



*TOMORROW
starts here.*

Cisco *live!*



Inside Cisco IT: Engineering Solutions for Monitoring and Investigations

COCSEC-1300

Simon Finn – InfoSec Architect


#clmel

Cisco *live!*

Agenda

- Introduction
- Monitoring Infrastructure
- Special Circumstances
- Operationalising
- Conclusion





Introduction

Big(ger) Data

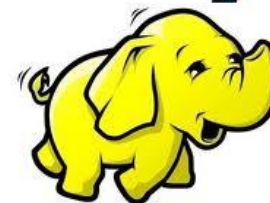
STAMFORD, Conn., February 6, 2014

[View All Press Releases](#)

By 2016, 25 Percent of Large Global Companies Will Have Adopted Big Data Analytics For At Least One Security or Fraud Detection Use Case

Source: <http://www.gartner.com/newsroom/id/2663015>

hadoop



Splunk App for Enterprise Security

The Big Data Approach to Security Intelligence


Today's attackers have realized that many security teams simply can't see threats buried within operations data, due to organizational data silos, data collection issues, scalability challenges or a lack of analytics capabilities. They also have the resources to create attack scenarios that bypass security point products and

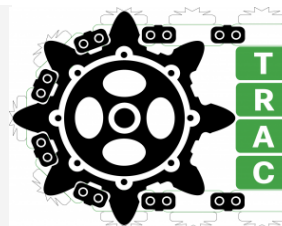
Cisco Blog > Security

Big Data in Security – Part I: TRAC Tools



Levi Gundert | December 9, 2013 at 6:49 am PST

(0 Comments) 



Cisco *live!*

Threat Landscape Evolution

Response

HOST-BASED
(ANTI-VIRUS)

2000

NETWORK PERIMETER
(IDS/IPS)

2005

GLOBAL REPUTATION
& SANDBOXING

2010

INTELLIGENCE
& ANALYTICS

Tomorrow

Threats

Worms



Spyware / Rootkits



APTs / Cyberware



Increased Attack Surface (Mobility & Cloud)





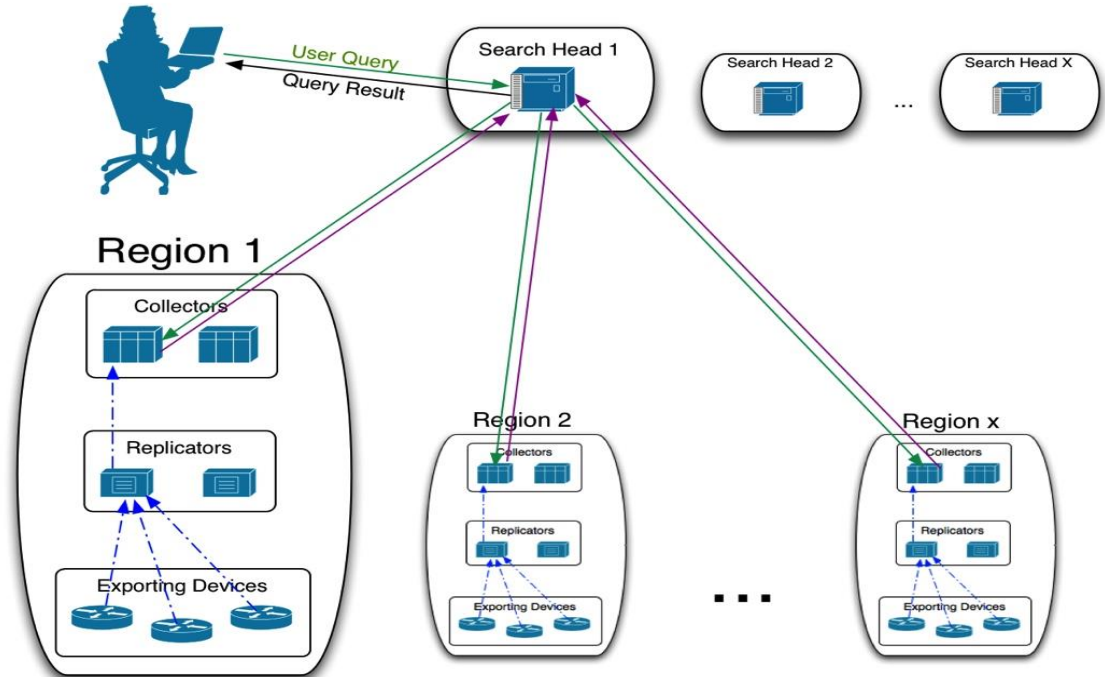
Monitoring Infrastructure

Know Your Network

- Network segmentation
- Asset information
- Attribution
- Identify high value assets:
 - Intellectual property, customer/employee data, brand protection, infrastructure

Common Collection Infrastructure

- Redundant forwarding
- Regional storage
- Global search
- Applies to netflow, log collection, pDNS and other

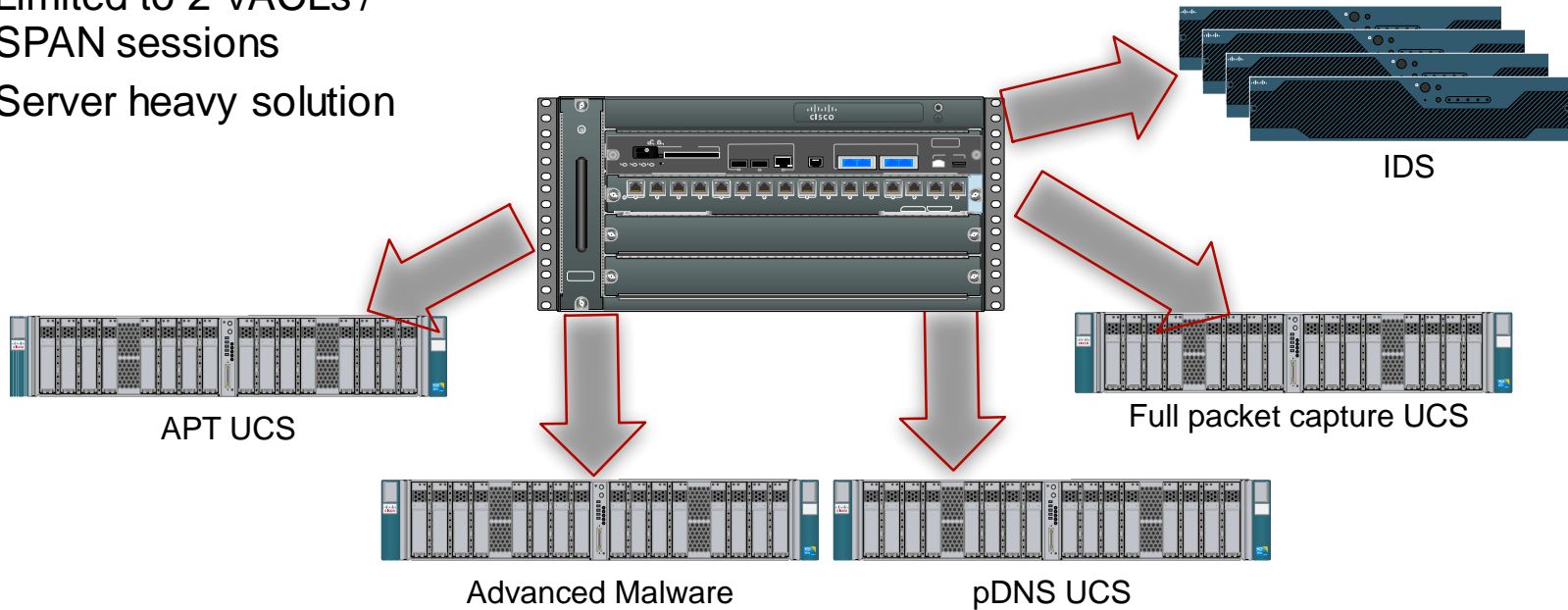


Changing Where Data is Aggregated

The old way

Catalyst 6500 based

- Limited to 2 VACLs / SPAN sessions
- Server heavy solution

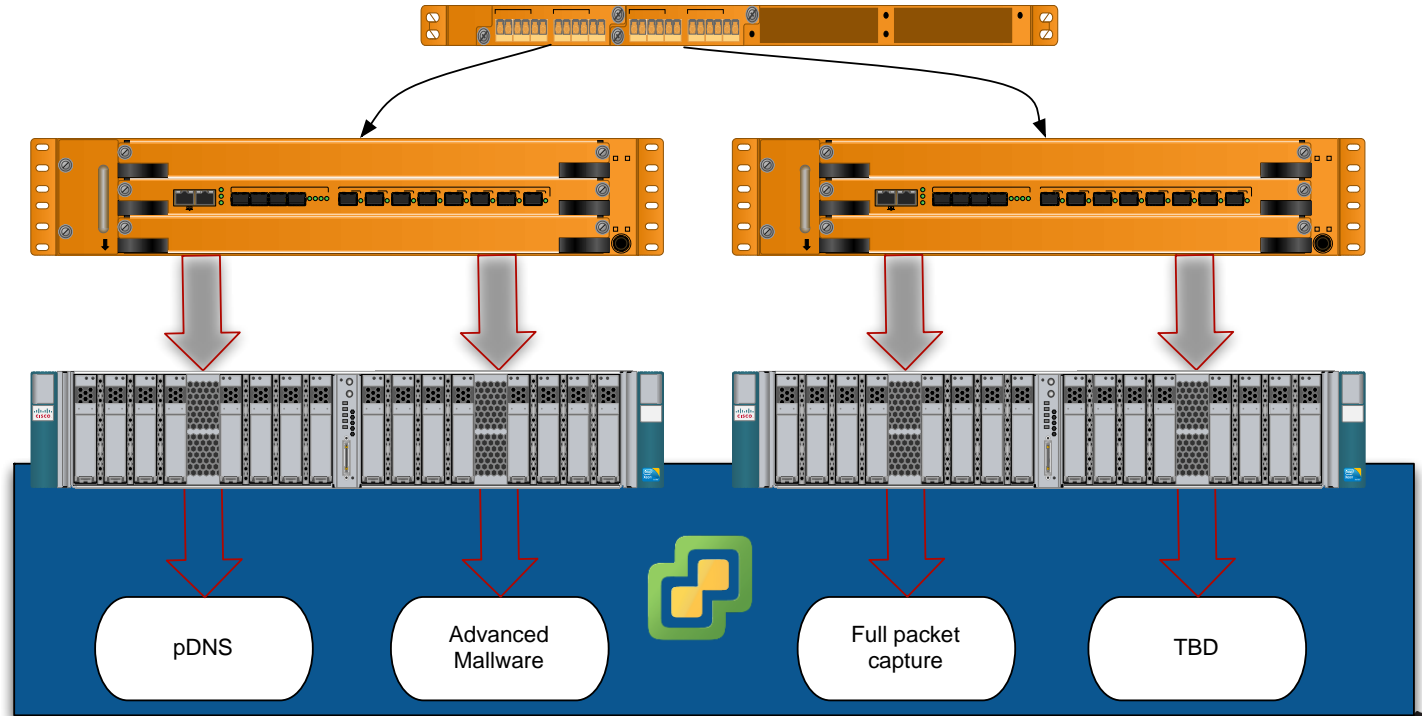


Changing Where Data is Aggregated

Advanced packet filtering and distribution

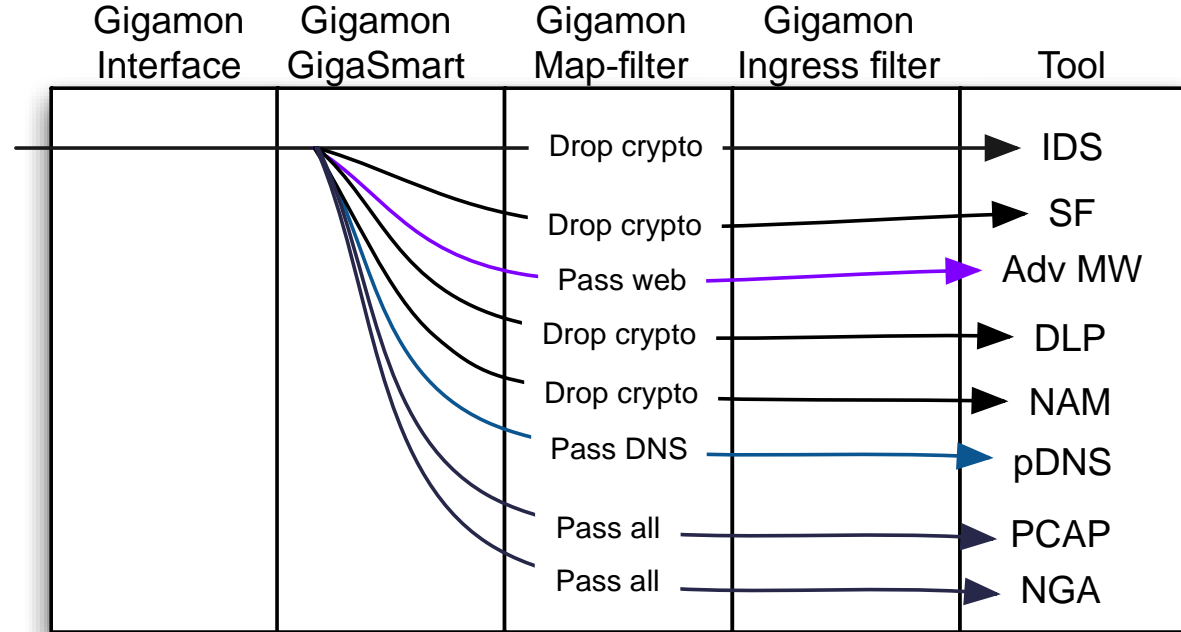
Lupa architecture

- Scalable
- Adaptable
- Maximises tool capacity



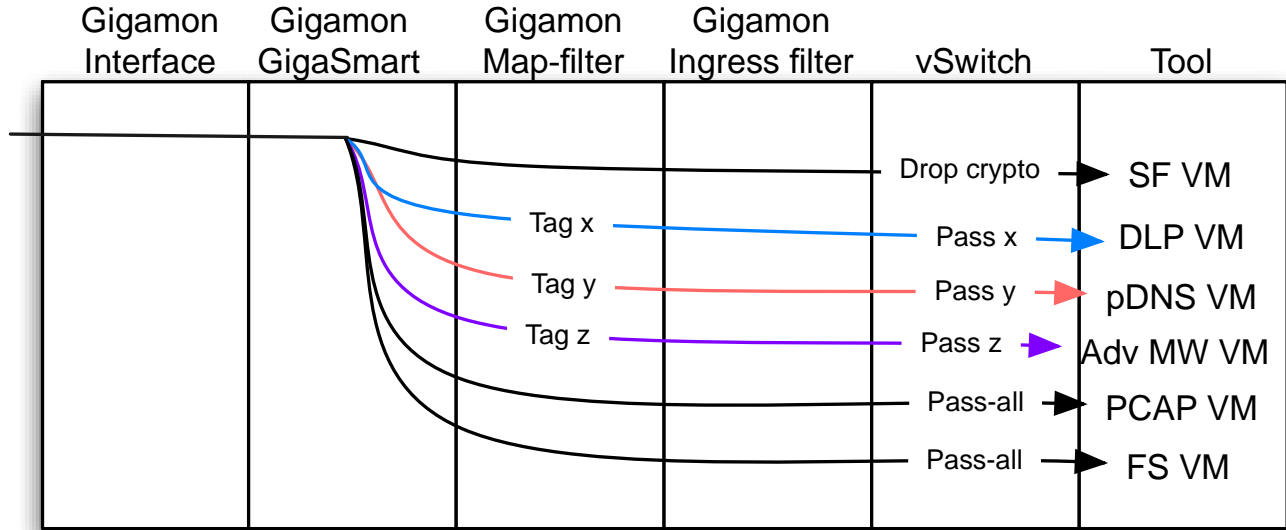
Changing Where Data is Aggregated

Dropping and filtering data destined to hardware appliances



Changing Where Data is Aggregated

Dropping and filtering data destined to VMs

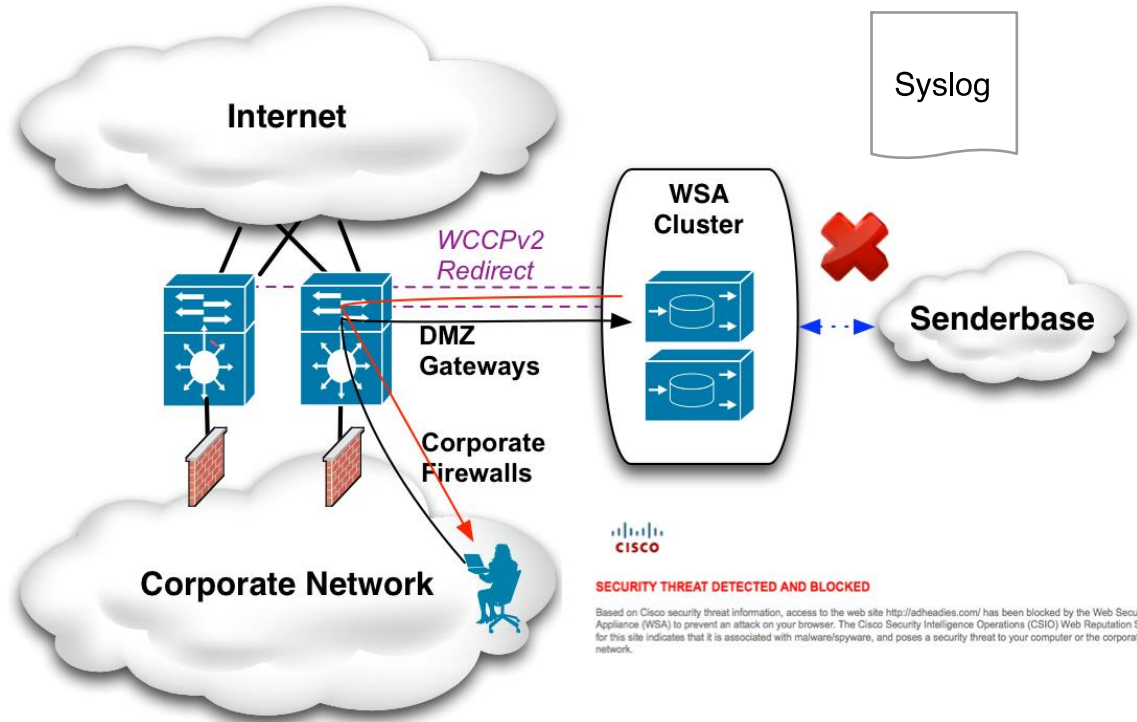


A long-exposure photograph of a city street at night. The foreground is dominated by vibrant, multi-colored light trails from moving vehicles, creating a sense of motion and energy. In the background, a modern urban landscape is visible, featuring a prominent pedestrian bridge with blue lighting, tall buildings with illuminated windows, and traffic lights. The overall scene is a blend of urban architecture and dynamic light patterns.

Security Event Sources

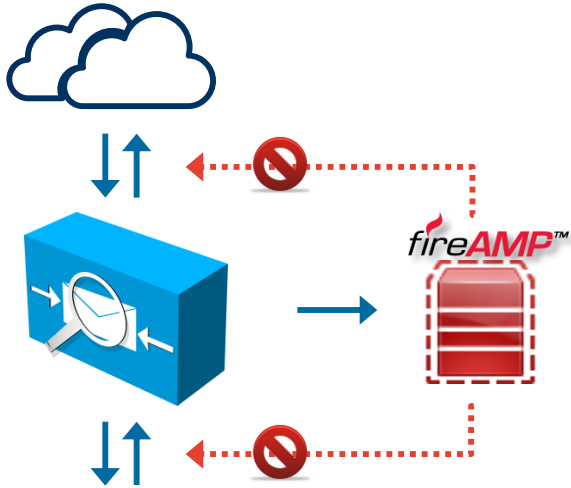
Web Security Appliance (WSA)

- Common web ports
- Reputation scoring
- Automatic client redirection

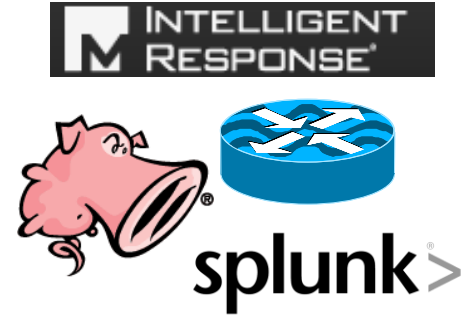


ESA and AMP

Sandboxing



- Process names
- Registry keys
- IP addresses
- DNS names



IDS

Filtering & Tuning

Search

```
index=ids signature="5474" 5474 earliest=-1d | stats values(attacker_locality) AS SourceLocation, earliest(_time) AS FirstEvent, latest(_time) AS LastEvent, EventCount AS EventCount, values(description) AS MaliciousActivity, values(target) AS TargetIPs, values(target_locality) AS TargetLocalities, values(signature) AS Signature
```

✓ 14,255 matching events

Home > Security Intelligence Operations > Latest Threat Information > Search Cisco Intrusion Prevention System Signatures

IPS Signatures

SQL Query in HTTP Request

Signature ID:

5474/1

Alarm Severity: Low



IDS

- More **precise queries** = more **effective plays**
- Additive **filtering** (more required matches = less events to review)
- Take indicators from **past** incidents, apply towards **future** incidents:

Search

```
index=ids OUT attacker_locality="OUT" signature="5474" OR signature="5930" earliest=-6d concat NOT WhiteHat  
earliest( time) AS FirstEvent latest( time) AS LastEvent count AS EventCount values(description) AS Malic
```

✓ 10 matching events

Home > Security Intelligence Operations > Latest Threat Information > Search Cisco Intrusion Prevention System Signatures

IPS Signatures

Generic SQL Injection

Signature ID:

5930/0

Alarm Severity: High





Non-Security Event Sources

Syslog

When to log

- Access, authenticate to, or modify **confidential info**
- Initiate or accept a **network connection**
- Manipulate **access rights**
- System or network **configuration changes**
- **Process state changes** (start, terminated, HUP, failure, etc.)
- New **services**



Syslog

What to log

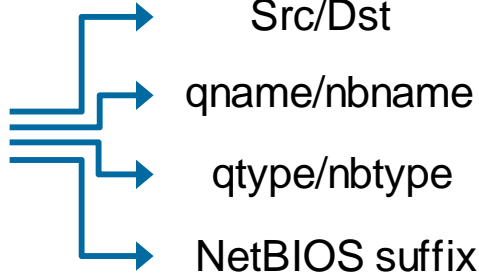
- **Type** of action performed
- **Subsystem** performing the action
- Identifiers for the **object requesting** the action
- Identifiers for the **object providing** the action
- **Date & time**
- **Status, outcome, or result** of the action

<http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf>

http://www.sans.org/security-resources/policies/info_sys_audit.pdf

Passive DNS

Q&A's



Questions



FARSIGHT SECURITY

DNSDB Search

Search mode: RRset Rdata
Record type: ANY
Domain name:
Bailiwick:

Search

Reset

RRset results for **ciscolive2014.com/ANY**

Returned 8 RRsets in 0.01 seconds.

bailiwick	com.
count	973
first seen in zone file	2010-04-24 16:12:21 -0000
last seen in zone file	2012-12-31 17:24:50 -0000
ciscolive2014.com.	NS ns2.wingateservices.com.
ciscolive2014.com.	NS ns3.wingateservices.com.

bailiwick	ciscolive2014.com.
count	461
first seen	2013-04-02 20:34:46 -0000
last seen	2014-03-30 05:24:44 -0000
ciscolive2014.com.	A 136.179.0.125

Answers

Netflow – Identifying Flooding and Beaconing

- Lancope sends syslog alarm when flood or beacon activity is observed

Bug 9099 - 200005-INV-FLOW-HOT_THREAT:
High volume UDP Amplification Attacks ([edit](#))

Status: DEPLOYED ([edit](#))

Product: CSIRT Playbook

Component: Investigative

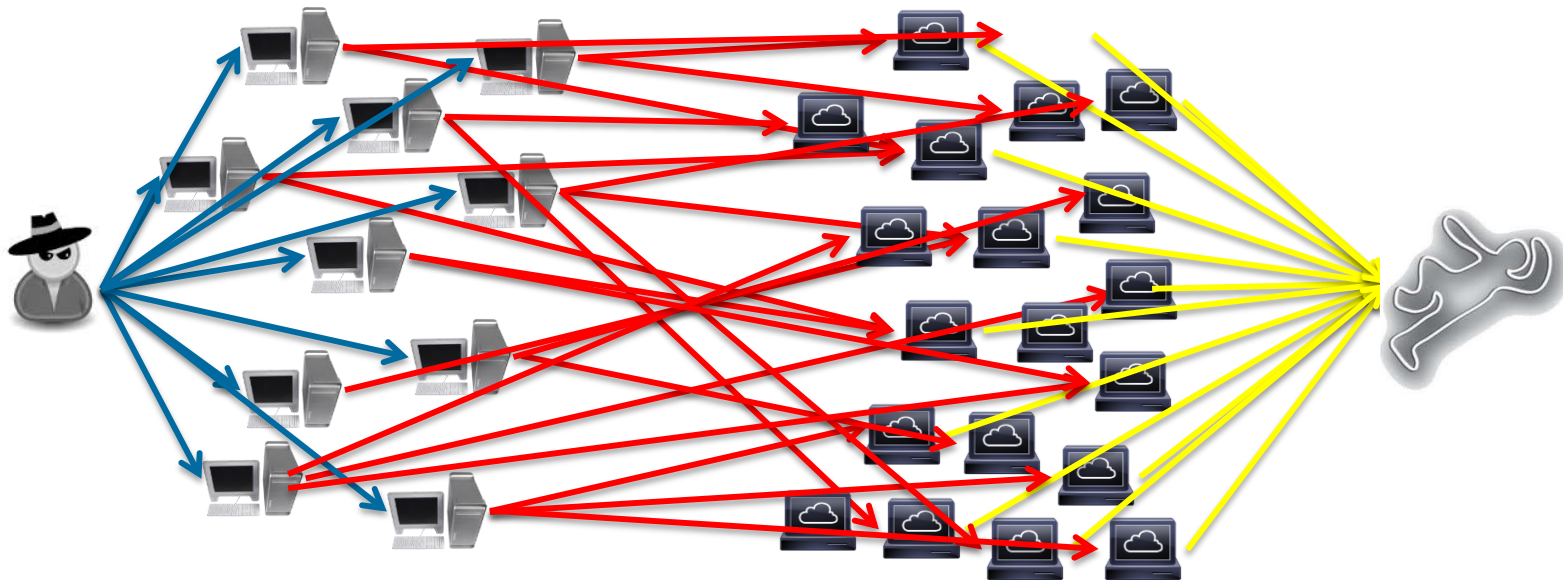
This rule is triggered if

The Domain that originated this alarm is and

of the following are true

<input type="text" value="Type"/>	is	<input type="text" value="Half Open Attack"/>
<input type="text" value="Type"/>	is	<input type="text" value="UDP Flood"/>
<input type="text" value="Type"/>	is	<input type="text" value="SYN Flood"/>
<input type="text" value="Type"/>	is	<input type="text" value="Packet Flood"/>
<input type="text" value="Type"/>	is	<input type="text" value="Port Flood"/>

Netflow UDP Amplification Detection



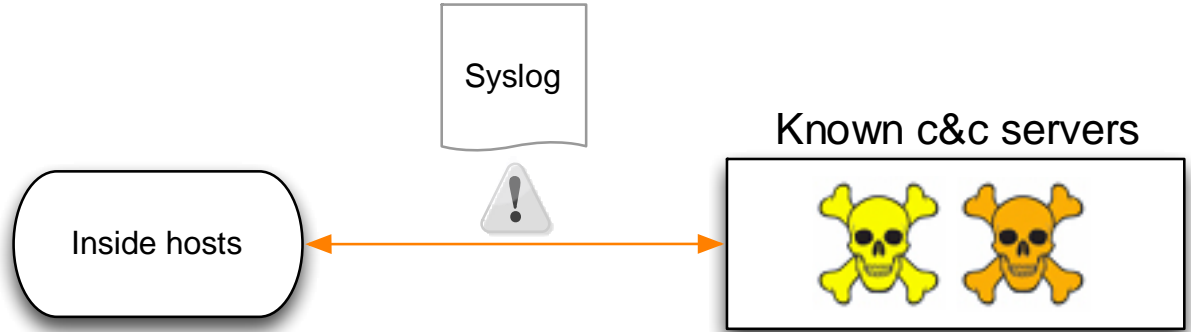
Report Filters:

- UDP ports susceptible to amplification
- Size of total traffic
- Number of packets

<http://blogs.cisco.com/security/a-smorgasbord-of-denial-of-service/>

Netflow Host Locking

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

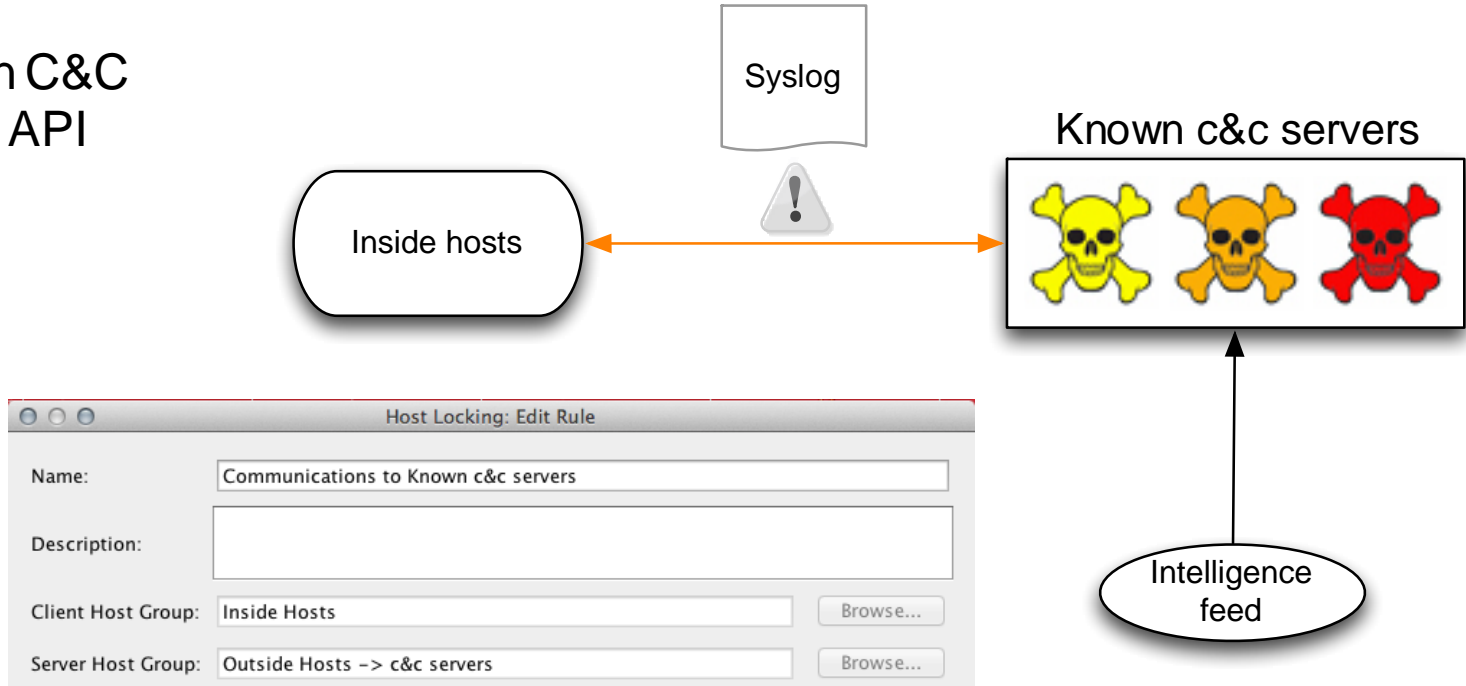


The screenshot shows a configuration window titled "Host Locking: Edit Rule". It contains the following fields and controls:

- Name:** Communications to Known c&c servers
- Description:** (Empty text area)
- Client Host Group:** Inside Hosts (with a "Browse..." button)
- Server Host Group:** Outside Hosts -> c&c servers (with a "Browse..." button)

Netflow Host Locking

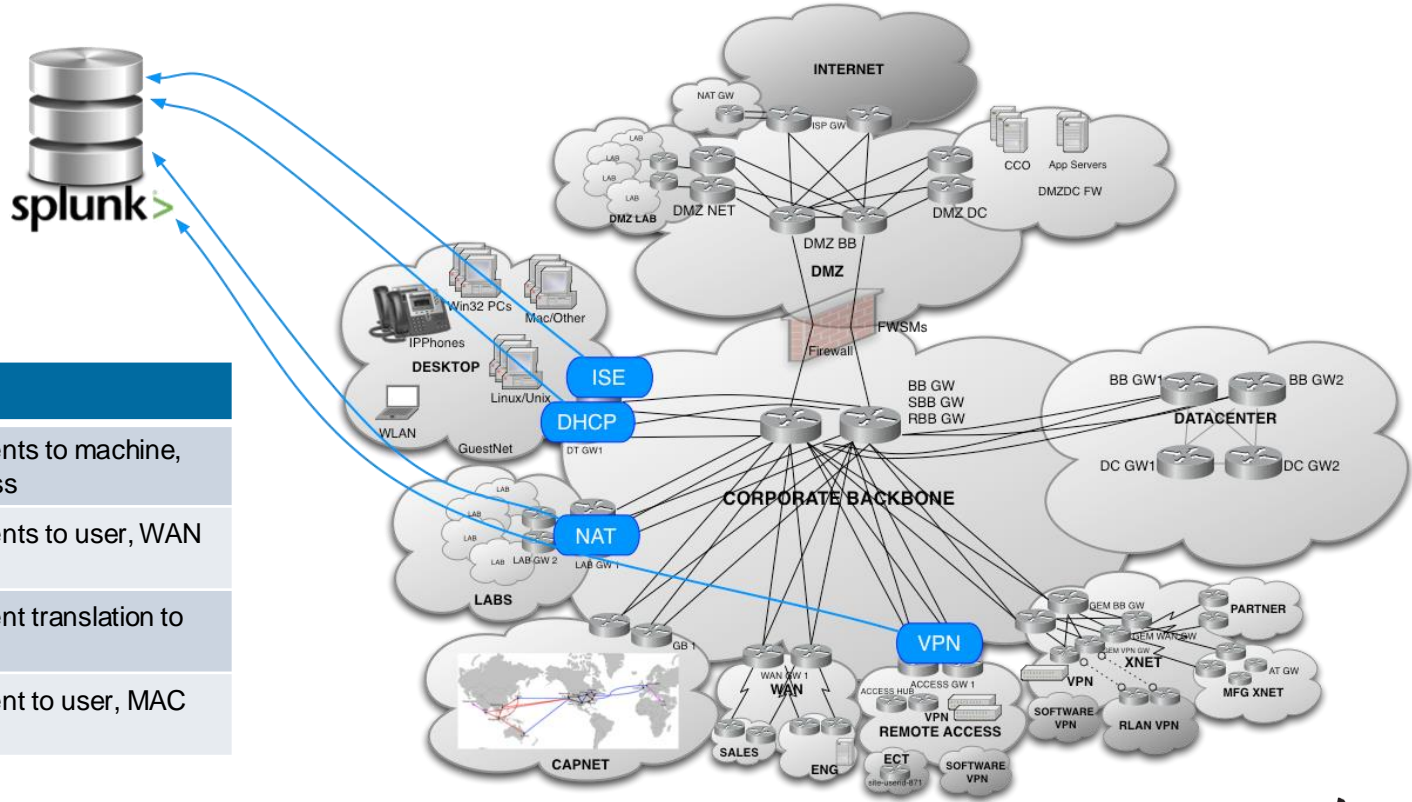
Modify known C&C server list via API





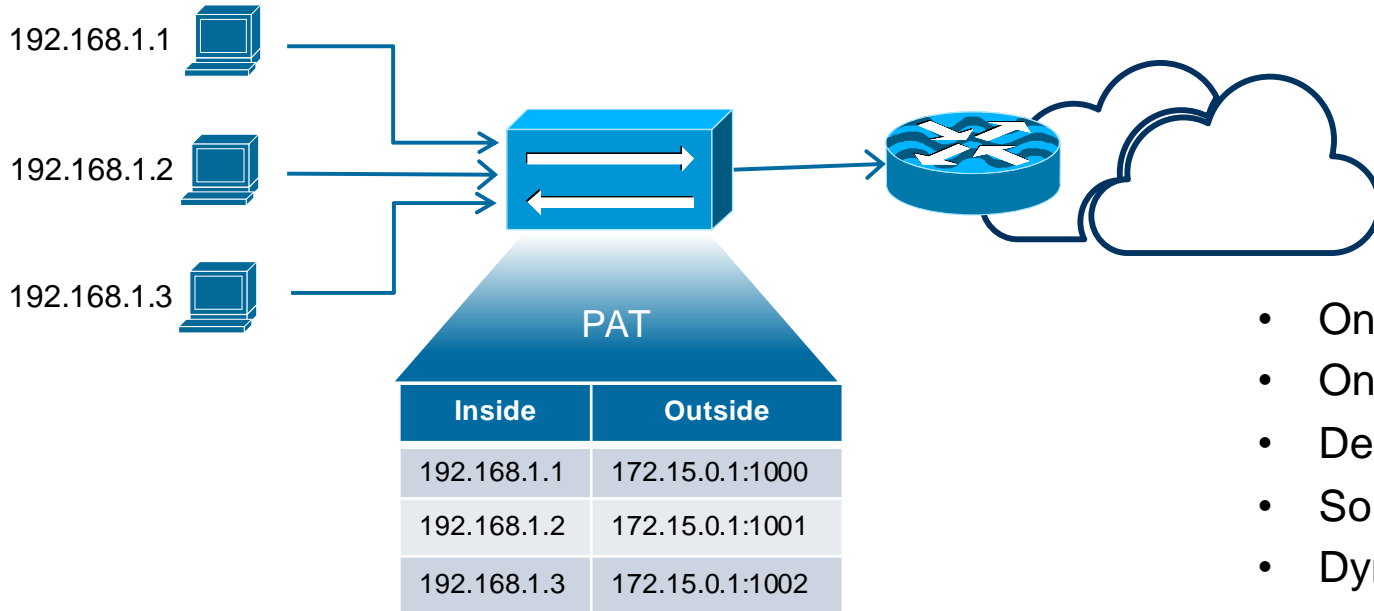
Attribution Data Sources

Attribution Data



Source	Provides
DHCP server	IP assignments to machine, MAC address
VPN server	IP assignments to user, WAN address
NAT gateway	IP assignment translation to RFC 1918
ISE	IP assignment to user, MAC address

NAT

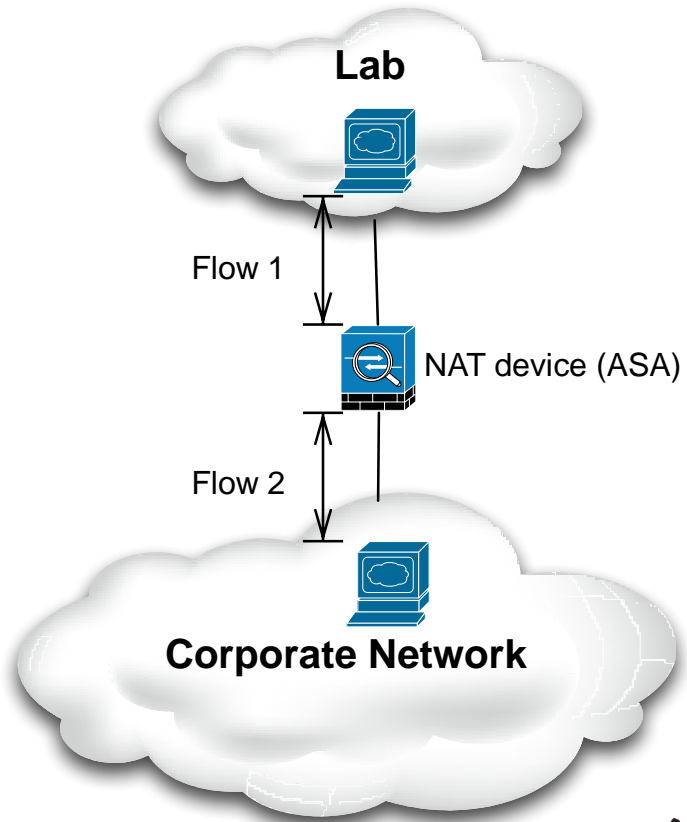


- One-to-one
- One-to-many
- Destination NAT
- Source/stateful/etc NAT
- Dynamic NAT

Before NAT Stitching

- Manual mapping required
- Xlate table logs

```
asa# sh xlate
53 in use, 57 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic,
r - portmap,
      s - static, T - twice, N - net-to-net
UDP PAT from inside:10.90.152.237/38021 to
outside:192.168.13.41/37236 flags ri idle 0:01:54 timeout
0:00:30
UDP PAT from inside:10.90.152.81/44232 to
outside:192.168.13.41/38292 flags ri idle 0:01:59 timeout
0:00:30
UDP PAT from inside:10.90.152.1237/44141 to
outside:192.168.13.41/38300 flags ri idle 0:01:59 timeout
0:00:30
```

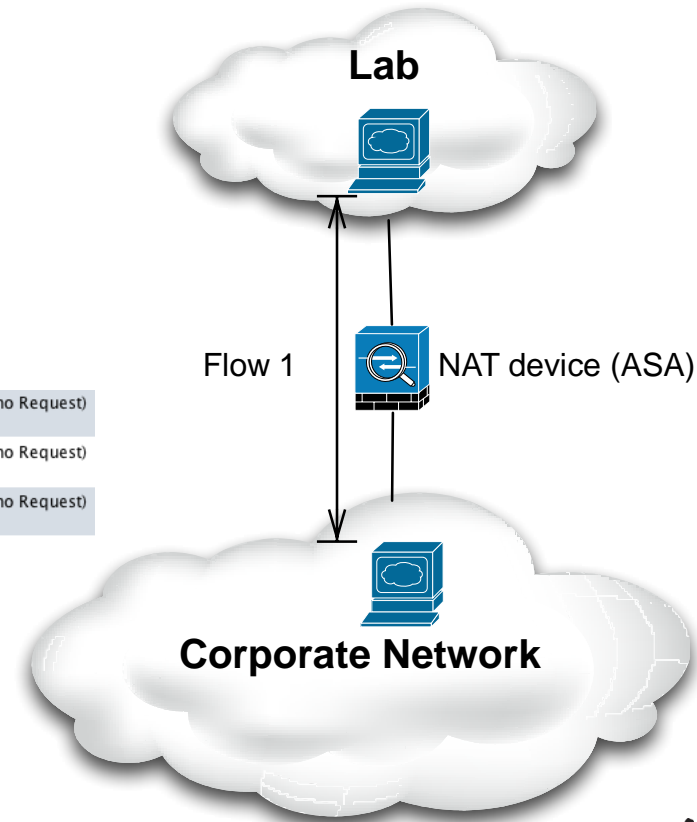


Cisco *live!*

After NAT Stitching

- Decreased investigation time

10.90.152.237	API ZONE: LAB, Private Addresses, ACL103	10.13.159.128	Private Addresses, ACL103	12 days 41 minutes	icmp (Echo Request)
10.90.152.237	API ZONE: LAB, Private Addresses, ACL103	10.13.159.132	Private Addresses, ACL103	12 days 41 minutes	icmp (Echo Request)
10.90.152.237	API ZONE: LAB, Private Addresses, ACL103	10.13.159.114	Private Addresses, ACL103	12 days 41 minutes	icmp (Echo Request)





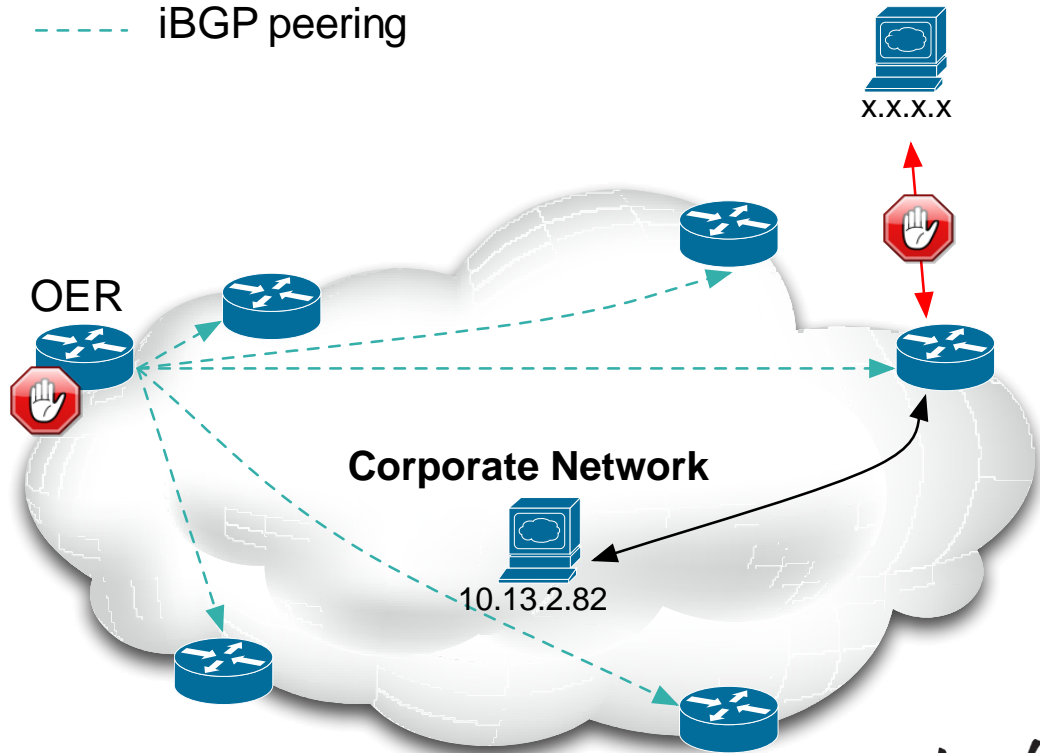
Mitigation Techniques

BGP BH

- Useful bidirectionally
- Quickly install null route
- Optimised Edge Routing (OER)
- uRPF required

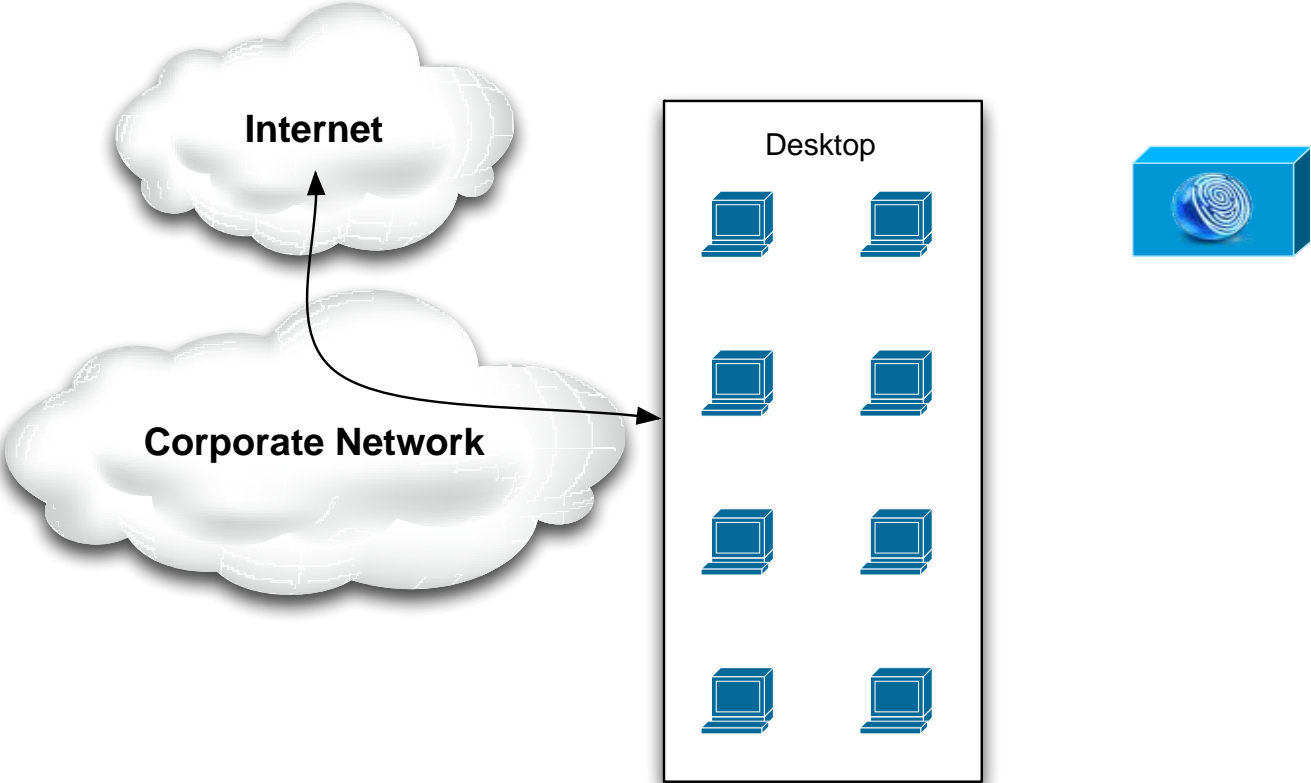
Install route on OER:

```
route x.x.x.x 255.255.255.255 null0
```

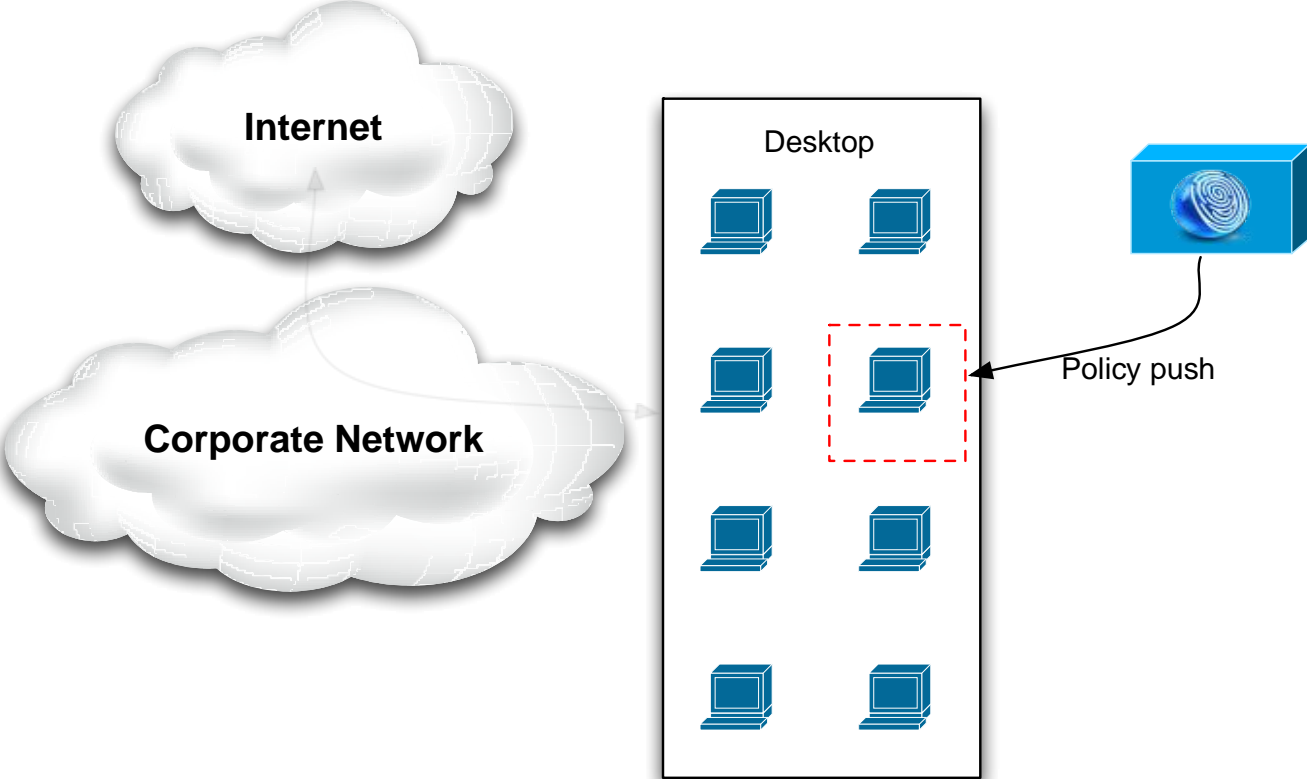


Cisco *live!*

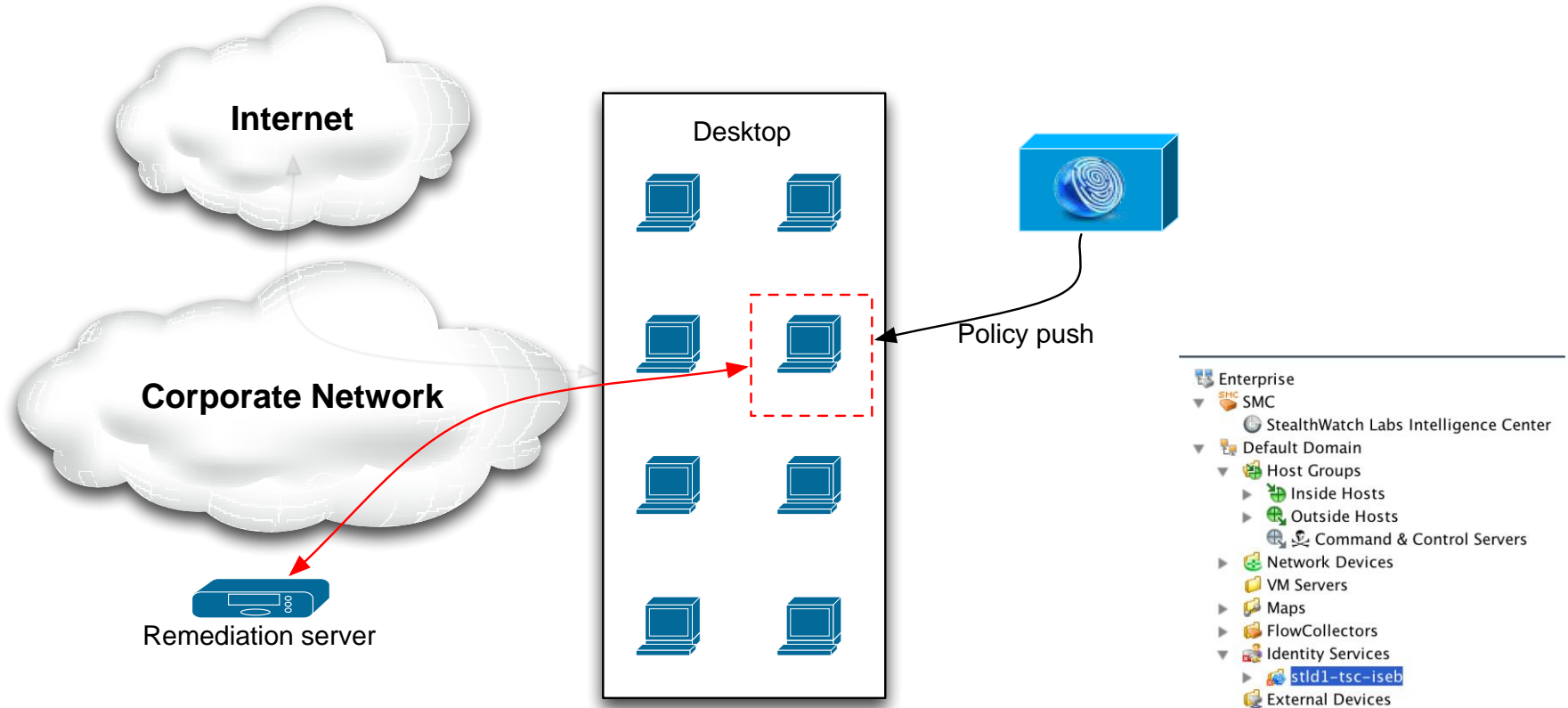
ISE Quarantine



ISE Quarantine



ISE Quarantine



Response Policy Zones (RPZ)

Mitigation Techniques

POLICY	RESULT	SYNTAX
NXDOMAIN	Returns non-existent domain	<code>badsite.com.rpz.mycompany.com CNAME .</code>
NODATA	Returns nothing	<code>www.badsite.com.rpz.mycompany.com CNAME *.</code>
Local Data	Returns a “walled garden” IP	<code>badsite.com A 192.168.7.77</code>
NO-OP	Allows subdomain exception to blocked domain *example.com is firewalled	<code>good.example.com CNAME good.example.com</code>

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



Special Circumstances

Missing Data Sources

- Causes and examples of workarounds
- Using policy as means to get data sources

Issue	Alternative
Spans disappear	Taps
Limited span support	Optical taps
Virtual environment limits ability to use taps	Virtual taps
Limited or no sampled netflow support	Netflow Generation Appliance

The Cloud:

As a consumer

The Problem:

- Loss of network visibility
- Loss of network controls
- Inability to mitigate
- Potential attribution gap
- Increase risk for data loss

The Solutions:

- Host based tools
- Policies
- Provider relationship

The Cloud:

As a provider

The Problem:

- Scalable monitoring toolset
- Openstack dependencies
- Platform security
- Mitigation
- Attribution
- IP Management

The Solutions:

- Host based tools
- Virtualised switch/span
- Tenant escalation procedures
- Acceptable Use/Terms of Service

Policies for Monitoring and Investigations



Official CSIRT Incident Response Handbook

1 Added by mn [REDACTED], last edited by [Matthew Valites](#) on Nov 22, 2013 ([view change](#))

This document contains the CSIRT Incident Response Handbook. It provides guidance for CSIRT staff engaged in incident response.

2.0 Organization

- [2.1 Computer Security Incident Response Team \(CSIRT\)](#)
- [2.2 Roles and Responsibilities](#)

3.0 Case Handling Procedures

- [3.1 Diversified Business Unit \(DBU\) IR Procedures \(Webex, Ironport, Linksys\)](#)
- [3.2 Special Engagement Procedures \(IPsoft\)](#)
- [3.3 Support for the used of the Information Sharing Traffic Light Protocol \(ISTLP\)](#)
- [3.4 Executive Support Escalation \(CxO Monitoring\)](#)
- [3.5 Cisco Cloud Services \(Nimbus\)](#)

- Critical vs. non-critical
- Who to contact
- Escalation procedures
- Define roles and responsibilities
- Coverage map

Targeted Environment Metadata

- Know your network addendums
- Detail network diagrams
- Data flows
- Behaviour baseline
- Escalation path
- Access to information



Operationalising

CSIRT Playbook

Operationalising

playbook | 'plā ,bŏk |

(noun)

A prescriptive collection of repeatable queries (reports) against security event data sources that lead to incident detection and response.




Incident Response Basics

Operationalising

- What am I trying to **protect**?
- What are the **threats**?
- How do I **detect** them?
- How do we **respond**?

Incident Discovery: Hunting () and Gathering ()

Operationalising

Method	Process
	Your security systems' indicators tell you about it as it happens
	Some one else tells you about indicators
	You discover indicators while hunting through logs

No Process is mutually exclusive of the other!



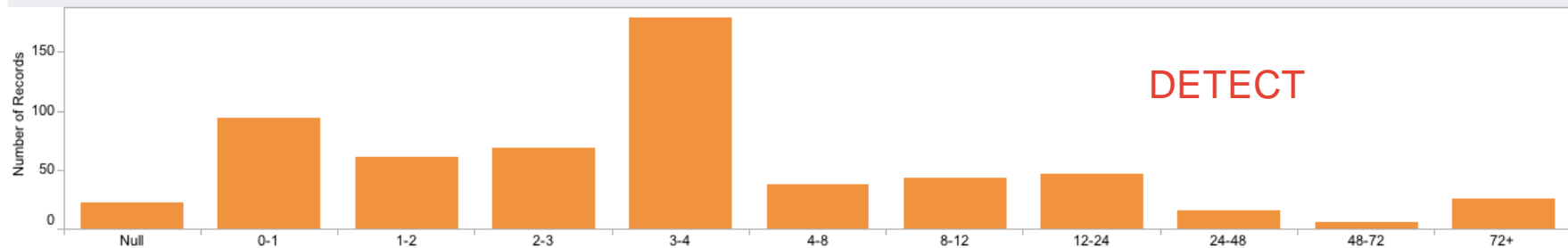
Demonstrating Value

Time To Detect / Time To Contain

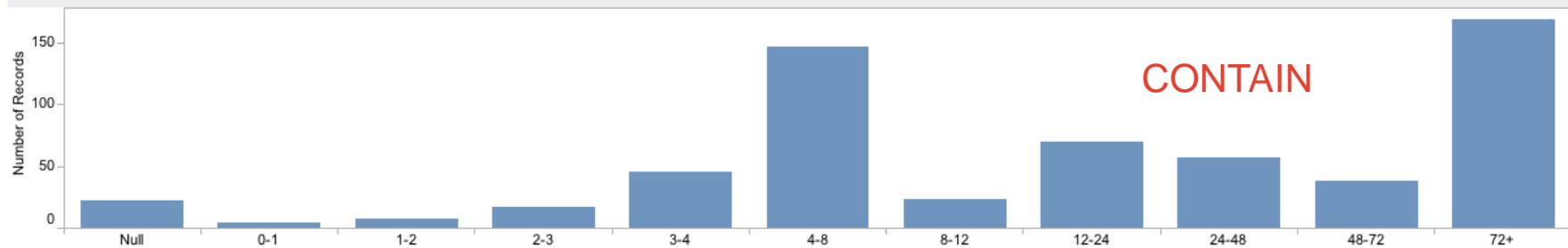
Demonstrating Success

The screenshot displays a web interface for case management. At the top, there are tabs for 'Case Information', 'Networking', 'Forensics', 'Legal Information', and 'DLP'. Below the tabs, there are input fields for 'Playbook ID', 'Notified By', and 'Incident Category'. A callout box highlights three time-related fields: 'First Activity Time', 'Detection Time', and 'Incident Containment Time'. Each field has a 'Click for Pop-up' button and is followed by 'UTC'. Below this callout, there is a 'Contacts' field with a text area and a note: 'Separate values with returns, whitespace, tabs, or commas.'

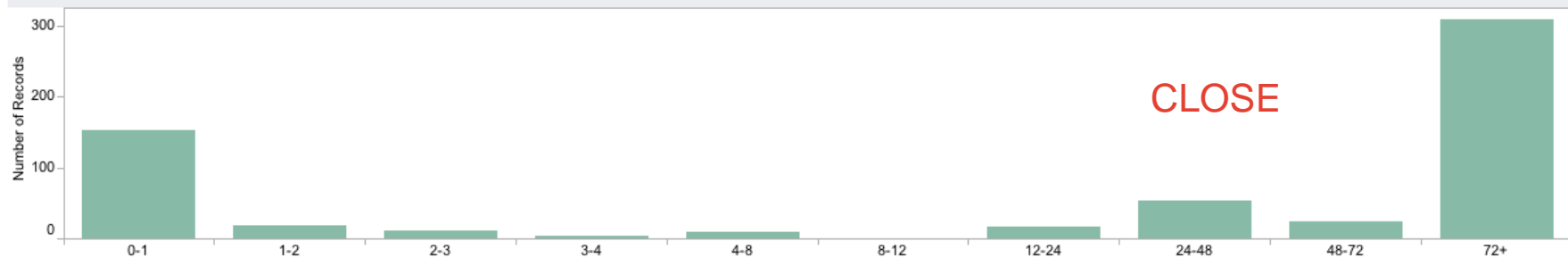
Time to **Detect** in Hours



Time to **Contain** in Hours



Time to **Close** in Hours



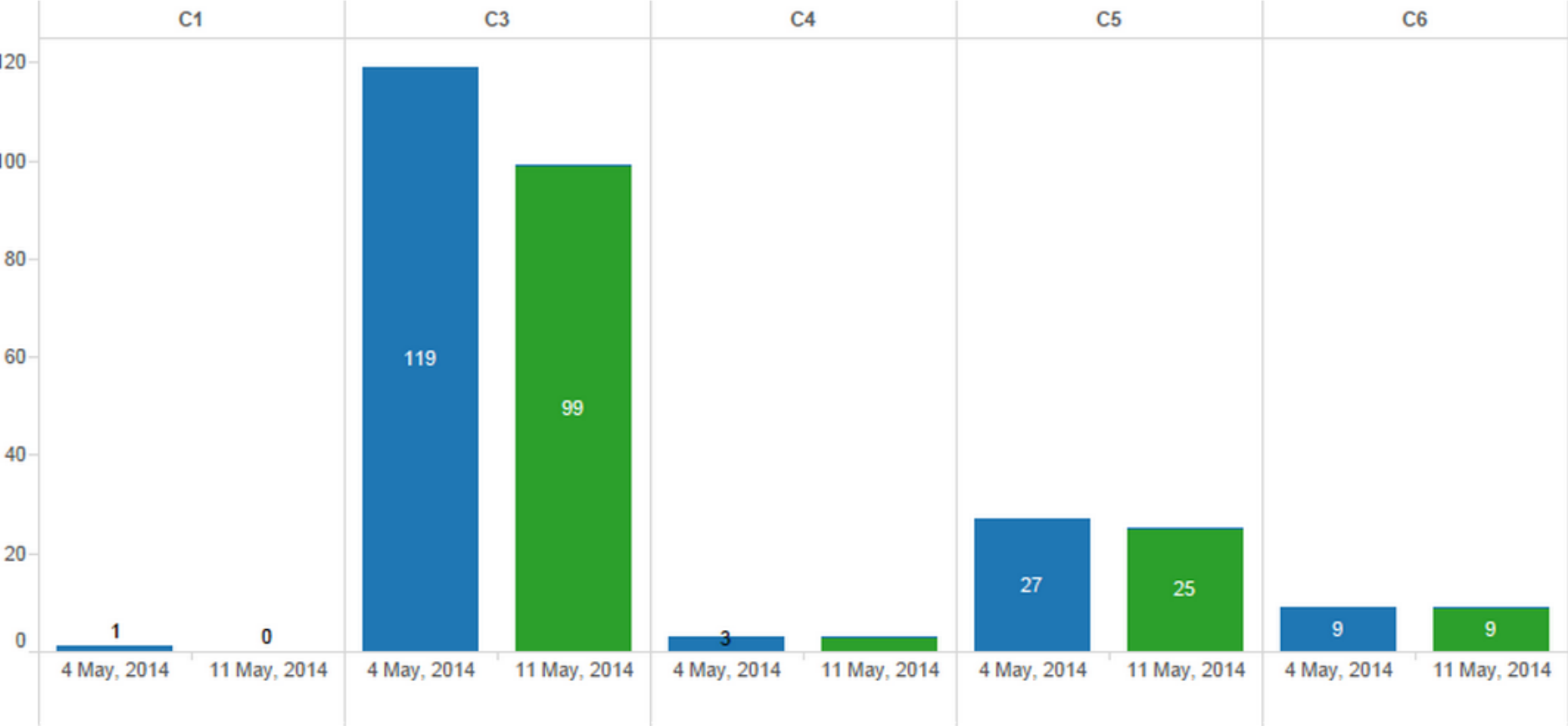
Incident Categories

Reference Table of CERT Categories

Category	Title	Description
CAT 0	Exercise / Network Defense Testing	Known vulnerability assessments, audits, Q/C incident tests, table-top exercises, etc.
CAT 1	Unauthorized Access	Logical or physical access without permission (regardless of awareness) to a Cisco network, system, application, data, or other resource from internal to external.
CAT 2	Denial of Service	<p>An attack that <i>successfully</i> prevents or impairs the normal authorized functionality of Cisco's networks, systems or applications by exhausting resources.</p> <p>This activity includes being the victim or participating in the DoS</p>
CAT 3	Malicious Code	<i>Successful</i> installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application.
CAT 4	Improper Usage	<p>Any acceptable-use ,lab, minimum host, general insecurity, or other policy violations, unscheduled vulnerability assessments, external vulnerability notification, etc.</p> <p>A Cisco employee violates acceptable computing use policies.</p>
CAT 5	Scans/Probes/Attempted Access	This category includes any activity that seeks to access or identify a Cisco asset, including computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.
CAT 6	Investigation	<i>Unconfirmed</i> incidents where evidence is inconclusive, or when supporting another team's investigation. Potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.

Incident Categories

Incident per Category - Week/Week



Detection Efficacy

Demonstrating Success

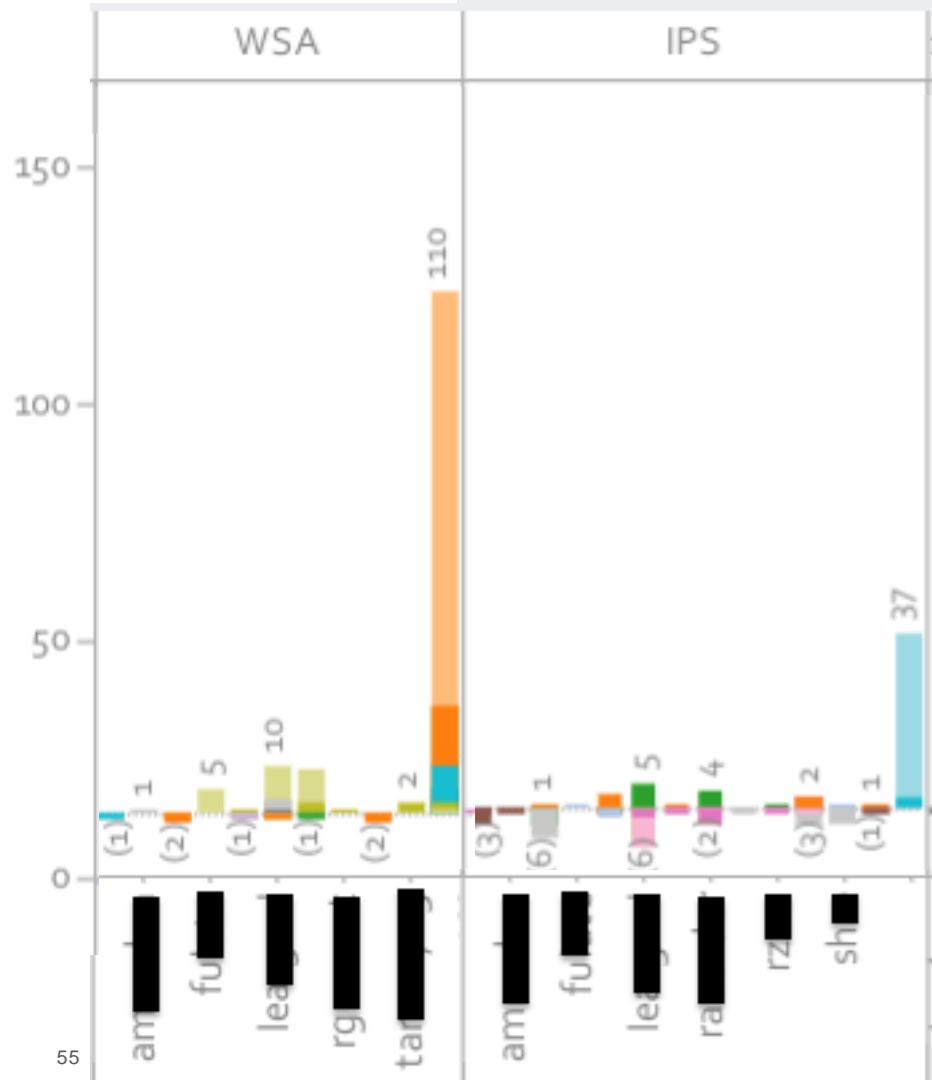
Efficacy	Definition
True Positive	The system correctly detected a valid threat against an extant risk as per the intended detection logic (where applicable).
False Positive	The system incorrectly detected a threat, or there is no extant risk.
Benign	The system correctly detected a valid threat, but there is no apparent risk due to the condition being expected. Example: Detecting web attacks from Infosec pen testing exercises.
Not Applicable	Indeterminable due to lack of data.

Detection Efficacy

Demonstrating Success

Metrics per:

- Data Source
- Play
- Analyst



Indicator Language

- Cybox
 - XMI Based
 - Used for STIX/Taxii
 - Allows Relationships
- IOC
 - XML based
 - Primarily host oriented
 - If/then structure for indicators
- Raw Text
 - Usually posted on internet forum/blogs
- CSV
 - Single indicator type to indicator



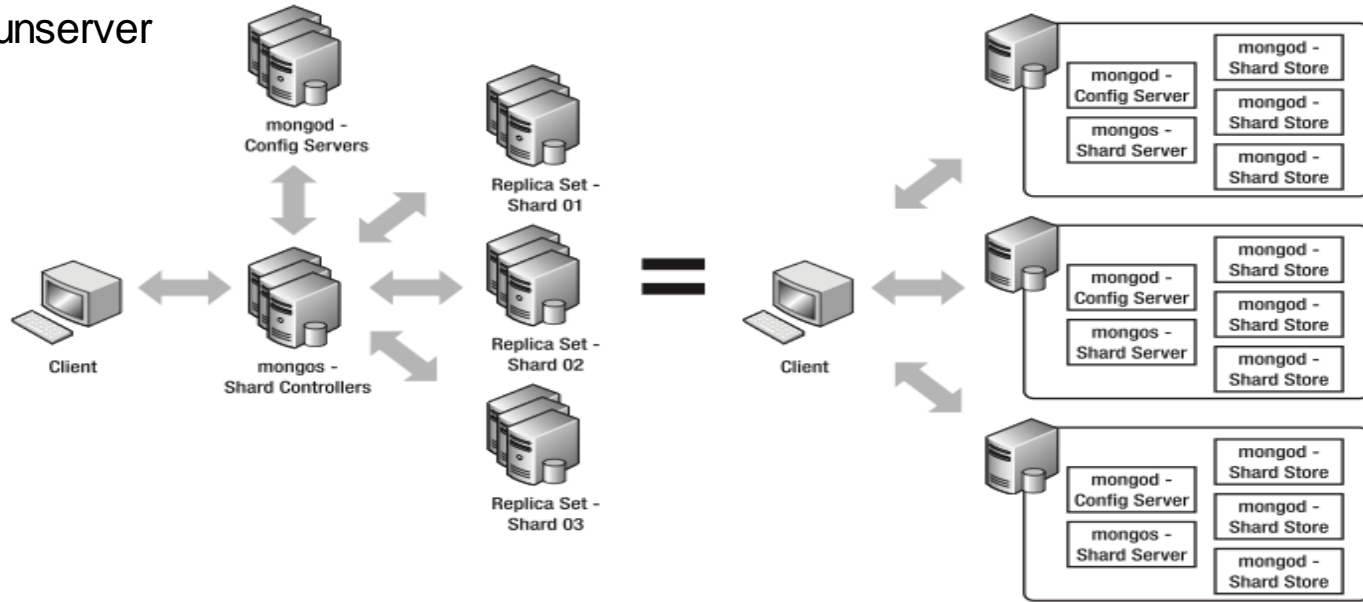
Indicator Sharing Classification (TLP)

Colour	Meaning
Red	Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.
Amber	Recipients may only share TLP: AMBER information with members of their own organisation who need to know, and only as widely as necessary to act on that information..
Green	Recipients may share TLP: GREEN information with peers and partner organisations within their sector or community, but not via publicly accessible channels.
White	TLP: WHITE information may be distributed without restriction, subject to copyright controls.

Source: <http://www.us-cert.gov/tlp>

What is CRiTs?

- Python/Django front end UI
 - Apache or Django runserver
- MongoDB backend
 - Fault Tolerant
 - High Performance
 - NO SQL
 - Mongo FS for files
- Document based
 - Files and metadata



Top Backdoors

Name	Samples
DPD	1
PIVY	

Top Campaigns

Name	Emails	Indicators	Samples
Group 3	0	2067	1
Group 17	0	818	11
Group 16	0	68	0
Group 13	0	13	0
Group 10	0	0	0

Latest Indicators

Value	Type	Date Added	Campaign	Source	Status
mx.xmlflash.net	Domain	2013-11-14	Group 3	OTHER	New
www.nbsd.k12.ms.us	Domain	2013-11-14	Group 4	OTHER	New
/serv/pte.exe	Domain	2013-11-14	Group 4	OTHER	New
www.myspace-login.com	Domain	2013-11-14	Group 4	OTHER	New
2014 individual income tax credit policy	String	2013-11-14	Group 4	OTHER	New

Recently Added/Modified Samples

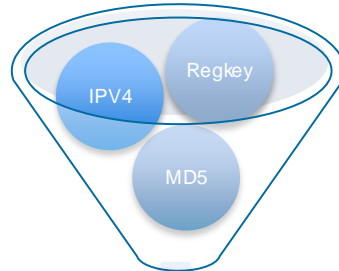
Filename	Size	Filetype	Receive	Backdoor(v)[C]	CVE
jack246.exe			08/12/2013		
Sample 60eed7a7c5f4f4aeace594e2e4d180a0.exe_carver			08/12/2013		
c5eb1cff314e4d682b1315dfab44e7dd			08/12/2013		
Sample 68aee94684ba33d1e5d97d7d27d0fe13.exe_carver			08/12/2013		

Indicator Actions

Current

In Progress

Future



CRITS

Prevent

BGP

ESA

DNS RPZ

HIPS

AV

WSA

Detect

NetFlow

host IDS

Mandiant

LUPA

pDNS

Syslog

Share

CSIRT

Govt

CDSA

Partner

SBG

Lookup Query

300042-INV-WSA-INTEL: TLP:GREEN URL Indicators

```
index=wsa earliest=-24h [inputlookup intel-url-green |  
  where like(confidence, "medium") AND NOT like(confidence, "benign") |  
  eval cs_url=indicator |  
  fields cs_url] |  
  `Intel-WSA-Output-Format(intel-url-green)`
```

20 Per Page ▾ Format ▾ Preview ▾

SourceIP ▾	FirstEvent ▾	LastEvent ▾	EventCount ▾	HTTP_CODE ▾	UserAgent(s) ▾	Client_MIME_Type ▾	MethodType(s) ▾	RequestedURLs ▾	Intel Indicator(s) ▾	Intel Source(s) ▾	Intel References ▾
10.79.100.23	05/15/2014 11:32:27 UTC	05/15/2014 11:32:30 UTC	2	200	Mozilla/5.0 (X11; Linux i686) AppleWebKit/537.36 (KHTML, like Gecko) Ubuntu Chromium/31.0.1650.63 Chrome/31.0.1650.63 Safari/537.36	text/html	GET	http://www.kennedywilson.com/	http://www.kennedywilson.com/	TLP:GREEN_CISCP	IB-13-10644

- Indicators
- Source
- References

Continue Your Education

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



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

Cisco *live!*



Thank you.

Cisco *live!*



CISCO