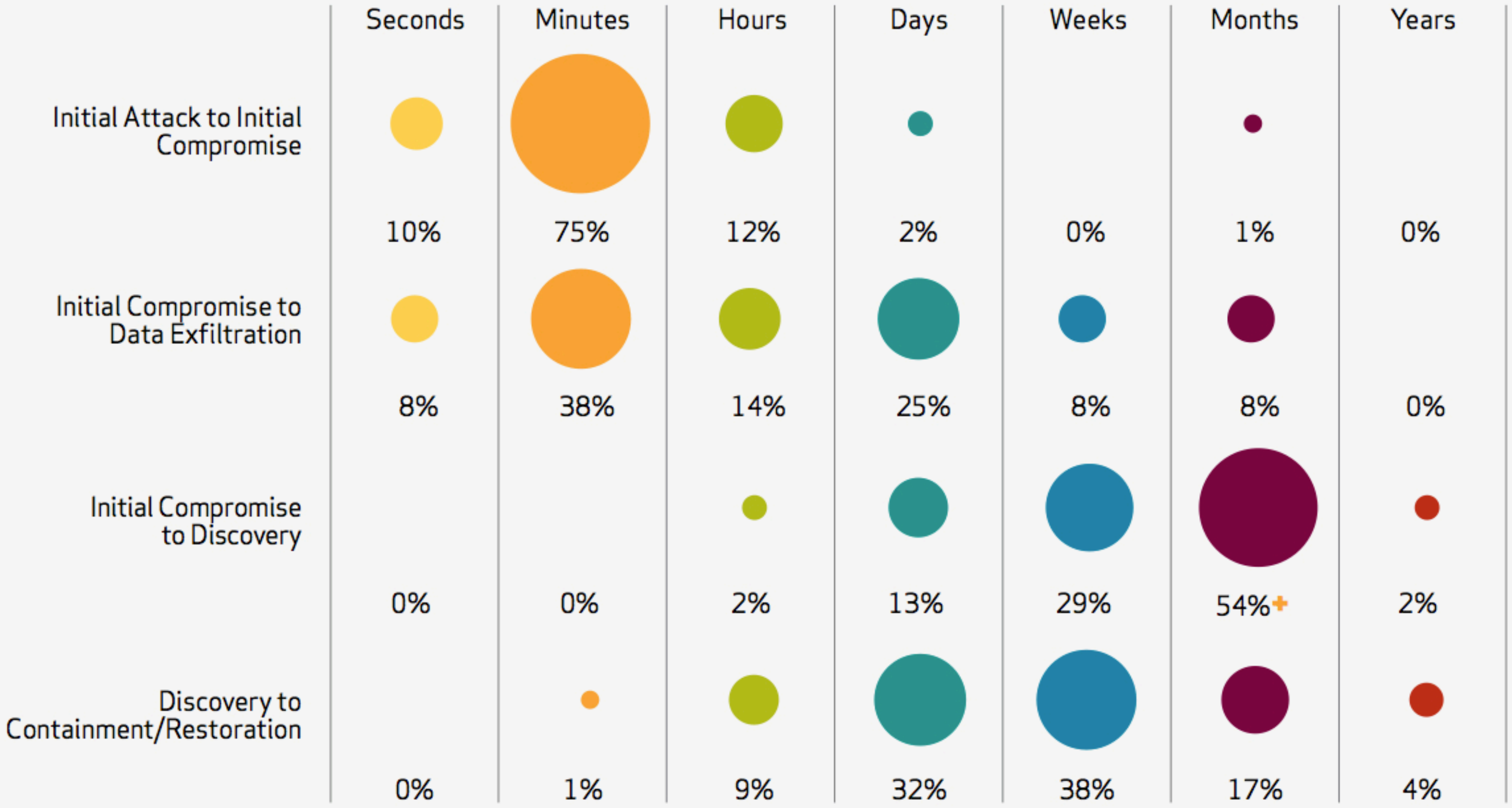
Engineering Solutions for Security Investigations and Monitoring

(Arming Security Investigators)

***Download PDF**: http://xianshield.org*

Figure 40. Timespan of events by percent of breaches



Source: 2012 Verizon Data Breach Investigations Report

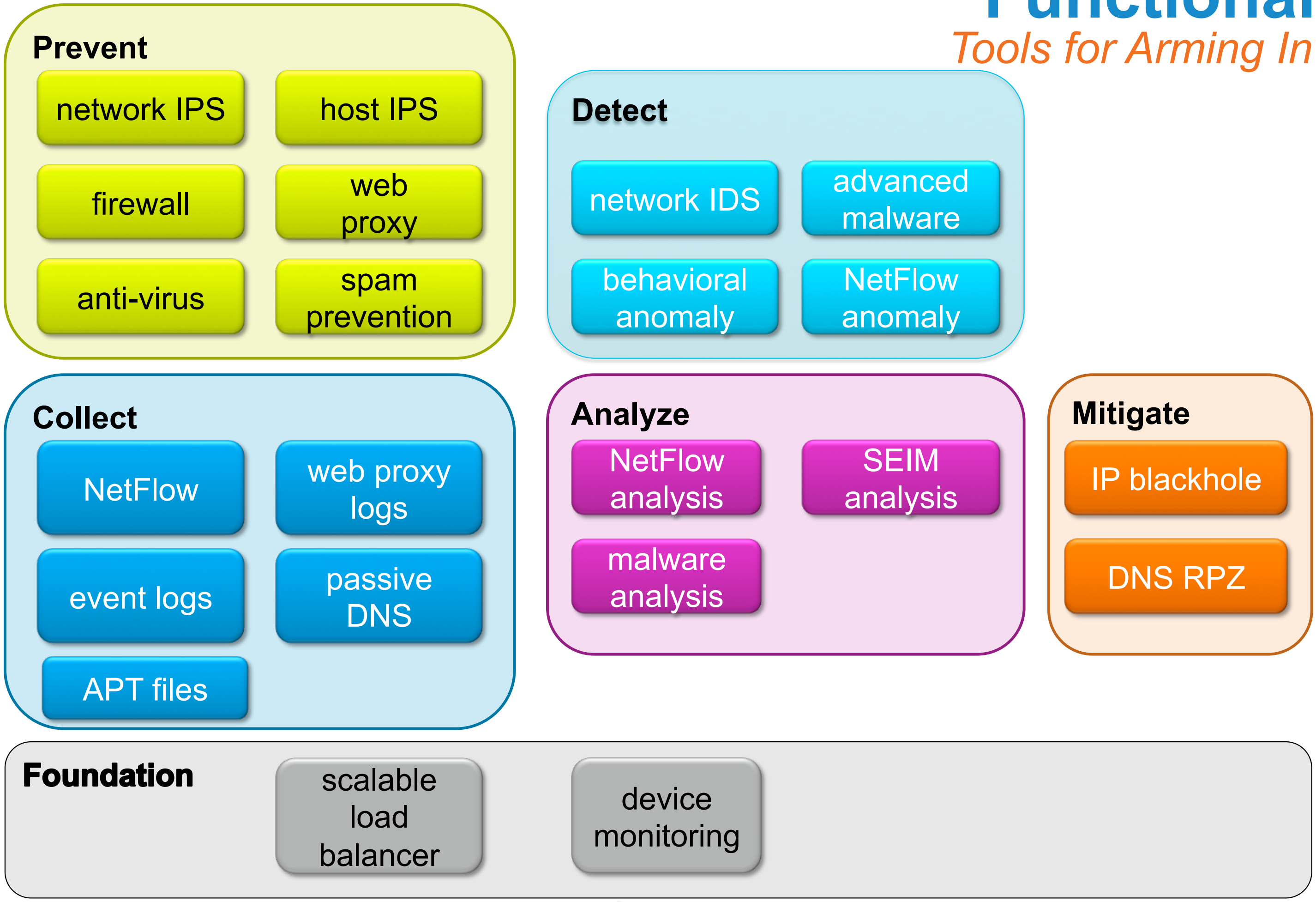
A Call to Arms

The Threat is Evolving

	2000	2005	2011	Next
Industry Posture	Unprotected desktops	Unmanaged desktops	Proliferating device types	Cloud-connected ecosystem
Malware	Worms	Rapidly changing and proliferating	Sophisticated	Beyond Windows
Network Behavior	Disruptive	Compromised hosts remotely controlled	Opaquely compromised hosts exfiltrate sensitive data	Hidden in e-mail and social networking
Threat Depth	Annoyance	Individual host	Sensitive infrastructure	Embedded
Industry Response	Deploy AV	1) Deploy HIPS 2) Detect botnets via IDS	1) Detect via reputation 2) Automate prevention 3) Detect via behavior	1) Augment detection with intel 2) Detect via precursors 3) Diversify intelligence and methods

Functional Model

Tools for Arming Investigators



Prevent

- network IPS
- host IPS
- firewall
- web proxy
- anti-virus
- spam prevention

Detect

- network IDS
- advanced malware
- behavioral anomaly
- NetFlow anomaly

Collect

- NetFlow
- web proxy logs
- event logs
- passive DNS
- APT files

Analyze

- NetFlow analysis
- SEIM analysis
- malware analysis

Mitigate

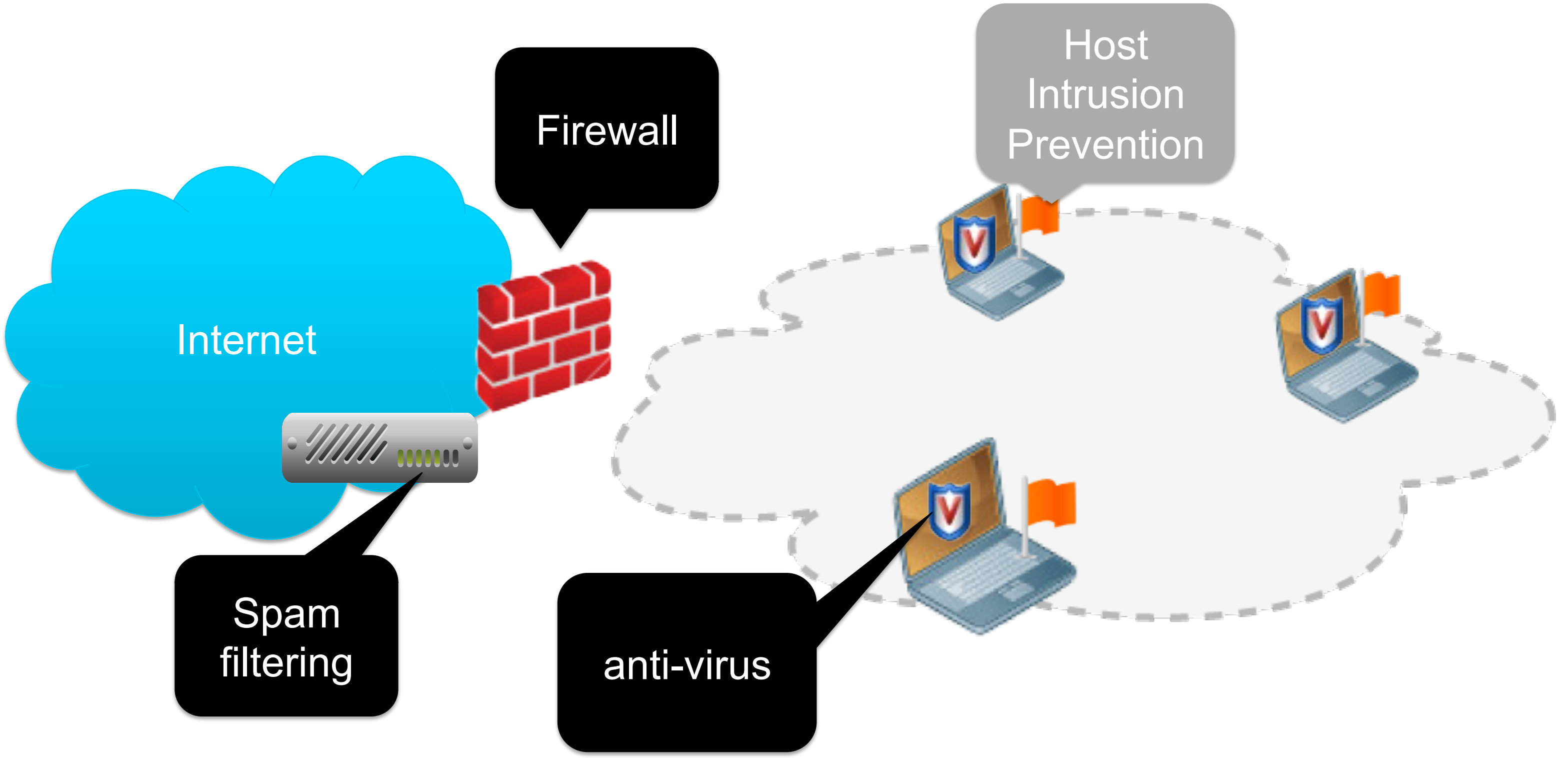
- IP blackhole
- DNS RPZ

Foundation

- scalable load balancer
- device monitoring

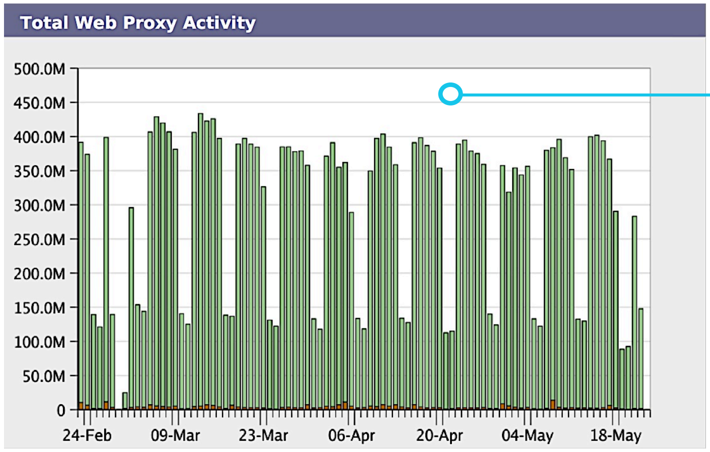
Incident Prevention

Basics



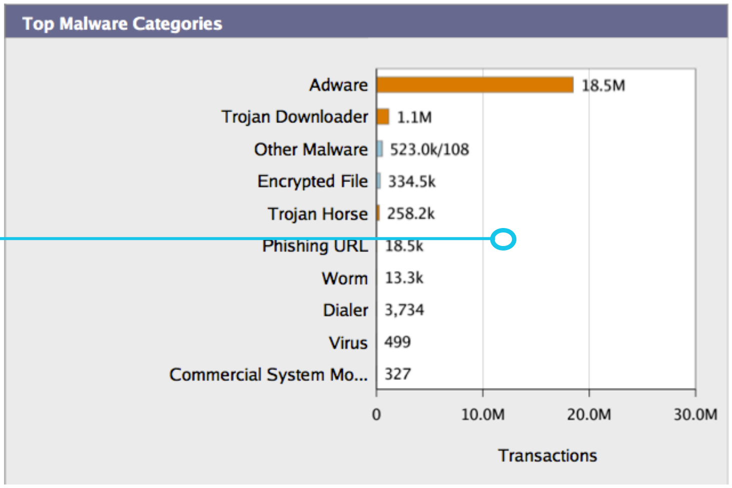
Incident Prevention: Web Proxy

WSA 90 Day Stats



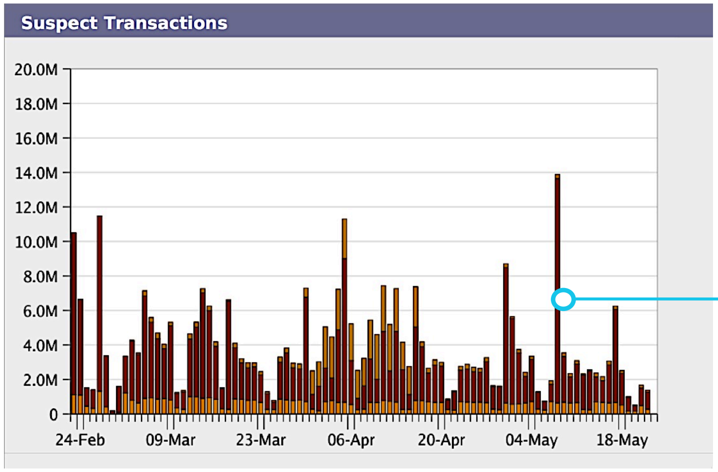
🟧 1.3% **Suspect** Transactions

🟩 98.7% **Clean** Transactions



🟦 **Monitored**

🟧 **Blocked**



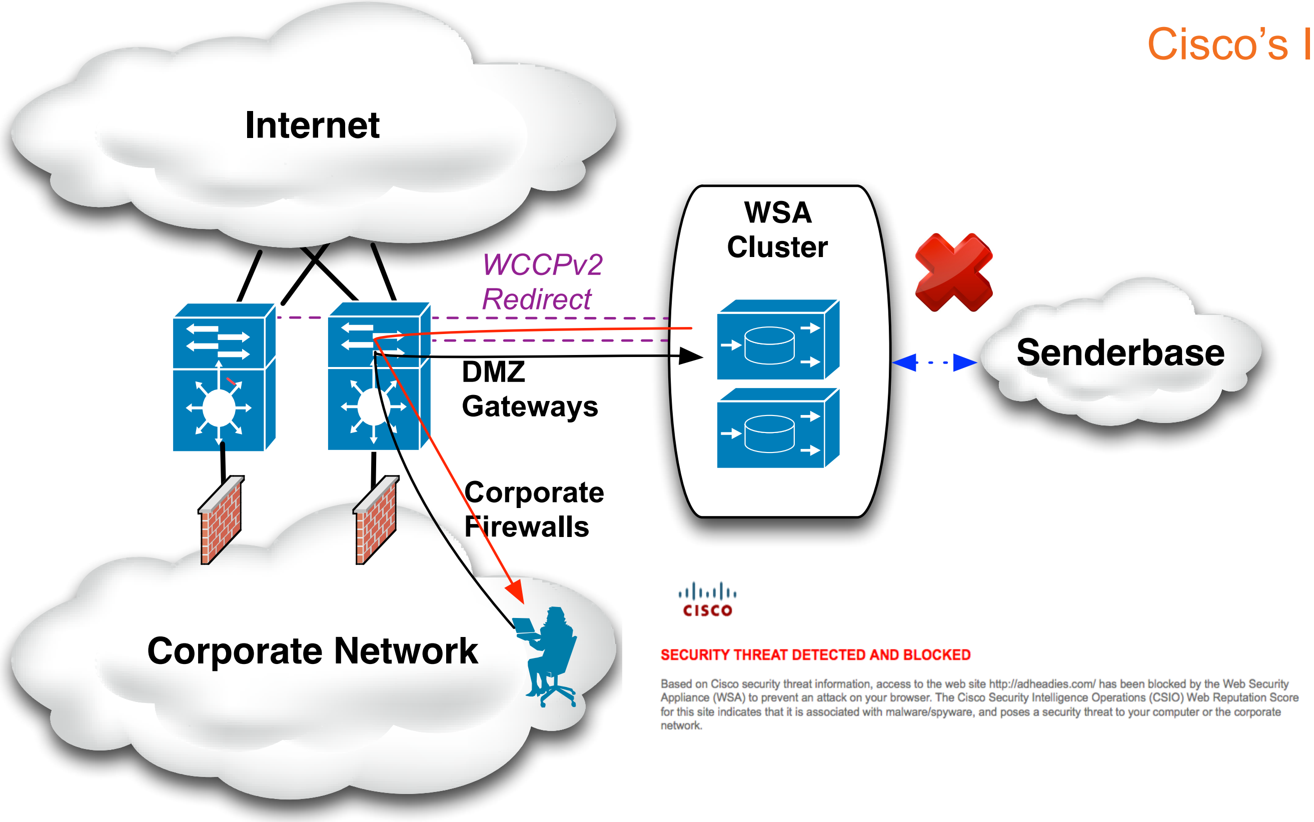
🟥 70.6% Blocked by **Web Reputation**

🟧 15.5% Detected by **Anti-Malware**

🟫 13.3% Blocked by **URL Category**

Incident Prevention: Web Proxy

Cisco's Internal WSA Deployment



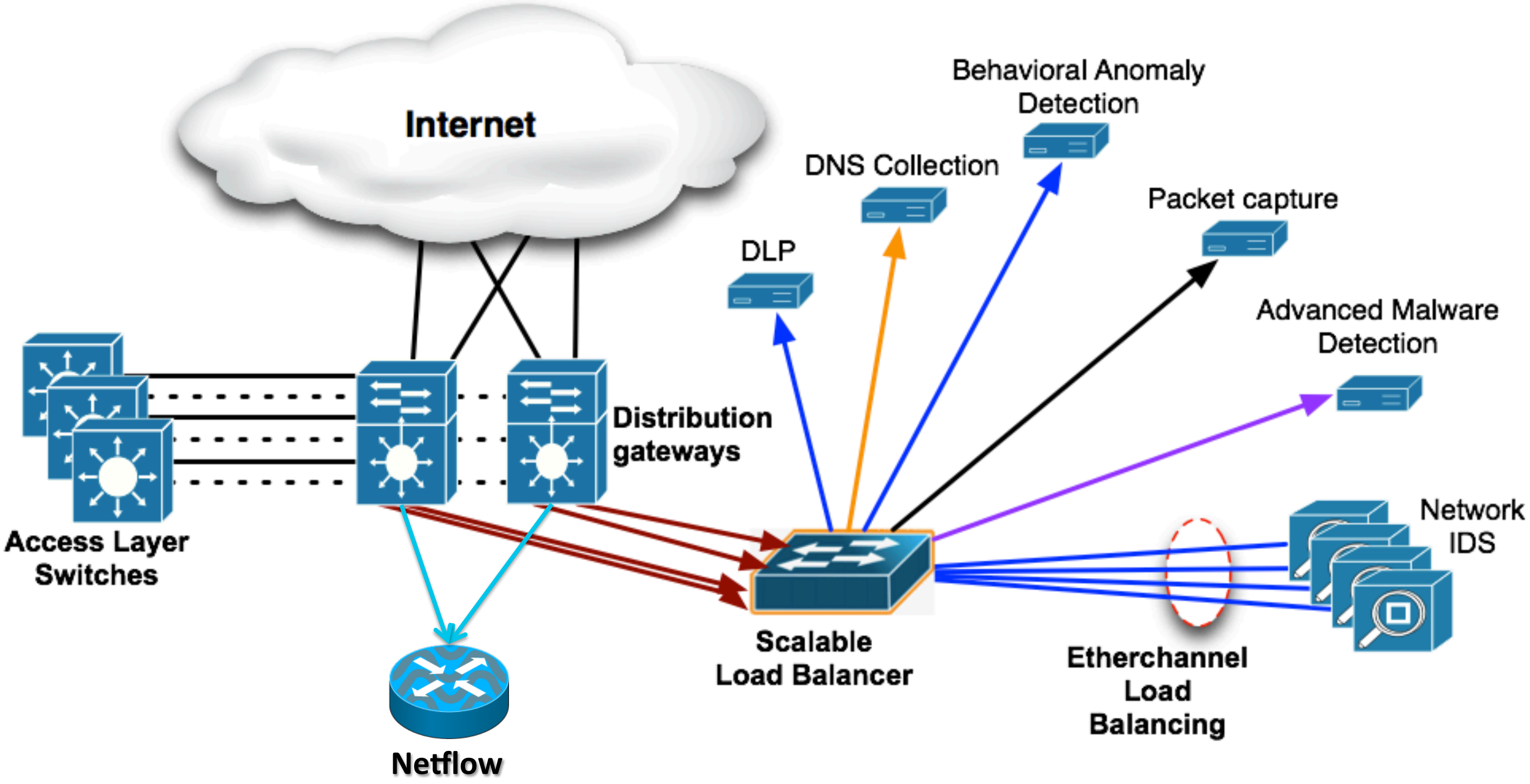
SECURITY THREAT DETECTED AND BLOCKED

Based on Cisco security threat information, access to the web site http://adheadies.com/ has been blocked by the Web Security Appliance (WSA) to prevent an attack on your browser. The Cisco Security Intelligence Operations (CSIO) Web Reputation Score for this site indicates that it is associated with malware/spyware, and poses a security threat to your computer or the corporate network.

- Position
  - – DMZ backbone gateways
  - – 2 per gateway
- Coverage
  - – Desktop
  - – Internal labs
  - – Data centers
  - – DMZ labs
  - – Remote access
- Model: S670

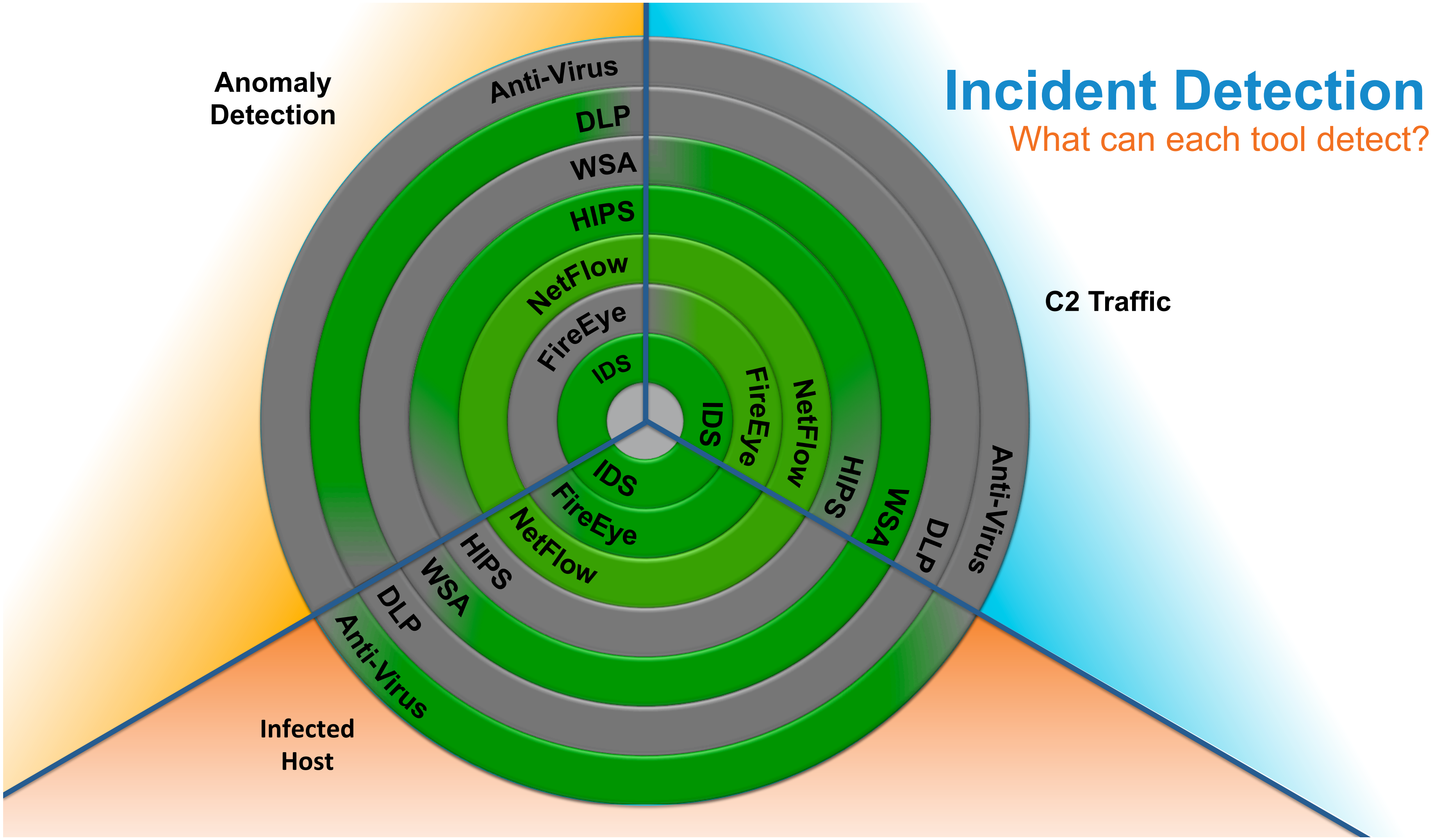
Incident Detection

Egress Detection Topology



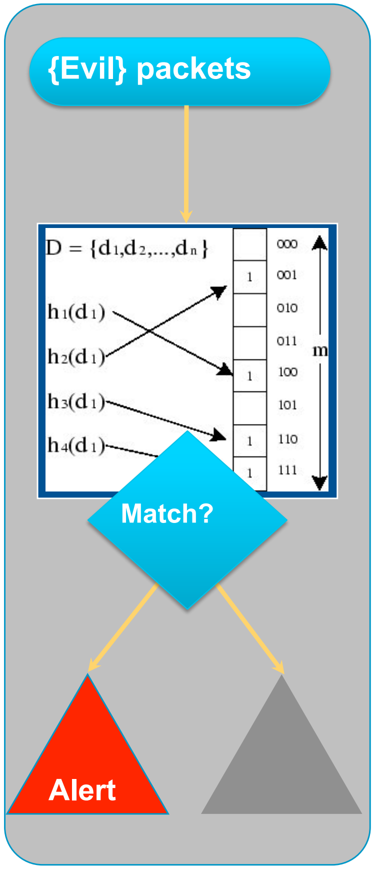
Incident Detection

What can each tool detect?



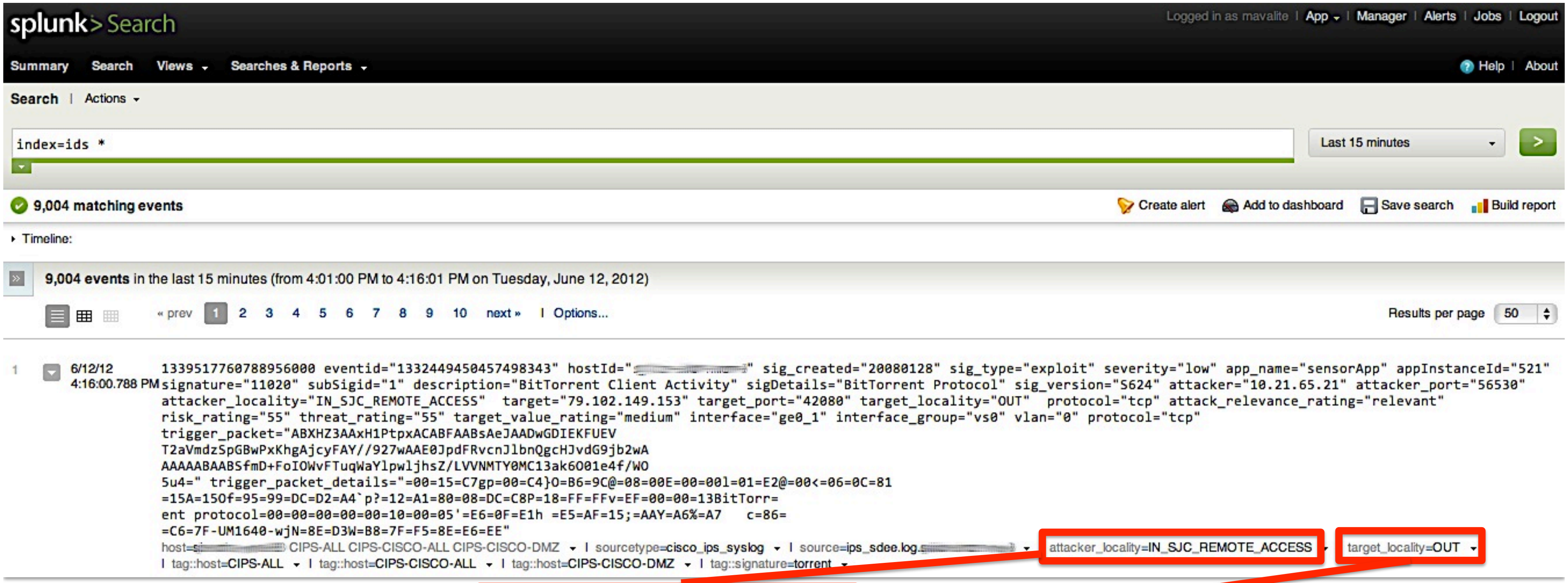
Incident Detection: Network IDS

How it Works



Incident Detection: Network IDS

Tuning Variables



```
index=ids *
```

9,004 matching events

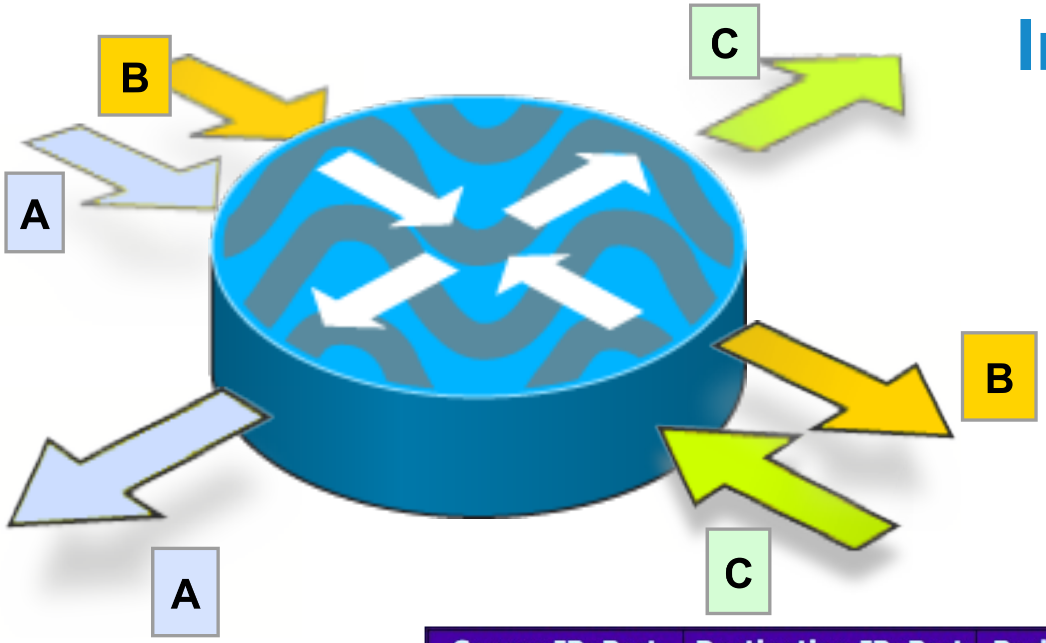
9,004 events in the last 15 minutes (from 4:01:00 PM to 4:16:01 PM on Tuesday, June 12, 2012)

```
1  6/12/12           1339517760788956000 eventid="1332449450457498343" hostId="[redacted]" sig_created="20080128" sig_type="exploit" severity="low" app_name="sensorApp" appInstanceId="521"
   4:16:00.788 PM    signature="11020" subSigid="1" description="BitTorrent Client Activity" sigDetails="BitTorrent Protocol" sig_version="S624" attacker="10.21.65.21" attacker_port="56530"
                     attacker_locality="IN_SJC_REMOTE_ACCESS"  target="79.102.149.153" target_port="42080" target_locality="OUT"  protocol="tcp" attack_relevance_rating="relevant"
                     risk_rating="55" threat_rating="55" target_value_rating="medium" interface="ge0_1" interface_group="vs0" vlan="0" protocol="tcp"
                     trigger_packet="ABXHZ3AAxH1PtpxACABFAABsAeJAADwGDIEKFUEV
                     T2aVmdzSpGBwPxKhgAjcyFAY//927wAAE0JpdFRvcnJlbnQgcHJvdG9jb2wA
                     AAAAABAABSfmD+FoIOWvFTuqWaYlpwljhsZ/LVVNMTY0MC13ak6O01e4f/WO
                     5u4=" trigger_packet_details="=00=15=C7gp=00=C4}O=B6=9C@=08=00E=00=00l=01=E2@=00<=06=0C=81
                     =15A=15Of=95=99=DC=D2=A4`p?=12=A1=80=08=DC=C8P=18=FF=FFv=EF=00=00=13BitTorr=
                     ent protocol=00=00=00=00=00=10=00=05'=E6=0F=E1h =E5=AF=15;=AAY=A6%=A7   c=86=
                     =C6=7F-UM1640-wjN=8E=D3W=B8=7F=F5=8E=E6=EE"
                     host=[redacted] CIPS-ALL CIPS-CISCO-ALL CIPS-CISCO-DMZ ▾ | sourcetype=cisco_ips_syslog ▾ | source=ips_sdee.log.[redacted] ▾  attacker_locality=IN_SJC_REMOTE_ACCESS ▾  target_locality=OUT ▾
                     | tag::host=CIPS-ALL ▾ | tag::host=CIPS-CISCO-ALL ▾ | tag::host=CIPS-CISCO-DMZ ▾ | tag::signature=torrent ▾
```

Locality variable enables context tags in IDS alerts

Incident Detection: NetFlow

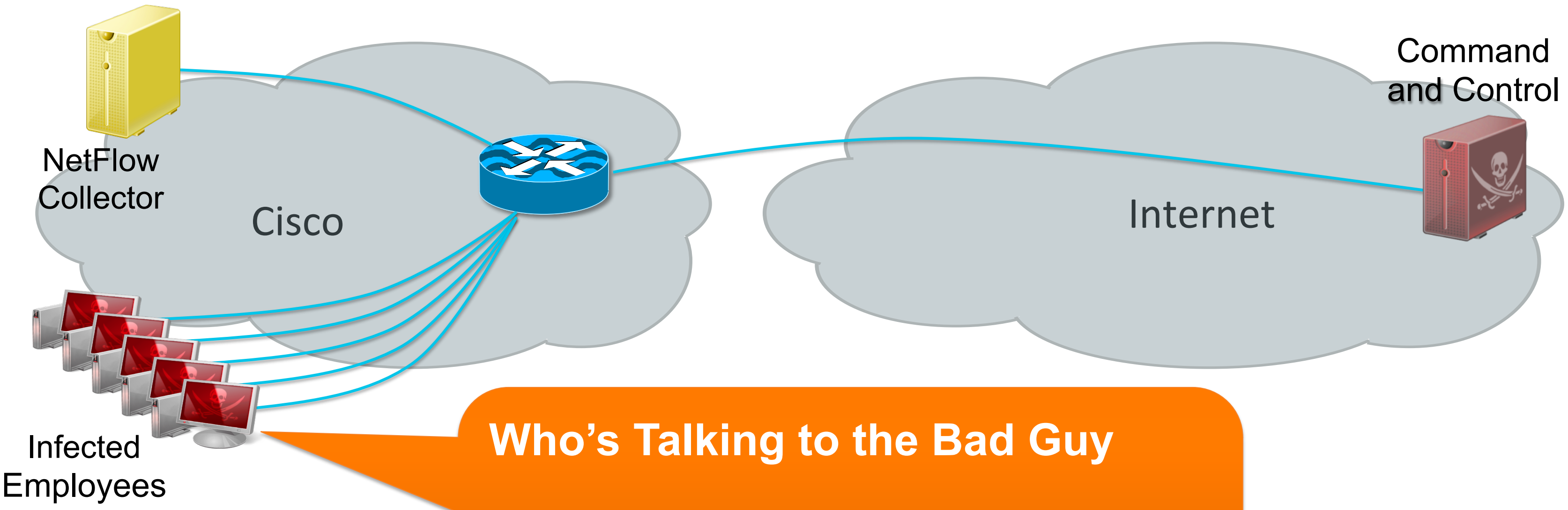
It's like a phone bill!



	Source IP: Port	Destination IP: Port	Packets	Date/Time
A	192.168.15.7:2068	211.160.17.195:8080	7	5/7/2009 8:11:13 GMT
B	192.168.21.5:1042	72.18.45.223:21	219	5/7/2009 9:00:03 GMT
C	192.168.6.22:3161	172.18.15.188:80	1	5/7/2009 9:05:16 GMT

Incident Detection: NetFlow

NetFlow Case Scenario - Botnet

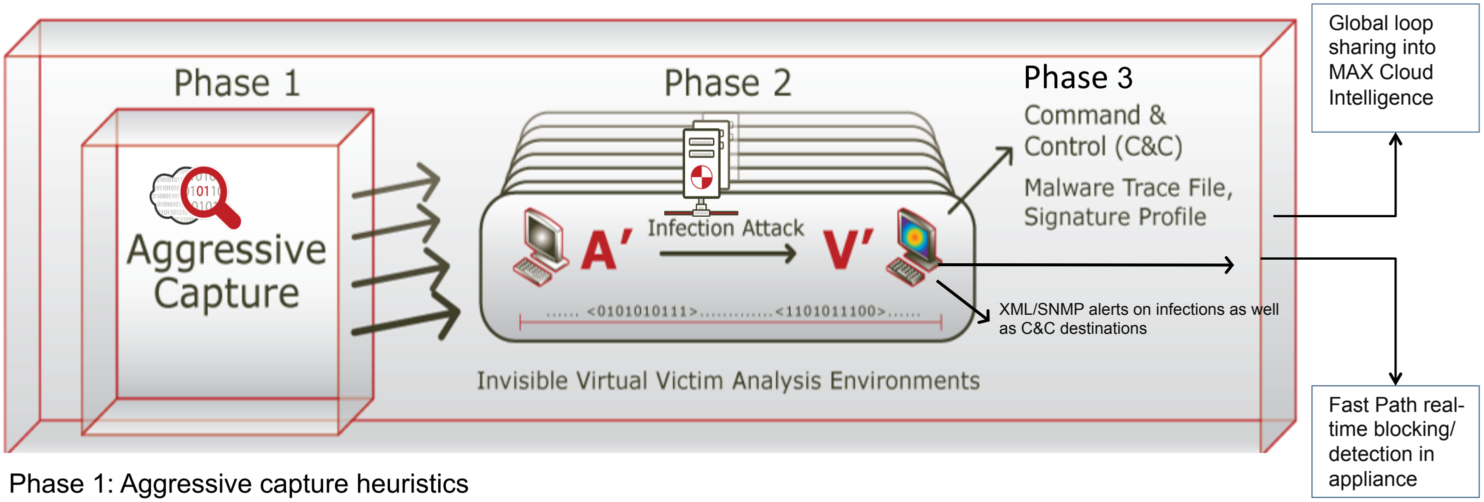


Who's Talking to the Bad Guy

Query NetFlow collectors to find all internal hosts connecting to the Command and Control server (C2)

Incident Detection: Advanced Malware

FireEye: Detecting compromised hosts


Phase 1
Aggressive Capture
Phase 2
A'
Infection Attack
V'
...... <0101010111>............<1101011100>......
Invisible Virtual Victim Analysis Environments
Phase 3
Command & Control (C&C)
Malware Trace File, Signature Profile
XML/SNMP alerts on infections as well as C&C destinations
Global loop sharing into MAX Cloud Intelligence
Fast Path real-time blocking/ detection in appliance

Phase 1: Aggressive capture heuristics

- Deploys out-of-band/passive or inline
- Multi-protocol capture of HTML, files (e.g. PDF), & EXEs
- Maximizes capture of potential zero-day attacks

Phase 2: Virtual machine analysis

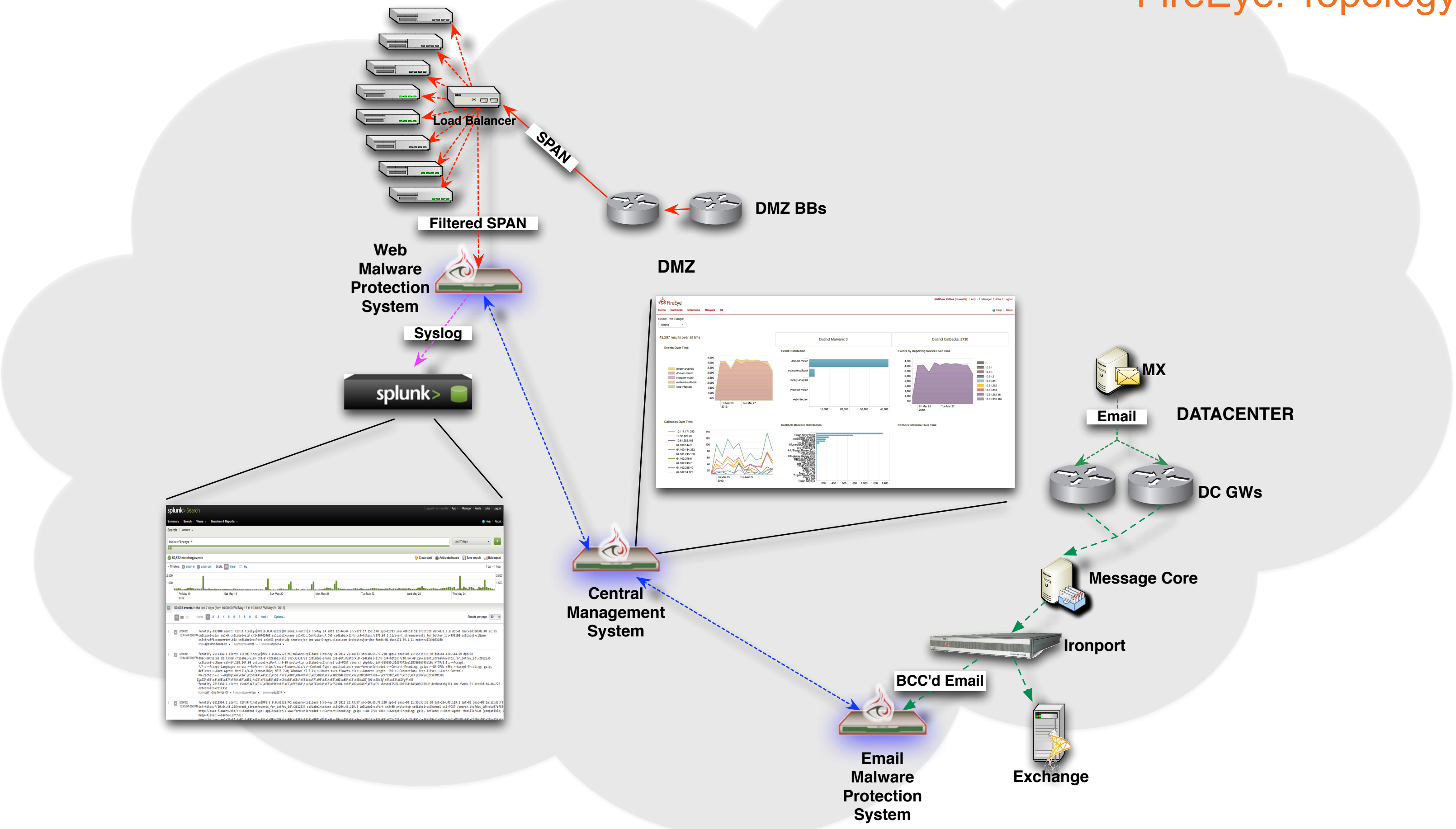
- Confirmation of malicious attacks
- Removal of false positives

Phase 3: Detect or Block Call Back (CnC)

- Stop data and asset theft

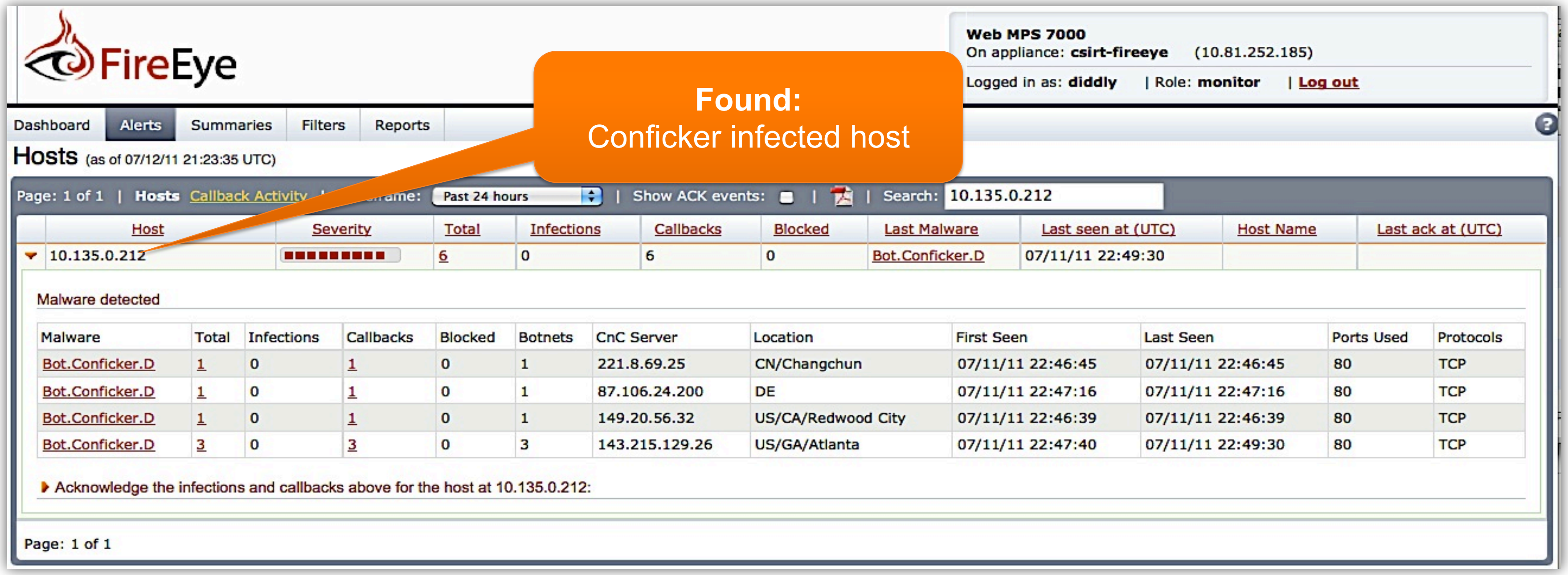
Incident Detection: Advanced Malware

FireEye: Topology



Incident Detection: Advanced Malware

FireEye Example Incident



Found:
Conficker infected host

Web MPS 7000
On appliance: csirt-fireeye (10.81.252.185)
Logged in as: diddly | Role: monitor | Log out

Hosts (as of 07/12/11 21:23:35 UTC)

Page: 1 of 1 | Hosts Callback Activity | …ame: Past 24 hours | Show ACK events: □ | | Search: 10.135.0.212

Host	Severity	Total	Infections	Callbacks	Blocked	Last Malware	Last seen at (UTC)	Host Name	Last ack at (UTC)
10.135.0.212	■■■■■■■■■■	6	0	6	0	Bot.Conficker.D	07/11/11 22:49:30		

Malware detected

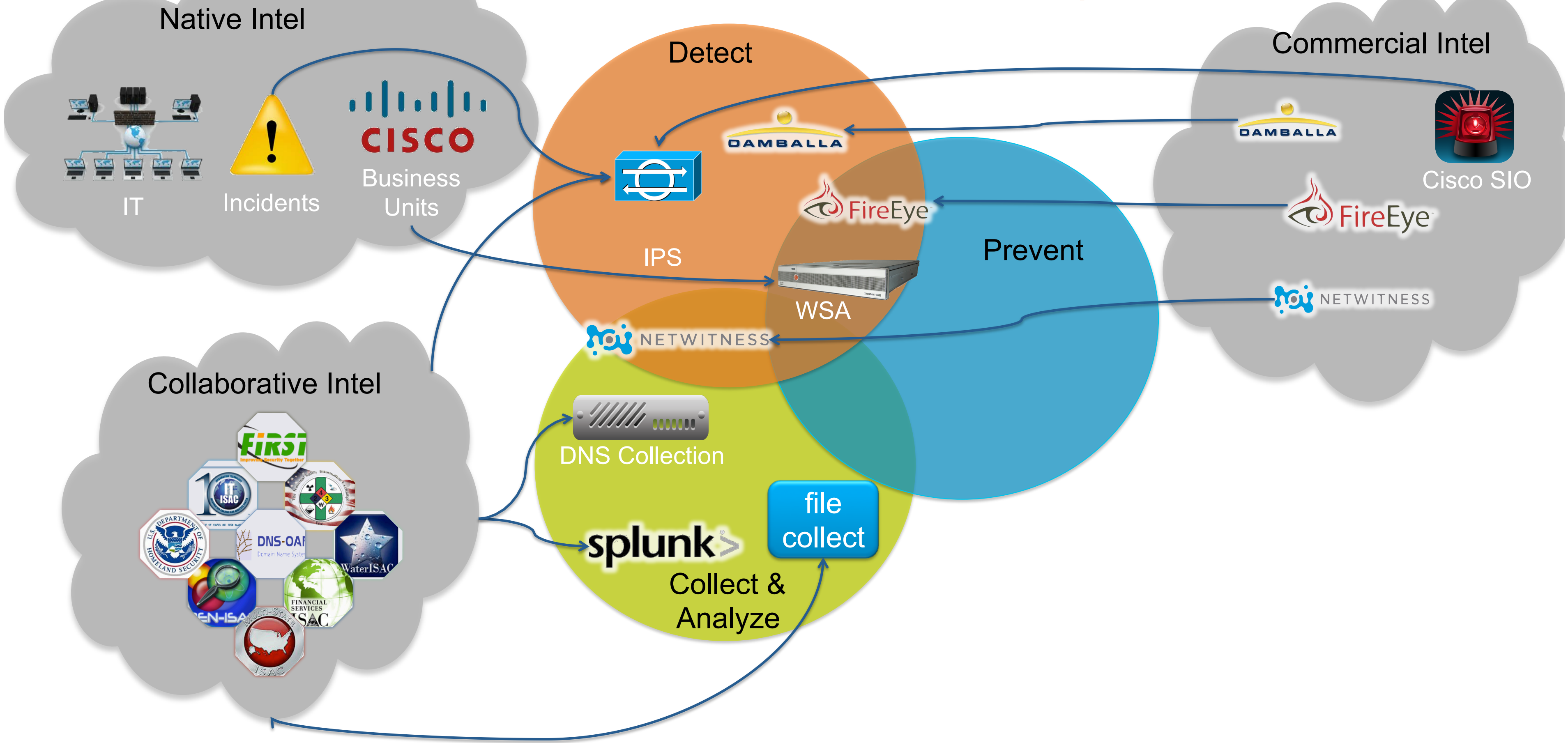
Malware	Total	Infections	Callbacks	Blocked	Botnets	CnC Server	Location	First Seen	Last Seen	Ports Used	Protocols
Bot.Conficker.D	1	0	1	0	1	221.8.69.25	CN/Changchun	07/11/11 22:46:45	07/11/11 22:46:45	80	TCP
Bot.Conficker.D	1	0	1	0	1	87.106.24.200	DE	07/11/11 22:47:16	07/11/11 22:47:16	80	TCP
Bot.Conficker.D	1	0	1	0	1	149.20.56.32	US/CA/Redwood City	07/11/11 22:46:39	07/11/11 22:46:39	80	TCP
Bot.Conficker.D	3	0	3	0	3	143.215.129.26	US/GA/Atlanta	07/11/11 22:47:40	07/11/11 22:49:30	80	TCP

Acknowledge the infections and callbacks above for the host at 10.135.0.212:

Page: 1 of 1

Incident Detection

Operational Use of Intel



Native Intel

IT

Incidents

CISCO

Business Units

Detect

IPS

DAMBALLA

FireEye

WSA

NETWITNESS

Prevent

Commercial Intel

DAMBALLA

Cisco SIO

FireEye

NETWITNESS

Collaborative Intel

FIRST

IT-ISAC

DNS-OARC

WaterISAC

FINANCIAL SERVICES ISAC

REN-ISAC

MULTI-STATE ISAC

DNS Collection

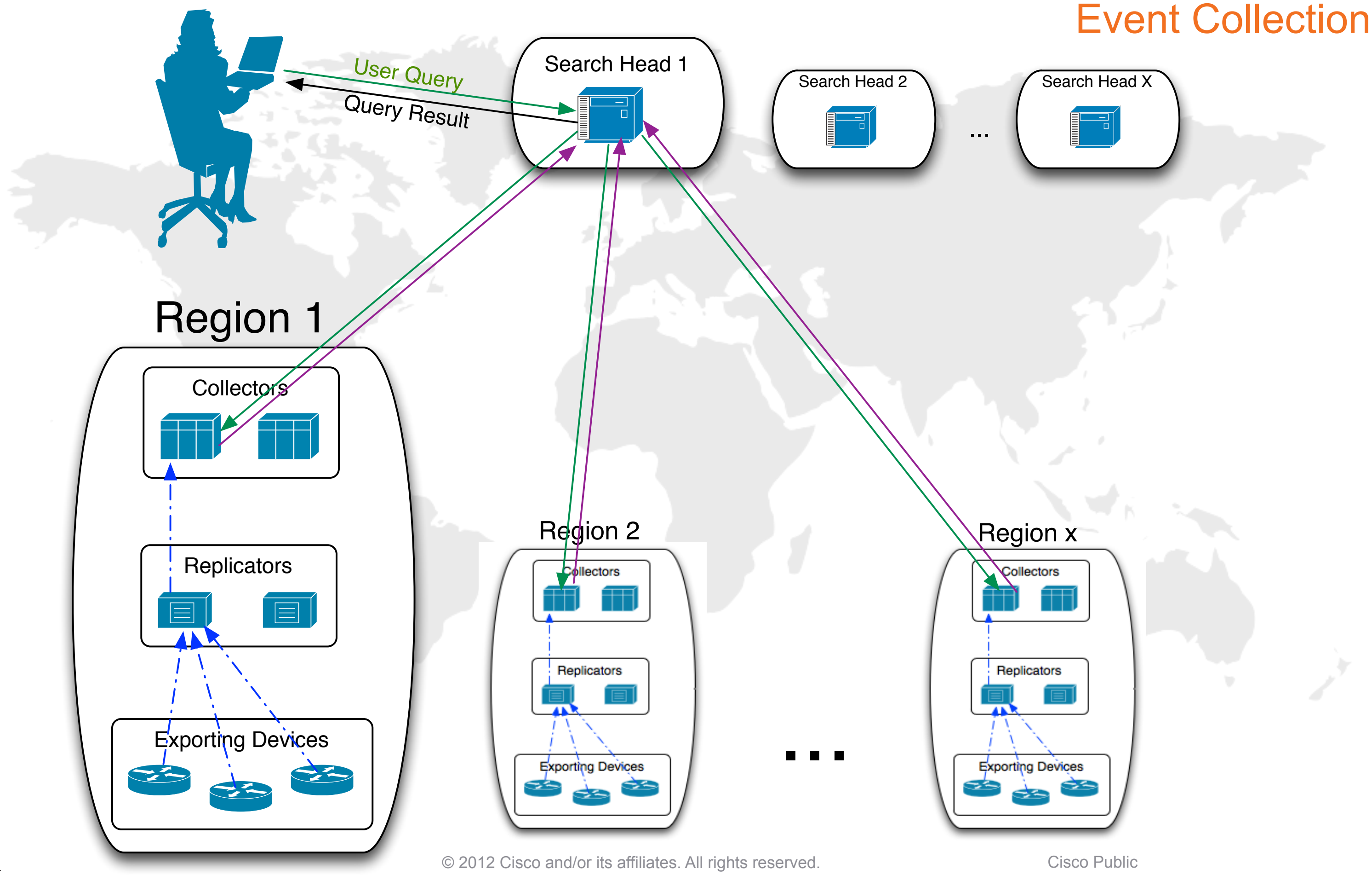
splunk>

file collect

Collect & Analyze

Collect: Architecture

Event Collection Overview



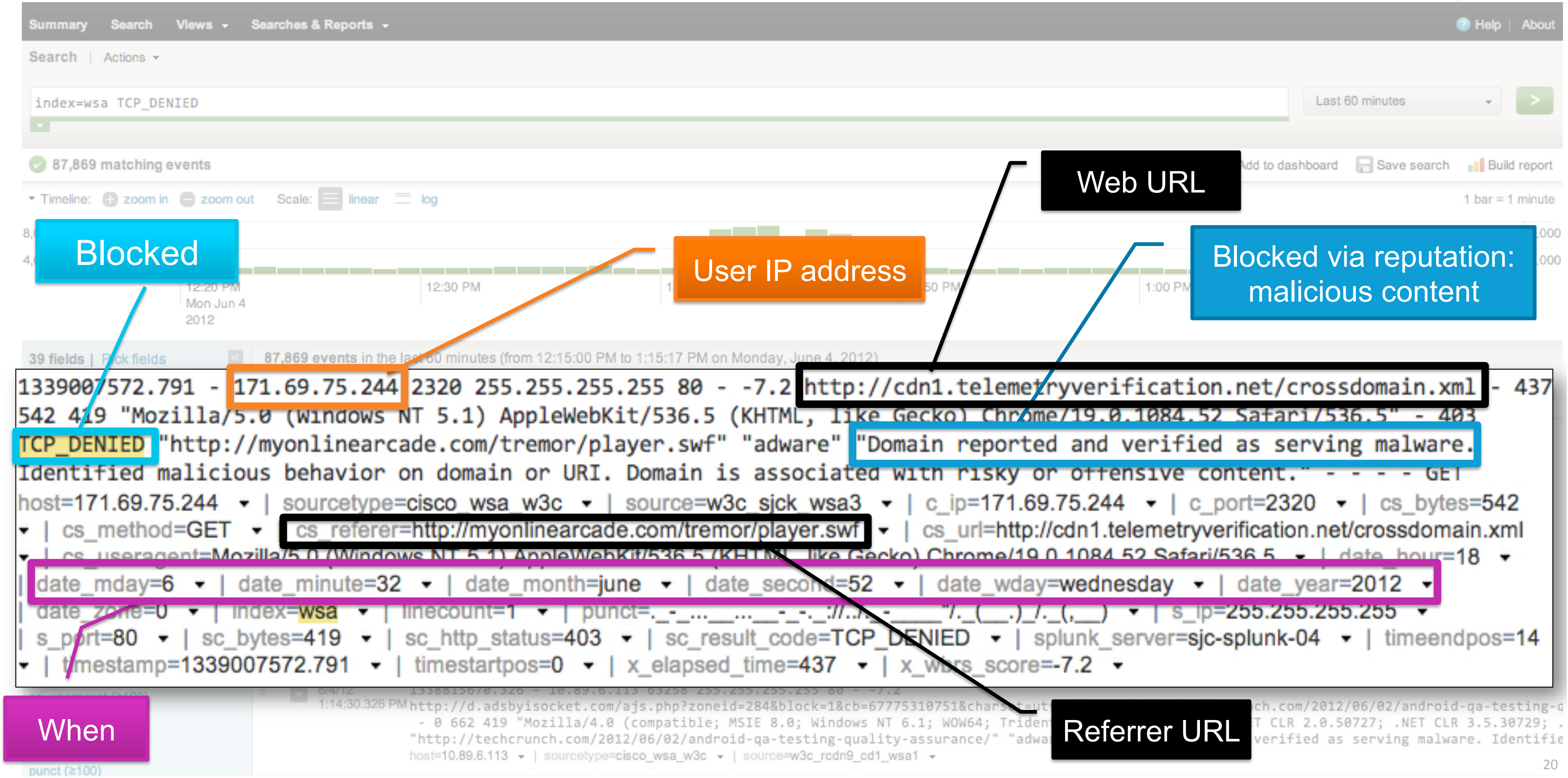
Collect:Event Logs

Types of Events to Collect

Event Type	Source	Events
Attribution	DHCP server	IP assignments to machine, MAC address
	VPN server	IP assignments to user, WAN address
	NAT gateway	IP assignment translation to RFC 1918
	802.1x auth	IP assignment to user, MAC address
System activity	Server or device syslog	• Authentication/authorization • Services starting/stopping • Config changes • Security events (Tripwire, etc.)
Web proxy logs	Web proxies	Web malware downloads, C2 check-ins
Spam filter logs	Spam filter (ESA, etc.)	Malicious URLs, malicious attachments
Web server logs	Web servers	Access logs, Error logs

Collect: WSA

Collection into Splunk



```
index=wsa TCP_DENIED
```

```
1339007572.791 - 171.69.75.244 2320 255.255.255.255 80 - -7.2 http://cdn1.telemetryverification.net/crossdomain.xml - 437
542 419 "Mozilla/5.0 (Windows NT 5.1) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.52 Safari/536.5" - 403
TCP_DENIED "http://myonlinearcade.com/tremor/player.swf" "adware" "Domain reported and verified as serving malware.
Identified malicious behavior on domain or URI. Domain is associated with risky or offensive content." - - - - GET
host=171.69.75.244 | sourcetype=cisco_wsa_w3c | source=w3c_sjck_wsa3 | c_ip=171.69.75.244 | c_port=2320 | cs_bytes=542
| cs_method=GET | cs_referer=http://myonlinearcade.com/tremor/player.swf | cs_url=http://cdn1.telemetryverification.net/crossdomain.xml
| cs_useragent=Mozilla/5.0 (Windows NT 5.1) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.52 Safari/536.5 | date_hour=18
| date_mday=6 | date_minute=32 | date_month=june | date_second=52 | date_wday=wednesday | date_year=2012
| date_zone=0 | index=wsa | linecount=1 | punct=._-_..._..._-_-._://../.-_____"/._(__)_/._(,__) | s_ip=255.255.255.255
| s_port=80 | sc_bytes=419 | sc_http_status=403 | sc_result_code=TCP_DENIED | splunk_server=sjc-splunk-04 | timeendpos=14
| timestamp=1339007572.791 | timestartpos=0 | x_elapsed_time=437 | x_wbrs_score=-7.2
```

```
6/4/12 1338815670.326 - 10.89.6.113 63258 255.255.255.255 80 - -7.2
1:14:30.326 PM http://d.adsbyisocket.com/ajs.php?zoneid=284&block=1&cb=67775310751&charset=ut ... ch.com/2012/06/02/android-qa-testing-q
 - 0 662 419 "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Triden ... T CLR 2.0.50727; .NET CLR 3.5.30729; .
"http://techcrunch.com/2012/06/02/android-qa-testing-quality-assurance/" "adwa ... verified as serving malware. Identifie
host=10.89.6.113 | sourcetype=cisco_wsa_w3c | source=w3c_rcdn9_cd1_wsa1
```

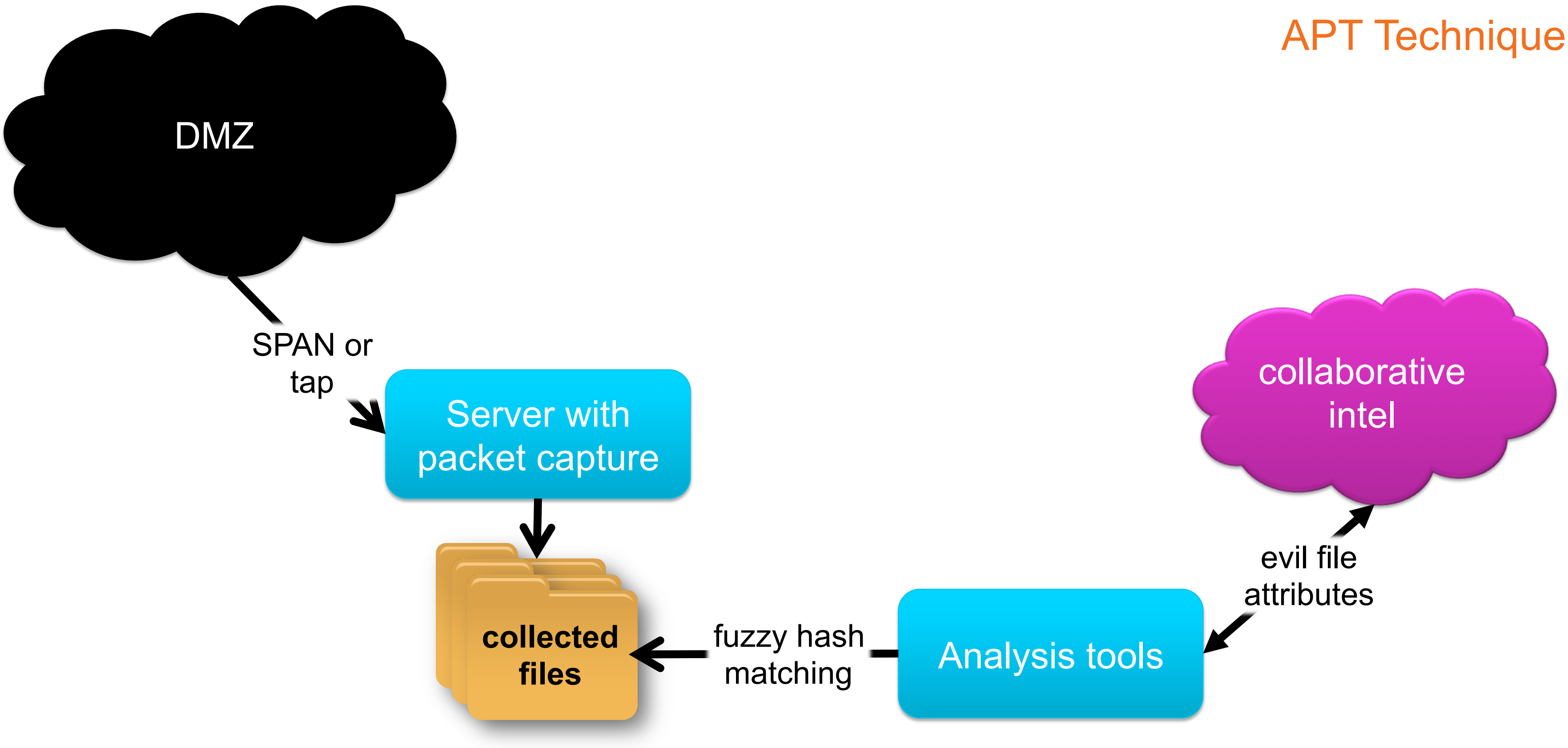
Collect: DNS

How Queries Work

```
[diddly@kujo-prod02 ~]$ /dns/questions/search --qname xianshield.org --max-results=20
ts                                src                                         dst                   qname             qtype
2012-06-12 15:32:18.204666+00:00  10.150.32.162                               64.102.6.247          xianshield.org        A
2012-06-12 15:32:18.205428+00:00  2001:420:210d:0:20f:20ff:fe96:ffb9          2001:500:40::1        xianshield.org        A
2012-06-12 15:32:19.005644+00:00  2001:420:210d:0:20f:20ff:fe96:ffb9          2001:500:c::1         xianshield.org        A
2012-06-12 15:32:19.209020+00:00  10.150.32.162                               64.102.6.247          xianshield.org        A
2012-06-12 15:32:19.806379+00:00  2001:420:210d:0:20f:20ff:fe96:ffb9          2001:500:e::1         xianshield.org        A
2012-06-12 15:32:20.606738+00:00  64.102.6.173                                199.249.120.1         xianshield.org        A
2012-06-12 15:32:20.666796+00:00  64.102.6.173                                217.160.83.147        xianshield.org        A
2012-06-12 15:32:20.606136+00:00  64.102.6.173                                199.249.120.1         xianshield.org        A
2012-06-12 15:32:20.606159+00:00  64.102.6.173                                199.249.120.1         xianshield.org        A
2012-06-12 15:32:20.666183+00:00  64.102.6.173                                217.160.83.147        xianshield.org        A
2012-06-12 15:32:20.666190+00:00  64.102.6.173                                217.160.83.147        xianshield.org        A
Search: 100% |#######################################################| Time: 0:00:07 Files:  720/720
```

Collect: Files

APT Technique



DMZ

SPAN or tap

Server with packet capture

collected files

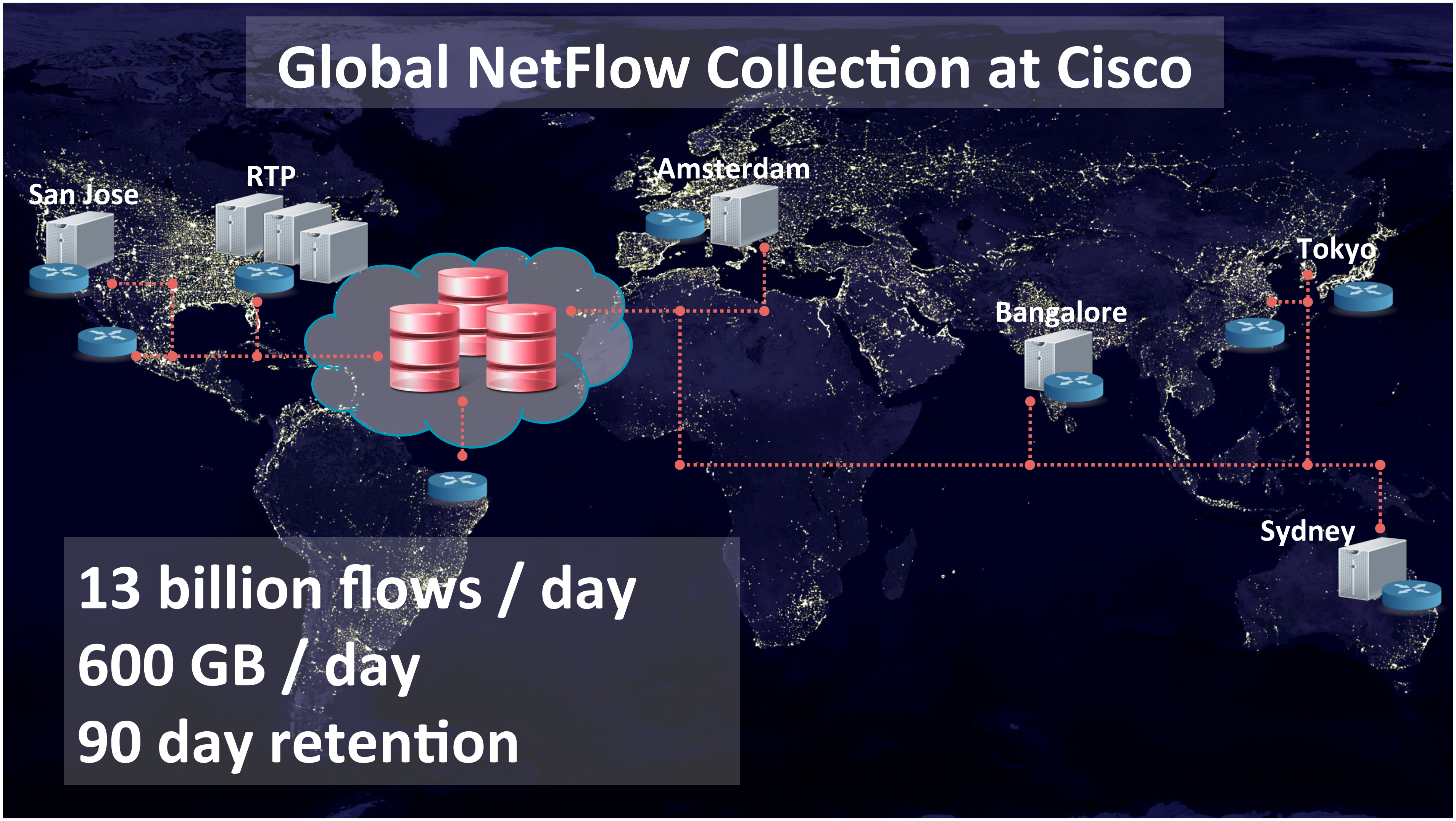
fuzzy hash matching

Analysis tools

evil file attributes

collaborative intel

Global NetFlow Collection at Cisco



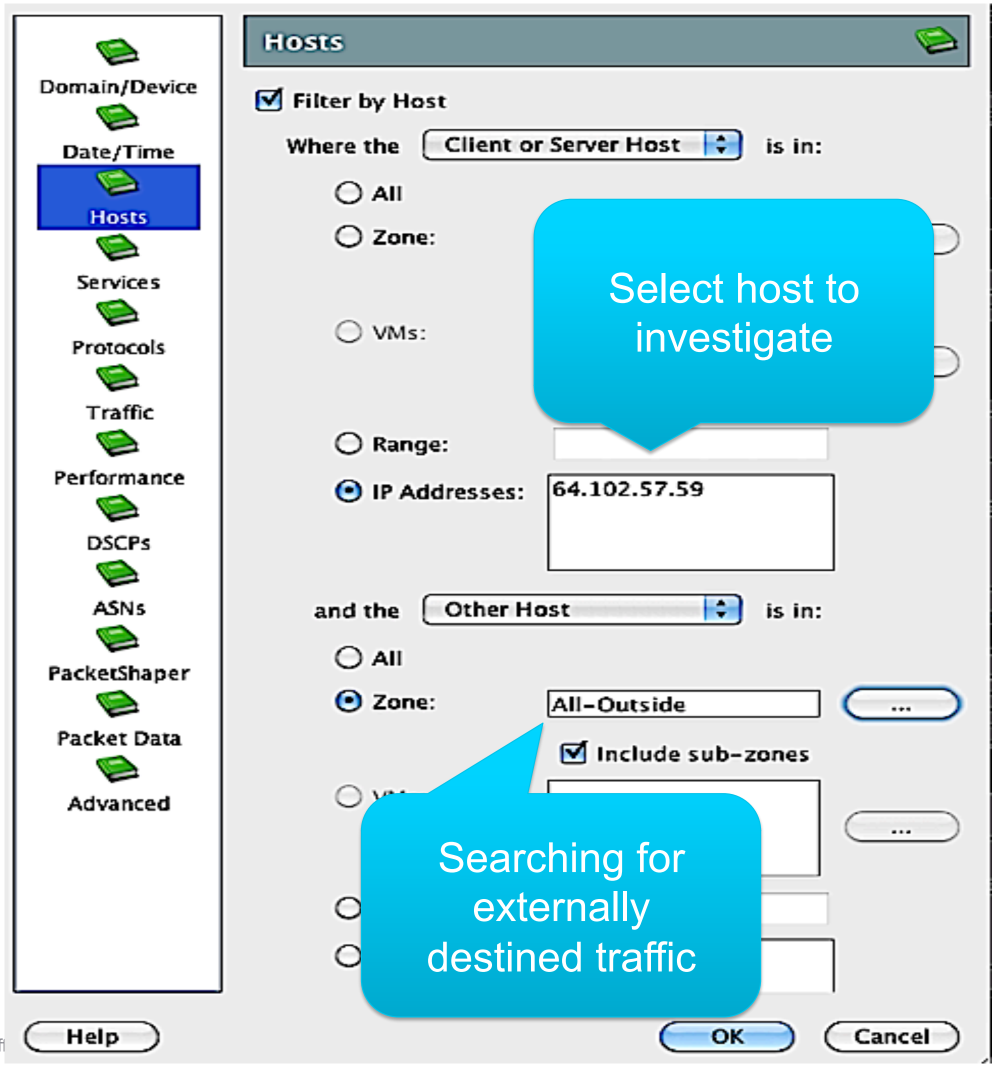
13 billion flows / day

600 GB / day

90 day retention

Analyze: NetFlow

Lancope – Flow Query



☑ Filter by Host

Where the Client or Server Host is in:

○ All
○ Zone:
○ VMs:
○ Range:
● IP Addresses: 64.102.57.59

and the Other Host is in:

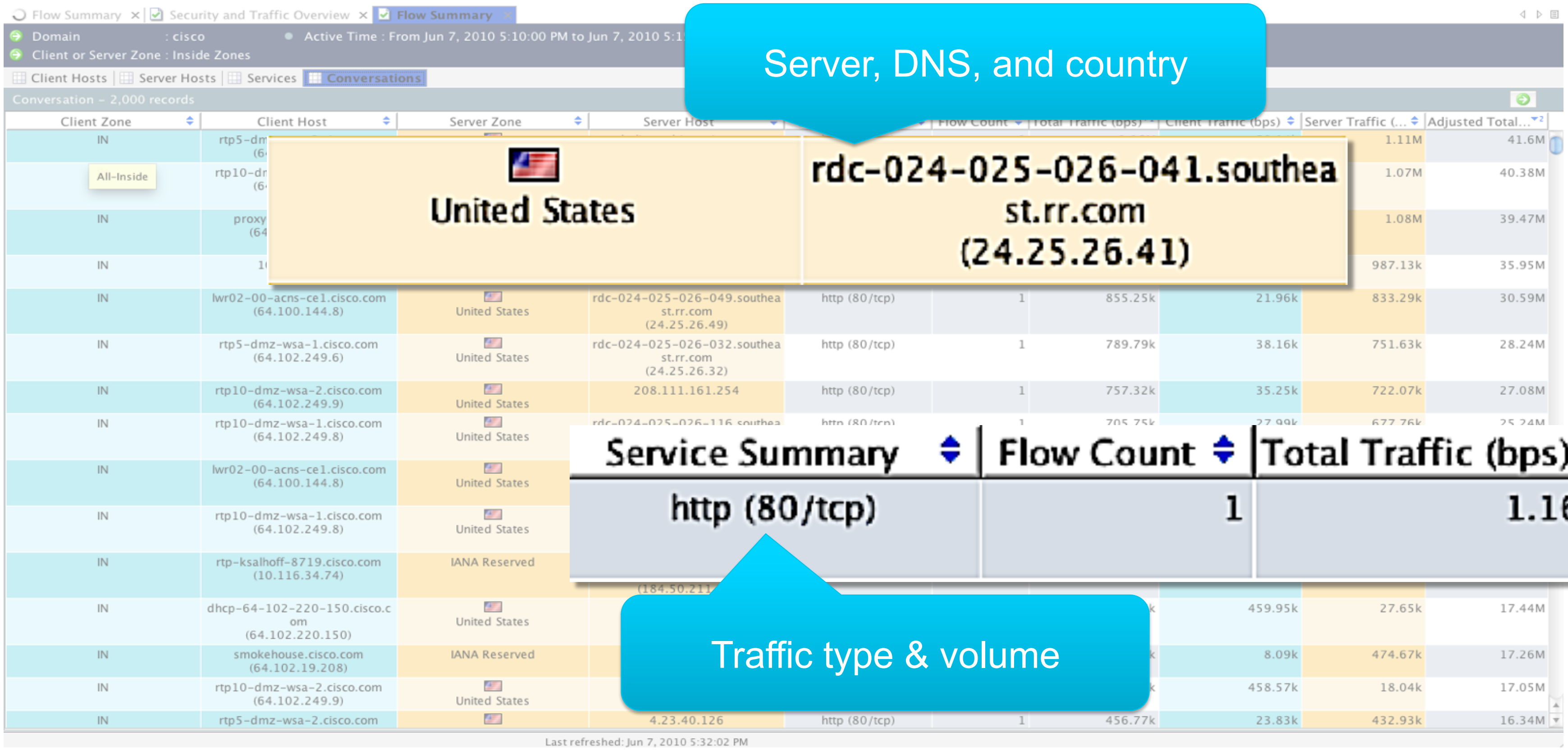
○ All
● Zone: All-Outside
☑ Include sub-zones

Select host to investigate

Searching for externally destined traffic

Analyze: NetFlow

Lancope – Flow Query Results



Flow Summary | Security and Traffic Overview | Flow Summary

Domain : cisco
Active Time : From Jun 7, 2010 5:10:00 PM to Jun 7, 2010 5:1
Client or Server Zone : Inside Zones

Client Hosts | Server Hosts | Services | Conversations

Conversation – 2,000 records

Client Zone	Client Host	Server Zone	Server Host		Flow Count	Total Traffic (bps)	Client Traffic (bps)	Server Traffic (...	Adjusted Total...
IN	rtp5-dm (6							1.11M	41.6M
All-Inside	rtp10-dr (6							1.07M	40.38M
IN	proxy (64							1.08M	39.47M
IN	1(							987.13k	35.95M
IN	lwr02-00-acns-ce1.cisco.com (64.100.144.8)	United States	rdc-024-025-026-049.southeast.rr.com (24.25.26.49)	http (80/tcp)	1	855.25k	21.96k	833.29k	30.59M
IN	rtp5-dmz-wsa-1.cisco.com (64.102.249.6)	United States	rdc-024-025-026-032.southeast.rr.com (24.25.26.32)	http (80/tcp)	1	789.79k	38.16k	751.63k	28.24M
IN	rtp10-dmz-wsa-2.cisco.com (64.102.249.9)	United States	208.111.161.254	http (80/tcp)	1	757.32k	35.25k	722.07k	27.08M
IN	rtp10-dmz-wsa-1.cisco.com (64.102.249.8)	United States	rdc-024-025-026-116.southea	http (80/tcp)	1	705.75k	27.99k	677.76k	25.24M
IN	lwr02-00-acns-ce1.cisco.com (64.100.144.8)	United States							
IN	rtp10-dmz-wsa-1.cisco.com (64.102.249.8)	United States							
IN	rtp-ksalhoff-8719.cisco.com (10.116.34.74)	IANA Reserved	(184.50.211						
IN	dhcp-64-102-220-150.cisco.com (64.102.220.150)	United States				k	459.95k	27.65k	17.44M
IN	smokehouse.cisco.com (64.102.19.208)	IANA Reserved				k	8.09k	474.67k	17.26M
IN	rtp10-dmz-wsa-2.cisco.com (64.102.249.9)	United States				k	458.57k	18.04k	17.05M
IN	rtp5-dmz-wsa-2.cisco.com		4.23.40.126	http (80/tcp)	1	456.77k	23.83k	432.93k	16.34M

Last refreshed: Jun 7, 2010 5:32:02 PM

Server, DNS, and country

United States	rdc-024-025-026-041.southeast.rr.com (24.25.26.41)

Service Summary	Flow Count	Total Traffic (bps)
http (80/tcp)	1	1.16M

Traffic type & volume

Analyze: Splunk

Power of Scripting

```
index="wsa" x_wbrs_threat_type="" (NOT (cs_referer="")) [search
index="csa" "attempted to initiate a connection as a client on TCP port 80 "allowed" |
        rex "on TCP port 80 to (?<csa_dst_ip>\d+\.\d+\.\d+\.\d+) using" |
        dedup csa_dst_ip |
        rename csa_dst_ip AS s_ip |
        fields s_ip] |
rex field=cs_url "http:\/\/(?<domain>)” |
rex field=cs_url "\/(?<script_name>[^\/?]+) (?=$|?)” |
dedup script_name |
dedup domain |
dedup c_ip |
dedup cs_url |
dedup cs_useragent
```

Searches CSA for outgoing tcp/80 connections and uses those IPs to find corresponding WSA logs

Analyze: Playbooks

Playbook Reports

144_MALWARE

Objective:

Report the top 10 IP’s that continuously make HTTP request to sites with web reputation scores of -8.0 or less.

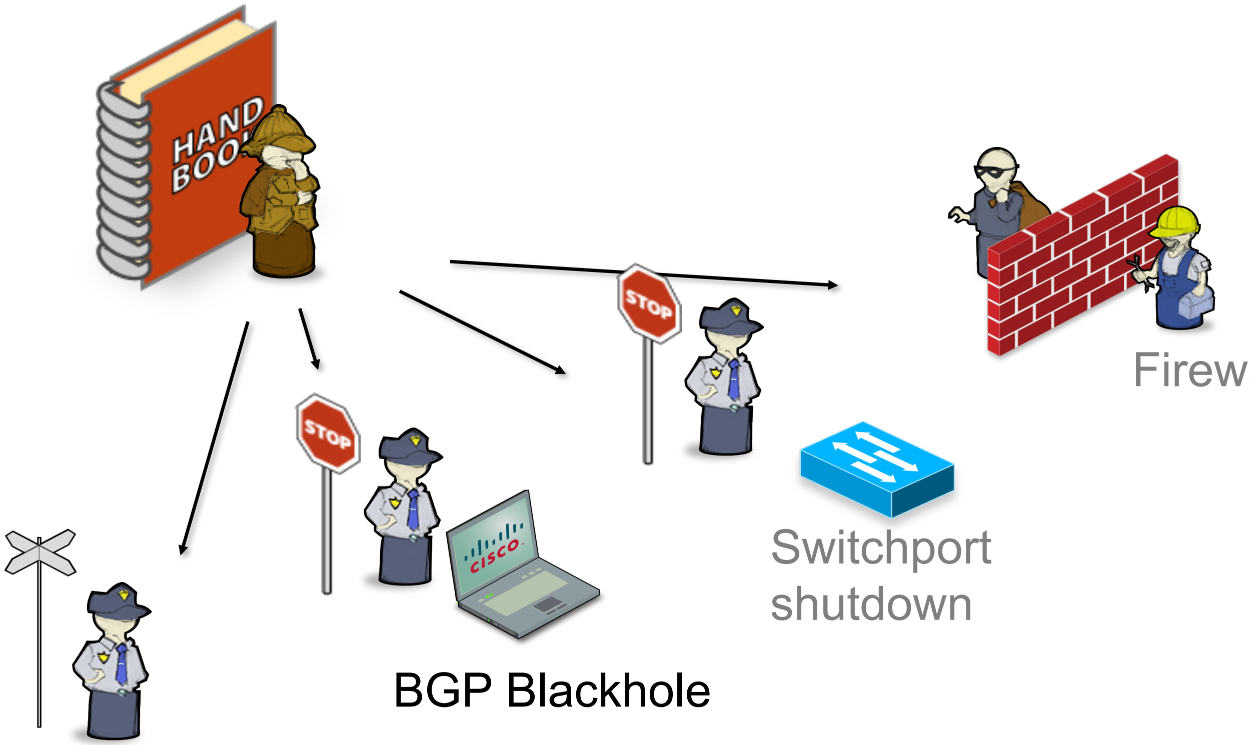
Working:

```
   index="wsa" AND x_wbrs_score <= -8.0 AND TCP_DENIED AND NOT (tag=acns) AND
   earliest=-24h | stats count by c_ip | sort -count limit=10 | rename c_ip as
   "Source IP", count as "# of TCP_DENIED to WBRS < -8.0”
```

An email will be sent to csirt-xxxxxxx@cisco.com

Analysis: The generated report is high fidelity - about 90% of the results have been found to be infected with either malware or adware and need to be submitted to the malware remediation process. If a DC host is found, those hosts will be escalated to the on-duty investigator.

Mitigate
Options



Firewall ACLs

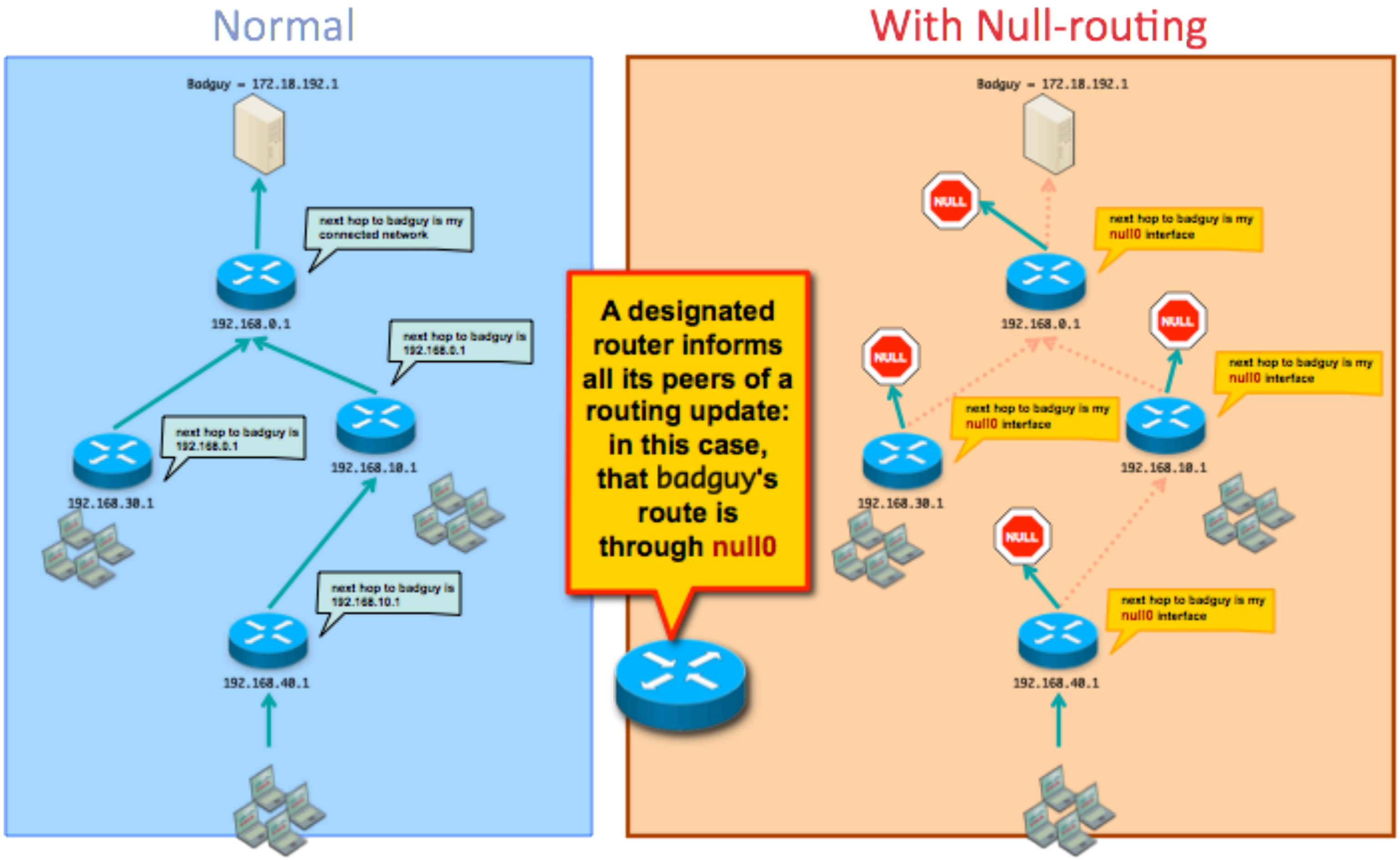
Switchport shutdown

BGP Blackhole

DNS RPZ

Mitigate

BGP Blackhole


Normal
Badguy = 172.18.192.1
next hop to badguy is my connected network
192.168.0.1
next hop to badguy is 192.168.0.1
192.168.10.1
next hop to badguy is 192.168.0.1
192.168.30.1
next hop to badguy is 192.168.10.1
192.168.40.1
With Null-routing
Badguy = 172.18.192.1
NULL
next hop to badguy is my null0 interface
192.168.0.1
NULL
next hop to badguy is my null0 interface
NULL
next hop to badguy is my null0 interface
192.168.10.1
192.168.30.1
NULL
next hop to badguy is my null0 interface
192.168.40.1

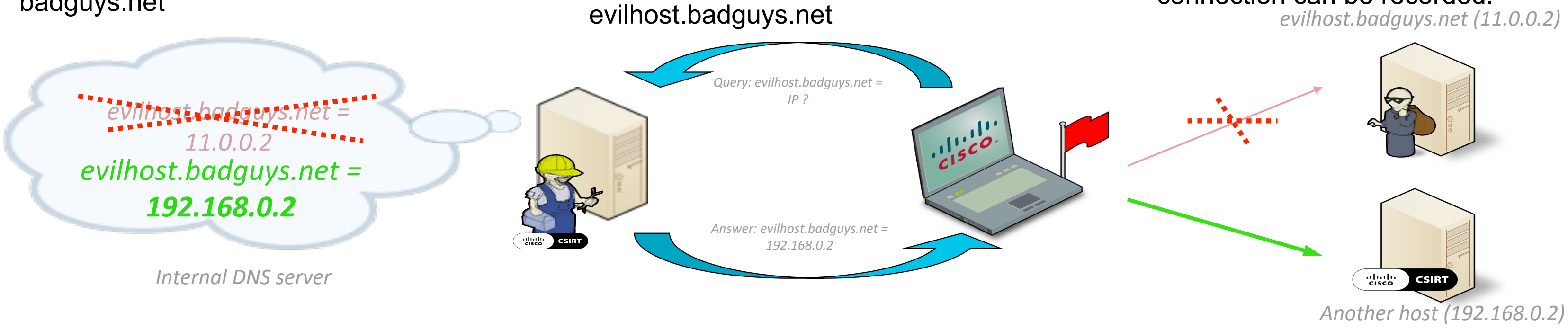
A designated router informs all its peers of a routing update: in this case, that badguy's route is through null0

Mitigate: Poison DNS

1. Cisco DNS servers are ready with a new IP address to map to badguys.net

2. A computer makes a query for evilhost.badguys.net

3. The returned query points the computer to another destination. The connection can be recorded.


evilhost.badguys.net (11.0.0.2)
~~evilhost.badguys.net = 11.0.0.2~~
evilhost.badguys.net = 192.168.0.2
Internal DNS server
CSIRT
Query: evilhost.badguys.net = IP ?
Answer: evilhost.badguys.net = 192.168.0.2
CISCO
CSIRT
Another host (192.168.0.2)

- Relies on advance information about predetermined DNS requests
- Leverage internal DNS servers
- CSIRT’ s partnership with DNS administrators makes this possible
- IDS still detects the resolver queries to uncontrolled DNS servers
- New method: DNS Resource Policy Zones

Mitigate: DNS Resource Policy Zones (RPZs)

Examples

- If *rpz.badguy.com* is a response policy zone and *badguy.com* is a name to be blacked out:

```
badguy.com.rpz.mycompany.com CNAME .
```

- If *badguy.com/A* should be redirected:

```
badguy.com A 198.168.7.77
```

- If *badguy.com* is to appear empty:

```
badguy.com.rpz.mycompany.com CNAME *.
```

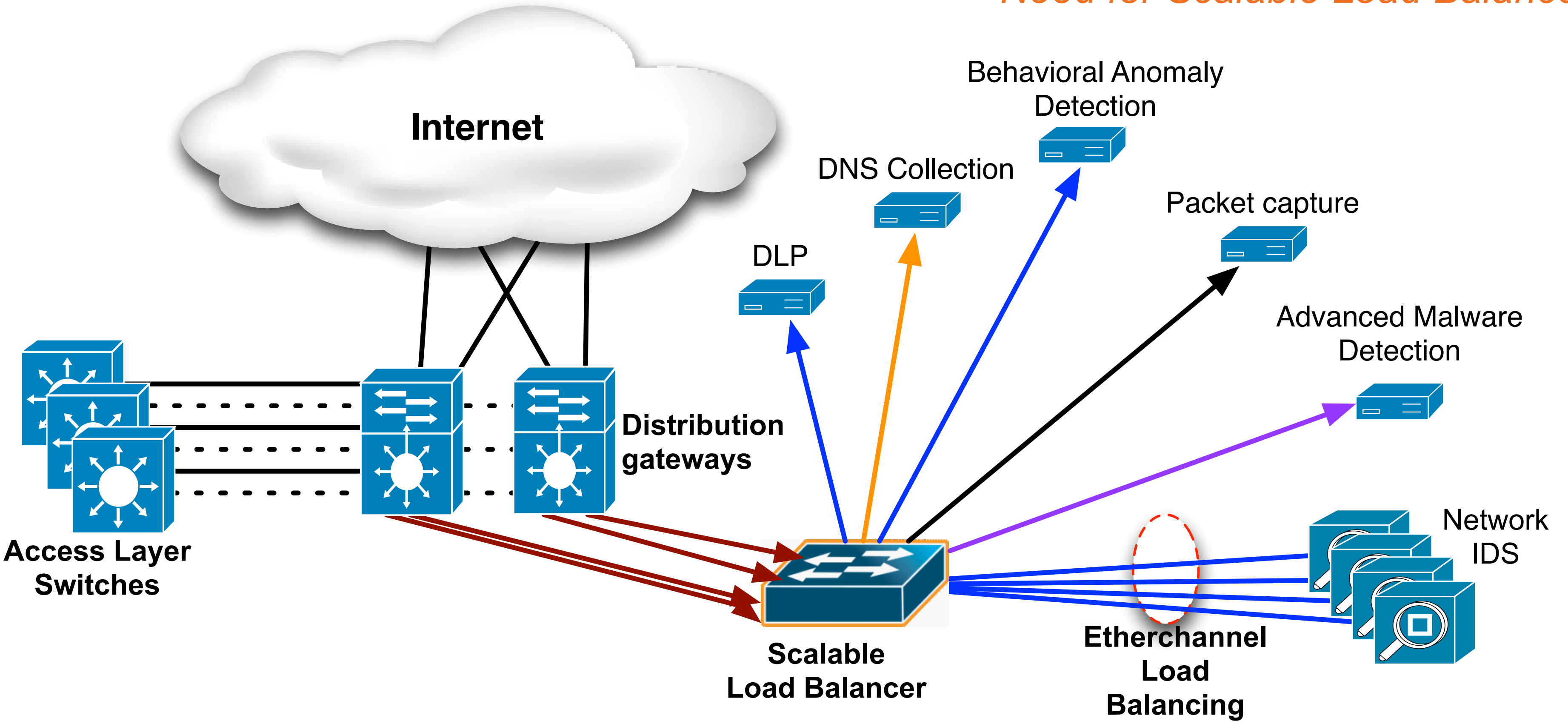
- If A RRs in 192.168.1.0/24 are to be replaced with a local walled garden address:

```
24.0.1.168.192.rpz-ip.rpz.badguys.com A 192.168.7.77
```

Reference: http://ftp.isc.org/isc/dnsrpz/isc-tn-2010-1.txt

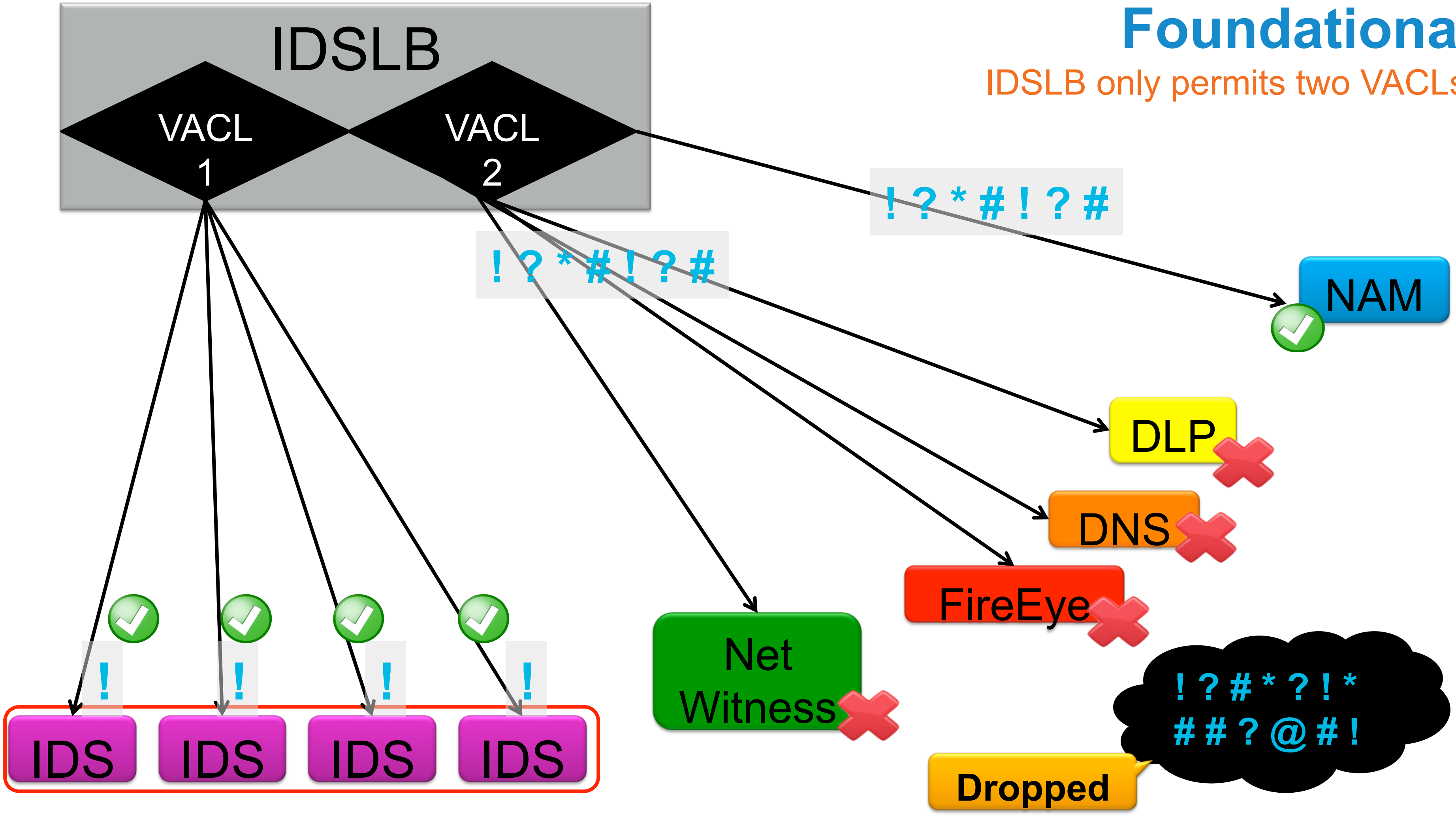
Foundational: Topological Overview

Need for Scalable Load Balancer



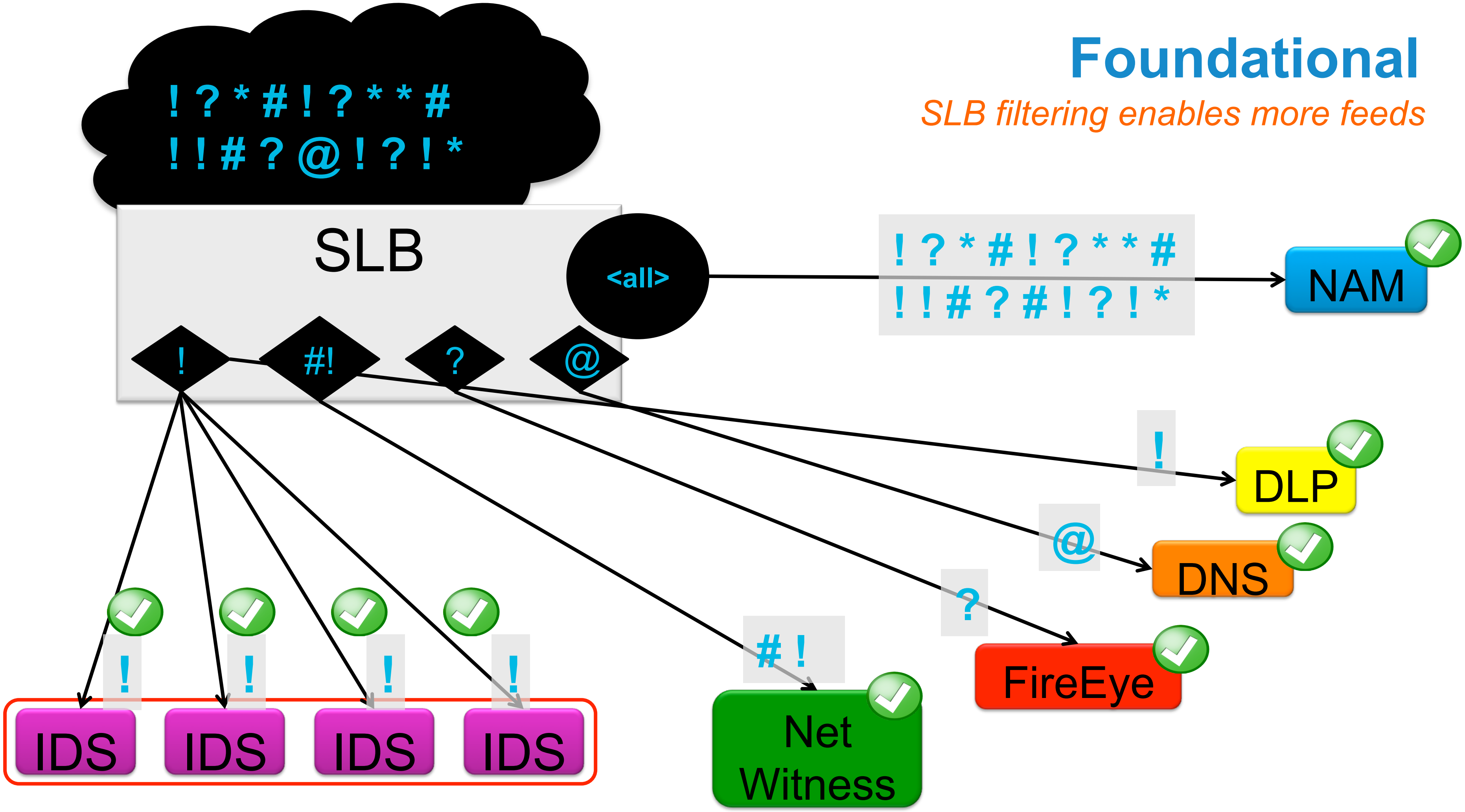
Foundational

IDSLB only permits two VACLs



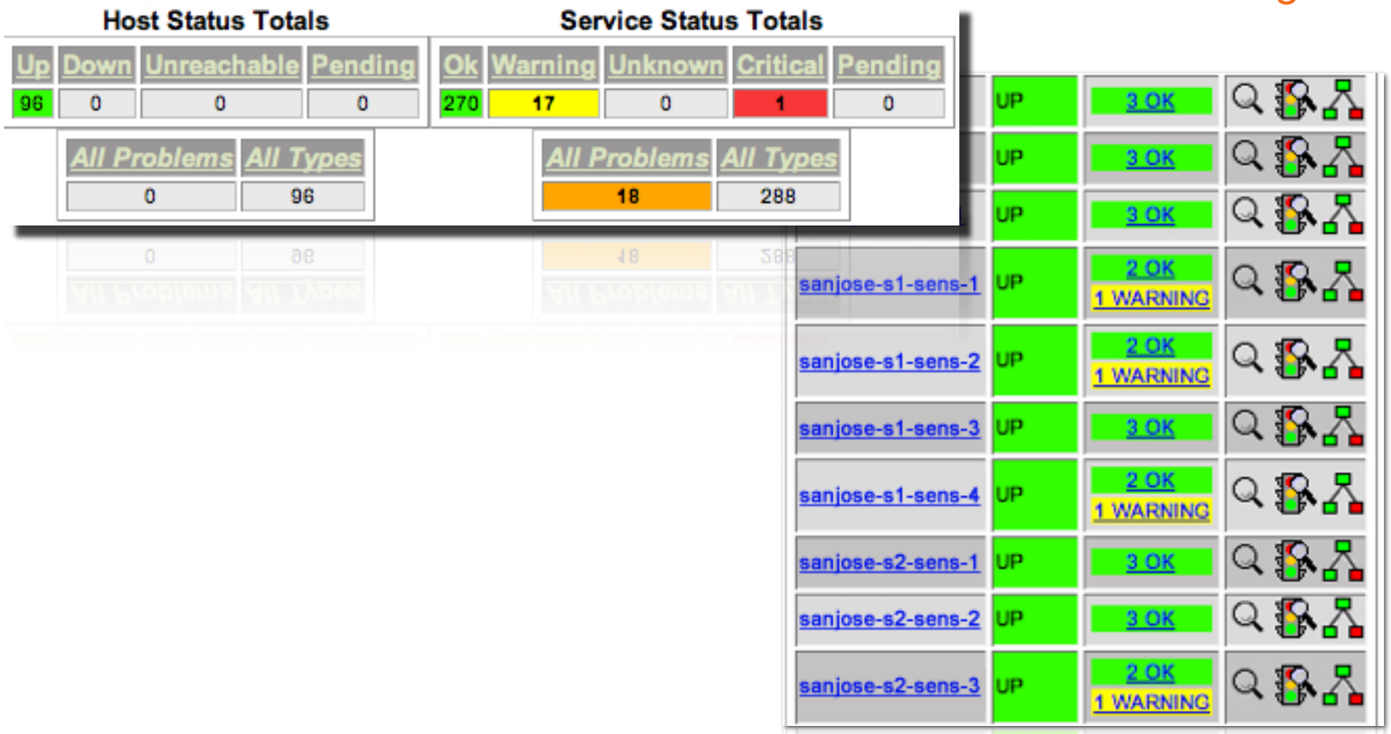
Foundational

SLB filtering enables more feeds



Foundational

Monitoring Tools



Host Status Totals

Up	Down	Unreachable	Pending
96	0	0	0

All Problems	All Types
0	96

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
270	17	0	1	0

All Problems	All Types
18	288

	UP	3 OK
	UP	3 OK
	UP	3 OK
sanjose-s1-sens-1	UP	2 OK 1 WARNING
sanjose-s1-sens-2	UP	2 OK 1 WARNING
sanjose-s1-sens-3	UP	3 OK
sanjose-s1-sens-4	UP	2 OK 1 WARNING
sanjose-s2-sens-1	UP	3 OK
sanjose-s2-sens-2	UP	3 OK
sanjose-s2-sens-3	UP	2 OK 1 WARNING

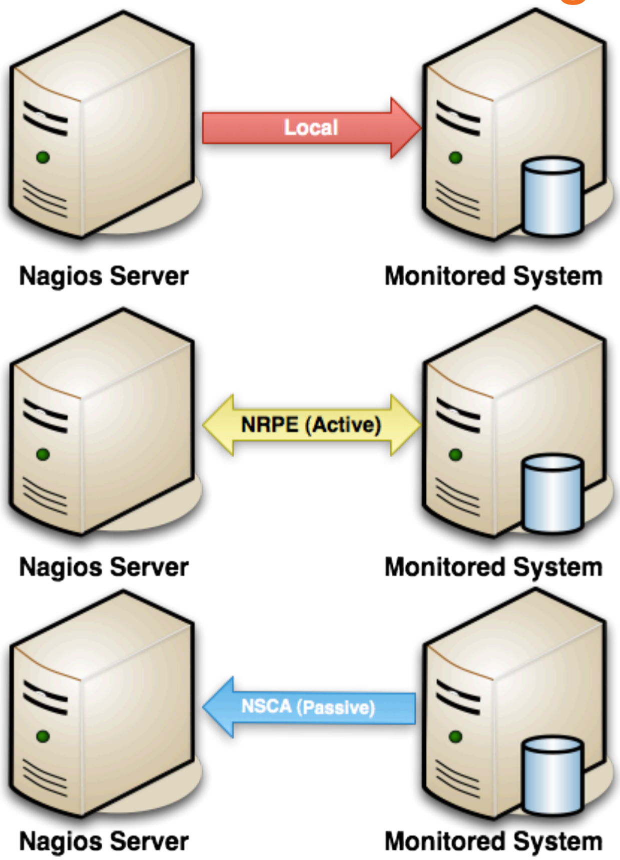
CSIRT

Foundational

How Nagios Works

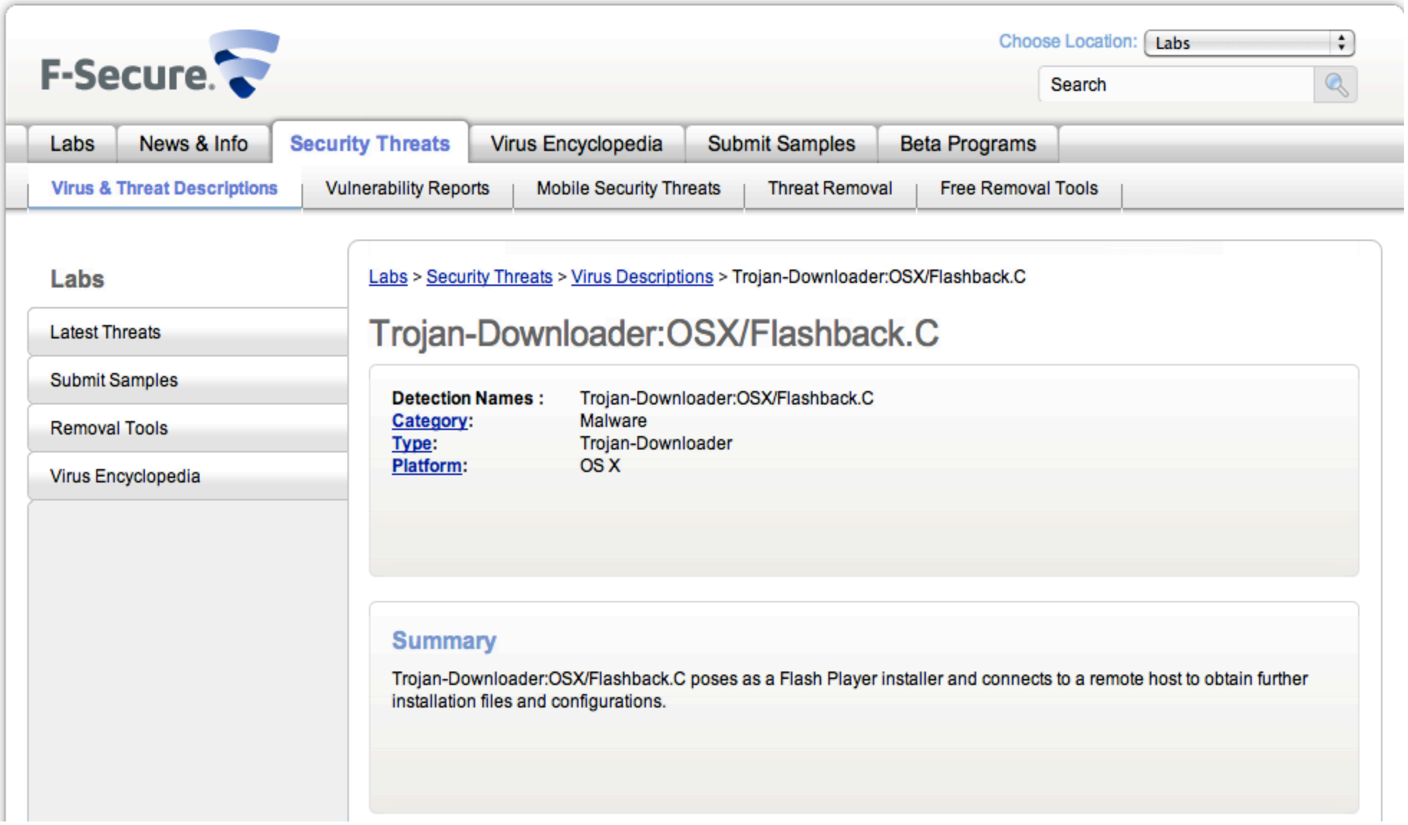
- Server local checks
    - HTTP(S)
    - Ping
    - SNMP
    - Telnet/SSH
    - And more…

- Remote checks
    - NRPE (active)
        - Server triggers check
    - NSCA (passive)
        - Client reports results to server



Example Incident

Mac OSX Flashback Trojan



Labs > Security Threats > Virus Descriptions > Trojan-Downloader:OSX/Flashback.C

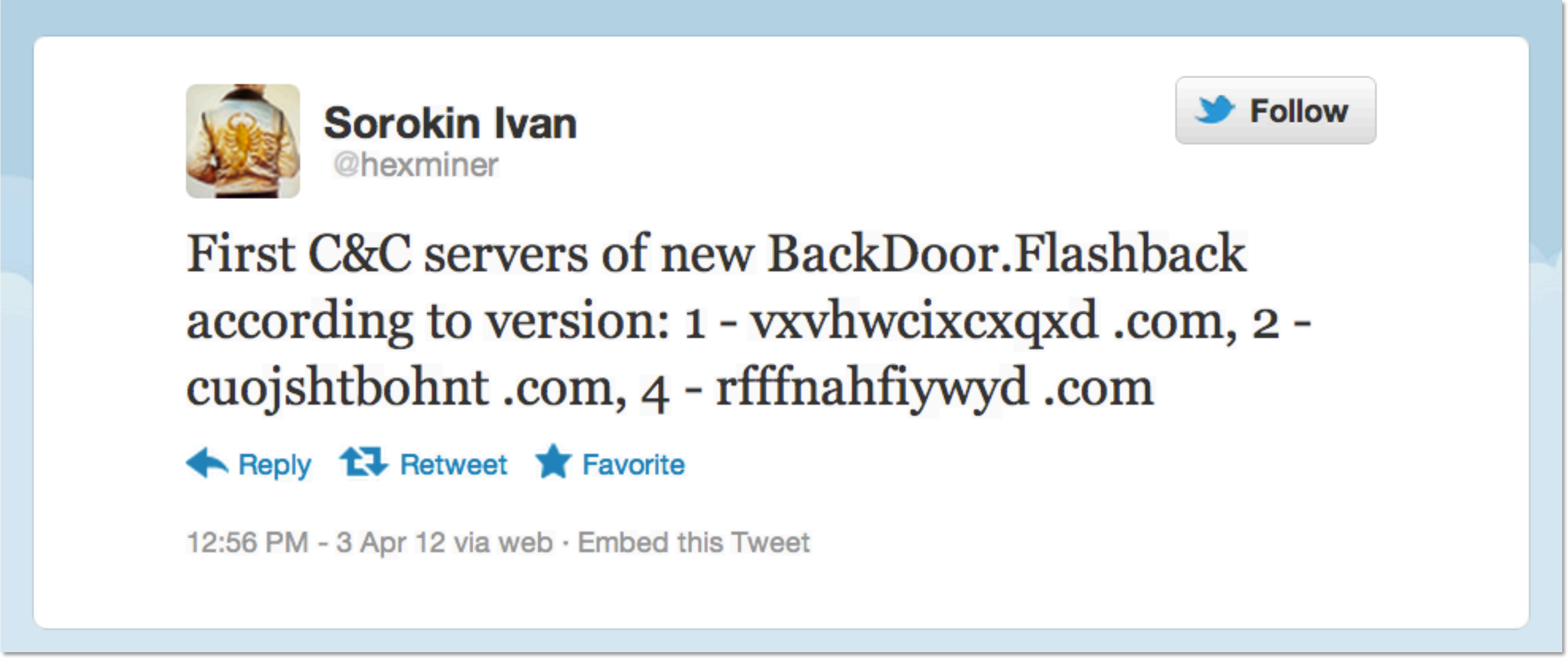
Trojan-Downloader:OSX/Flashback.C

Detection Names :	Trojan-Downloader:OSX/Flashback.C
Category:	Malware
Type:	Trojan-Downloader
Platform:	OS X

Summary

Trojan-Downloader:OSX/Flashback.C poses as a Flash Player installer and connects to a remote host to obtain further installation files and configurations.

- Not detected by Anti-Virus, FireEye, or WSA
- Drive-by attacks against CVE-2021-0507

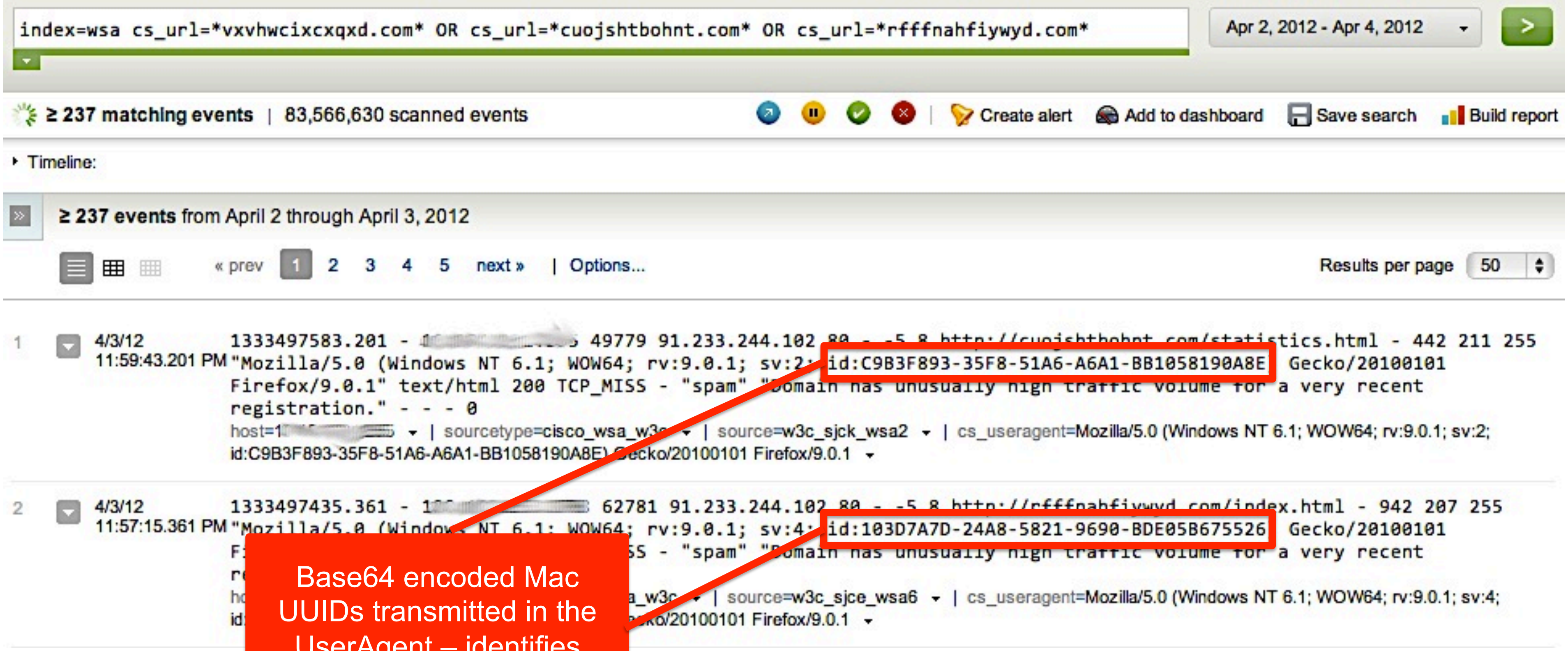


Sorokin Ivan
@hexminer

First C&C servers of new BackDoor.Flashback according to version: 1 - vxvhwcixcxqxd .com, 2 - cuojshtbohnt .com, 4 - rfffnahfiywyd .com

12:56 PM - 3 Apr 12 via web · Embed this Tweet

Search external intelligence for domains, URLs, or IPs used by flashback



index=wsa cs_url=*vxvhwcixcxqxd.com* OR cs_url=*cuojshtbohnt.com* OR cs_url=*rfffnahfiywyd.com*
Apr 2, 2012 - Apr 4, 2012
>

≥ 237 matching events | 83,566,630 scanned events

Create alert
Add to dashboard
Save search
Build report
Timeline:

≥ 237 events from April 2 through April 3, 2012

« prev 1 2 3 4 5 next » | Options...
Results per page 50

```
1   4/3/12           1333497583.201 - [redacted] 49779 91.233.244.102 80 - -5 8 http://cuojshtbohnt.com/statistics.html - 442 211 255
    11:59:43.201 PM "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:9.0.1; sv:2; id:C9B3F893-35F8-51A6-A6A1-BB1058190A8E) Gecko/20100101
                     Firefox/9.0.1" text/html 200 TCP_MISS - "spam" "Domain has unusually high traffic volume for a very recent
                     registration." - - - 0
                     host=[redacted] | sourcetype=cisco_wsa_w3c | source=w3c_sjck_wsa2 | cs_useragent=Mozilla/5.0 (Windows NT 6.1; WOW64; rv:9.0.1; sv:2;
                     id:C9B3F893-35F8-51A6-A6A1-BB1058190A8E) Gecko/20100101 Firefox/9.0.1

2   4/3/12           1333497435.361 - [redacted] 62781 91.233.244.102 80 - -5 8 http://rfffnahfiywyd.com/index.html - 942 207 255
    11:57:15.361 PM "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:9.0.1; sv:4; id:103D7A7D-24A8-5821-9690-BDE05B675526) Gecko/20100101
                     F                                       SS - "spam" "Domain has unusually high traffic volume for a very recent
                     r
                     h                                       a_w3c | source=w3c_sjce_wsa6 | cs_useragent=Mozilla/5.0 (Windows NT 6.1; WOW64; rv:9.0.1; sv:4;
                     id                                      ecko/20100101 Firefox/9.0.1
```

Base64 encoded Mac UUIDs transmitted in the UserAgent – identifies compromised machines

Investigative Approach

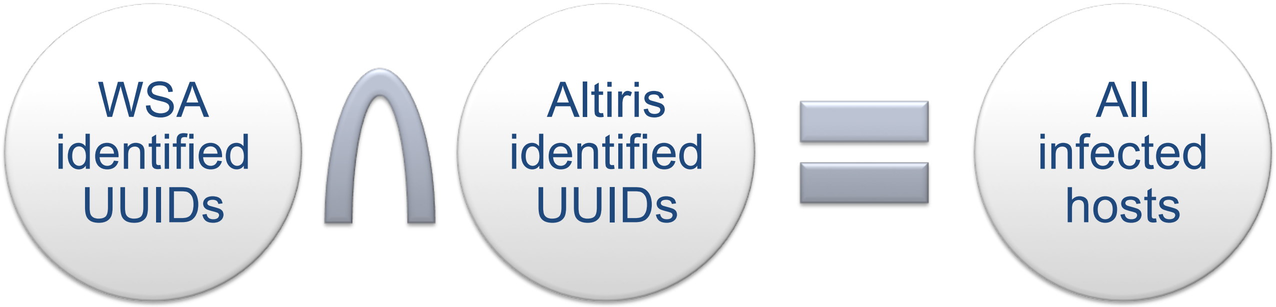
What you could do…

```
index=wsa
cs_url="http://ASDFUH982HDODJC.COM*"; OR cs_url="http://95.215.63.38*"; OR
cs_url="http://godofwar3.rr.nu*"; OR cs_url="http://ironmanvideo.rr.nu*"; OR
cs_url="http://killaoftime.rr.nu*"; OR cs_url="http://
gangstasparadise.rr.nu*"; OR cs_url="http://mystreamvideo.rr.nu*"; OR
cs_url="http://bestustreamtv.rr.nu*"; OR cs_url="http://ustreambesttv.rr.nu*";
OR cs_url="http://ustreamtvonline.rr.nu*"; OR cs_url="http://ustream-
tv.rr.nu*"; OR cs_url="http://ustream.rr.nu*"; OR cs_url="http://
johncartermovie2012.com*"; OR cs_url="http://bodyrocks.rr.nu*"; OR
s_ip=95.215.63.38 OR cs_url="http://31.31.79.87*"; …..
```

- “Whack-a-mole” technique
- Inefficient and un-manageable

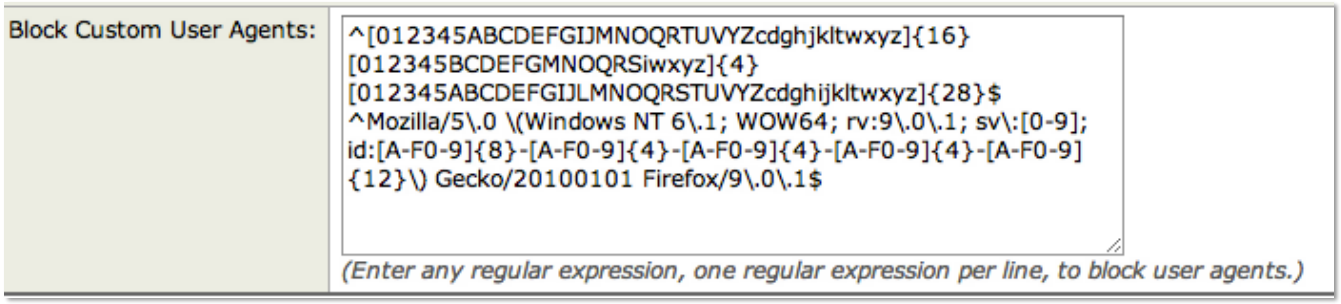
Remediation

Identify all infections:



WSA identified UUIDs ∩ Altiris identified UUIDs = All infected hosts

Prevent further infections via WSA:



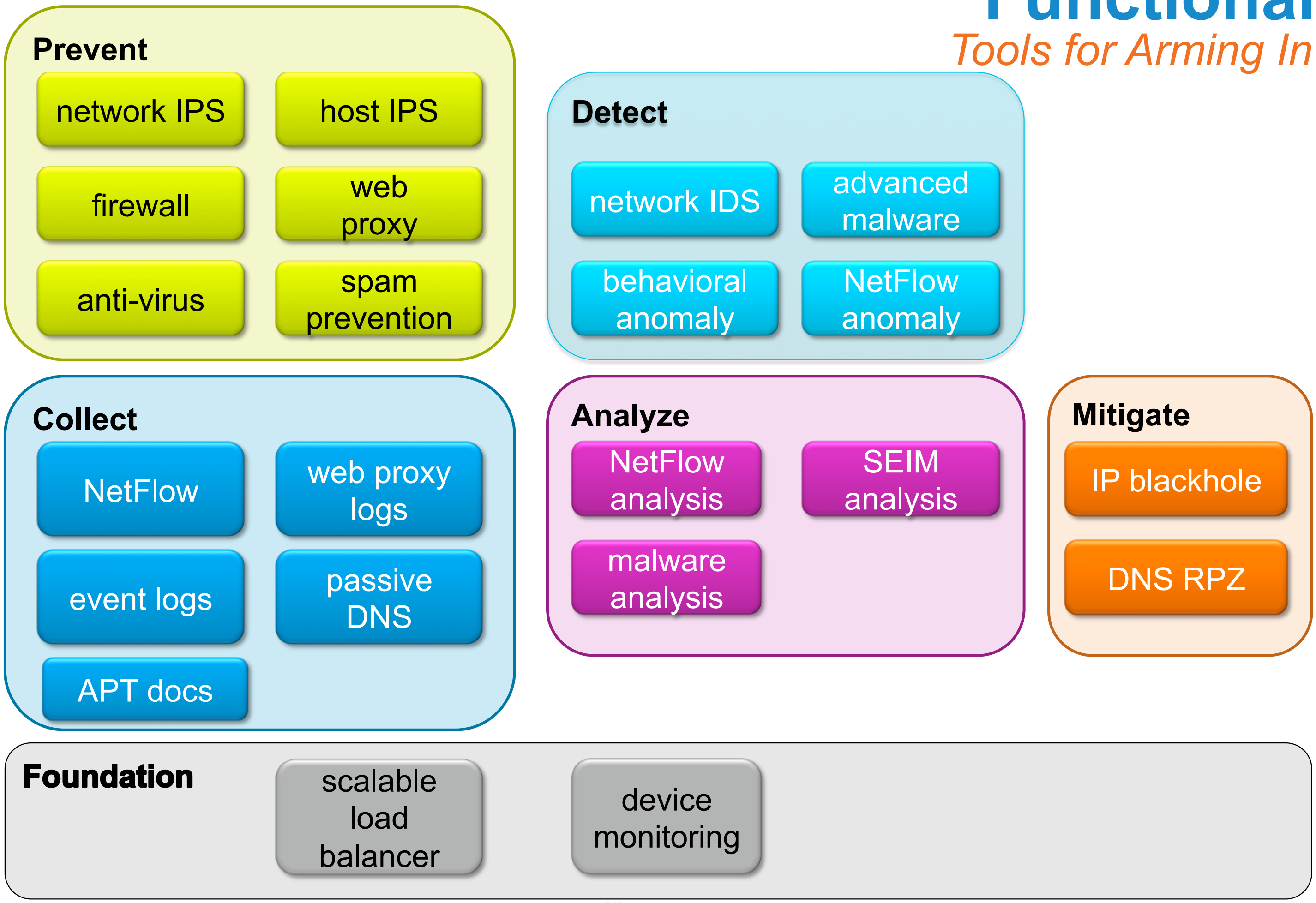
Block Custom User Agents:

```
^[012345ABCDEFGIJMNOQRTUVYZcdghjkltwxyz]{16}
[012345BCDEFGMNOQRSiwxyz]{4}
[012345ABCDEFGIJLMNOQRSTUVYZcdghijkltwxyz]{28}$
^Mozilla/5\.0 \(Windows NT 6\.1; WOW64; rv:9\.0\.1; sv\:[0-9];
id:[A-F0-9]{8}-[A-F0-9]{4}-[A-F0-9]{4}-[A-F0-9]{4}-[A-F0-9]
{12}\) Gecko/20100101 Firefox/9\.0\.1$
```

(Enter any regular expression, one regular expression per line, to block user agents.)

Functional Model

Tools for Arming Investigators



Prevent

- network IPS
- host IPS
- firewall
- web proxy
- anti-virus
- spam prevention

Detect

- network IDS
- advanced malware
- behavioral anomaly
- NetFlow anomaly

Collect

- NetFlow
- web proxy logs
- event logs
- passive DNS
- APT docs

Analyze

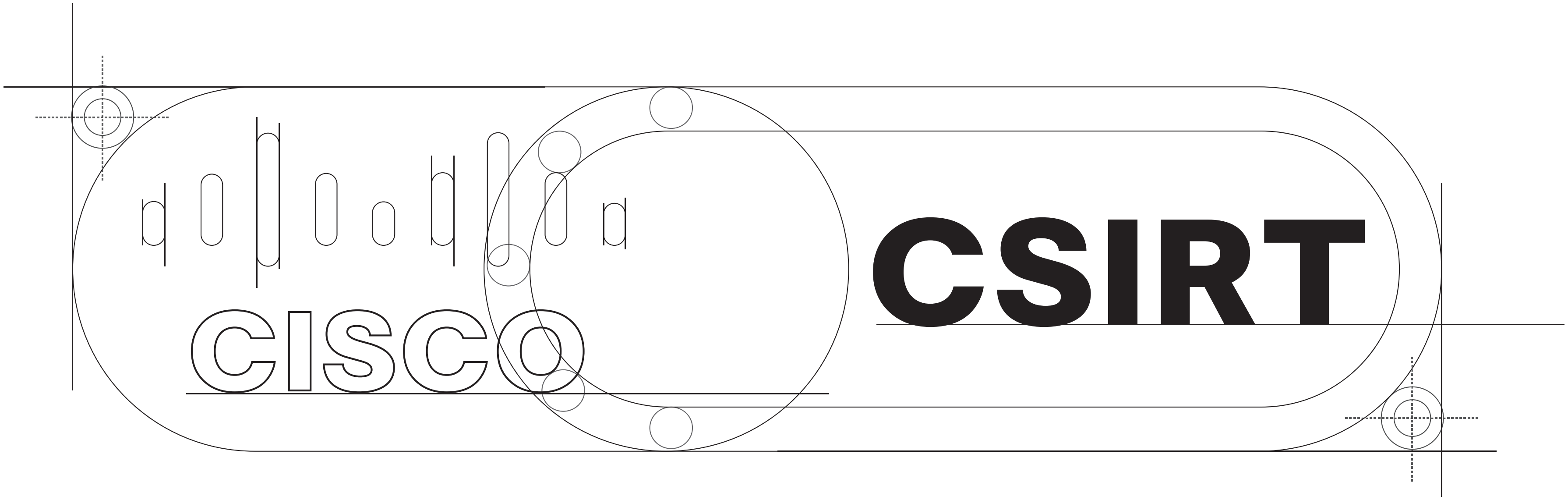
- NetFlow analysis
- SEIM analysis
- malware analysis

Mitigate

- IP blackhole
- DNS RPZ

Foundation

- scalable load balancer
- device monitoring



Paul Eckstein
pigsty@cisco.com

Martin Nystrom
diddly@cisco.com