
TOMORROW
starts here.
CISCO
Cisco live!

Cisco CSIRT: Security Analytics and Forensics with NetFlow

BRKSEC-2073

Michael Scheck – CSIRT Investigations Manager

Paul Eckstein – CSIRT Engineering Manager

#clmel

Cisco live!

Agenda

- Heartbleed Use Case
- Netflow Growth
- Deployment
- Problems Solved
- Use Cases
- Conclusion


Heartbleed

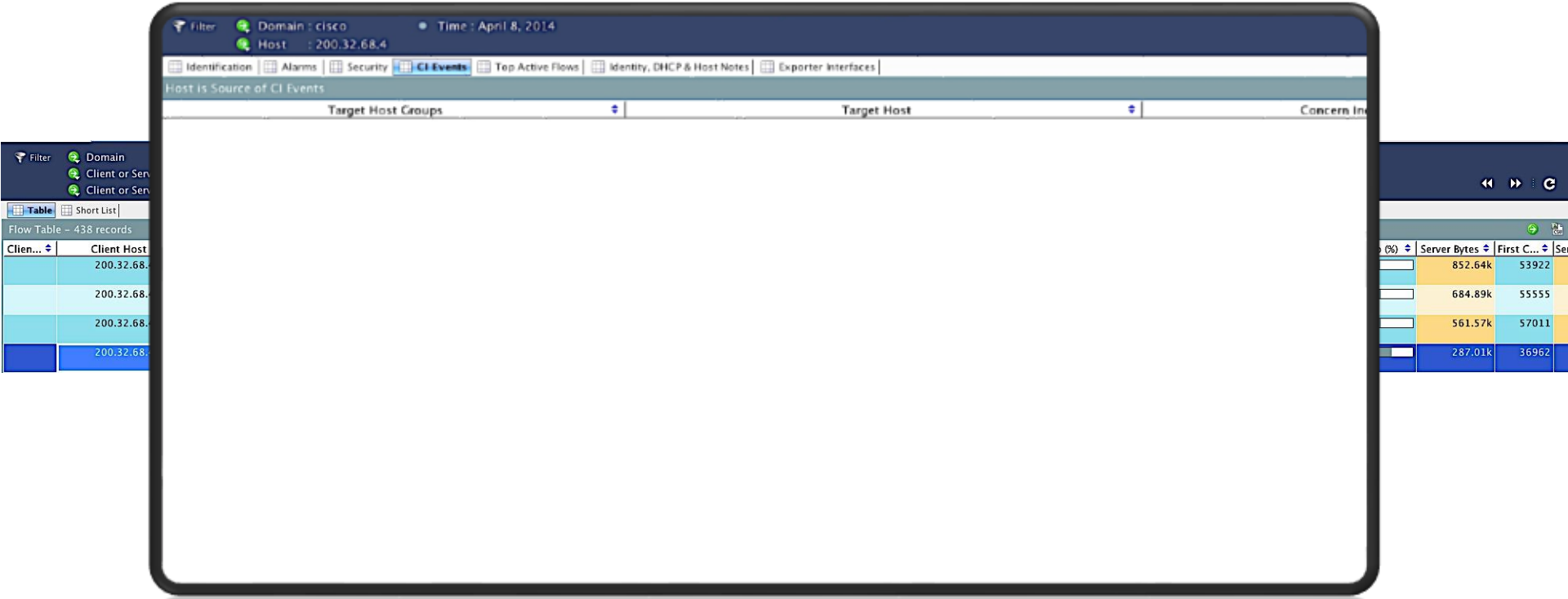
April 8, 2014: Heartbleed Vulnerability

- The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by SSL

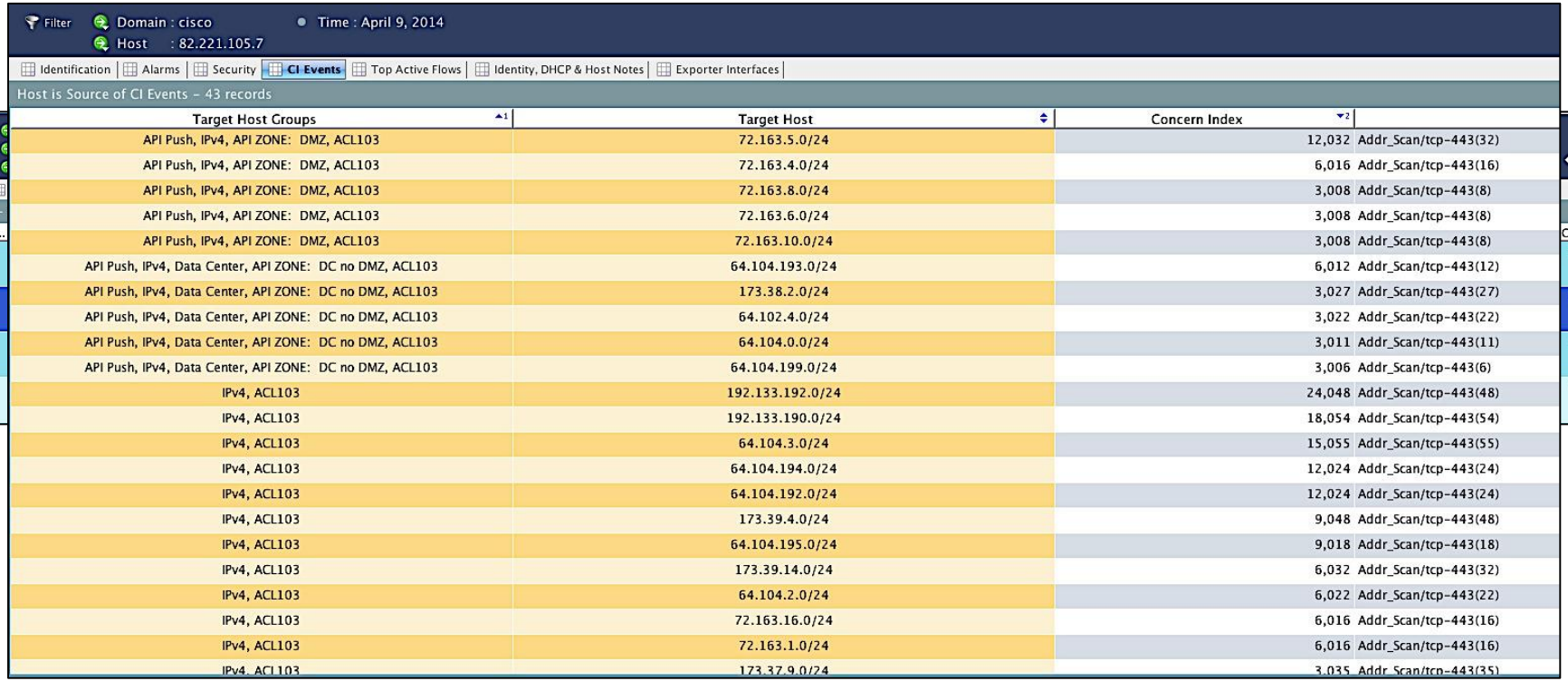
Cisco CSIRT Response to Heartbleed

- Preparation
  - Scanned 1.2M vulnerable servers - 300 needed repair
  - Helped develop signatures for Sourcefire and Cisco IDS
  - Deployed signatures to IDS
- Monitoring and response
  - Discovered 25 attacks: 21 benign, 4 malicious
  - Researched attack via NetFlow analysis to discern normal connections from those that were anomalous and malicious

Heartbleed Benign Host



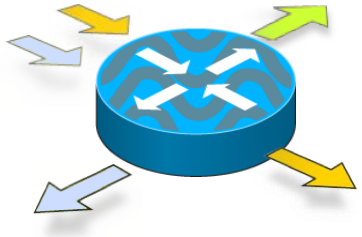
Heartbleed Benign Host



Target Host Groups	Target Host	Concern Index	
API Push, IPv4, API ZONE: DMZ, ACL103	72.163.5.0/24	12,032	Addr_Scan/tcp-443(32)
API Push, IPv4, API ZONE: DMZ, ACL103	72.163.4.0/24	6,016	Addr_Scan/tcp-443(16)
API Push, IPv4, API ZONE: DMZ, ACL103	72.163.8.0/24	3,008	Addr_Scan/tcp-443(8)
API Push, IPv4, API ZONE: DMZ, ACL103	72.163.6.0/24	3,008	Addr_Scan/tcp-443(8)
API Push, IPv4, API ZONE: DMZ, ACL103	72.163.10.0/24	3,008	Addr_Scan/tcp-443(8)
API Push, IPv4, Data Center, API ZONE: DC no DMZ, ACL103	64.104.193.0/24	6,012	Addr_Scan/tcp-443(12)
API Push, IPv4, Data Center, API ZONE: DC no DMZ, ACL103	173.38.2.0/24	3,027	Addr_Scan/tcp-443(27)
API Push, IPv4, Data Center, API ZONE: DC no DMZ, ACL103	64.102.4.0/24	3,022	Addr_Scan/tcp-443(22)
API Push, IPv4, Data Center, API ZONE: DC no DMZ, ACL103	64.104.0.0/24	3,011	Addr_Scan/tcp-443(11)
API Push, IPv4, Data Center, API ZONE: DC no DMZ, ACL103	64.104.199.0/24	3,006	Addr_Scan/tcp-443(6)
IPv4, ACL103	192.133.192.0/24	24,048	Addr_Scan/tcp-443(48)
IPv4, ACL103	192.133.190.0/24	18,054	Addr_Scan/tcp-443(54)
IPv4, ACL103	64.104.3.0/24	15,055	Addr_Scan/tcp-443(55)
IPv4, ACL103	64.104.194.0/24	12,024	Addr_Scan/tcp-443(24)
IPv4, ACL103	64.104.192.0/24	12,024	Addr_Scan/tcp-443(24)
IPv4, ACL103	173.39.4.0/24	9,048	Addr_Scan/tcp-443(48)
IPv4, ACL103	64.104.195.0/24	9,018	Addr_Scan/tcp-443(18)
IPv4, ACL103	173.39.14.0/24	6,032	Addr_Scan/tcp-443(32)
IPv4, ACL103	64.104.2.0/24	6,022	Addr_Scan/tcp-443(22)
IPv4, ACL103	72.163.16.0/24	6,016	Addr_Scan/tcp-443(16)
IPv4, ACL103	72.163.1.0/24	6,016	Addr_Scan/tcp-443(16)
IPv4, ACL103	173.37.9.0/24	3,035	Addr_Scan/tcp-443(35)

Netflow Growth

NetFlow Overview



Source IP: Port	Destination IP: Port	Packets	Date / Time
192.168.15.7:2068	211.160.17.195:8080	7	3/12/2015 08:15:02 GMT
192.168.21.5:1042	72.18.45.223:21	219	3/12/2015 09:02:51 GMT
192.168.6.22:3161	172.18.15.188:80	1	3/12/2015 09:12:42 GMT

NetFlow Collection and Analysis Solutions

	OSU FlowTools	Nfdump	Lancope StealthWatch
License	OpenSource from Ohio State	OpenSource from SourceForge	Commercial
NetFlow Versions	V5 and up	V5 and up	V5 and up
IPv6?	Yes	Yes	Yes
Syntax	Command-line, like ACLs	Command-line, like tcpdump	GUI, API
Support	Ad-hoc via Google Code	Up-to-date	Up-to-date

NetFlow at Cisco Before StealthWatch

- OSU FlowTools
- 25+ systems running in parallel
  - Speeds up query time, but routers have to point at each collector
- 20+ Tb of physical storage
  - Files were stored in native nfdump/flowtools compressed format
- No flow aggregation
  - Some connections passed through multiple devices, causing duplicate flows
  - Routers splitting up long running flows
  - Exporter information obscured by fanout tool

NetFlow Challenge: Support

- Support of open source tools
- OS support
- Training staff
- Feature requests
- Protocol changes (NetFlow and IP)
- Difficult to monitor for flow loss

NetFlow Investigation with OSU FlowTools

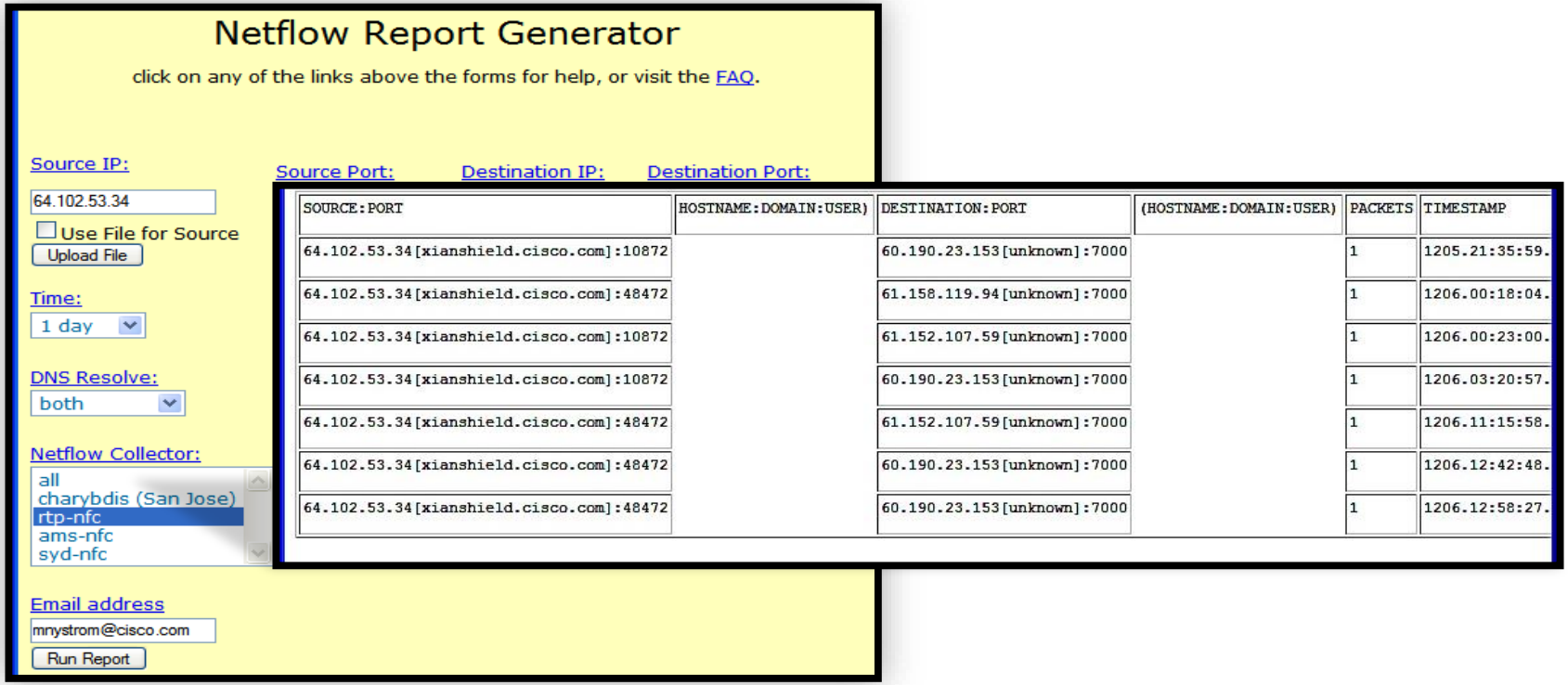
Query

```
[mynfchost]$ head bot.acl
ip access-list standard bot permit host 69.50.180.3
ip access-list standard bot permit host 66.182.153.176

[mynfchost]$ flow-cat /var/local/flows/data/2007-02-12/ft* | flow-filter -Sbot -o -...

Start             End               Sif   SrcIPaddress    SrcP  DIf   DstIPaddress  DstP
0213.08:39:49.911 0213.08:40:34.519 58    10.10.71.100    8343  98    69.50.180.3   31337
0213.08:40:33.590 0213.08:40:42.294 98    69.50.180.3     31337 58    10.10.71.100  83
```


Cisco live!

NetFlow Investigation with OSU FlowTools

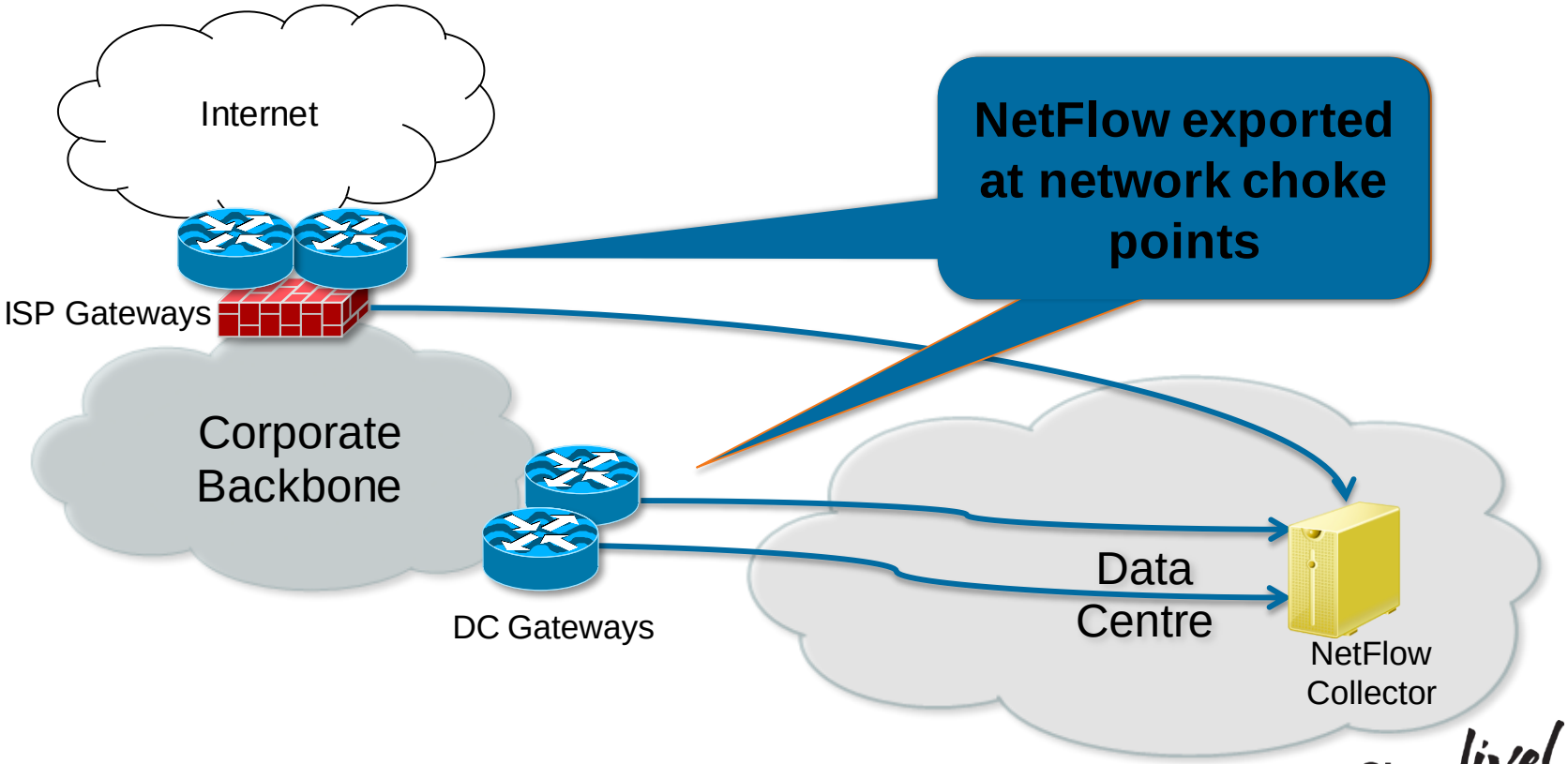
Custom NetFlow report generator



Deployment

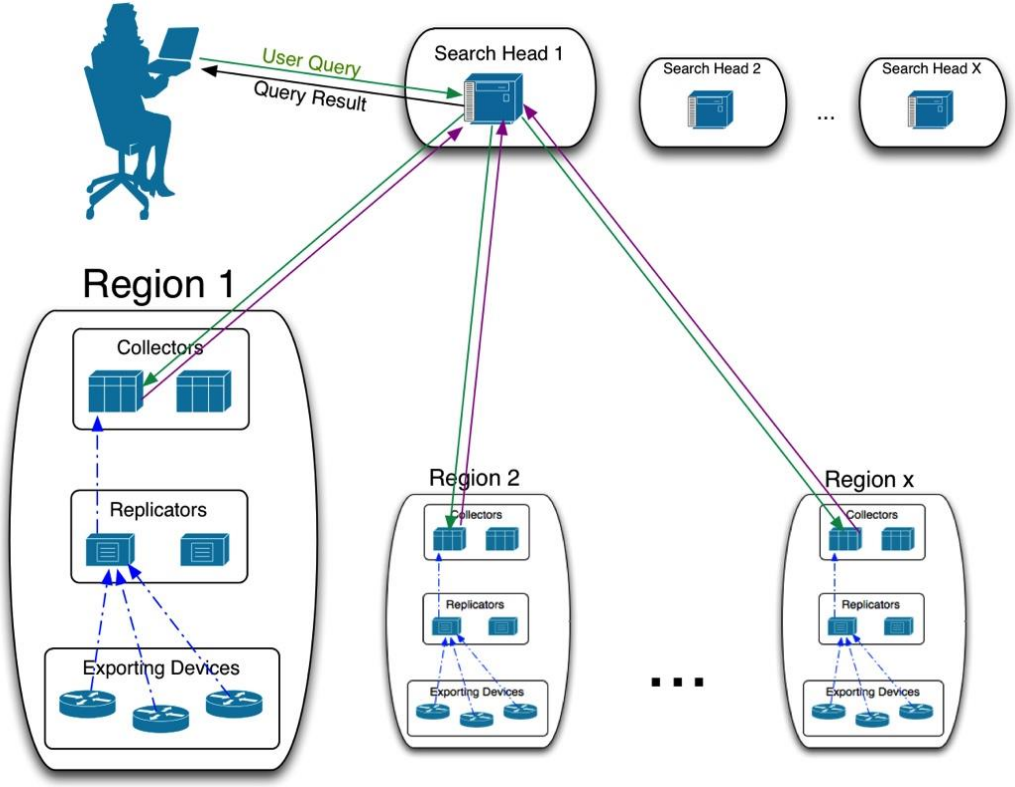
NetFlow Export at Cisco

Collect at chokepoints for egress detection



NetFlow Architecture

- Redundant forwarding
- Regional storage
- Global search



Lancope Devices and Count

2

Stealthwatch Management Console

13

FlowSensor

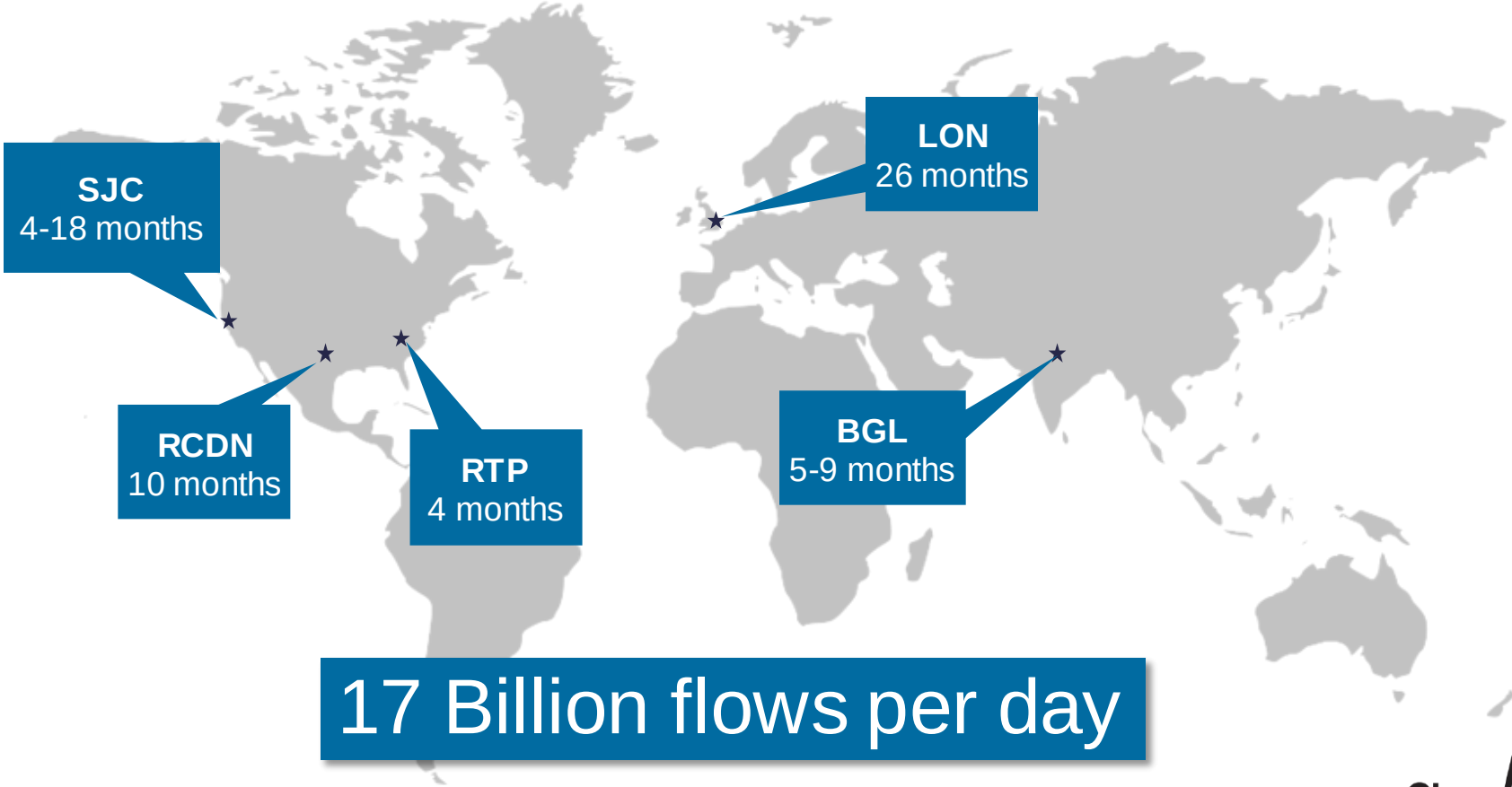
16

UDP Director

21

FlowCollector

NetFlow Retention



17 Billion flows per day

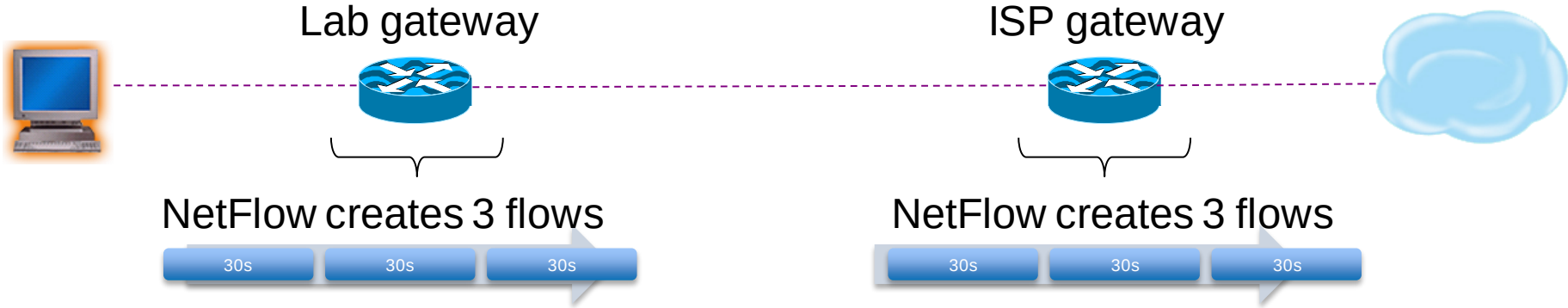
Problems Solved

Cisco live!

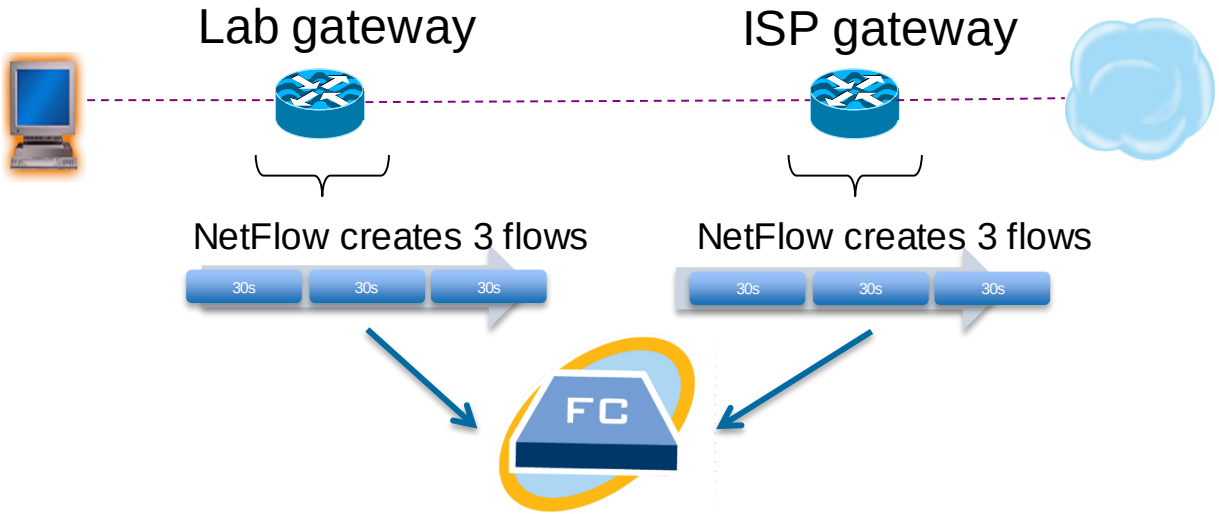
NetFlow Challenge: Flow Timeouts

One 90s flow creates **6 flows**

30s timeout 90/30 = 3 x 2 collectors



Business Benefit #1 Storage Capacity



Client Exporters IP (IF)

Client → Server

Exporter	Exporter T...	Interface	Direction	TTL	DSCP	Flow Action
gwy03-dc-gw1.cisco.com (10.53.41.4)	Exporter	ifIndex-1	Outbound			
gwy03-dc-gw1.cisco.com (10.53.41.4)	Exporter	ifIndex-61	Inbound		best_effort	

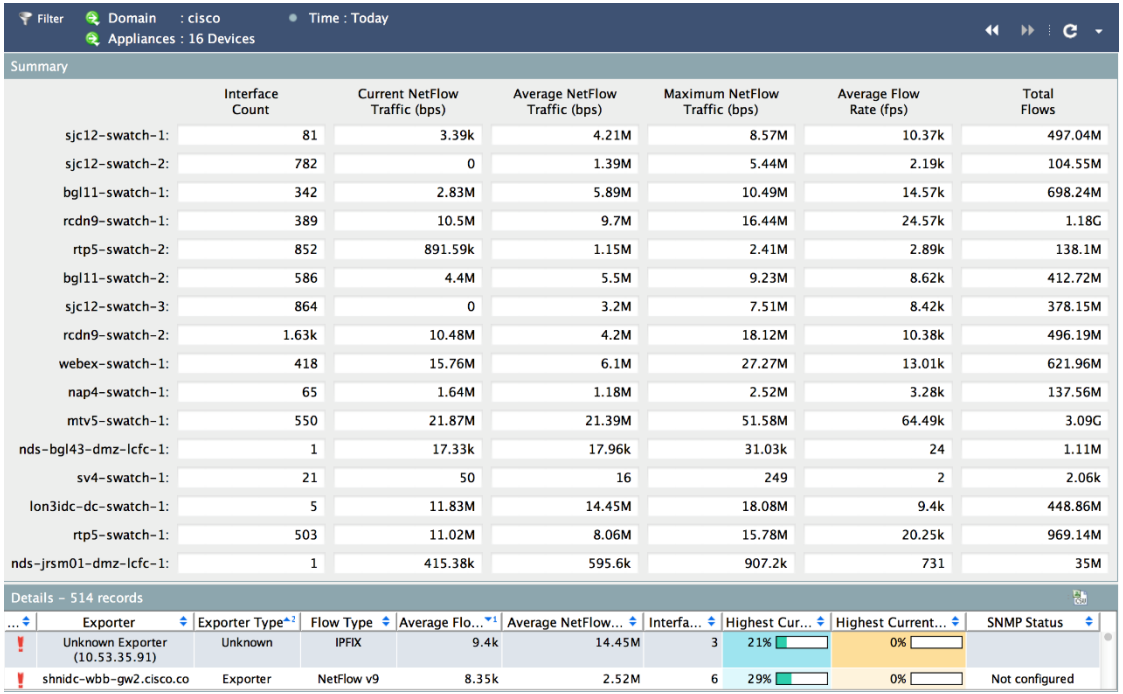
Server Exporters IP (IF)

Client ← Server

Exporter	Exporter T...	Interface	Direction	TTL	DSCP	Flow Action
gwy03-dc-gw2.cisco.com (10.53.41.5)	Exporter	ifIndex-2	Inbound		best_effort	
gwy03-dc-gw2.cisco.com (10.53.41.5)	Exporter	ifIndex-61	Outbound			

Business Benefit #2 Ease of Support

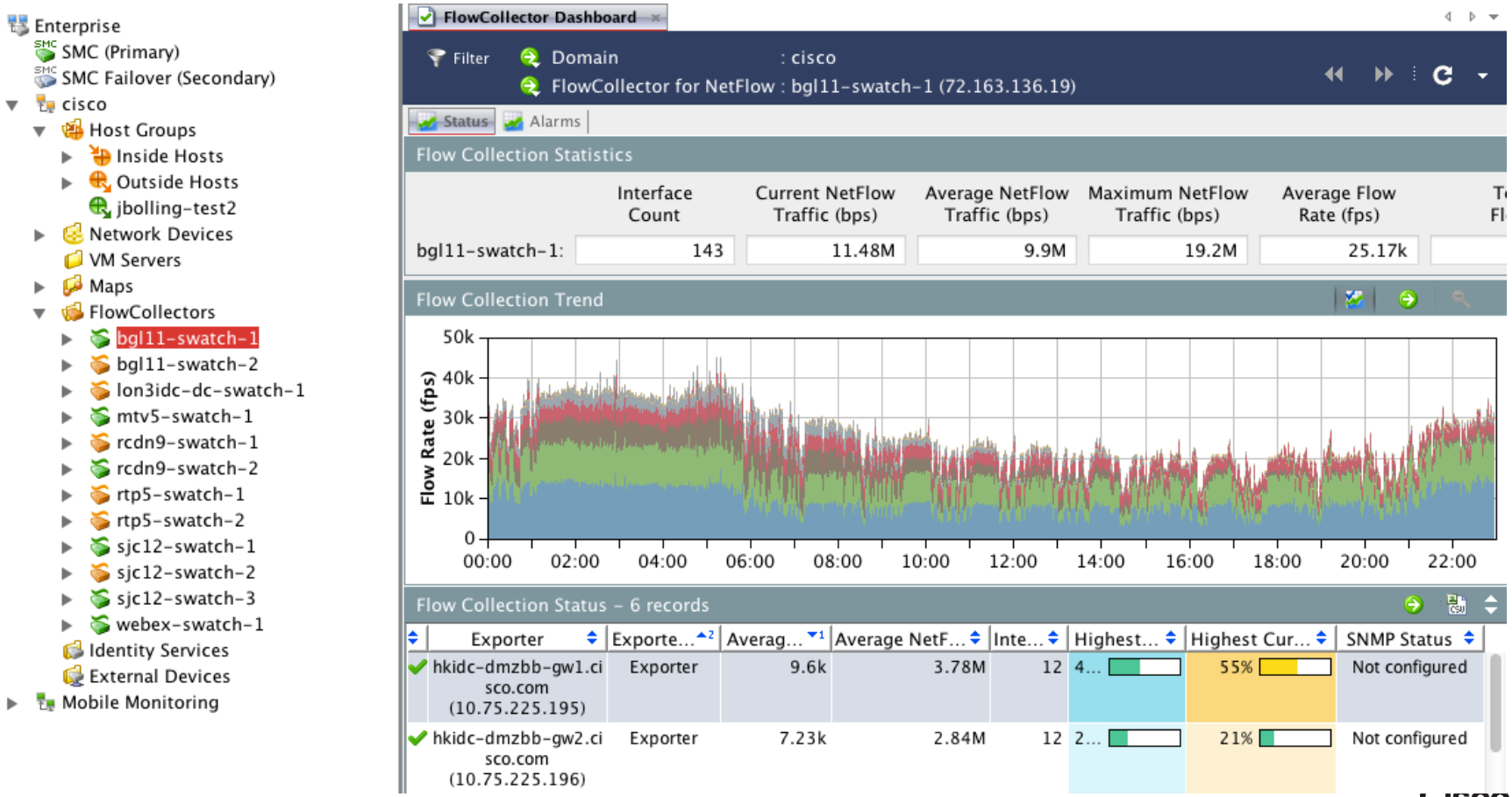
- IPv4/IPv6 both supported
- Netflow v5/v9 both supported
- All supported on the same system, on the same port!
- No system administration required
- Alarms built in for monitoring of lost flows



	Interface Count	Current NetFlow Traffic (bps)	Average NetFlow Traffic (bps)	Maximum NetFlow Traffic (bps)	Average Flow Rate (fps)	Total Flows
sjc12-swatch-1:	81	3.39k	4.21M	8.57M	10.37k	497.04M
sjc12-swatch-2:	782	0	1.39M	5.44M	2.19k	104.55M
bgl11-swatch-1:	342	2.83M	5.89M	10.49M	14.57k	698.24M
rcdn9-swatch-1:	389	10.5M	9.7M	16.44M	24.57k	1.18G
rtp5-swatch-2:	852	891.59k	1.15M	2.41M	2.89k	138.1M
bgl11-swatch-2:	586	4.4M	5.5M	9.23M	8.62k	412.72M
sjc12-swatch-3:	864	0	3.2M	7.51M	8.42k	378.15M
rcdn9-swatch-2:	1.63k	10.48M	4.2M	18.12M	10.38k	496.19M
webex-swatch-1:	418	15.76M	6.1M	27.27M	13.01k	621.96M
nap4-swatch-1:	65	1.64M	1.18M	2.52M	3.28k	137.56M
mtv5-swatch-1:	550	21.87M	21.39M	51.58M	64.49k	3.09G
nds-bgl43-dmz-lcfc-1:	1	17.33k	17.96k	31.03k	24	1.11M
sv4-swatch-1:	21	50	16	249	2	2.06k
lon3idc-dc-swatch-1:	5	11.83M	14.45M	18.08M	9.4k	448.86M
rtp5-swatch-1:	503	11.02M	8.06M	15.78M	20.25k	969.14M
nds-jrsm01-dmz-lcfc-1:	1	415.38k	595.6k	907.2k	731	35M

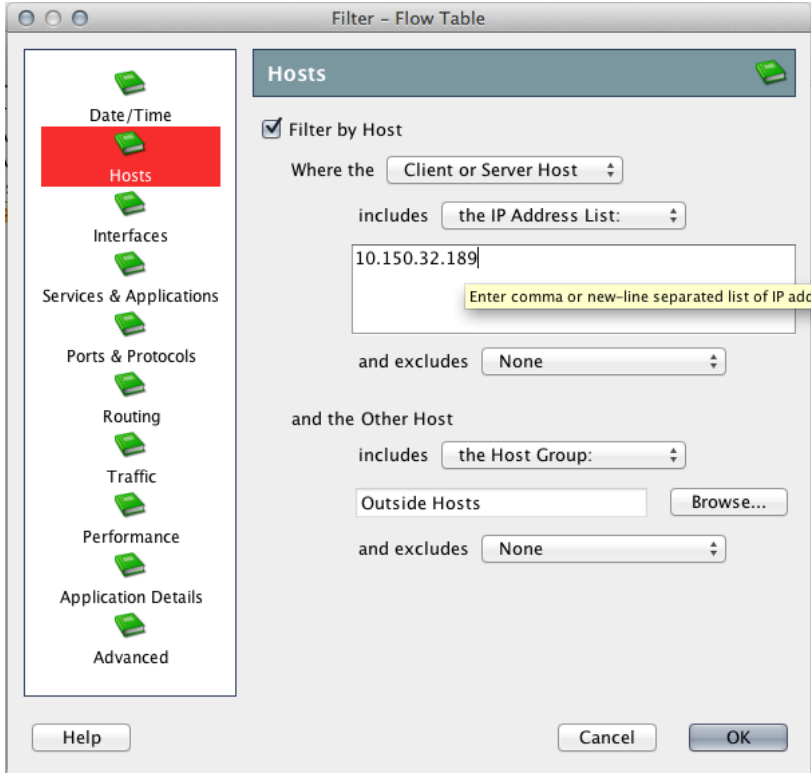
...	Exporter	Exporter Type	Flow Type	Average Flo...	Average NetFlow...	Interfa...	Highest Cur...	Highest Current...	SNMP Status
!	Unknown Exporter (10.53.35.91)	Unknown	IPFIX	9.4k	14.45M	3	21%	0%	
!	shnidc-wbb-gw2.cisco.co	Exporter	NetFlow v9	8.35k	2.52M	6	29%	0%	Not configured

Business Benefit #3 Ease of Use



Flow Table Query

- Other variables: host groups, time range, interfaces, ports
- Defaults to 2000 flow records returned
- Much simpler than syntax for CLI (example below)



1. Create a file called‘flow.acl’with a named access list:

```
linux-machine#  cat ip access-list  standard  botnet permit  ip
10.31.33.7  >flow.acl
```

2. Run a query for the time period you are interested in using the ACL

```
linux-machine#  flow-cat  /var/local/flows/data/2006-12-01/ft*
  | flow-filter  -f ~/flow.acl  -Sbotnet  -o -Dbotnet  | flow-
  print  -f5
```

Flow Table Output

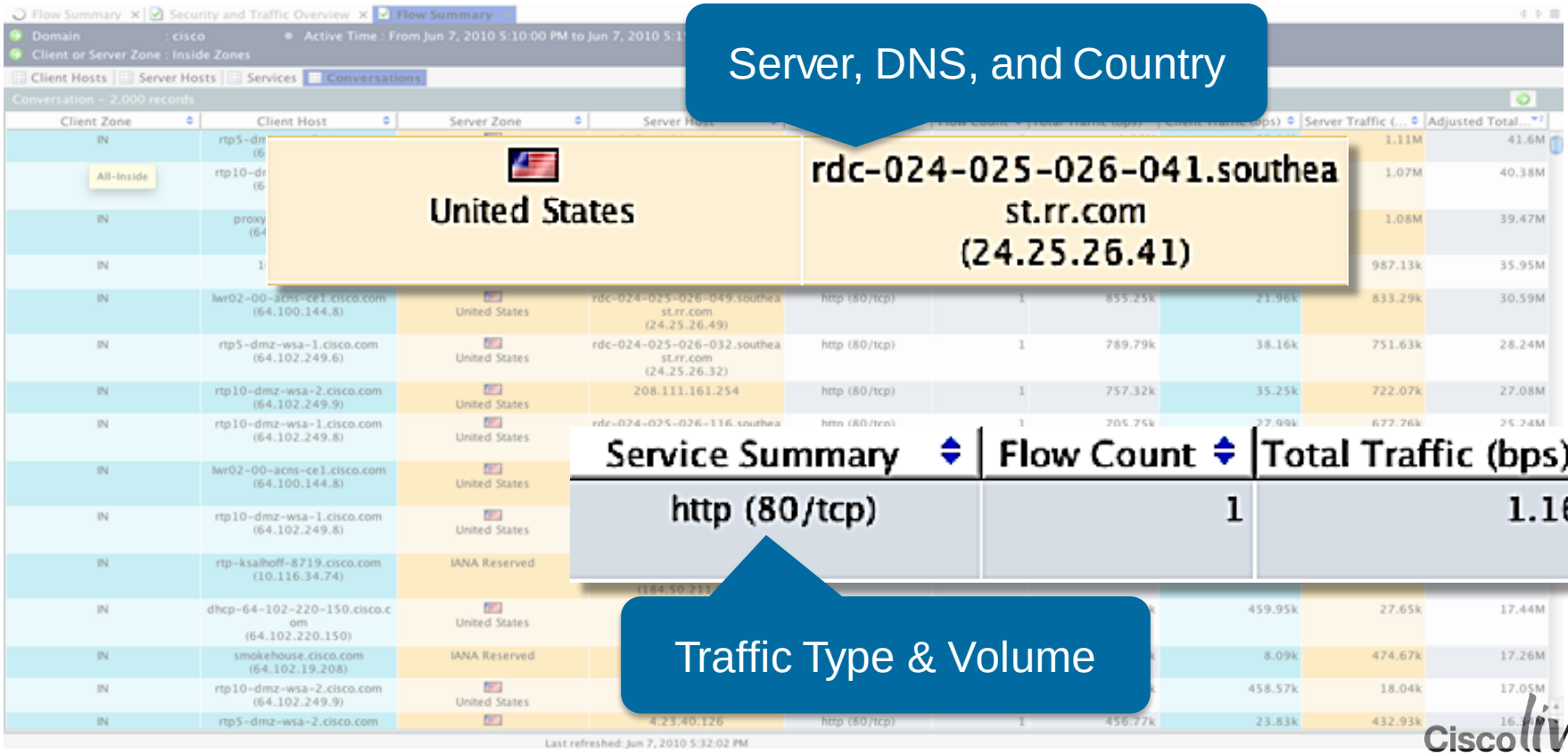
Filter
Domain : cisco
Client or Server Host : dhcp-10-150-32-189.cisco.com (10.150.32.189)
Client or Server Host Group : Outside Hosts
Time : Last 2 hours 5 minutes

Table | Short List

Flow Table - 148 records

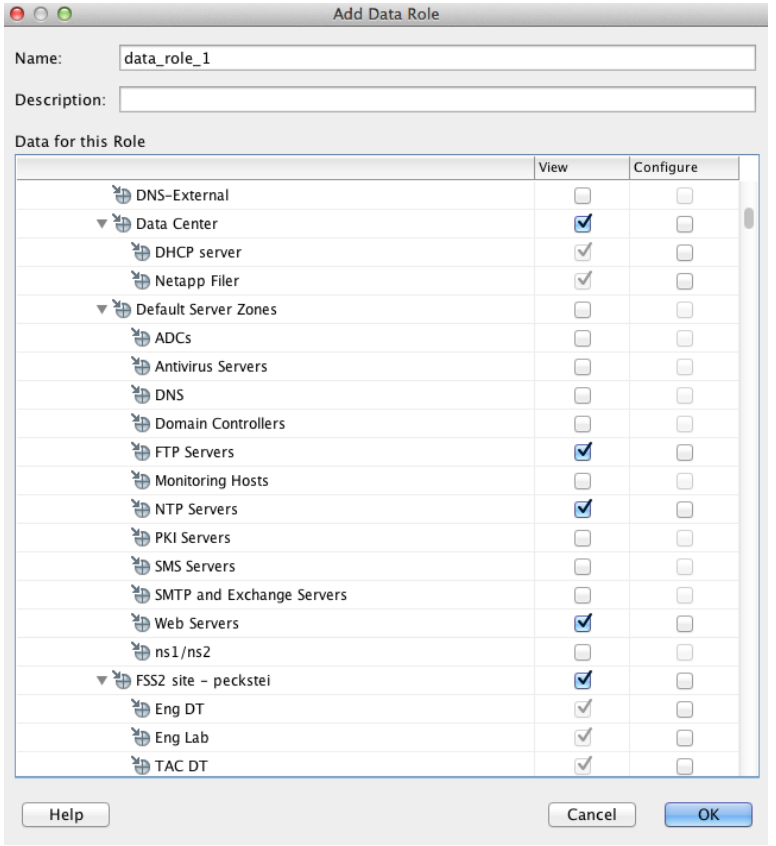
Client Host	Client Host Groups	Server Host	Server Host Groups	Duration ▼2	Application	Service Summary	Total Tr... ▼3	Total Bytes ▼1
dhcp-10-150-32-189.cisco.com (10.150.32.189)	Private Addresses, ACL103	74.125.228.33	United States	5 minutes 11s	HTTP (unclassified)	http (80/tcp)	4.21k	159.95k
dhcp-10-150-32-189.cisco.com (10.150.32.189)	Private Addresses, ACL103	69.171.237.16	United States	17 minutes 50s	HTTP (unclassified)	http (80/tcp)	1.03k	134.28k
dhcp-10-150-32-189.cisco.com (10.150.32.189)	Private Addresses, ACL103	199.47.216.147	United States	2 hours 8 minutes 3s	HTTP (unclassified)	http (80/tcp)	101	91.39k
dhcp-10-150-32-189.cisco.com (10.150.32.189)	Private Addresses, ACL103	31.13.76.26	Ireland, IANA Reserved	5 minutes 11s	HTTP (unclassified)	http (80/tcp)	1.99k	75.53k
dhcp-10-150-32-189.cisco.com (10.150.32.189)	Private Addresses, ACL103	74.125.228.44	United States	5 minutes 10s	HTTP (unclassified)	http (80/tcp)	1.92k	72.56k
dhcp-10-150-32-189.cisco.com (10.150.32.189)	Private Addresses, ACL103	23.67.250.154	IANA Reserved, United States	8 minutes 21s	HTTP (unclassified)	http (80/tcp)	1.13k	69.35k
dhcp-10-150-32-189.cisco.com (10.150.32.189)	Private Addresses, ACL103	iad23s05-in-f12.1e100.net (74.125.228.12)	United States	5 minutes 4s	HTTP (unclassified)	http (80/tcp)	1.81k	67.12k
dhcp-10-150-32-189.cisco.com (10.150.32.189)	Private Addresses, ACL103	205.188.7.243	United States	2 hours 9 minutes 12s	HTTPS (unclassified)	https (443/tcp)	68	62.01k

FlowTable Results



Role Based Access

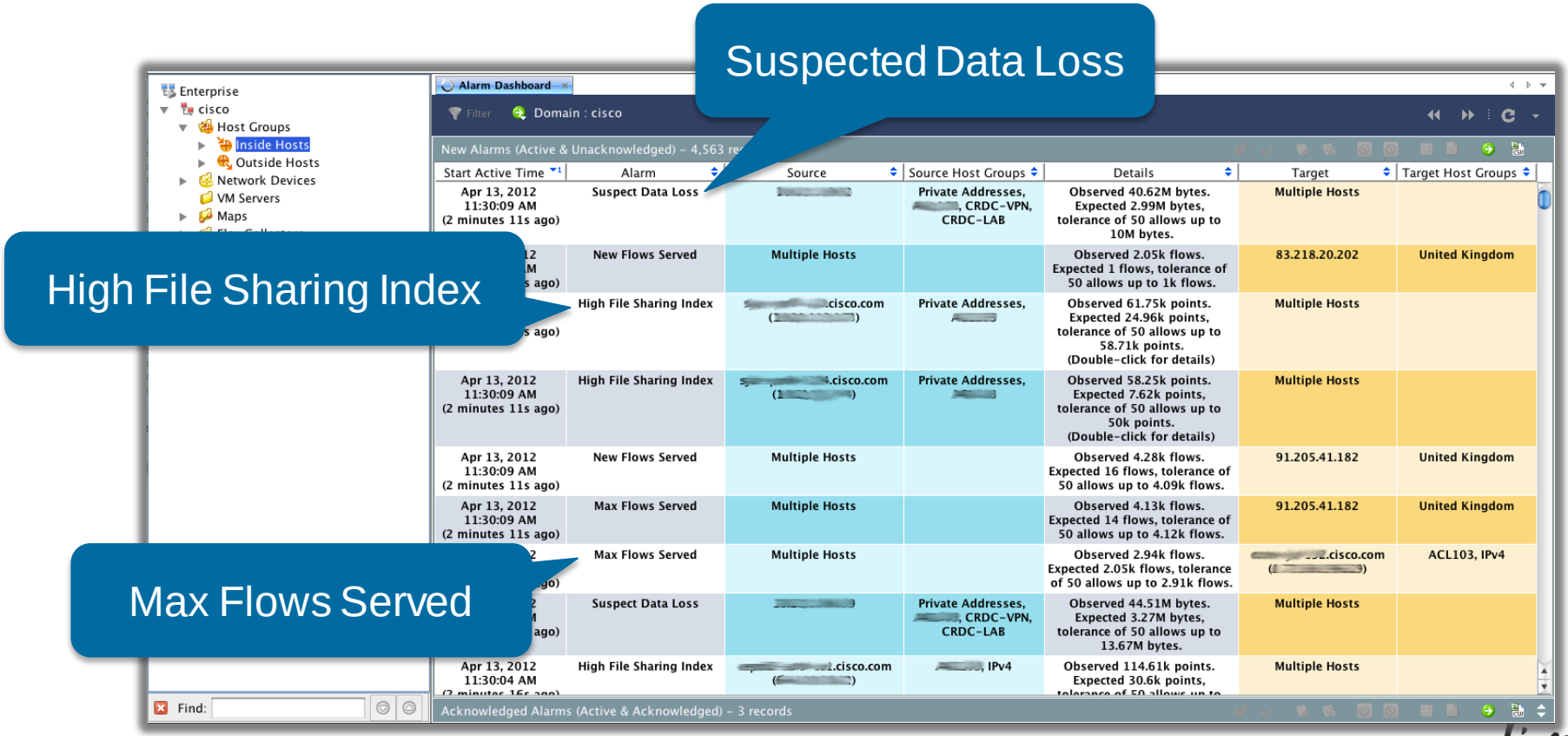
- Twofold restriction
  - Functional roles: configure appliances, policies, etc.
  - Data roles: view/edit x, y, z host groups
- Notes
  - Granular data restriction
  - No audit log of configuration changes!
  - CSIRT manages all SMC access and privileges



NetFlow Challenge: Limited Detection Capability

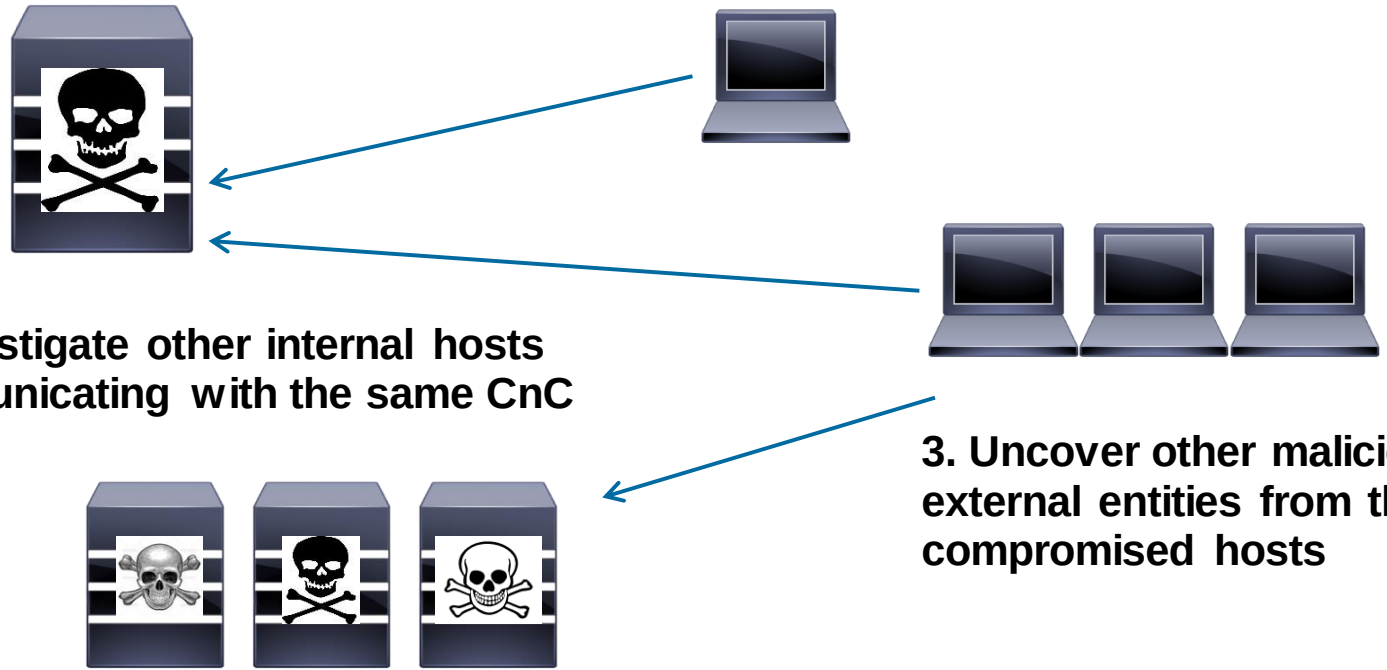
- No concept of host groups for query
- Effective for forensics
- Can do basic DOS detection
- Any other queries required writing algorithms

Business Benefit #4: Analytics

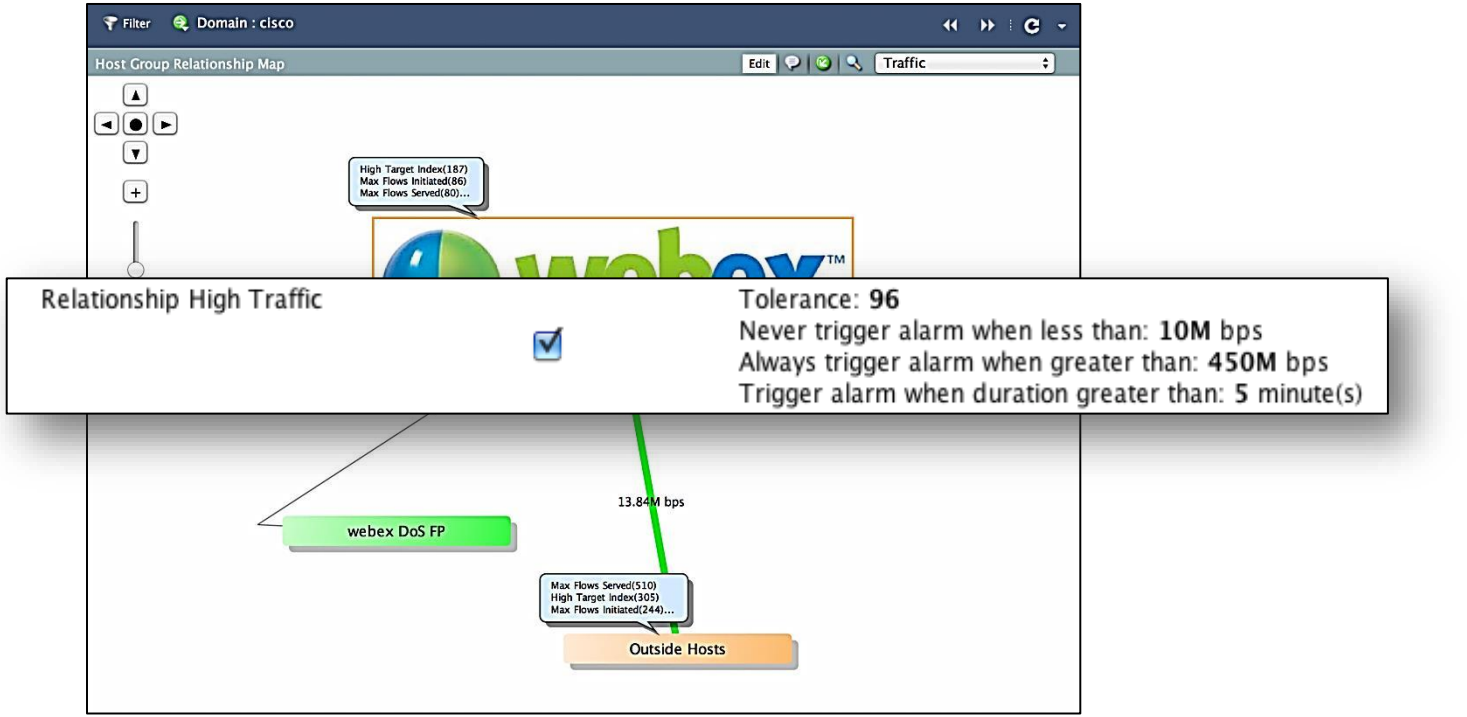


Use Cases

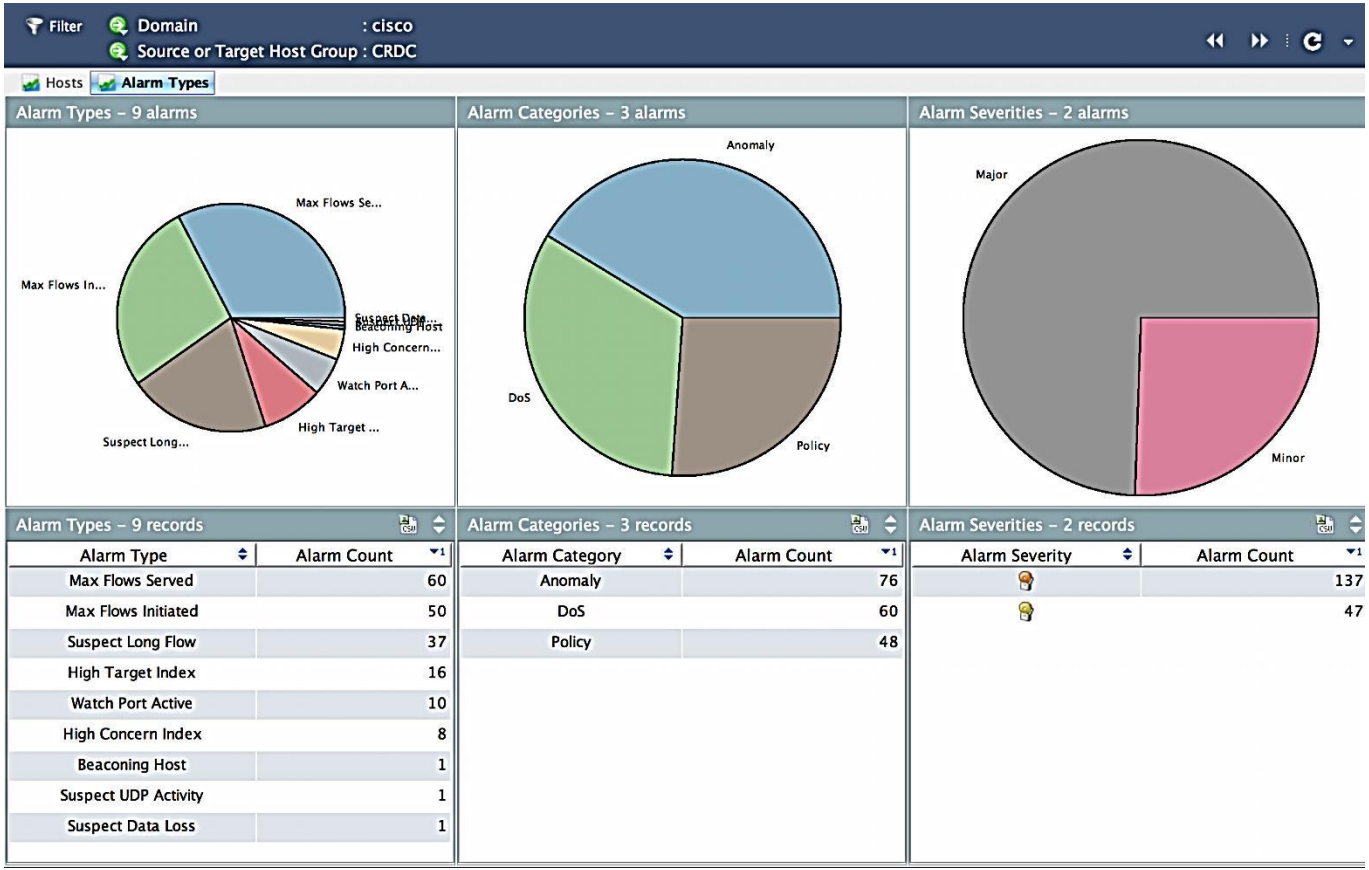
NetFlow CNC Discovery



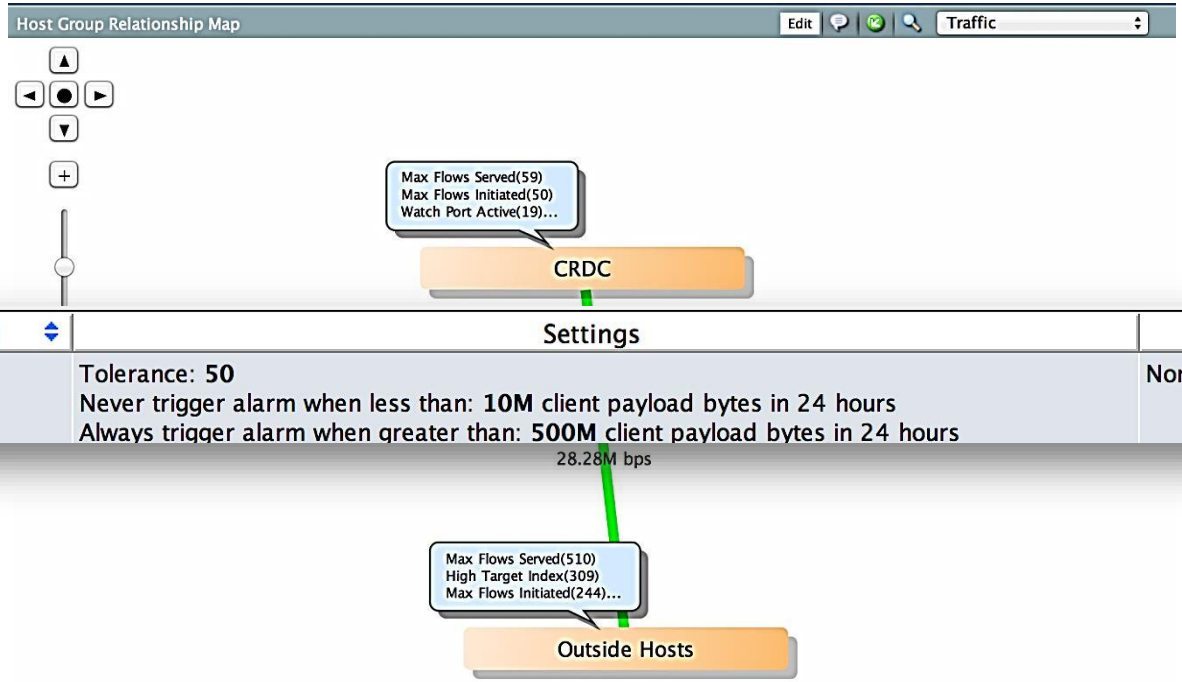
Targeted Monitoring:DoS Detection



Targeted Monitoring:DoS Detection



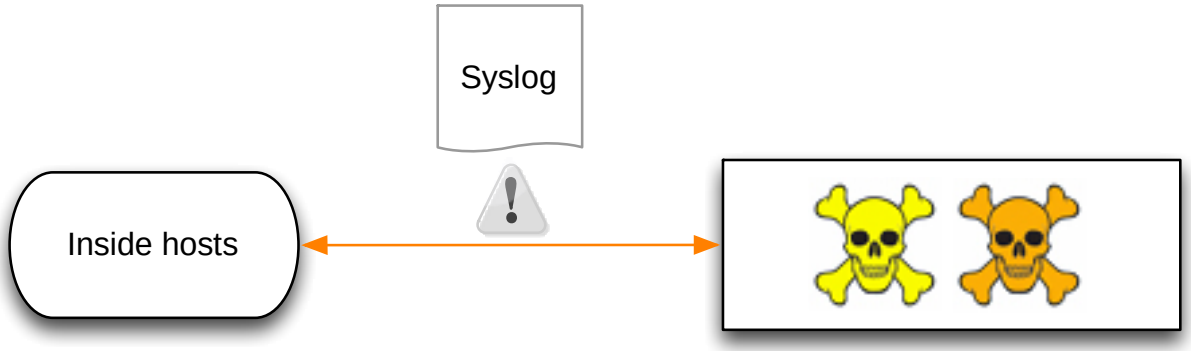
Targeted Monitoring – Data Loss

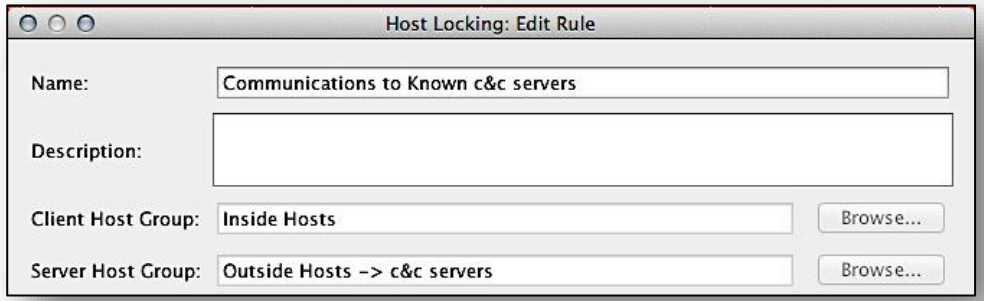


Alarm	Enabled	Settings	Mitigation
Suspect Data Loss	☑	Tolerance: **50** Never trigger alarm when less than: **10M** client payload bytes in 24 hours Always trigger alarm when greater than: **500M** client payload bytes in 24 hours	None

StealthWatch Host Locking

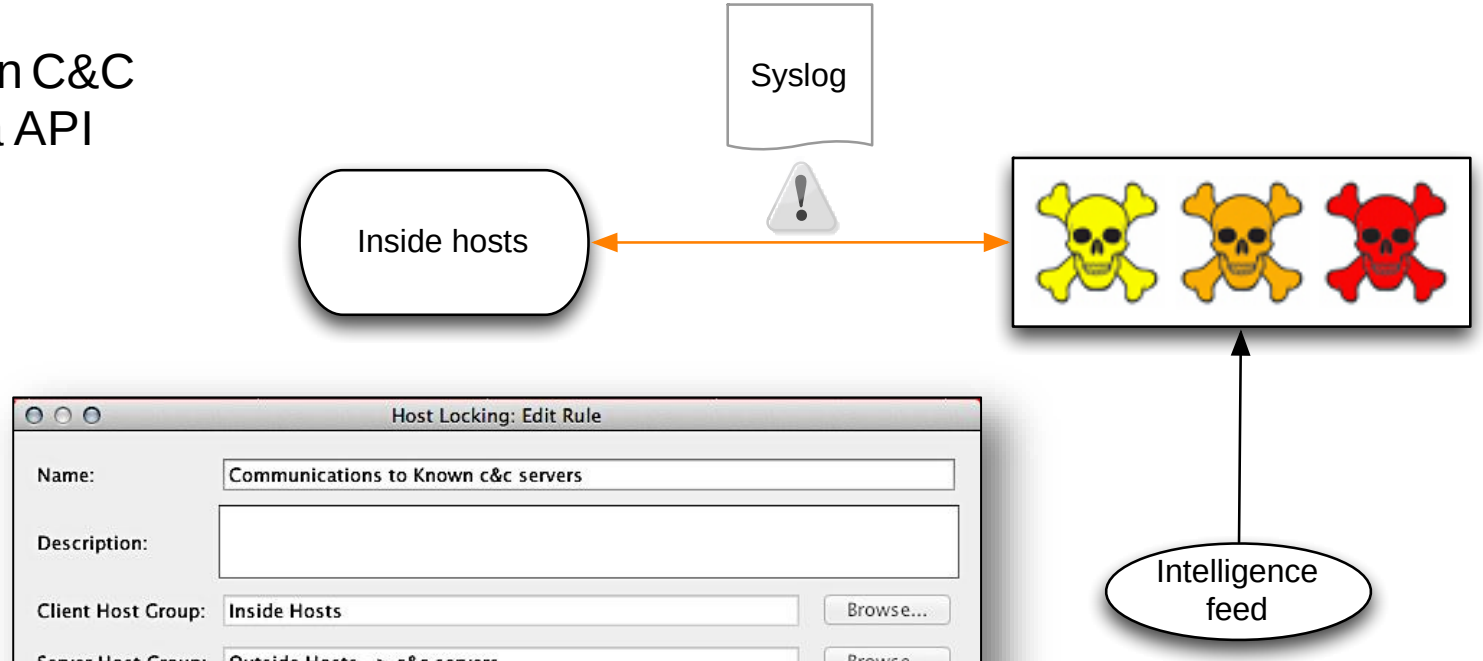
Send syslog for any traffic seen between insides hosts and known C&C servers





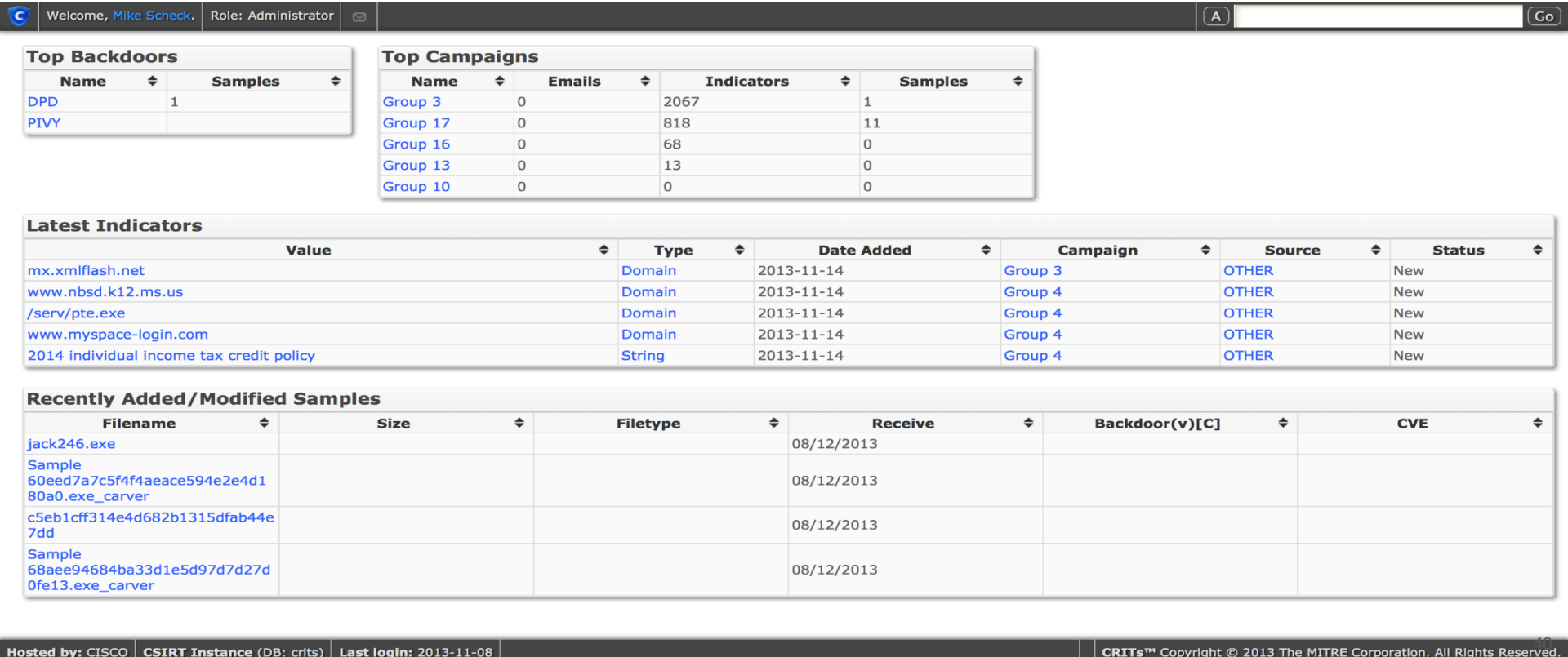
StealthWatch Host Locking

Modify known C&C server list via API



CRiTs

crits@mitre.org

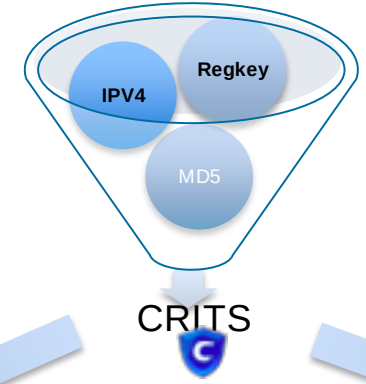


CRiTS Indicator Actions

Current

In Progress

Future



Prevent

BGP

ESA

DNS RPZ

HIPS

AV

WSA

Detect

Lancope

host IDS

Mandiant

LUPA/ PCAP

passive DNS

Syslog

Share

CSIRT

Govt

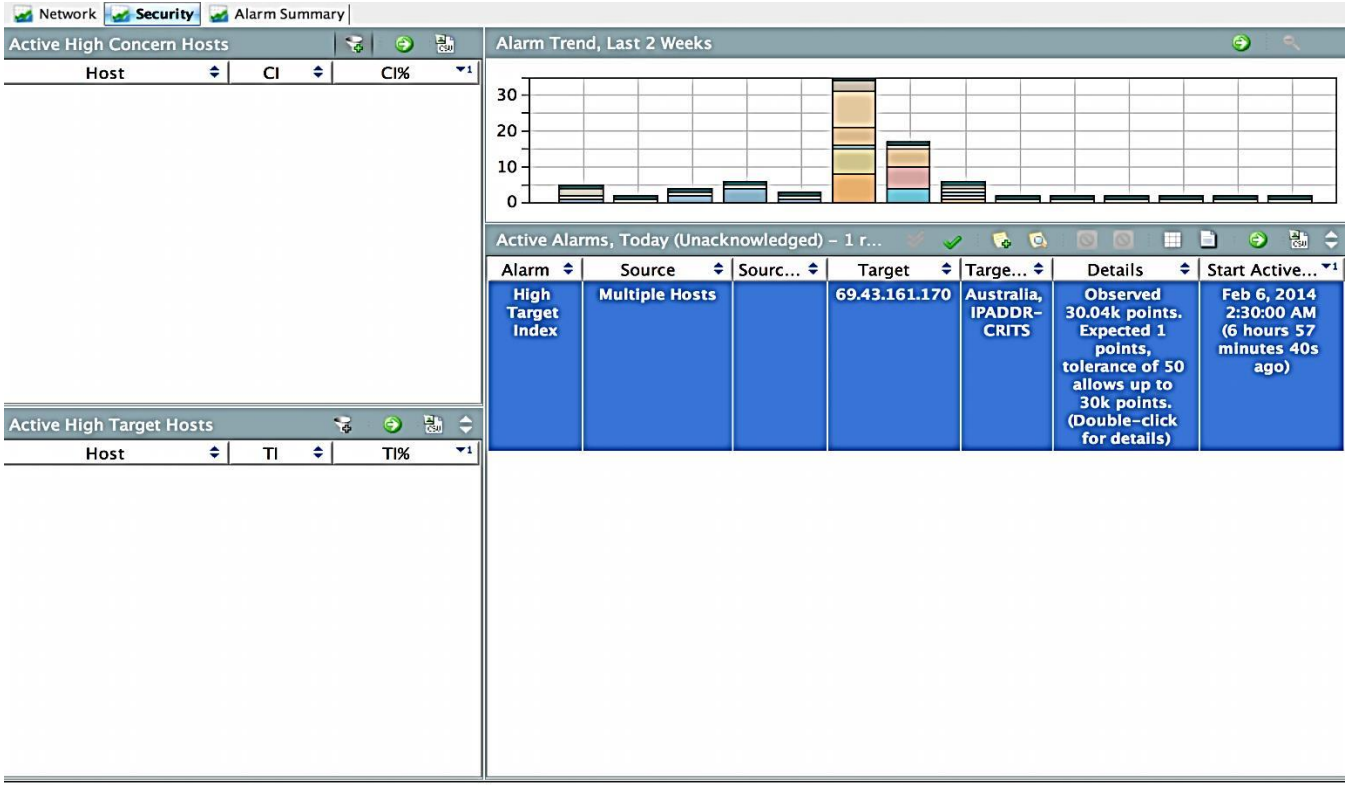
CDSA

Partner

SBG

Cisco live!

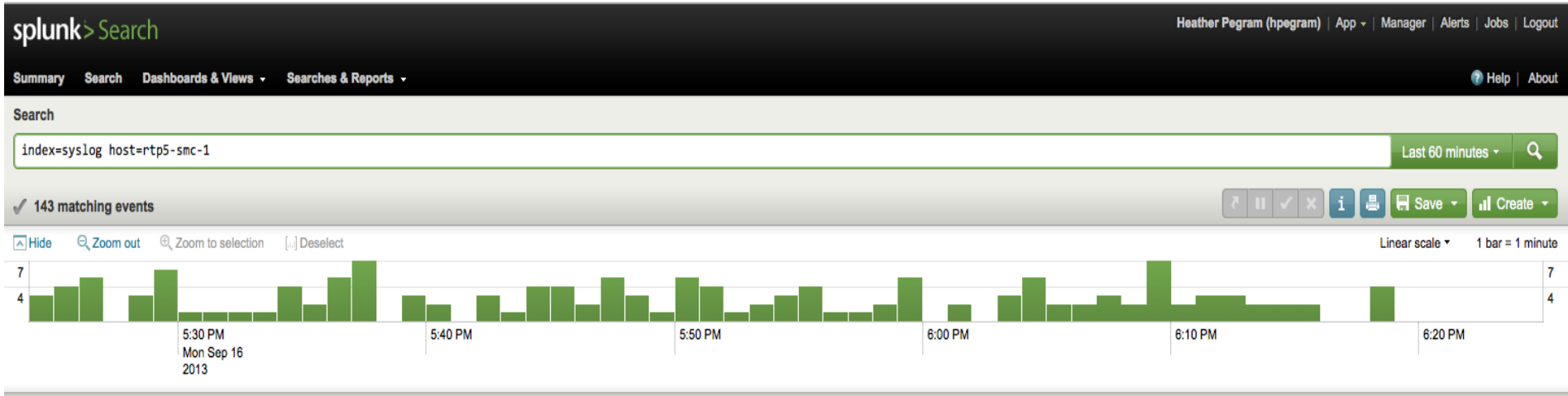
CRiTs Netflow Alarms



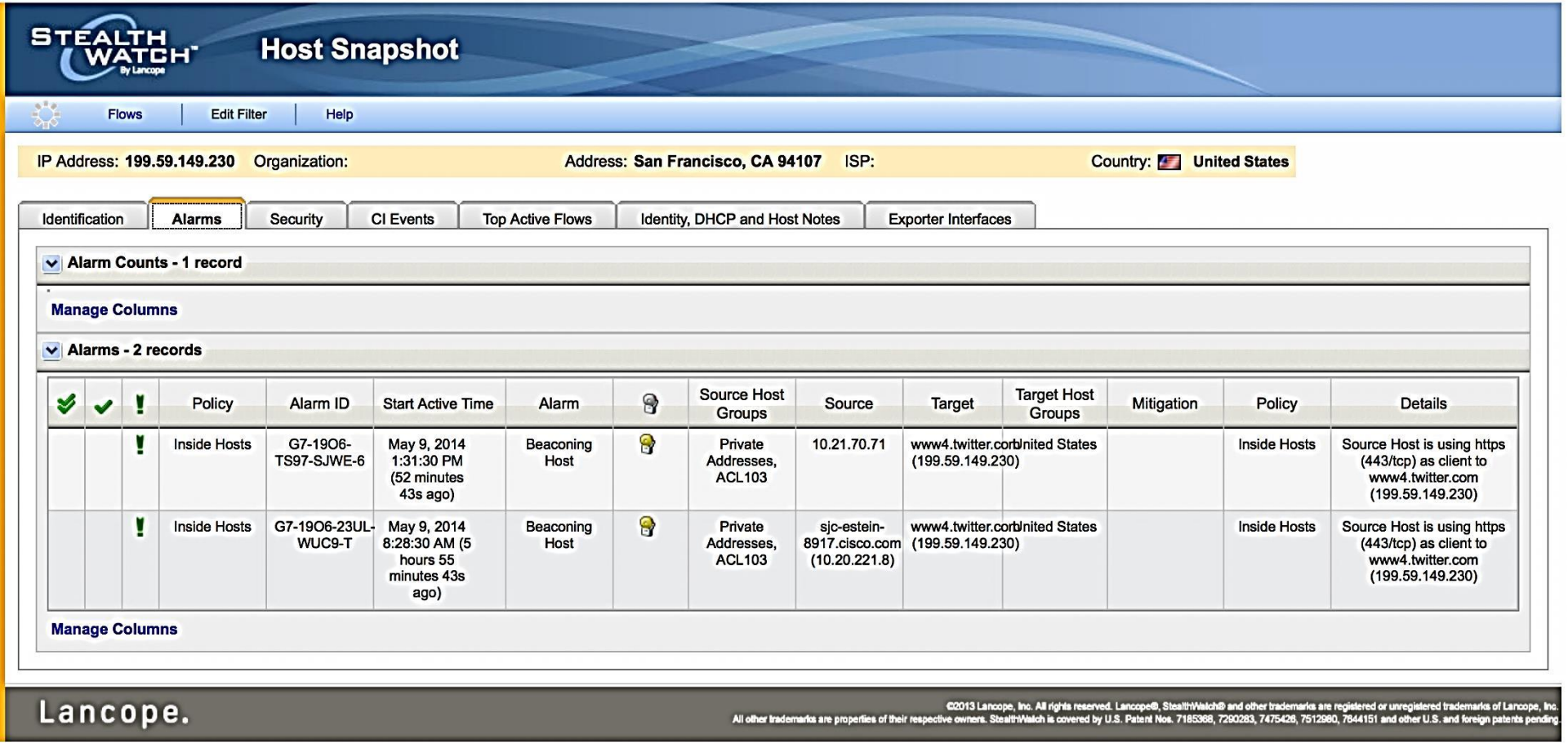
Splunk Integration – SMC Alarms

Requirement: integrate flow events with other logs for a single investigation interface

Solution: send relevant alarms as syslog messages to in-house Splunk™ architecture



StealthWatch Splunk Alerts

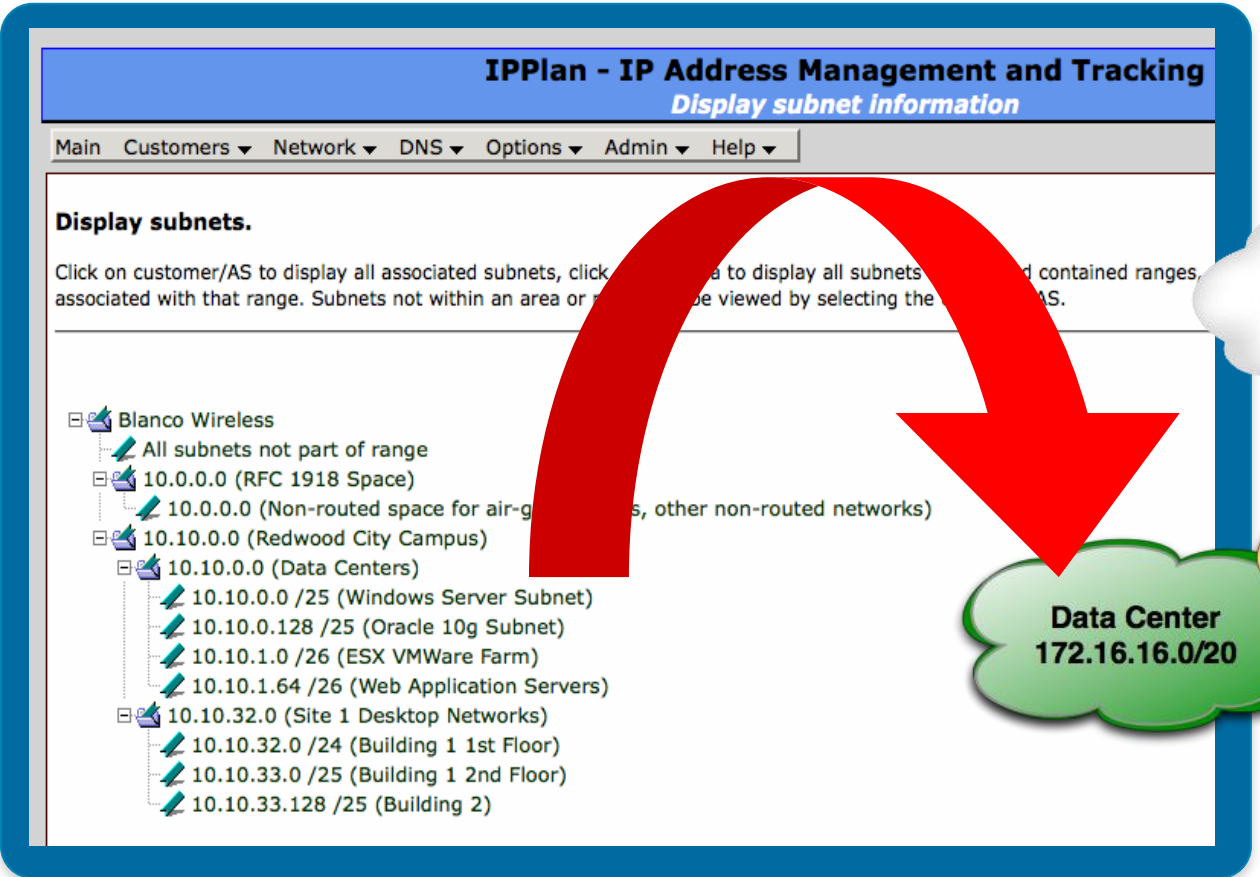


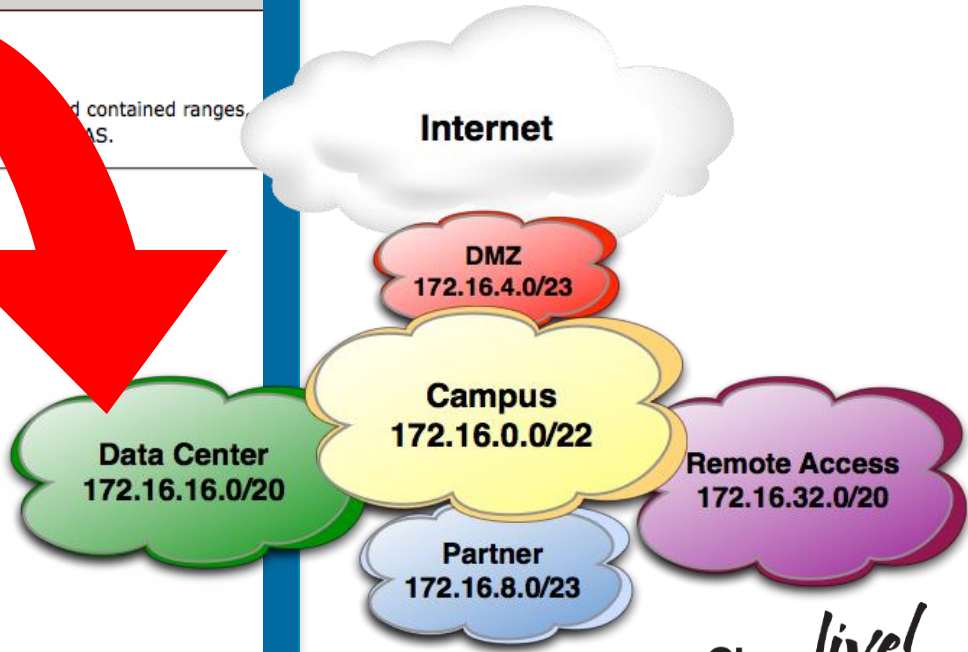
API Use Cases

Requirement	Problem	API Script Solution
Pull *all* flows for given time period	SMC ←→Flow Collector query limit	Run consecutive, small queries then concatenate
Keep SMC host groups up to date	Manual configuration, old data	Query internal source of truth, push subnet lists to host groups automatically
Look up events for a particular IP for a specific timeframe	No user attribution (yet)	Find IP and lease time from internal source of truth, query StealthWatch for related events

Network Subnets

Mapped from IPAM

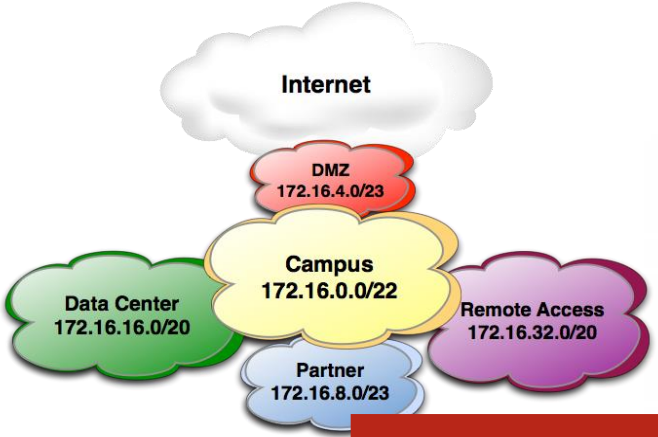


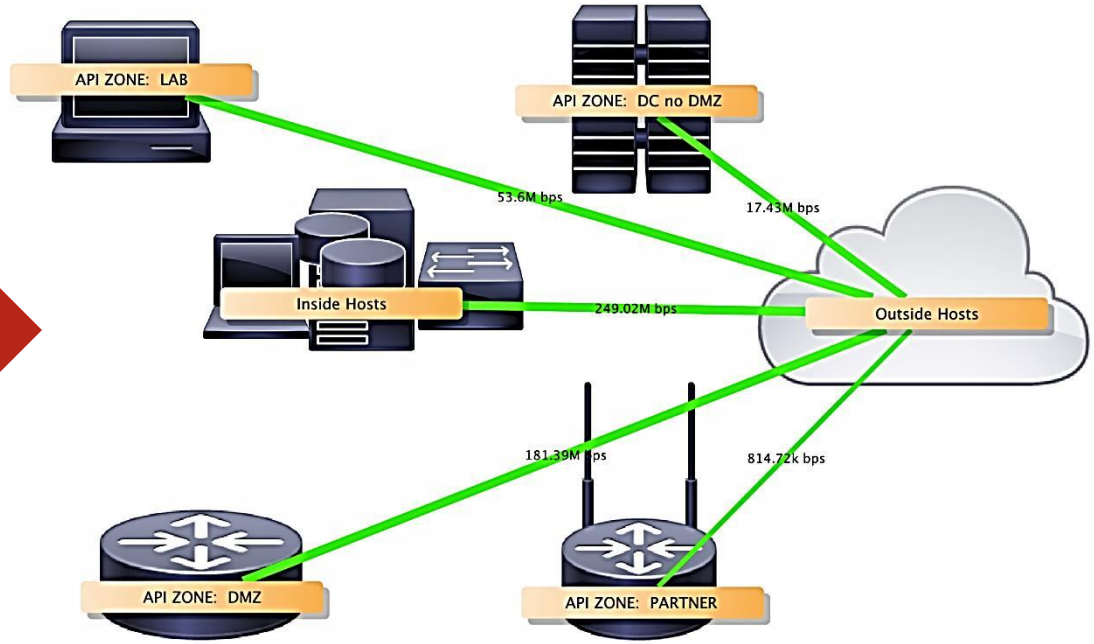


Cisco live!

Network Subnets

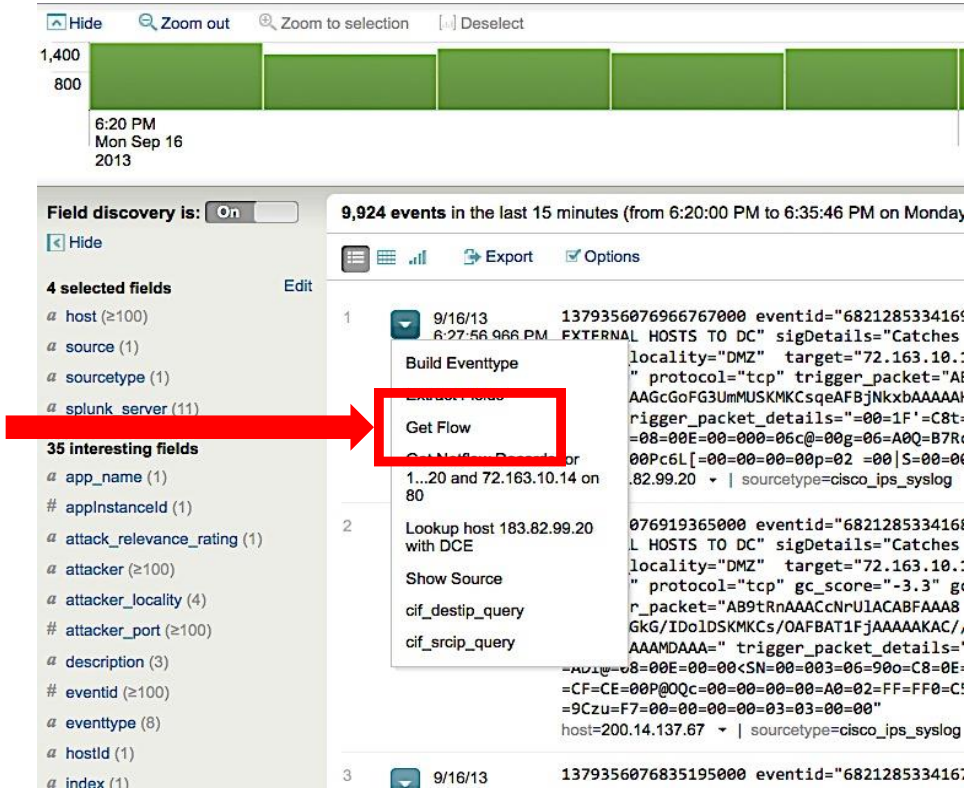
Map to Lancope Zones





Splunk Integration - GetFlows

- Find NetFlow Events via Lancope API with the respective src/dst



Splunk Integration - GetFlows

1379356076966767000 eventid="6821285334169" hostId="rcdn9-dmz-nms-1" sig_created="20000101" sig_type="other" severity="high" app_name="sensorApp" appInstanceId="25977" signature="64003" subSigid="0" description="INBOUND
EXTERNAL HOSTS TO DC" sig_version="custom" **attacker="183.82.99.20" attacker_port="51870"** attacker_locality="OUT" **target="72.163.10.14" target_port="80"** target_locality="DMZ" **target="72.163.10.10" target_port="80"** tar
target_value_rating="medium" interface="te0_1" interface_group="vs0" vlan="0" protocol="tcp" trigger_packet="AB8nyHQAACcNrUkACABF AAAwBmNAAGcGoFG3UmMUSKMKCsqeAFBjNkxbAAAAAHACIAB8UwAAAgQE7AEB B
=CA=9E=00Pc6L[=00=00=00=00p=02 =00lS=00=00=02=04=04=EC=01=01=04=02"

Flow of 183.82.99.20 from 2013-09-16 17:57:56 UTC to 2013-09-16 18:57:56 UTC

Start	End	Client IP	Client Name	Client Port	Server IP	Server Name	Server Port	Client Bytes	Server Bytes	Total Bytes
2013-09-16T18:27:56Z	**2013-09-16T18:29:46Z**	**183.82.99.20**	**183.82.99.20**	**51870**	**72.163.10.10**	**cisco-tags.cisco.com**	**80**	**39609**	**8206**	**47815**
2013-09-16T18:27:56Z	2013-09-16T18:29:46Z	183.82.99.20	183.82.99.20	51865	72.163.10.14	news-tags.cisco.com	80	42298	10206	52504
2013-09-16T18:27:56Z	2013-09-16T18:27:57Z	183.82.99.20	183.82.99.20	51856	173.37.145.8	tools2.cisco.com	80	1012	6748	7760
2013-09-16T18:27:56Z	2013-09-16T18:29:15Z	183.82.99.20	183.82.99.20	51866	72.163.10.14	news-tags.cisco.com	80	42298	0	42298
2013-09-16T18:28:22Z	2013-09-16T18:28:41Z	183.82.99.20	183.82.99.20	51941	173.37.144.208	sso-prod2.cisco.com	443	3340	5217	8557
2013-09-16T18:28:21Z	2013-09-16T18:29:43Z	183.82.99.20	183.82.99.20	51939	173.37.144.208	sso-prod2.cisco.com	80	7716	2732	10448

Download Report (CSV format)

IP Matched logs (highlighted ones are exact matches, ip and port)

Start	End	Client IP	Client Name	Client Port	Server IP	Server Name	Server Port	Client Bytes	Server Bytes	Total Bytes
2013-09-16T18:27:56Z	**2013-09-16T18:29:46Z**	**183.82.99.20**	**183.82.99.20**	**51870**	**72.163.10.10**	**cisco-tags.cisco.com**	**80**	**39609**	**8206**	**47815**
2013-09-16T18:27:56Z	2013-09-16T18:29:46Z	183.82.99.20	183.82.99.20	51865	72.163.10.14	news-tags.cisco.com	80	42298	10206	52504
2013-09-16T18:27:56Z	2013-09-16T18:29:15Z	183.82.99.20	183.82.99.20	51866	72.163.10.14	news-tags.cisco.com	80	42298	0	42298

Conclusion

Conclusion

NetFlow benefits to Incident Respons teams

- Robust data set
- Due to size and deduplication, significant retention possible
- Ability to integrate NetFlow data with other security tools leveraging API

Participate in the “My Favorite Speaker” Contest

Promote Your Favorite Speaker and You Could be a Winner

- Promote your favorite speaker through Twitter and you could win $200 of Cisco Press products (@CiscoPress)
- Send a tweet and include
  - Your favorite speaker’s Twitter handle <Speaker – enter your twitter handle here>
  - Two hashtags: #CLUS #MyFavoriteSpeaker
- You can submit an entry for more than one of your “favorite” speakers
- Don’t forget to follow @CiscoLive and @CiscoPress
- View the official rules at http://bit.ly/CLUSwin

Cisco live!

Continue Your Education

- Demos in the Cisco Campus
- Walk-in Self-Paced Labs
- Meet the Expert 1:1 meetings

Cisco live!


Q & A
Cisco live!

Complete Your Online Session Evaluation

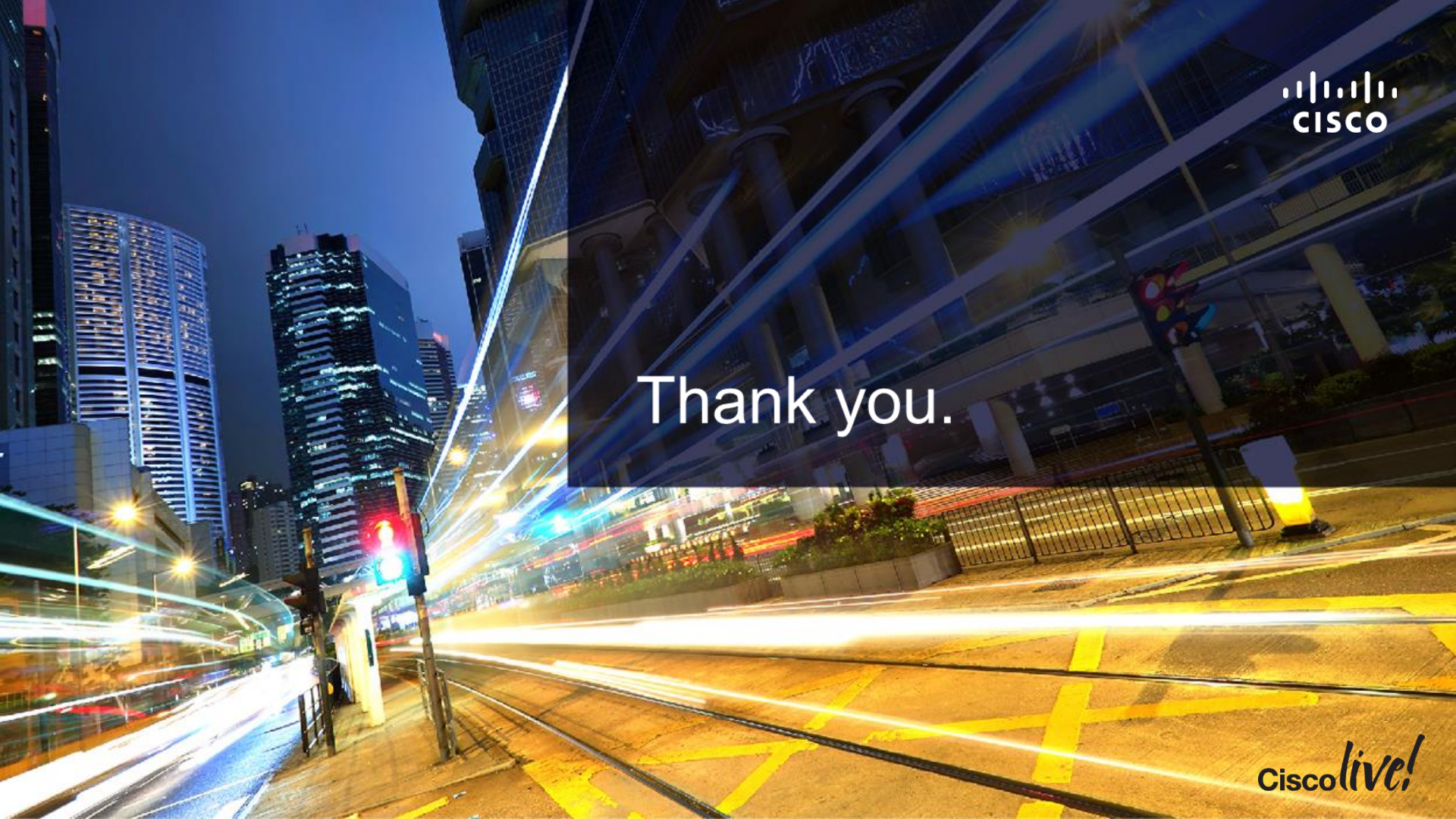
Give us your feedback and receive a Cisco Live 2015 T-Shirt!

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 http://showcase.genie-connect.com/clmelbourne2015
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected in the World of Solutions on Friday 20 March 12:00pm - 2:00pm

Learn online with Cisco Live!
Visit us online after the conference for full access to session videos and presentations. www.CiscoLiveAPAC.com


Thank you.


CISCO