

Three Friends in Security : Identity, Visibility and Enforcement

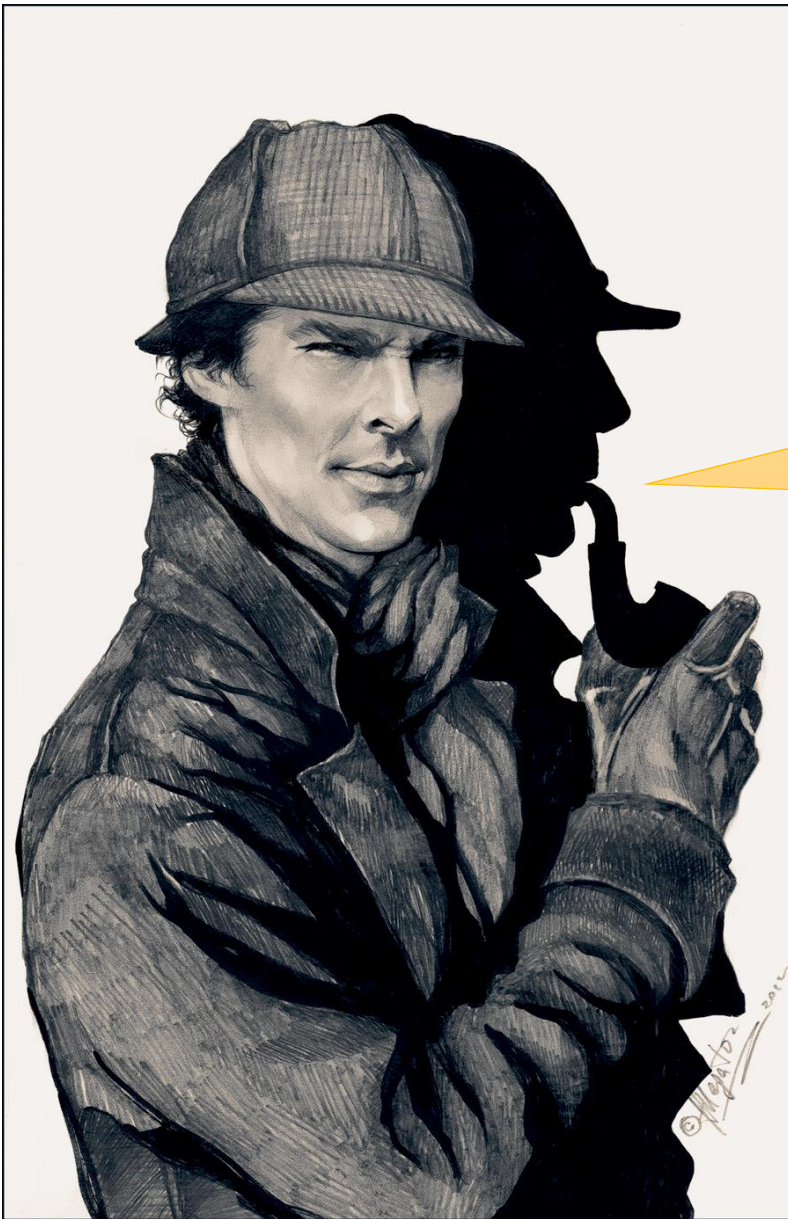


Stop the bad guys immediately

György Ács

Cisco Systems





“The world is full of obvious things which nobody by any chance observes.”

Sherlock Holmes, *The Hound of the Baskervilles*

This session is about using network analysis (our obvious things) to observe and mitigate an attack.

Agenda



- The Problem is Threats
 - Network as a Sensor / Enforcer
 - Identity
 - Visibility
 - Policy and Indication of Compromise, IoC
 - Enforcement
 - Summary
-

The Problem is Threats

VULNERABILITY REPORTS

 [TALOS VULNERABILITY REPORTING PGP KEY](#)

[COORDINATED DISCLOSURE POLICY](#)

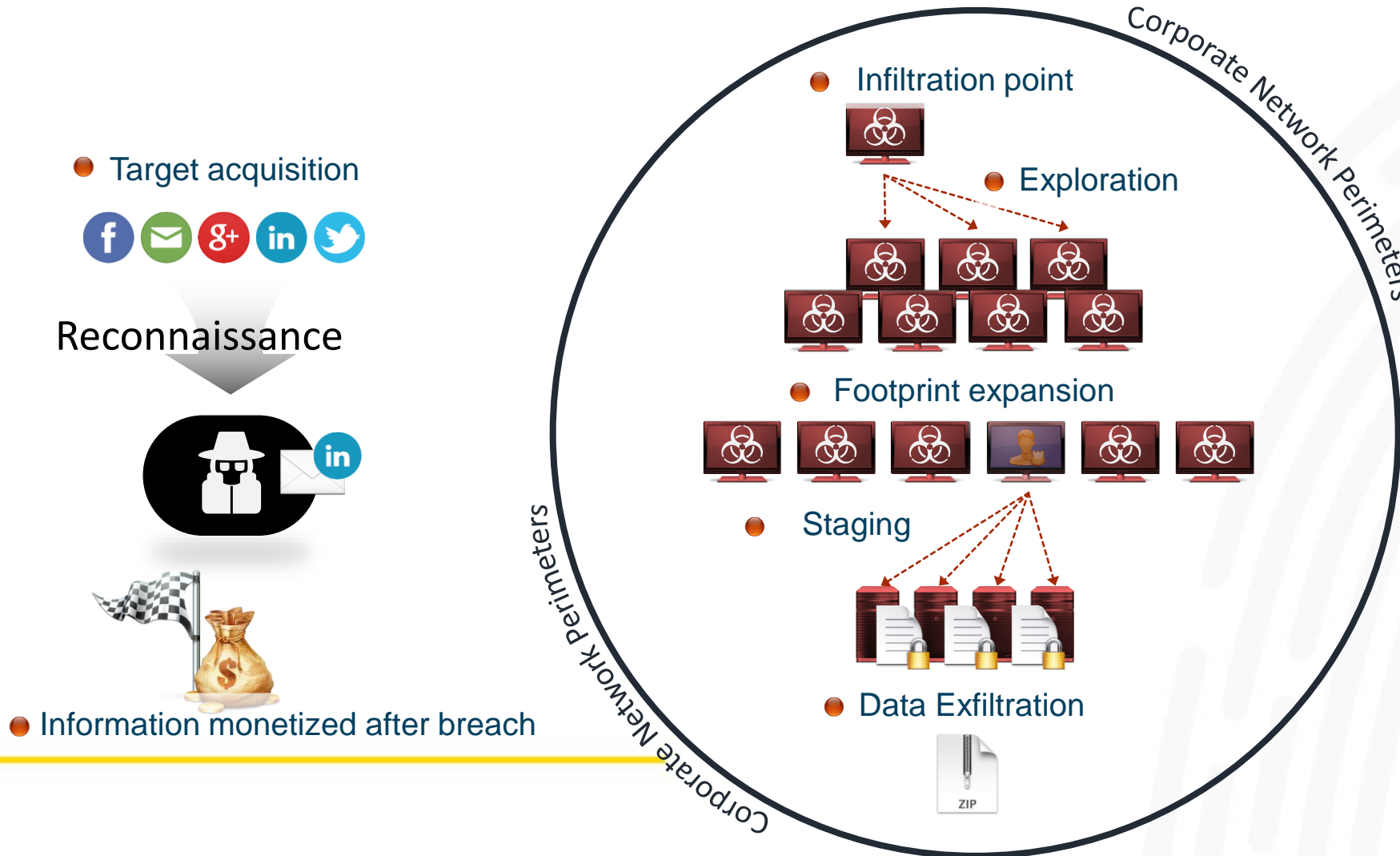
ZERODAY REPORTS

[VIEW FULL LIST OF ZERODAY REPORTS](#)

REPORT ID	SOFTWARE VENDOR	REPORT DATE
TALOS-CAN-0065	NTP	2015-09-29
TALOS-CAN-0064	NTP	2015-09-29
TALOS-CAN-0063	NTP	2015-09-29
TALOS-CAN-0062	NTP	2015-09-29
TALOS-CAN-0061	Libgraphite	2015-10-8
TALOS-CAN-0060	Libgraphite	2015-10-08
TALOS-CAN-0059	Libgraphite	2015-10-08
TALOS-CAN-0058	Libgraphite	2015-10-08
TALOS-CAN-0056	Vmware	2015-09-29
TALOS-CAN-0055	NTP	2015-09-29

Dissecting a Data Breach (Kill Chain)

You Can't Protect What You Don't See !



New ransomware abuses Windows PowerShell, Word document macros

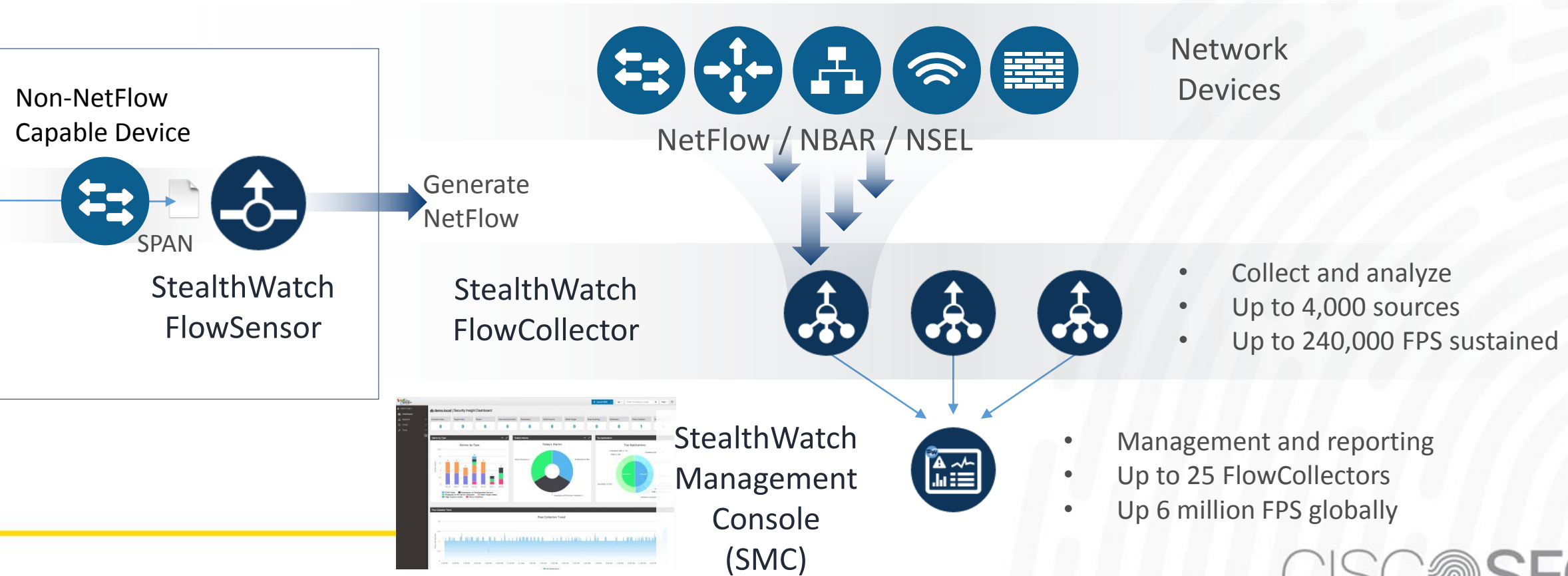




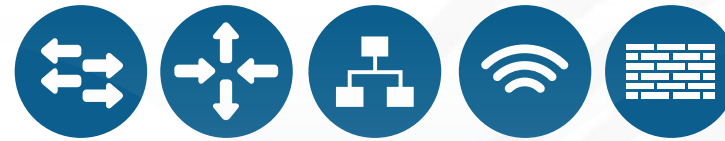
Network as a Sensor / Enforcer



Cisco StealthWatch: System Overview



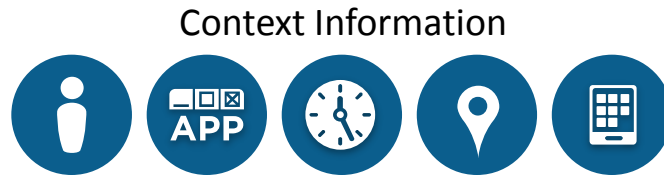
Network as a Sensor: Cisco StealthWatch



NetFlow



Cisco ISE



Mitigation Action

ISE pxgrid for
Remediation

Lancope

VISION TO SECURE, INTELLIGENCE TO PROTECT



Real-time visibility at all network layers

- Data Intelligence throughout network
- Assets discovery
- Network profile
- Security policy monitoring
- Anomaly detection
- Accelerated incident response



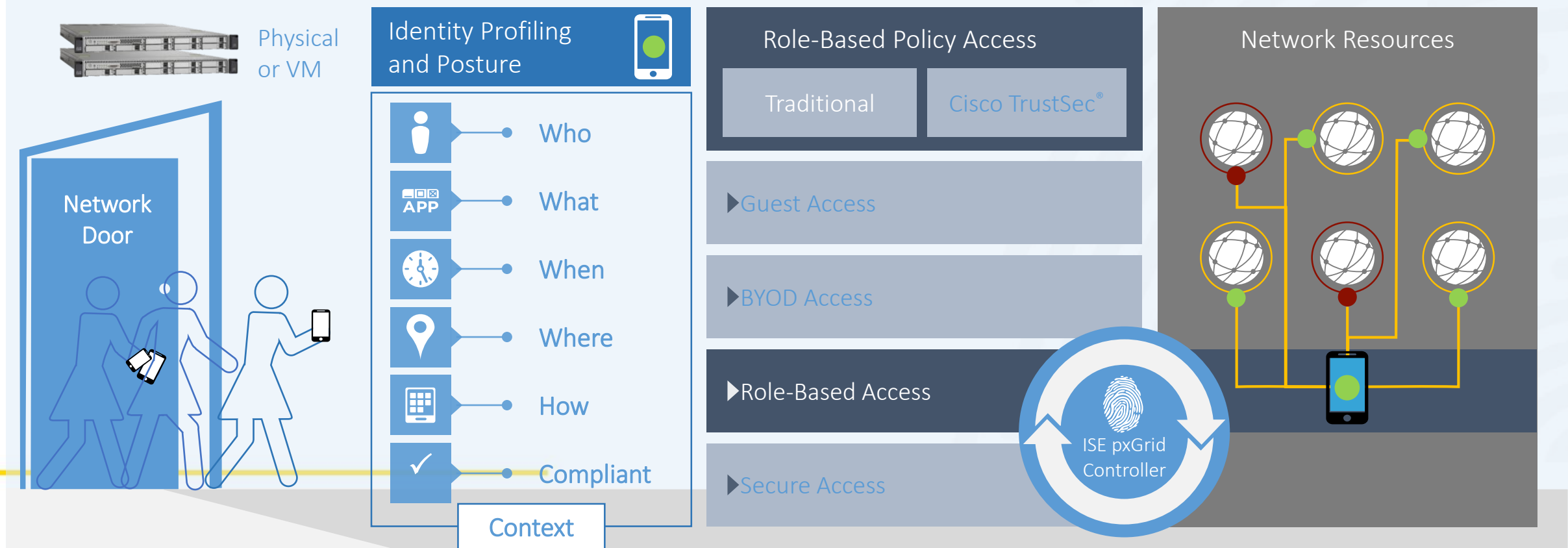
Identity



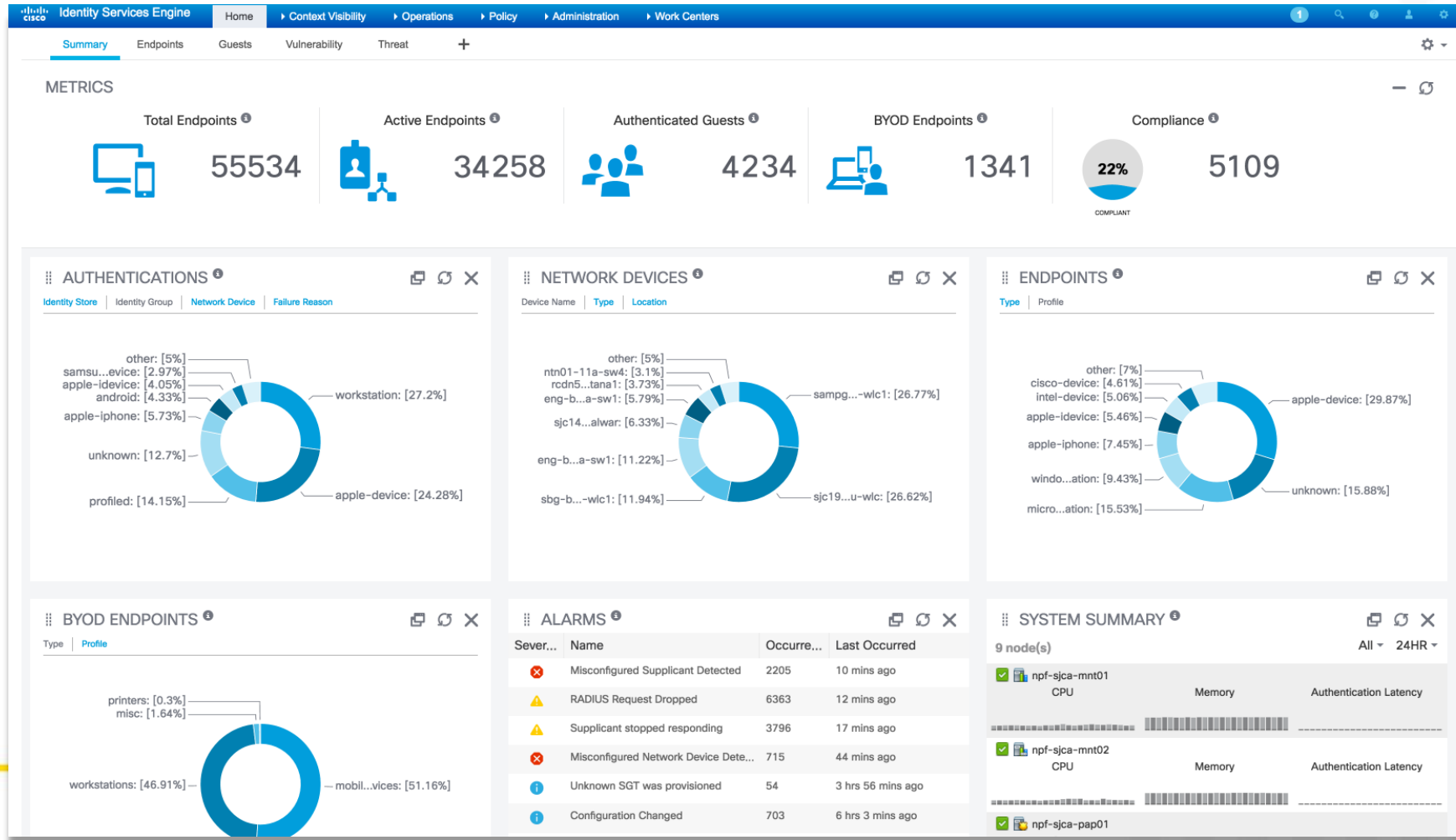
Cisco Identity Services Engine



A centralized security solution that automates context-aware access to network resources and shares contextual data



Security starts with 'Visibility'



Role-Based Access

TACACS+ Device Administration Support for Cisco ISE 2.0



What's New for Cisco ISE 2.0?

Customers can now use TACACS+ with Cisco ISE to simplify device administration and enhance security through flexible, granular control of access to network devices.

Benefits



Simplified, Centralized Device Administration
Increase security, compliance, and auditing for a full range of administration use cases



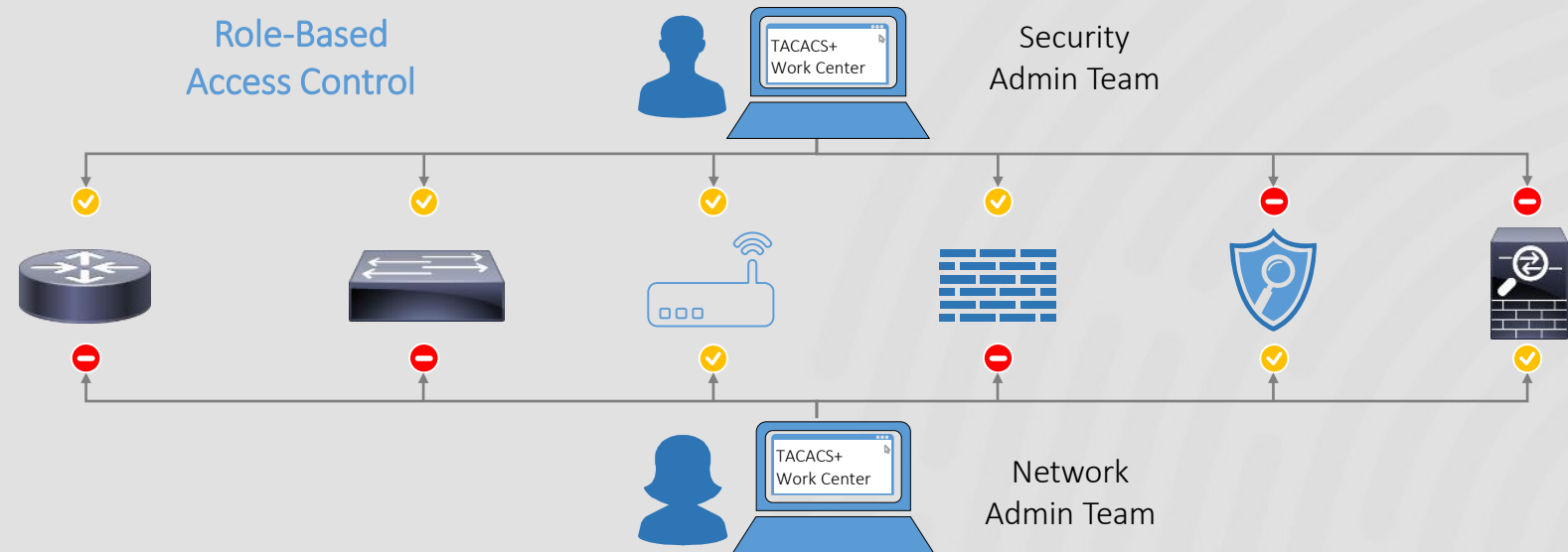
Flexible, Granular Control
Control and audit the configuration of network devices



Holistic, Centralized Visibility
Get a comprehensive view of TACACS+ configurations with the TACACS+ administrator work center

TACACS+ Device Administration

Role-Based Access Control



Capabilities

- Role-based access control
- Flow-based user experience
- Command-level authorization with detailed logs for auditing

- Dedicated TACACS+ work center for network administrators
- Support for core Cisco Secure Access Control System 5 (ACS5) features

Visibility



Versions of NetFlow



Version 5
Fixed Format
18 Defined Entities

Version 9
Template Based
108 Defined Entities

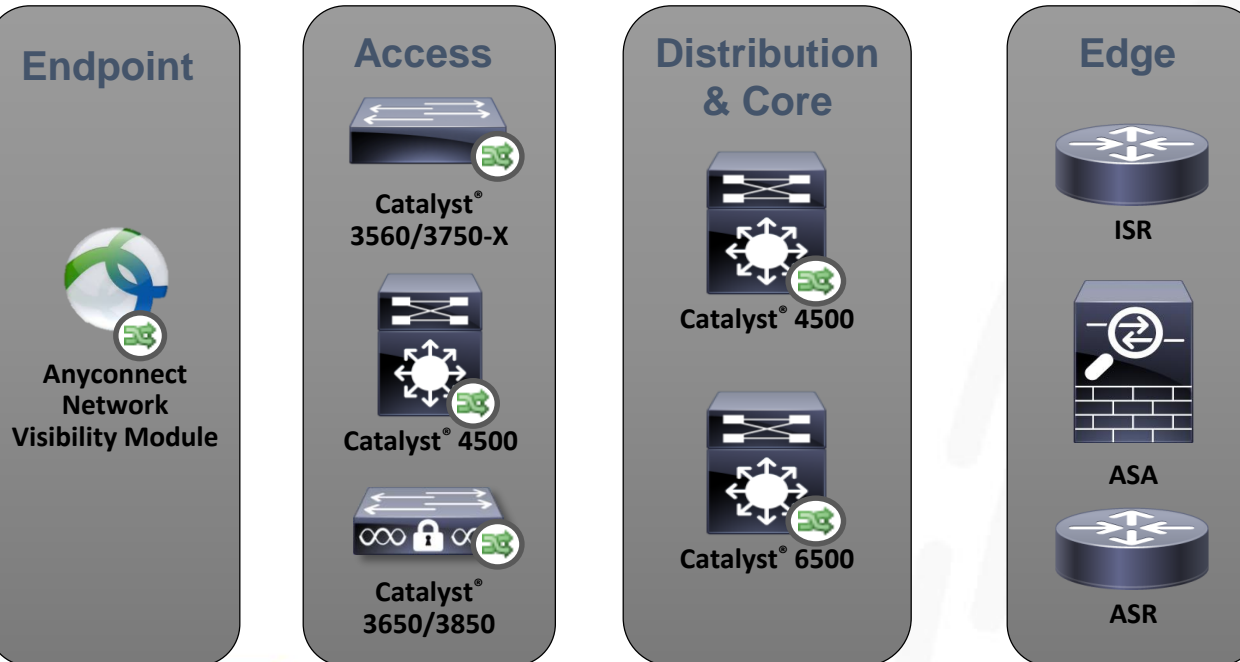
IPFIX
Standardized
Template Based
Variable Length Fields
450+ Defined Entities



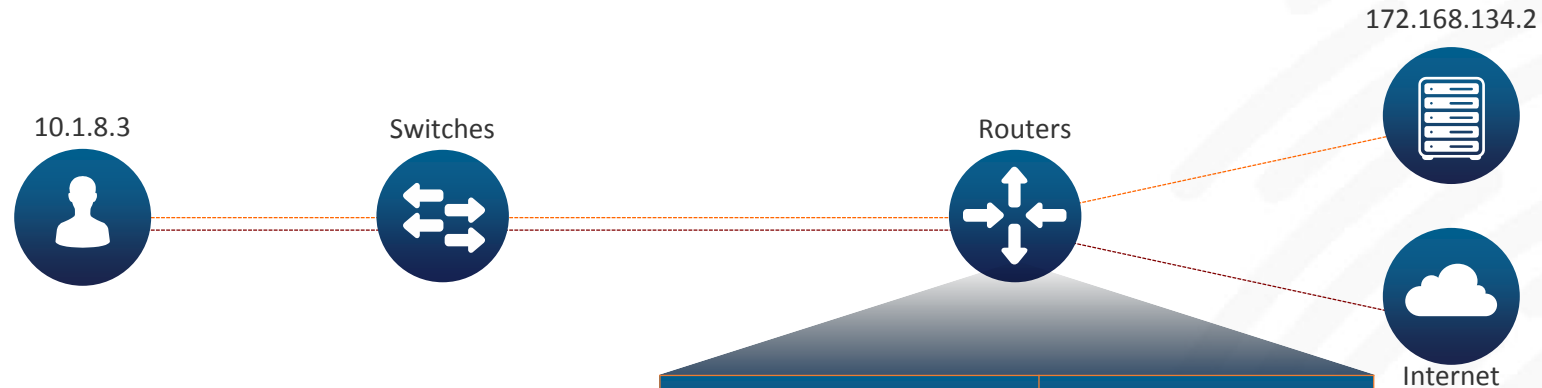
NetFlow Deployment



Each network layer offers unique telemetry capabilities



Visibility through NetFlow



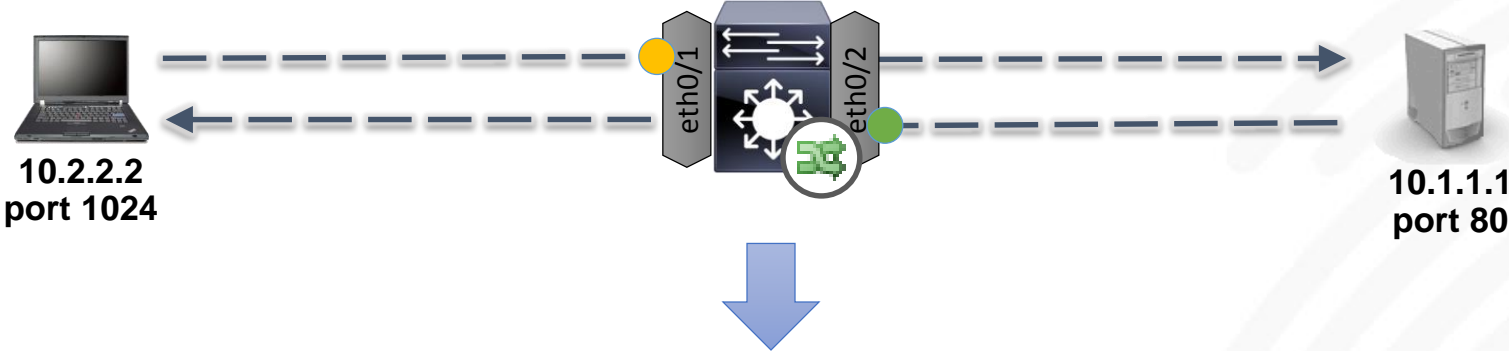
NetFlow provides

- **Trace of every conversation** in your network
- An ability to collect record **everywhere** in your network (switch, router, or firewall)
- Network usage measurement
- An ability to find north-south as well as east-west **communication**
- **Light weight visibility** compared to SPAN based traffic analysis
- **Indications of Compromise (IOC)**
- Security Group Information

Flow Information	Packets
SOURCE ADDRESS	10.1.8.3
DESTINATION ADDRESS	172.168.134.2
SOURCE PORT	47321
DESTINATION PORT	443
INTERFACE	Gi0/0/0
IP TOS	0x00
IP PROTOCOL	6
NEXT HOP	172.168.25.1
TCP FLAGS	0x1A
SOURCE SGT	100
:	:
APPLICATION NAME	NBAR SECURE-HTTP



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 - The Network Phone Bill



Telephone Bill



Monthly Statement
Bill At-A-Glance

#	Date	Time	Number Called	Min	Airtime Charge	LD/Add'l Charge	Feature	Total Charge
1	01/06/2013	02:05PM	678-936-2247	7	0.00	0.00	M2AM	0.00
2	01/06/2013	02:13PM	678-617-8151	1	0.00	0.00	M2AM	0.00
3	01/06/2013	02:14PM	678-617-7783	1	0.00	0.00	M2AM	0.00
4	01/06/2013	02:19PM	678-617-7783	7	0.00	0.00	M2AM	0.00
5	01/06/2013	02:35PM	678-997-8365	2	0.00	0.00	M2AM	0.00
6	01/06/2013	03:58PM	678-617-6101	2	0.00	0.00	M2AM	0.00
7	01/06/2013	04:00PM	678-617-6151	15	0.00	0.00	CW	0.00
8	01/06/2013	05:46PM	678-617-6151	36	0.00	0.00	M2AM	0.00
9	01/06/2013	06:23PM	678-997-8365	2	0.00	0.00	M2AM	0.00
10	01/06/2013	07:42PM	678-617-6151	6	0.00	0.00	M2AM	0.00
11	01/06/2013	07:47PM	678-617-7783	4	0.00	0.00	CW	0.00



Flow Record

NetFlow = shows you the **who, what, where and when**. It's a phone bill, which we use to look for out of the ordinary behaviour.

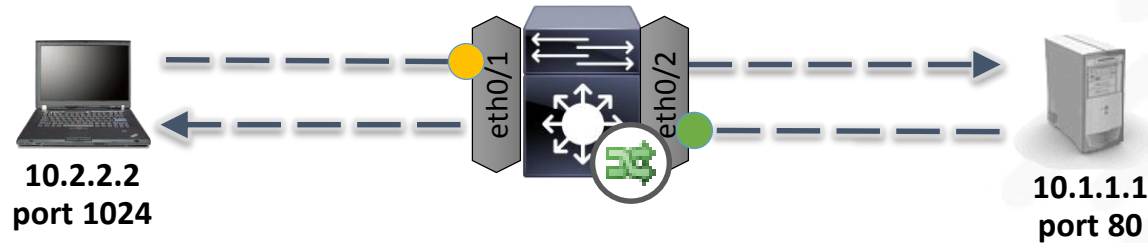
Flow Table - 840 records

Start Active Time	Client Host	Client Zone	Server Host	Server Zone	Service Summary	Average Rat...
Apr 12, 2010 8:41:56 AM 16 hours 32 minutes 109 ago	10.201.3.96	Sales and Marketing	72.21.202.71	United States	http (80/tcp)	6.66M
Apr 12, 2010 8:43:14 AM 16 hours 30 minutes 57 ago	10.201.3.96	Sales and Marketing	216.165.129.141	United States	http (80/tcp)	2.65M
Apr 17, 2010 6:45:51 AM 16 hours 28 minutes 15 ago	10.201.3.96	Sales and Marketing	68.142.118.67	United States	http (80/tcp)	2.51M
Apr 17, 2010 6:41:34 AM 16 hours 30 minutes 52 ago	10.201.3.96	Sales and Marketing	77.21.202.98	United States	http (80/tcp)	1.81M
Apr 12, 2010 8:52:48 AM 16 hours 21 minutes 186 ago	10.201.3.96	Sales and Marketing	10.201.1.221	United States	http (80/tcp)	1.81M
Apr 14, 2010 7:22:52 AM 17 hours 51 minutes 131 ago	10.201.3.96	Sales and Marketing	10.202.1.221	Engineering	http-alk (8080/tcp)	1.5M
Apr 12, 2010 9:02:34 AM 16 hours 11 minutes 37 ago	10.201.3.96	Sales and Marketing	10.202.1.221	Engineering	http-alk (8080/tcp)	960.19k
Apr 17, 2010 6:47:36 AM 16 hours 30 minutes 50 ago	10.201.3.96	Sales and Marketing	72.233.96.254	United States	http-alk (8080/tcp)	952.29k
Apr 17, 2010 6:57:51 AM 16 hours 18 minutes 181 ago	10.201.3.96	Sales and Marketing	77.197.164.64	United States	http-alk (8080/tcp)	823.24k
Apr 12, 2010 10:18:55 AM 16 hours 37 minutes 186 ago	10.201.3.96	Sales and Marketing	77.21.202.165	United States	http (80/tcp)	699.28k
Apr 14, 2010 6:42:35 AM 16 hours 30 minutes 211 ago	10.201.3.96	Sales and Marketing	10.201.0.15	United States	http (80/tcp)	644.78k
Apr 12, 2010 2:59:36 PM 14 minutes 305 ago	10.201.3.96	Sales and Marketing	63.245.217.21	United States	http (80/tcp)	530.9k
Apr 12, 2010 6:43:09 AM 16 hours 30 minutes 57 ago	10.201.3.96	Sales and Marketing	72.5.124.55	United States	http (80/tcp)	512.61k
Apr 12, 2010 6:43:10 AM 16 hours 30 minutes 57 ago	10.201.3.96	Sales and Marketing	63.245.209.115	United States	http (80/tcp)	326.48k
Apr 12, 2010 6:43:10 AM 16 hours 30 minutes 57 ago	10.201.3.96	Sales and Marketing	72.4.114.305	United States	http (80/tcp)	295.9k

NetFlow Collection: Flow Stitching



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



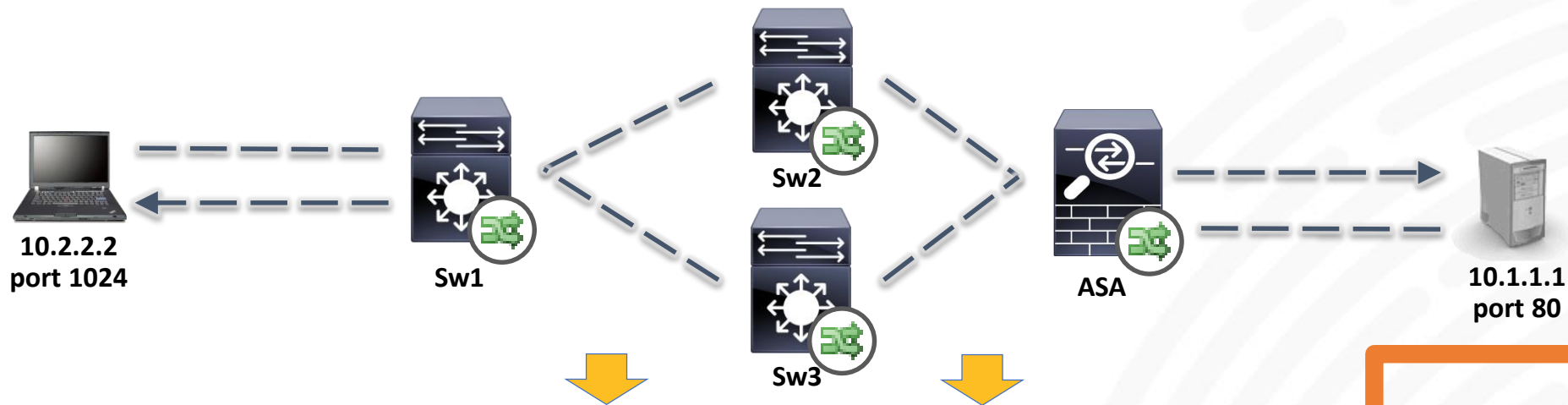
Start Time	Client IP	Client Port	Server IP	Server Port	Proto	Client Bytes	Client Pkts	Server Bytes	Server Pkts	Client SGT	Server SGT	Interfaces
10:20:12.221	10.2.2.2	1024	10.1.1.1	80	TCP	1025	5	28712	17	100	1010	eth0/1 eth0/2

Bi-directional:

- Conversation flow record
- Allows easy visualization and analysis

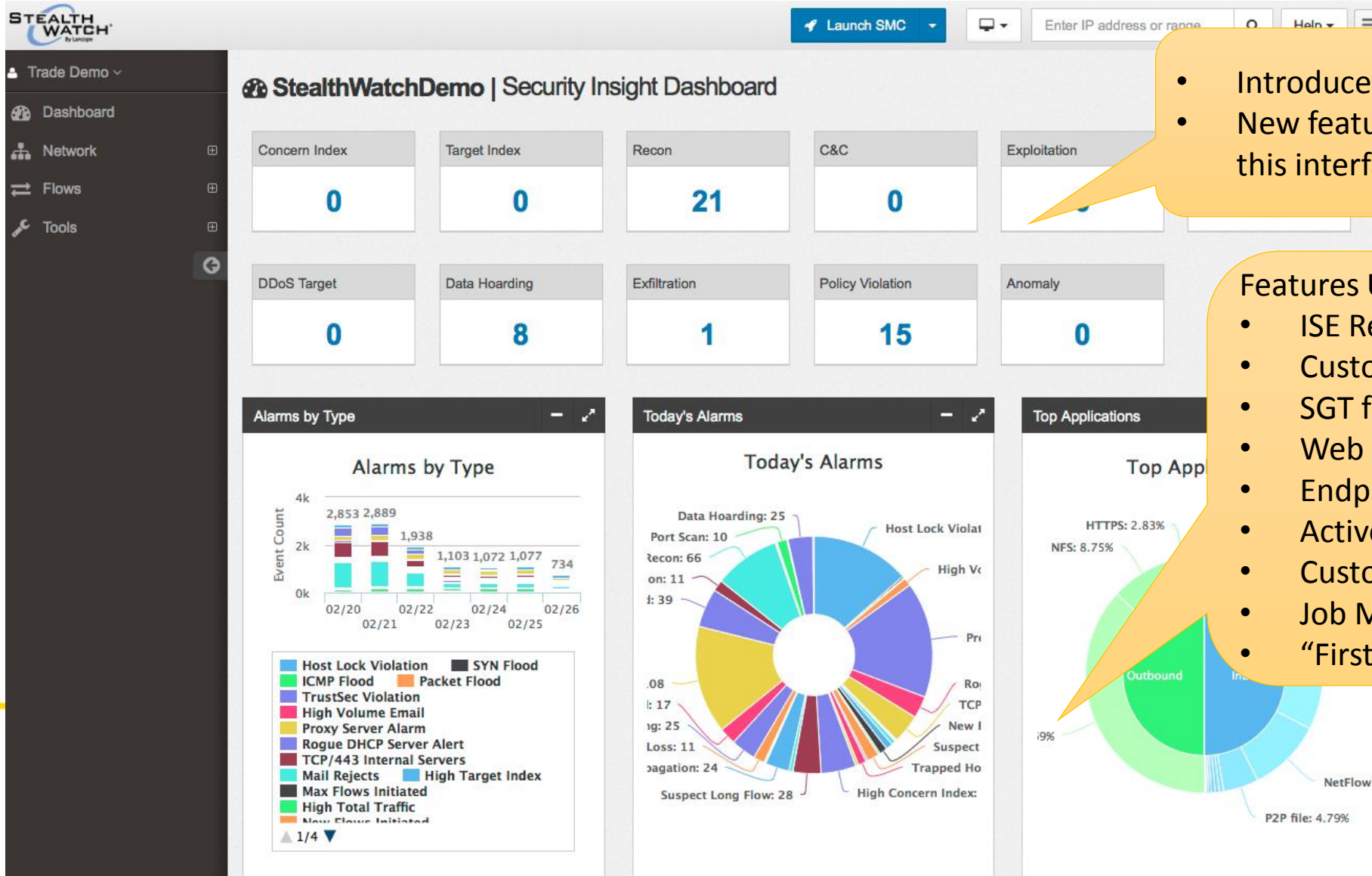


NetFlow Collection: De-duplication



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

Aside: SMC Interface 1: “Web” Interface



• Introduced in Stealthwatch 6.5
• New features/functionality is added to this interface

Features Unique to Web Interface:

- ISE Remediation
- Custom Events
- SGT fields in Flow Record
- Web proxy data
- Endpoint data
- Active Directory Configuration
- Custom Applications
- Job Management
- “First Seen”



Aside: SMC Interface 2: Java (Swing) Client



The screenshot displays the StealthWatch Management Console interface. The left sidebar shows a tree view of the network hierarchy under 'Enterprise', including 'SMC', 'StealthWatch Labs Intelligence Cent', and 'StealthWatchDemo'. The main area is divided into several panels:

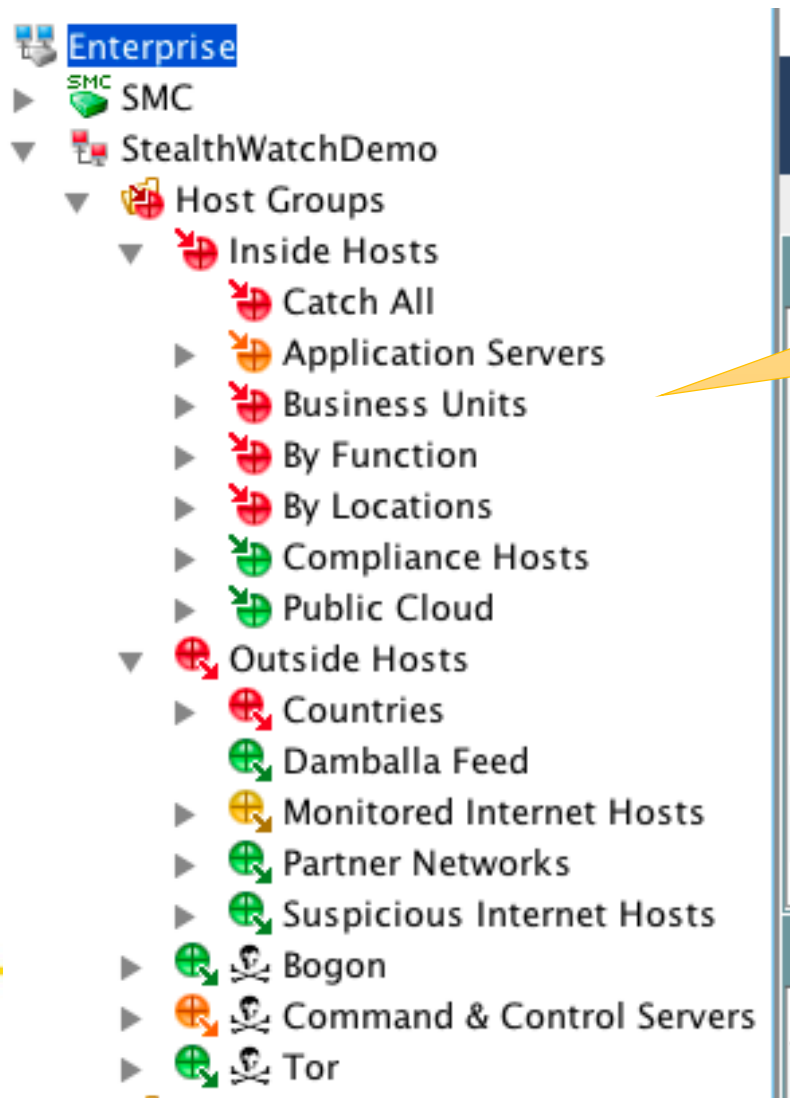
- Cyber Threats**: Filtered by Domain: StealthWatchDemo. Includes tabs for Reputation, Reconnaissance, Data Loss, and Malware.
- Suspicious Internal Hosts - Today - 4...**: Table with columns: Host Gr..., Host, CI%, Alerts. Data rows include Atlanta, Infrastructure, Desktops, Virtual Desktop (10.201.3.83), Catch All (199.204.23.227), New York, Desktops (10.10.101.24), and Sales and (wkstation50).
- Suspicious Outside Hosts - Today - ...**: Table with columns: Country, Host, CI%, Alerts. Data rows include United States (69.160.42.248), China (58.221.60.166), Turkey (78.187.95.226), and (61.175.101.118).
- Possible Victims - Today - 44 records summ...**: Table with columns: Touched..., Touched..., High CI Co..., High CI Host. Data rows include New York, Desktops (10.20.10.254), Servers (10.201.0.28), Servers (10.201.0.19), Domain Controller/DNS (10.201.0.16), and Atlanta, Infrastructure, Desktops (10.201.3.83).

At the bottom, it says 'Last refreshed: Feb 26, 2016 10:31:37 AM'.

- Original interface
- Years of development and functionality
- Built by engineers for engineers
- New development minimal

SEC

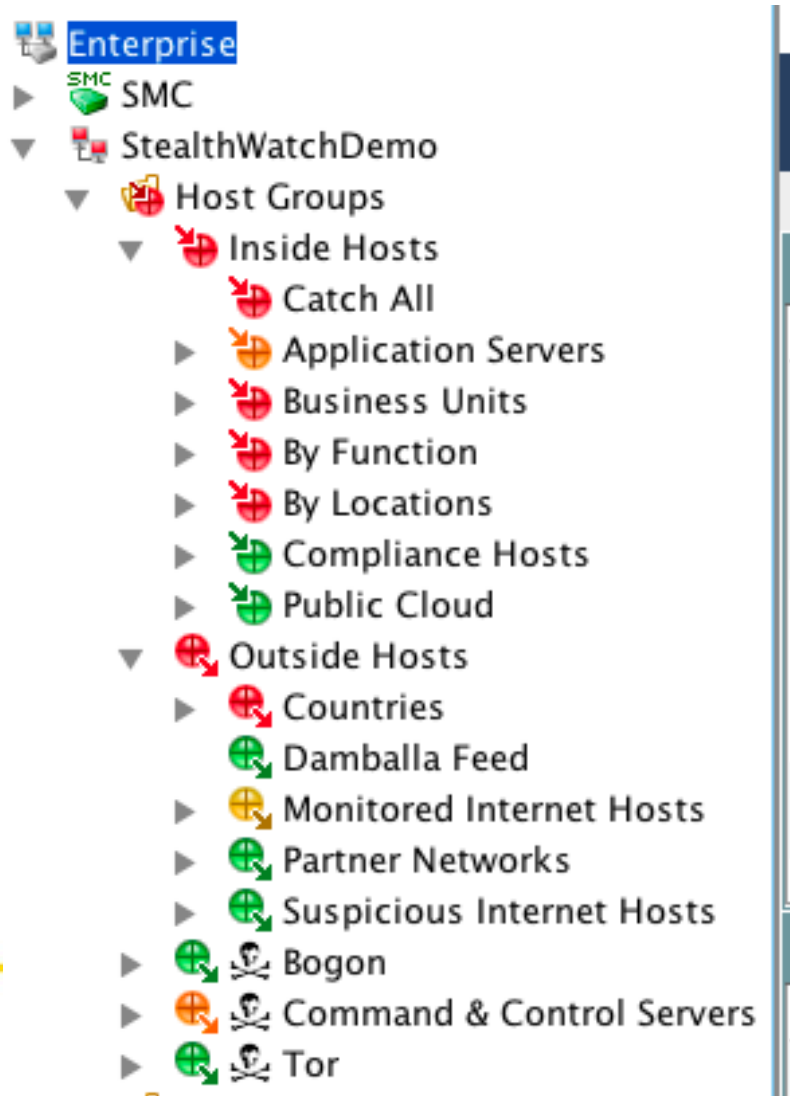
Concept: Host Groups



- Virtual Container of IP Addresses
- User defined
- Similar attributes
- Model any Process/Application



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
- **SLIC Created**
 - Bogon
 - Command & Control Servers
 - Tor

Conversational Flow Record



Duration	Who	Search Subject	Port	Traffic Summary	Port	Peer
Start: 05/29 - 12:19:18 PM End: 05/29 - 12:20:58 PM Duration: 1m 40s		10.10.18.102 RFC 1918 employee1 00:50:56:b4:3f:af	4866/TCP	11.49KB 285 packets → HTTP ← 1.62MB 1.15K packets	80/TCP	216.191.247.145 Canada crl.entrust.net

When

Where

How

What

Who

More context

- Highly scalable (enterprise class) collection
- High compression => long term storage
 - Months of data retention

Flow Detailed Summary: 10.10.18.102

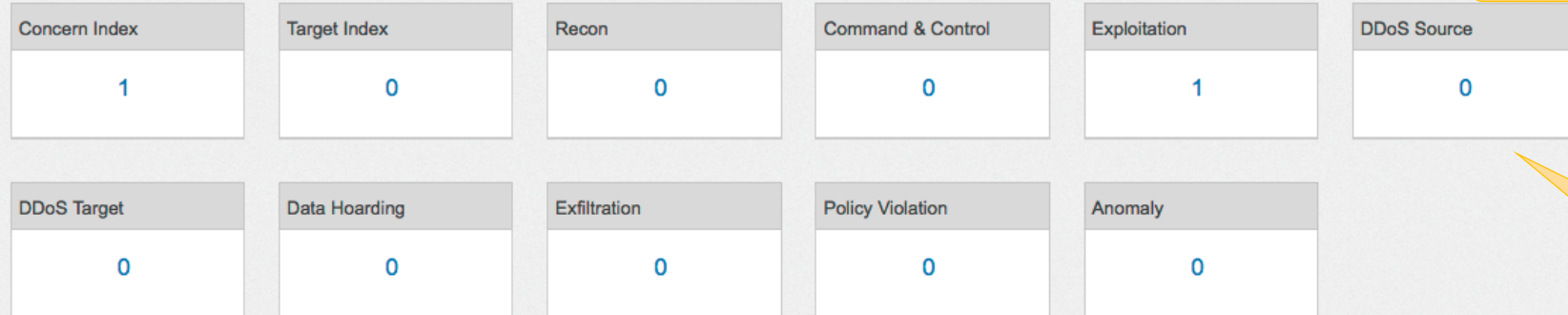
Search Subject Details	Totals	Peer Details
Packets: 285	Packets: 1.44K	Packets: 1.15K
Packet Rate: 2.85pps	Packet Rate: 14.37pps	Packet Rate: 11.52pps
Bytes: 11.49KB	Bytes: 1.63MB	Bytes: 1.62MB
Byte Rate: 117.69bps	Byte Rate: 17.11Kbps	Byte Rate: 16.99Kbps
Percent Transfer: 0.6879458949171267%	Search Subject/Peer Ratio: 0.01	Percent Transfer: 99.31205410508288%
Host Groups: Desktops	TCP Connections: 2	Host Groups: Canada
TrustSec ID: 100	RTT: 2ms	Payload: 200 OK
TrustSec Name: Employees	SRT: 498ms	TrustSec ID: 0
Payload: GET http://crl.entrust.net/2048ca.crl		TrustSec Name: Unknown

[Close](#)

Profiling a Host



Lancope | Host Report for 10.201.3.59



Host report for 10.201.3.59

Behavior alarms

Host Summary

Host IP
10.201.3.59

View Flows | Classify | History

Status: Active

Hostname: lsharp-I1.lancope.local

Host Groups: Atlanta, Sales and Marketing, Desktops

Location: RFC 1918

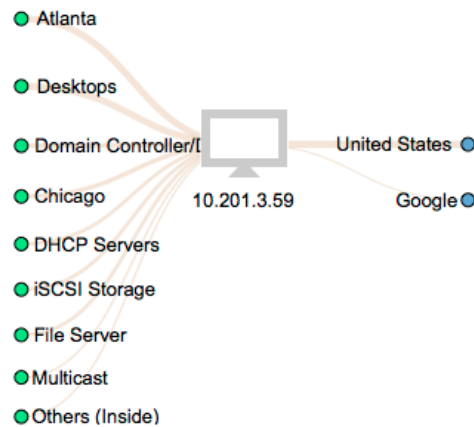
Last Seen: 6/5/15 1:08 PM

Policies: High Target Index Supress, Inside

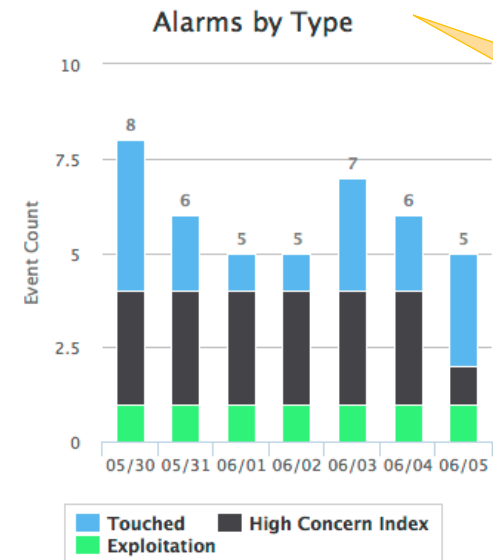
MAC Address: c8:2a:14:26:a8:61 (Apple Inc)

Summary information

Traffic by Peer Host Group (last 12 hours)



Alarms by Type (last 7 days)



Quick view of host group communication



New: StealthWatch to ThreatGrid External Lookup



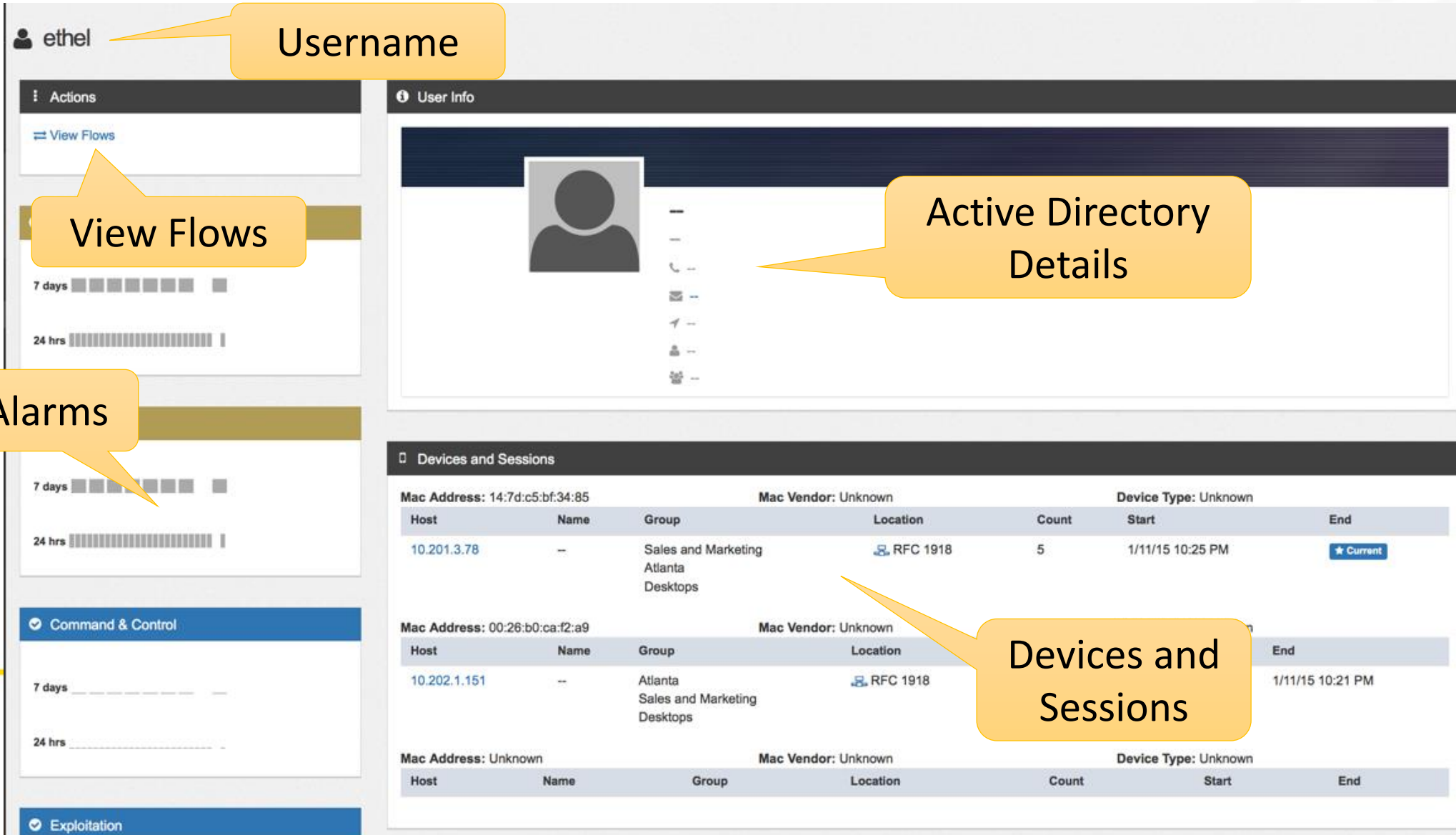
Flow Query Results

Duration	Search Subject	Port	Traffic Summary	Port	Peer
Start: 06/15/2015 - 10:49:20 PM End: 06/15/2015 - 10:49:20 PM Duration: 0s	10.10.18.104 REC.1918	53272/UDP	386B 2 packets → LDAP (unclassified) ← 0B 0 packets	389/UDP	 10.1.100.100 RFC 1918
Start: 06/15/2015 - 10:46:05 PM End: 06/15/2015 - 10:49:16 PM Duration: 3m 11s	Ziften: Source Lookup Cisco ThreatGrid	P	4.87KB 60 packets → NetBIOS (unclassified)	138/UDP	 10.1.100.100

Dynamic Analysis
lookup



Extrapolating to a User



The screenshot displays a user profile for 'ethel'. The interface includes a left sidebar with navigation options: 'Actions' (containing 'View Flows'), 'Alarms', 'Command & Control', and 'Exploitation'. The main content area is divided into 'User Info' and 'Devices and Sessions'.

Username: ethel

View Flows: A section with a 'View Flows' link and two bar charts for '7 days' and '24 hrs'.

Alarms: A section with two bar charts for '7 days' and '24 hrs'.

Active Directory Details: A section showing a user profile icon and a list of icons representing various details.

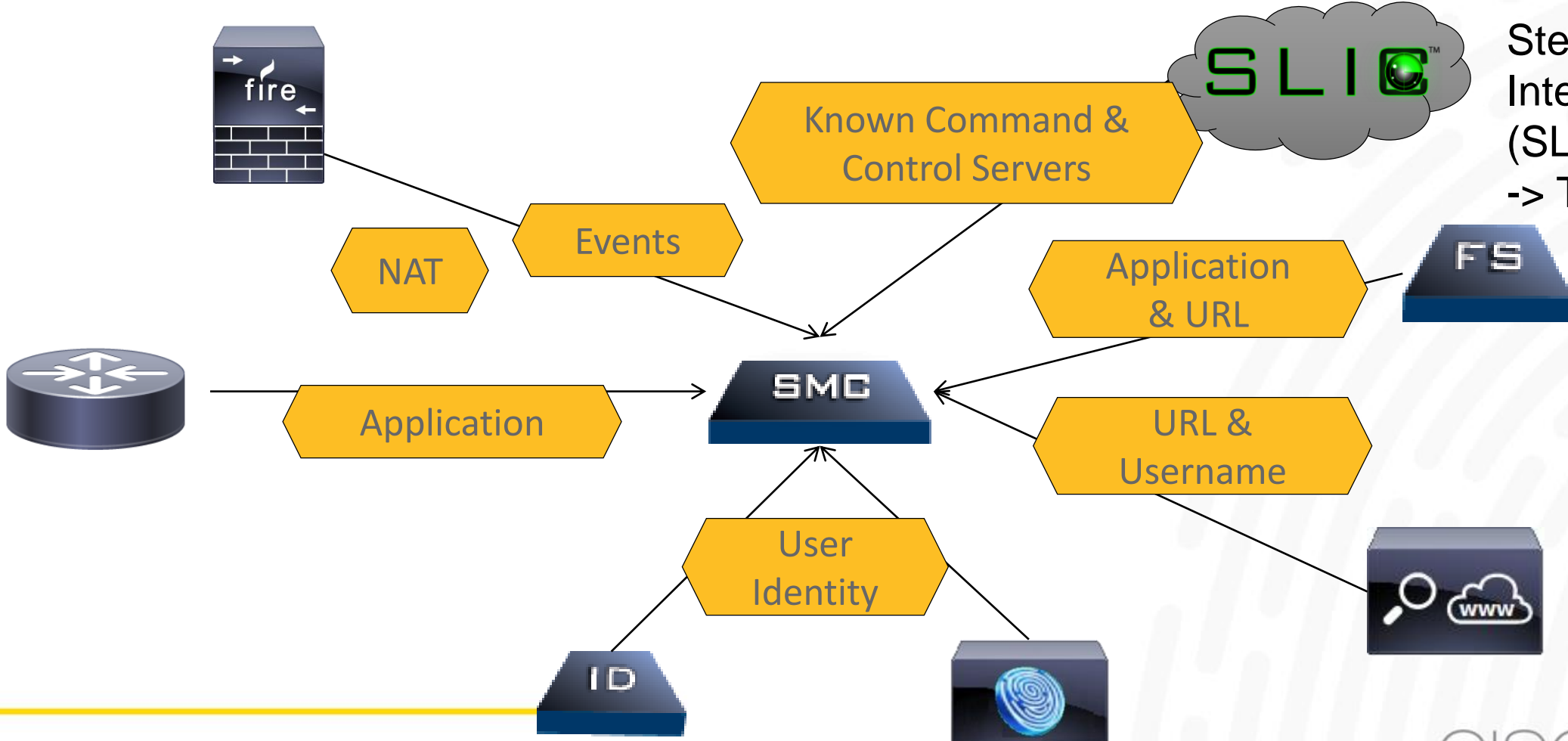
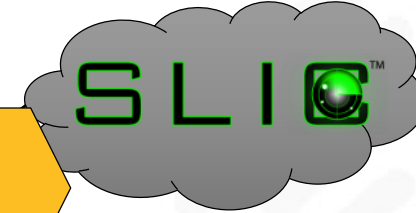
Devices and Sessions: A table listing active sessions for the user.

Mac Address	Mac Vendor	Device Type				
14:7d:c5:bf:34:85	Unknown	Unknown				
Host	Name	Group	Location	Count	Start	End
10.201.3.78	--	Sales and Marketing Atlanta Desktops	RFC 1918	5	1/11/15 10:25 PM	★ Current
00:26:b0:ca:f2:a9	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown
Host	Name	Group	Location	Count	Start	End
10.202.1.151	--	Atlanta Sales and Marketing Desktops	RFC 1918			1/11/15 10:21 PM
Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown
Host	Name	Group	Location	Count	Start	End

Adding Context and Situation Awareness



StealthWatch Labs
Intelligence Center
(SLIC) Threat Feed
-> TALOS



Policy and Indication of Compromise IoC

NetFlow Analysis with StealthWatch can help:

Discovery

- Identify business critical applications and services across the network

Identify additional IOCs

- Policy & Segmentation
- Network Behaviour & Anomaly Detection (NBAD)

Better understand / respond to an IOC:

- Audit trail of all host-to-host communication

Locate Assets – Discovery



Search:

Enterprise
SMC
demo.local
Host Groups
Inside Hosts
Outside Hosts
Bo...
Co...
To...
Network
VM Server
Maps
Funct...
Intern...
Intern...
FlowColl...
sfc.de...
Ex...
FlowSensors
Identity Services
ise-ciscolive.cts.local

Active Hosts x Host Information x
Filter Domain : demo.local
Host Group : Inside Hosts
Time : Last 1 day ending Today
Summary - 67 records summarized in...

Host Group Dashboard
Host Groups
Catch All
Catch All
Active Hosts
Host Information
Host Notes
Identity and Device Table
Host Group Trends
Catch All
Catch All

Filter - Host Information
Hosts
Server Services
Client Services
Server Applications
Client Applications
Alarms
Alerts
Events
Systems

Server Applications
 Filter by applications
Match Any All
Clearcase
DHCP
DNS
DNS (unclassified)
Decryption Client
Dropbox
ESPN
FIX
FTP
FTP (unclassified)
Facebook
File Sharing
Finger
Flickr
Gopher
HTTP
HTTP (unclassified)
HTTPS

Help Cancel OK

Find hosts communicating on the network

- Pivot based on transactional data

- Enterprise
- ▶ SMC
- ▼ StealthWatchDemo
 - ▼ Host Groups
 - ▼ Inside Hosts
 - ▶ Catch All
 - ▶ Application Servers
 - ▶ Business Units
 - ▶ By Function
 - ▶ By Locations
 - ▶ Compliance Hosts
 - ▶ Public Cloud
 - ▼ Outside Hosts
 - ▶ Countries
 - ▶ Damballa Feed
 - ▶ Monitored Internet Hosts
 - ▶ Partner Networks
 - ▶ Suspicious Internet Hosts
 - ▶ Bogon
 - ▶ Command & Control Servers
 - ▶ Tor

Host groups and reports make it easier to hunt

Host Groups – Discovering Rogue Hosts



The screenshot shows the Cisco ISE Host Groups tree. The 'Catch All' group is highlighted under 'Inside Hosts'. A context menu is open for 'Catch All', showing options like 'Host Group Dashboard', 'Top', 'Status', 'Security', 'Hosts', 'Traffic', 'Reports', 'Flows', and 'Configuration'. The 'Hosts' option is selected, and a sub-menu is open showing 'Active Hosts', 'Host Information', 'Host Notes', 'Identity and Device Table', and 'Host Group Trends'. The 'Identity and Device Table' is highlighted. Two callouts are present: one pointing to 'Catch All' with the text 'Catch All: All unclassified RFC1918 addresses', and another pointing to 'Identity and Device Table' with the text 'Table of all individual hosts'.

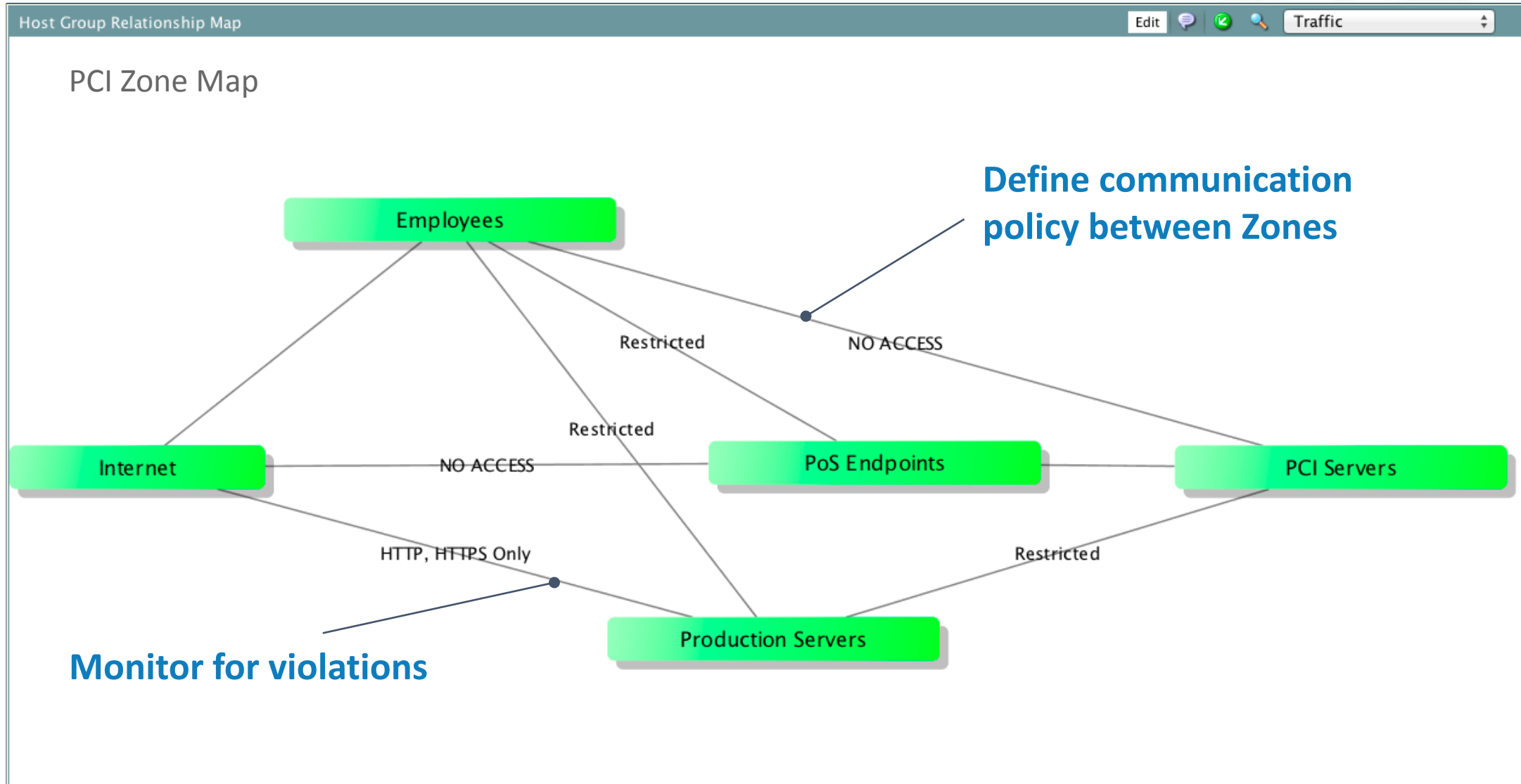
Catch All: All unclassified RFC1918 addresses

Table of all individual hosts

Host Group	Sub-Group	Option
Enterprise	Host Groups	Host Group Dashboard
		Top
		Status
		Security
		Hosts
		Traffic
		Reports
		Flows
		Configuration
		Expand All
		Collapse All
		Refresh Tree
		Active Hosts
		Host Information
Host Notes		
Identity and Device Table		
Host Group Trends		



Policy & Segmentation with StealthWatch



Policy Violation: Host Locking



Host Locking: Add Rule

Name:

Description:

Client Host Group:

Server Host Group:

Disallow all traffic except
 Allow all traffic except

Services

- 0-hop
- 3pc
- a/n
- afs
- ah
- Alan's port
- aol-im

Applications

- ActiveX
- Adobe Connect
- AFS
- authentication
- Blackberry
- business systems
- Citrix
- Clearcase

Unidirectional UDP traffic triggers alarm
 Unidirectional TCP traffic triggers alarm

Client group

Server group

Client traffic conditions

Server traffic conditions

Successful or unsuccessful



Policy Violation: Custom Security Events



Custom Event: Employee to PCI Servers

Rule/Event Name:
Employee to PCI Servers

Description:
Violation of Security Group Policy

Object

Host: +
User: +
Devices: +
Port/Protocol: +
TrustSec ID:
includes 100 +
TrustSec Name: +
Application: +
Orientation:
either

Peer

Host: +
User: +
Devices: +
Port/Protocol: +
TrustSec ID:
includes 2000 +
TrustSec Name: +
Application: +

Connection Details

Total Bytes greater than: ex. 4KB
Time of day: any

Total Packets greater than: ex. 4M
Duration greater than: ex. 2 hours

Custom event triggers on traffic condition

Rule name and description

Object conditions

Peer conditions

Source Tag

Destination Tag

Connection conditions



Policy Violation: Custom Security Events



demo.local | Alarm Dashboard : Policy Violation (1)

Alarm dashboard showing all Policy alarms

Alarms

First Active	Source Host Groups	Source	Target Host Groups	Target	Policy	Event Alarms	Source User	Details
5/25/15 4:42 PM	Catch All	10.10.18.102	--	Multiple Hosts	Inside Hosts	Employee to Production Servers	employee1	Expected 1 points, tolerance of 75 allows up to 300k points.

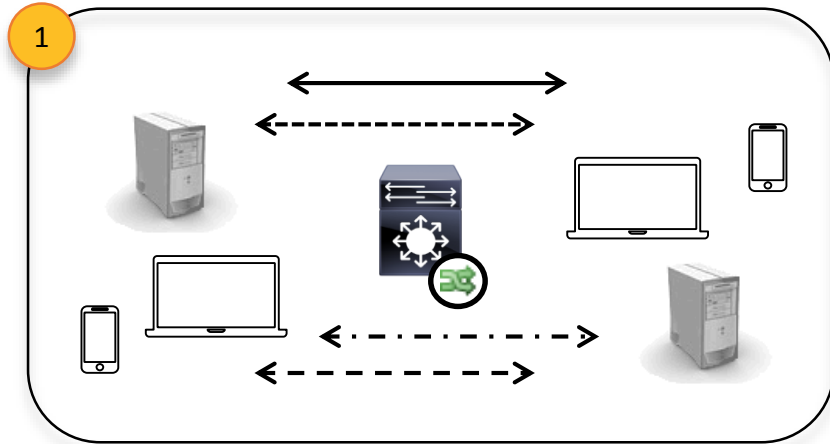
demo.local | Alarms : Employee to Production Servers for 5/25/2015 (1)

Details of "Employee to Productions Servers" alarm occurrences

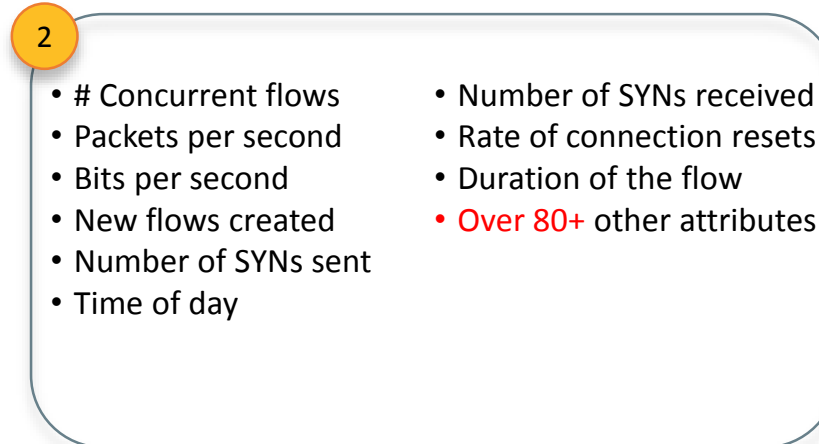
Alarms

First Active	Source Host Groups	Source	Target Host Groups	Target	Alarm	Policy	Source User	Details	Last Active	Active	Acknowledged
5/25/15 4:42 PM	Catch All	10.10.18.102	Catch All	10.3.200.10	Employee to Production Servers	Inside Hosts	employee1	View Details	Current	Yes	No

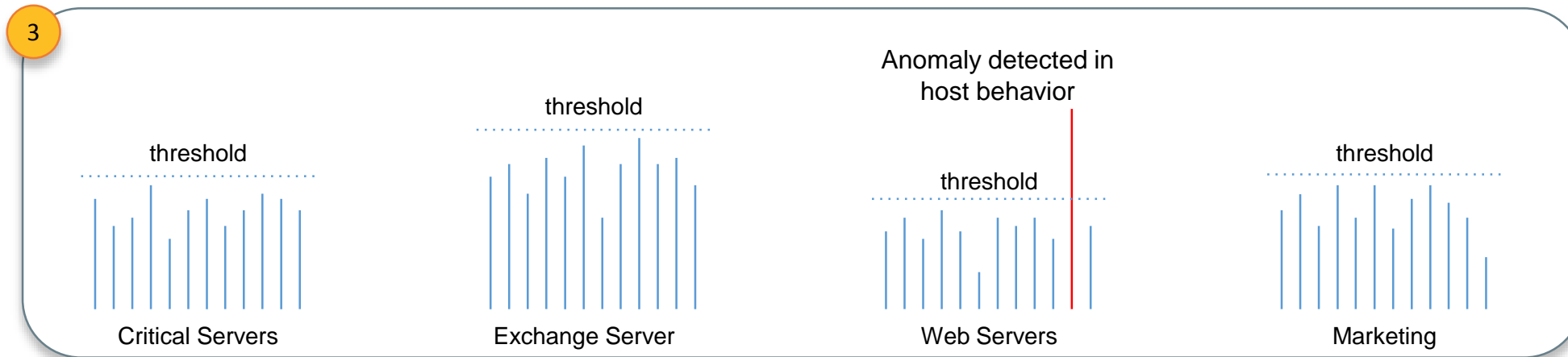
Flow-based Anomaly Detection



Collect & Analyze Flows

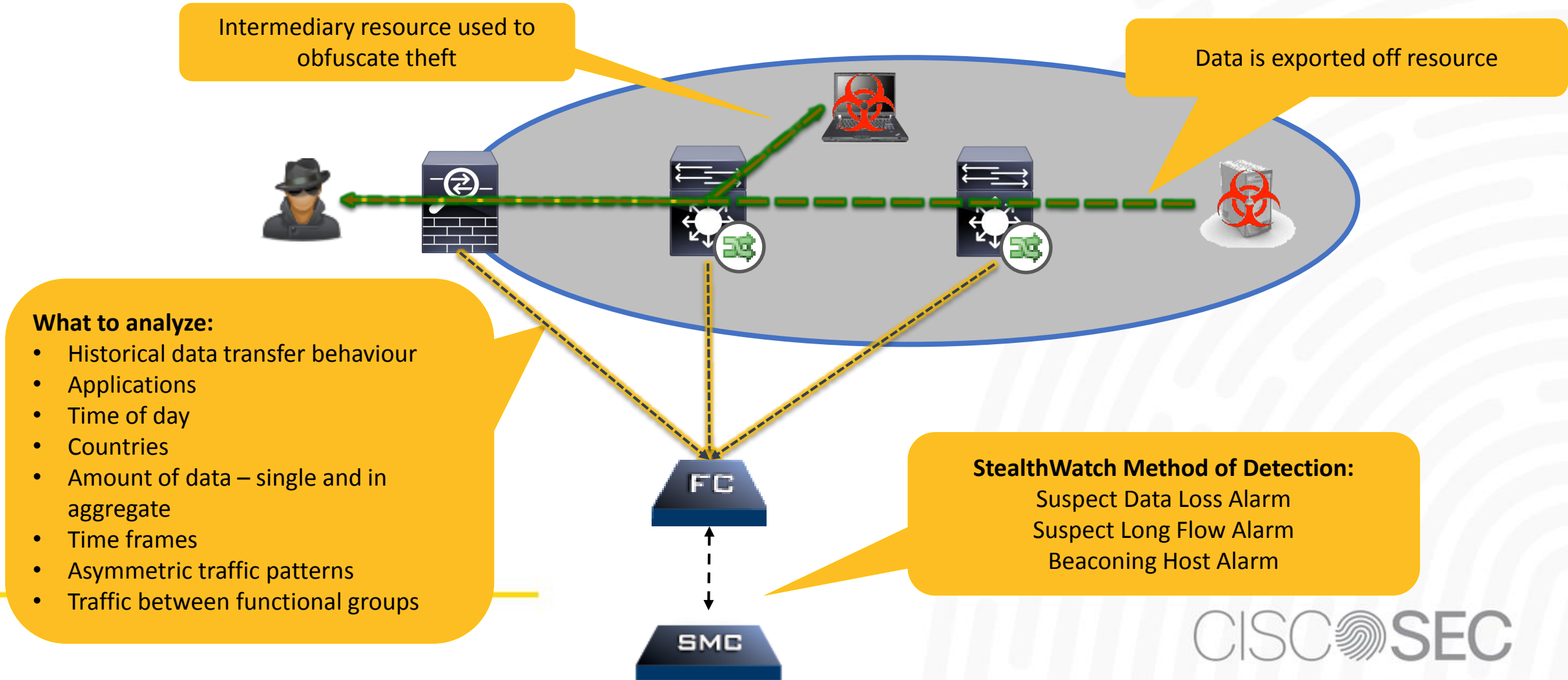


Establish Baseline of Behaviors



Alarm on Anomalies & Changes in Behavior

Detecting Data Loss



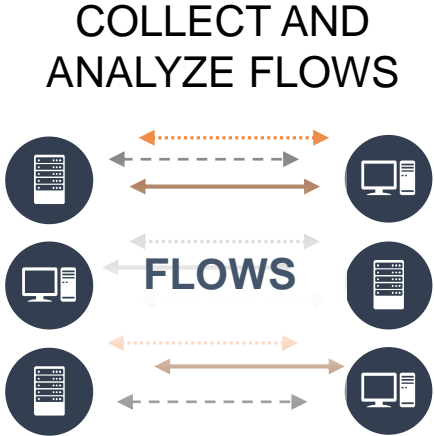
Behavioral Algorithms Are Applied to Build “Security Events”



SECURITY EVENTS (94 +)

ALARM CATEGORY

RESPONSE



- Addr_Scan/tcp
- Addr_Scan/udp
- Bad_Flag_ACK**
- Beaconing Host
- Bot Command Control Server
- Bot Infected Host - Attempted
- Bot Infected Host - Successful
- Flow_Denied
- .
- ICMP Flood
- .
- Max Flows Initiated
- Max Flows Served
- .
- Suspect Long Flow
- Suspect UDP Activity
- SYN Flood
- .

- Concern
- Recon
- C&C
- Exploitation
- Data Hoarding
- Exfiltration
- DDoS Target

- Alarm Table
- Host Snapshot
- Email
- Syslog / SIEM
- Mitigation



HTTPS Unclassified now **Known**



- AnyConnect **NVM** with Cisco Stealthwatch

Start	End	Duration	Subject Orientation	Subject IP Address	Subject NAT	Process Name
Dec 21, 2015 5:57:48 PM	Dec 21, 2015 6:16:59 PM	19m 11s	Client	172.16.31.14	10.0.0.6	Dropbox

- **Application Identified** – Dropbox
- **Application Hash** – Who else is running?
- **Identity** – nedzaldivar (even without ISE or Identity, from non domain asset)

File Hash	Process Username	Connection Application
8B46902FE7A294A1F59EC830122161540A527726D72900E6534D39AA7723E523	Neds-MacBook-Pro.local\nedzaldivar	HTTPS (unclassified)





Demo

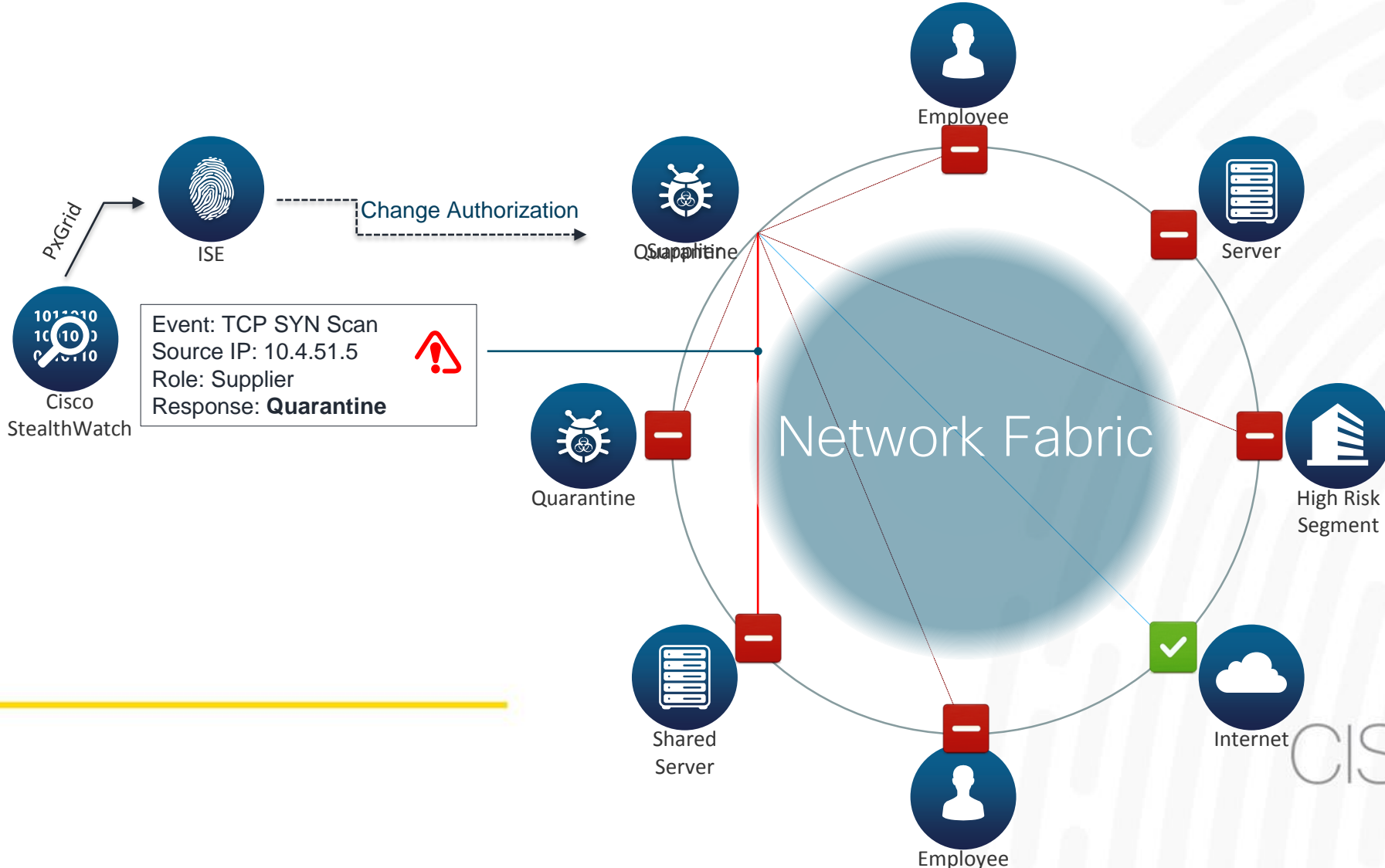
CISCO  SEC

Enforcement



CISCO  SEC

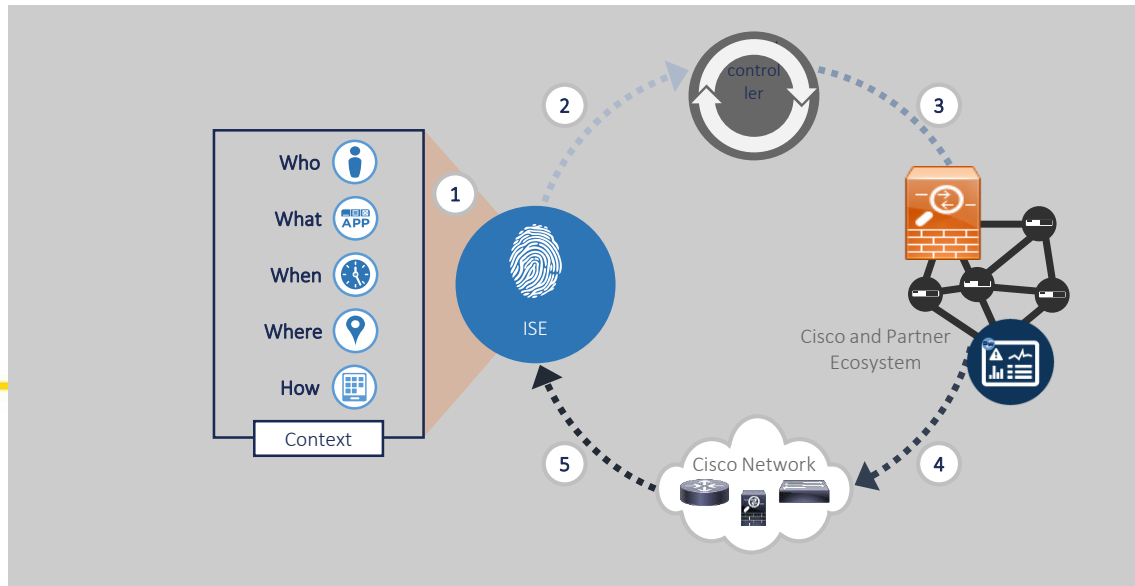
Integrated Threat Defense (Detection & Containment)



Adaptive Network Control



Quarantine/Unquarantine via pxGrid



The screenshot shows the "Host Summary" page for a specific host. At the top, there is a monitor icon and the "Host IP" 192.168.100.101. Below this are three buttons: "View Flows", "Classify", and "History". The main section lists various attributes: Status: Active; Hostname: sjo-i3-svr-101.cisco.com; Host Groups: PCI Servers; Location: RFC 1918; Last Seen: 1/9/15 1:56 PM; Policies: Inside, Servers; MAC Address: --. At the bottom, there are two buttons: "Quarantine" (highlighted with a purple border) and "Unquarantine".

Host IP	192.168.100.101
Status:	Active
Hostname:	sjo-i3-svr-101.cisco.com
Host Groups:	PCI Servers
Location:	RFC 1918
Last Seen:	1/9/15 1:56 PM
Policies:	Inside, Servers
MAC Address:	--

Authorization Policy in ISE using Quarantine Service



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

Quarantine state as one of the conditions

Quarantine definition in ISE

Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	EPS-Quarantine-WIRELESS	if (Session:EPSStatus EQUALS Quarantine AND Radius:NAS-Port-Type EQUALS Wireless - IEEE 802.11)	then WIRELESS-AUTHZ-QUARANTINE
✓	EPS-Quarantine-WIRED	if (Session:EPSStatus EQUALS Quarantine AND Radius:NAS-Port-Type EQUALS Ethernet)	then WIRED-AUTHZ-QUARANTINE
✓	AP-CAP3702	if Cisco-AIR-CAP-3702	then WIRED-AUTHZ-AP
✓	DOT1X-WIRELESS	if Wireless_802.1X	then WIRELESS-AUTHZ-ALLOW-ALL
✓	DOT1X-WIRED	if Wired_802.1X	then WIRED-AUTHZ-ALLOW-ALL

Monitoring Devices



Quarantine state change => Quarantine authorization profile

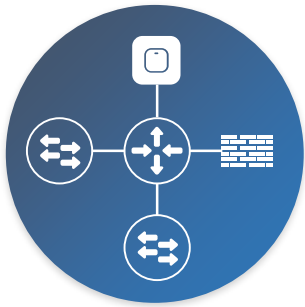
Show Live Sessions Add or Remove Columns Refresh Refresh Every 3 seconds Show Latest 20 records within Last 60 seconds

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Event	Authorization Profile
2014-10-01 18:27:26.442			0	test2	7C:7A:91:33:F4:00	WindowsXP-Worksta...	Session State i...	
2014-10-01 18:27:26.433				test2	7C:7A:91:33:F4:00	WindowsXP-Worksta...	Authentication...	WIRELESS-AUTHZ-QUARANTINE
2014-10-01 18:27:23.134					7C:7A:91:33:F4:00		Dynamic Autho..	

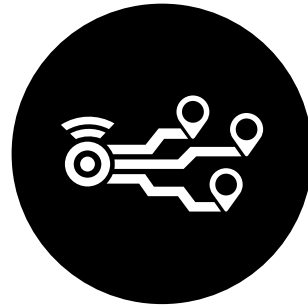


Summary

Three Friends in Security : Identity, Visibility and Enforcement



The network is a key asset for **threat detection** and control



NetFlow and Cisco StealthWatch provides **visibility and intelligence**



TrustSec provides software defined (micro) **segmentation**





Thank you

György Ács
Cisco Systems
gacs@cisco.com

