Cisco live!

What You Make Possible

TOMORROW
starts here.

CISCO

Cyber Threat Defence

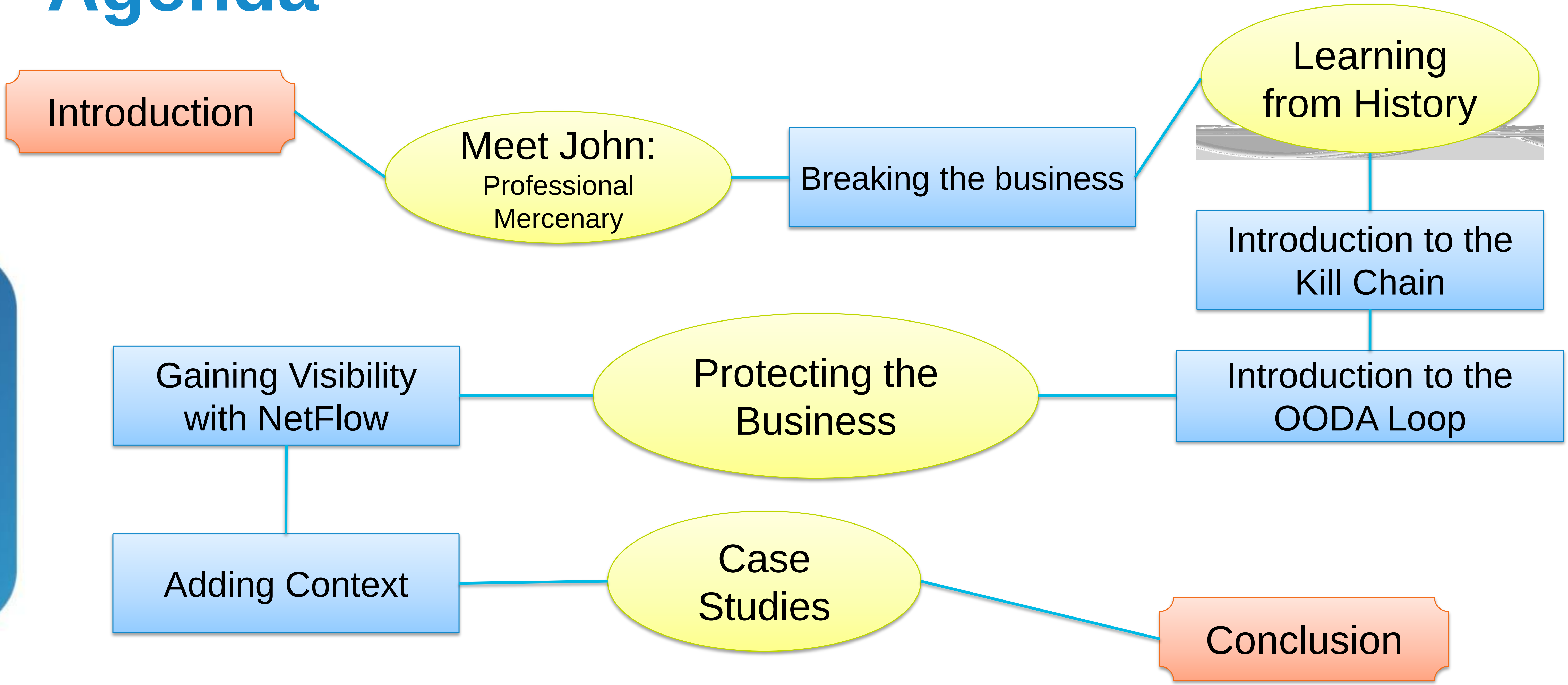
BRKSEC-2661

TOMORROW starts here.

Abstract

Trends such as BYOD and the rise of the Advance Persistent Threat (APT) have led to the erosion of the security perimeter of the enterprise. The Cisco Cyber Threat Defence Solution takes a systems approach to leveraging technology already present in the network, such as NetFlow, to provide visibility in order to identify suspicious activity on the interior network. Context, which can be used to differentiate between the insidious threats and day-to-day operations, is added through other network technologies such as the ISE. This session will present the technologies that comprise the solution as well as deployment and implementation best practices. Use cases such as detecting data loss and network reconnaissance activity as well as detecting botnet command and control activity and tracking the spread of a malware infection throughout the network will be covered.

Agenda



Introduction

Meet John: Professional Mercenary

Breaking the business

Learning from History

Introduction to the Kill Chain

Introduction to the OODA Loop

Protecting the Business

Gaining Visibility with NetFlow

Adding Context

Case Studies

Conclusion

Session Objectives

- At the end of the session, the participants should be able to:
  - Understand the key challenges to complex threat visibility
  - Define Cisco's approach to solving this problem
  - Understand how to instrument their network infrastructure to gain visibility and context
  - How to use the increased level of visibility and context to identify cyber threats

Meet John

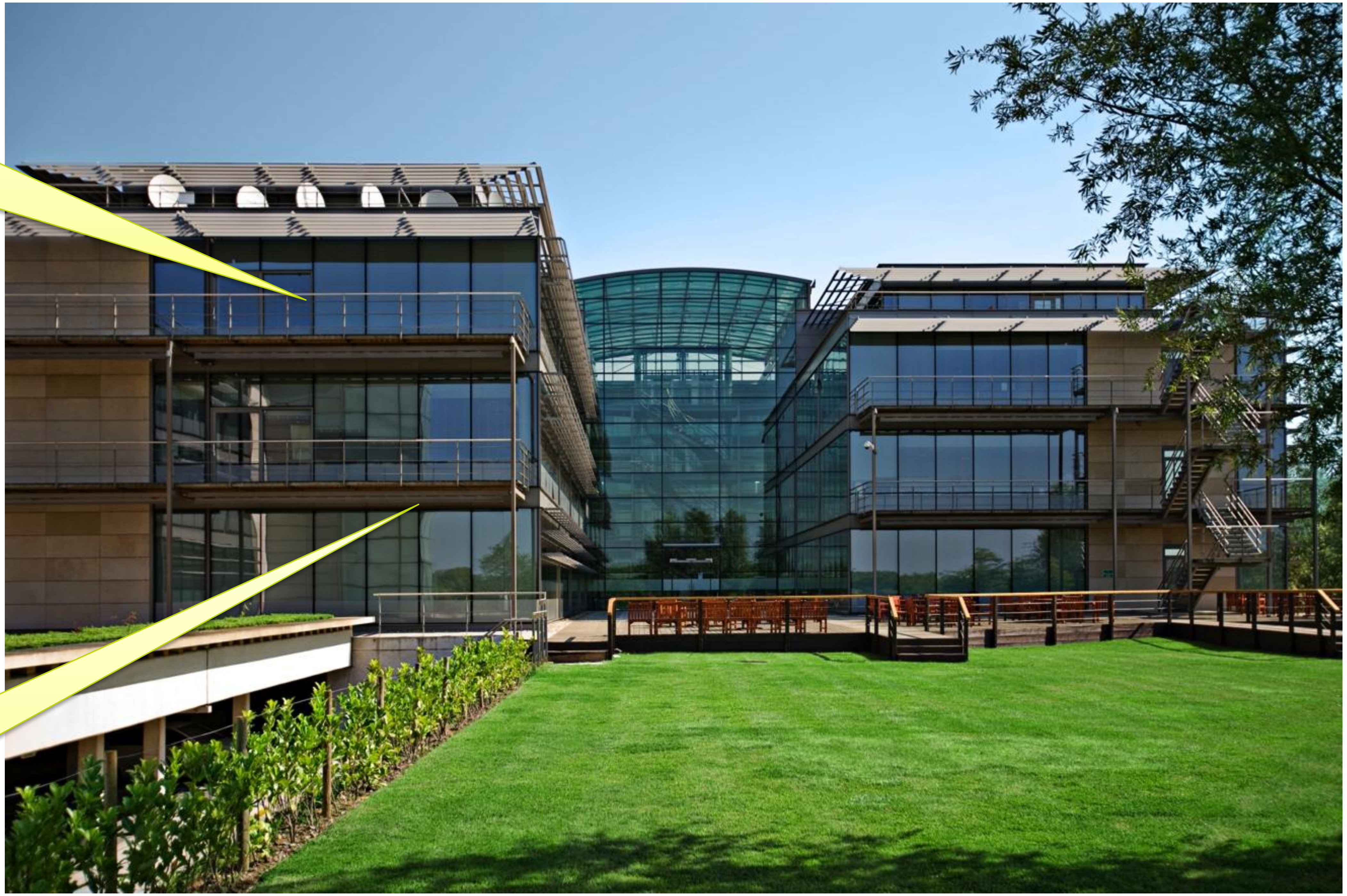
Professional Mercenary

University Graduate

Contracted by a Nation State

Success Driven

Objective



Assigned by Employer – payment on delivery

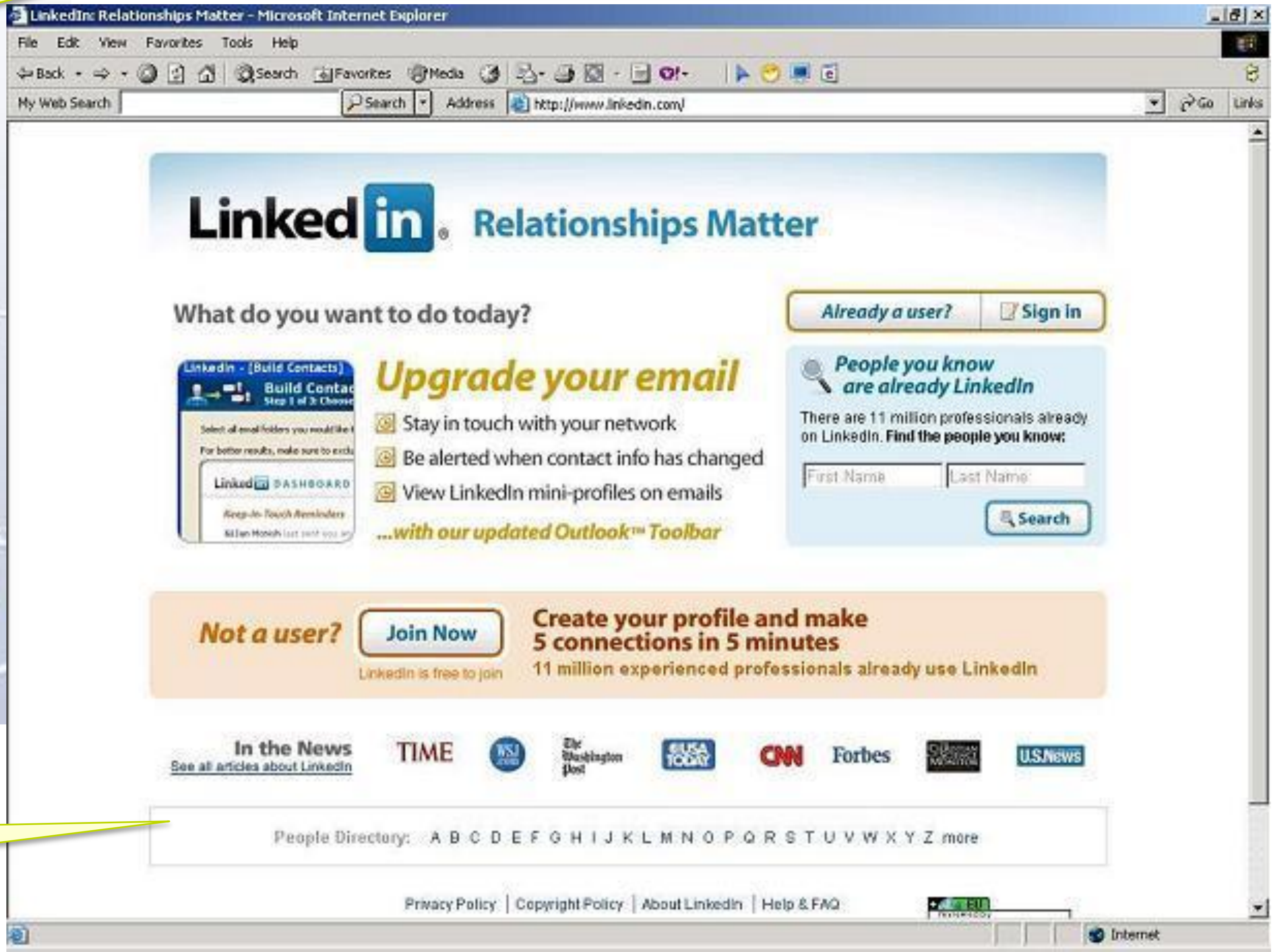
Steal critical secrets

Step 1: Reconnaissance

Learn personal information

facebook

Facebook helps you connect and share with the people in your life.



LinkedIn: Relationships Matter - Microsoft Internet Explorer

Address: http://www.linkedin.com/

Linked in. Relationships Matter

What do you want to do today?

Already a user? Sign In

Upgrade your email

- Stay in touch with your network
- Be alerted when contact info has changed
- View LinkedIn mini-profiles on emails

...with our updated Outlook™ Toolbar

People you know are already LinkedIn

There are 11 million professionals already on LinkedIn. Find the people you know:

First Name: Last Name:

Search

Not a user? Join Now

LinkedIn is free to join

Create your profile and make 5 connections in 5 minutes

11 million experienced professionals already use LinkedIn

In the News

See all articles about LinkedIn

People Directory: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z more

Privacy Policy | Copyright Policy | About LinkedIn | Help & FAQ

Identify employees

Step 2: Infection

Installs remote control software using legitimate password

Step 3: Propagation

Performs exploratory activity in internal network. Identifies assets, information, targets

Gains access to target systems

Step 4: Exfiltration

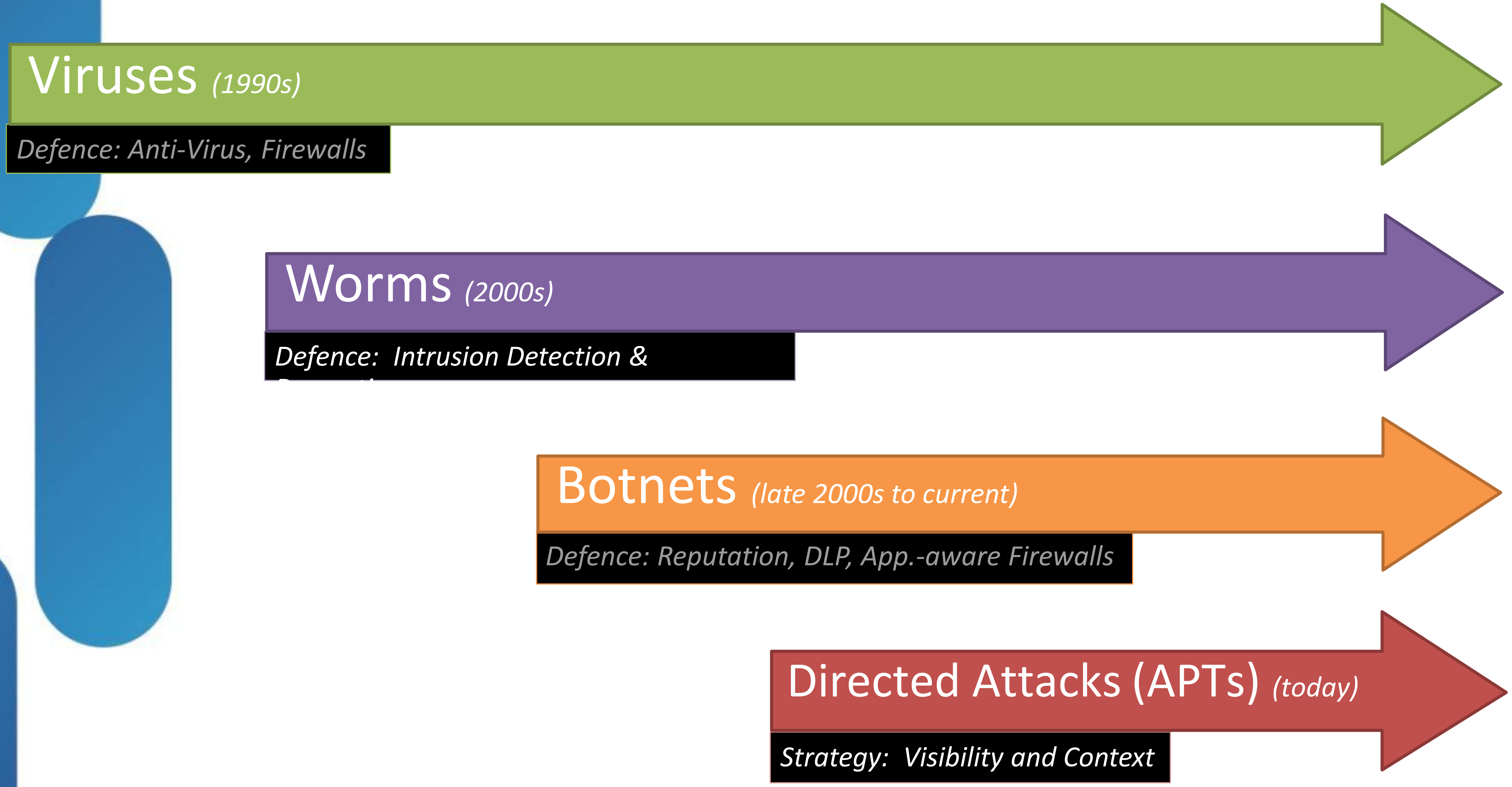
Data is obtained from repository and stolen.

Debrief

So What Happened Here?

- Skilled, determined, motivated attacker with defined measure of success
- Perimeter successfully bypassed
- Propagation throughout the internal network
- Valid credentials used
- Data moved from critical asset and exfiltrated

The Evolution of Cyber Threats



Viruses *(1990s)*

Defence: Anti-Virus, Firewalls

Worms *(2000s)*

Defence: Intrusion Detection &

Botnets *(late 2000s to current)*

Defence: Reputation, DLP, App.-aware Firewalls

Directed Attacks (APTs) *(today)*

Strategy: Visibility and Context

ILOVEYOU
Melissa
Anna Kournikova

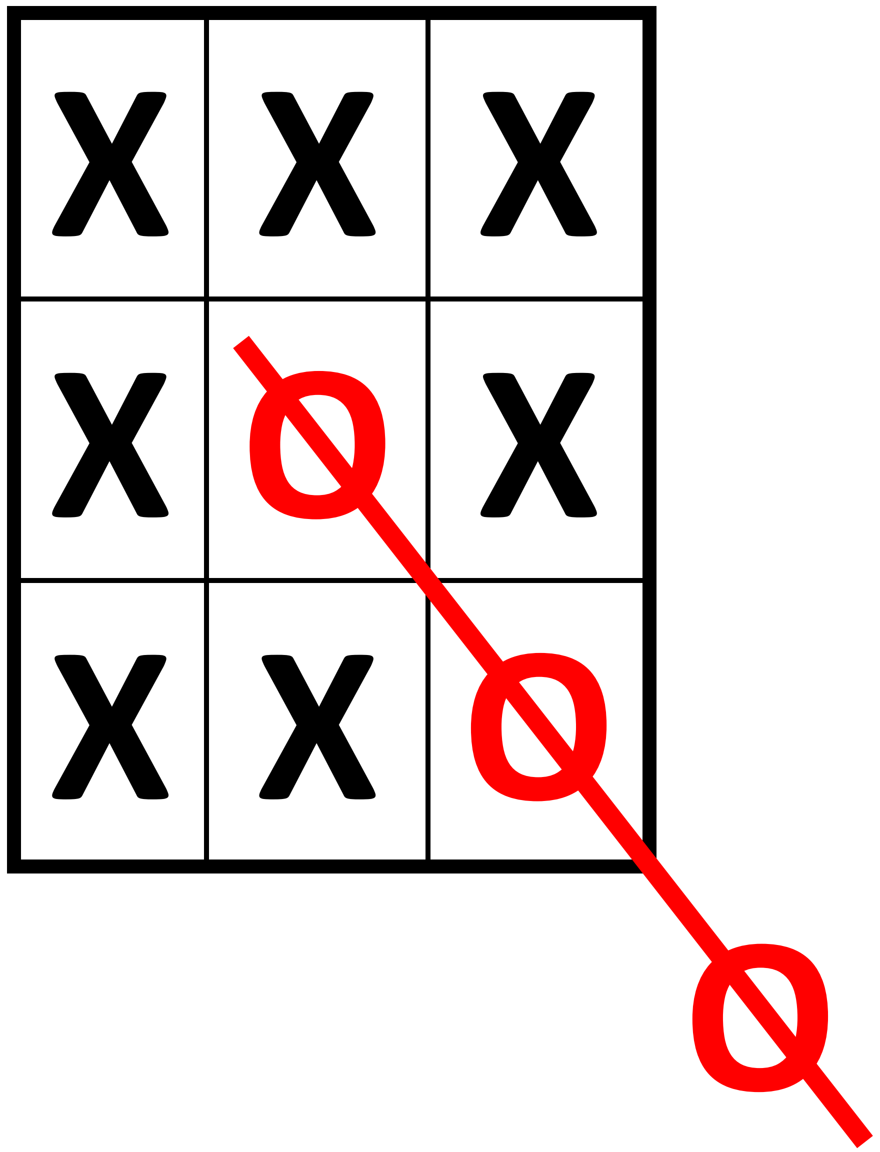
Nimda
SQL Slammer
Conficker

Tedroo
Rustock
Conficker

Aurora
Shady Rat
Duqu

Thinking Beyond the Perimeter

Advanced Persistent Threats and other Modern threats are consistently bypassing the security perimeter as they redraw the map



Once on the network APT’s hide in plain sight

Concept: Kill Chain

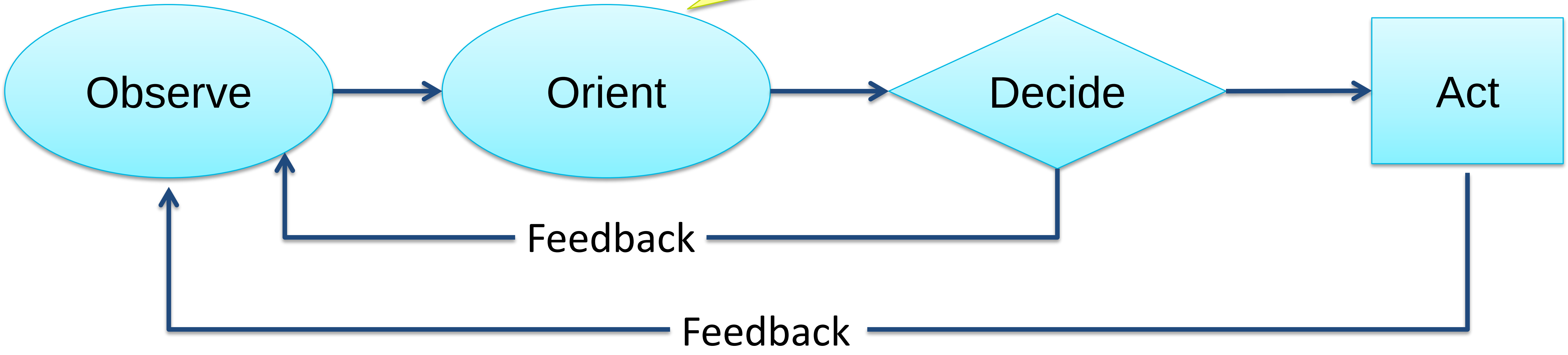
Reconnaissance	• Harvesting email addresses, identifying information, etc.
Weaponisation	• Coupling exploit with backdoor into deliverable payload
Delivery	• Delivering weaponised bundle to the victim via email, web, USB, etc.
Exploitation	• Exploiting a vulnerability to execute code in victim system
Command and Control	• Command channel for remote manipulation of victim
Actions on Objectives	• Intruders accomplish their original goal

- http://computer-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain/

Concept: OODA Loop

- Unfolding circumstances
- Implicit guidance
- Outside information
- Unfolding interaction with environment

- Cultural Traditions
- Genetic Heritage
- Analysis & Synthesis
- New information
- Previous Experiences



Unfolding interaction with environment

Know the Attacker

Who?	• Nation-state? Competitor? Individual?
What?	• What is the target?
When?	• Is there a time when the attacker is most active?
Where?	• Where is the attacker? Where are they successful?
Why?	• Why are they attacking – what is their goal?
How?	• How are they attacking – Zero-day? Known-passwords? Insider?

Know Yourself

Who?	• Is on the the network?
What?	• Are your users doing? application? Behaviour?
When?	• The device was on the network? Is it normal?
Where?	• Where do users normally access the network from?
Why?	• Why are they using that application?
How?	• Are they accessing the network?

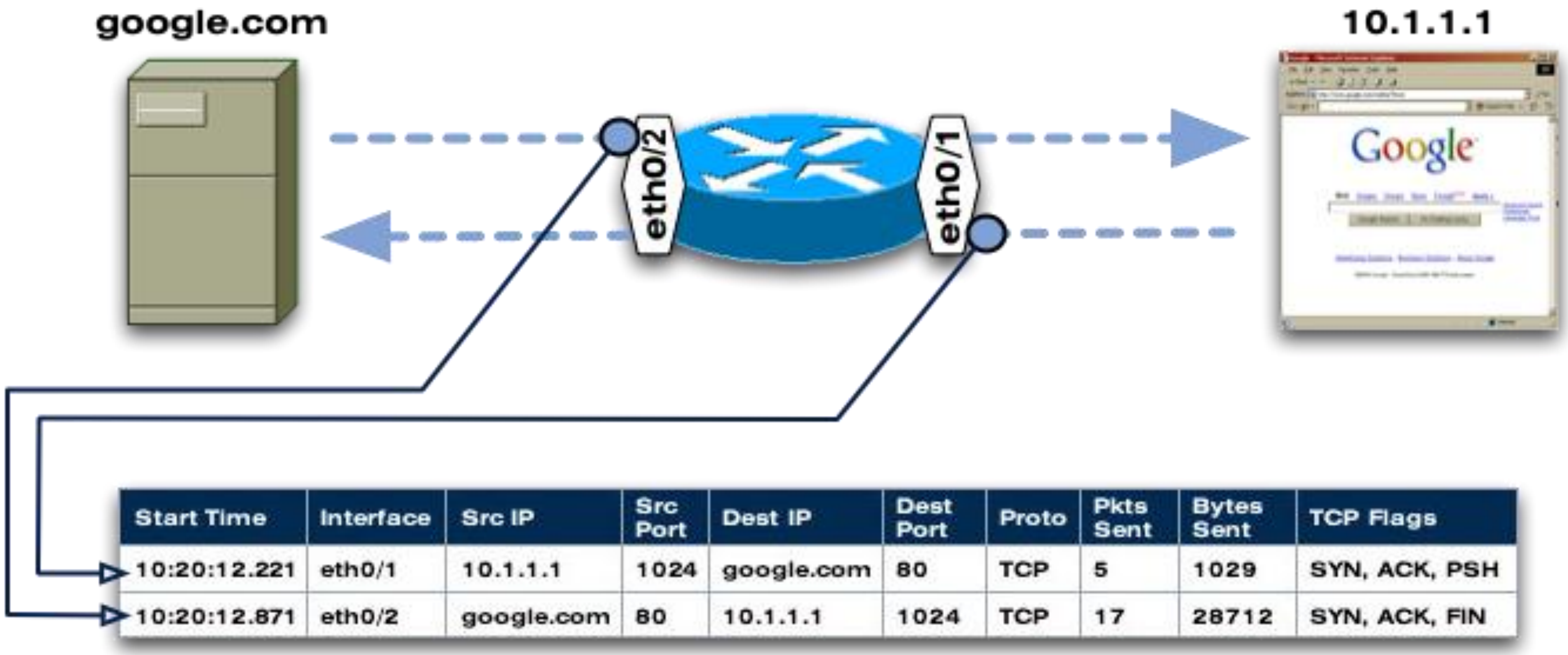
Telemetry – Measure at a Distance

- SIGINT
- Traffic Analysis
- Usage patterns
- Information flow

- Visibility and Context

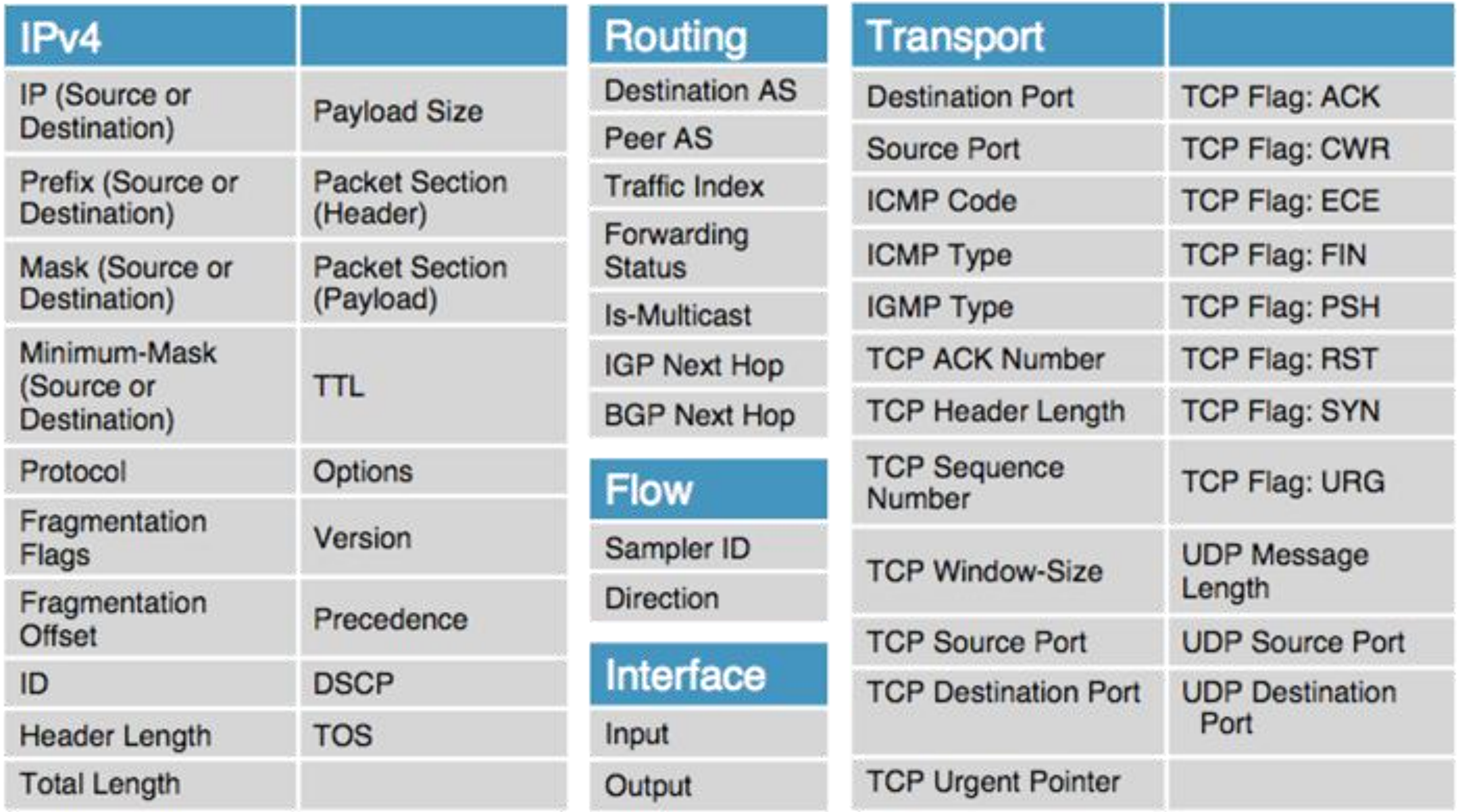
CANADA
ENGLAND
WASHINGTON
WEST VIRGINIA
GERMANY
ECHELON
TELECOM
ECHELON
TELECOM
ECHELON
TELECOM
AUSTRALIA
NEW ZEALAND
Echelon Global Electronic Surveillance System

NetFlow



Start Time	Interface	Src IP	Src Port	Dest IP	Dest Port	Proto	Pkts Sent	Bytes Sent	TCP Flags
10:20:12.221	eth0/1	10.1.1.1	1024	google.com	80	TCP	5	1029	SYN, ACK, PSH
10:20:12.871	eth0/2	google.com	80	10.1.1.1	1024	TCP	17	28712	SYN, ACK, FIN

NetFlow



IPv4	
IP (Source or Destination)	Payload Size
Prefix (Source or Destination)	Packet Section (Header)
Mask (Source or Destination)	Packet Section (Payload)
Minimum-Mask (Source or Destination)	TTL
Protocol	Options
Fragmentation Flags	Version
Fragmentation Offset	Precedence
ID	DSCP
Header Length	TOS
Total Length	

Routing
Destination AS
Peer AS
Traffic Index
Forwarding Status
Is-Multicast
IGP Next Hop
BGP Next Hop

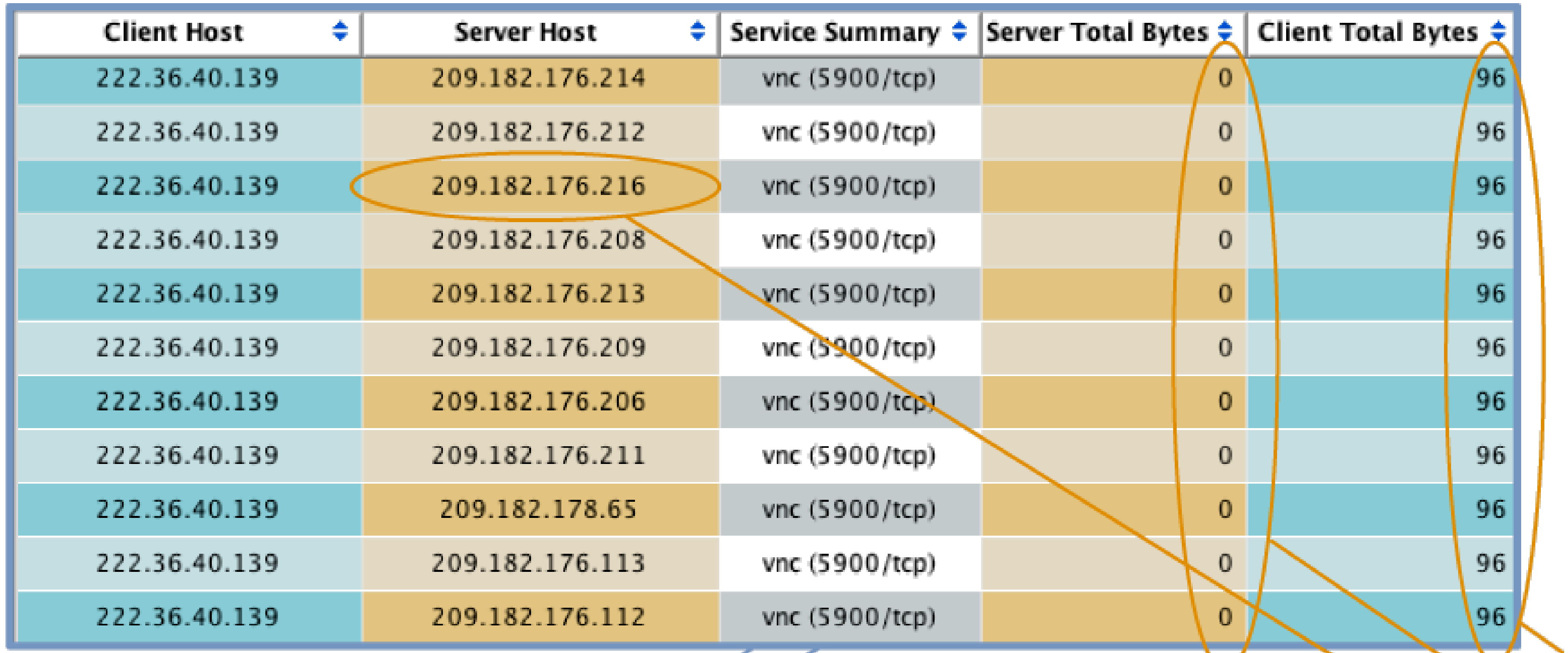
Flow
Sampler ID
Direction

Interface
Input
Output

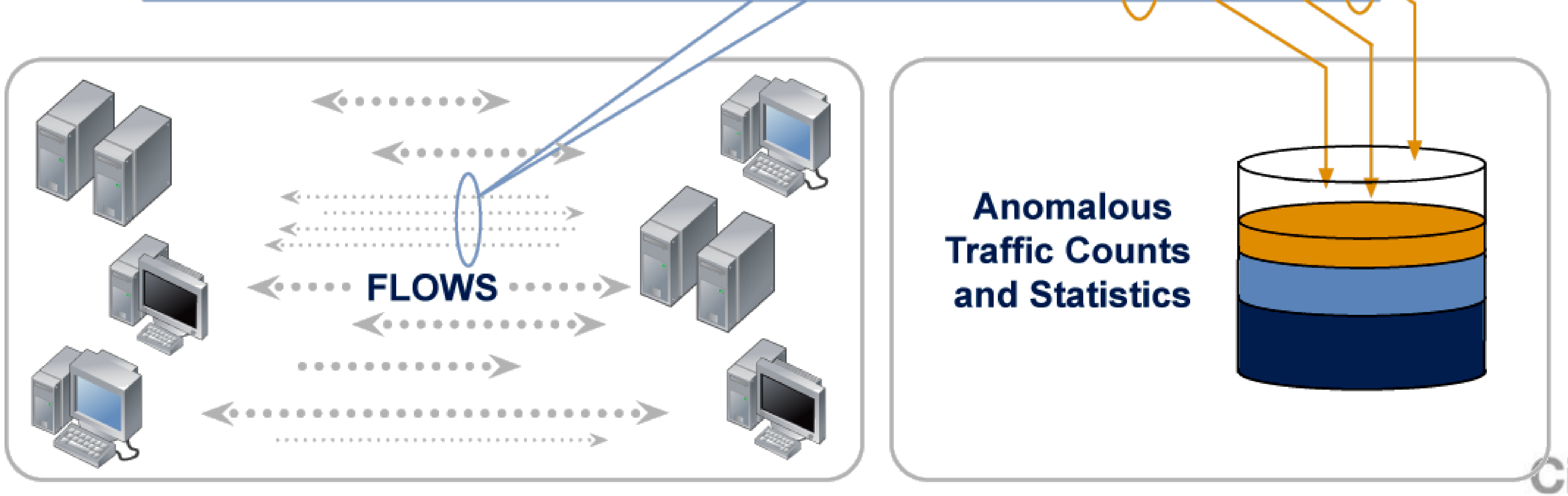
Transport	
Destination Port	TCP Flag: ACK
Source Port	TCP Flag: CWR
ICMP Code	TCP Flag: ECE
ICMP Type	TCP Flag: FIN
IGMP Type	TCP Flag: PSH
TCP ACK Number	TCP Flag: RST
TCP Header Length	TCP Flag: SYN
TCP Sequence Number	TCP Flag: URG
TCP Window-Size	UDP Message Length
TCP Source Port	UDP Source Port
TCP Destination Port	UDP Destination Port
TCP Urgent Pointer	

NetFlow v9 160+ fields to choose from including IPv6 and payload sections

Flow Based Anomaly Detection

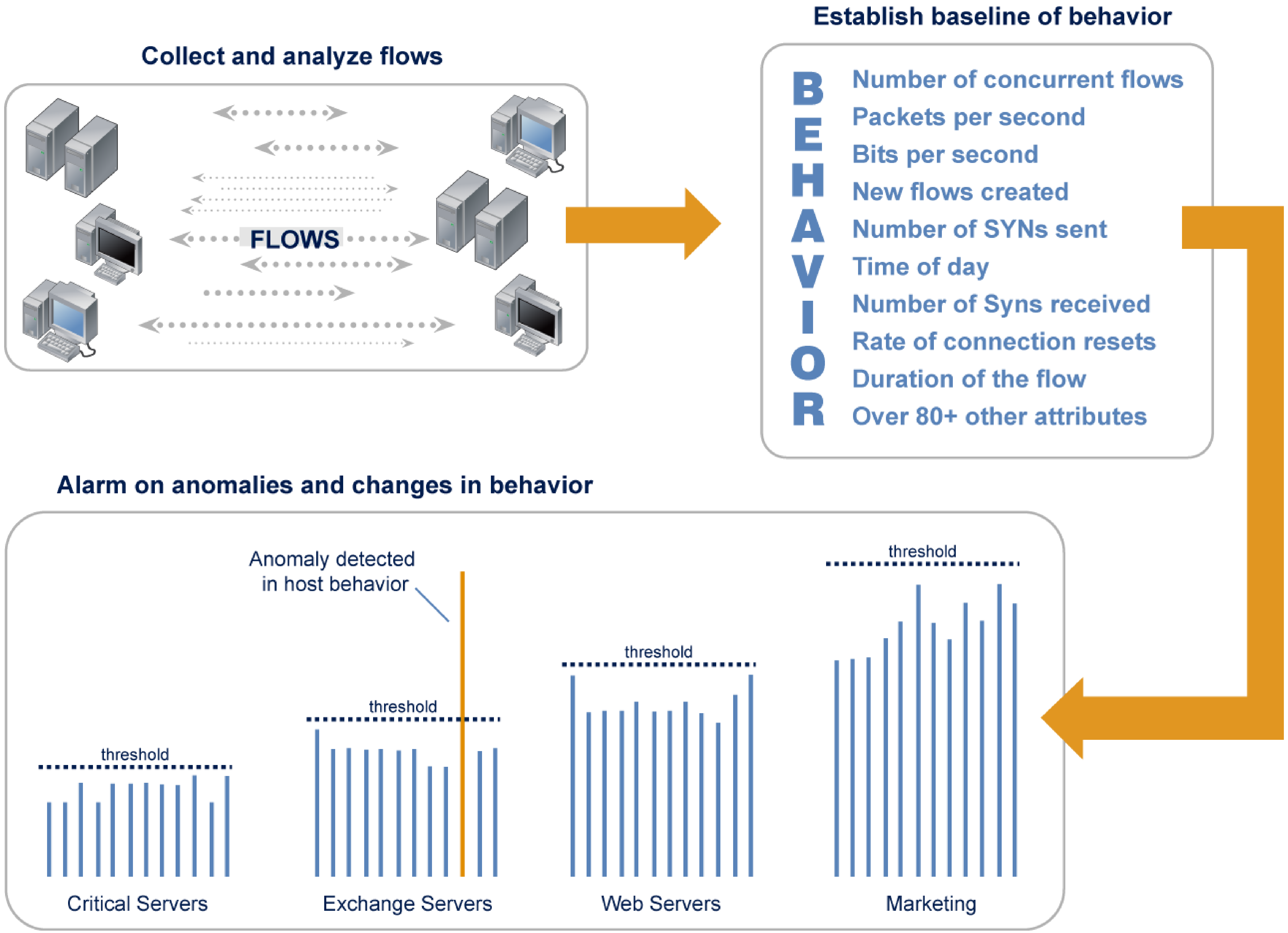


Client Host	Server Host	Service Summary	Server Total Bytes	Client Total Bytes
222.36.40.139	209.182.176.214	vnc (5900/tcp)	0	96
222.36.40.139	209.182.176.212	vnc (5900/tcp)	0	96
222.36.40.139	209.182.176.216	vnc (5900/tcp)	0	96
222.36.40.139	209.182.176.208	vnc (5900/tcp)	0	96
222.36.40.139	209.182.176.213	vnc (5900/tcp)	0	96
222.36.40.139	209.182.176.209	vnc (5900/tcp)	0	96
222.36.40.139	209.182.176.206	vnc (5900/tcp)	0	96
222.36.40.139	209.182.176.211	vnc (5900/tcp)	0	96
222.36.40.139	209.182.178.65	vnc (5900/tcp)	0	96
222.36.40.139	209.182.176.113	vnc (5900/tcp)	0	96
222.36.40.139	209.182.176.112	vnc (5900/tcp)	0	96



Anomalous Traffic Counts and Statistics

Behaviour Based Analysis



Collect and analyze flows

Establish baseline of behavior

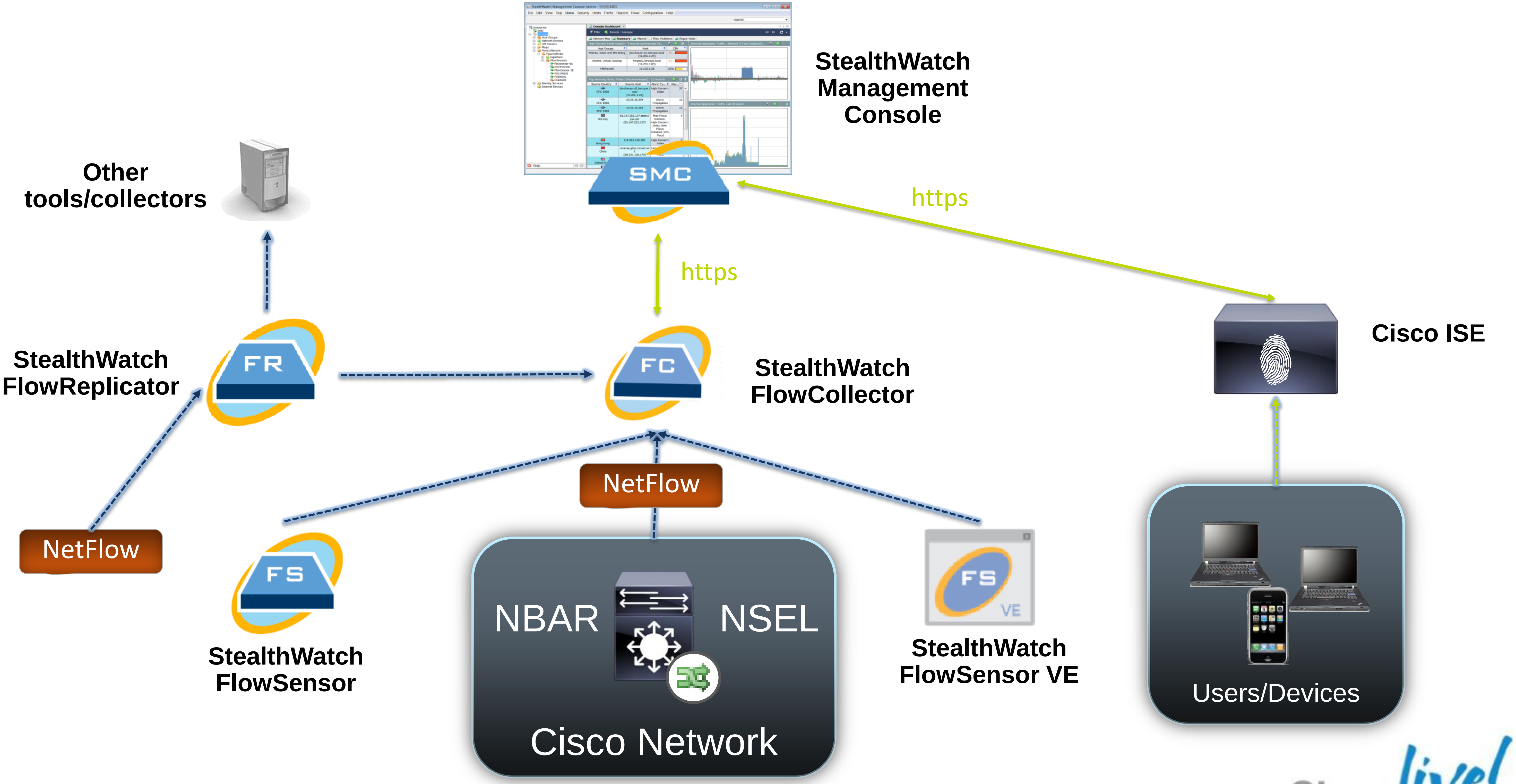
B E H A V I O R

- Number of 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

Alarm on anomalies and changes in behavior

Leveraging NetFlow

Components for Advanced Threat Detection



StealthWatch Management Console

SMC

https

https

Other tools/collectors

StealthWatch FlowReplicator

FR

FC

StealthWatch FlowCollector

Cisco ISE

NetFlow

NetFlow

FS

StealthWatch FlowSensor

NBAR

NSEL

Cisco Network

FS VE

StealthWatch FlowSensor VE

Users/Devices

Cisco NetFlow Support

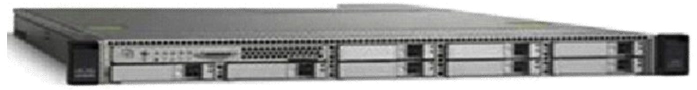
Cisco ASA

Cisco 2900

Cisco 2800

Cisco 1700

Cisco 7600


Cisco NGA

Cisco 7200 VXR

Cisco ISR G2

Cisco XR 12000

Hardware Supported

Cisco Nexus 7000

Cisco ASR

Cisco 3560/3750-X

Cisco Catalyst 4500

Cisco Catalyst 6500

Versions of NetFlow

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	Standardised – 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

1. Configure the Exporter

```
Router(config)# flow exporter my-exporter

Router(config-flow-exporter)# destination 1.1.1.1
```

2. Configure the Flow Record

```
Router(config)# flow record my-record
Router(config-flow-record)# match ipv4 destination address
Router(config-flow-record)# match ipv4 source address
Router(config-flow-record)# collect counter bytes
```

3. Configure the Flow Monitor

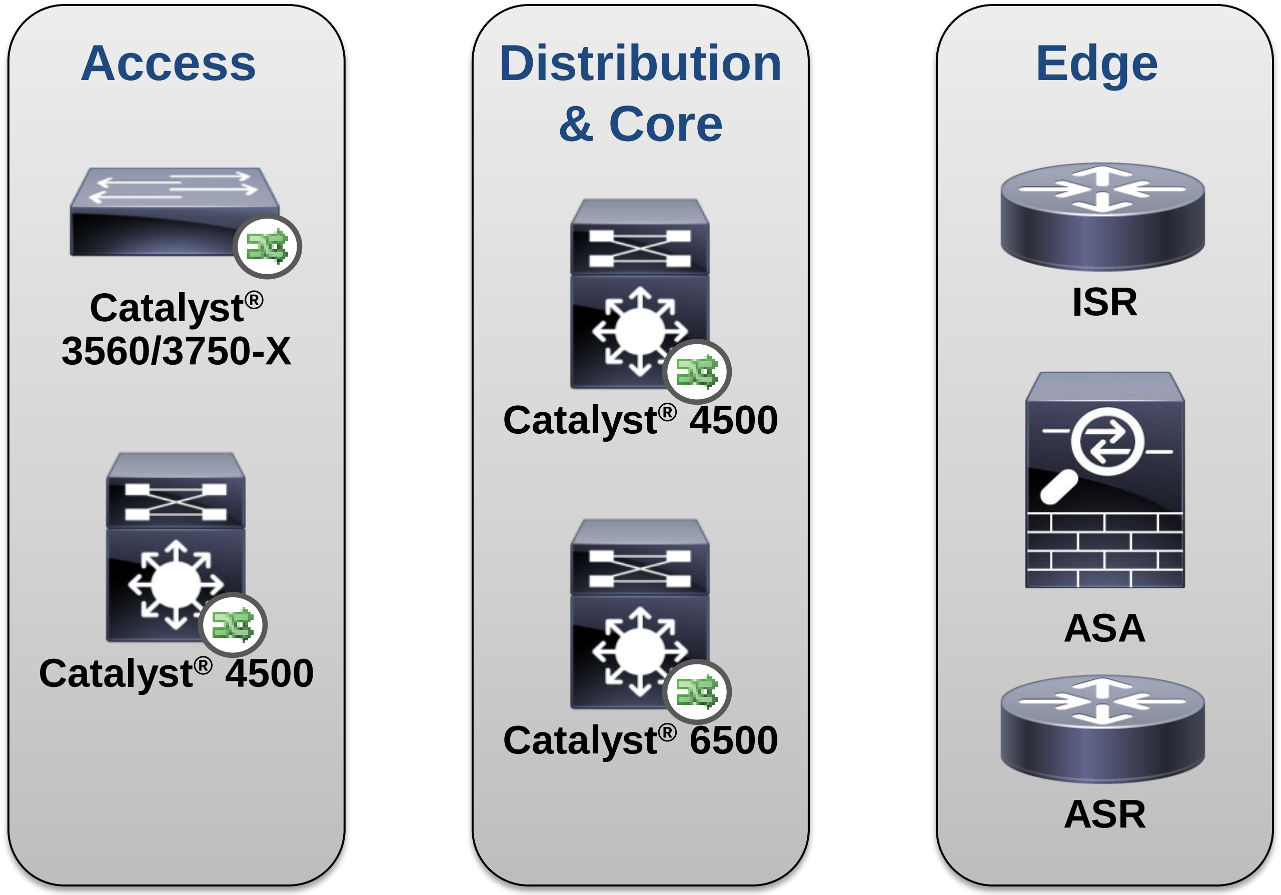
```
Router(config)# flow monitor my-monitor

Router(config-flow-monitor)# exporter my-exporter

Router(config-flow-monitor)# record my-record
```

4. Apply to an Interface

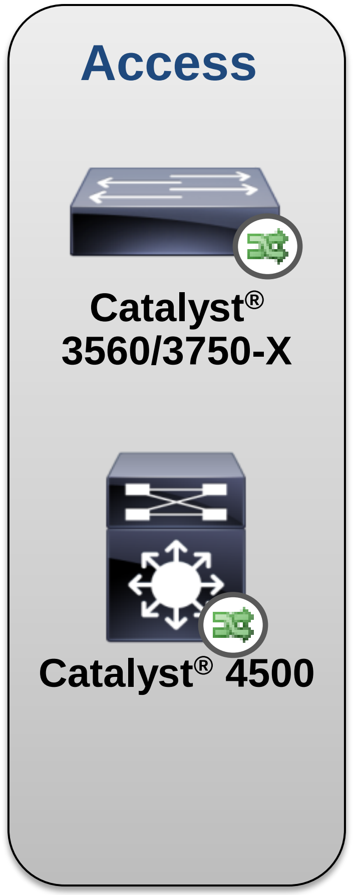
```
Router(config)# interface s3/0

Router(config-if)# ip flow monitor my-monitor input
```

NetFlow Deployment

Each network layer offers unique NetFlow capabilities



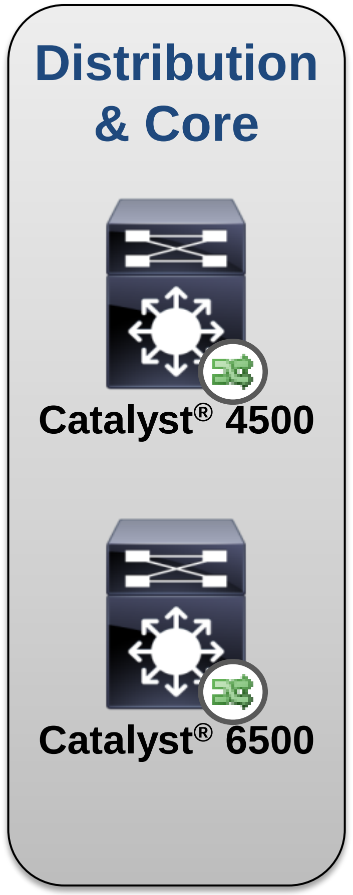
NetFlow Deployment



Access:

- New network edge
  - Detect threats as the enter the network
- Detect threats inside the switch
  - east-west
  - Layer 2 traffic
- Fewer false positives
  - Higher-granular visibility
- Identify the endpoint
  - collect MAC Address

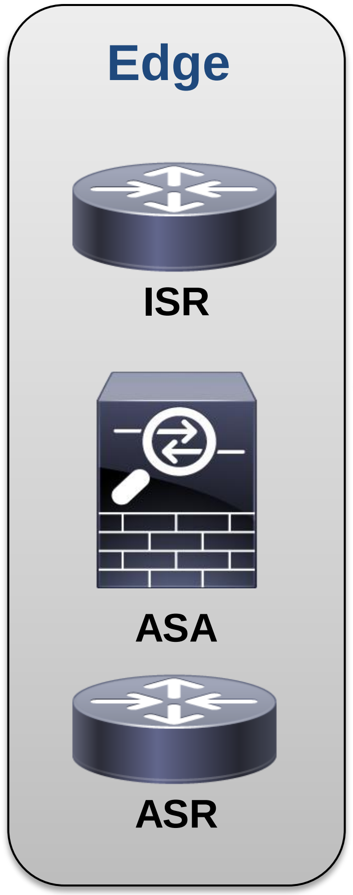
NetFlow Deployment



Distribution & Core:

- Traditional deployment
  - Minimal recommended deployment
- Enable at critical points/bottle necks
- Typically done on a Layer 3 boundary
- Detect threats internal to the VLAN
  - When deployed on an SVI interface
- Detect threats as they traverse the internal network
  - Move between subnets

NetFlow Deployment

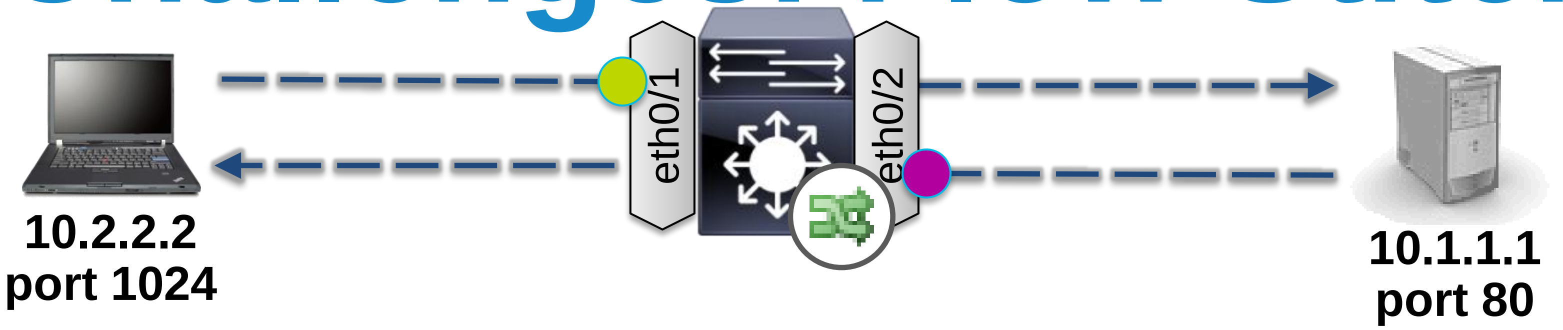


Edge:

- Detect threats as they enter and leave the network
- Monitor communication between branches
- Gain context from edge devices
  - Application - NBAR
  - Events - NSEL

NetFlow Challenges: Flow Stitching

Uni-directional flow 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

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

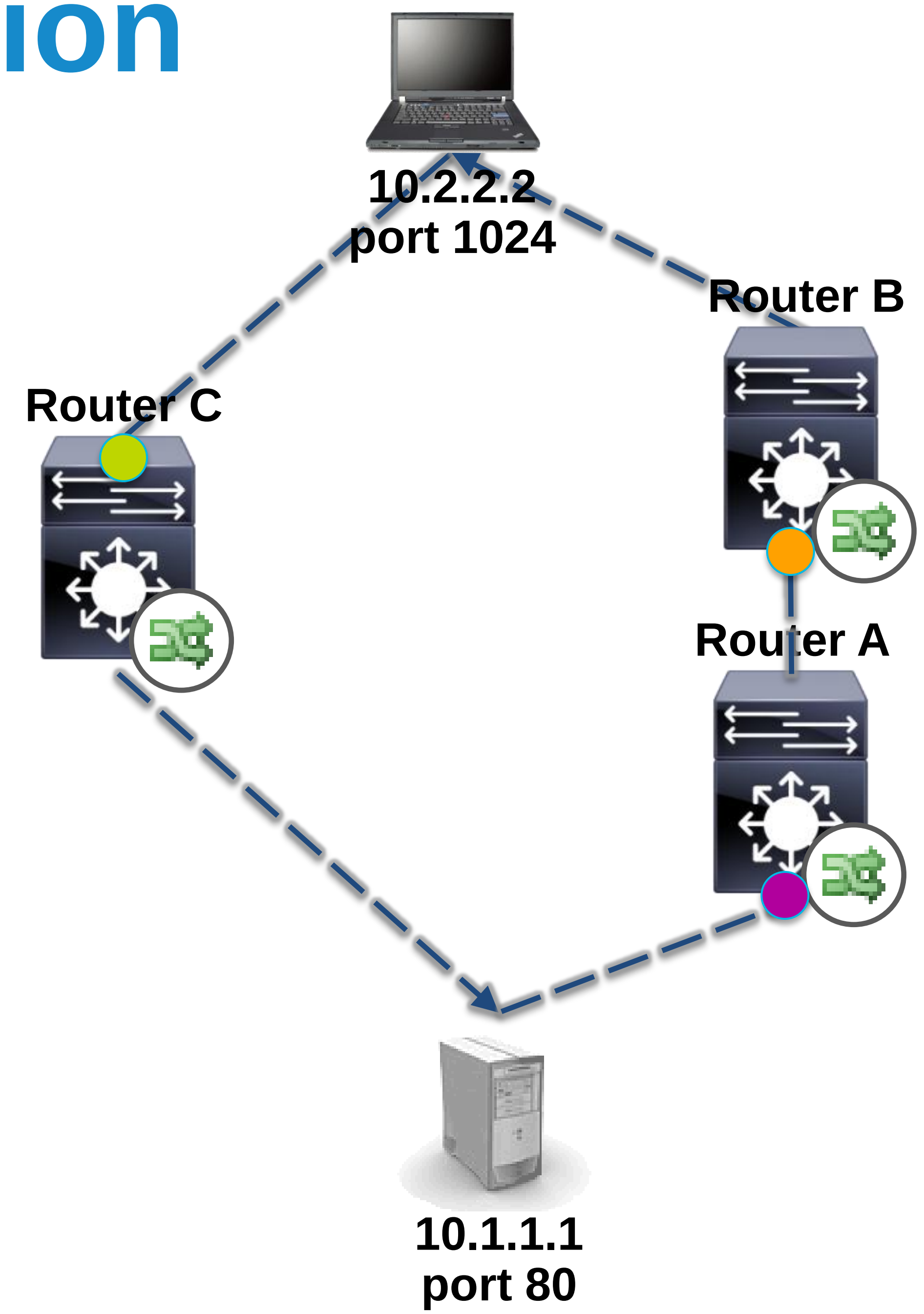
Bi-directional:

- Conversation flow record
- Allows easy visualisation and analysis

NetFlow Challenges: De-duplication

Duplicates

- ● Router A: 10.2.2.2:1024 -> 10.1.1.1:80
- ● Router B: 10.2.2.2:1024 -> 10.1.1.1:80
- ● Router C: 10.1.1.1:80 -> 10.2.2.2:1024

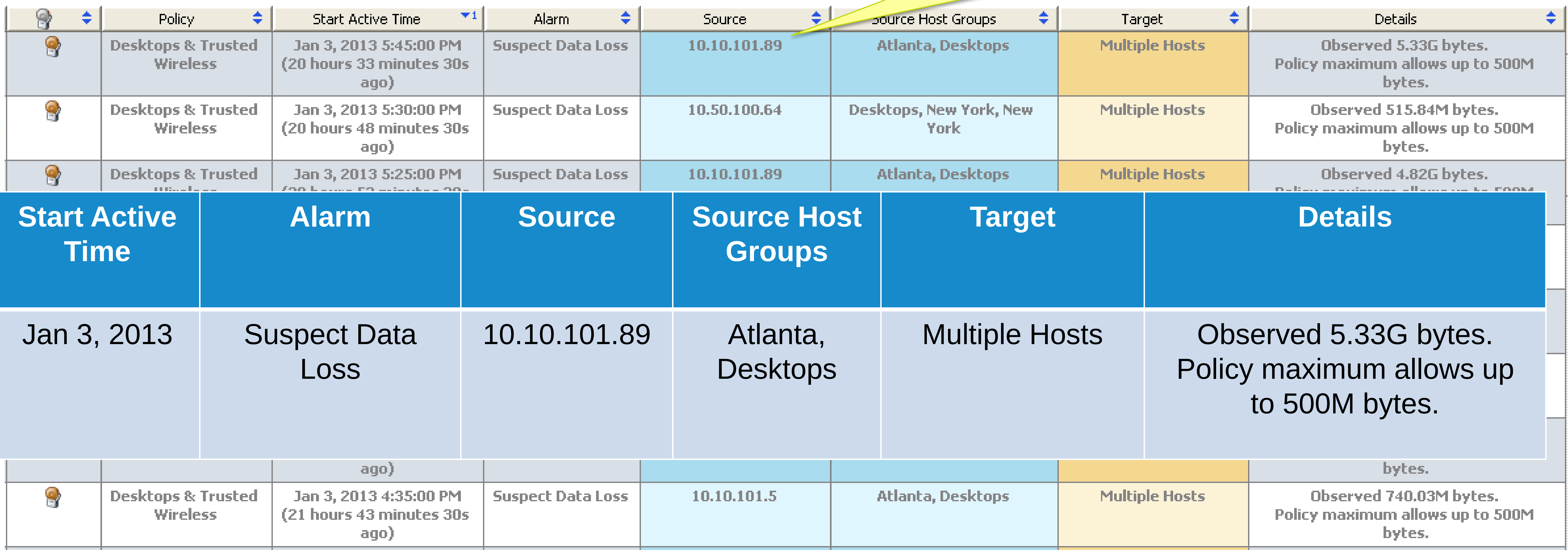


- Without de-duplication:
  - Traffic volume can be misreported
  - False positive would occur
- Allows for the efficient storage of flow data
- Necessary for accurate host-level reporting
- Does not discard data

The Need for Context

A Key Challenge in Threat Visibility

Who is 10.10.101.89?

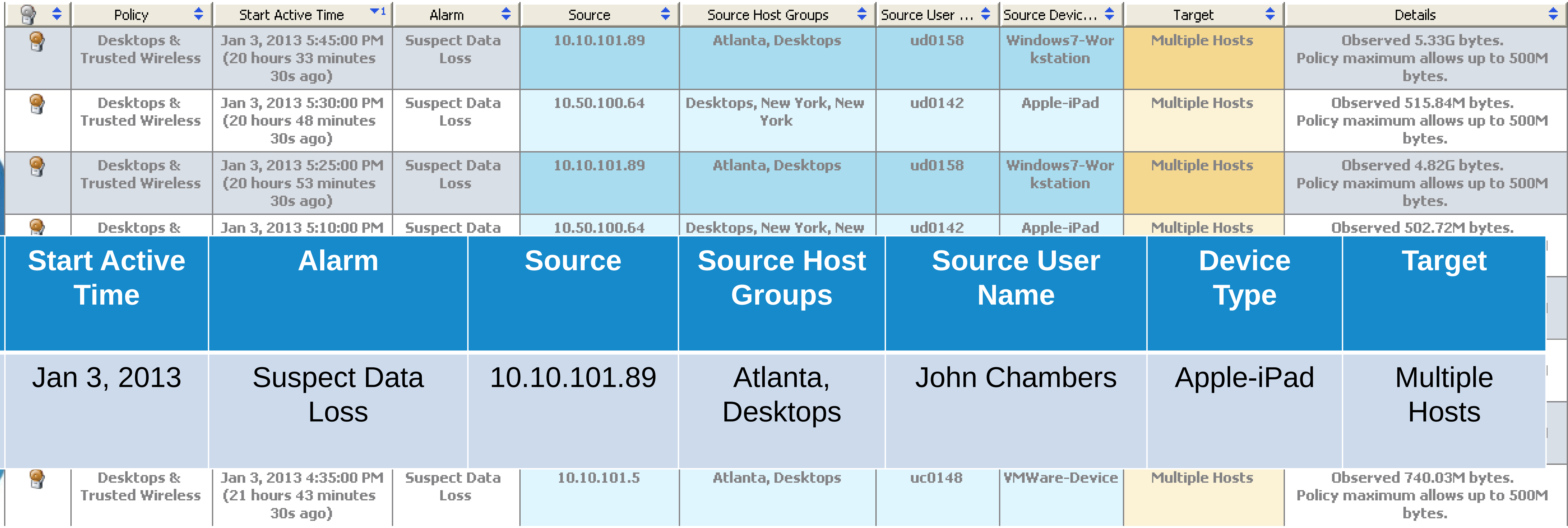


	Policy	Start Active Time	Alarm	Source	Source Host Groups	Target	Details
	Desktops & Trusted Wireless	Jan 3, 2013 5:45:00 PM (20 hours 33 minutes 30s ago)	Suspect Data Loss	10.10.101.89	Atlanta, Desktops	Multiple Hosts	Observed 5.33G bytes. Policy maximum allows up to 500M bytes.
	Desktops & Trusted Wireless	Jan 3, 2013 5:30:00 PM (20 hours 48 minutes 30s ago)	Suspect Data Loss	10.50.100.64	Desktops, New York, New York	Multiple Hosts	Observed 515.84M bytes. Policy maximum allows up to 500M bytes.
	Desktops & Trusted	Jan 3, 2013 5:25:00 PM	Suspect Data Loss	10.10.101.89	Atlanta, Desktops	Multiple Hosts	Observed 4.82G bytes.
		ago)					bytes.
	Desktops & Trusted Wireless	Jan 3, 2013 4:35:00 PM (21 hours 43 minutes 30s ago)	Suspect Data Loss	10.10.101.5	Atlanta, Desktops	Multiple Hosts	Observed 740.03M bytes. Policy maximum allows up to 500M bytes.

Policy	Start Active Time	Alarm	Source	Source Host Groups	Target	Details
Desktops & Trusted Wireless	Jan 3, 2013	Suspect Data Loss	10.10.101.89	Atlanta, Desktops	Multiple Hosts	Observed 5.33G bytes. Policy maximum allows up to 500M bytes.

Obtain Context Through the Cisco ISE

Attribute Flows and Behaviours to a User and Device

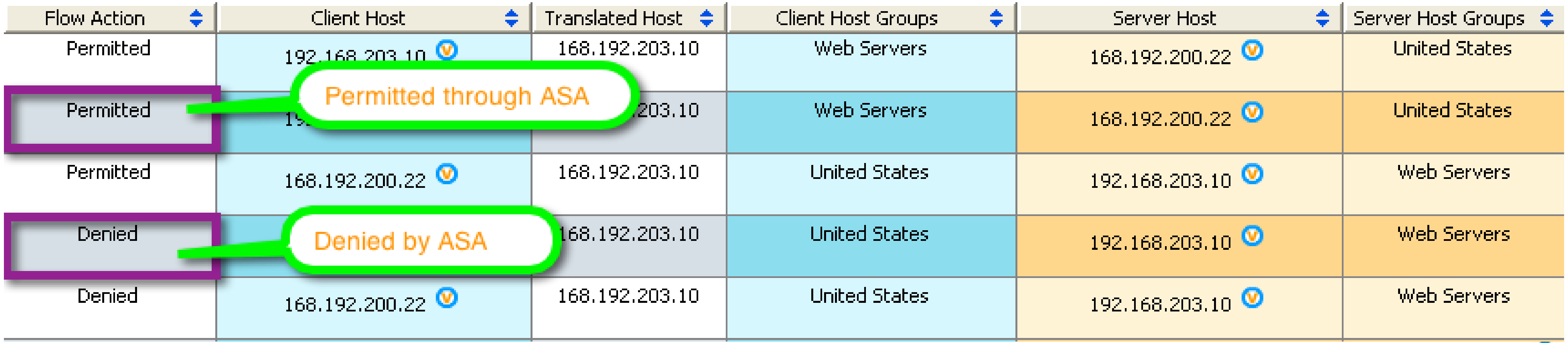


	Policy	Start Active Time	Alarm	Source	Source Host Groups	Source User ...	Source Devic...	Target	Details
	Desktops & Trusted Wireless	Jan 3, 2013 5:45:00 PM (20 hours 33 minutes 30s ago)	Suspect Data Loss	10.10.101.89	Atlanta, Desktops	ud0158	Windows7-Workstation	Multiple Hosts	Observed 5.33G bytes. Policy maximum allows up to 500M bytes.
	Desktops & Trusted Wireless	Jan 3, 2013 5:30:00 PM (20 hours 48 minutes 30s ago)	Suspect Data Loss	10.50.100.64	Desktops, New York, New York	ud0142	Apple-iPad	Multiple Hosts	Observed 515.84M bytes. Policy maximum allows up to 500M bytes.
	Desktops & Trusted Wireless	Jan 3, 2013 5:25:00 PM (20 hours 53 minutes 30s ago)	Suspect Data Loss	10.10.101.89	Atlanta, Desktops	ud0158	Windows7-Workstation	Multiple Hosts	Observed 4.82G bytes. Policy maximum allows up to 500M bytes.
	Desktops &	Jan 3, 2013 5:10:00 PM	Suspect Data	10.50.100.64	Desktops, New York, New	ud0142	Apple-iPad	Multiple Hosts	Observed 502.72M bytes.
	Desktops & Trusted Wireless	Jan 3, 2013 4:35:00 PM (21 hours 43 minutes 30s ago)	Suspect Data Loss	10.10.101.5	Atlanta, Desktops	uc0148	VMWare-Device	Multiple Hosts	Observed 740.03M bytes. Policy maximum allows up to 500M bytes.

Policy	Start Active Time	Alarm	Source	Source Host Groups	Source User Name	Device Type	Target
Desktops & Trusted Wireless	Jan 3, 2013	Suspect Data Loss	10.10.101.89	Atlanta, Desktops	John Chambers	Apple-iPad	Multiple Hosts

Obtaining Context Through NSEL

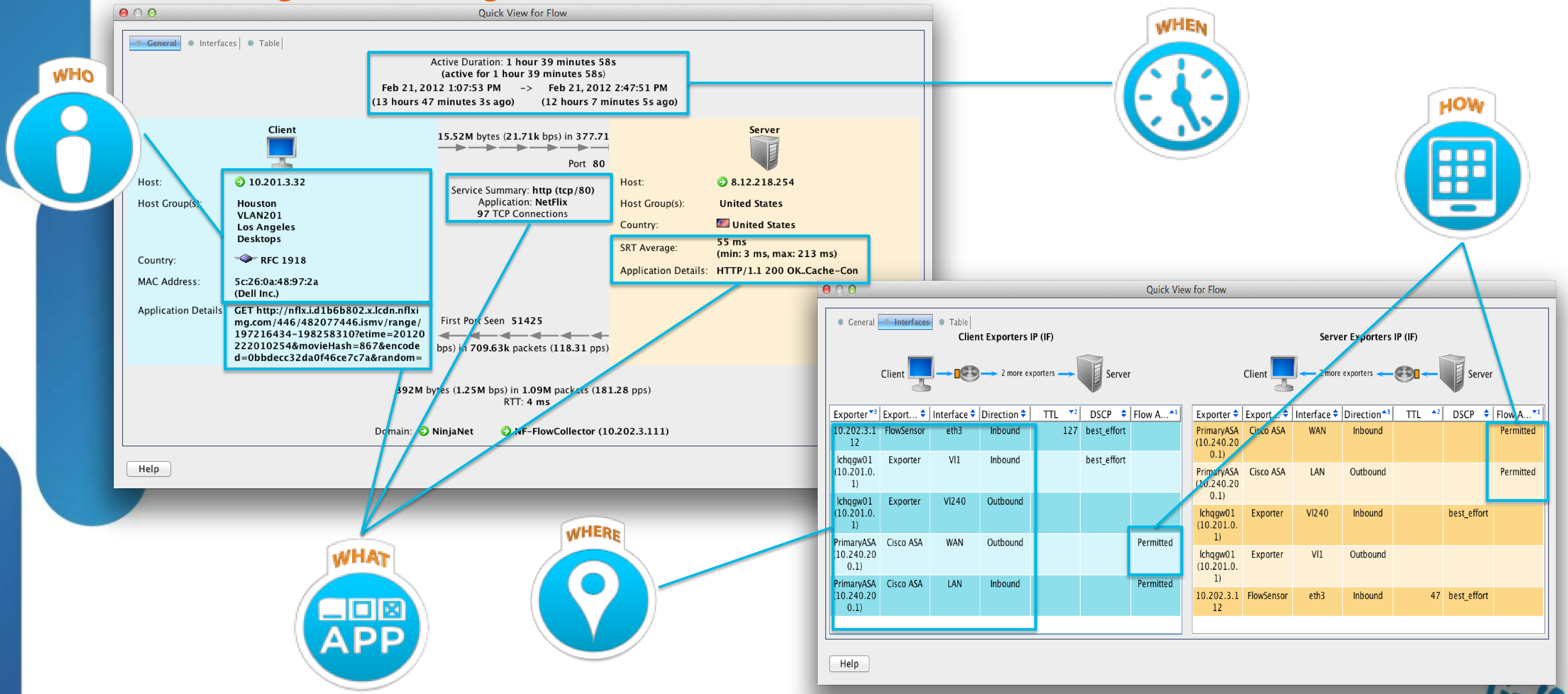
- Flow Action field can provide additional context
- State-based NSEL reporting is taken into consideration in StealthWatch's behavioural analysis
  - Concern Index points accumulated for Flow Denied events
- NAT stitching



Flow Action	Client Host	Translated Host	Client Host Groups	Server Host	Server Host Groups
Permitted	192.168.203.10	168.192.203.10	Web Servers	168.192.200.22	United States
Permitted	19[illegible]	[illegible]203.10	Web Servers	168.192.200.22	United States
Permitted	168.192.200.22	168.192.203.10	United States	192.168.203.10	Web Servers
Denied	[illegible]	168.192.203.10	United States	192.168.203.10	Web Servers
Denied	168.192.200.22	168.192.203.10	United States	192.168.203.10	Web Servers

Providing Scalable Visibility

Drilling into a Single Flow Yields a Wealth of Information



Active Duration: 1 hour 39 minutes 58s
(active for 1 hour 39 minutes 58s)
Feb 21, 2012 1:07:53 PM -> Feb 21, 2012 2:47:51 PM
(13 hours 47 minutes 3s ago) (12 hours 7 minutes 5s ago)

15.52M bytes (21.71k bps) in 377.71

Port 80

Host: 10.201.3.32

Host Group(s): Houston
VLAN201
Los Angeles
Desktops

Country: RFC 1918

MAC Address: 5c:26:0a:48:97:2a
(Dell Inc.)

Application Details GET http://nflx.i.d1b6b802.x.lcdn.nflximg.com/446/482077446.ismv/range/197216434-198258310?etime=20120222010254&movieHash=867&encoded=0bbdecc32da0f46ce7c7a&random=

Service Summary: http (tcp/80)
Application: NetFlix
97 TCP Connections

First Port Seen 51425

bps) in 709.63k packets (118.31 pps)

Host: 8.12.218.254

Host Group(s): United States

Country: United States

SRT Average: 55 ms
(min: 3 ms, max: 213 ms)

Application Details: HTTP/1.1 200 OK..Cache-Con

392M bytes (1.25M bps) in 1.09M packets (181.28 pps)
RTT: 4 ms

Domain: NinjaNet NF-FlowCollector (10.202.3.111)

Client Exporters IP (IF)

Client → 2 more exporters → Server

Exporter	Export...	Interface	Direction	TTL	DSCP	Flow A...
10.202.3.112	FlowSensor	eth3	Inbound	127	best_effort	
lchqgw01 (10.201.0.1)	Exporter	Vl1	Inbound		best_effort	
lchqgw01 (10.201.0.1)	Exporter	Vl240	Outbound			
PrimaryASA (10.240.200.1)	Cisco ASA	WAN	Outbound			Permitted
PrimaryASA (10.240.200.1)	Cisco ASA	LAN	Inbound			Permitted

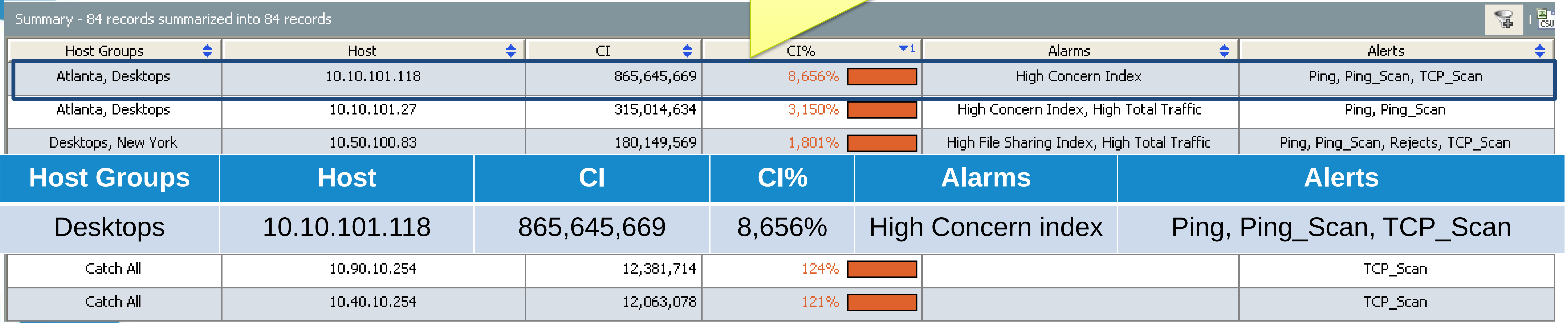
Server Exporters IP (IF)

Client ← 2 more exporters ← Server

Exporter	Export...	Interface	Direction	TTL	DSCP	Flow A...
PrimaryASA (10.240.200.1)	Cisco ASA	WAN	Inbound			Permitted
PrimaryASA (10.240.200.1)	Cisco ASA	LAN	Outbound			Permitted
lchqgw01 (10.201.0.1)	Exporter	Vl240	Inbound		best_effort	
lchqgw01 (10.201.0.1)	Exporter	Vl1	Outbound			
10.202.3.112	FlowSensor	eth3	Inbound	47	best_effort	

Attack Detection without Signatures

High Concern Index indicates a significant number of suspicious events that deviate from established baselines



Summary - 84 records summarized into 84 records

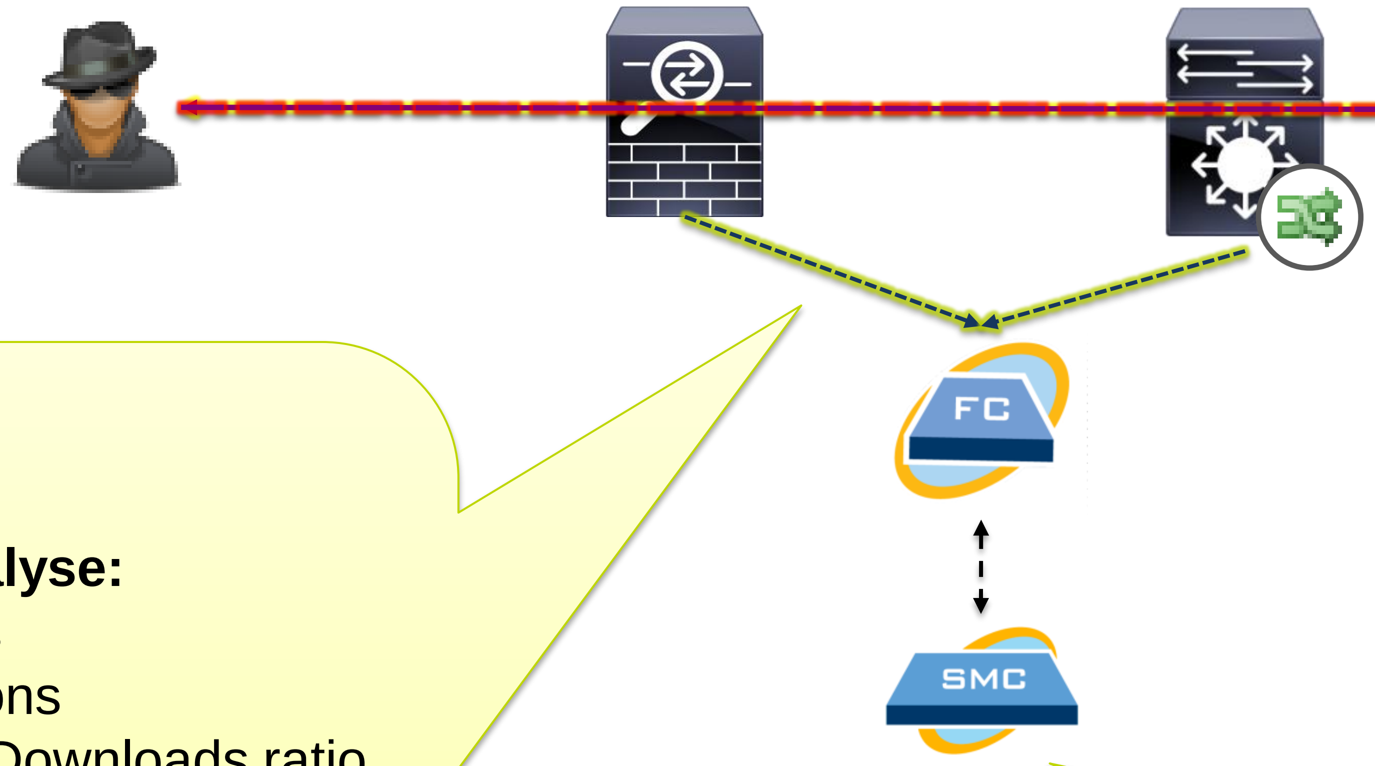
Host Groups	Host	CI	CI%	Alarms	Alerts
Atlanta, Desktops	10.10.101.118	865,645,669	8,656%	High Concern Index	Ping, Ping_Scan, TCP_Scan
Atlanta, Desktops	10.10.101.27	315,014,634	3,150%	High Concern Index, High Total Traffic	Ping, Ping_Scan
Desktops, New York	10.50.100.83	180,149,569	1,801%	High File Sharing Index, High Total Traffic	Ping, Ping_Scan, Rejects, TCP_Scan
Catch All	10.90.10.254	12,381,714	124%		TCP_Scan
Catch All	10.40.10.254	12,063,078	121%		TCP_Scan

Host Groups	Host	CI	CI%	Alarms	Alerts
Desktops	10.10.101.118	865,645,669	8,656%	High Concern index	Ping, Ping_Scan, TCP_Scan

Monitor and baseline activity for a host and within host groups.

Working with NetFlow

Detecting Command and Control



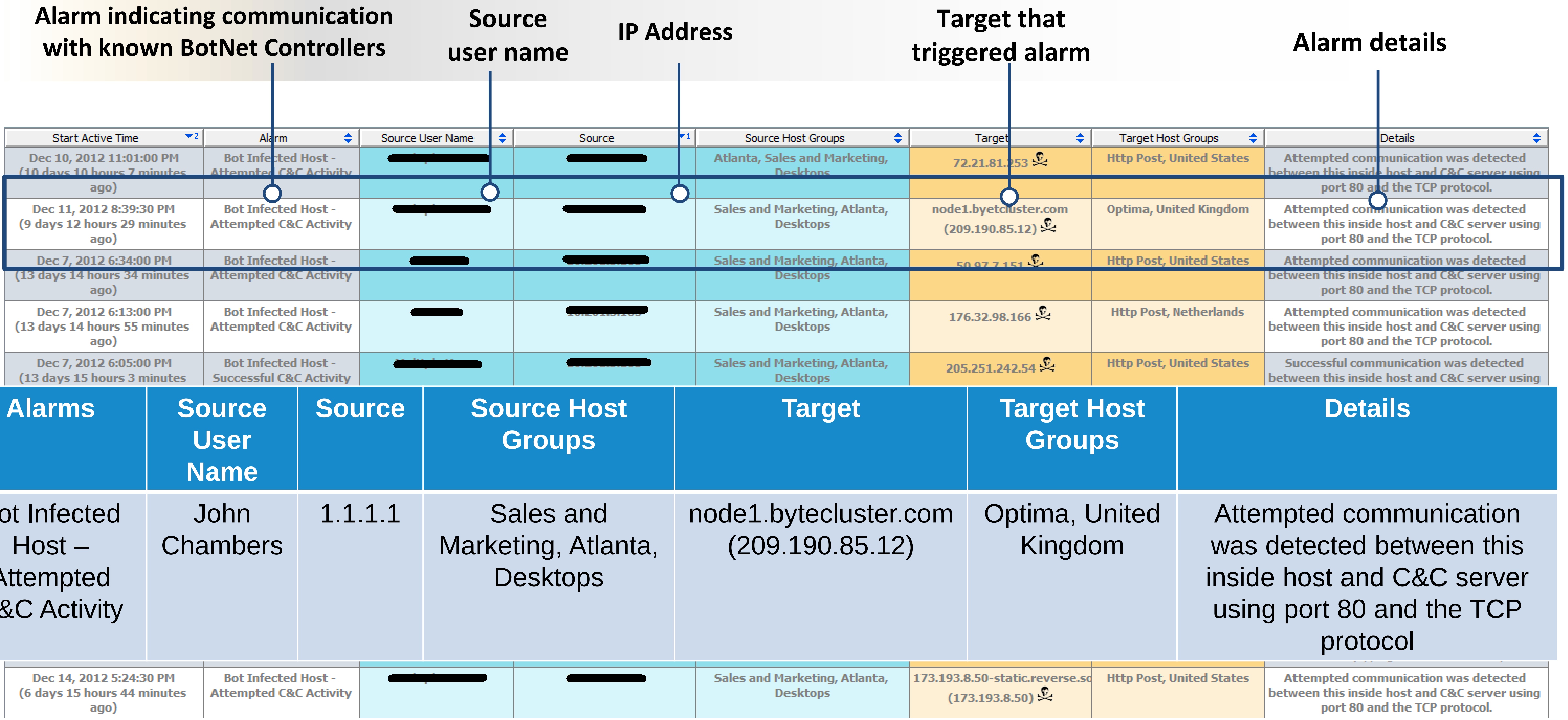
Periodic “phone home” activity

What to analyse:

- Countries
- Applications
- Uploads/Downloads ratio
- Time of day
- Repeated connections
- Beaconing - Repeated dead connections
- Long lived flows
- Known C&C servers

StealthWatch Method of Detection:
Host Lock Violation
Suspect Long Flow
Beaconing Host
SLIC Reputation Feed

Detecting Command and Control



Alarm indicating communication with known BotNet Controllers

Source user name

IP Address

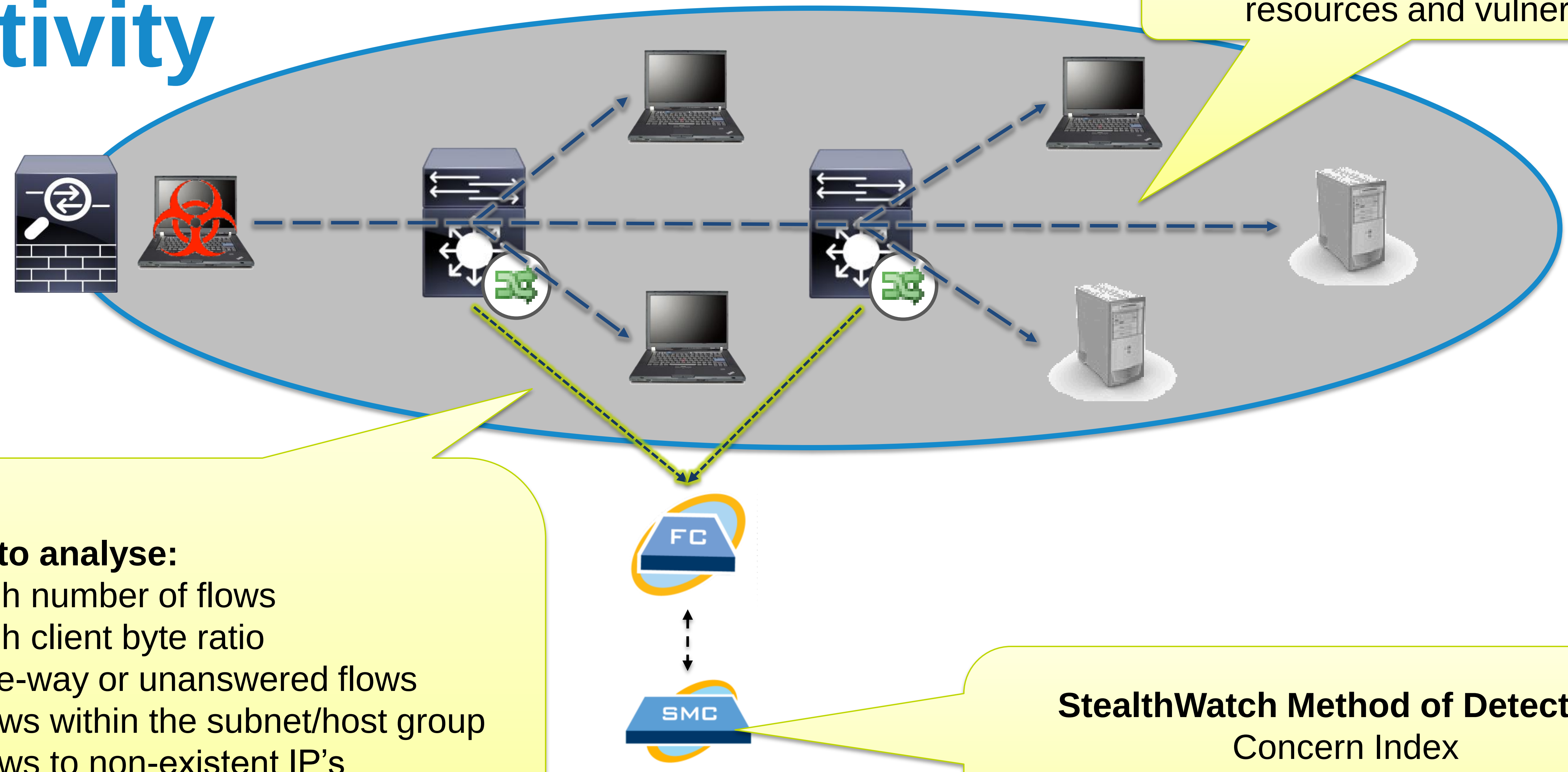
Target that triggered alarm

Alarm details

Start Active Time	Alarm	Source User Name	Source	Source Host Groups	Target	Target Host Groups	Details
Dec 10, 2012 11:01:00 PM (10 days 10 hours 7 minutes ago)	Bot Infected Host - Attempted C&C Activity	[redacted]	[redacted]	Atlanta, Sales and Marketing, Desktops	72.21.81.253 ☠	Http Post, United States	Attempted communication was detected between this inside host and C&C server using port 80 and the TCP protocol.
Dec 11, 2012 8:39:30 PM (9 days 12 hours 29 minutes ago)	Bot Infected Host - Attempted C&C Activity	[redacted]	[redacted]	Sales and Marketing, Atlanta, Desktops	node1.byetcluster.com (209.190.85.12) ☠	Optima, United Kingdom	Attempted communication was detected between this inside host and C&C server using port 80 and the TCP protocol.
Dec 7, 2012 6:34:00 PM (13 days 14 hours 34 minutes ago)	Bot Infected Host - Attempted C&C Activity	[redacted]	[redacted]	Sales and Marketing, Atlanta, Desktops	50.97.7.151 ☠	Http Post, United States	Attempted communication was detected between this inside host and C&C server using port 80 and the TCP protocol.
Dec 7, 2012 6:13:00 PM (13 days 14 hours 55 minutes ago)	Bot Infected Host - Attempted C&C Activity	[redacted]	[redacted]	Sales and Marketing, Atlanta, Desktops	176.32.98.166 ☠	Http Post, Netherlands	Attempted communication was detected between this inside host and C&C server using port 80 and the TCP protocol.
Dec 7, 2012 6:05:00 PM (13 days 15 hours 3 minutes	Bot Infected Host - Successful C&C Activity	[redacted]	[redacted]	Sales and Marketing, Atlanta, Desktops	205.251.242.54 ☠	Http Post, United States	Successful communication was detected between this inside host and C&C server using
Dec 14, 2012 5:24:30 PM (6 days 15 hours 44 minutes ago)	Bot Infected Host - Attempted C&C Activity	[redacted]	[redacted]	Sales and Marketing, Atlanta, Desktops	173.193.8.50-static.reverse.sc (173.193.8.50) ☠	Http Post, United States	Attempted communication was detected between this inside host and C&C server using port 80 and the TCP protocol.

Start Active Time	Alarms	Source User Name	Source	Source Host Groups	Target	Target Host Groups	Details
Dec 11, 2012	Bot Infected Host – Attempted C&C Activity	John Chambers	1.1.1.1	Sales and Marketing, Atlanta, Desktops	node1.bytecluster.com (209.190.85.12)	Optima, United Kingdom	Attempted communication was detected between this inside host and C&C server using port 80 and the TCP protocol

Identifying Reconnaissance Activity



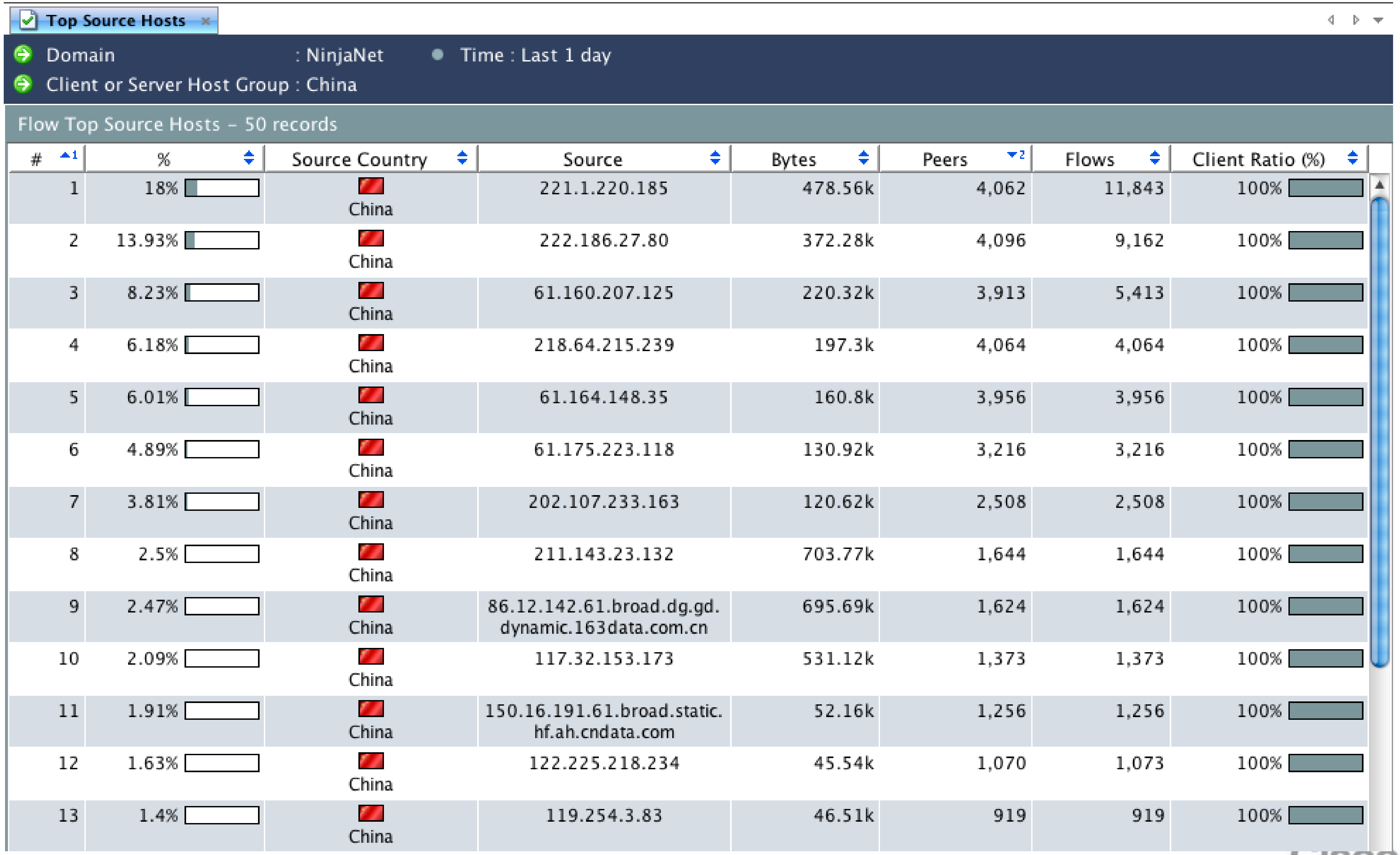
Long and slow activity to discover resources and vulnerabilities

What to analyse:

- High number of flows
- High client byte ratio
- One-way or unanswered flows
- Flows within the subnet/host group
- Flows to non-existent IP’s
- Flow patterns
- Abnormal behaviour

StealthWatch Method of Detection:
Concern Index
High Traffic
High Connections
Trapped Hosts

Identifying Reconnaissance Activity



Top Source Hosts

Domain : NinjaNet ● Time : Last 1 day

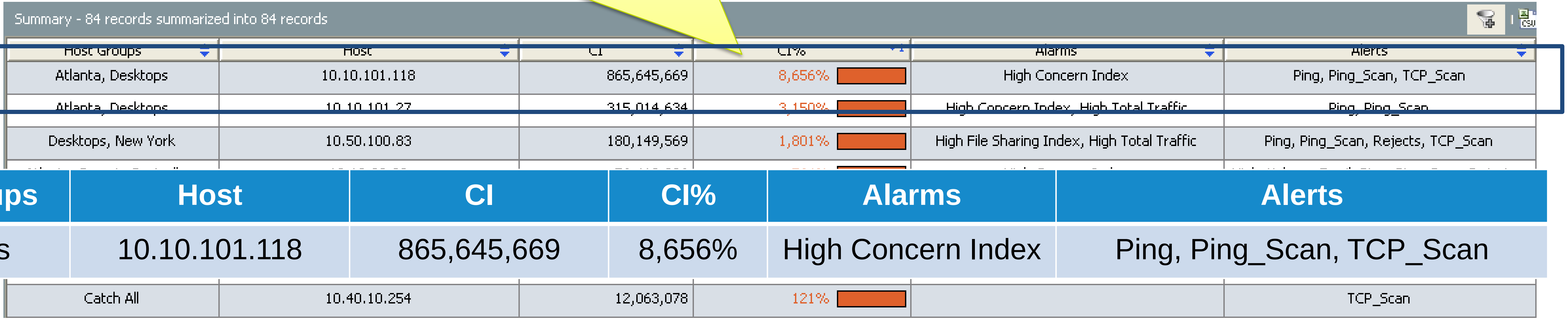
Client or Server Host Group : China

Flow Top Source Hosts – 50 records

#	%	Source Country	Source	Bytes	Peers	Flows	Client Ratio (%)
1	18%	China	221.1.220.185	478.56k	4,062	11,843	100%
2	13.93%	China	222.186.27.80	372.28k	4,096	9,162	100%
3	8.23%	China	61.160.207.125	220.32k	3,913	5,413	100%
4	6.18%	China	218.64.215.239	197.3k	4,064	4,064	100%
5	6.01%	China	61.164.148.35	160.8k	3,956	3,956	100%
6	4.89%	China	61.175.223.118	130.92k	3,216	3,216	100%
7	3.81%	China	202.107.233.163	120.62k	2,508	2,508	100%
8	2.5%	China	211.143.23.132	703.77k	1,644	1,644	100%
9	2.47%	China	86.12.142.61.broad.dg.gd.dynamic.163data.com.cn	695.69k	1,624	1,624	100%
10	2.09%	China	117.32.153.173	531.12k	1,373	1,373	100%
11	1.91%	China	150.16.191.61.broad.static.hf.ah.cndata.com	52.16k	1,256	1,256	100%
12	1.63%	China	122.225.218.234	45.54k	1,070	1,073	100%
13	1.4%	China	119.254.3.83	46.51k	919	919	100%

Identifying Reconnaissance Activity

High Concern Index indicates a significant number of suspicious events that deviate from established baselines

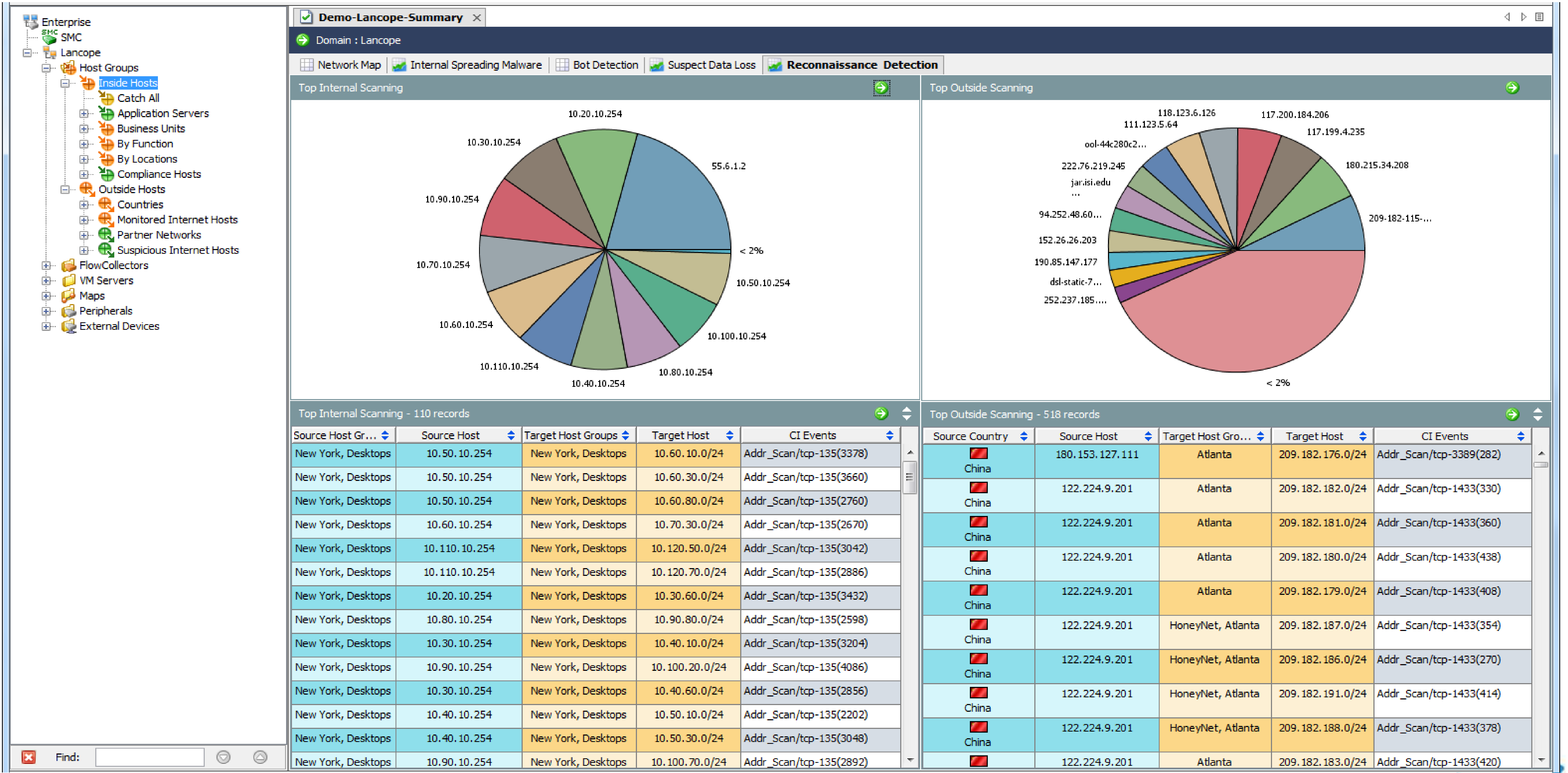


Summary - 84 records summarized into 84 records

Host Groups	Host	CI	CI%	Alarms	Alerts
Atlanta, Desktops	10.10.101.118	865,645,669	8,656%	High Concern Index	Ping, Ping_Scan, TCP_Scan
Atlanta, Desktops	10.10.101.27	315,014,634	3,150%	High Concern Index, High Total Traffic	Ping, Ping_Scan
Desktops, New York	10.50.100.83	180,149,569	1,801%	High File Sharing Index, High Total Traffic	Ping, Ping_Scan, Rejects, TCP_Scan
Catch All	10.40.10.254	12,063,078	121%		TCP_Scan

Host Groups	Host	CI	CI%	Alarms	Alerts
Desktops	10.10.101.118	865,645,669	8,656%	High Concern Index	Ping, Ping_Scan, TCP_Scan

Identifying Reconnaissance Activity



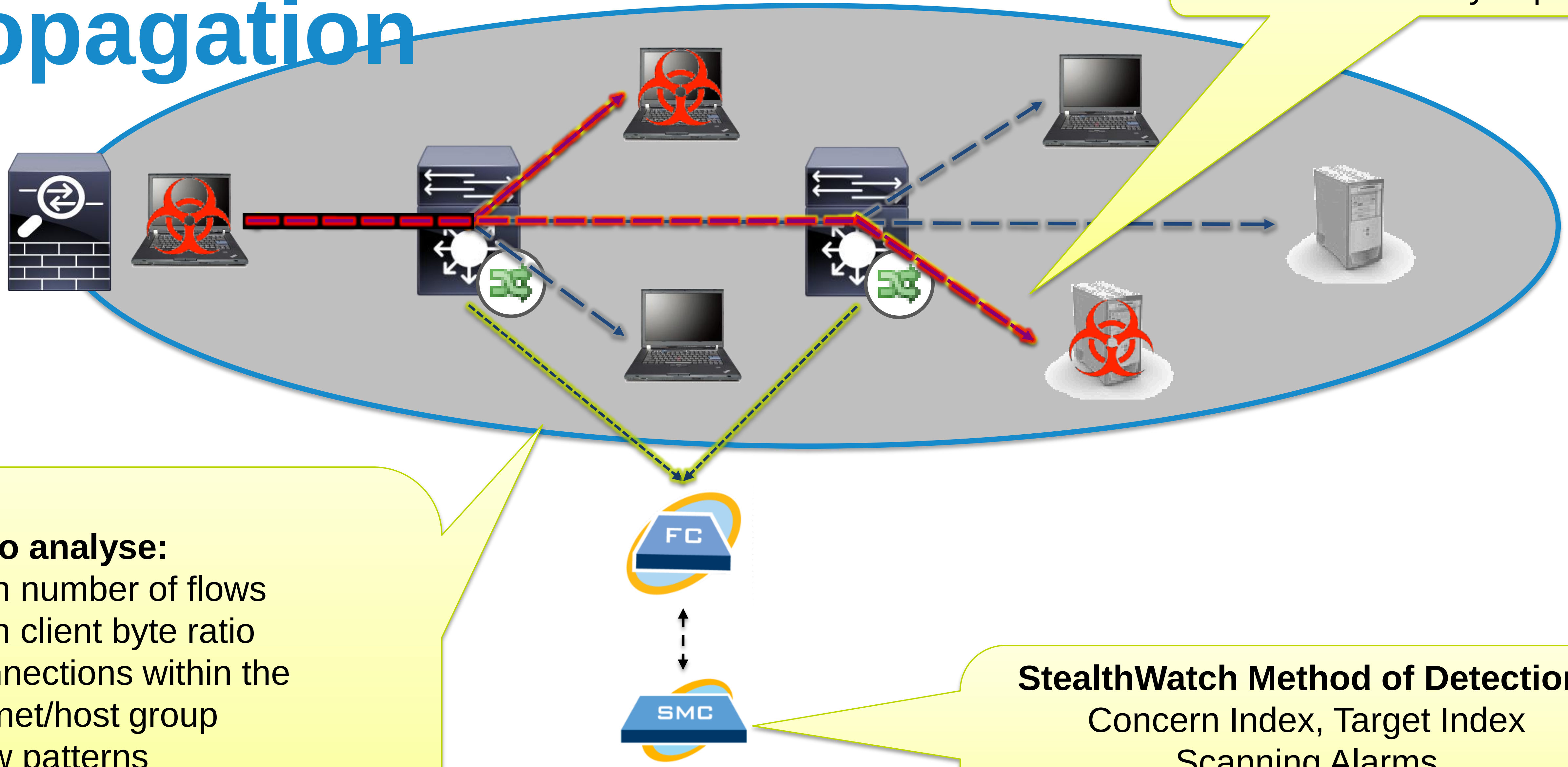
Top Internal Scanning - 110 records

Source Host Gr...	Source Host	Target Host Groups	Target Host	CI Events
New York, Desktops	10.50.10.254	New York, Desktops	10.60.10.0/24	Addr_Scan/tcp-135(3378)
New York, Desktops	10.50.10.254	New York, Desktops	10.60.30.0/24	Addr_Scan/tcp-135(3660)
New York, Desktops	10.50.10.254	New York, Desktops	10.60.80.0/24	Addr_Scan/tcp-135(2760)
New York, Desktops	10.60.10.254	New York, Desktops	10.70.30.0/24	Addr_Scan/tcp-135(2670)
New York, Desktops	10.110.10.254	New York, Desktops	10.120.50.0/24	Addr_Scan/tcp-135(3042)
New York, Desktops	10.110.10.254	New York, Desktops	10.120.70.0/24	Addr_Scan/tcp-135(2886)
New York, Desktops	10.20.10.254	New York, Desktops	10.30.60.0/24	Addr_Scan/tcp-135(3432)
New York, Desktops	10.80.10.254	New York, Desktops	10.90.80.0/24	Addr_Scan/tcp-135(2598)
New York, Desktops	10.30.10.254	New York, Desktops	10.40.10.0/24	Addr_Scan/tcp-135(3204)
New York, Desktops	10.90.10.254	New York, Desktops	10.100.20.0/24	Addr_Scan/tcp-135(4086)
New York, Desktops	10.30.10.254	New York, Desktops	10.40.60.0/24	Addr_Scan/tcp-135(2856)
New York, Desktops	10.40.10.254	New York, Desktops	10.50.10.0/24	Addr_Scan/tcp-135(2202)
New York, Desktops	10.40.10.254	New York, Desktops	10.50.30.0/24	Addr_Scan/tcp-135(3048)
New York, Desktops	10.90.10.254	New York, Desktops	10.100.70.0/24	Addr_Scan/tcp-135(2892)

Top Outside Scanning - 518 records

Source Country	Source Host	Target Host Gro...	Target Host	CI Events
🟥 China	180.153.127.111	Atlanta	209.182.176.0/24	Addr_Scan/tcp-3389(282)
🟥 China	122.224.9.201	Atlanta	209.182.182.0/24	Addr_Scan/tcp-1433(330)
🟥 China	122.224.9.201	Atlanta	209.182.181.0/24	Addr_Scan/tcp-1433(360)
🟥 China	122.224.9.201	Atlanta	209.182.180.0/24	Addr_Scan/tcp-1433(438)
🟥 China	122.224.9.201	Atlanta	209.182.179.0/24	Addr_Scan/tcp-1433(408)
🟥 China	122.224.9.201	HoneyNet, Atlanta	209.182.187.0/24	Addr_Scan/tcp-1433(354)
🟥 China	122.224.9.201	HoneyNet, Atlanta	209.182.186.0/24	Addr_Scan/tcp-1433(270)
🟥 China	122.224.9.201	HoneyNet, Atlanta	209.182.191.0/24	Addr_Scan/tcp-1433(414)
🟥 China	122.224.9.201	HoneyNet, Atlanta	209.182.188.0/24	Addr_Scan/tcp-1433(378)
🟥	122.224.9.201	Atlanta	209.182.183.0/24	Addr_Scan/tcp-1433(420)

Identifying Malware Propagation



Discovered host answers and vulnerability exploited

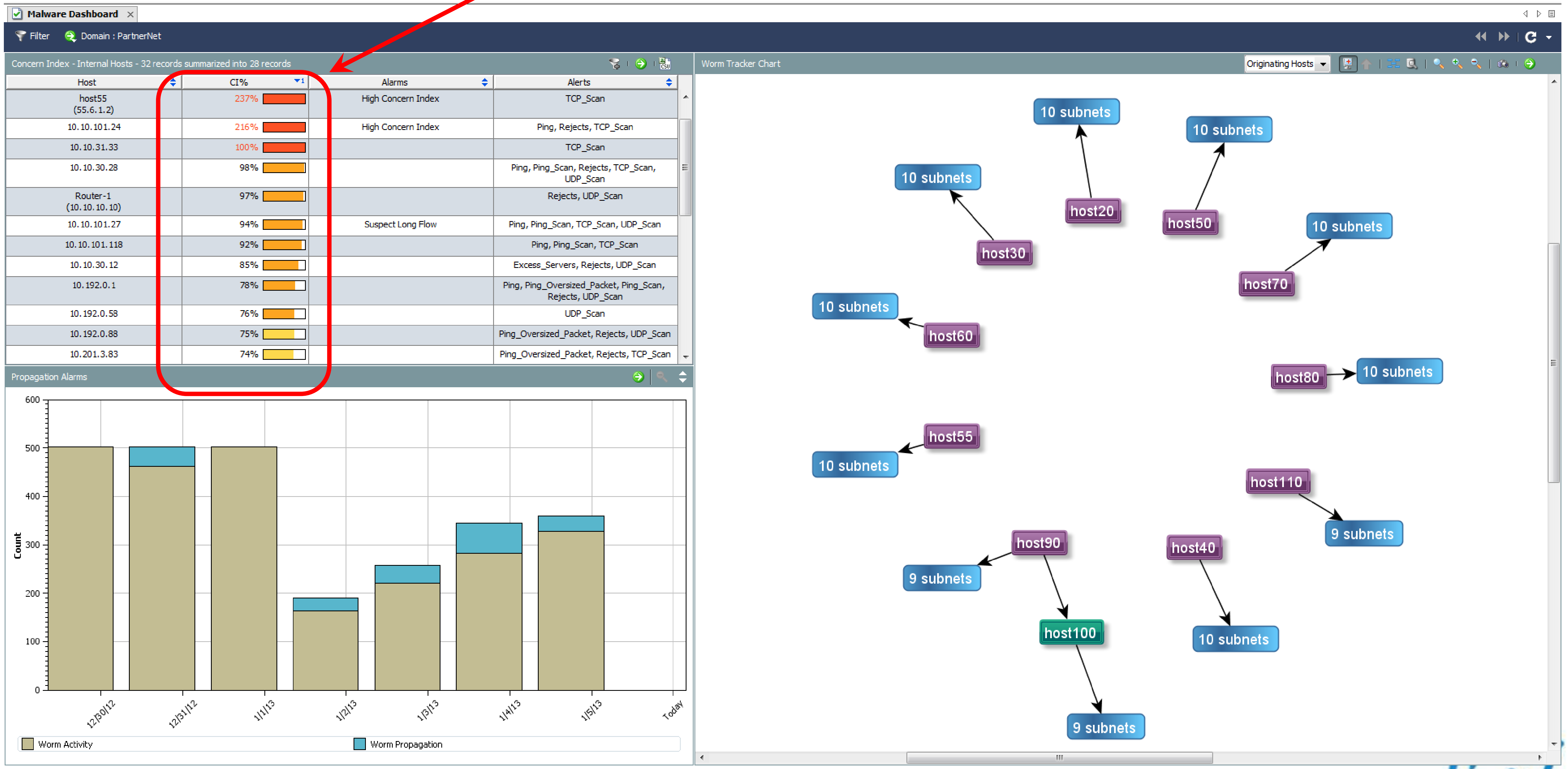
What to analyse:

- High number of flows
- High client byte ratio
- Connections within the subnet/host group
- Flow patterns
- Abnormal behaviour

StealthWatch Method of Detection:
Concern Index, Target Index
Scanning Alarms
Touched Host
Worm Propagation Alarm
Worm Tracker

Detecting Internally Spreading Malware

Prioritised Threats



Malware Dashboard

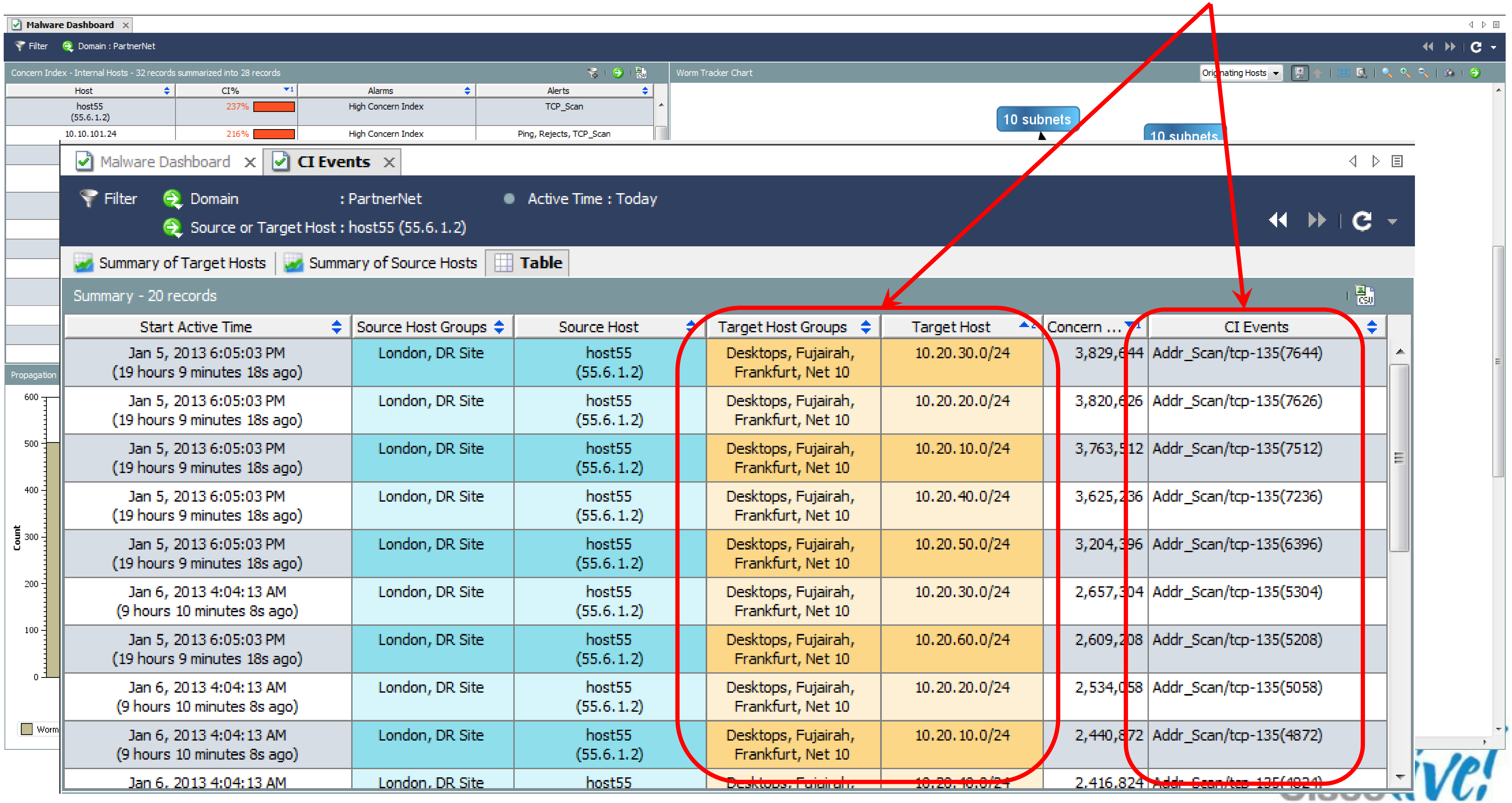
Filter · Domain : PartnerNet

Concern Index - Internal Hosts - 32 records summarized into 28 records

Host	CI%	Alarms	Alerts
host55 (55.6.1.2)	237%	High Concern Index	TCP_Scan
10.10.101.24	216%	High Concern Index	Ping, Rejects, TCP_Scan
10.10.31.33	100%		TCP_Scan
10.10.30.28	98%		Ping, Ping_Scan, Rejects, TCP_Scan, UDP_Scan
Router-1 (10.10.10.10)	97%		Rejects, UDP_Scan
10.10.101.27	94%	Suspect Long Flow	Ping, Ping_Scan, TCP_Scan, UDP_Scan
10.10.101.118	92%		Ping, Ping_Scan, TCP_Scan
10.10.30.12	85%		Excess_Servers, Rejects, UDP_Scan
10.192.0.1	78%		Ping, Ping_Oversized_Packet, Ping_Scan, Rejects, UDP_Scan
10.192.0.58	76%		UDP_Scan
10.192.0.88	75%		Ping_Oversized_Packet, Rejects, UDP_Scan
10.201.3.83	74%		Ping_Oversized_Packet, Rejects, TCP_Scan

Detecting Internally Spreading Malware

Targeted resources and behaviour



Concern Index - Internal Hosts - 32 records summarized into 28 records

Host	CI%	Alarms	Alerts
host55 (55.6.1.2)	237%	High Concern Index	TCP_Scan
10.10.101.24	216%	High Concern Index	Ping, Rejects, TCP_Scan

Filter Domain : PartnerNet Active Time : Today

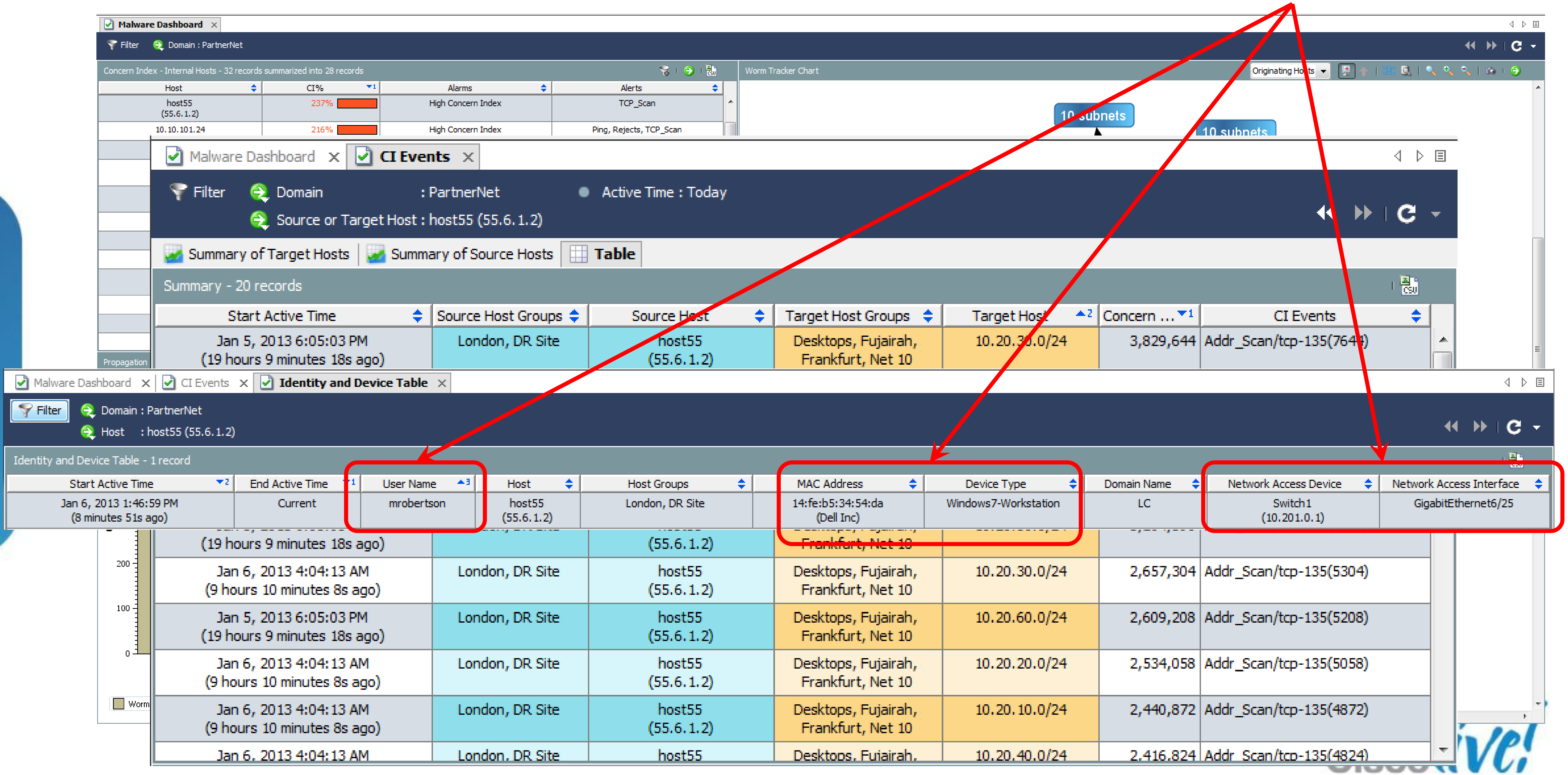
Source or Target Host : host55 (55.6.1.2)

Summary - 20 records

Start Active Time	Source Host Groups	Source Host	Target Host Groups	Target Host	Concern ...	CI Events
Jan 5, 2013 6:05:03 PM (19 hours 9 minutes 18s ago)	London, DR Site	host55 (55.6.1.2)	Desktops, Fujairah, Frankfurt, Net 10	10.20.30.0/24	3,829,644	Addr_Scan/tcp-135(7644)
Jan 5, 2013 6:05:03 PM (19 hours 9 minutes 18s ago)	London, DR Site	host55 (55.6.1.2)	Desktops, Fujairah, Frankfurt, Net 10	10.20.20.0/24	3,820,626	Addr_Scan/tcp-135(7626)
Jan 5, 2013 6:05:03 PM (19 hours 9 minutes 18s ago)	London, DR Site	host55 (55.6.1.2)	Desktops, Fujairah, Frankfurt, Net 10	10.20.10.0/24	3,763,512	Addr_Scan/tcp-135(7512)
Jan 5, 2013 6:05:03 PM (19 hours 9 minutes 18s ago)	London, DR Site	host55 (55.6.1.2)	Desktops, Fujairah, Frankfurt, Net 10	10.20.40.0/24	3,625,236	Addr_Scan/tcp-135(7236)
Jan 5, 2013 6:05:03 PM (19 hours 9 minutes 18s ago)	London, DR Site	host55 (55.6.1.2)	Desktops, Fujairah, Frankfurt, Net 10	10.20.50.0/24	3,204,396	Addr_Scan/tcp-135(6396)
Jan 6, 2013 4:04:13 AM (9 hours 10 minutes 8s ago)	London, DR Site	host55 (55.6.1.2)	Desktops, Fujairah, Frankfurt, Net 10	10.20.30.0/24	2,657,304	Addr_Scan/tcp-135(5304)
Jan 5, 2013 6:05:03 PM (19 hours 9 minutes 18s ago)	London, DR Site	host55 (55.6.1.2)	Desktops, Fujairah, Frankfurt, Net 10	10.20.60.0/24	2,609,208	Addr_Scan/tcp-135(5208)
Jan 6, 2013 4:04:13 AM (9 hours 10 minutes 8s ago)	London, DR Site	host55 (55.6.1.2)	Desktops, Fujairah, Frankfurt, Net 10	10.20.20.0/24	2,534,058	Addr_Scan/tcp-135(5058)
Jan 6, 2013 4:04:13 AM (9 hours 10 minutes 8s ago)	London, DR Site	host55 (55.6.1.2)	Desktops, Fujairah, Frankfurt, Net 10	10.20.10.0/24	2,440,872	Addr_Scan/tcp-135(4872)
Jan 6, 2013 4:04:13 AM	London, DR Site	host55	Desktops, Fujairah,	[illegible]	2,416,824	[illegible]

Detecting Internally Spreading Malware

Source user, asset and connection point



Filter Domain : PartnerNet

Concern Index - Internal Hosts - 32 records summarized into 28 records

Host	CI%	Alarms	Alerts
host55 (55.6.1.2)	237%	High Concern Index	TCP_Scan
10.10.101.24	216%	High Concern Index	Ping, Rejects, TCP_Scan

Filter Domain : PartnerNet Active Time : Today

Source or Target Host : host55 (55.6.1.2)

Summary of Target Hosts | Summary of Source Hosts | Table

Summary - 20 records

Start Active Time	Source Host Groups	Source Host	Target Host Groups	Target Host	Concern ...	CI Events
Jan 5, 2013 6:05:03 PM (19 hours 9 minutes 18s ago)	London, DR Site	host55 (55.6.1.2)	Desktops, Fujairah, Frankfurt, Net 10	10.20.30.0/24	3,829,644	Addr_Scan/tcp-135(7644)
(19 hours 9 minutes 18s ago)		(55.6.1.2)	Frankfurt, Net 10			
Jan 6, 2013 4:04:13 AM (9 hours 10 minutes 8s ago)	London, DR Site	host55 (55.6.1.2)	Desktops, Fujairah, Frankfurt, Net 10	10.20.30.0/24	2,657,304	Addr_Scan/tcp-135(5304)
Jan 5, 2013 6:05:03 PM (19 hours 9 minutes 18s ago)	London, DR Site	host55 (55.6.1.2)	Desktops, Fujairah, Frankfurt, Net 10	10.20.60.0/24	2,609,208	Addr_Scan/tcp-135(5208)
Jan 6, 2013 4:04:13 AM (9 hours 10 minutes 8s ago)	London, DR Site	host55 (55.6.1.2)	Desktops, Fujairah, Frankfurt, Net 10	10.20.20.0/24	2,534,058	Addr_Scan/tcp-135(5058)
Jan 6, 2013 4:04:13 AM (9 hours 10 minutes 8s ago)	London, DR Site	host55 (55.6.1.2)	Desktops, Fujairah, Frankfurt, Net 10	10.20.10.0/24	2,440,872	Addr_Scan/tcp-135(4872)
Jan 6, 2013 4:04:13 AM	London, DR Site	host55	Desktops, Fujairah,	10.20.40.0/24	2,416,824	Addr_Scan/tcp-135(4824)

Filter Domain : PartnerNet

Host : host55 (55.6.1.2)

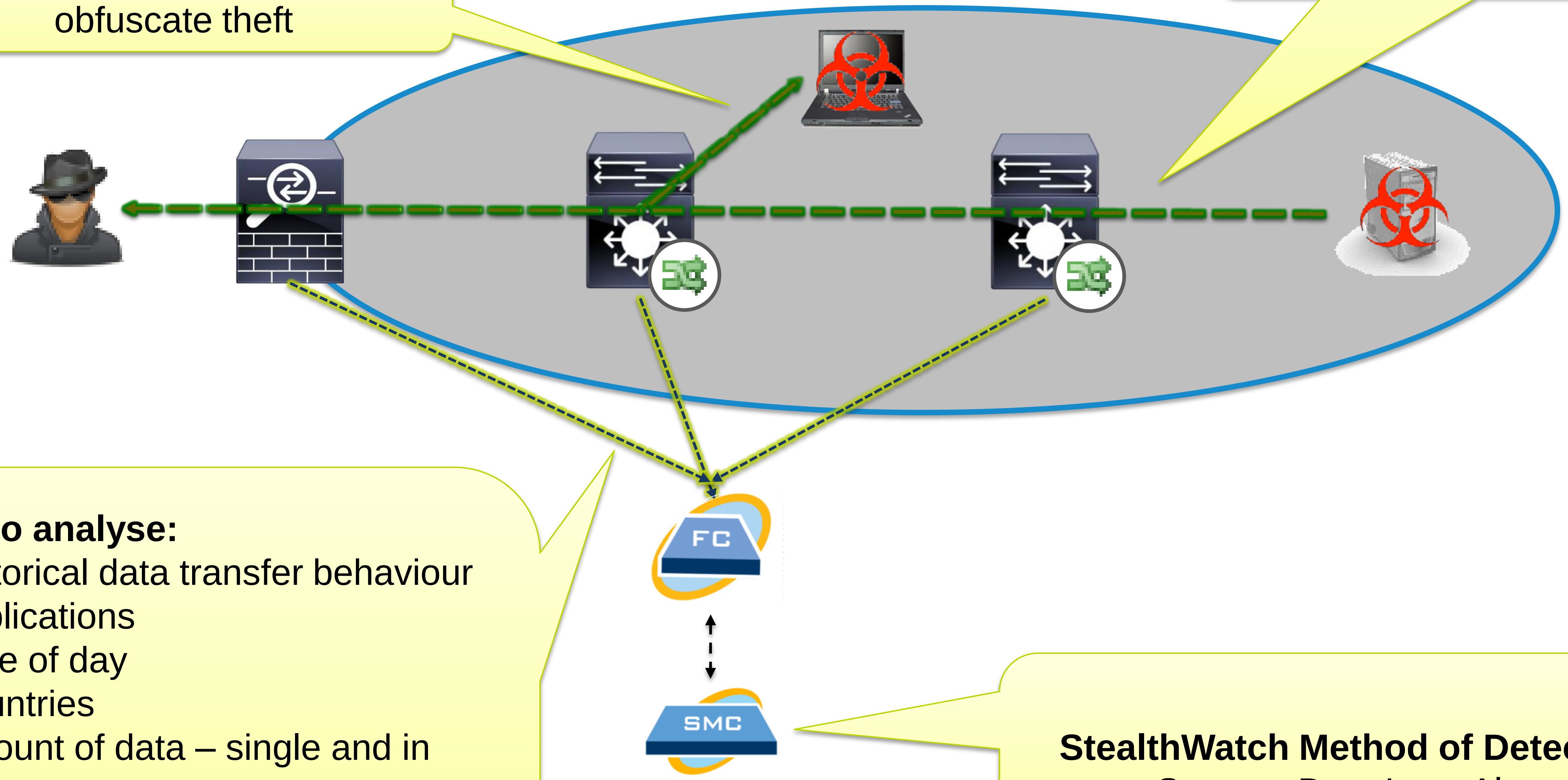
Identity and Device Table - 1 record

Start Active Time	End Active Time	User Name	Host	Host Groups		MAC Address	Device Type	Domain Name	Network Access Device	Network Access Interface
Jan 6, 2013 1:46:59 PM (8 minutes 51s ago)	Current	mrobertson	host55 (55.6.1.2)	London, DR Site		14:fe:b5:34:54:da (Dell Inc)	Windows7-Workstation	LC	Switch1 (10.201.0.1)	GigabitEthernet6/25

Detecting Data Loss

Intermediary resource used to obfuscate theft

Data is exported off resource

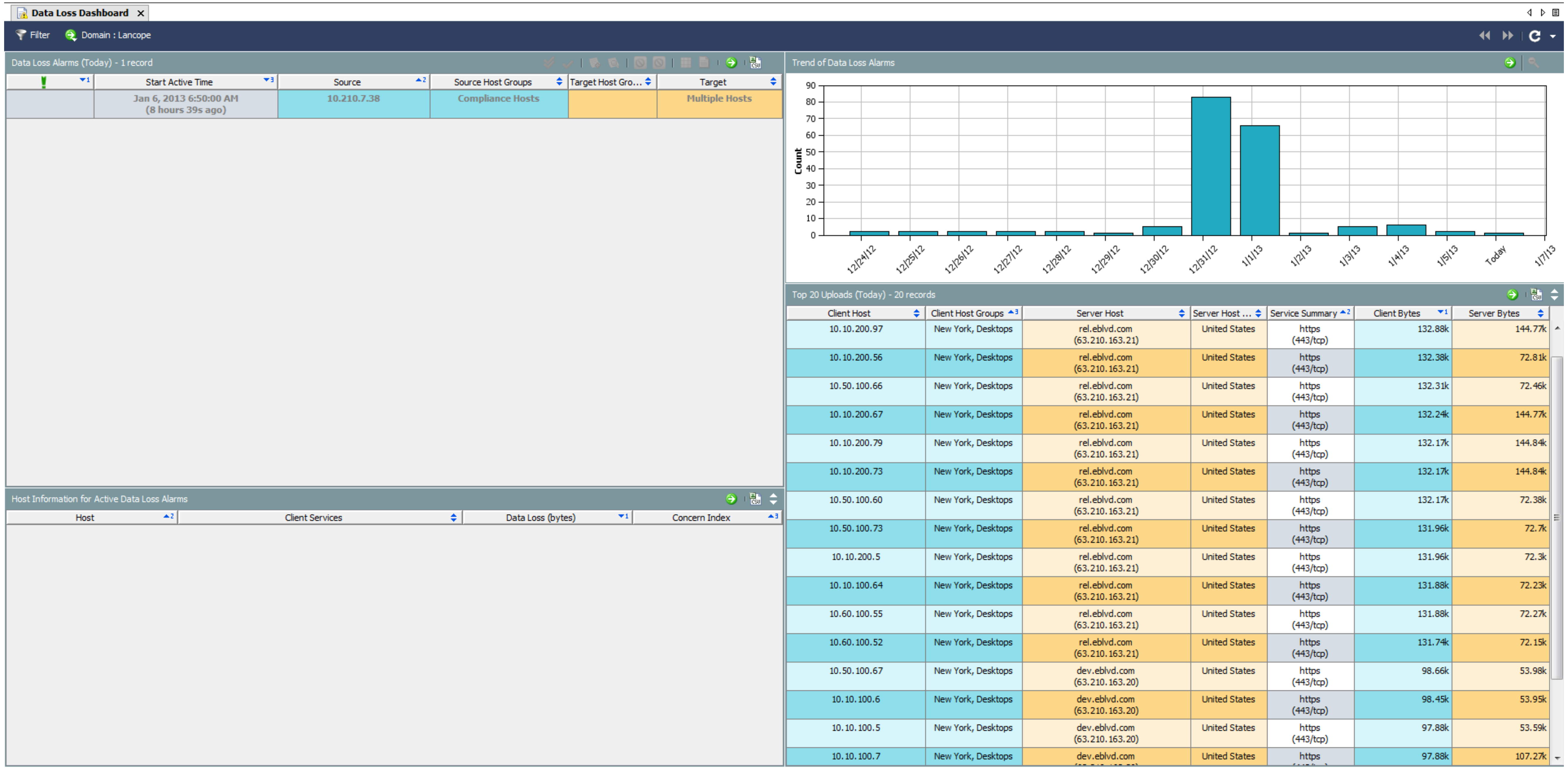


What to analyse:

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

StealthWatch Method of Detection:
Suspect Data Loss Alarm

Detecting Data Loss



Data Loss Alarms (Today) - 1 record

!	Start Active Time	Source	Source Host Groups	Target Host Gro...	Target
	Jan 6, 2013 6:50:00 AM (8 hours 39s ago)	10.210.7.38	Compliance Hosts		Multiple Hosts

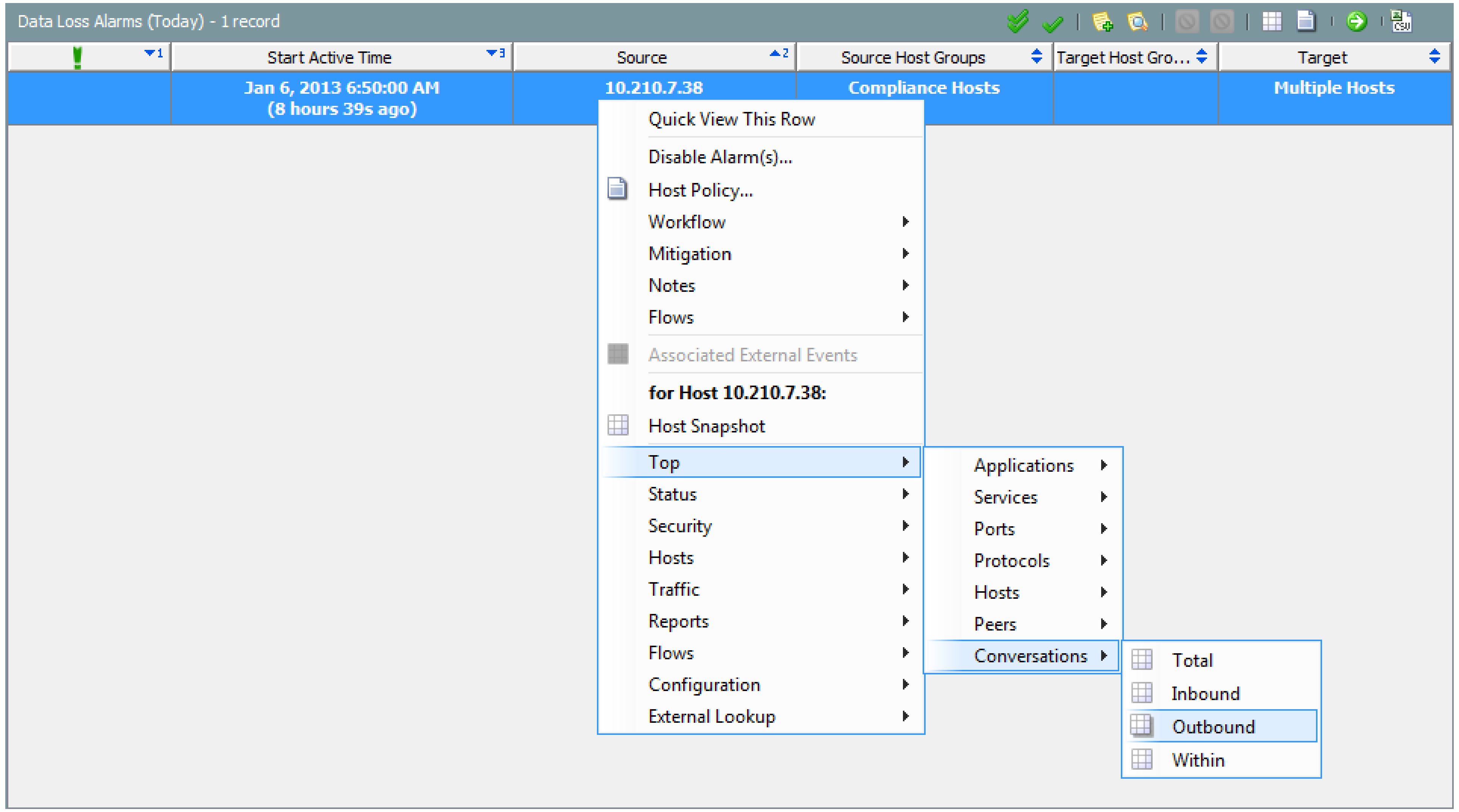
Host Information for Active Data Loss Alarms

Host	Client Services	Data Loss (bytes)	Concern Index

Top 20 Uploads (Today) - 20 records

Client Host	Client Host Groups	Server Host	Server Host ...	Service Summary	Client Bytes	Server Bytes
10.10.200.97	New York, Desktops	rel.eblvd.com (63.210.163.21)	United States	https (443/tcp)	132.88k	144.77k
10.10.200.56	New York, Desktops	rel.eblvd.com (63.210.163.21)	United States	https (443/tcp)	132.38k	72.81k
10.50.100.66	New York, Desktops	rel.eblvd.com (63.210.163.21)	United States	https (443/tcp)	132.31k	72.46k
10.10.200.67	New York, Desktops	rel.eblvd.com (63.210.163.21)	United States	https (443/tcp)	132.24k	144.77k
10.10.200.79	New York, Desktops	rel.eblvd.com (63.210.163.21)	United States	https (443/tcp)	132.17k	144.84k
10.10.200.73	New York, Desktops	rel.eblvd.com (63.210.163.21)	United States	https (443/tcp)	132.17k	144.84k
10.50.100.60	New York, Desktops	rel.eblvd.com (63.210.163.21)	United States	https (443/tcp)	132.17k	72.38k
10.50.100.73	New York, Desktops	rel.eblvd.com (63.210.163.21)	United States	https (443/tcp)	131.96k	72.7k
10.10.200.5	New York, Desktops	rel.eblvd.com (63.210.163.21)	United States	https (443/tcp)	131.96k	72.3k
10.10.100.64	New York, Desktops	rel.eblvd.com (63.210.163.21)	United States	https (443/tcp)	131.88k	72.23k
10.60.100.55	New York, Desktops	rel.eblvd.com (63.210.163.21)	United States	https (443/tcp)	131.88k	72.27k
10.60.100.52	New York, Desktops	rel.eblvd.com (63.210.163.21)	United States	https (443/tcp)	131.74k	72.15k
10.50.100.67	New York, Desktops	dev.eblvd.com (63.210.163.20)	United States	https (443/tcp)	98.66k	53.98k
10.10.100.6	New York, Desktops	dev.eblvd.com (63.210.163.20)	United States	https (443/tcp)	98.45k	53.95k
10.10.100.5	New York, Desktops	dev.eblvd.com (63.210.163.20)	United States	https (443/tcp)	97.88k	53.59k
10.10.100.7	New York, Desktops	dev.eblvd.com	United States	https	97.88k	107.27k

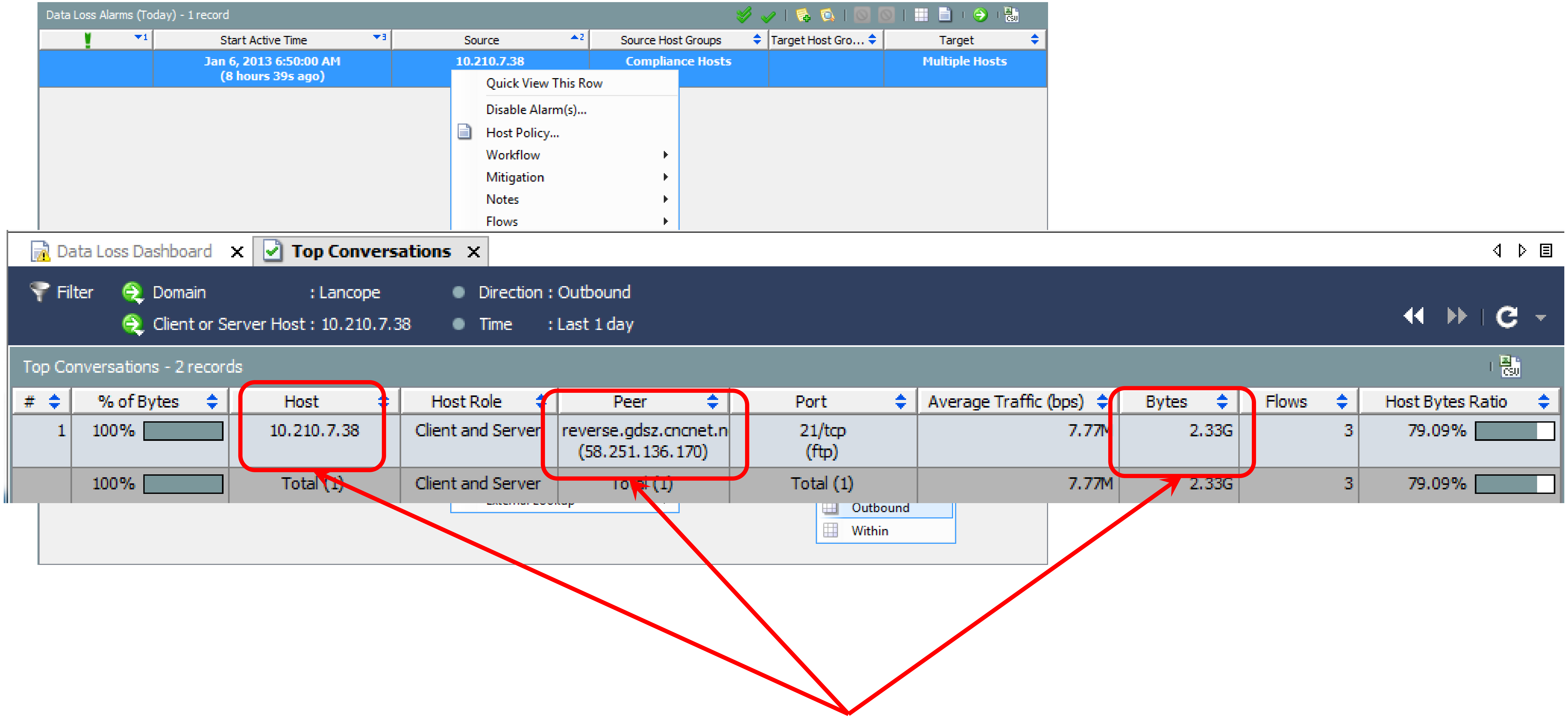
Detecting Data Loss



Data Loss Alarms (Today) - 1 record

!	Start Active Time	Source	Source Host Groups	Target Host Gro...	Target
	Jan 6, 2013 6:50:00 AM (8 hours 39s ago)	10.210.7.38	Compliance Hosts		Multiple Hosts

Detecting Data Loss



Data Loss Alarms (Today) - 1 record

!	Start Active Time	Source	Source Host Groups	Target Host Gro...	Target
	Jan 6, 2013 6:50:00 AM (8 hours 39s ago)	10.210.7.38	Compliance Hosts		Multiple Hosts

Filter Domain : Lancope
Direction : Outbound
Client or Server Host : 10.210.7.38
Time : Last 1 day

Top Conversations - 2 records

#	% of Bytes	Host	Host Role	Peer	Port	Average Traffic (bps)	Bytes	Flows	Host Bytes Ratio
1	100%	10.210.7.38	Client and Server	reverse.gdsz.cncnet.n (58.251.136.170)	21/tcp (ftp)	7.77M	2.33G	3	79.09%
	100%	Total (1)	Client and Server	Total (1)	Total (1)	7.77M	2.33G	3	79.09%

Source host, peer and data volume

Key Takeaways

- Advanced threats are consistently bypassing the traditional security perimeter.
- Threat detection requires visibility and context into network traffic.
- NetFlow can provide the necessary visibility and when joined with context from products such as the Cisco ISE, ASA, ISR and Lancope StealthWatch, these threats can be detected.

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2013 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 8 March 12:00pm-2:00pm

Cisco live! 365

Don't forget to activate your Cisco Live 365 account for access to all session material, communities, and on-demand and live activities throughout the year. Log into your Cisco Live portal and click the "Enter Cisco Live 365" button.

www.ciscoliveaustralia.com/portal/login.ww

Cisco live!