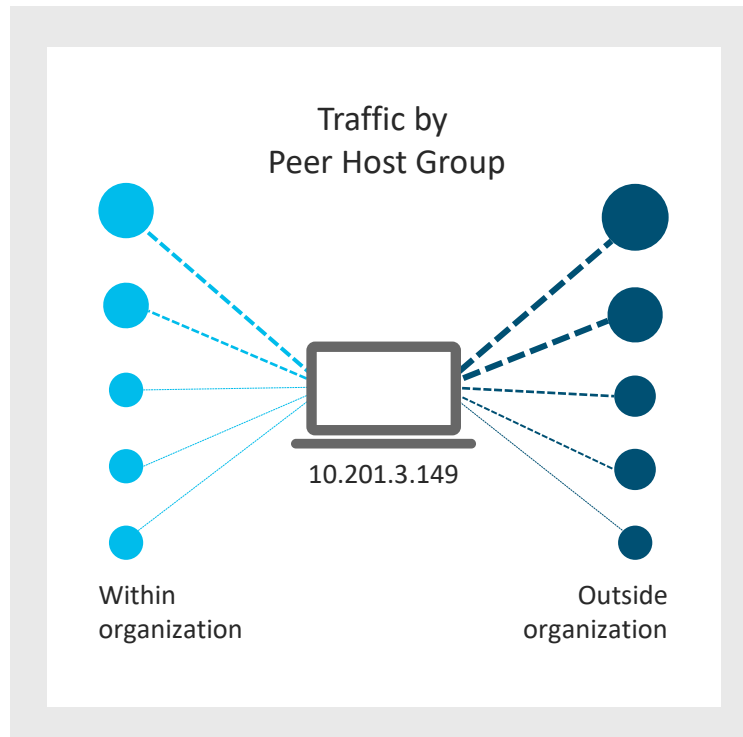
# Investigating a host

### Host Summary

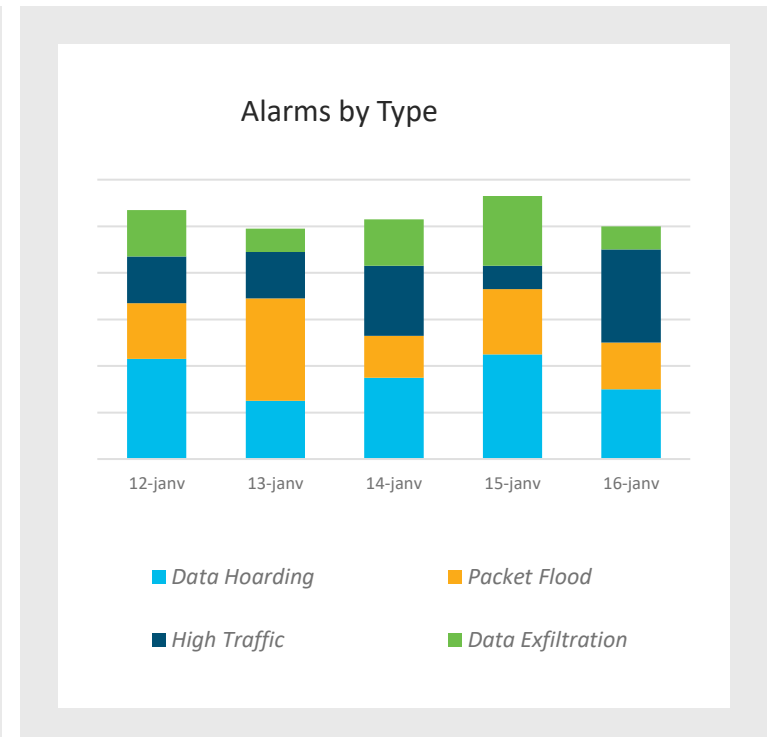


The Host Summary UI features a laptop icon at the top left. Below it are two buttons: 'Flows' and 'History'. A list of fields follows, each with a label and a corresponding input field: 'User Name:', 'Device Name:', 'Device Type:', 'Host Group:', 'Location:', 'Last Active Status:', 'Session Information:', and 'Policies:'. At the bottom, there are two buttons: 'Quarantine' and 'Unquarantine'.

Summary of aggregated host information



Observed communication patterns



Historical alarming behavior

# Host Group and Layer Detection

# Host Classification



Network Analytics

dcloud ▾

Host Group Management ⓘ

Filter by Host Group Name

▾ dcloud ...

- ▶  Inside Hosts ...
- ▶  Outside Hosts ...
- ▶  Authorized to Protected Assets ...
- ▶  Bogon ...
- ▶  Command & Control Servers ...
- ▶  Tor ...

## Inside Hosts

- All Hosts specifically defined as part of the network
- By Default –“Catch All”

## Threats Intelligence

- All Hosts not specifically defined as part of the network
- Countries –GEO-IP

## Outside Hosts

- Bogon
- Command & Control Servers

# Layer Detection

## On-Box

Custom Security Events

Relationship Events

Core Events

## Cloud Enabled

Global Threat Alerts  
(Cognitive Intelligence)

Threat Intelligence

Secure Cloud Analytics

# On-box Layer Detection

## Custom Security Events

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

## Relationship Events

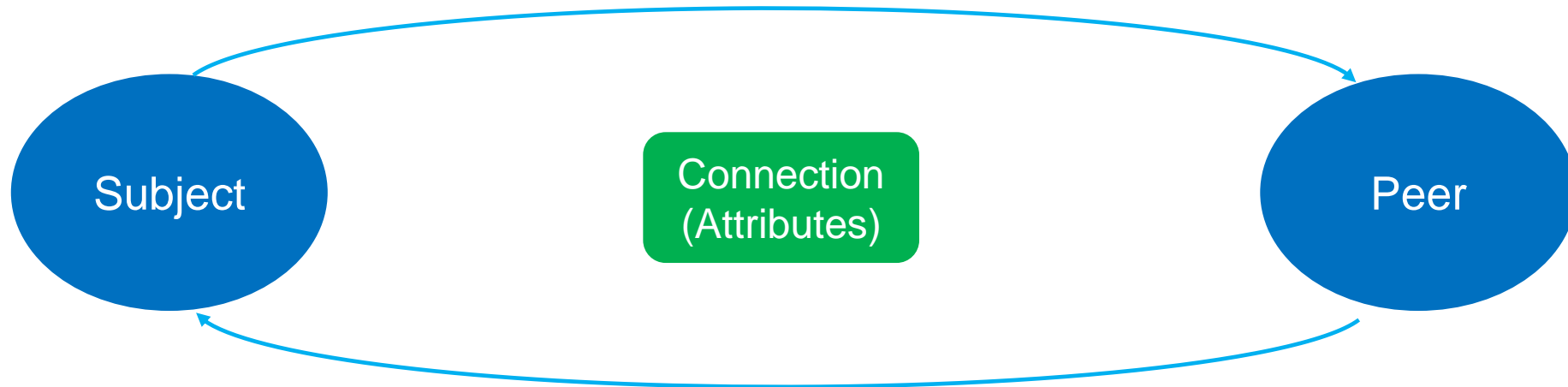
- Interaction between host groups that violate a policy setting like high volume traffic
- Directly created or automatically created from network diagram

## Core Events

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

# Custom Security Event

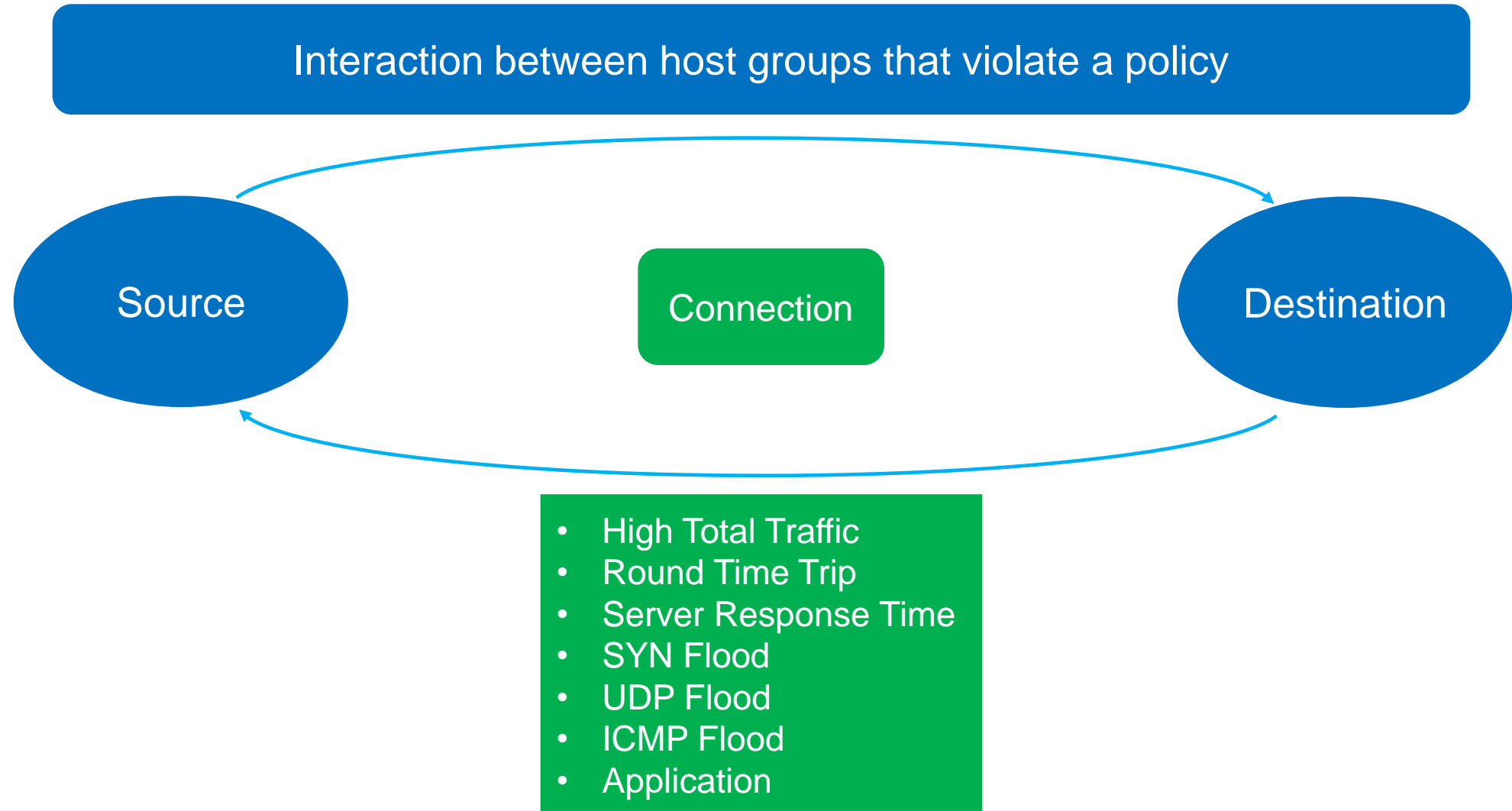
Generate an action when a single flow matches the selected conditions



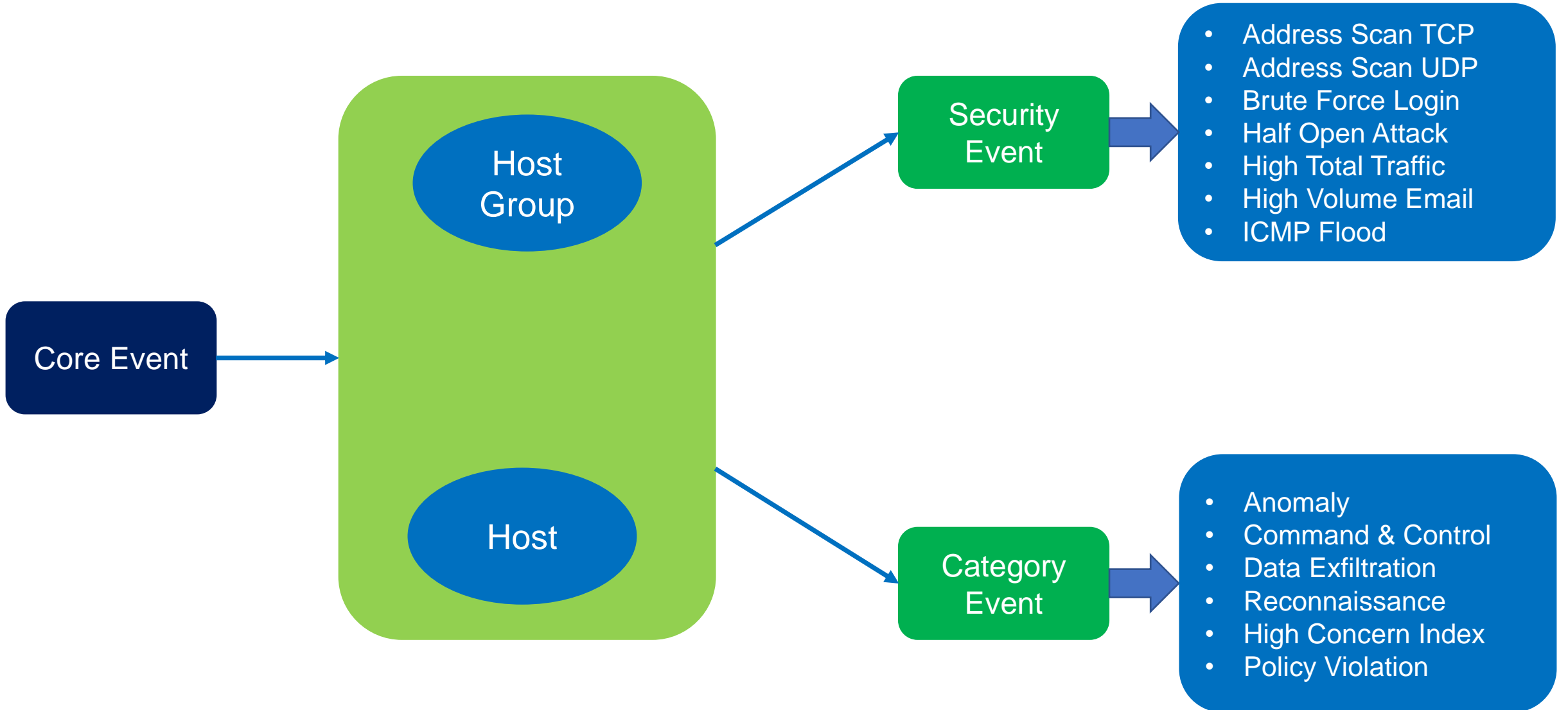
- Subject Port/protocol
- Subject Application
- Subject Byte
- Subject Users

- Peer Port/protocol
- Peer Application
- Peer Byte
- Peer Users
- Encryption TLS Version

# Relationship Event

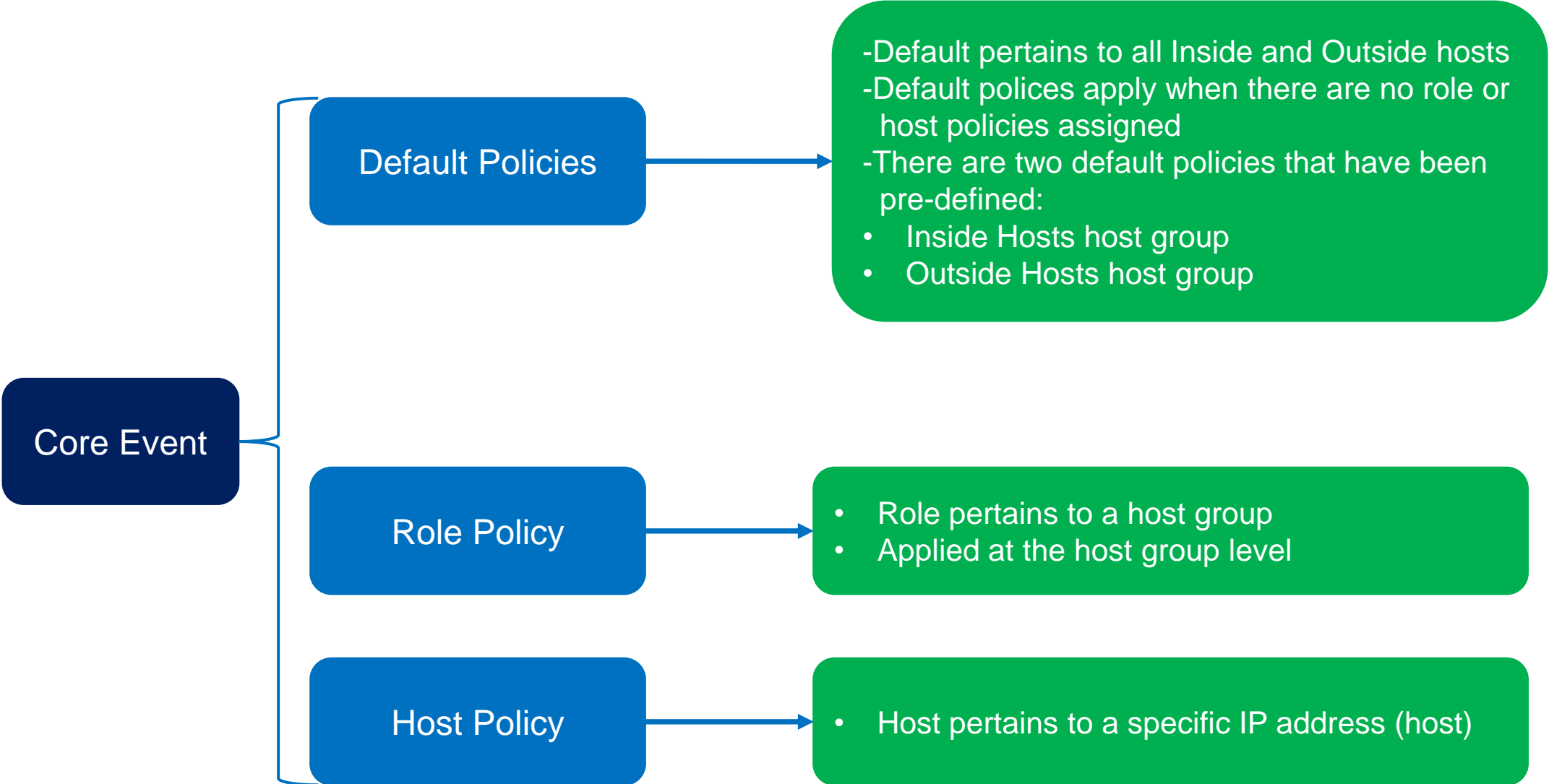


# Core Event





# Core Event



# Custom Security Event Example

The reason you should be concerned about rogue DNS servers on your network is that they could redirect traffic from the intended hosts that a client is attempting to reach. For example, a user that is attempting to access Amazon.com could be redirected by a rogue DNS server to a phishing site that has been crafted to look like Amazon, thus potentially compromising their account. This is known as DNS Hijacking.

Name *	Description	Status
<input type="text" value="CSE: Unauthorized DNS Servers"/>	<input type="text" value="ex. Event will trigger based on this rule"/>	<input type="checkbox"/> Off

When any host within **Inside Hosts** communicates with any host within **Outside Hosts** except those within **Umbrella DN Servers**; through **53/UDP** or **53/TCP**, an alarm is raised.

Find ⓘ			Actions
Subject Host Groups ⓘ	<input type="text" value="Inside Hosts X"/>	⊗ AND	<input type="checkbox"/> Alarm when a single flow matches this event.
Peer Host Groups ⓘ	<input type="text" value="Outside Hosts X EXCEPT ! Umbrella DN Servers X"/>	⊗ AND	
Peer Port/Protocols	<input type="text" value="53/UDP X 53/TCP X"/>	⊗	

# Custom Security Event Example

Detect hosts on the network bypassing proxy servers and connecting directly to the internet – policy violation.

Policy Management | Custom Security Event

Name \*

CSE: Proxy Bypass

Description

ex. Event will trigger based on this rule

When any host within *Inside Hosts* communicates with any host within *Outside Hosts*; through *80/TCP* or *443/TCP*, an alarm is raised.

Find i

Subject Host Groups i

Inside Hosts X

X AND

Peer Host Groups i

Outside Hosts X

X AND

Peer Port/Protocols

80/TCP X 443/TCP X

X

# Relationship Event Example

Policy Management | Relationship Policy

Name \*

Inside to Outside

Description

Host Group - Side 1 \*

+ Inside Hosts X

Host Group - Side 2 \*

+ Outside Hosts X

Traffic By Services And Applications

+ All Services

All Applications

Map Or Diagram Name

Relationship Events (0)

You must select at least one event before saving this policy. [Click here to select events.](#)

# Relationship Event Example

Traffic by Services and Applications



*Include All Except*

Services (0)

Applications (0)

Q Search

Select All Deselect All

- 3com AMP3
- 3Com TSMUX
- ACAP
- AccessBuilder
- ActiveX
- Adobe Connect
- Adobe EchoSign
- Adobe Services
- Adult Site
- AFS
- Akamai Cloud
- Alibaba

Policy Management | Relationship Policy

Name \*

Inside to Outside

Description

Host Group - Side 1 \*

Host Group - Side 2 \*

+ Inside Hosts X

+ Outside Hosts X

Map Or Diagram Name

Traffic By Services And Applications

+ All Services

All Applications

Relationship Events (0)

You must select at least one event before saving this policy. [Click here to select events.](#)

Events



Q 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

# Relationship Event Example

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...	Ex. "Inside Hosts"	Ex. "https"	Ex. "Corporate Email"	Ex. "On"	
Relationship High Total Traffic	Inside to Outside		Inside Hosts ↔ Outside Hosts	All Services	All Applications	<input checked="" type="checkbox"/> On	Delete

**Description**

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

Behavioral and Threshold      Tolerance  / 100

Threshold Only

Never trigger alarm when less than:  bytes in 24 hours

Always trigger alarm when greater than:  bytes in 24 hours

Trigger alarm when duration greater than:  minutes

# Relationship Event Example

A company's security policy dictates that only HTTP and HTTPS traffic is allowed between the finance users and the web servers. A High Total Traffic Relationship Policy is configured with an exception for HTTP and HTTPS traffic that will alarm when there is non-HTTP or non-HTTPS traffic between the finance Group and the Web Server Host Group. The threshold is set for 1 K in one minute to catch all traffic that is not compliant.

Name \*  
NON-HTTP Traffic from Finance Group

Description

Host Group - Side 1 \*  
+ Finance X

Host Group - Side 2 \*  
+ Web Servers X

Map Or Diagram Name

Traffic By Services And Applications  
+ Only Services http X https X  
All Applications excluded

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...	Ex. "Inside Hosts"	Ex. "https"	Ex. "Corporate Email"	Ex. "On"	
Relationship High Total Traffic	NON-HTTP Traffic from Finance Group		Finance ↔ Web Servers	Only Services http, https	--	<input checked="" type="checkbox"/> On	Delete

**Description**

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

Behavioral and Threshold

Threshold Only

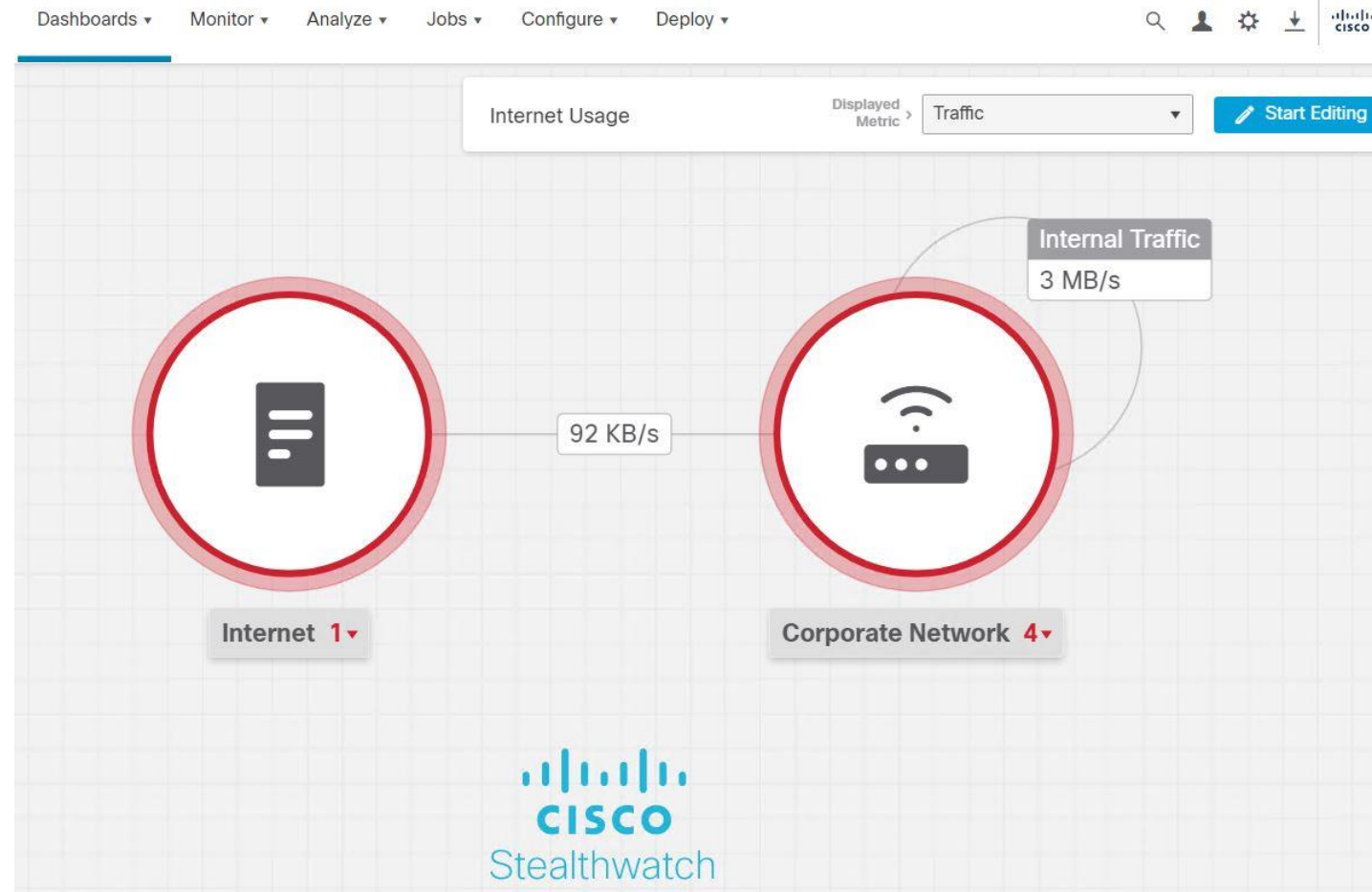
Tolerance  / 100

Never trigger alarm when less than:  bytes in 24 hours

Always trigger alarm when greater than:  bytes in 24 hours

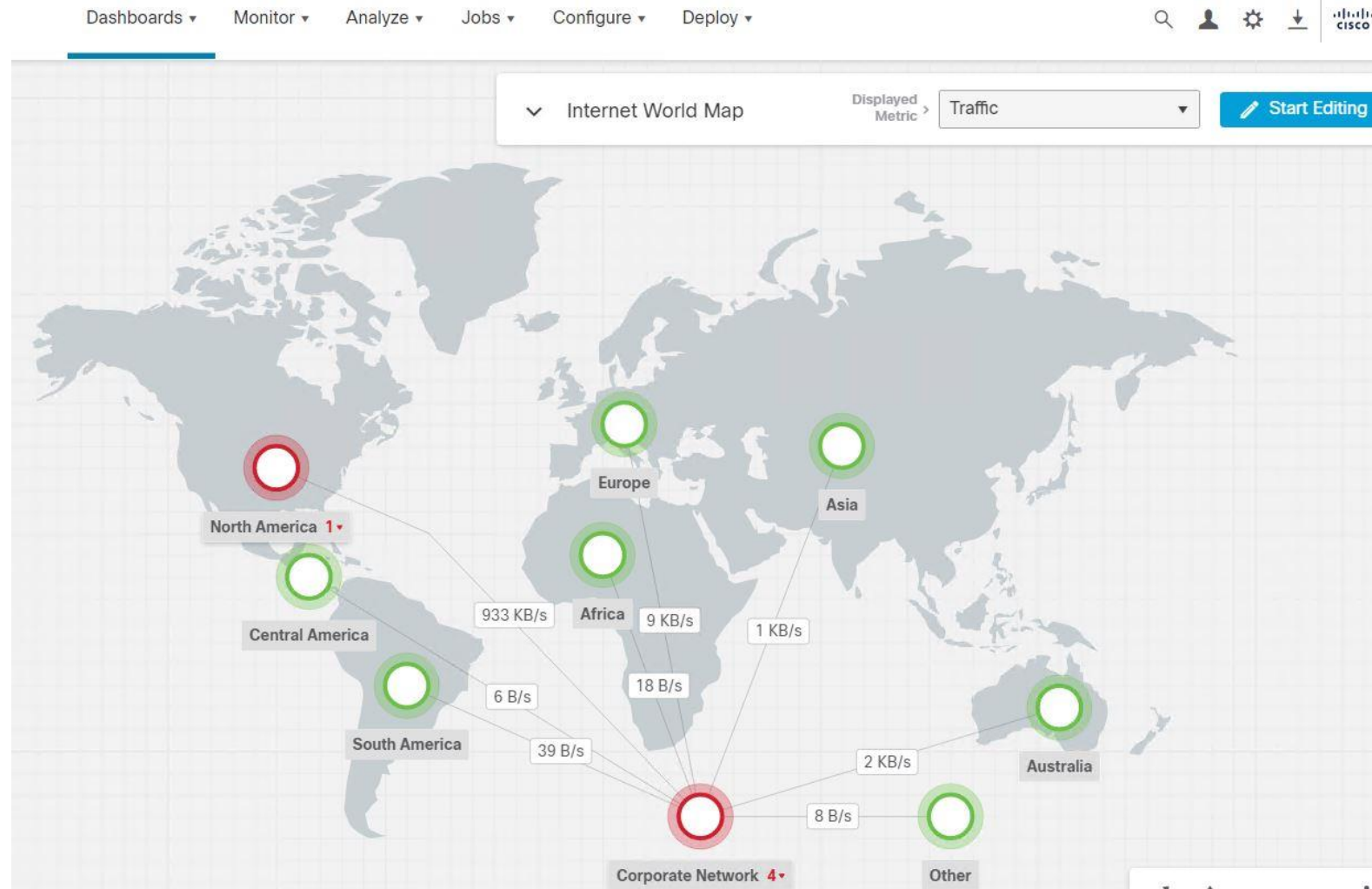
Trigger alarm when duration greater than:  minutes

# Relationship Event with Network Diagram





# Relationship Event with Network Diagram



# Core Event Example

Name \*  
Exclude DNS Servers

Description  
Exclude Traffic Events For DNS Servers

Host Groups  
+ DNS Servers X Authorized External DNS Servers X

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

# Core Event Example

Network Management & Scanning Servers

Policy for servers that exhibit scanning like activity (e.g. anti virus, vulnerability scanners, etc.)

Host Groups

+ Network Scanners X SMS Servers X Antivirus Servers X

IP Address Or Range

Core Events (52)

Select Events

Event	Event Type	When Host Is Source	When Host Is Target	Actions
Ex. Anomaly	Ex. Category	Ex. On + Alarm	Ex. On + Alarm	
▶ Addr_Scan/tcp	Security	Off	Off	Delete
▶ Addr_Scan/udp	Security	Off	Off	Delete

# Core Event Example

Event	Event Type	Policy Name	Policy Type	Hosts	When Host Is Source	When Host Is Target
High Concern Index	Ex. C...	DC Policy	Ex. Role	Ex. Network Scanners	Ex. On + Alarm	Ex. On + Alarm
High Concern Index	Category	DC Policy	Role	198.19.30.36	On + Alarm	NA

**This is a category event made up of the following security events:**

- Addr\_Scan/tcp, Addr\_Scan/udp, Bad\_Flag\_ACK, Bad\_Flag\_All, Bad\_Flag\_NoFlg, Bad\_Flag\_RST, Bad\_Flag\_Rsrvd, Bad\_Flag\_SYN\_FIN, Bad\_Flag\_URG, Beaconing Host, Bot Command & Control Server, Bot Infected Host - Attempted C&C Activity, Bot Infected Host - Successful C&C Activity, Brute Force Login, Connection From Bogon Address Attempted, Connection From Bogon Address Successful, Connection From Tor Attempted, Connection From Tor Successful, Connection To Bogon Address Attempted, Connection To Bogon Address Successful [More\(69\)](#)

Behavioral and Threshold      Tolerance  / 100

Threshold Only

Never trigger alarm when less than:  points in 24 hours

**Always trigger alarm when greater than:  points in 24 hours**

## Concern Index | 198.19.30.36 (1)

### Alarms

First Active	Source Host Groups	Source	Target Host Groups	Target	Policy	Event Alarms	Source User	Details
3/22/23 4:10 AM	File Servers	198.19.30.36 ...	--	Multiple Hosts	DC Policy	--	admininstrator	Observed 28.25k points <b>Policy maximum allows up to 25k points.</b>

# Events and Alarms best practices

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

# Cisco SNA Dashboard

## Alarming Hosts 1

since the last reset hour. The trend chart at the bottom displays the number of hosts receiving alarms contributing to this category within the last seven days.

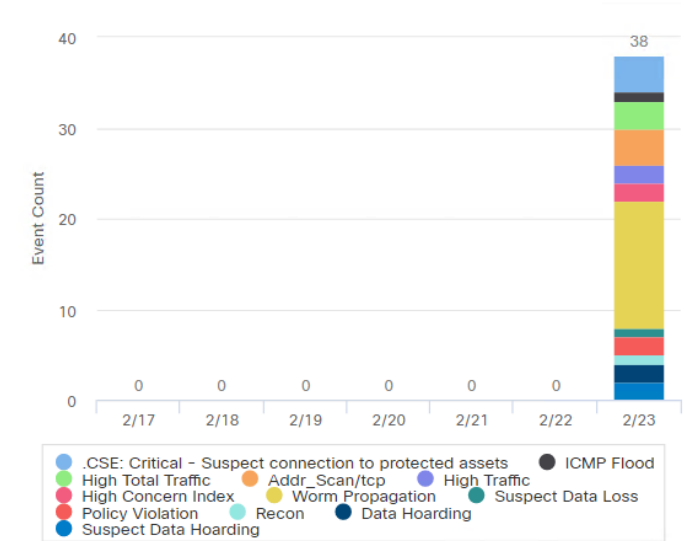


## Top Alarming Hosts

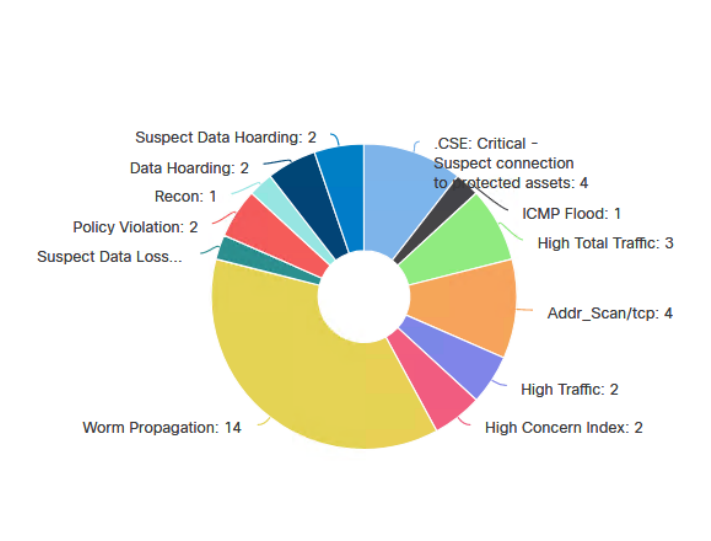
Host	Category
198.19.30.36 ... File Servers	PV CI DH RC
198.19.20.134 ... Protected Asset Monitoring	PV
10.201.3.149 ... Employee Wireless	DH CI

[View All Hosts >](#)

## Alarms by Type



## Today's Alarms



# Cisco SNA Traffic by Host

## Alarm Categories

Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Policy Violation	Anomaly
1	0	1	0	0	0	0	0	0	2	0

## Host Summary



Host IP

198.19.30.36 ...

Flows

Classify

History

**Status:** Active

**Hostname:** wkst1.dcloud.local

**Host Groups:** [File Servers](#)

**Location:** Unknown

**First Seen:** 9/27/20 7:39 AM

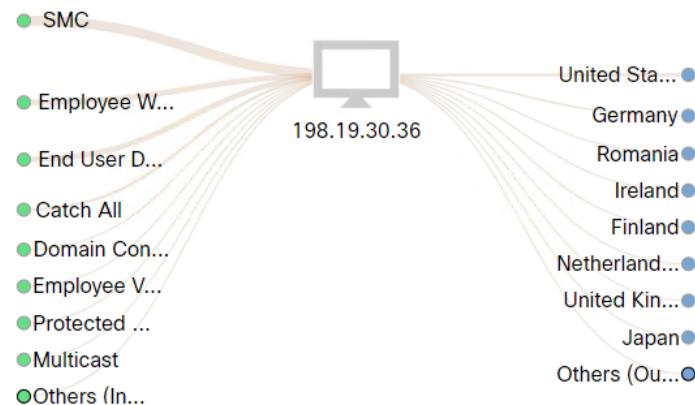
**Last Seen:** 4/23/23 5:21 AM

**Policies:** DC Policy, Inside

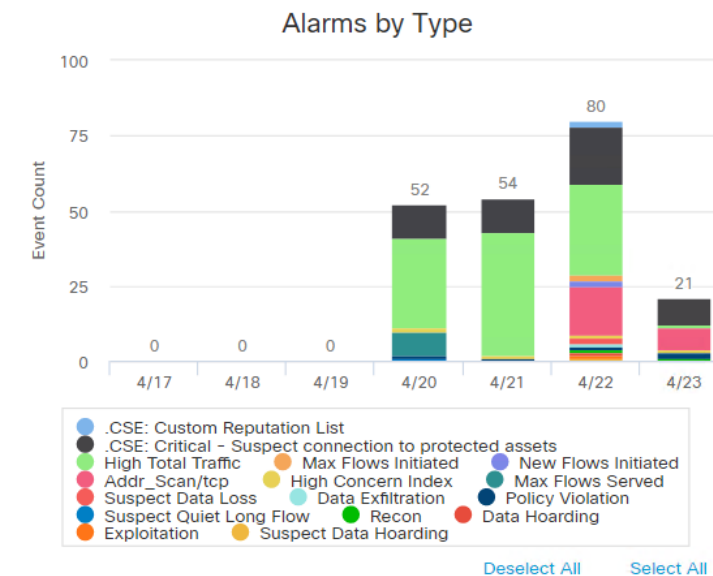
**MAC Address:** --

**ISE ANC Policy:** -- [Edit](#)

## Traffic by Peer Host Group (last 12 hours)



## Alarms by Type (last 7 days)



# Cisco SNA Flow Search

Flow Search ?

**Last 5 minutes** (Time Range) **2,000** (Max Records)

[Restore Defaults](#) [Load Saved Search](#) [Save](#) [Search](#)

Subject: **198.19.30.36** **Either** (Orientation)

Connection: **All** (Flow Direction)

Peer: **Countries** (Host Groups)

Search Type

Time Range ? \*

Search Name \*

Max Records Returned

**Subject**

Host IP Address

Host Groups  
[Select](#)

**Connection**

Port / Protocol

Applications  
[Select](#)

**Peer**

Host IP Address

Host Groups  
[Select](#)  
**Countries**

Advanced Subject Options ?

Advanced Connection Options ?

Advanced Peer Options ?



# Cisco SNA Flow Search

Flow Search Results (25)

[Edit Search](#)
Last 5 minutes (Time Range)
2,000 (Max Records)

Subject: 198.19.30.36 Either (Orientation)

Connection: All (Flow Direction)

Peer: Countries (Host Groups)

[Save Search](#)
[Save Results](#)
[Start New Search](#)

100% Complete
[Delete Search](#)

Manage Columns
[Summary](#)
[Export](#) v
[More](#) v
☰

Start	Duration	Subject IP Add...	Subject Port/Pr...	Subject Host G...	Subject Bytes	Subject Proces...	Application	Application (Fl...	Application (N...	Total Bytes	Peer IP Address	Peer Port/Pr
<i>Ex. 06/09/</i>	<i>Ex. &lt;=50min4</i>	<i>Ex. 10.10.10.1</i>	<i>Ex. 57100/UD</i>	<i>Ex. "catch All"</i>	<i>Ex. &lt;=50M</i>	<i>Ex. chrome.ex</i>	<i>Ex. "Corporate</i>	<i>Ex. HTTP</i>	<i>Ex. netbios</i>	<i>Ex. &lt;=50M</i>	<i>Ex. 10.255.25:</i>	<i>Ex. 2055/U</i>
▶ Apr 23, 2023 5:25:54 AM (6min 6s ago)	4min 5s	198.19.30.36 ...	57430/UDP	File Servers	946.37 M	--	Web	--	google-services	949.32 M	142.251.214.142 ...	443/UDP
▶ Apr 23, 2023 5:16:33 AM (15min 27s ago)	13min 26s	198.19.30.36 ...	27274/TCP	File Servers	504.81 K	--	HTTPS (unclassified)	--	ssl	14.06 M	217.79.181.76 ...	443/TCP
▶ Apr 23, 2023 5:24:52 AM (7min 8s ago)	5min 7s	198.19.30.36 ...	59380/UDP	File Servers	21.73 K	--	Web	--	google-services	36.49 K	142.251.46.206 ...	443/UDP

# Cisco SNA Flow Search – Traffic by Countries

Top Peers Search ⓘ

Last 5 minutes (Time Range)

Restore Defaults

Load Saved Search ▾

Save

Search

Subject: 198.19.30.36 ✕ Either (Orientation)

Connection: Total (Direction)

Peer: Countries (Host Groups) ✕ !Americas (Host Groups) ✕

Search Type

Top Peers ▾

Time Range ⓘ \*

Last 5 minutes

Search Name \*

Top Countries Traffic To 198.19.30.36

## Subject

Host IP Address

198.19.30.36 ✕

Host Groups

Select

## Connection

Port / Protocol

ex. 80/tcp or I80/tcp

Applications

Select

Direction

Total ▾

## Peer

Host IP Address

ex. 192.168.10.10 or I192.168.10.10

Host Groups

Select

Countries ✕

!Americas ✕

# Cisco SNA Flow Search – Traffic by Countries

Top Peers Search Results (5)

Edit Search

Last 5 minutes (Time Range)

Save Search

Save Results

Start New Search

Subject:

198.19.30.36

Either (Orientation)

100% Complete

Delete Search

Connection:

Total (Direction)

Peer:

Countries (Host Groups)

! Americas (Host Groups)

Manage Columns

Export

% Of Bytes	Peer IP Address	Peer Name	Peer Host Groups	Bytes	Peer Byte Ratio	Packets	Flows	Hosts	Peer Role
94.92%	85.9.31.130 ...	--	Romania	4.12 M	85.83%	4.94 K	1	1	Server
4.83%	217.79.181.76 ...	tor-proxy-00.for-privacy.net	Germany	214.68 K	70.43%	396	1	1	Server
0.10%	51.104.167.48 ...	--	Ireland	4.35 K	69.77%	21	1	1	Server
0.10%	20.54.24.246 ...	--	Ireland	4.35 K	69.78%	21	1	1	Server
0.06%	20.54.24.148 ...	--	Ireland	2.56 K	71.99%	14	1	1	Server

# Cisco SNA Flow Search – Detect Command and Control Traffic

## Top Peers Search ?

Last 7 Days (Time Range)

Restore Defaults

Load Saved Search ▾

Save

Search

Subject: Countries (Host Groups) × !Americas (Host Groups) × Either (Orientation)

Connection: Total (Direction)

Peer: 10.201.3.0/24 ×

Search Type

Top Peers ▾

Time Range ? \*

Last 7 Days

Search Name \*

Connection From Suspect Countries

### Subject

Host IP Address

ex. 192.168.10.10 or !192.168.10.10

Host Groups

Select

Countries × !Americas ×

### Connection

Port / Protocol

ex. 80/tcp or !80/tcp

Applications

Select

Direction

Total ▾

### Peer

Host IP Address

10.201.3.0/24 ×

Host Groups

Select

# Cisco SNA Flow Search – Detect Command and Control Traffic

∨ Advanced Options ⓘ

## SUBJECT ORIENTATION

- Either
- Client
- Server

RECORDS RETURNED \*

50

ORDER BY

Flows

Flow Collector Name

Interfaces

Select

# Cisco SNA Flow Search – Detect Command and Control Traffic

Top Peers Search Results (51)

Edit Search

Last 7 Days (Time Range)

Save Search

Save Results

Start New Search

Subject: Countries (Host Groups) !Americas (Host Groups) Either (Orientation)

100% Complete [Delete Search](#)

Connection: Total (Direction)

Peer: 10.201.3.0/24 (Host IP Address)

[Manage Columns](#) [Export](#) ∨

% Of Bytes	Peer IP Address	Peer Name	Peer Host Groups	Bytes	Peer Byte Ratio	Packets	Flows	Hosts	Peer Role
7.98%	10.201.3.5 ...	--	Employee Wireless , End User Devices , Sales and Marketing	110.29 M	7.89%	240.79 K	1,120	248	Client
5.11%	10.201.3.15 ...	--	Employee Wireless , End User Devices , Sales and Marketing	11.31 M	5.12%	21.35 K	717	77	Client and Server
4.97%	10.201.3.142 ...	--	Employee Wireless , End User Devices , Sales and Marketing	31.05 M	6.82%	60.45 K	698	68	Client and Server

# Cisco SNA Flow Search – Detect Command and Control Traffic

Flow Search Results (699)

Edit Search

04/16/2023 09:55 AM - 04/23/2023 09:55 AM (Time Range) 1,000 (Max Records)

Save Search

Save Results

Start New Search

Subject: Countries (Host Groups) !Americas (Host Groups) Either (Orientation)

28% Complete [Cancel Search](#)

Connection: All (Flow Direction) fcnf (Flow Collector Name)

Peer: 10.201.3.15 (Host IP Address)



Manage Columns

Summary

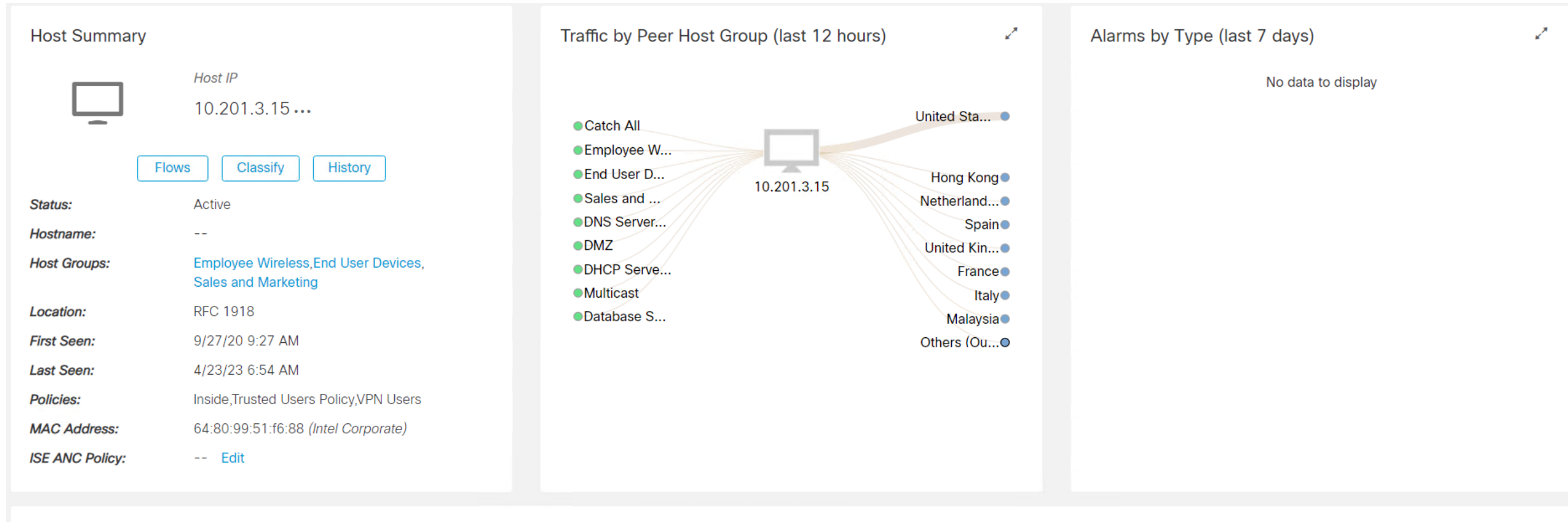
Export

More



Start	Duration	Subject IP Add...	Subject Port/Pr...	Subject Host G...	Subject Bytes	Subject Proces...	Application	Application (Fl...	Application (N...	Total Bytes	Peer IP Address	Peer Port/Pr...
<i>Ex. 06/09/...</i>	<i>Ex. &lt;=50min4l</i>	<i>Ex. 10.10.10.1</i>	<i>Ex. 57100/UDl</i>	<i>Ex. "catch All"</i>	<i>Ex. &lt;=50M</i>	<i>Ex. chrome.ex</i>	<i>Ex. "Corporate</i>	<i>Ex. HTTP</i>	<i>Ex. netbios</i>	<i>Ex. &lt;=50M</i>	<i>Ex. 10.255.25:</i>	<i>Ex. 2055/U</i>
Apr 23, 2023 2:39:17 AM (7hr 16min 53s ago)	25min 41s	31.13.77.58 ...	80/TCP	Hong Kong	1.16 M	--	HTTP (unclassified)	--	--	1.17 M	10.201.3.15 ...	50357/TCP
Apr 22, 2023 2:39:16 AM (1d 7hr 16min 54s ago)	25min 41s	31.13.77.58 ...	80/TCP	Hong Kong	1.16 M	--	HTTP (unclassified)	--	--	1.17 M	10.201.3.15 ...	50357/TCP

# Cisco SNA Flow Search – Detect Command and Control Traffic



Top Security Events for 10.201.3.15

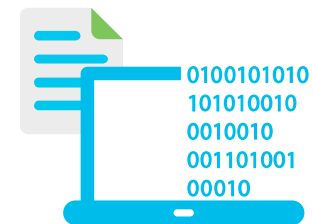
In the Top Security Events section, Identify if the Security Event "Suspect Quiet Long Flow" is there.



# Encrypted Traffic Analysis (ETA)

# Encrypted Traffic Analytics (ETA)

Visibility and malware detection with decryption



## Malware in Encrypted Traffic

Is the payload within the TLS session malicious?

- End to end confidentiality
- Channel integrity during inspection
- Adapts with encryption standards

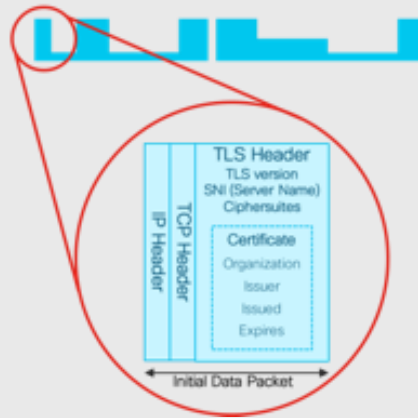
## Cryptographic compliance

How much of my digital business uses strong encryption?

- Audit for TLS policy violations
- Passive detection of Ciphersuite vulnerabilities
- Continuous monitoring of network opacity

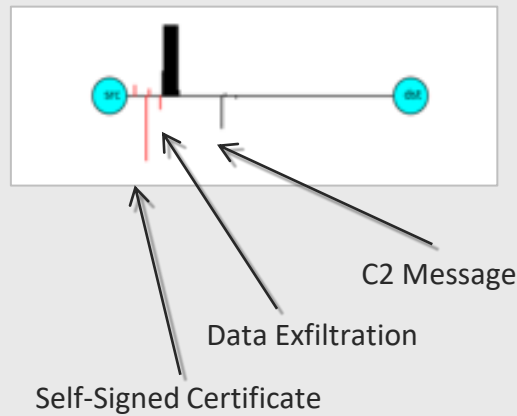
# Detect malware in encrypted traffic

Initial data packet



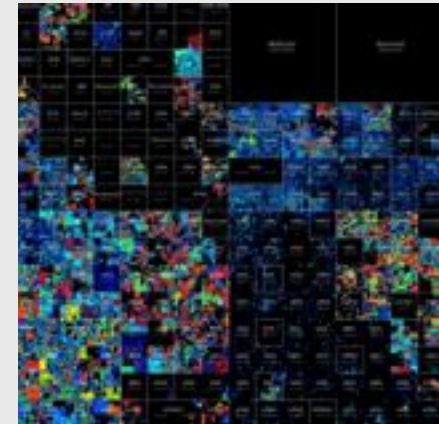
Make the most of the unencrypted fields

Sequence of packet lengths and times



Identify the content type through the size and timing of packets

Global Risk Map



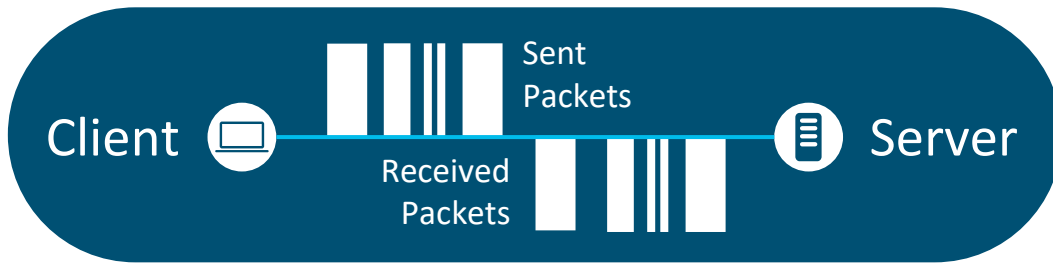
Know who's who of the Internet's dark side

# Identifying malicious encrypted traffic

## Google Search Page Download



## Model



Packet lengths, arrival times and durations tend to be inherently different for malware than benign traffic

## Initiate Command and Control

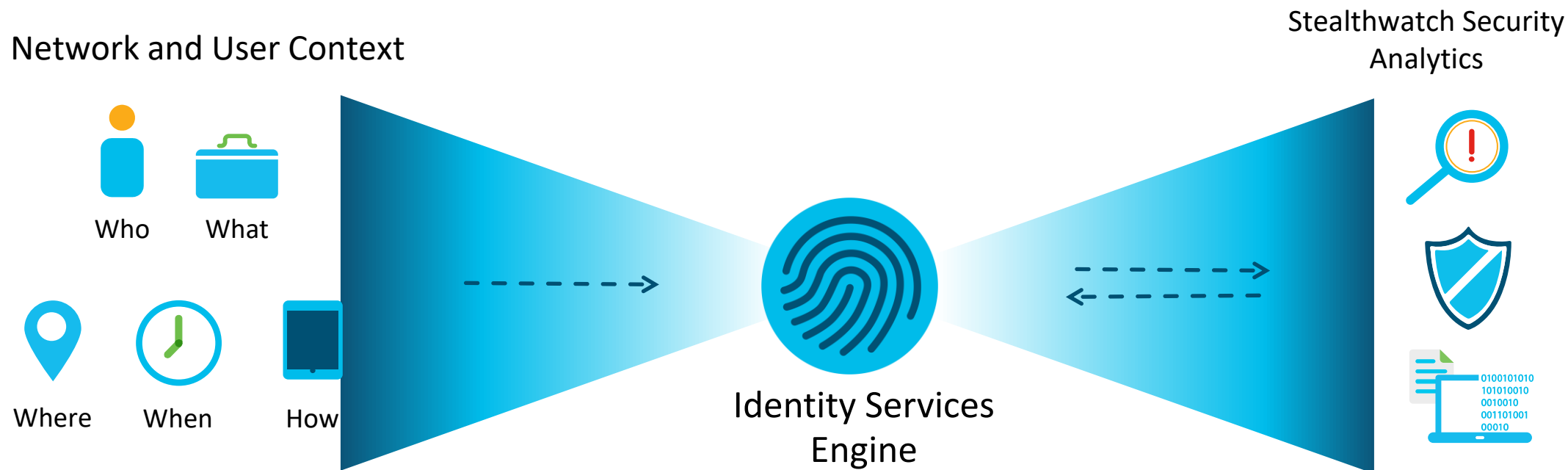


## Exfiltration



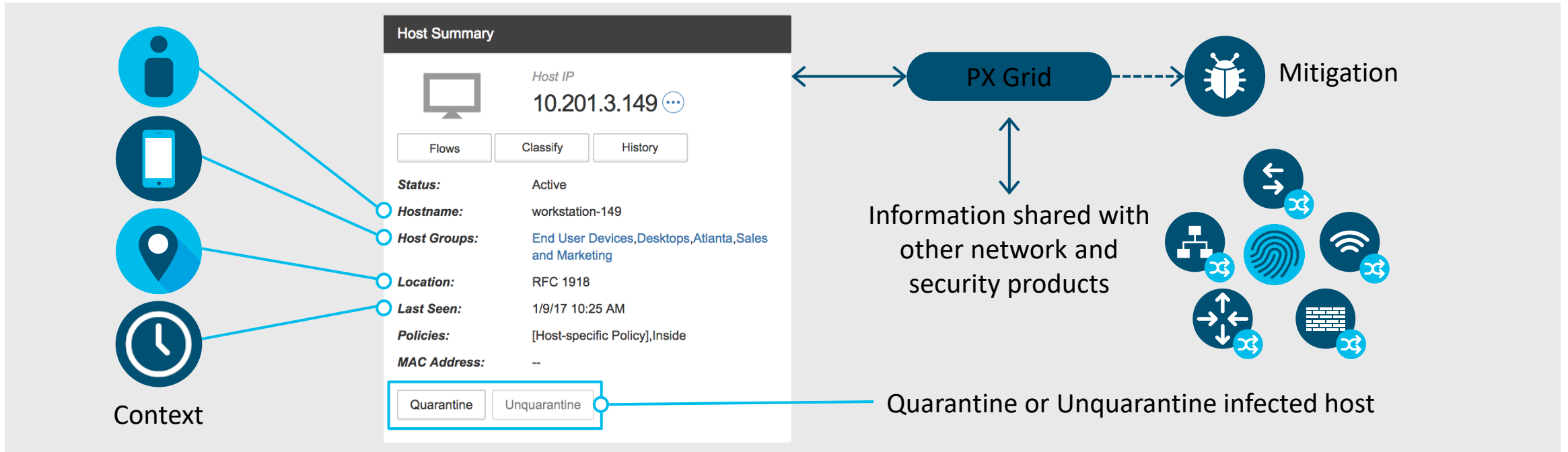
# Integration with Cisco ISE

# Integration with Cisco Identity Services Engine (ISE)



**Send contextual data collected from users, devices, and network to Stealthwatch Enterprise for advanced insight**

# Rapid Threat Containment



Cisco®  
Identity Services Engine



Stealthwatch  
Management Console

# Adaptive Network Control ANC with Cisco ISE

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers License Warning

Policy Sets Profiling Posture Client Provisioning Policy Elements

Default Default policy set Default Network Access

Authentication Policy (3)

Authorization Policy - Local Exceptions (0)

	Status	Rule Name	Conditions	Results	Profiles	Security Groups
		ANC Quarantine Local	Session-ANCPolicy EQUALS SW_Quarantine			Select from list

Authorization Policy - Global Exceptions (0)

	Status	Rule Name	Conditions	Results	Profiles	Security Groups
		ANC Quarantine Global	Session-ANCPolicy EQUALS SW_Quarantine			Select from list

Authorization Policy (10)



# Adaptive Network Control ANC with Cisco ISE

## Alarm Categories

Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Policy Violation	Anomaly
1	0	0	0	0	0	0	1	0	0	0

## Host Summary



Host IP  
10.201.3.149 ...

- Flows
- Classify
- History

**Status:** Active

**Hostname:** --

**Host Groups:** Employee Wireless, End User Devices, Sales and Marketing

**Location:** RFC 1918

**First Seen:** 9/27/20 9:27 AM

**Last Seen:** 2/23/23 5:13 AM

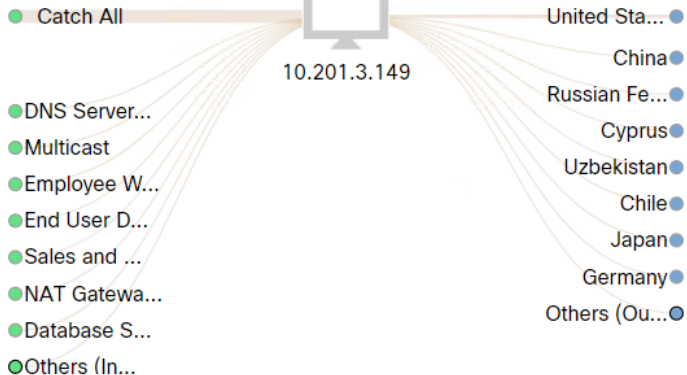
**Policies:** 10.201.3.149, Inside, Trusted Users Policy

**MAC Address:** --

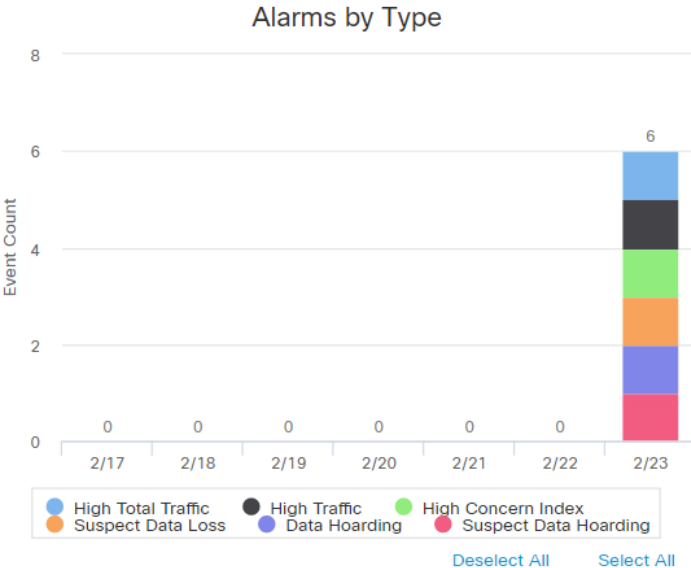
**ISE ANC Policy:** -- [Edit](#)



## Traffic by Peer Host Group (last 12 hours)



## Alarms by Type (last 7 days)



# Response Management – Automatic Quarantine with Cisco ISE

## Response Management

Rules   Actions   Syslog Formats

### Rules | Host Alarm

Cancel Save

Name

VPN Users Scan Alarms

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

Addr\_Scan/tcp

Processing Time

Severity

Type

IP Address or Range

Host Group

Define Condition

ASSOC

# Response Management – Automatic Quarantine with Cisco ISE

Define Action

Associated Actions

Execute the following actions when the alarm becomes **active**:

Name ↑	Type	Description	Used By Rules	Assigned
Auto Mitigation - Source Host	ISE ANC Policy	Automatically quarantine the offending source host leveraging an ISE ANC policy action.	3	<input checked="" type="checkbox"/>
Send email	Email	Sends an email to the recipients designated in the To field on the Email Action page.	4	<input type="checkbox"/>
Send to Syslog	Syslog Message	Sends a message to the syslog server designated in the Syslog Address field using the default Syslog Message format.	4	<input type="checkbox"/>

# Response Management – Automatic Quarantine with Cisco ISE

## ISE ANC Policy Assignments

<input type="checkbox"/>	Host IP Address	ISE Cluster	MAC Address	Assignment Mode	Requested By	Time	Requested ANC Policy	Effective ANC Policy	Assign ANC Policy
<input type="checkbox"/>	<a href="#">198.19.30.36</a>	dCloud ISE	00:50:56:bb:9e:7b	Automatic	(Response Management)	4/23/2023 4:51 AM	SW_Quarantine	<a href="#">Retrieve ↻</a>	...
<input type="checkbox"/>	<a href="#">198.19.10.100</a>	dCloud ISE	00:50:56:bd:f8:2c	Automatic	(Response Management)	4/23/2023 4:44 AM	SW_Quarantine	<a href="#">Retrieve ↻</a>	...

# Response Management – Automatic Quarantine with Cisco ISE

## Host Summary



Host IP

198.19.10.100 ...

Flows

Classify

History

Status:

Active

Hostname:

--

Host Groups:

Employee VPN

Location:

Unknown

First Seen:

10/10/20 10:45 AM

Last Seen:

4/23/23 4:43 AM

Policies:

Inside,Trusted Users Policy,VPN Users

MAC Address:

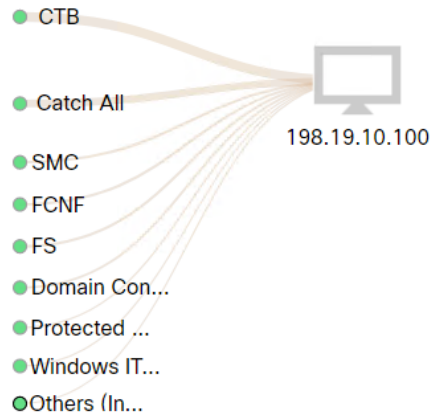
--

ISE ANC Policy:

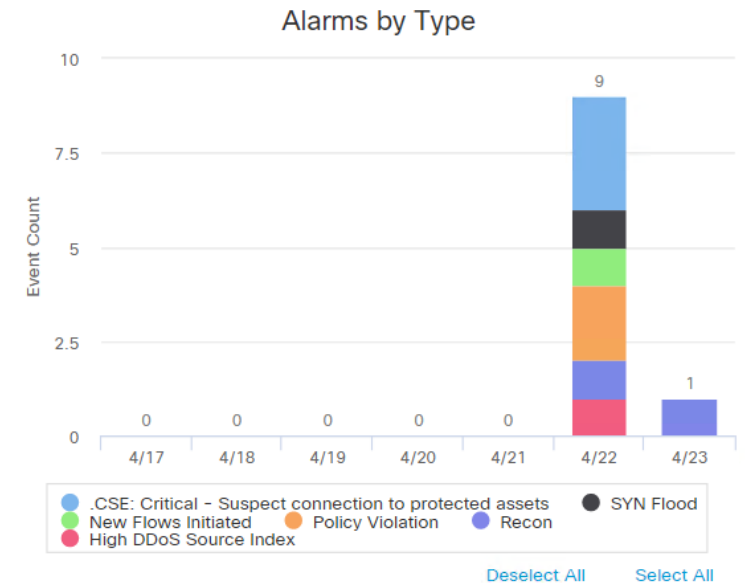
SW\_Quarantine

Edit

## Traffic by Peer Host Group (last 12 hours)



## Alarms by Type (last 7 days)



Automatic Quarantine

# Global Threat Alerts

# Global Threat Alerts

Detects suspicious web traffic and/or Stealthwatch flow records and responds to attempts to establish a presence in your environment and to attacks that are already under way

Stealthwatch sends flow records to the Cognitive Intelligence cloud for analysis.

Two categories of data are sent to the Cognitive Intelligence data center.

## **1. Stealthwatch flow records, if any of the following conditions are met:**

- Records for inside/outside host group traffic
- Records for specific internal host group traffic (Inside Hosts)
- Records for DNS requests, if the server port is 53
- Records for Encrypted Traffic Analytics, if you have an ETA enabled switch and router

## **2. Web log data.**

# Netflow IOS Commands

```
flow record STEALTHWATCH_FLOW_RECORD
description NetFlow record for SW
match ipv4 tos
match ipv4 source address
match ipv4 destination address
match transport destination-port
match transport source-port
match interface input
match ipv4 protocol
collect interface output
collect counter bytes
collect counter packets
collect timestamp sys-uptime first
collect timestamp sys-uptime last
collect application name
```

```
flow monitor IPv4_NETFLOW
exporter NETFLOW_TO_STEALTHWATCH
cache timeout active 60
record STEALTHWATCH_FLOW_RECORD
```

```
interface GigabitEthernet1
ip flow monitor IPv4_NETFLOW input
ip nbar protocol-discovery
!
interface GigabitEthernet1
ip flow monitor IPv4_NETFLOW input
ip nbar protocol-discovery
```

```
flow exporter NETFLOW_TO_STEALTHWATCH
description Export NetFlow to SW
destination 198.19.20.139
transport udp 2055
```





# Useful Link

## **Security Analytics with Stealthwatch - Cisco Live BRKSEC-3014:**

<https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/BRKSEC-3014.pdf>

## **Visibility, Detection and Response with Cisco Secure Network Analytics - Cisco Live BRKSEC-3019:**

<https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2023/pdf/BRKSEC-3019.pdf>

## **Cisco Secure Network Analytics - Security Events and Alarm Categories 7.4.2:**

[https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/management\\_console/securit\\_events\\_alarm\\_categories/7\\_4\\_2\\_Security\\_Events\\_and\\_Alarm\\_Categories\\_DV\\_2\\_1.pdf](https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/management_console/securit_events_alarm_categories/7_4_2_Security_Events_and_Alarm_Categories_DV_2_1.pdf)

## **Cisco Secure Network Analytics Desktop Client User Guide 7.4:**

[https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/management\\_console/smc\\_users\\_guide/7\\_4\\_Desktop\\_Client\\_User\\_Guide\\_DV\\_2\\_0.pdf](https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/management_console/smc_users_guide/7_4_Desktop_Client_User_Guide_DV_2_0.pdf)

## **Cisco Secure Network Analytics Global Threat Alerts Configuration Guide 7.4.2:**

[https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/cta/configuration/SNA\\_7\\_4\\_2\\_Global\\_Threat\\_Alerts\\_Guide\\_DV\\_1\\_0.pdf](https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/cta/configuration/SNA_7_4_2_Global_Threat_Alerts_Guide_DV_1_0.pdf)

# Useful Link

## **Cisco NetFlow Configuration:**

[https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/netflow/Cisco\\_NetFlow\\_Configuration.pdf](https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/netflow/Cisco_NetFlow_Configuration.pdf)

## **Configuring and Troubleshooting NetFlow for Cisco Stealthwatch:**

<https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/netflow/config-trouble-netflow-stealth.pdf>

## **Cisco Secure Network Analytics ISE and ISE-PIC Configuration Guide 7.4.2:**

[https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/ISE/7\\_4\\_2\\_ISE\\_Configuration\\_Guide\\_DV\\_1\\_0.pdf](https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/ISE/7_4_2_ISE_Configuration_Guide_DV_1_0.pdf)

## **Cisco Secure Network Analytics Use Cases:**

<https://community.cisco.com/t5/security-knowledge-base/welcome-to-secure-analytics-use-cases/tac-p/4418614#M7279>

## **Encrypted Traffic Analytics:**

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_data\\_eta/configuration/xe-16-8/sec-data-encrypted-traffic-analytics-xe-16-8-book/sec-data-encrypted-traffic-analytics-xe-16-6-book\\_chapter\\_01.pdf](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_eta/configuration/xe-16-8/sec-data-encrypted-traffic-analytics-xe-16-8-book/sec-data-encrypted-traffic-analytics-xe-16-6-book_chapter_01.pdf)

## **ENCRYPTED TRAFFIC ANALYSIS Use Cases & Security Challenges:**

<https://www.enisa.europa.eu/publications/encrypted-traffic-analysis>