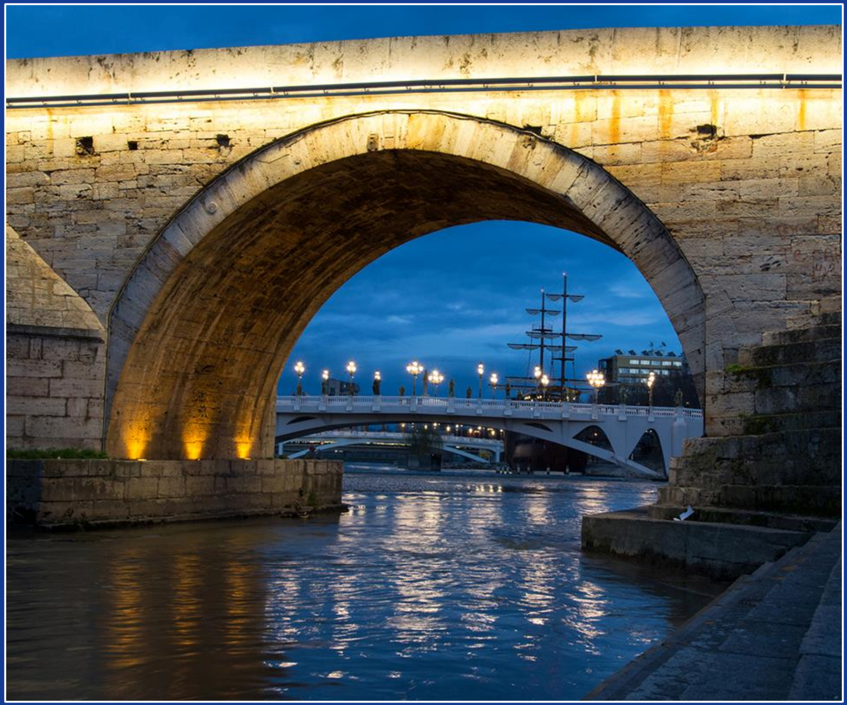
Three Friends in Security : Identity, Visibility and Enforcement Stop the bad guys immediately



György Ács

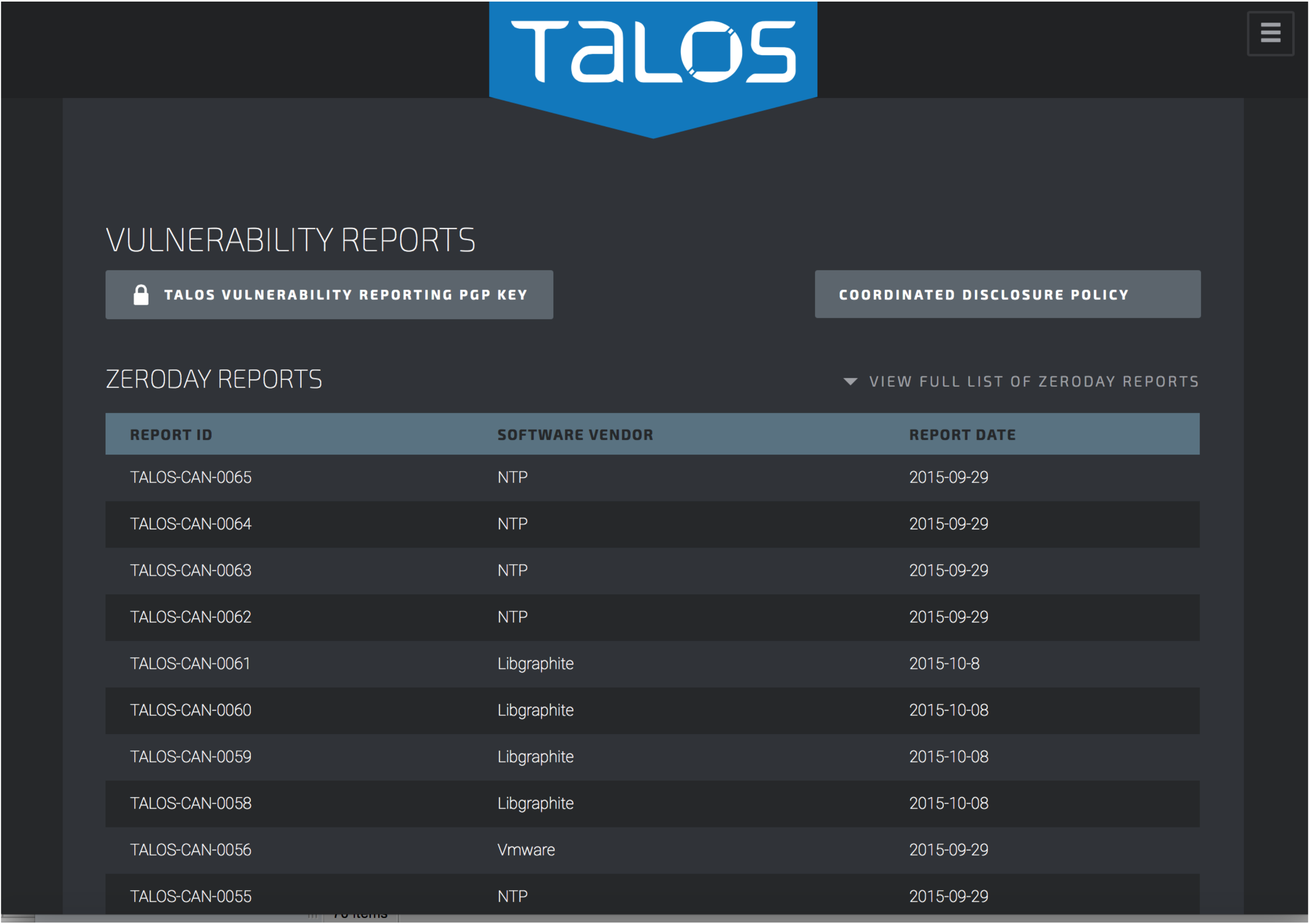
IT Security Consulting Systems Engineer

October 2016

Agenda

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

The Problem is Threats

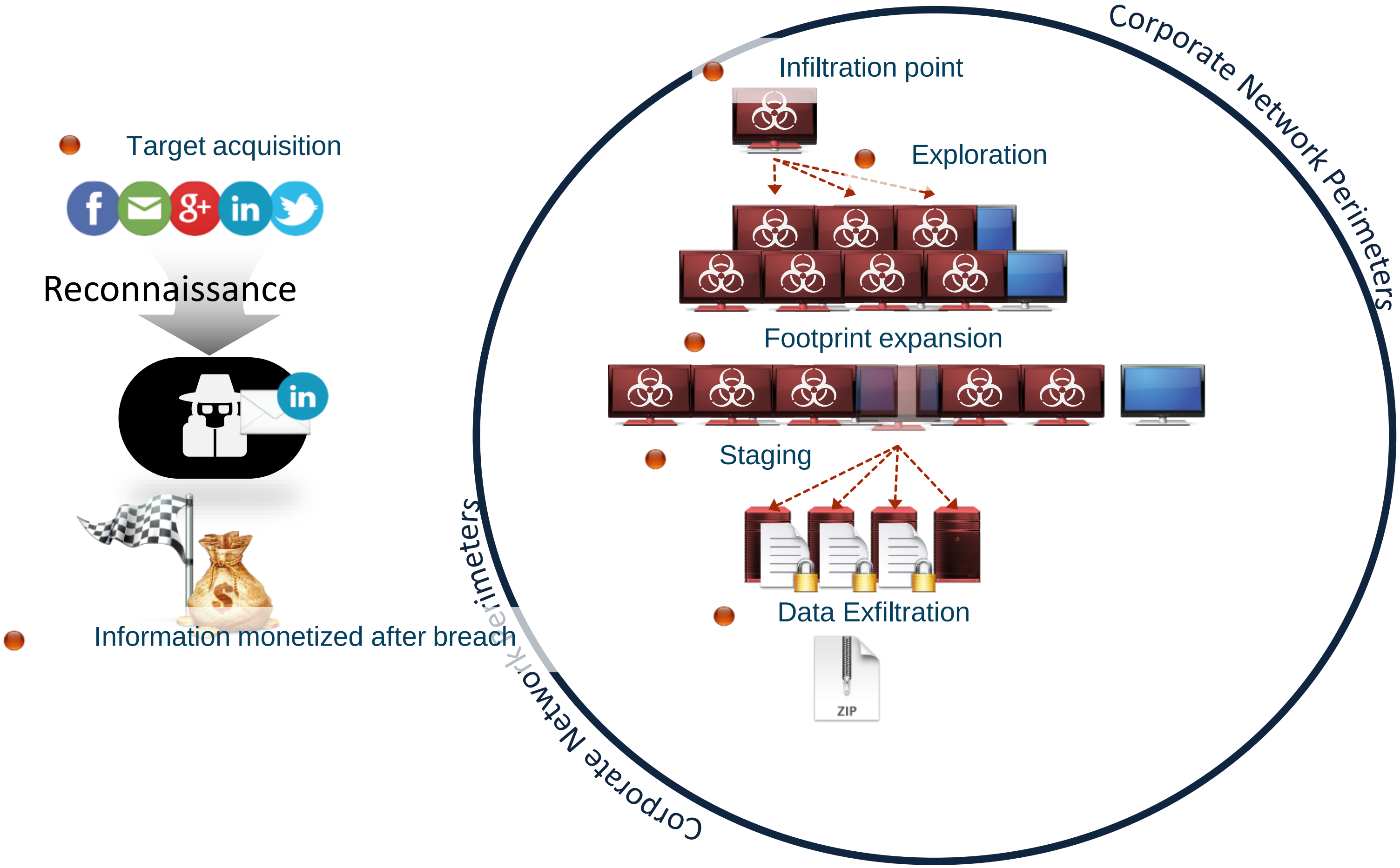

Talos
TALOS VULNERABILITY REPORTING PGP KEY
COORDINATED DISCLOSURE POLICY
VIEW FULL LIST OF ZERODAY REPORTS

VULNERABILITY REPORTS

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 !



Target acquisition

Reconnaissance

Information monetized after breach

Corporate Network Perimeters

Infiltration point

Exploration

Footprint expansion

Staging

Data Exfiltration

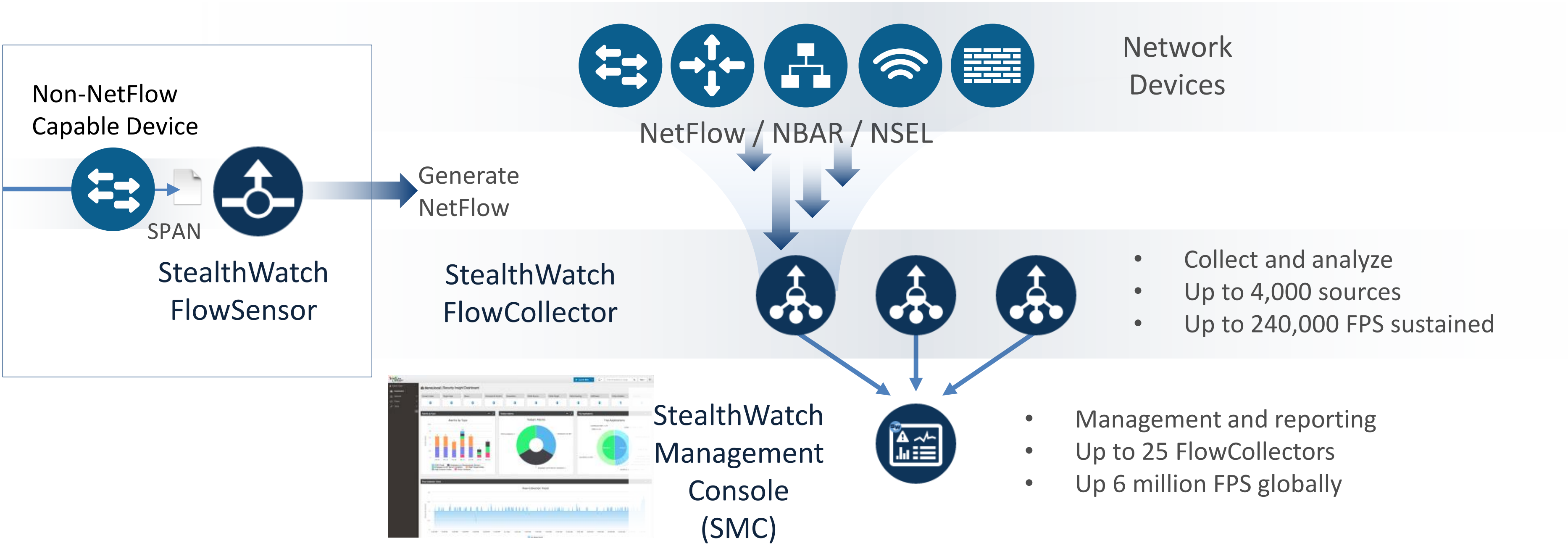
Corporate Network Perimeters

Manamecrypt, a new ransomware that sneaks through torrents	New ransomware abuses Windows PowerShell, Word document macros

cisco

Network as a Sensor / Enforcer

Cisco StealthWatch: System Overview (Earlier : Lancope)



Non-NetFlow Capable Device

SPAN

StealthWatch FlowSensor

Generate NetFlow

Network Devices

NetFlow / NBAR / NSEL

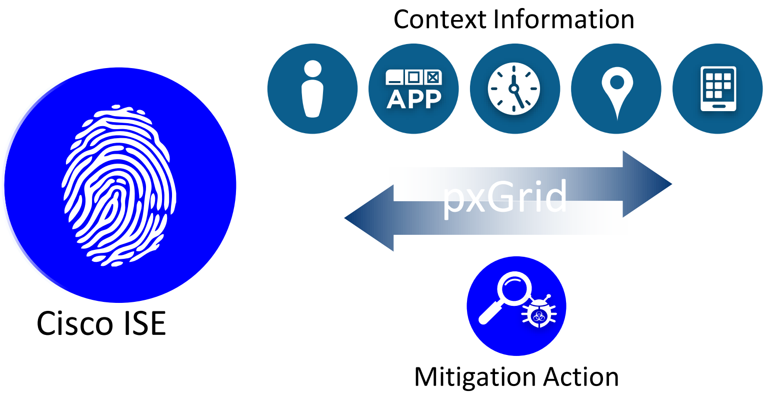
StealthWatch FlowCollector

- Collect and analyze
- Up to 4,000 sources
- Up to 240,000 FPS sustained

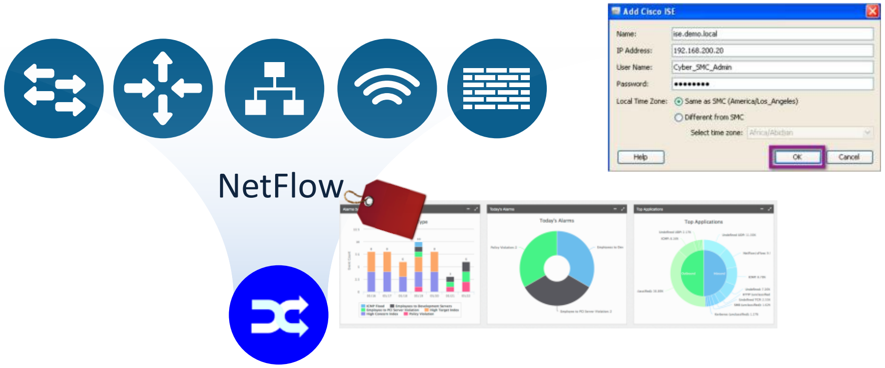
StealthWatch Management Console (SMC)

- Management and reporting
- Up to 25 FlowCollectors
- Up 6 million FPS globally

Network as a Sensor: Cisco StealthWatch



ISE pxgrid for Remediation



Add Cisco ISE

Name: ise.demo.local
IP Address: 192.168.200.20
User Name: Cyber_SMC_Admin
Password: ●●●●●●●●●
Local Time Zone: ● Same as SMC (America/Los_Angeles)
○ Different from SMC
Select time zone: Africa/Abidjan

Help | OK | Cancel

Real-time visibility at all network layers

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

Identity

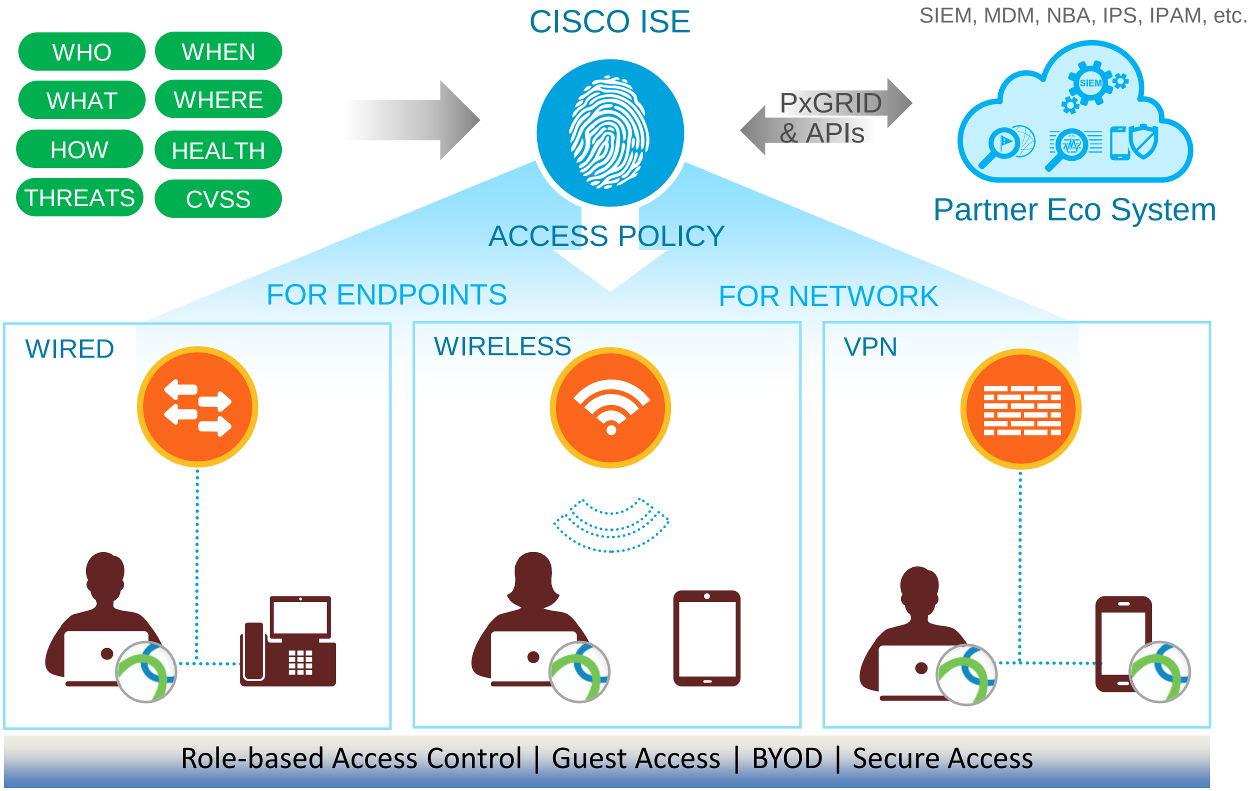
Cisco Identity Services Engine

Cisco ISE

Context aware policy service, to control access and threat across wired, wireless and VPN networks

Cisco Anyconnect

Supplicant for wired, wireless and VPN access. Services include: Posture assessment, Malware protection, Web security, MAC Security, Network visibility and more.



Context is everything

UNKNOWN

Poor context awareness	Rich context awareness
IP ADDRESS: 192.168.2.101	BOB (EMPLOYEE)
UNKNOWN	WINDOWS WORKSTATION
UNKNOWN	BUILDING-A FLOOR-1
UNKNOWN	10:30 AM EST on APR 27
UNKNOWN	WIRELESS
UNKNOWN	NO THREATS / VULNERABILITIES

RESULT

ACCESS TO IP (ANY DEVICE / USER)

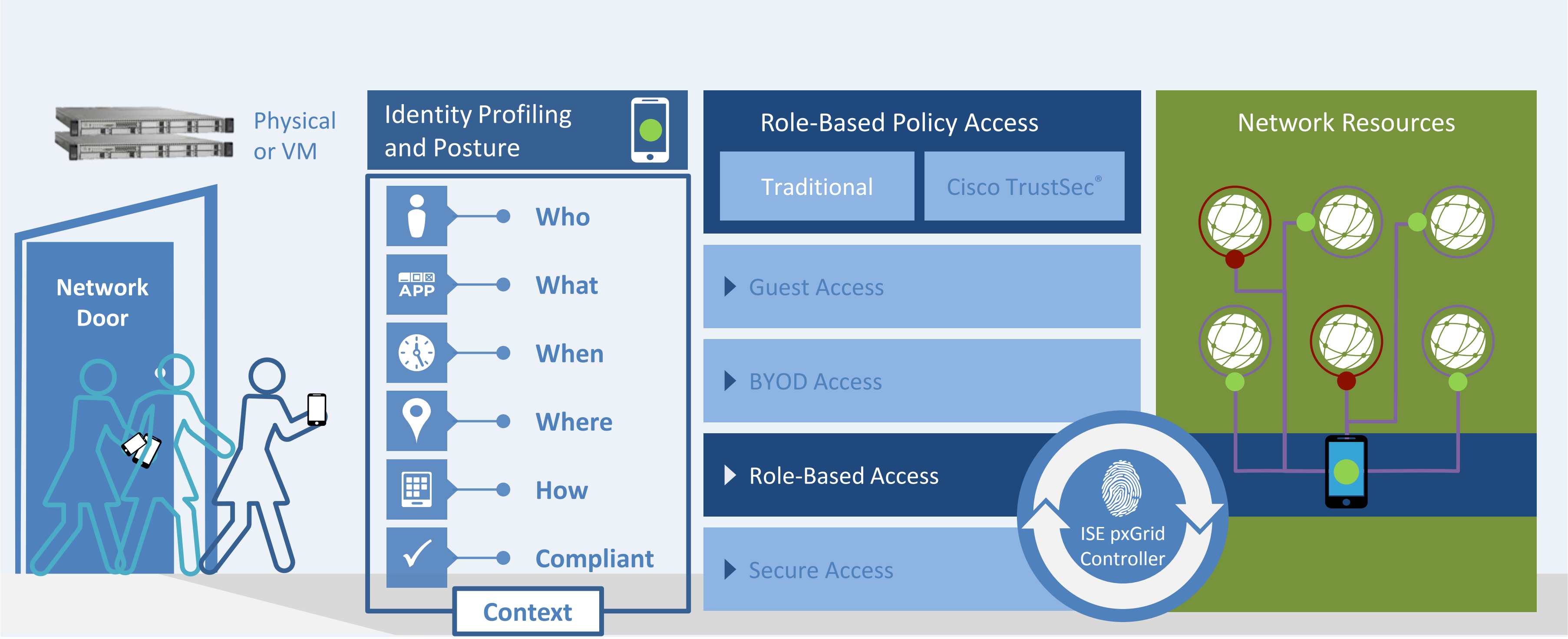
RESULT

ROLE BASED ACCESS

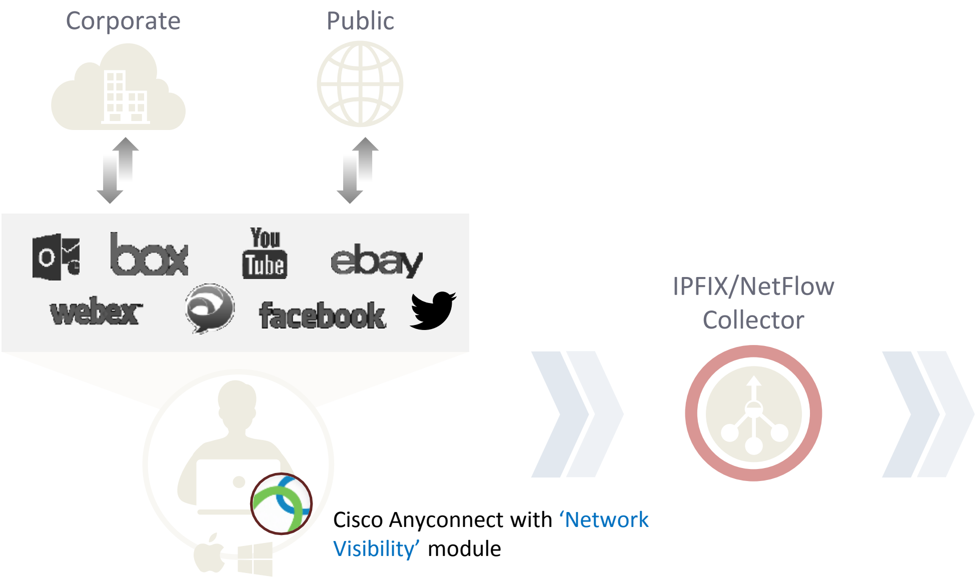
KNOWN

Cisco Identity Services Engine

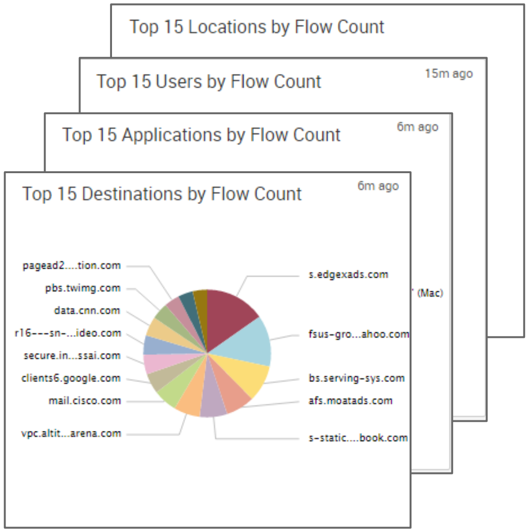
A centralized security solution that automates context-aware access to network resources and shares contextual data



Application ‘Visibility’ via Anyconnect



Cisco Anyconnect with ‘Network Visibility’ module


Top 15 Locations by Flow Count

Top 15 Users by Flow Count

Top 15 Applications by Flow Count

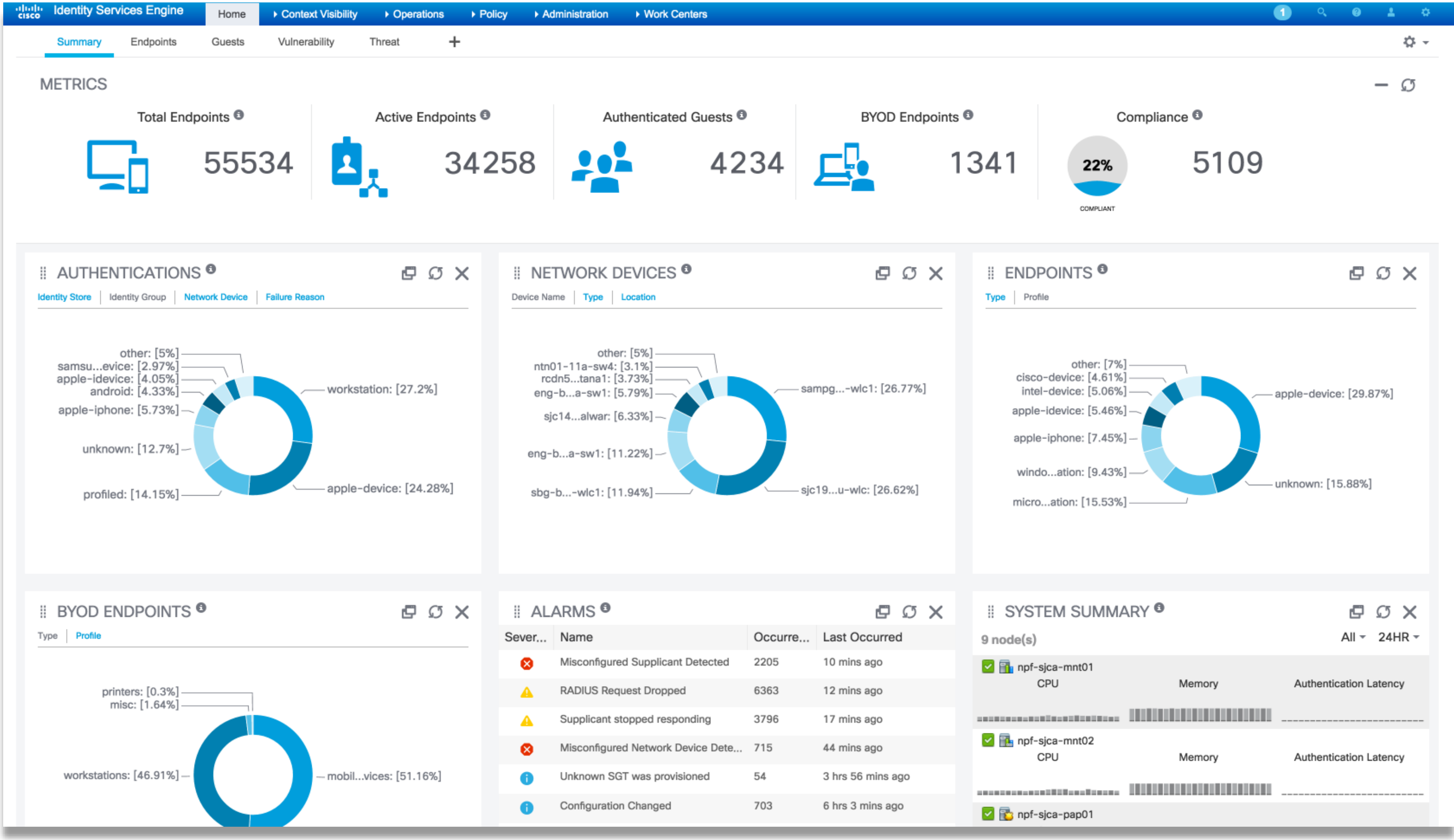
Top 15 Destinations by Flow Count

Visibility
in to process, process hash, URLs, and more

Context
for Network Behavioral Analysis

Control
run-time applications via ’Posture Policies’

Security starts with ‘Visibility’



METRICS

Total Endpoints	Active Endpoints	Authenticated Guests	BYOD Endpoints	Compliance
55534	34258	4234	1341	5109

AUTHENTICATIONS

NETWORK DEVICES

ENDPOINTS

BYOD ENDPOINTS

ALARMS

Sever...	Name	Occurre...	Last Occurred
☒	Misconfigured Supplicant Detected	2205	10 mins ago
⚠	RADIUS Request Dropped	6363	12 mins ago
⚠	Supplicant stopped responding	3796	17 mins ago
☒	Misconfigured Network Device Dete...	715	44 mins ago
ℹ	Unknown SGT was provisioned	54	3 hrs 56 mins ago
ℹ	Configuration Changed	703	6 hrs 3 mins ago

SYSTEM SUMMARY

9 node(s)

All ▾ 24HR ▾

☑ npf-sjca-mnt01
CPU Memory Authentication Latency

☑ npf-sjca-mnt02
CPU Memory Authentication Latency

☑ npf-sjca-pap01

Threat Centric NAC

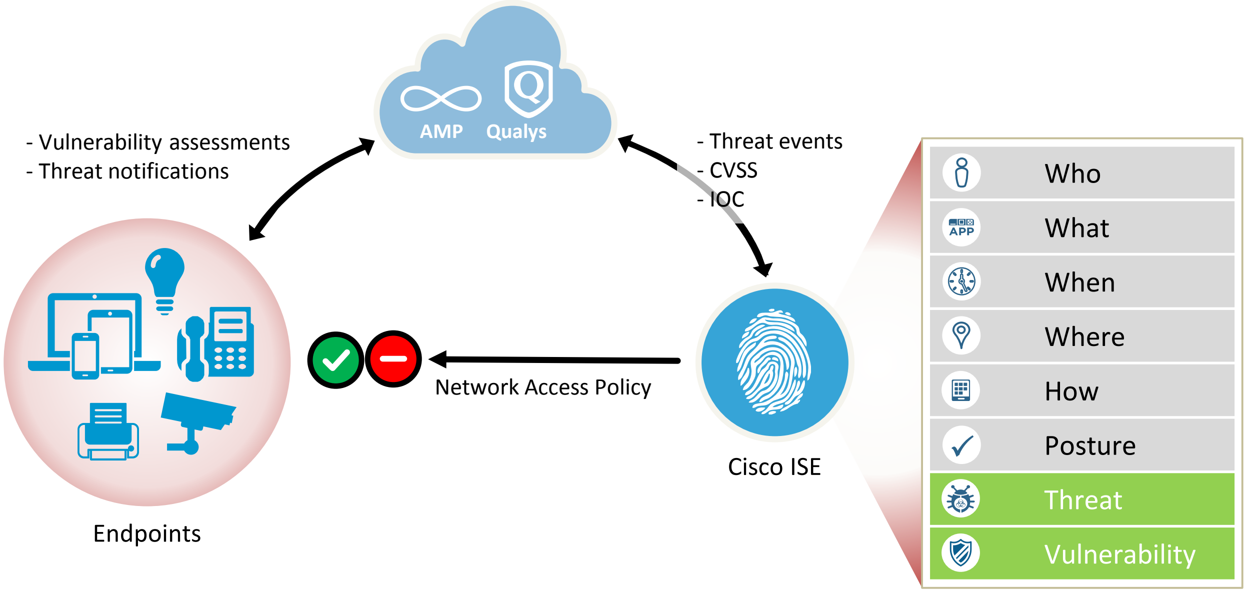
Cisco ISE protects your network from data breaches by segmenting compromised and vulnerable endpoints for remediation.

Compliments Posture
Vulnerability data tells endpoint's posture from the outside

Expanded control
driven by threat intelligence and vulnerability assessment data

Faster response
with automated, real-time policy updates based on vulnerability data and threat metrics

Create ISE authorization policies based on the threat and vulnerability attributes



Same ISE for 'Network Device' Administration

Feature Highlight

Customers can now use Terminal Access Controller Access Control System (TACACS) with ISE to simplify device administration and enhance security through flexible, granular control of access to network devices.

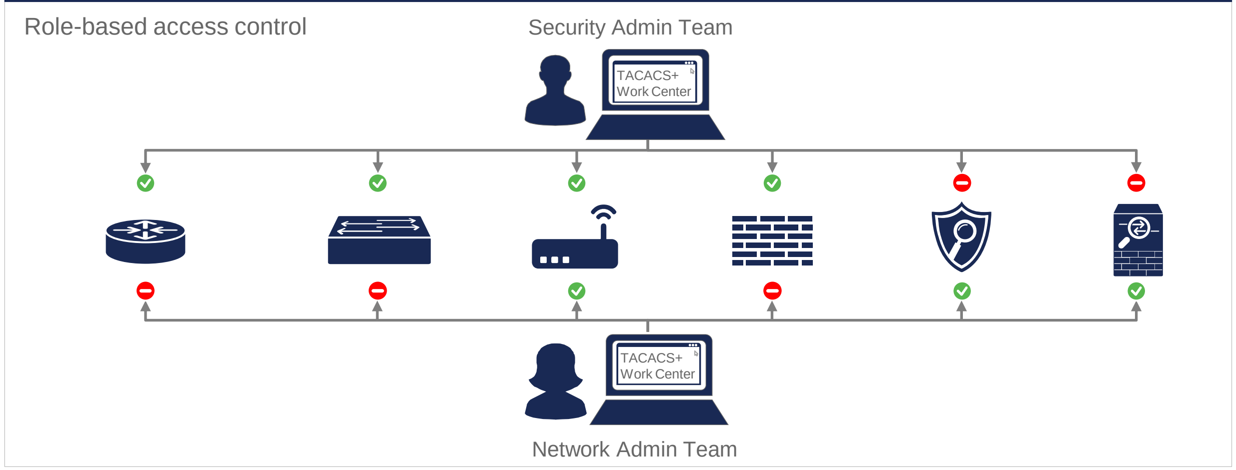
Benefits

Simplified, centralized device administration
Increase security, compliancy, 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



Capabilities

- Role-based access control
- Flow-based user experience
- Command level authorization with detailed logs for auditing
- Dedicated TACACS+ workcenter for network administrators
- Support for core ACS5 features

Visibility

Versions of NetFlow

For Your Reference

Version	Major Advantage	Limits/Weaknesses
V5	Defines 18 exported fields Simple and compact format Most commonly used format	IPv4 only Fixed fields, fixed length fields only Single flow cache
V9	Template-based IPv6 flows transported in IPv4 packets MPLS and BGP nexthop supported Defines 104 fields, including L2 fields Reports flow direction	IPv6 flows transported in IPv4 packets Fixed length fields only Uses more memory Slower performance Single flow cache
Flexible NetFlow (FNF)	Template-based flow format (built on V9 protocol) Supports flow monitors (discrete caches) Supports selectable key fields and IPv6 Supports NBAR data fields	Less common Requires more sophisticated platform to produce Requires more sophisticated system to consume
IP Flow Information Export (IPFIX) AKA NetFlow V10	Standardized – RFC 5101, 5102, 6313 Supports variable length fields, NBAR2 Can export flows via IPv4 and IPv6 packets	Even less common Only supported on a few Cisco platforms
NSEL (ASA only)	Built on NetFlow v9 protocol State-based flow logging (context) Pre and Post NAT reporting	Missing many standard fields Limited support by collectors

Configuring Flexible NetFlow (FNF)
4 easy steps (Cat 3k-X):

- Configure Flow Records, Setting key and non key fields
  - „match” => key record, „collect”=> non key
- Configure Flow Exporter
- Configure Flow Monitor, tying the record to exporter
- Apply the Flow Monitor to the interface

```
!
flow record C3KX_FLOW_RECORD   match
datalink mac source-address
 match datalink mac destination-address
 match ipv4 tos
 match ipv4 ttl
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port   collect
interface input snmp   collect interface
output snmp   collect counter
bytes   collect counter packets   collect
timestamp sys-uptime first
 collect timestamp sys-uptime last
!
```

Configuring Flexible NetFlow (FNF) 4 easy steps (Cat 3k-X):

- Configure Flow Records, Setting key and non key fields
  - „match” => key record, „collect”=> non key
- Configure Flow Exporter
- Configure Flow Monitor, tying the record to exporter
- Apply the Flow Monitor to the interface

```
!
flow exporter exporter-name
  description description
  destination {hostname | ip-address}
  export-protocol {netflow-v5 | netflow-v9 | ipfix}
  transport udp udp-port
!
!
flow monitor flow-monitor-name
     description description
     exporter exporter-name
     record C3KX_FLOW_RECORD
!
```

Configuring Flexible NetFlow (FNF) 4 easy steps (Cat 3k-X):

- Configure Flow Records, Setting key and non key fields
  - „match” => key record, „collect”=> non key
- Configure Flow Exporter
- Configure Flow Monitor, tying the record to exporter
- Apply the Flow Monitor to the interface

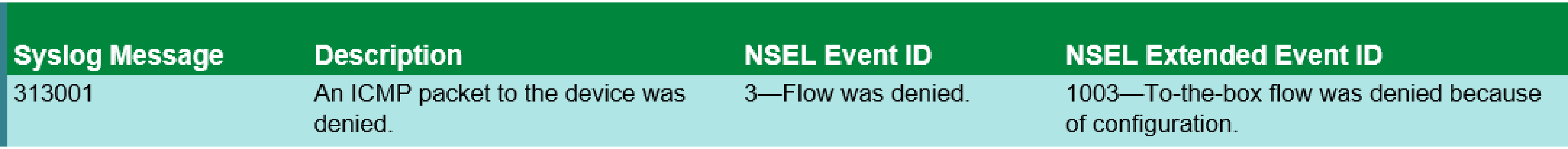
```
!
 interface type number
        ip flow monitor flow-monitor-name
input
!
```

ASA NSEL Configuration

For Your Reference

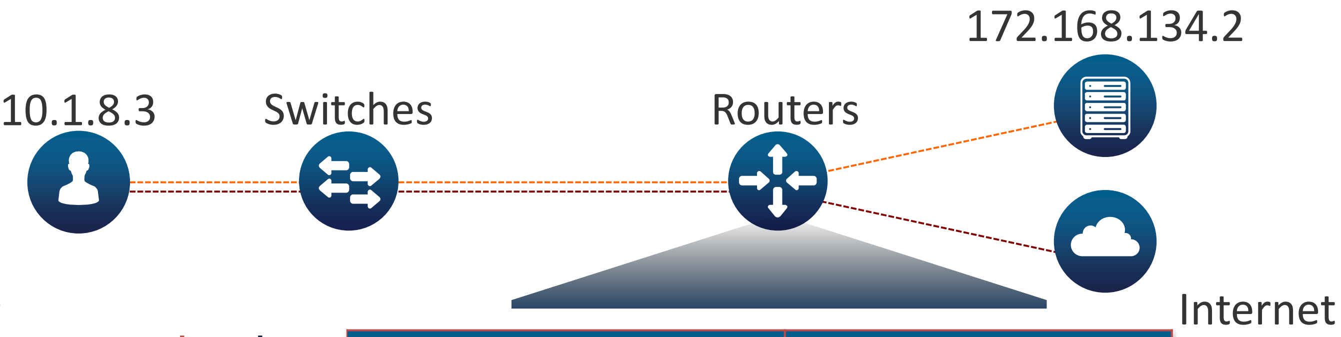
```
!
flow-export destination management <ip-address> 2055
!
policy-map global_policy
 class class-default
  flow-export event-type all destination <ip-address>
!
flow-export template timeout-rate 2
logging flow-export syslogs disable
!
```

NetFlow Security Event Logs (NSEL) – tracks flow create, teardown, update and denied events
 (only when event occurs)



Syslog Message	Description	NSEL Event ID	NSEL Extended Event ID
313001	An ICMP packet to the device was denied.	3—Flow was denied.	1003—To-the-box flow was denied because of configuration.

Visibility through NetFlow

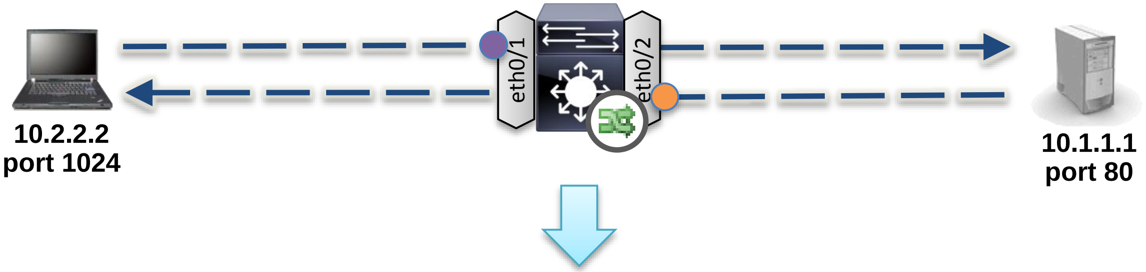


NetFlow provides

- 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

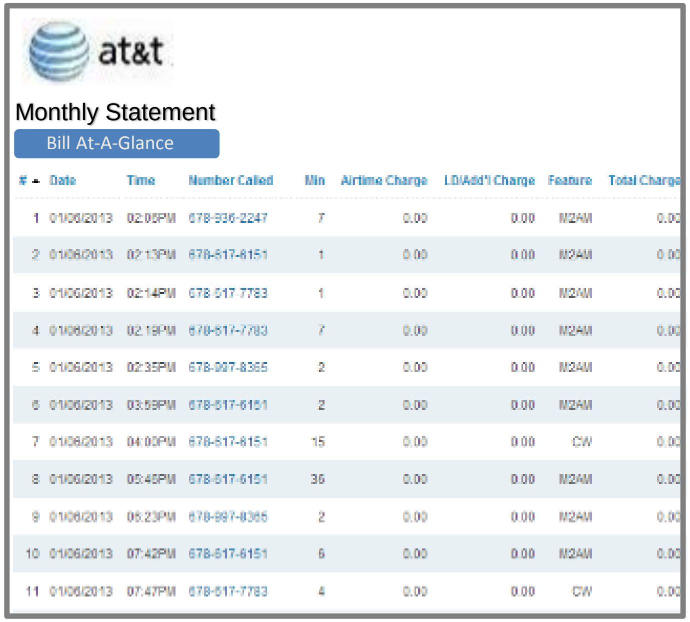
NetFlow



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



at&t

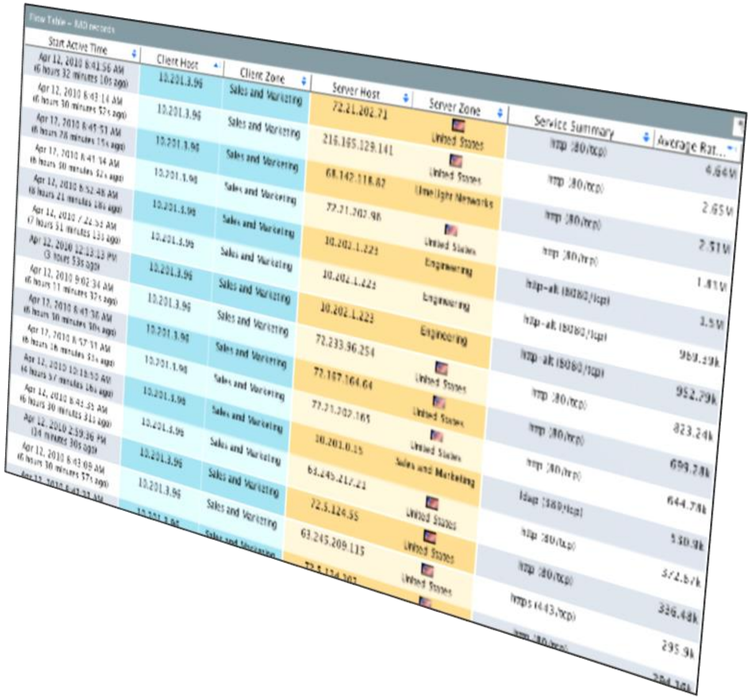
Monthly Statement

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	678-617-6151	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	03:59PM	678-617-6151	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

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.

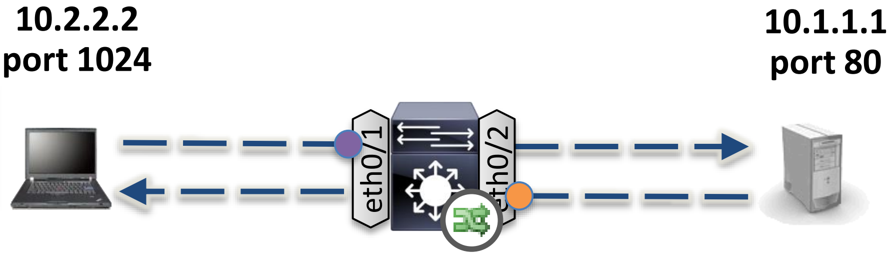
Flow Record



Flow Table – 840 records

Start Active Time	Client Host	Client Zone	Server Host	Server Zone	Service Summary	Average Rat...
Apr 12, 2010 6:41:56 AM (6 hours 32 minutes 10s ago)	10.201.3.96	Sales and Marketing	72.21.202.71	United States	http (80/tcp)	4.64M
Apr 12, 2010 6:43:14 AM (6 hours 30 minutes 52s ago)	10.201.3.96	Sales and Marketing	216.165.129.141	United States	http (80/tcp)	2.65M
Apr 12, 2010 6:45:51 AM (6 hours 28 minutes 15s ago)	10.201.3.96	Sales and Marketing	68.142.118.82	Limelight Networks	http (80/tcp)	2.51M
Apr 12, 2010 6:41:34 AM (6 hours 30 minutes 52s ago)	10.201.3.96	Sales and Marketing	72.21.202.98	United States	http (80/tcp)	1.81M
Apr 12, 2010 6:52:48 AM (6 hours 21 minutes 18s ago)	10.201.3.96	Sales and Marketing	10.202.1.223	Engineering	http-alt (8080/tcp)	1.5M
Apr 12, 2010 7:22:53 AM (7 hours 51 minutes 13s ago)	10.201.3.96	Sales and Marketing	10.202.1.223	Engineering	http-alt (8080/tcp)	969.19k
Apr 12, 2010 12:13:13 PM (3 hours 53s ago)	10.201.3.96	Sales and Marketing	10.202.1.223	Engineering	http-alt (8080/tcp)	952.79k
Apr 12, 2010 9:02:34 AM (6 hours 11 minutes 37s ago)	10.201.3.96	Sales and Marketing	72.233.96.254	United States	http (80/tcp)	823.24k
Apr 12, 2010 6:47:36 AM (6 hours 30 minutes 30s ago)	10.201.3.96	Sales and Marketing	72.107.164.64	United States	http (80/tcp)	699.78k
Apr 12, 2010 6:57:31 AM (6 hours 16 minutes 35s ago)	10.201.3.96	Sales and Marketing	72.21.202.165	United States	http (80/tcp)	644.78k
Apr 12, 2010 10:15:50 AM (4 hours 57 minutes 16s ago)	10.201.3.96	Sales and Marketing	10.201.0.15	Sales and Marketing	ldap (389/tcp)	530.9k
Apr 12, 2010 6:41:35 AM (6 hours 30 minutes 31s ago)	10.201.3.96	Sales and Marketing	63.245.217.21	United States	http (80/tcp)	372.57k
Apr 12, 2010 2:59:36 PM (14 minutes 30s ago)	10.201.3.96	Sales and Marketing	72.5.124.55	United States	http (80/tcp)	336.48k
Apr 12, 2010 6:43:09 AM (6 hours 30 minutes 57s ago)	10.201.3.96	Sales and Marketing	63.245.209.115	United States	https (443/tcp)	295.9k
Apr 12, 2010 6:47:31 AM	10.201.3.96	Sales and Marketing	72.5.124.207		http (80/tcp)	284.36k

NetFlow Collection: Flow Stitching



Uni-directional flow records

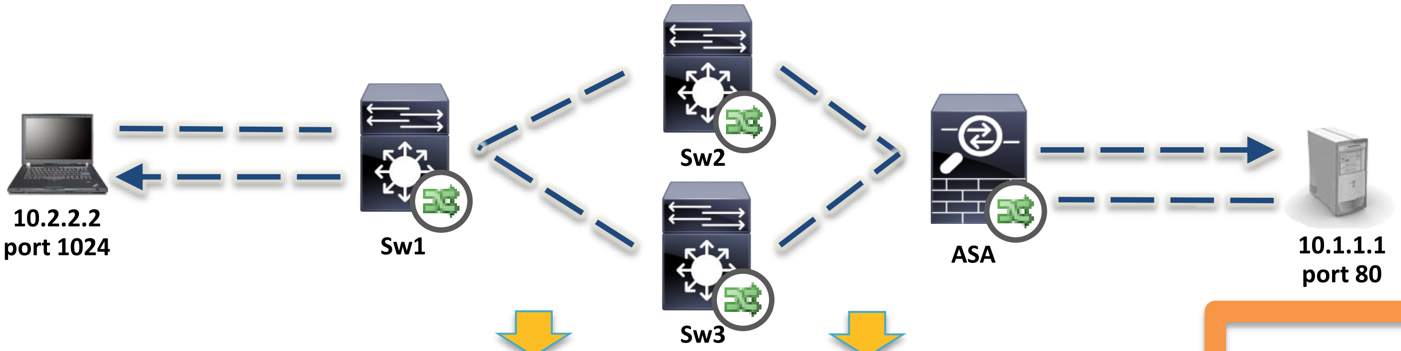
Start Time	Interface	Src IP	Src Port	Dest IP	Dest Port	Proto	Pkts Sent	Bytes Sent	SGT	DGT
10:20:12.221	eth0/1	10.2.2.2	1024	10.1.1.1	80	TCP	5	1025	100	1010
10:20:12.871	eth0/2	10.1.1.1	80	10.2.2.2	1024	TCP	17	28712	1010	100

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:

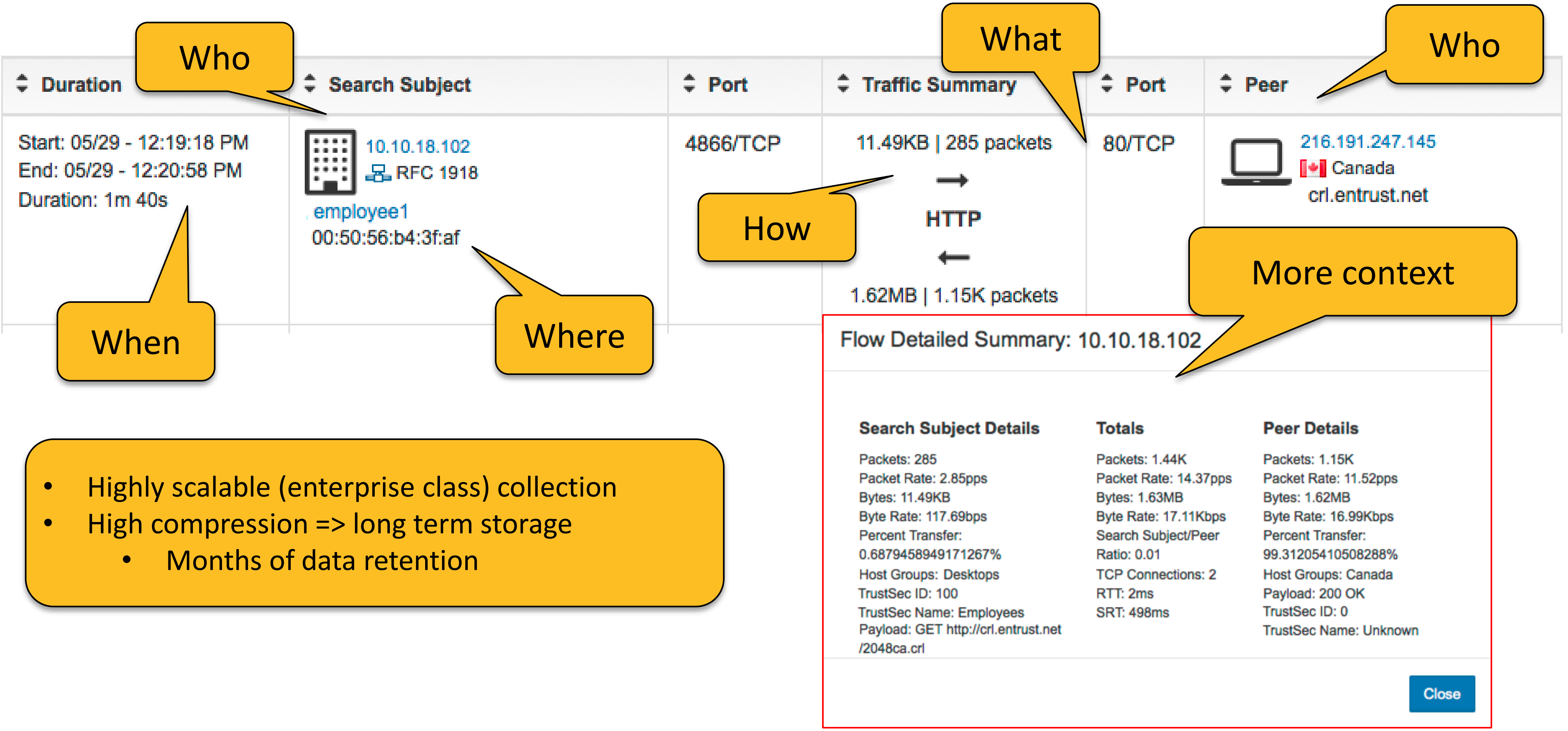
- Conversation flow record
- Allows easy visualization and analysis

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

Conversational Flow Record



Duration	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

Who

What

Who

How

When

Where

More context

Flow Detailed Summary: 10.10.18.102

Search Subject Details

Packets: 285
Packet Rate: 2.85pps
Bytes: 11.49KB
Byte Rate: 117.69bps
Percent Transfer: 0.6879458949171267%
Host Groups: Desktops
TrustSec ID: 100
TrustSec Name: Employees
Payload: GET http://crl.entrust.net/2048ca.crl

Totals

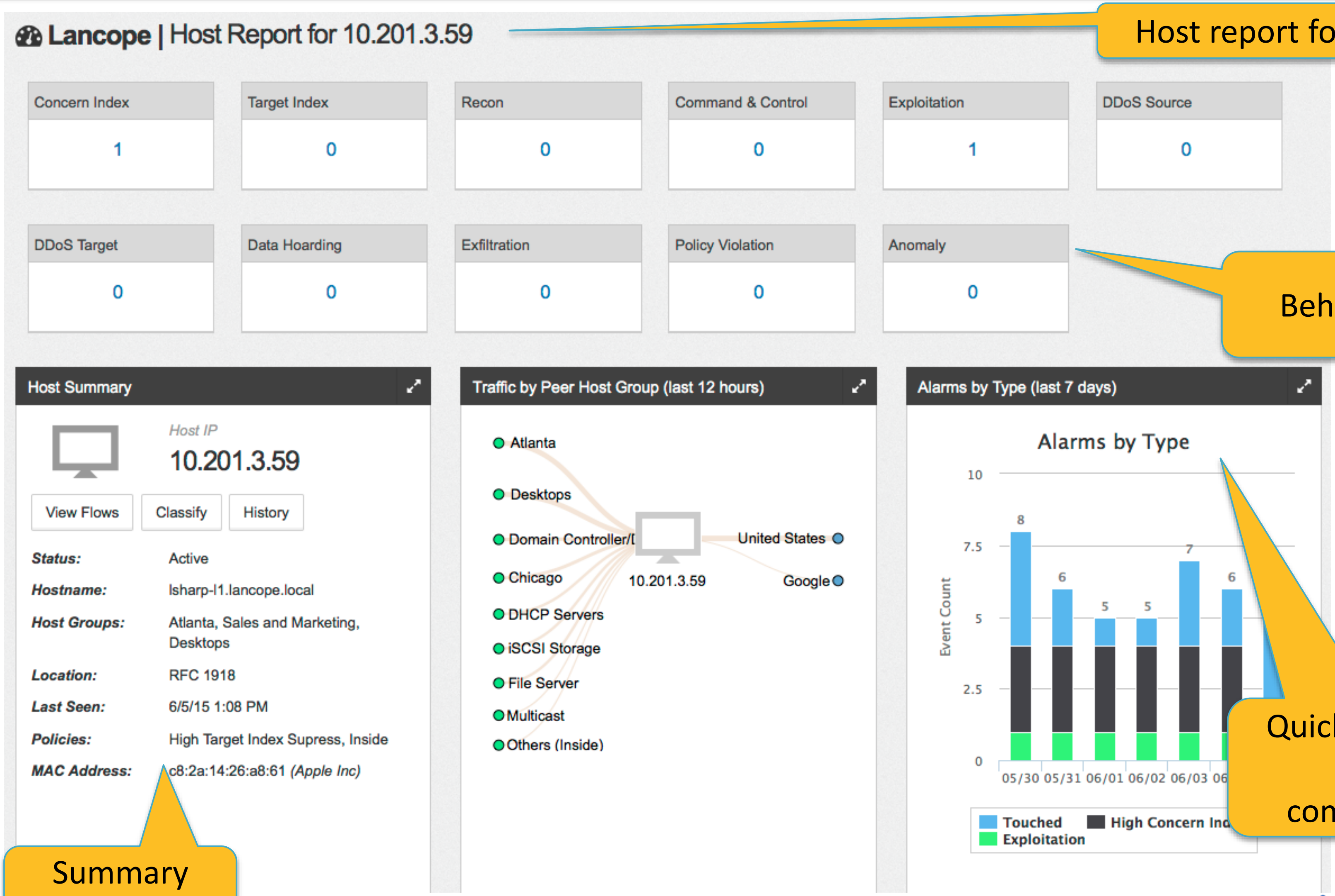
Packets: 1.44K
Packet Rate: 14.37pps
Bytes: 1.63MB
Byte Rate: 17.11Kbps
Search Subject/Peer Ratio: 0.01
TCP Connections: 2
RTT: 2ms
SRT: 498ms

Peer Details

Packets: 1.15K
Packet Rate: 11.52pps
Bytes: 1.62MB
Byte Rate: 16.99Kbps
Percent Transfer: 99.31205410508288%
Host Groups: Canada
Payload: 200 OK
TrustSec ID: 0
TrustSec Name: Unknown

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

Profiling a Host



Lancope | Host Report for 10.201.3.59

Concern Index	Target Index	Recon	Command & Control	Exploitation	DDoS Source
1	0	0	0	1	0

DDoS Target	Data Hoarding	Exfiltration	Policy Violation	Anomaly
0	0	0	0	0

Host Summary

Host IP

10.201.3.59

View Flows | Classify | History

Status:	Active
Hostname:	lsharp-l1.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)*

Traffic by Peer Host Group (last 12 hours)

Alarms by Type (last 7 days)

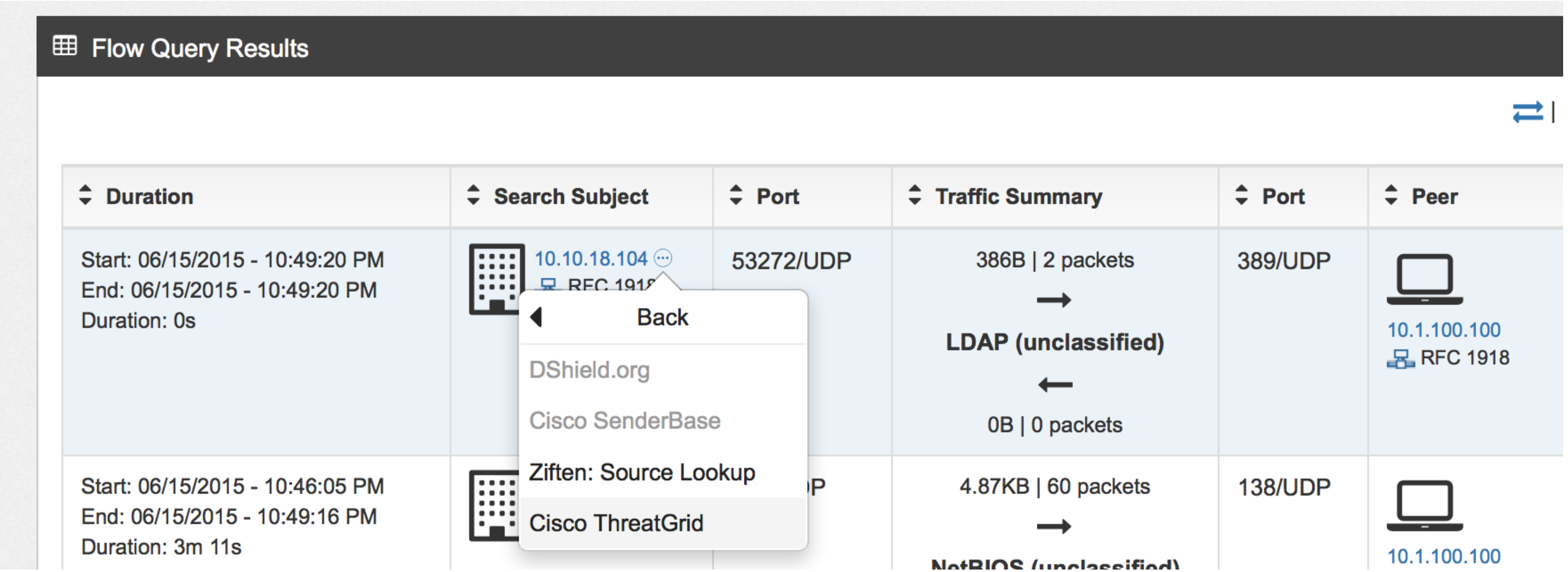
Host report for 10.201.3.59

Behavior alarms

Quick view of host group communication

Summary information

New: StealthWatch to ThreatGrid External Lookup

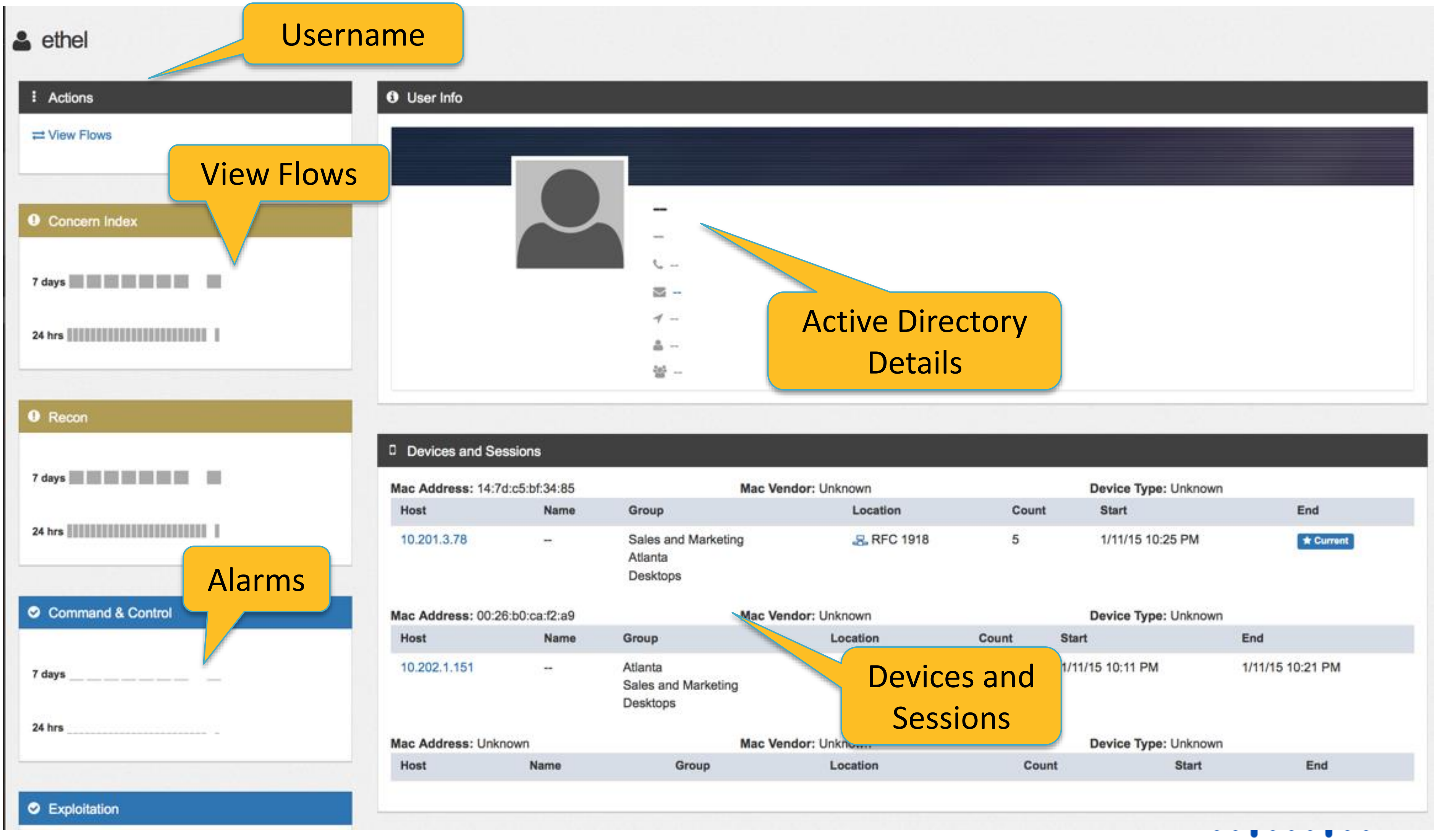


Flow Query Results

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 RFC 191	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		P	4.87KB | 60 packets → NetBIOS (unclassified)	138/UDP	10.1.100.100

Dynamic Analysis lookup

Extrapolating to a User



Username

View Flows

Active Directory Details

Alarms

Devices and Sessions

ethel

Devices and Sessions

Mac Address: 14:7d:c5:bf:34:85 **Mac Vendor:** Unknown **Device Type:** 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

Mac Address: 00:26:b0:ca:f2:a9 **Mac Vendor:** Unknown **Device Type:** Unknown

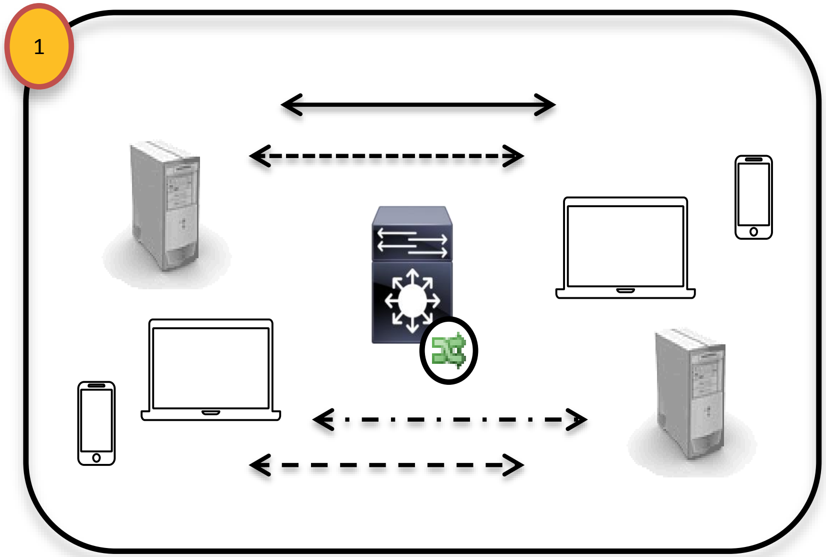
Host	Name	Group	Location	Count	Start	End
10.202.1.151	--	Atlanta Sales and Marketing Desktops			1/11/15 10:11 PM	1/11/15 10:21 PM

Mac Address: Unknown **Mac Vendor:** Unkn **Device Type:** Unknown

Host	Name	Group	Location	Count	Start	End

Policy and
Indication of Compromise IoC

Flow-based Anomaly Detection

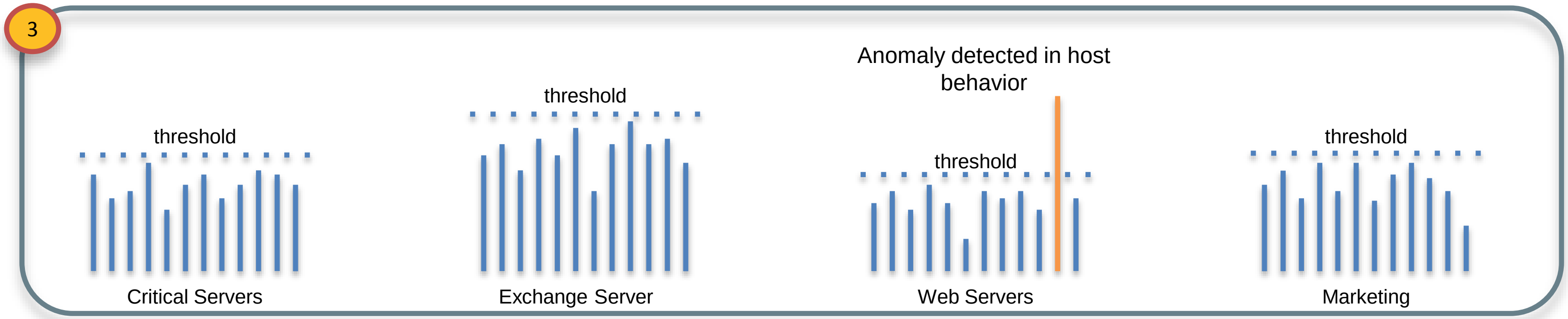


Collect & Analyze Flows

2

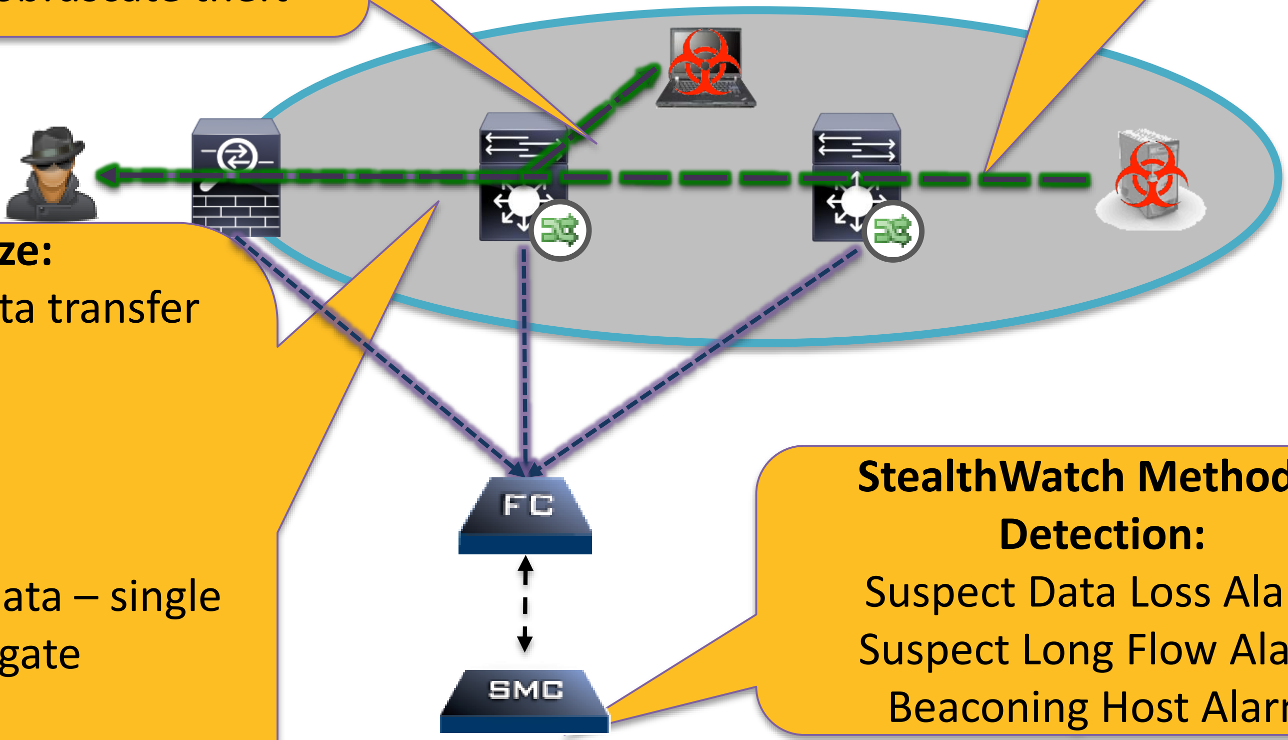
- # Concurrent flows
- Packets per second
- Bits per second
- New flows created
- Number of SYNs sent
- Time of day
- Number of SYNs received
- Rate of connection resets
- Duration of the flow
- Over 80+ other attributes

Establish Baseline of Behaviors



Alarm on Anomalies & Changes in Behavior

Detecting Data Loss



Intermediary resource used to obfuscate theft

Data is exported off resource

What to analyze:

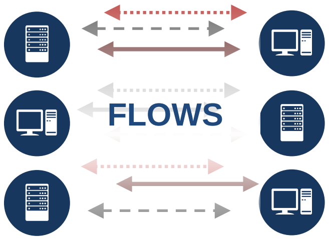
- Historical data transfer behaviour
- Applications
- Time of day
- Countries
- Amount of data – single and in aggregate
- Time frames
- Asymmetric traffic patterns
- Traffic between functional groups

StealthWatch Method of Detection:

Suspect Data Loss Alarm
Suspect Long Flow Alarm
Beaconing Host Alarm

Behavioral Algorithms Are Applied to Build “Security Events”

COLLECT AND ANALYZE FLOWS



SECURITY EVENTS (94 +)

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
.

ALARM CATEGORY

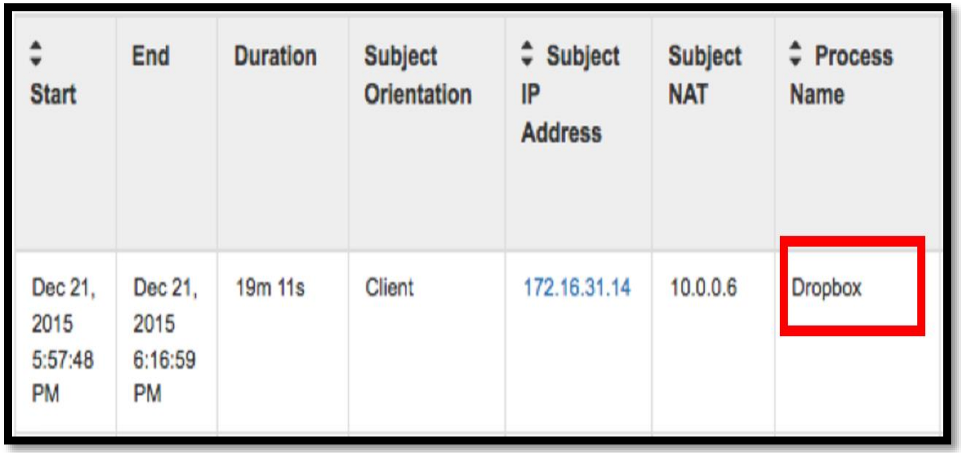
- Concern
- Recon
- C&C
- Exploitation
- Data Hoarding
- Exfiltration
- DDoS Target

RESPONSE

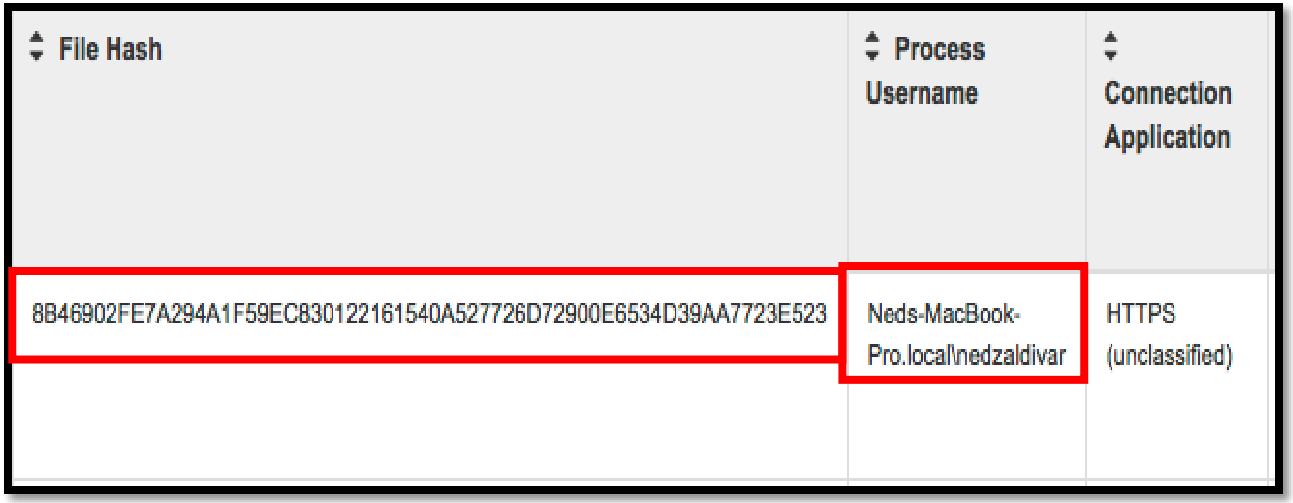
- Alarm Table
- Host Snapshot
- Email
- Syslog / SIEM
- Mitigation

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



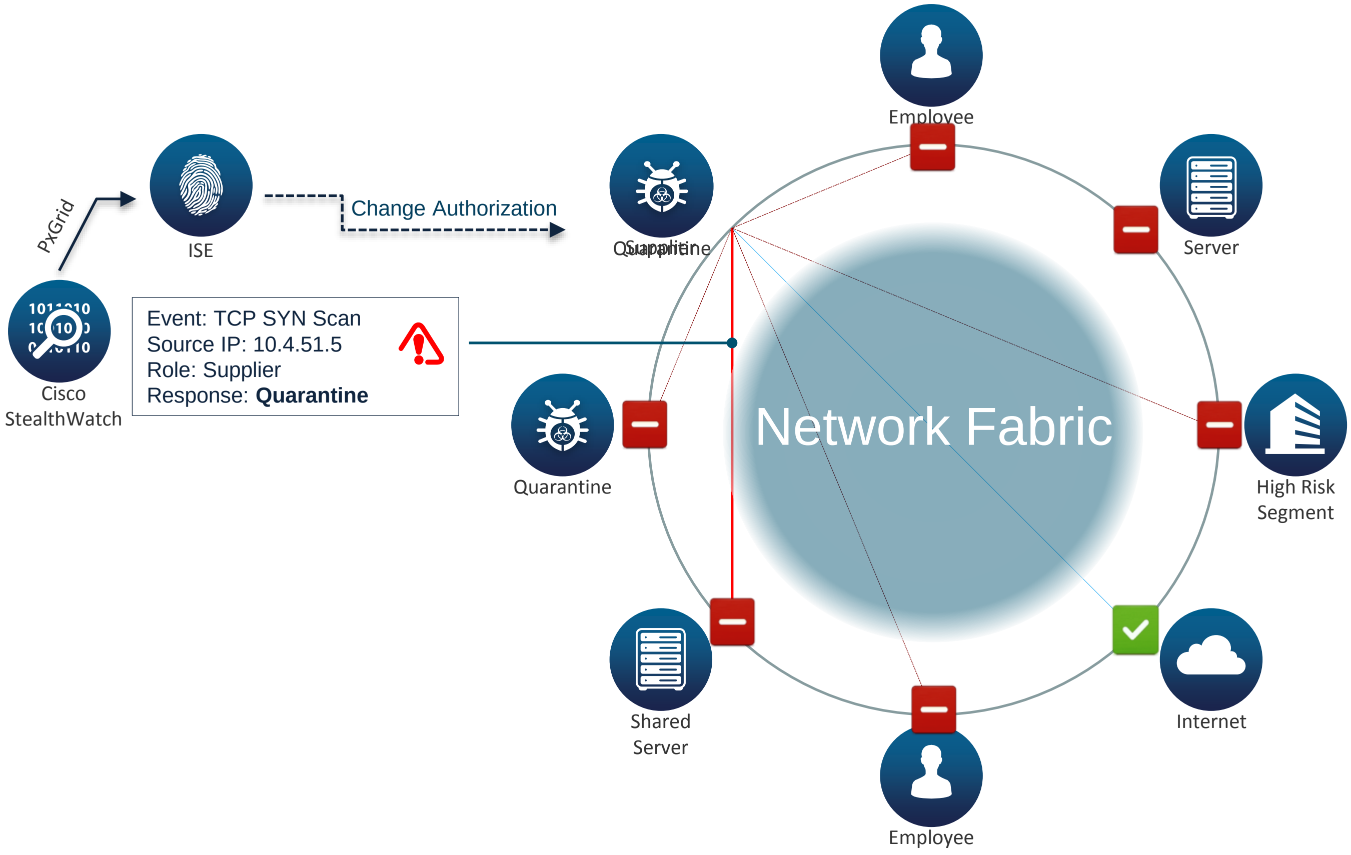
File Hash	Process Username	Connection Application
8B46902FE7A294A1F59EC830122161540A527726D72900E6534D39AA7723E523	Neds-MacBook-Pro.local\nedzaldivar	HTTPS (unclassified)

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

Demo

Enforcement

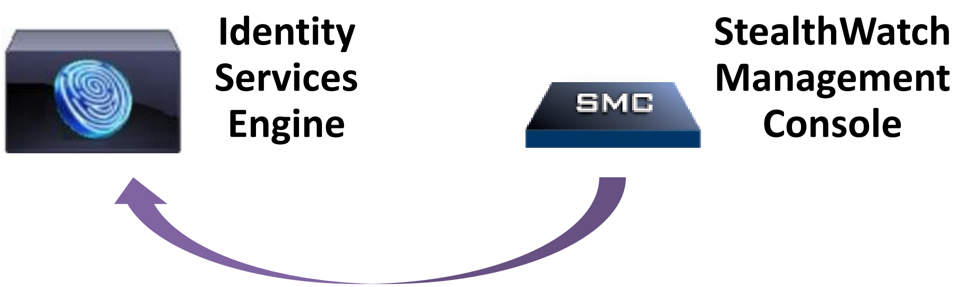
Integrated Threat Defense (Detection & Containment)



Event: TCP SYN Scan
Source IP: 10.4.51.5
Role: Supplier
Response: **Quarantine**

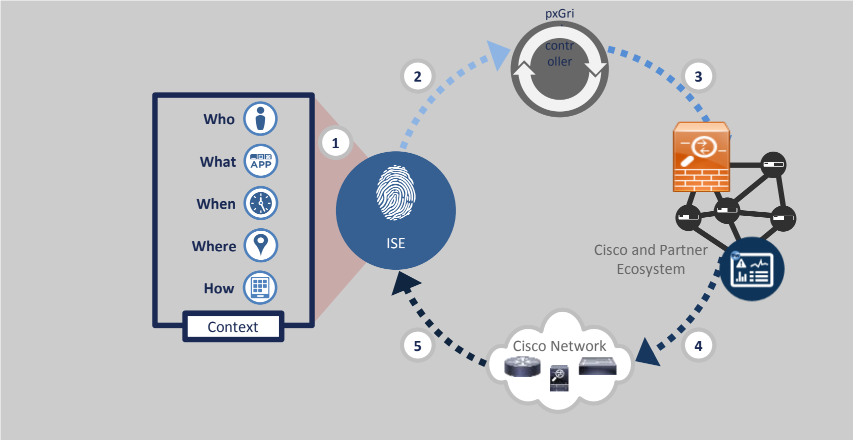
Adaptive Network Control

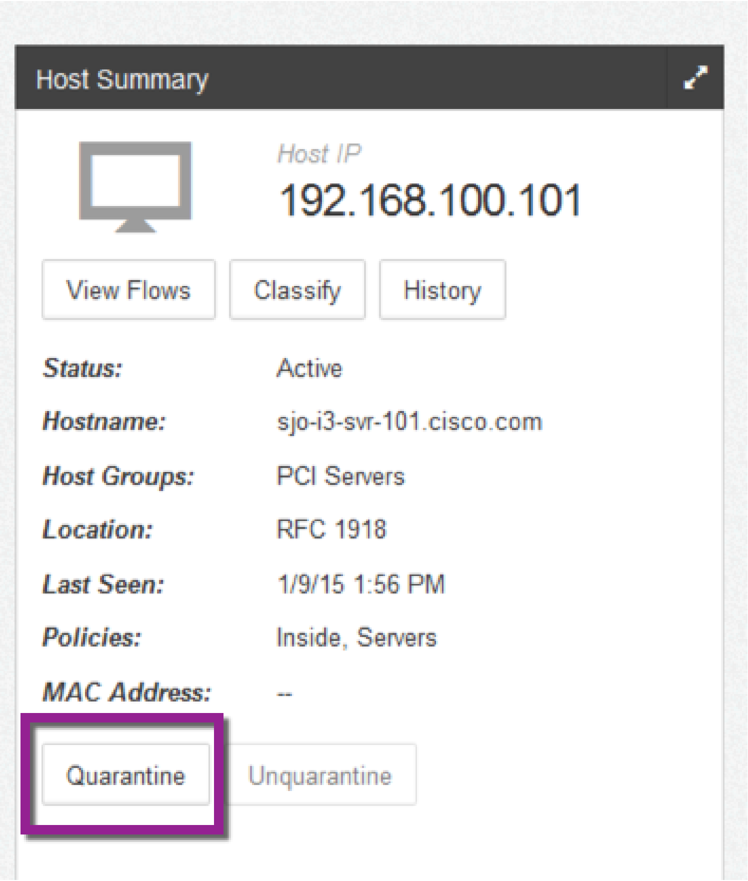
Quarantine/Unquarantine via pxGrid



Identity Services Engine

StealthWatch Management Console





Host Summary

Host IP
192.168.100.101

Status: Active

Hostname: sjo-i3-svr-101.cisco.com

Host Groups: PCI Servers

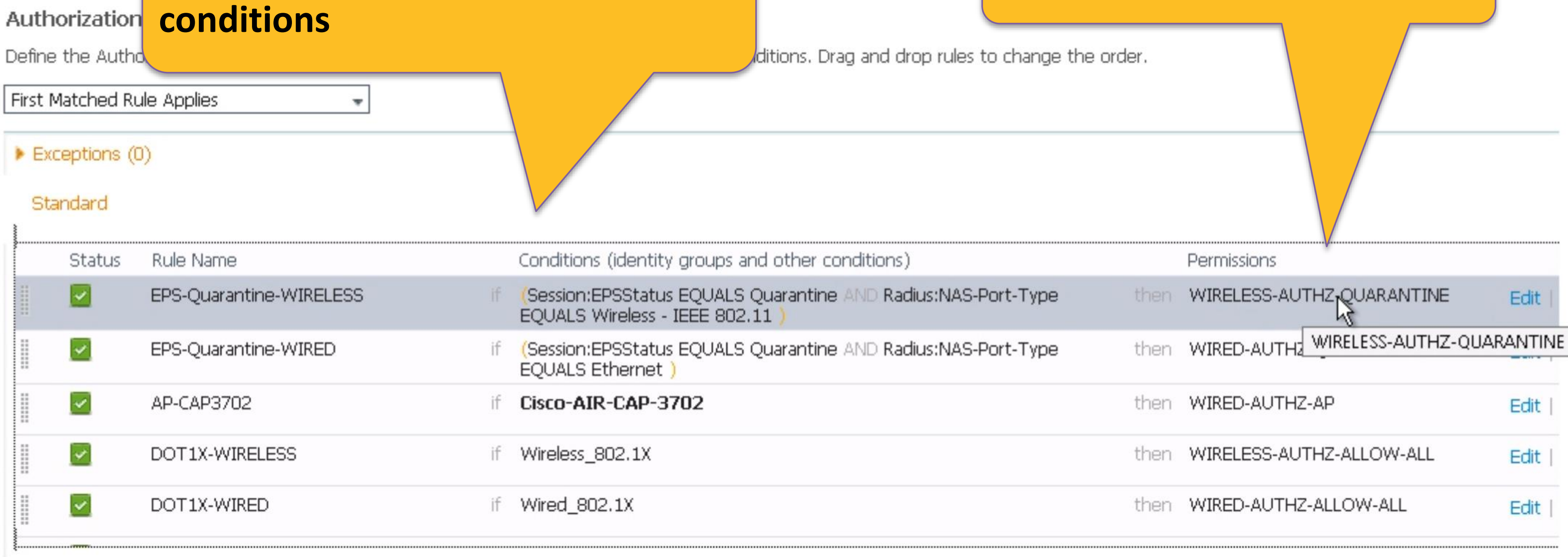
Location: RFC 1918

Last Seen: 1/9/15 1:56 PM

Policies: Inside, Servers

MAC Address: --

Authorization Policy in ISE using Quarantine Service



Quarantine state as one of the conditions

Quarantine definition in ISE

Authorization

Define the Autho ditions. Drag and drop rules to change the order.

First Matched Rule Applies ▾

▸ Exceptions (0)

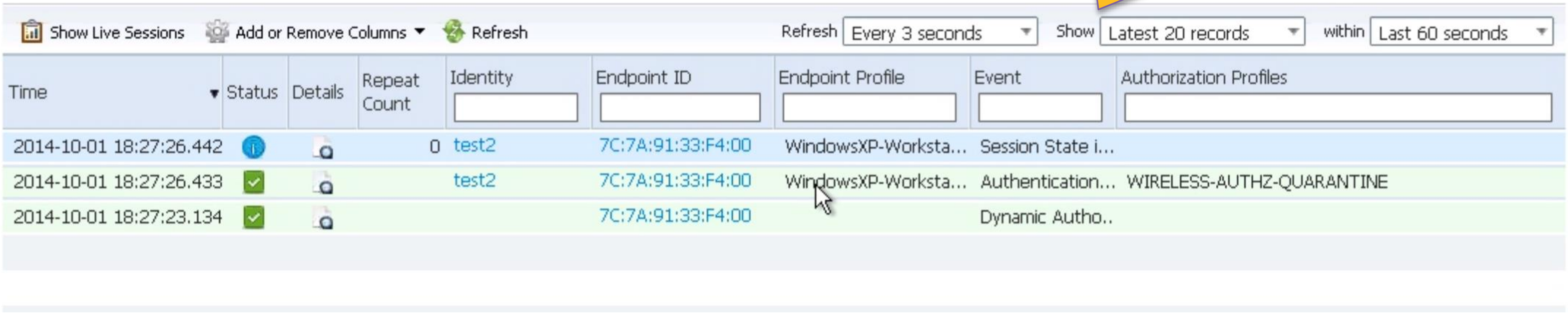
Standard

	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	Edit |
	✓	EPS-Quarantine-WIRED	if	(Session:EPSStatus EQUALS Quarantine AND Radius:NAS-Port-Type EQUALS Ethernet)	then	WIRED-AUTHZ	
	✓	AP-CAP3702	if	**Cisco-AIR-CAP-3702**	then	WIRED-AUTHZ-AP	Edit |
	✓	DOT1X-WIRELESS	if	Wireless_802.1X	then	WIRELESS-AUTHZ-ALLOW-ALL	Edit |
	✓	DOT1X-WIRED	if	Wired_802.1X	then	WIRED-AUTHZ-ALLOW-ALL	Edit |

WIRELESS-AUTHZ-QUARANTINE

Monitoring Devices

Quarantine state change => Quarantine authorization profile

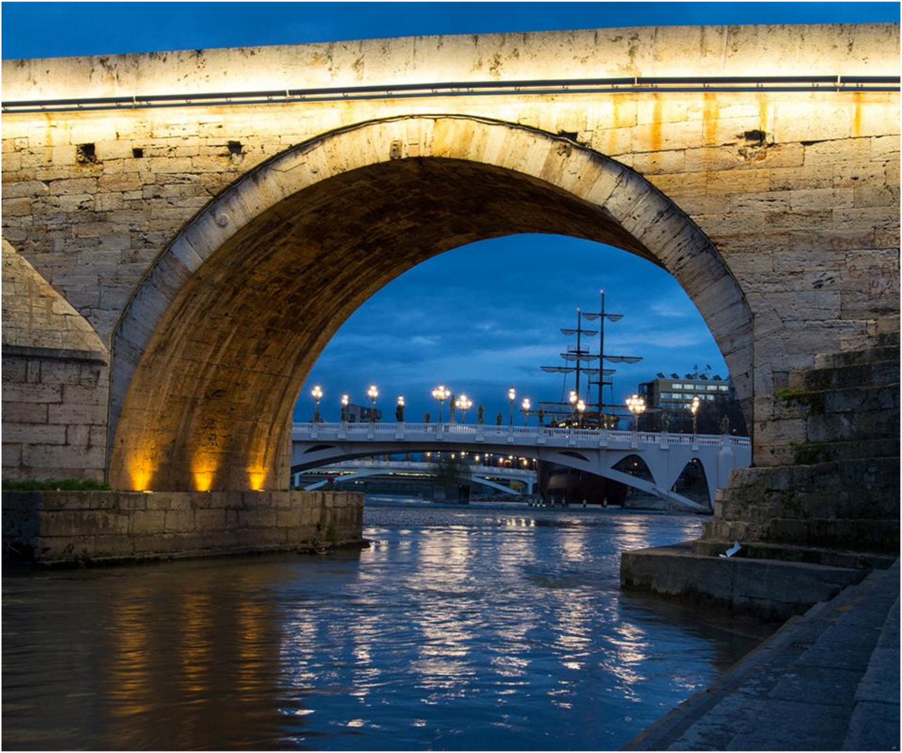


Show Live Sessions | Add or Remove Columns ▾ | Refresh

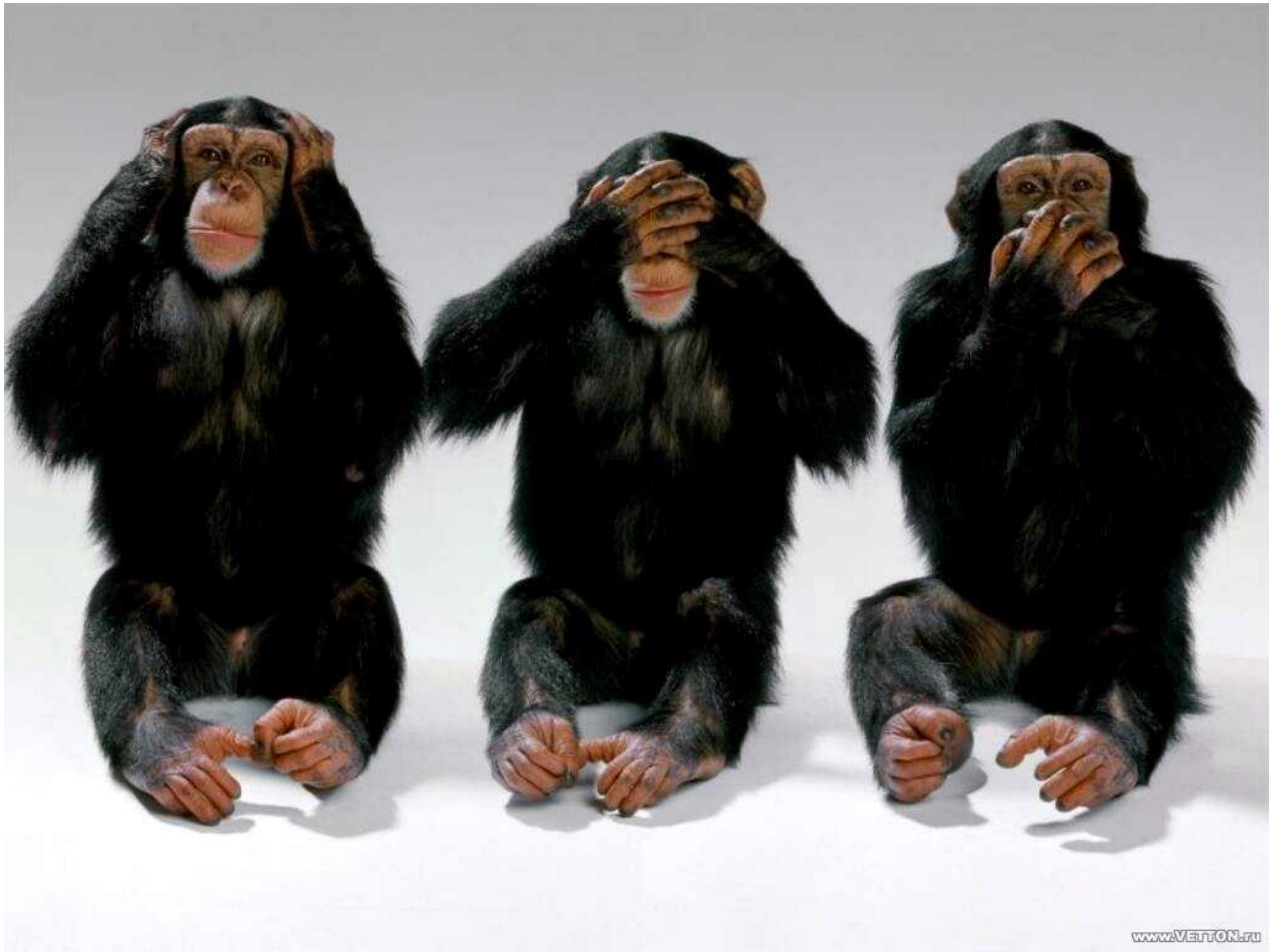
Refresh: Every 3 seconds ▾ | Show: Latest 20 records ▾ | within: Last 60 seconds ▾

Time ▾	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Event	Authorization Profiles
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



3 Friends



Source: gtaforums.com

3 Friends

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 cisco