
TOMORROW
starts here.
CISCO
Cisco live!

Cisco Advanced Services – MTD – CTI

BRKSEC-2693

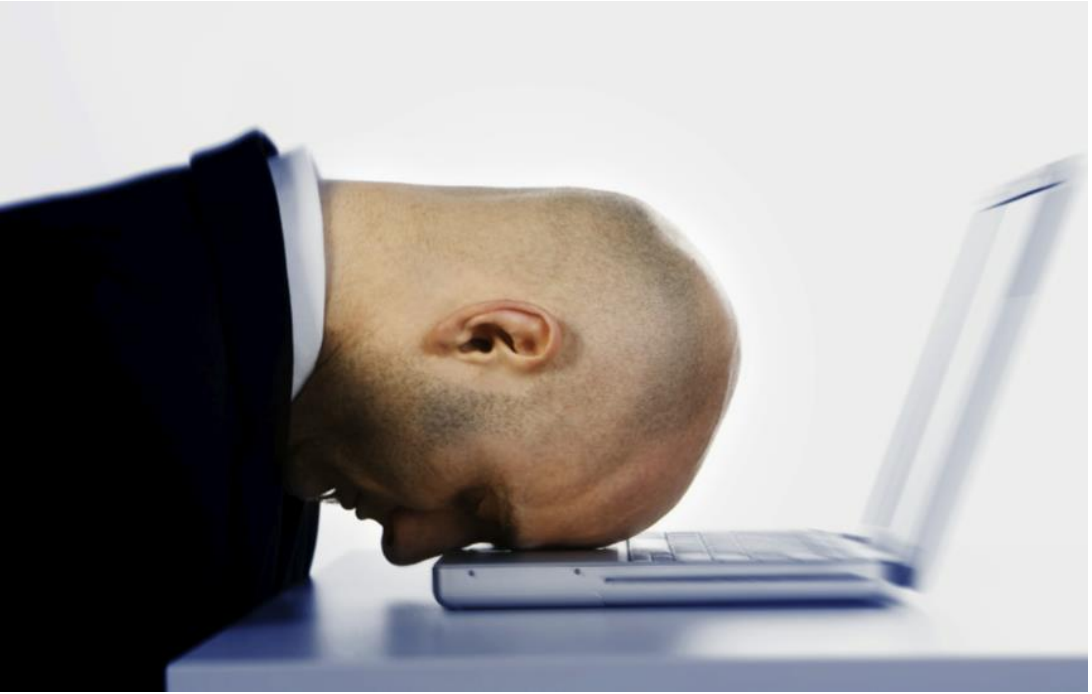
Alan Downey

Solutions Architect

#clmel

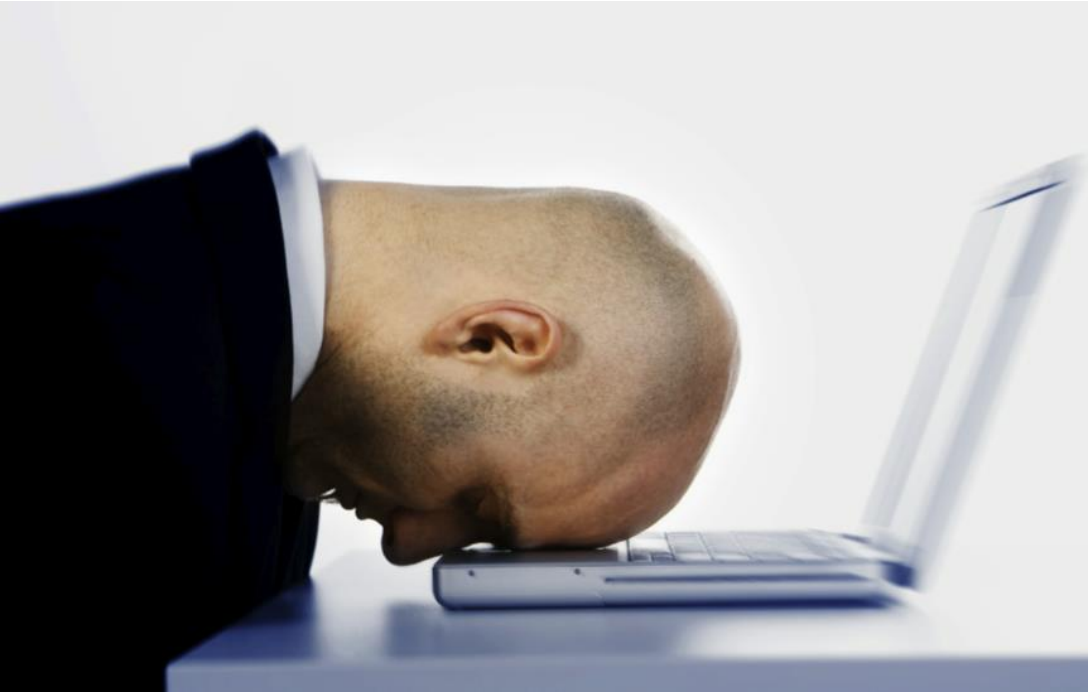
Cisco live!

The Situation…



- Worm propagation
- DOS symptoms
- Limited endpoint security
- No IPS
- Nothing left to do but …

The Ask…



- Identify Infected hosts
- Prevent further propagation.

The Solution…

- Pre-existing procedure
- Used IOS Router features to identify & drop worm propagation.

The Solution…

- Pre-existing procedure
- Used IOS Router features to identify & drop worm propagation.

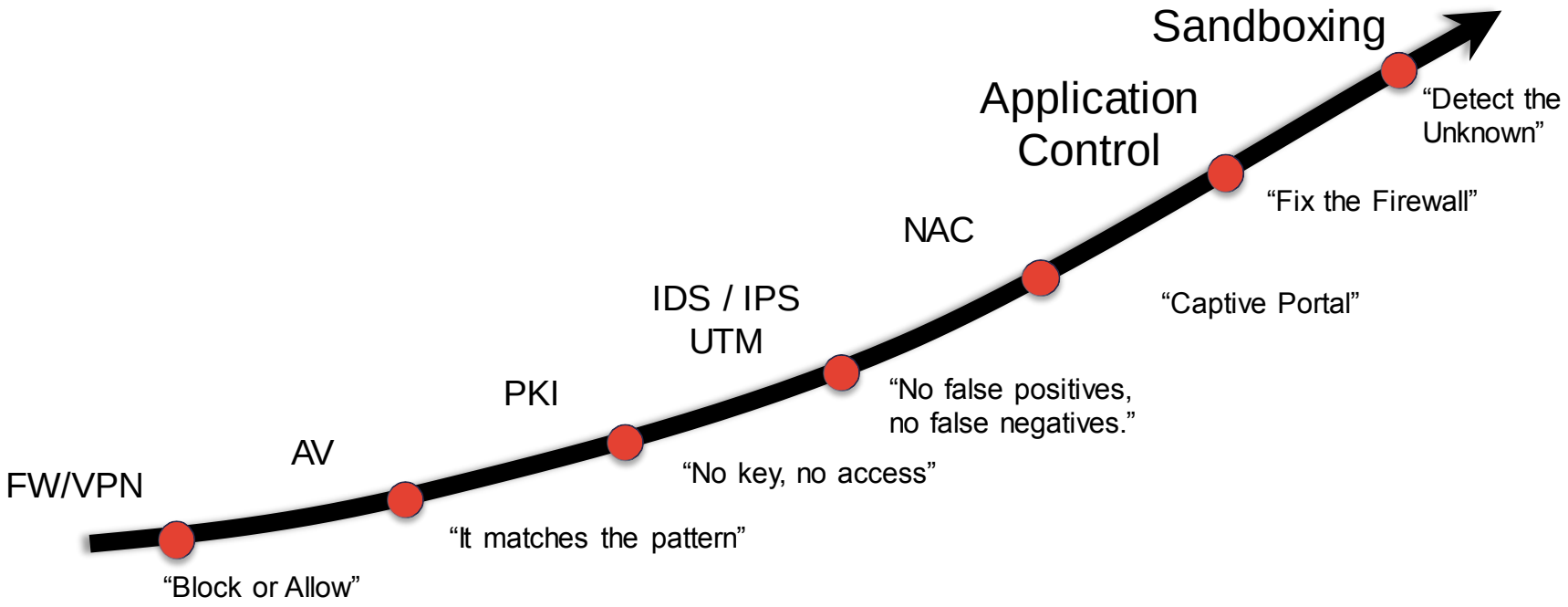
Using Network–Based Application Recognition and ACLs for Blocking the "Code Red" Worm

Document ID: 27842

Contents

Since Then…

The Silver Bullet Does Not Exist…



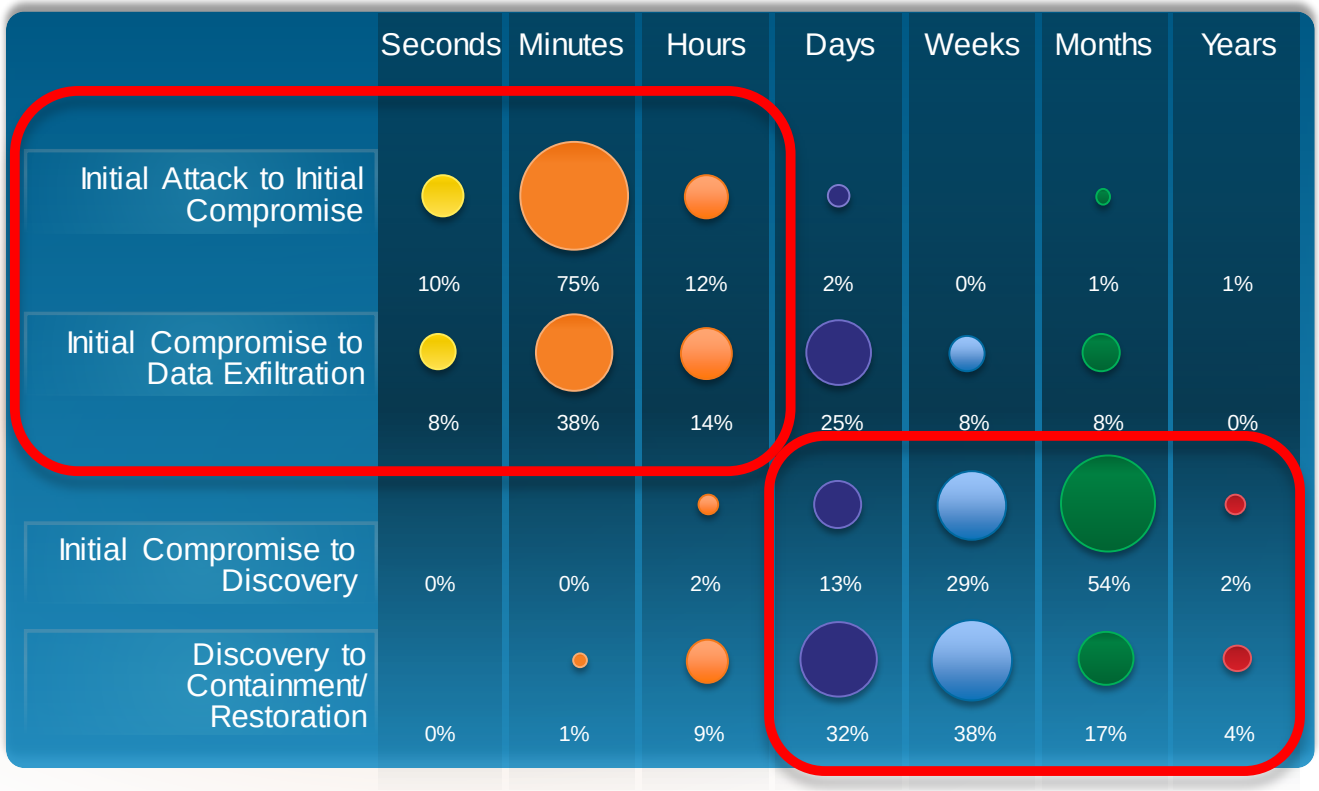
Core Challenges for Current Cyber Incident Response

- For most respondents, security incidents are on the rise
- Most incidents today are detected by people, not technology
  - Traditional SIEMs are only successful in identifying an incident 1/3 of the time
- Successful response is often impaired by
  - Insufficient skilled resources
  - Lack of threat intelligence
  - Poor information sharing
- Over 2/3 of executives believe that an effective incident response is an opportunity to enhance the company's reputation
- 70% of small firms and 80% of large firms engage external help, particularly around hard-to-retain forensics skills

Source: Economist Intelligence Unit, "Cyber incident response: Are business leaders ready" (March 2014)

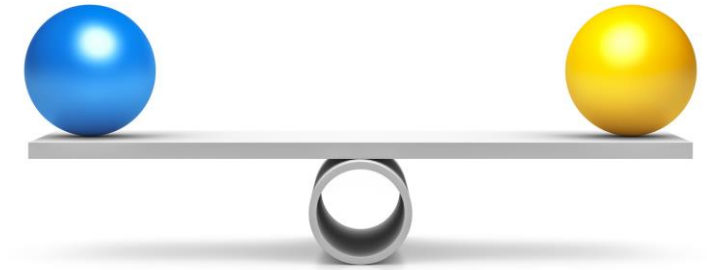
Breaches: Success In Hours, Undetected For Months

- **Breached in Minutes**
- **Months to Detect**
- **Weeks to Contain**



Source: Verizon DBIR 2014

Both Sides of Reality



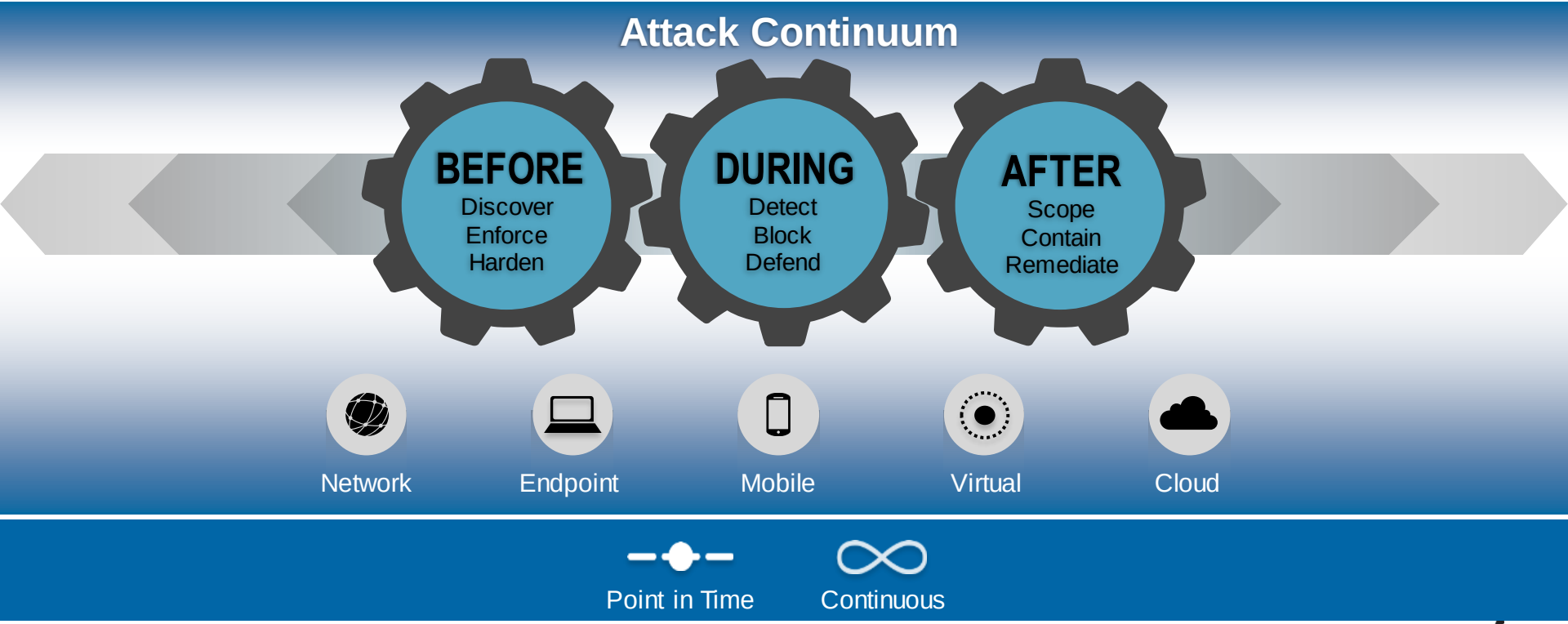
Statistic	Conclusion
“The majority of likely attacks can be prevented by doing the basics”	We need to do the basics well.
“Field efficacy for AV products for new malware is closer to 50% than the 99+% claimed by testing organisations.”	… but we need to be ready for the rest.

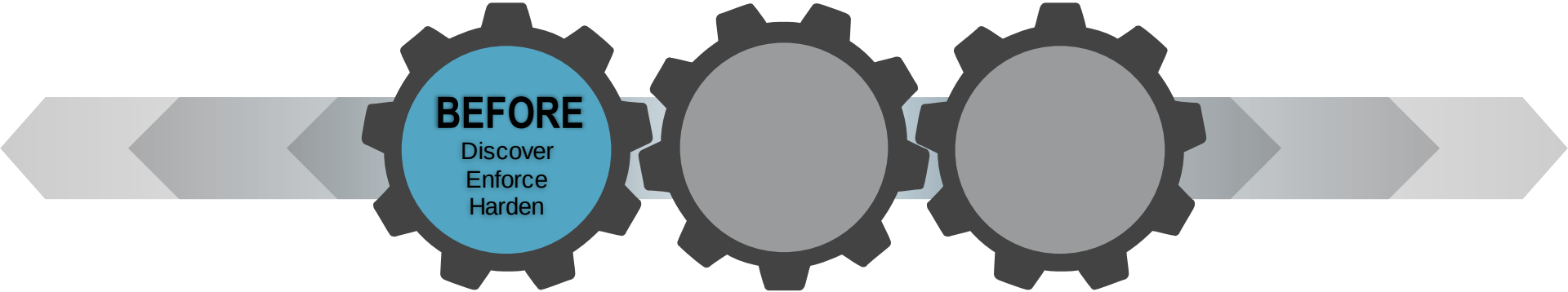
Customer Asks..

Work with us..

- To assess our current security posture.
- To maximise value from the tools and controls we already have.
- To deploy new technologies where required.
- To gain efficiencies by getting controls to work together
- To detect and respond to malicious behaviour more quickly.

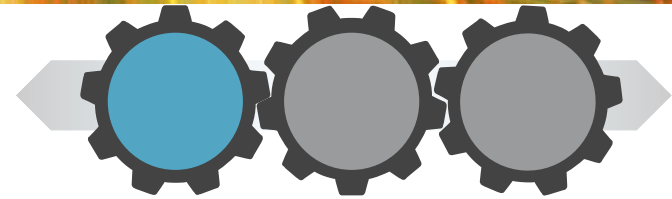
The Threat-Centric Security Model

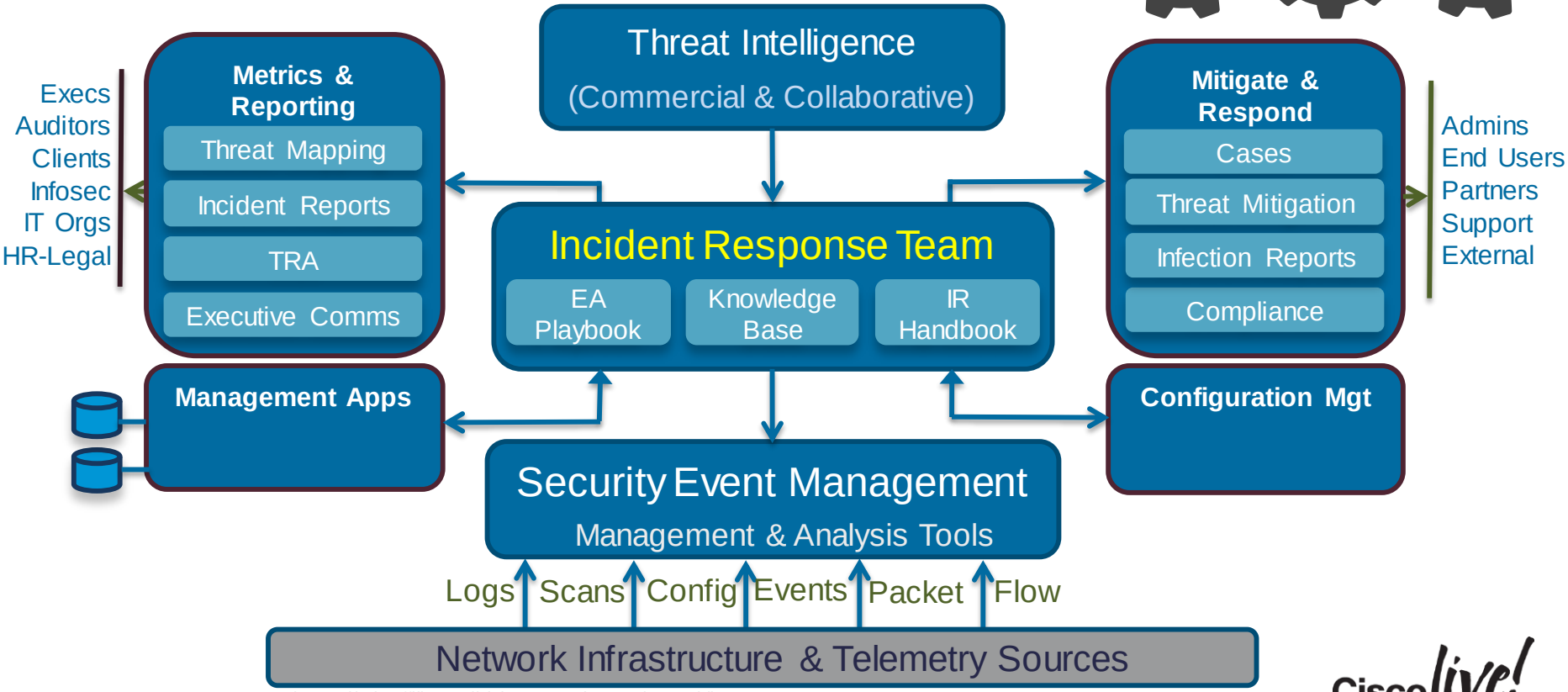




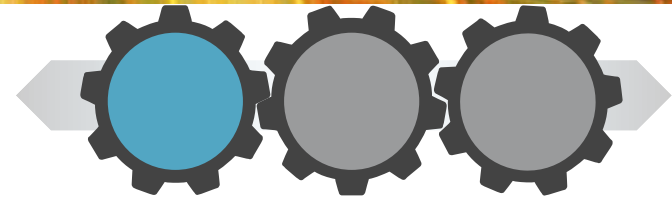
Why Are We Here?

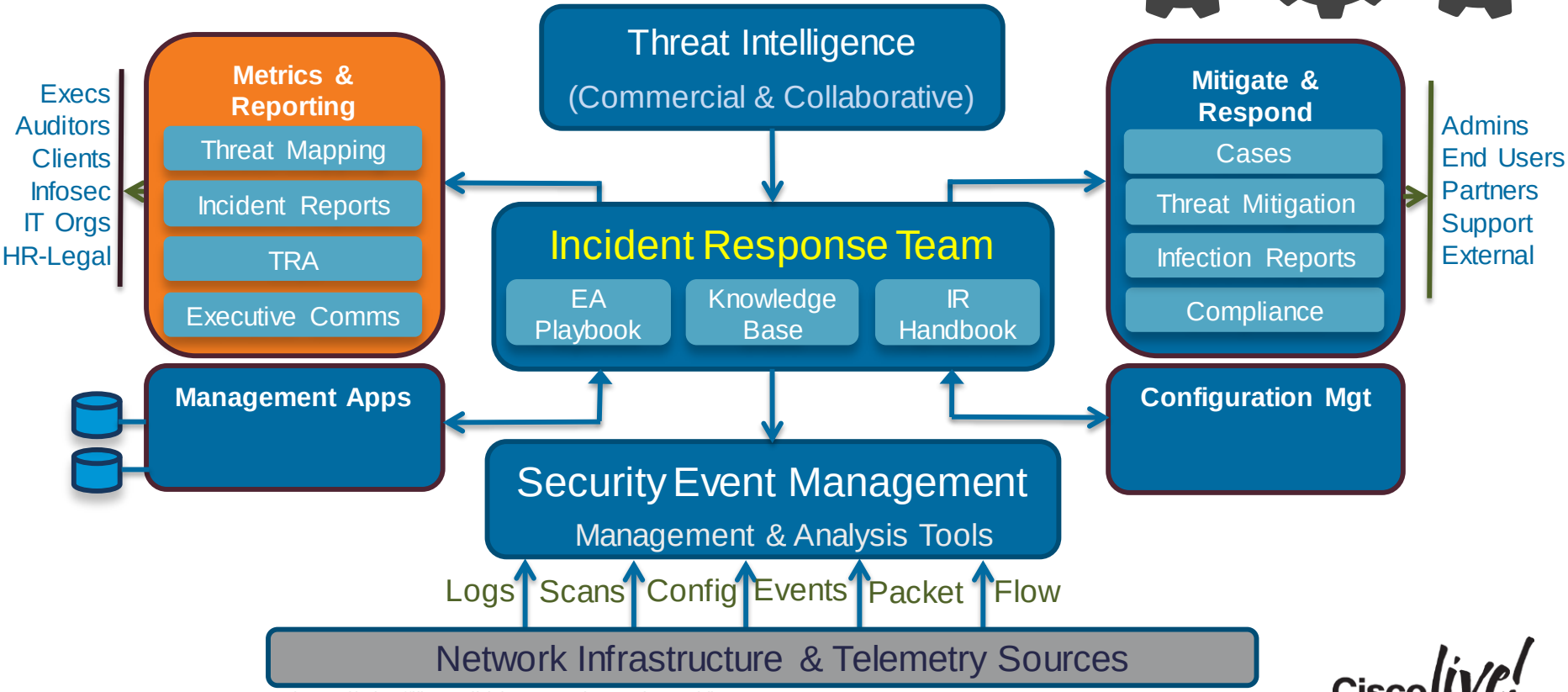
Why Are We Here?



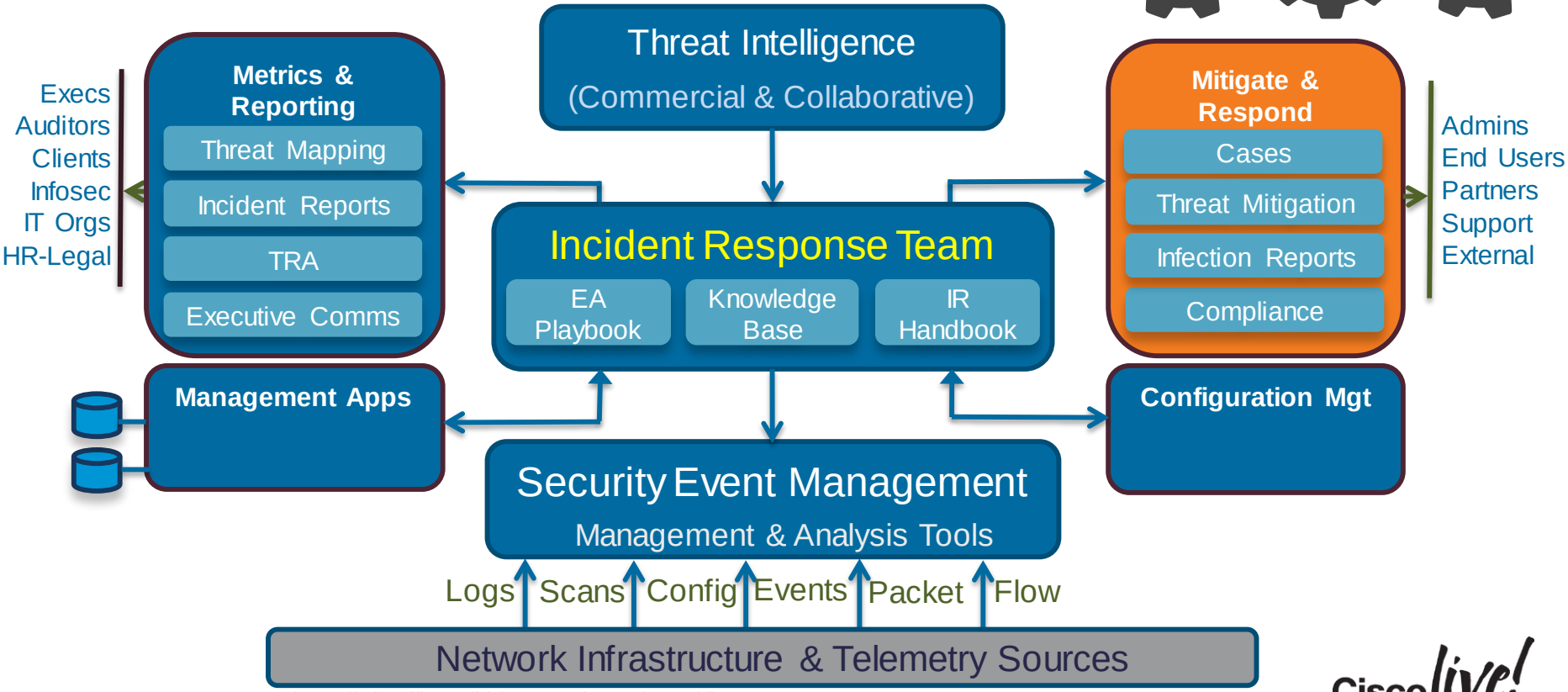


Why Are We Here?

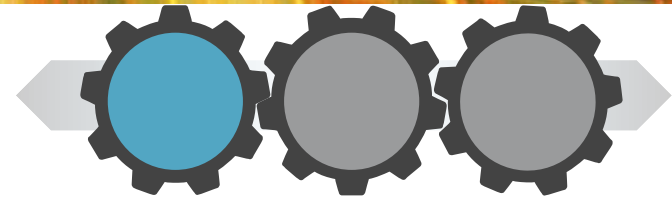


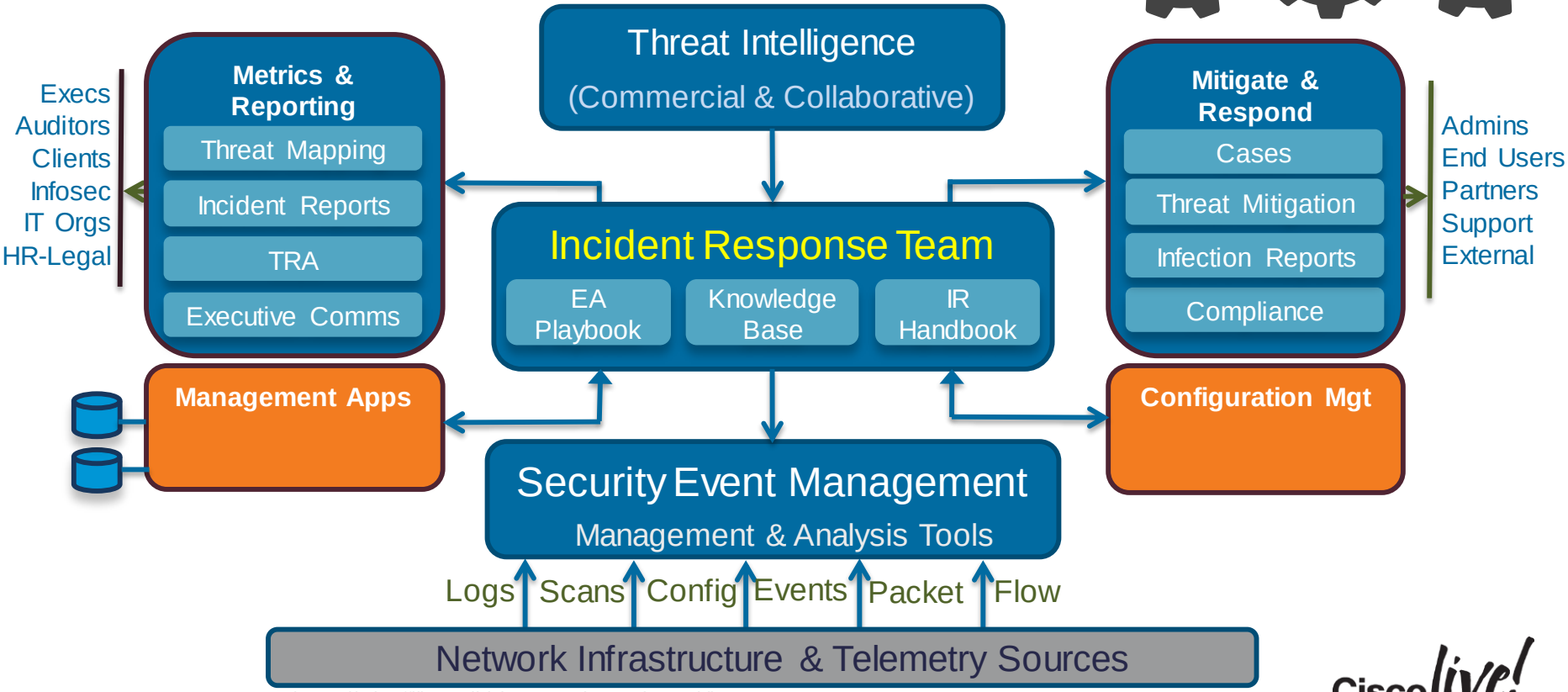


Why Are We Here?



Why Are We Here?





Lets Ask Ourselves..

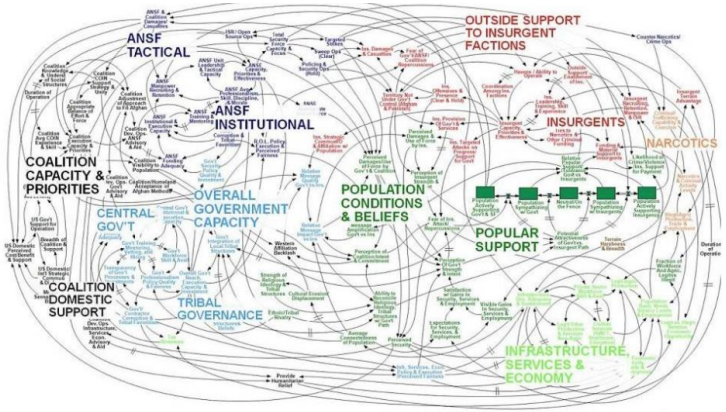
- What are we protecting?
- How can we see it ?
- What are the relevant threats ?
- How ready are we ?

What Are We Protecting?

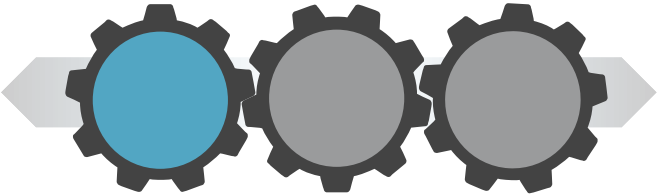
- Architecture / Designs
- Structured, Modular, Predictable
- CMDB, Asset Lists, IPAM
- Directory

What Are We Protecting?

- Architecture / Designs
- Structured, Modular, Predictable
- CMDB, Asset Lists, IPAM
- Directory



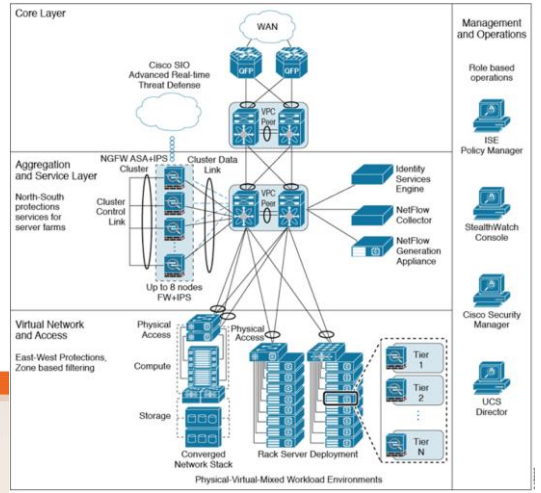
What Are We Protecting?

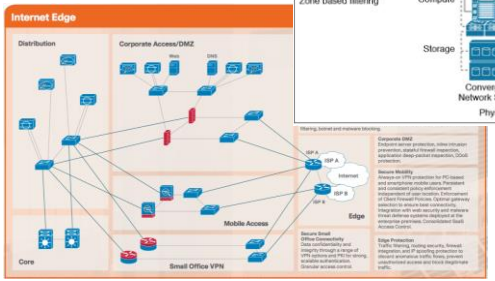


- Architecture / Designs
- Structured, Modular, Predictable
- CMDB, Asset Lists, IPAM
- Directory

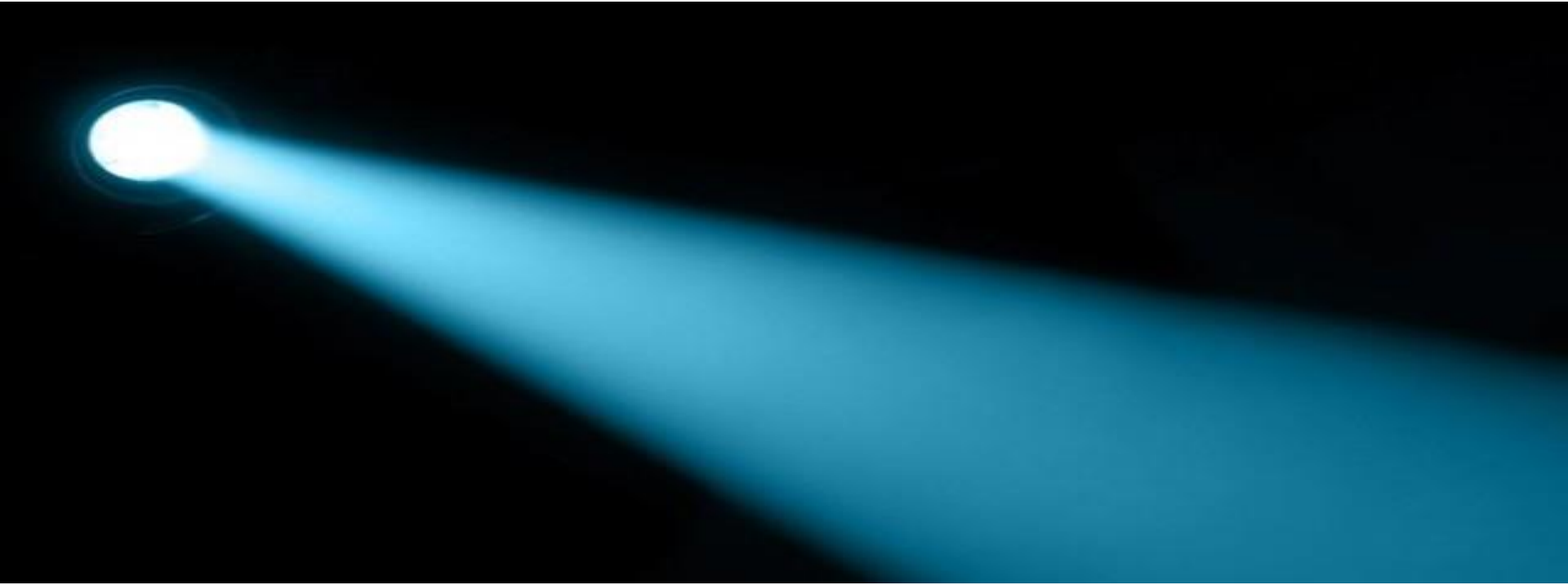
What Are We Protecting?

Reference	URL
Cisco SAFE Architecture	http://www.cisco.com/go/safe
Cisco Validated Designs	http://www.cisco.com/go/cvd





How Can We See It?

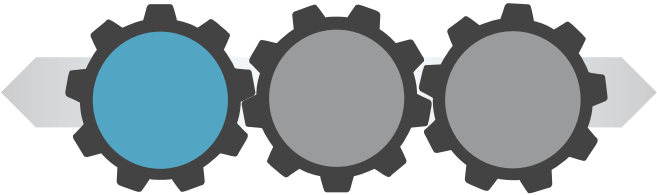


How Can We See It?

- System and Data Changes
- Network Activity
- Authentication, Authorisation
- Resource Access
- Malware Activity
- Failure and Critical Errors

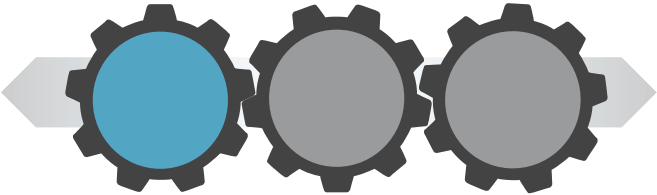
Source: SANS Top 6 Categories of Critical Log Information

How Can We See It?



SANS Categories	Sources, Patterns, and Indicators
AAA	Login Activity, Time Spent, Privileges, Endpoint Posture, AAA Logs, Directory Logs
System, Data Changes	File Hashes, AAA Logs, Host IDS, Change Records, ...
Network Activity	Netflow Stats, Firewall Conns, Proxy Logs, IDS Events, DNS Logs, Time Spent...
Resource Access	Email Stats, Proxy Logs, Netflow, Endpoint Posture, Directory Logs, ...
Malware Activity	File Downloads, Email Attachments, Firewall Conns, Malware Engine Scans…
Failure, Critical Errors	CPU, Memory, Disk, Process

How Can We See It?



Event Type	Source	Events
Attribution	DHCP Server	IP Assignments to machine , MAC Address
	VPN Server	IP Assignments to User, WAN Address
	Net Gateway	IP Assignment translation to RFC 1918
	802.1x Auth	IP Assignment to user, MAC Address
System Activity	Server syslog	AAA, Service Start/Stop, Config Changes, FireAmp
Web Proxy logs	Web Proxy (WSA)	Web Malware downloads, C2 Checkins
Spam Filter logs	ESA	Malicious URLs and Attachments, Policy violations
Firewall logs	ASA, WAF	Accepted and Denied Connections
Web Server logs	Web Servers	Access logs, Error logs

What Does It Look Like?

Device Type	Protocol	Sample
ASA Firewall	Syslog	`Jul 02 2014 23:14:06: %ASA-5-106100: access-list inbound denied tcp outside/193.201.30.23(135) inside/193.201.30.23(1922) hit-cnt 1 first hit [0x91c26a3, 0x0]`
Email Security Appliance	SCP / FTP / Syslog	`Thu Jul 02 23:15:54 2014 Info: MID 245170 Message-ID '<194961.85741.qm@web65710.mail.ac4.yahoo.com>'`
Web Security Appliance	SCP / FTP / Syslog	`1343913291.98 70 91.208.184.24 TCP_MISS/200 3454 GET http://www.flashgames247.com/thumb/80x70/images/ …`
Cisco IPS	HTTPS (SDEE)	`2014-07-02 17:58:34,670 - INFO - 1343894300486157000 eventid="6821322601693" hostId="ips.acme" sig_created="20061120" sig_type="other" severity="informational" app_name="sensorApp" appInstanceId="1588" signature="5575" …`
Generic IOS	Syslog	`Jul 2 23:24:20 10.48.24.32 Aug 2 2014 13:24:20 ace.acme: %ACE-3-251008: Health probe failed for server 192.168.111.12 on port 443 …`

What Does It Look Like?

Device Type	Protocol	Sample
Sourcefire	HTTPS (eStreamer)	rec_type=400 rec_type_simple="IPS EVENT" event_sec=1409300614 event_usec=919489 sensor=10.67.34.71 event_id=258025 msg="APP-DETECT failed FTP login attempt" sid=13360 gid=1 rev=6 class_desc="Misc Activity" class=misc-activity priority=low src_ip=192.168.100.98 dest_ip=192.168.10.18 …
Cyber Threat Defence (Lancope)	Syslog	Aug 29 17:59:00 stl-as-n07-cyber-smc-1.cisco.com Aug 29 16:59:00 stl-as-n07-cyber-smc-1 StealthWatch[2359]: alarm_category_name="Anomaly", alarm_severity_name="Major", alarm_status="ACTIVE", alarm_type_name="High Target Index", …
Wireless LAN Controller	Syslog	Aug 30 13:55:28 n07-3850-1-wlc.cisco.com 47920: 0.0.0.0: Aug 30 03:59:02.892: %EPM-6-POLICY_APP_SUCCESS: Policy Application succeded for Client [0.0.0.0] MAC [40f3.0868.59d5] AuditSession ID [0a43223754014c0600007e44] for POLICY_TYPE [URL Redirect] …
Cisco ISE / TrustSec	Syslog	Aug 31 15:08:13 stl-as-n07-ise-1.cisco.com Aug 31 15:08:14 stl-as-n07-ise-1 CISE_Passed_Authentications ... NOTICE Passed-Authentication: Authentication succeeded, ConfigVersionId=7, Device IP Address=10.67.34.55, DestinationIPAddress=10.67.34.38,…

Looking Closer - ASA

```
Aug 02 2014 23:14:06: %ASA-5-106100: access-list inbound denied tcp outside/173.246.103.92(1922)
inside/192.168.10.18(135) hit-cnt 1 first hit [0x91c26a3, 0x0]
```

Source

src_ip	173.246.103.92
src_port	1922
src_if	outside

Metadata

sourcetype	cisco:asa
host	asa5585-2
_time	Aug 02 2014 …
source	syslog_tcp
eventtype	firewall_deny

Destination

dest_ip	192.168.10.18
dest_port	135
dest_if	inside

Outcome

action	blocked ("denied")
cause	Firewall Drop
direction	inbound

Looking Closer - Netflow

```
router# show flow monitor CYBER cache
..
IPV4 SOURCE ADDRESS:        192.168.100.100
IPV4 DESTINATION ADDRESS:   192.168.20.2
TRNS SOURCE PORT:           47891
TRNS DESTINATION PORT:      443
INTERFACE INPUT:            Gi1/1/1
IP TOS:                     0x00
IP PROTOCOL:                6
ipv4 next hop address:      192.168.20.2
tcp flags:                  0x1A
interface output:           Gi0/0/0
counter bytes:              1482
counter packets:            20
timestamp first:            8:30:00.456
timestamp last:             8:30:00.943
ip dscp:                    0x00
ip ttl min:                 127
ip ttl max:                 127
application name:           nbar secure-http
…
```

Who ?

Where ?

How ?

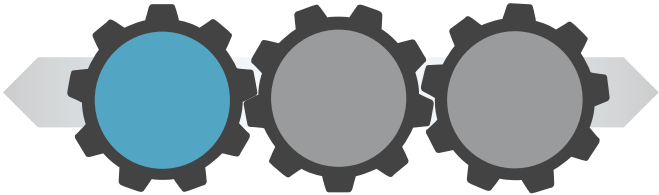
When ?

What ?

Looking Closer – Email Security

- Transactional Data
  - ICID / MID / DCID
- MTA Information
  - address <…> reverse dns host <…> verfied <…> - DNS info about the sending MTA
  - SG <…> … SBRS <…> - HAT group and SenderBase score details
- SMTP Conversation Details
  - From: <…> … To: <…> - sender and recipient
- Key Message Headers
  - Message-ID | Envelope From / To | Subject | Message Size
- Processing
  - AV/AS Verdicts | DLP Verdict | Attachment Info | Content Filters

Looking Closer – Web Security



```
accesslogs_splunk_tcp: Info: 1390159677.065 5 192.168.100.252
```

Timestamp

Elapsed Time (ms)

Client IP Address

Response Size (bytes)

```
TCP_MISS/200 441 HEAD http://ds.download.windowsupdate.com/ -
```

Cache Result / HTTP Status Code

Request Method

Request URL

User Identity

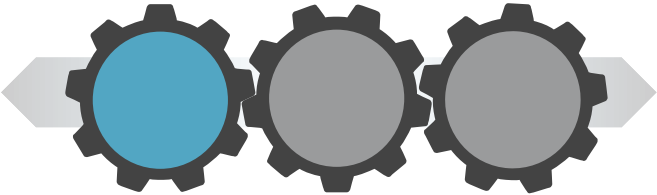
Example:
"unsuspecting_user@CyberRange"

```
DIRECT/ds.download.windowsupdate.com application/octet-stream
```

Hierarchy / From

MIME Type

Looking Closer – Web Security



```
"Windows-Update-Agent" - 144.135.8.162 "Software Updates" 177
```

User Agent

HTTP Referrer
Example:
"http://www.news.com.au/"

Destination IP Address

URL Category Name

Request Size (bytes)

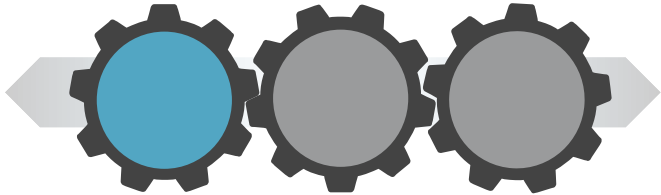
*** Custom Fields**

“The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him;

not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.”

Sun Tsu, “The Art of War”

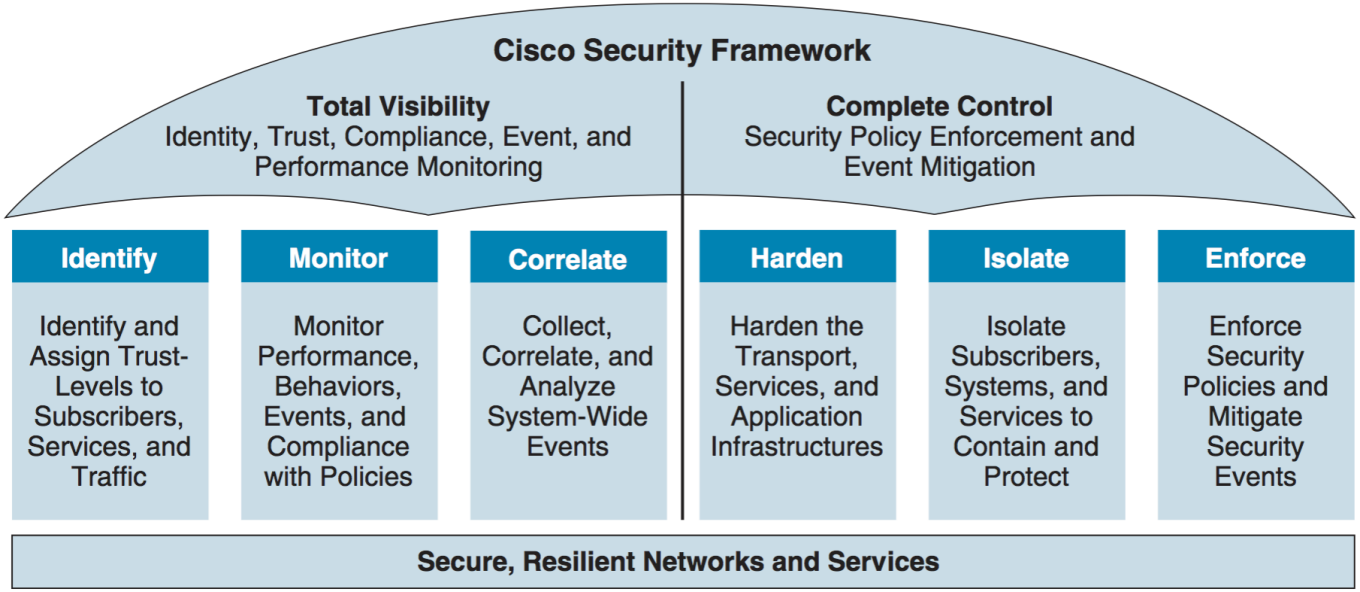
How Ready Are We?

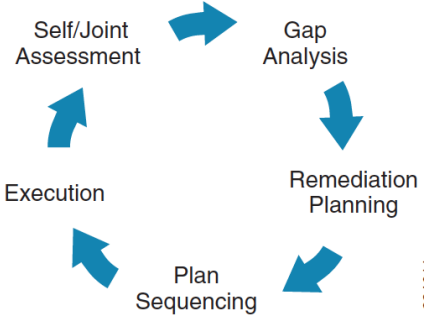


- Red Team / Ethical Hack
- Configuration Standards
- Vulnerability Management
- **Regular** Review and Remediation Program

How Ready Are We?

Configuration Standards





http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/Baseline_Security/securebasebook.html

How Ready Are We?

Configuration Standards

Reference	URL
Security Controls Framework	http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/CiscoSCF.html
Network Security Baseline	http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/Baseline_Security/securebasebook.html
IOS Hardening Guide	http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html
IOS XR Hardening Guide	http://www.cisco.com/web/about/security/intelligence/CiscoIOSXR.html
NXOS Hardening Guide	http://www.cisco.com/c/en/us/products/collateral/switches/nexus-7000-series-switches/guide_c07-665160.html

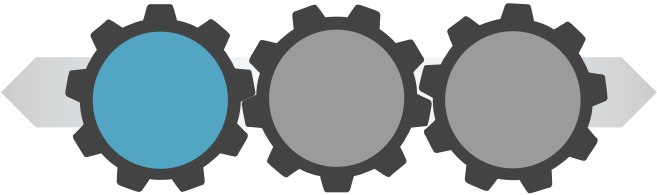
How Ready Are We?

ASD Top 35 Mapping

#	Title	Compliance	Solution
1	Application Whitelisting	Meets	Application Whitelisting with FireAmp
2	Patch Applications	Assists	ISE & NAC
3	Patch OS Vulnerabilities	Meets (I)	Cisco Prime suite
4	Restrict Administrative Privileges	Meets (I)	Cisco Secure ACS
5 (18)	User Application hardening	Assists	FireSight Host Profiles
6 (new)	Dynamic analysis of email & web content in a sandbox.	Meets	AMP Sandboxing (including with Ironport, CWS)
8 (11)	Host based IDS	Assists	AMP for Endpoints
10 (7)	Network Segmentation	Meets	VLAN, VRF, VPN, ACL, SGT/SGACL, ZBF

How Ready Are We?

Vulnerability Management and Cisco PSIRT



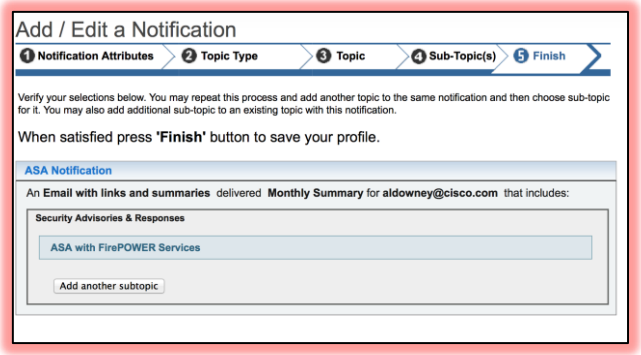
Type	Description
Security Advisories	Significant, Effecting Cisco Equipment, Requiring Action
Security Responses	Responses to 3rd party announcements
Security Notices	Medium / Low Impact

http://www.**cisco**.com/go/**psirt**

How Ready Are We?

Vulnerability Management and Cisco PSIRT

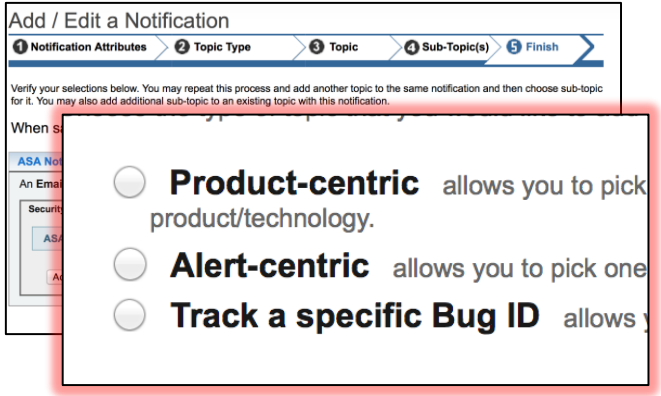
- Staying Informed
- Customisable Alerts
- Regular Review
- Make it someone's role



How Ready Are We?

Vulnerability Management and Cisco PSIRT

- Staying Informed
- Customisable Alerts
- Regular Review
- Make it someone's role



How Ready Are We?

Vulnerability Management and Cisco PSIRT

- Staying Informed
- Customisable Alerts
- Regular Review
- Make it someone's role

http://www.cisco.com/cisco/support/notifications.html#

How Ready Are We?

Vulnerability Management and Cisco PSIRT

- Reacting to an Advisory
- Assess Impact Applicability
  - Hardware Model
  - Software Version
  - Feature in use
  - Regular Updates
- Fix / Workaround as required

Affected Products

Cisco is currently investigating its product line to determine which products may be affected and the extent of the impact of the vulnerability on its products. Additional Cisco products will be added as the investigation progresses.

The following Cisco products are currently under investigation

None

Vulnerable Products

Products Confirmed Not Vulnerable

Top of the section Close Section

Details

Vulnerability Scoring Details

Impact

Software Versions and Fixes

Workarounds

Obtaining Fixed Software

Exploitation and Public Announcements

Status of This Notice: Final

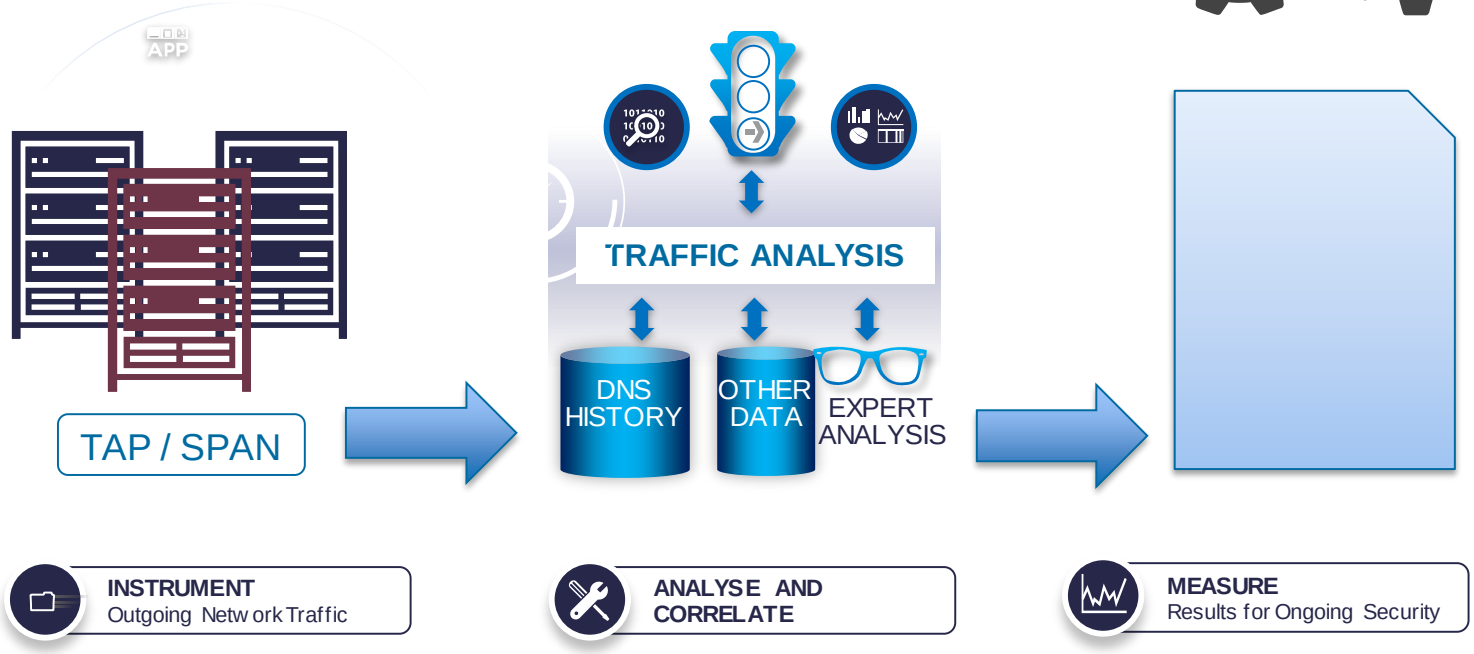
Distribution

Revision History

Cisco Security Procedures

DNS Inspection as a Measure

Custom Threat Intelligence



See also: https://www.icann.org/news/blog/monitor-dns-traffic-you-just-might-catch-a-rat

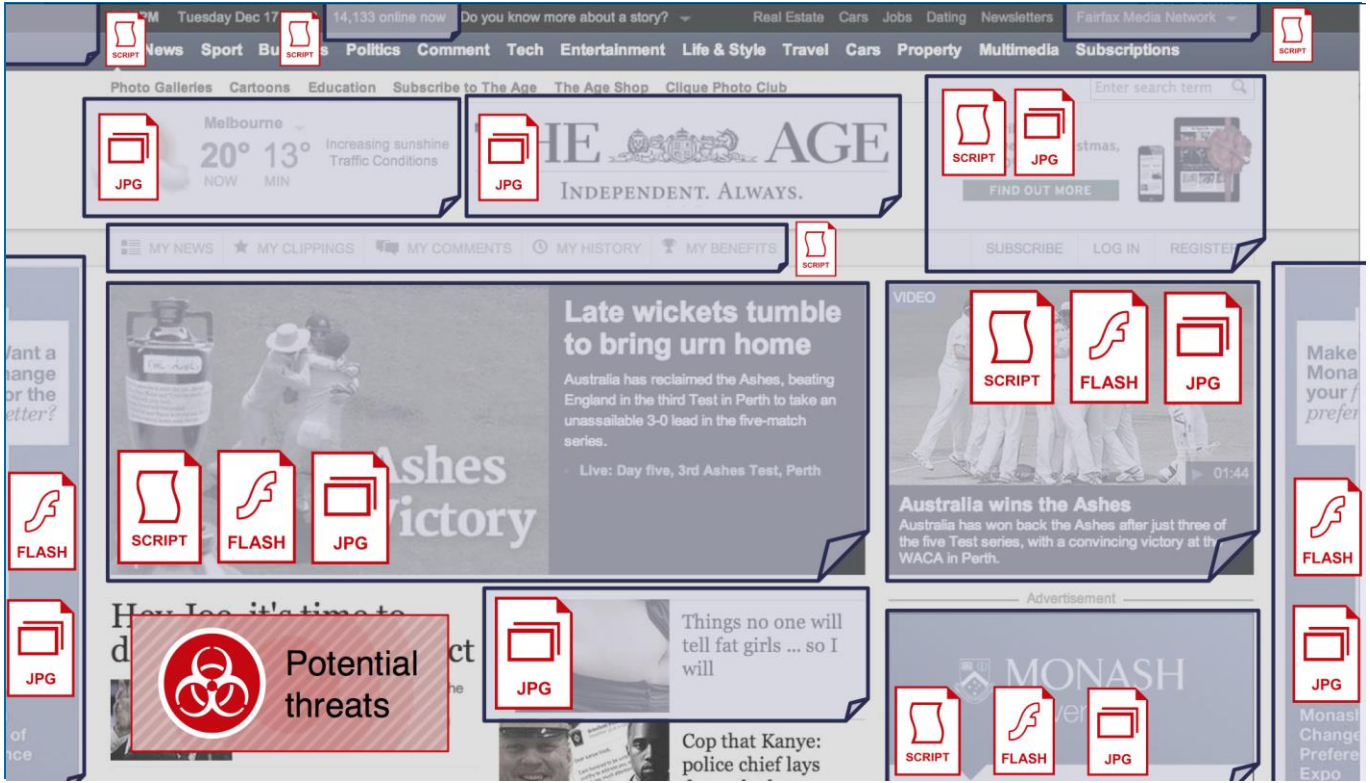
DNS Inspection as a Measure

Custom Threat Intelligence

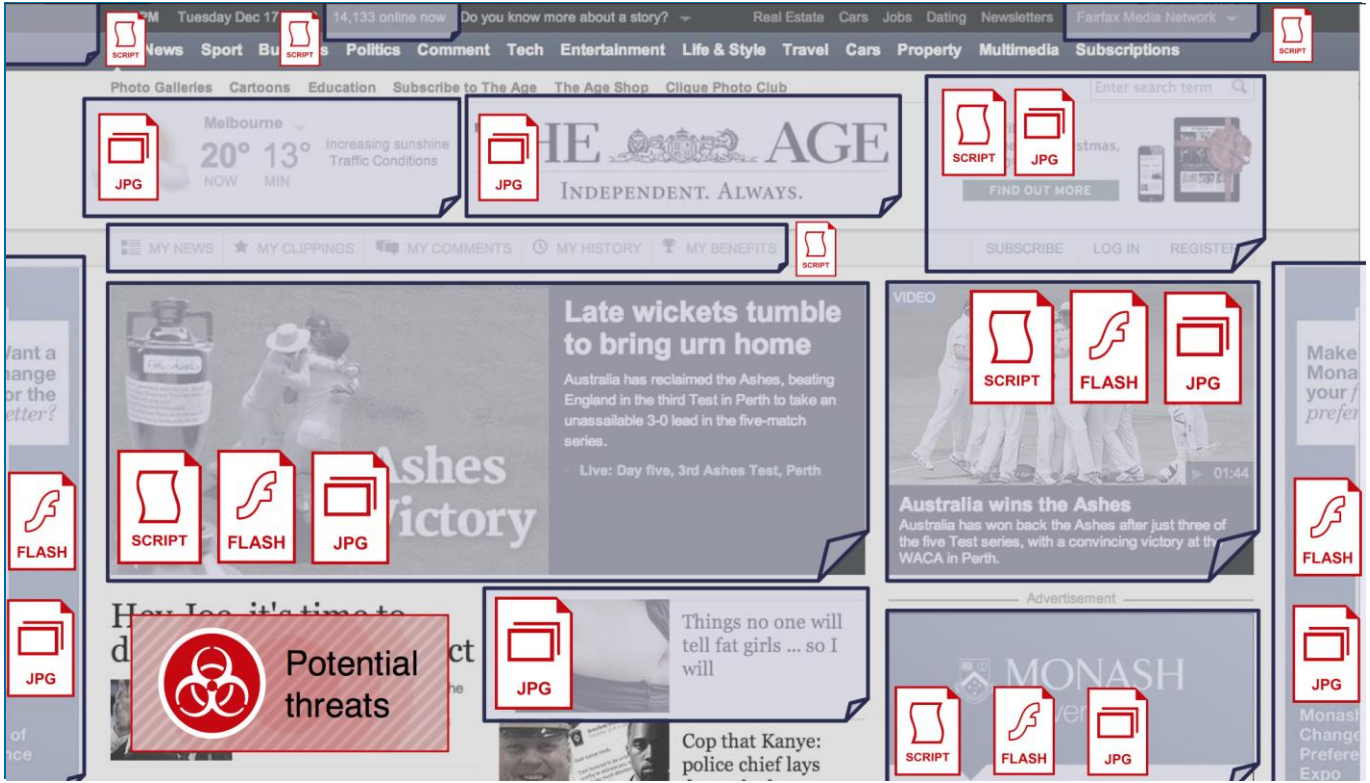
- High Threat Malware (Zeus, Palevo, SpyEye)
- Malware Distribution Sites
- Compromised Sites
- HT Parked Domains
- No Content Sites
- DNS Tunnelling
- Hate Related or other Illegal Material
- Suspect DNS Requests

Enforcing Web Security

Enforcing Web Security

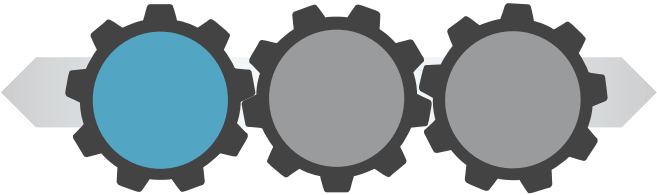


Enforcing Web Security



162 Distinct Objects
2 HTML Docs
4 Style Sheets
111 Images
14 Scripts
7 Flash/Adv Content
18 Errors
27 Unique Domains
29 Unique Hosts
107 Kbytes

Enforcing Web Security



Unknown Traffic In..

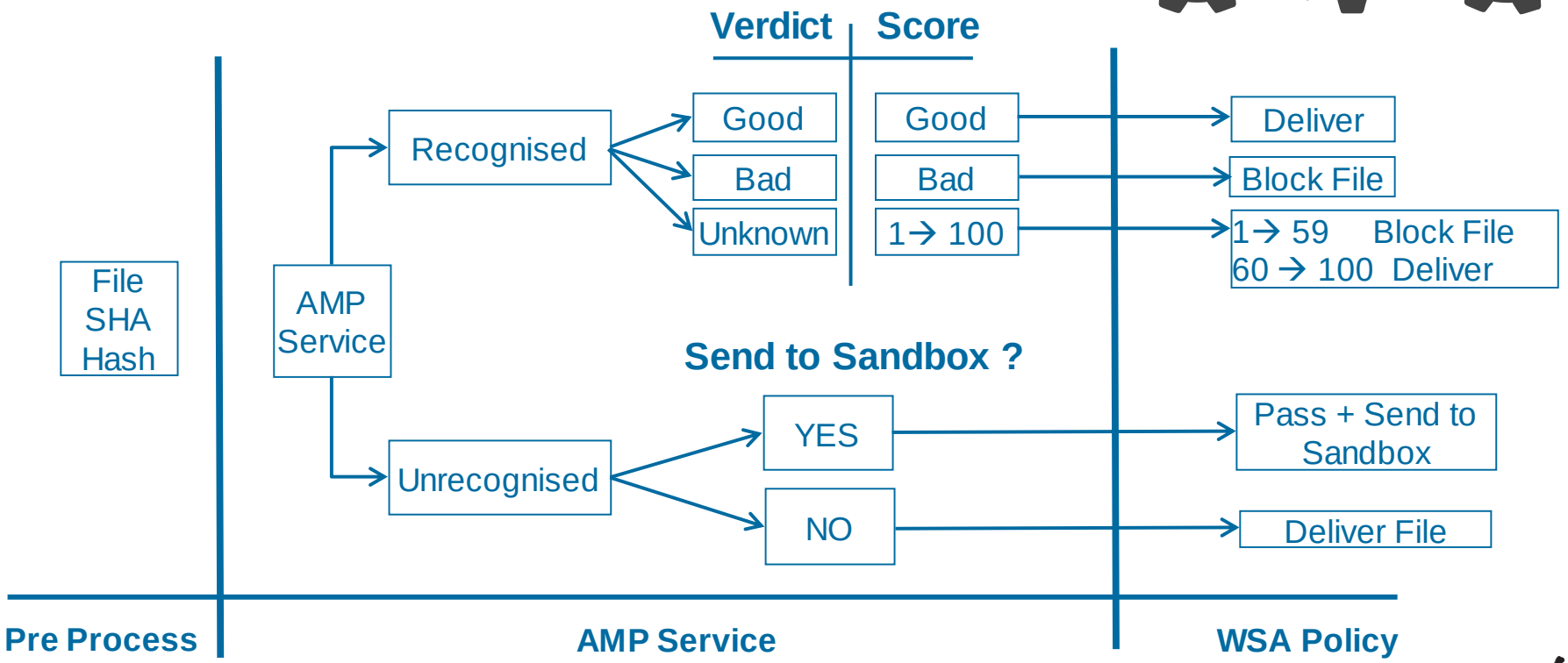
Web Security Monitoring | Usage & Threat Reporting

AsyncOS for Web™

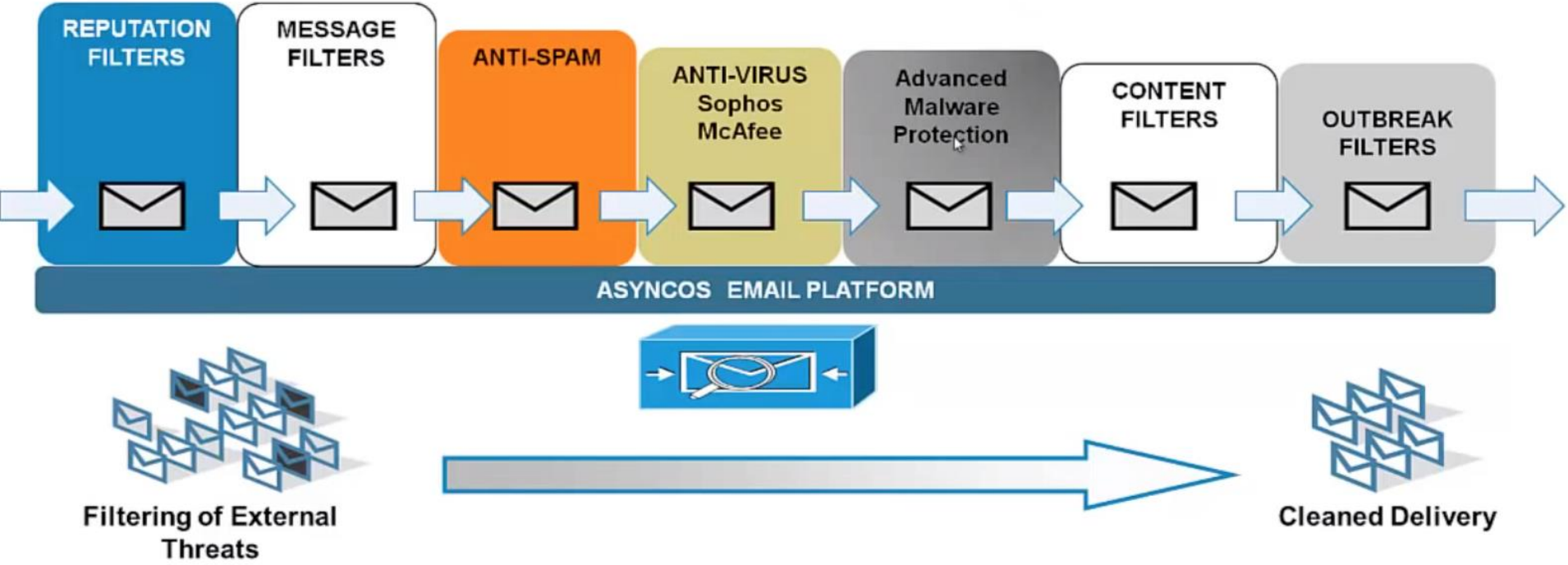
Proxy & Cache	URL Filtering	Web Reputation Filters	HTTPs Decryption & Scanning	Anti-Malware Scanning (Spyware/Adware)	Web Anti-Virus Scanning	Layer 4 Traffic Monitor	Data Security And External DLP
Comprehensive web security appliance with integrated Proxy & Cache	Category based URL filter with time based policies	Simplifies protection of your users, by using an external reputation score.	Enforce acceptable use and security policies over HTTPs-decrypted data	Incredibly fast malware filter, checks all inbound data.	Inline on-box AV scanning for maximum throughput and minimal latency	Uniquely detects Malware phone home traffic on all 65535 ports at wire speed	Policy based deep content visibility and control.

Clean Traffic Out..

Web Security with AMP



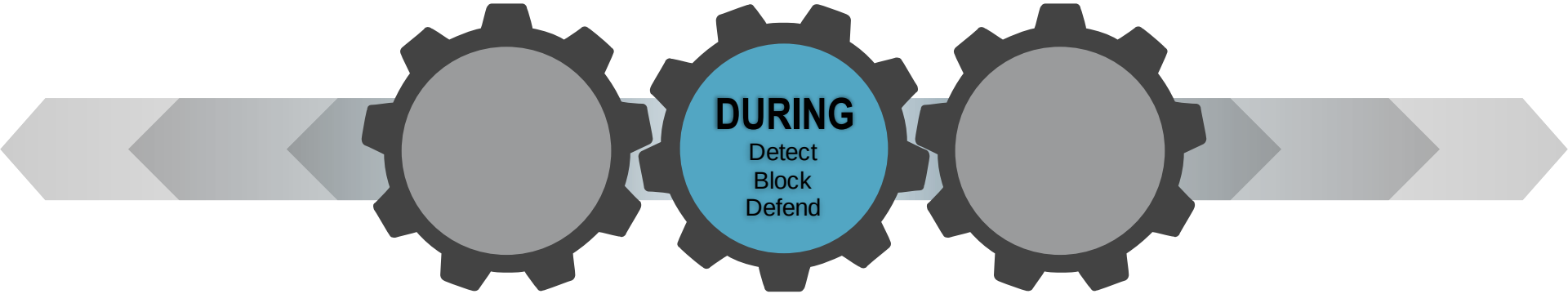
Enforcing Email Security



Email Security and AMP

AMP uses cloud-based services to protect against zero-day and targeted file-based threats in email attachments by:

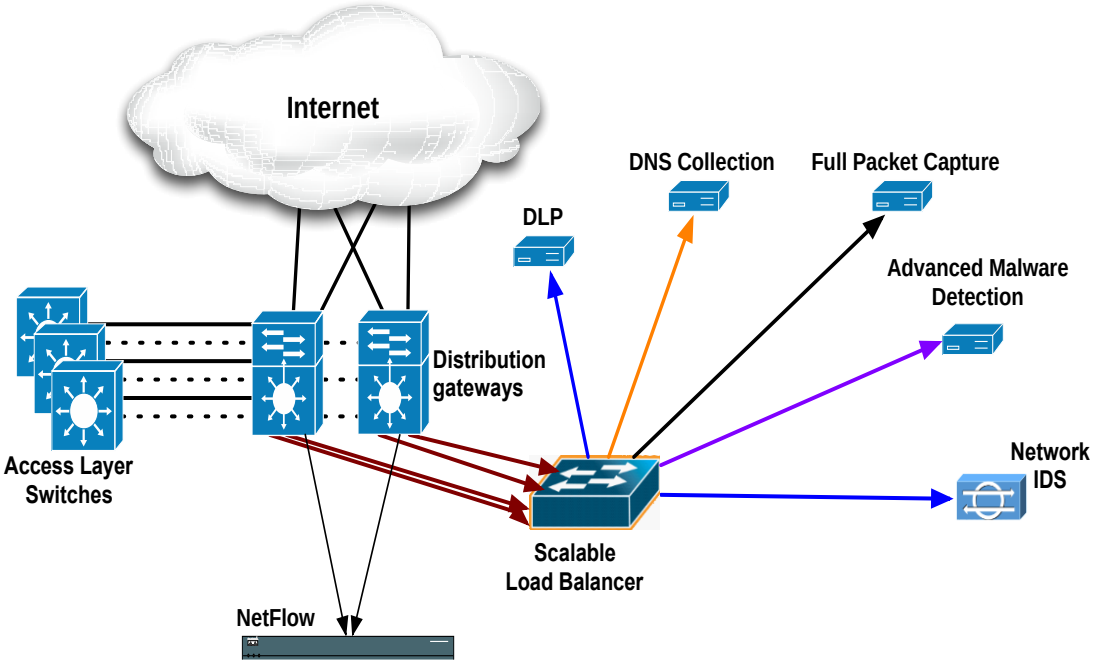
- Obtaining each file's reputation
- Analysing the behaviour of files with unknown reputations
- Notifying you about files determined to be threats after they have entered the network.



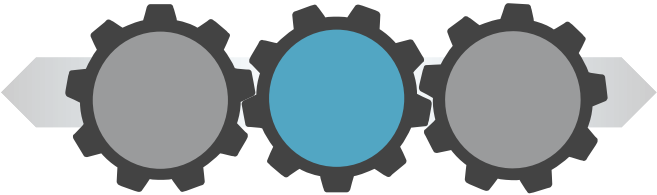
Can’t See The Wood For The Trees?

Bringing it all together

- 22 TB of Traffic Inspected
- 6 million HTTP transactions
- 750 GB of logs
- 4 billion DNS Records
- 1% Blocked as Malware
- 13 Billion Netflow records
- 400+ Application Providers
- 12 Critical Data Centres



Event Analysis Playbook



- Defines:
  - **Objective**: Tell me if you see this happening…
  - **Query**: Query string used for detection
  - **Result Analysis:** Explanation of Logic/Approach
  - **ID, Notes:** Reference and Refinement Comments
- Benefit:
  - Best Blend Human Skill & Automation
  - Process Efficiency
  - Knowledge Sharing
  - Continuous Refinement

Event Analysis Playbook

Firewall blocks suspicious probe on outside

```
Aug 02 2014 23:14:06: %ASA-5-106100: access-list inbound
denied tcp outside/173.246.103.92(1922)
inside/192.168.10.18(135) hit-cnt 1 first hit [0x91c26a3,
0x0]
```

action	dropped
cause	Firewall Drop
direction	inbound
src_ip	**173.246.103.92**

Event Analysis Playbook

Firewall blocks suspicious probe on outside

```
Aug 02 2014 23:14:06: %ASA-5-106100: access-list inbound
denied tcp outside/173.246.103.92(1922)
inside/192.168.10.18(135) hit-cnt 1 first hit [0x91c26a3,
0x0]
```

action	dropped
cause	Firewall Drop
direction	inbound
src_ip	**173.246.103.92**

```
1409754862.736 33628 192.168.10.18 TCP_MISS/200 4333
TCP_CONNECT 173.246.103.92:8443 …
173.246.103.92 "Computer Security" 1028
```

action	allowed (HTTP/200)
cause	Acceptable Use
direction	outbound
dest_ip	**173.246.103.92**

Proxy sees connection attempt to same IP

Event Analysis Playbook

Firewall blocks suspicious probe on outside

```
Aug 02 2014 23:14:06: %ASA-5-106100: access-list inbound
denied tcp outside/173.246.103.92(1922)
inside/192.168.10.18(135) hit-cnt 1 first hit [0x91c26a3,
0x0]
```

action	dropped
cause	Firewall Drop
direction	inbound
src_ip	**173.246.103.92**

src_ip OR dest_ip	**173.246.103.92**

action	allowed (HTTP/200)
cause	Acceptable Use
direction	outbound
dest_ip	**173.246.103.92**

```
1409754862.736 33628 192.168.10.18 TCP_MISS/200 4333
TCP_CONNECT 173.246.103.92:8443 …
173.246.103.92 "Computer Security" 1028
```

Proxy sees connection attempt to same IP

Event Analysis Playbook

Firewall blocks suspicious probe on outside

```
Aug 02 2014 23:14:06: %ASA-5-106100: access-list inbound
denied tcp outside/173.246.103.92(1922)
inside/192.168.10.18(135) hit-cnt 1 first hit [0x91c26a3,
0x0]
```

action	dropped
cause	Firewall Drop
direction	inbound
src_ip	**173.246.103.92**

```
query_id="SPL-MW-003-05"
query_description="Inbound Scan w/ Outbound Access"
incident_id="1115258_0800_20-Aug-14"
attacker_ip="173.246.103.92" severity="med"
sourcetype="cisco:wsa,cisco:asa" _time="20 Aug 2014"
raw_event="<Firewall Event> … <Web Sec Event> …"
```

src_ip OR dest_ip	**173.246.103.92**

```
1409754862.736 33628 192.168.10.18 TCP_MISS/200 4333
TCP_CONNECT 173.246.103.92:8443 …
173.246.103.92 "Computer Security" 1028
```

action	allowed (HTTP/200)
cause	Acceptable Use
direction	outbound
dest_ip	**173.246.103.92**

Proxy sees connection attempt to same IP

Event Analysis Playbook

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.

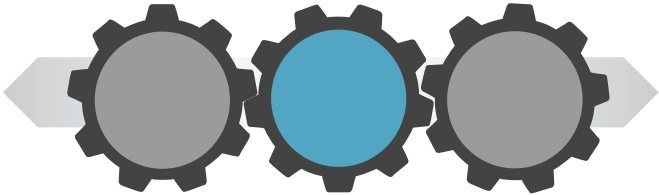
Working:

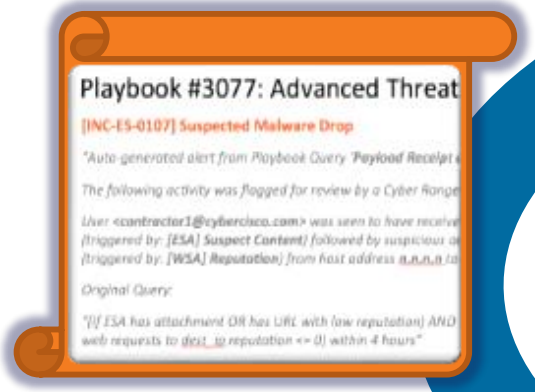
```
index="wsa" AND x_wbrs_score <= -8.0 AND TCP_DENIED AND NOT (tag=acns) AND
earliest=-24h | stats count by c_ip | sort -count limit=10 | rename c_ip as
"Source IP", count as "# of TCP_DENIED to WBRS < -8.0"
```

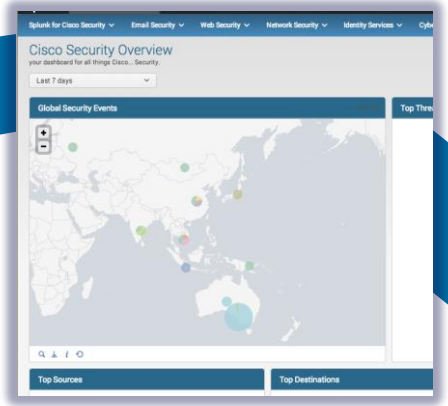
An email will be sent to csirt-xxxxxxx@cisco.com

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.

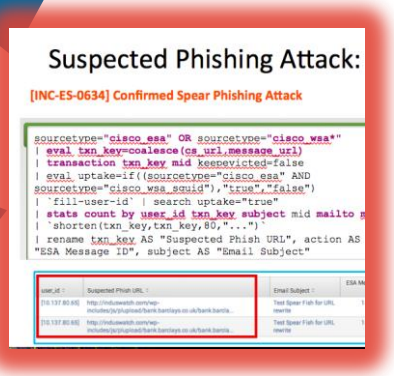
Event Analysis Playbook







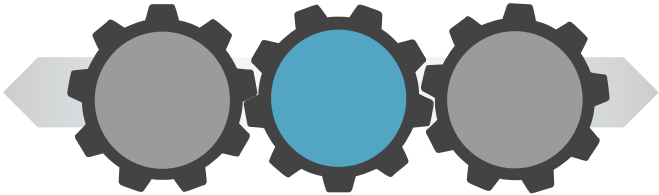
Study the data

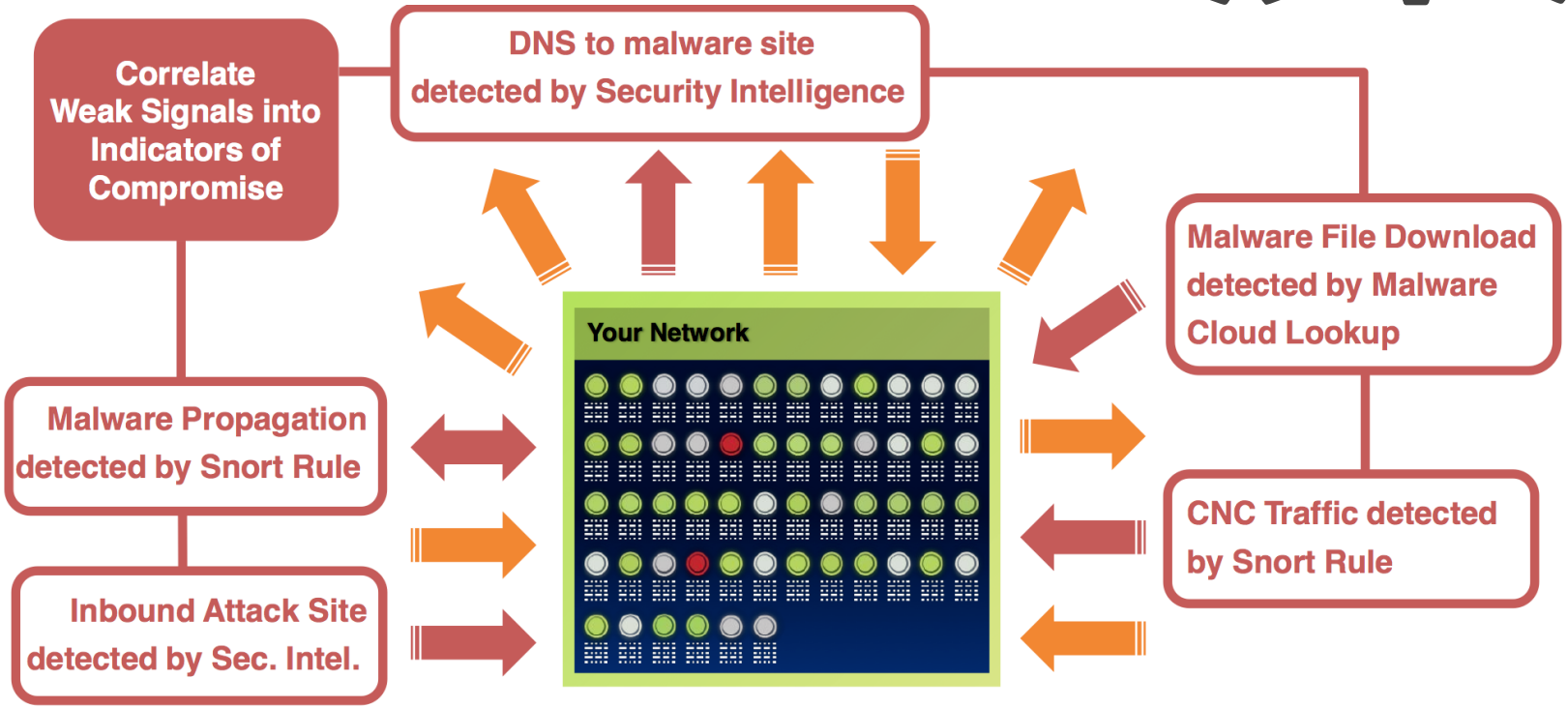


Trial by fire

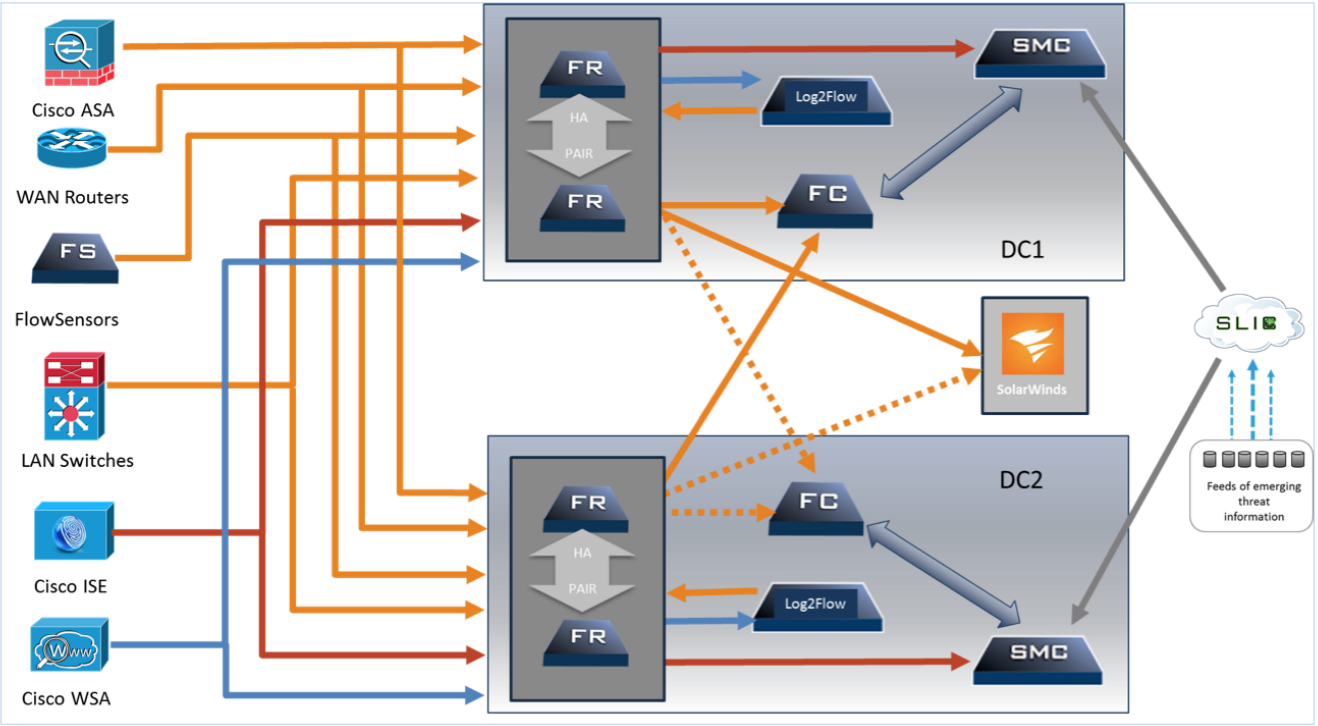
Build your arsenal

Correlating Weak Signals into IOCs





Flow Based Anomaly Detection



Flow Based Anomaly Detection

Telemetry from the ISE

Host : 10.10.200.59

Identification | Alarms | Security | CI Events | Top Active Flows | **Identity, DHCP & Host Notes** | Exporter Interfaces

Identity and Device Table - 1 record

Start Active Time	End Active Time	User Name	MAC Address	Device Type	Domain Name	Network ...	Netwo...	Securi...
Jun 10, 2013 11:27:37 PM (8 days 20 hours 26 minutes ago)	Current	bmcmahon	00:d0:b8:0d:fd:27 (Iomega Corporation)	Windows7-Workstation	LC	Unknown Exporter (10.10.1.1)	GigabitEthernet5/37	

Username

Infected machine

Combining Flow and Identity

Monitor Mode

- Open Mode, Multi-Auth
- Unobstructed Access
- No impact on productivity
- Profiling, posture assessment
- Gain Visibility

syslog

Cisco ISE

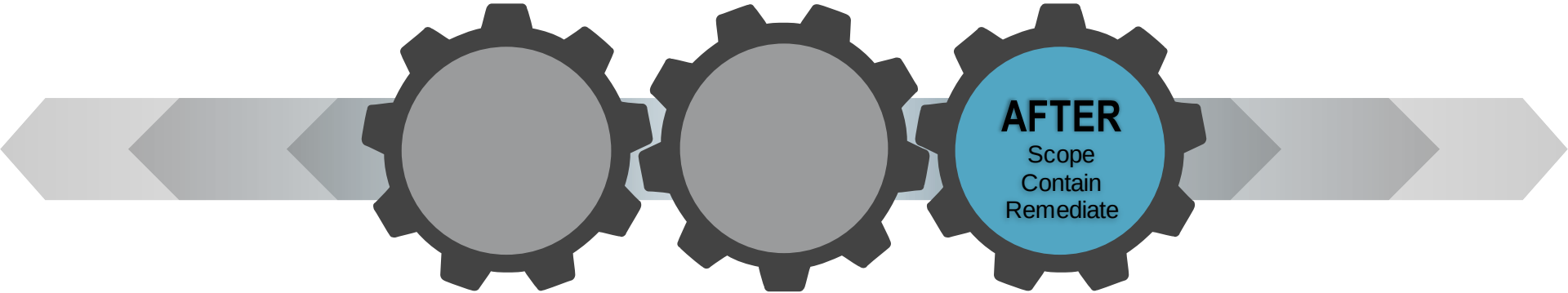
StealthWatch Management Console

- Maintain historical session table
- Correlate NetFlow to username
- Build User-centric reports

Start Active Time	End Active Ti...	User Name	Host	Device Type	MAC Address
Apr 15, 2013 2:08:33 PM (17 minutes 18s ago)	Current	student01	192.168.103.101	VMWare-Device	00:50:56:85:5c:3d (VMware, Inc.)
Apr 15, 2013 2:08:21 PM (17 minutes 18s ago)	Current	DEMO\student04	192.168.104.100	WindowsXP-Workstation	00:50:56:85:13:c4 (VMware, Inc.)
Apr 15, 2013 2:08:21 PM (17 minutes 18s ago)	Current	host/pod08-mgmt.demo.local	192.168.108.100	WindowsXP-Workstation	00:50:56:85:13:cc (VMware, Inc.)
Apr 15, 2013 2:08:21 PM (17 minutes 18s ago)	Current	host/pod09-mgmt.demo.local	192.168.109.100	WindowsXP-Workstation	00:50:56:85:13:ce (VMware, Inc.)
Apr 15, 2013 2:08:21 PM (17 minutes 18s ago)	Current	DEMO\student05	192.168.105.100	WindowsXP-Workstation	00:50:56:85:13:c6 (VMware, Inc.)

Time	Status	Details	Identity	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles
Apr 15,13 02:08:33.241 PM	✓		student01	00:50:56:85:5C:3D	192.168.103.1...	sw1	GigabitEthernet0/4	PermitAccess
Apr 15,13 02:08:21.241 PM	✓		DEMO\student04	00:50:56:85:13:C4	192.168.104.1...	sw1	GigabitEthernet0/5	PermitAccess
Apr 15,13 02:08:21.219 PM	✓		host/pod08-mgmt.demo.local	00:50:56:85:13:CC	192.168.108.1...	sw1	GigabitEthernet0/9	PermitAccess
Apr 15,13 02:08:21.192 PM	✓		host/pod09-mgmt.demo.local	00:50:56:85:13:CE	192.168.109.1...	sw1	GigabitEthernet0/10	PermitAccess
Apr 15,13 02:08:21.144 PM	✓		DEMO\student05	00:50:56:85:13:C6	192.168.105.1...	sw1	GigabitEthernet0/6	PermitAccess
Apr 15,13 02:08:21.082 PM	✓		DEMO\stu[illegible]	00:50:56:85:13:CA	192.168.107.1...	sw1	GigabitEthernet0/8	PermitAccess

Authenticated Session Table



Tracking File Trajectory using AMP

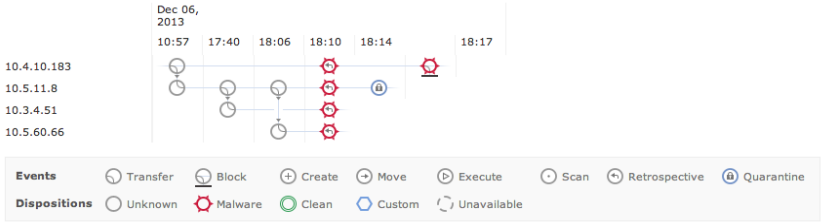
Overview | Analysis | Policies | Devices | Objects | FireAMP | Health | System | Help | admin

Context Explorer | Connections | Intrusions | Files ▸ Network File Trajectory | Hosts | Users | Vulnerabilities | Correlation | Custom | Search

Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374	**First Seen**	2013-12-06 10:57:13 on 10.4.10.183
File Name	WindowsMediaInstaller.exe	**Last Seen**	2013-12-06 18:17:27 on 10.4.10.183
File Type	MSEXE	**Event Count**	7
File Category	Executables	**Seen On**	4 hosts
Current Disposition	Malware	**Seen On Breakdown**	2 senders → 3 receivers
Threat Score	High		

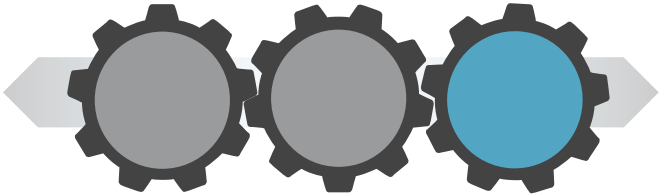
Trajectory



Events

Time	Event Type	Sending IP	Receiving IP	File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

Tracking File Trajectory using AMP



Overview | Analysis | Policies | Devices | Objects | FireAMP | Health | System | Help | admin

Context Explorer | Connections | Intrusions | Files ▸ Network File Trajectory | Hosts | Users | Vulnerabilities | Correlation | Custom | Search

Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374	First Seen	2013-12-06 10:57:13 on 10.4.10.183
File Name	WindowsMediaInstaller.exe	Last Seen	2013-12-06 18:17:27 on 10.4.10.183
File Type	MSEXE	Event Count	7
File Category	Executables	Seen On	4 hosts
Current Disposition	Malware	Seen On Breakdown	2 senders → 3 receivers
Threat Score	High		

Trajectory

Dec 06, 2013

10:57 | 17:40 | 18:06 | 18:10 | 18:14 | 18:17

10.4.10.183
10.5.11.8
10.3.4.51
10.5.60.66

Events: Transfer | Block | Create | Move | Execute | Scan | Retrospective | Quarantine

Dispositions: Unknown | Malware | Clean | Custom | Unavailable

Events

Time	Event	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retros						
2013-12-06 17:40:28	Transf						Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transf						Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transf						Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retros						
2013-12-06 18:14:23	File Qu						
2013-12-06 18:17:27	Transf						

Time	2013-12-06 17:40:28
Event Type	File Sent
IP Address	10.4.10.183
Sent To	10.5.11.8
File Name	WindowsMediaInstaller.exe
Disposition	Unknown
Action	Malware Cloud Lookup
Application Protocol	HTTP
Client	Firefox

An unknown file is present on IP: 10.4.10.183, having been downloaded with Firefox

Tracking File Trajectory using AMP

Overview | Analysis | Policies | Devices | Objects | FireAMP | Health | System | Help | admin

Context Explorer | Connections | Intrusions | Files ▸ Network File Trajectory | Hosts | Users | Vulnerabilities | Correlation | Custom | Search

Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374	First Seen	2013-12-06 10:57:13 on 10.4.10.183
File Name	WindowsMediaInstaller.exe	Last Seen	2013-12-06 18:17:27 on 10.4.10.183
File Type	MSEXE	Event Count	7
File Category	Executables	Seen On	4 hosts
Current Disposition	Malware	Seen On Breakdown	2 senders → 3 receivers
Threat Score	High		

Trajectory

Dec 06, 2013

10:57 | 17:40 | 18:06 | 18:10 | 18:14 | 18:17

10.4.10.183
10.5.11.8
10.3.4.51
10.5.60.66

Events: Transfer | Block | Create | Move | Execute | Scan | Retrospective | Quarantine

Dispositions: Unknown | Malware | Clean | Custom | Unavailable

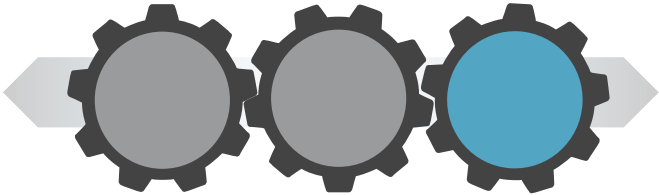
Events

Time	Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13		Malwa...					
2013-12-06 17:40:28	...dowsMediaIn						...ospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	...dowsMediaIn						...ospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	...dowsMediaIn						...ospective Event, Fri Dec 6 ...
2013-12-06 18:14:10							
2013-12-06 18:14:23	...dowsMediaIn						
2013-12-06 18:17:27	...dowsMediaIn						

Time	2013-12-06 17:40:28
Event Type	File Received
IP Address	10.5.11.8
Received From	10.4.10.183
File Name	WindowsMediaInstaller.exe
Disposition	Unknown
Action	Malware Cloud Lookup
Application Protocol	HTTP
Client	Firefox

At 10:57, the unknown file is transferred from IP 10.4.10.183 to IP: 10.5.11.8

Tracking File Trajectory using AMP



Overview | Analysis | Policies | Devices | Objects | FireAMP | Health | System | Help | admin

Context Explorer | Connections | Intrusions | Files ▸ Network File Trajectory | Hosts | Users | Vulnerabilities | Correlation | Custom | Search

Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374	First Seen	2013-12-06 10:57:13 on 10.4.10.183
File Name	WindowsMediaInstaller.exe	Last Seen	2013-12-06 18:17:27 on 10.4.10.183
File Type	MSEXE	Event Count	7
File Category	Executables	Seen On	4 hosts
Current Disposition	Malware	Seen On Breakdown	2 senders → 3 receivers
Threat Score	High		

Trajectory

Dec 06, 2013

10:57 | 17:40 | 18:06 | 18:10 | 18:14 | 18:17

10.4.10.183
10.5.11.8
10.3.4.51
10.5.60.66

Events: Transfer, Block, Create, Move, Execute, Scan, Retrospective, Quarantine

Dispositions: Unknown, Malware, Clean, Custom, Unavailable

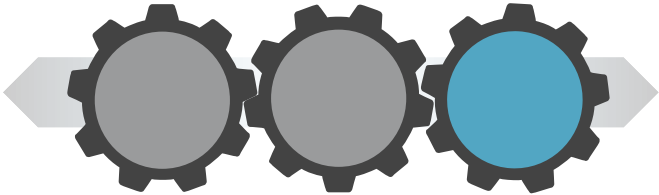
Events

Time	Event Type	Dis...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...	Mal...					
2013-12-06 17:40:28	Transfer	Unk...	Ma...				...
2013-12-06 18:06:03	Transfer	Unk...					...
2013-12-06 18:10:03	Transfer	Unk...					...
2013-12-06 18:14:10	Retrospectiv...	Mal...					
2013-12-06 18:14:23	File Quaranti...	Mal...					
2013-12-06 18:17:27	Transfer	Mal...	Ma...				

Time	2013-12-06 18:06:03
Event Type	File Received
IP Address	10.3.4.51
Received From	10.5.11.8
File Name	WindowsMediaInstaller.exe
Disposition	Unknown
Action	
Application Protocol	NetBIOS-ssn (SMB)

Seven hours later the file is then transferred to a third device (10.3.4.51) using an SMB application

Tracking File Trajectory using AMP



Overview | Analysis | Policies | Devices | Objects | FireAMP | Health | System | Help | admin

Context Explorer | Connections | Intrusions | Files ▸ Network File Trajectory | Hosts | Users | Vulnerabilities | Correlation | Custom | Search

Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374	First Seen	2013-12-06 10:57:13 on 10.4.10.183
File Name	WindowsMediaInstaller.exe	Last Seen	2013-12-06 18:17:27 on 10.4.10.183
File Type	MSEXE	Event Count	7
File Category	Executables	Seen On	4 hosts
Current Disposition	Malware	Seen On Breakdown	2 senders → 3 receivers
Threat Score	High		

Trajectory

Dec 06, 2013

10:57 | 17:40 | 18:06 | 18:10 | 18:14 | 18:17

10.4.10.183
10.5.11.8
10.3.4.51
10.5.60.66

Events: Transfer, Block, Creat, Move, Execute, Scan, Retrospective, Quarantine

Dispositions: Unknown, Malware, Clear, Custom, Unavailable

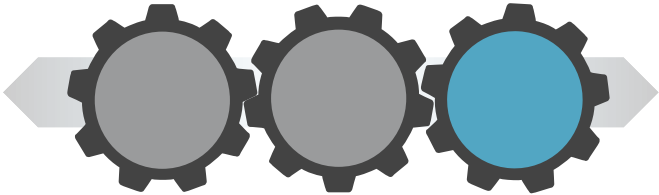
Events

Time	Event Type	Sending	ction
2013-12-06 10:57:13	Retrospectiv...		
2013-12-06 17:40:28	Transfer	10.4.10.1	alware Cloud L
2013-12-06 18:06:03	Transfer	10.5.11.8	
2013-12-06 18:10:03	Transfer	10.5.11.8	
2013-12-06 18:14:10	Retrospectiv...		
2013-12-06 18:14:23	File Quaranti...		
2013-12-06 18:17:27	Transfer	10.4.10.1	alware Block

Time	2013-12-06 18:10:03
Event Type	File Received
IP Address	10.5.60.66
Received From	10.5.11.8
File Name	WindowsMediaInstaller.exe
Disposition	Unknown
Action	
Application Protocol	NetBIOS-ssn (SMB)

The file is copied yet again onto a fourth device (10.5.60.66) through the same SMB application a half hour later

Tracking File Trajectory using AMP



Overview | Analysis | Policies | Devices | Objects | FireAMP | Health | System | Help | admin

Context Explorer | Connections | Intrusions | Files ▸ Network File Trajectory | Hosts | Users | Vulnerabilities | Correlation | Custom | Search

Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374	First Seen	2013-12-06 10:57:13 on 10.4.10.183
File Name	WindowsMediaInstaller.exe	Last Seen	2013-12-06 18:17:27 on 10.4.10.183
File Type	MSEXE	Event Count	7
File Category	Executables	Seen On	4 hosts
Current Disposition	Malware	Seen On Breakdown	2 senders → 3 receivers
Threat Score	High		

Trajectory

Dec 06, 2013

10:57 | 17:40 | 18:06 | 18:10 | 18:14 | 18:17

10.4.10.183
10.5.11.8
10.3.4.51
10.5.60.66

Events: Transfer, Block, Create, Execute, Scan, Retrospective, Quarantine

Dispositions: Unknown, Malware, Clean, Unavailable

Events

Time	Event Type	Sending IP
2013-12-06 10:57:13	Retrospectiv...	
2013-12-06 17:40:28	Transfer	10.4.10.183
2013-12-06 18:06:03	Transfer	10.5.11.8
2013-12-06 18:10:03	Transfer	10.5.11.8
2013-12-06 18:14:10	Retrospectiv...	
2013-12-06 18:14:23	File Quaranti...	
2013-12-06 18:17:27	Transfer	10.4.10.183

Time 2013-12-06 18:14:10
Event Type Retrospective Event
Disposition Malware
Action

The Cisco Collective Security Intelligence Cloud has learned this file is malicious and a retrospective event is raised for all four devices immediately.

Tracking File Trajectory using AMP

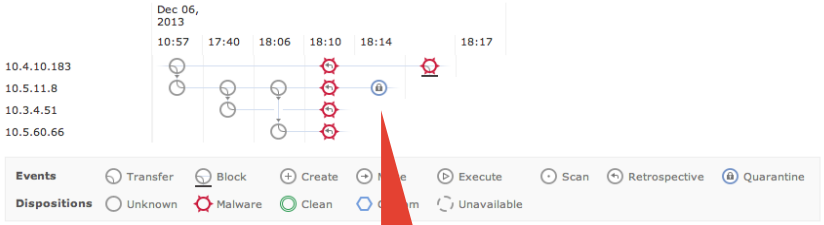
Overview | Analysis | Policies | Devices | Objects | FireAMP | Health | System | Help | admin

Context Explorer | Connections | Intrusions | Files ▸ Network File Trajectory | Hosts | Users | Vulnerabilities | Correlation | Custom | Search

Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374	First Seen	2013-12-06 10:57:13 on 10.4.10.183
File Name	WindowsMediaInstaller.exe	Last Seen	2013-12-06 18:17:27 on 10.4.10.183
File Type	MSEXE	Event Count	7
File Category	Executables	Seen On	4 hosts
Current Disposition	Malware	Seen On Breakdown	2 senders → 3 receivers
Threat Score	High		

Trajectory



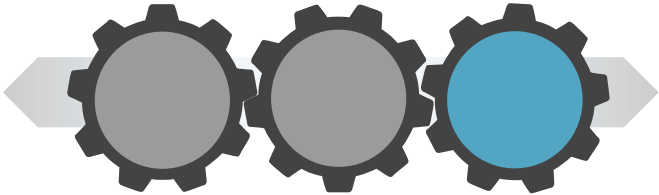
Events

Time	Event Type	Sending IP
2013-12-06 10:57:13	Retrospectiv...	
2013-12-06 17:40:28	Transfer	10.4.10.183
2013-12-06 18:06:03	Transfer	10.5.11.8
2013-12-06 18:10:03	Transfer	10.5.11.8
2013-12-06 18:14:10	Retrospectiv...	
2013-12-06 18:14:23	File Quaranti...	
2013-12-06 18:17:27	Transfer	10.4.10.183

Time	2013-12-06 18:14:23
Event Type	File Quarantined
IP Address	10.5.11.8
File Name	WindowsMediaInstaller.exe
Disposition	Malware
Action	

At the same time, a device with the FireAMP endpoint connector reacts to the retrospective event and immediately stops and quarantines the newly detected malware

Tracking File Trajectory using AMP



Overview | Analysis | Policies | Devices | Objects | FireAMP | Health | System | Help | admin

Context Explorer | Connections | Intrusions | Files ▸ Network File Trajectory | Hosts | Users | Vulnerabilities | Correlation | Custom | Search

Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374	First Seen	2013-12-06 10:57:13 on 10.4.10.183
File Name	WindowsMediaInstaller.exe	Last Seen	2013-12-06 18:17:27 on 10.4.10.183
File Type	MSEXE	Event Count	7
File Category	Executables	Seen On	4 hosts
Current Disposition	Malware	Seen On Breakdown	2 senders → 3 receivers
Threat Score	High		

Trajectory

Dec 06, 2013

10:57 | 17:40 | 18:06 | 18:10 | 18:14 | 18:17

10.4.10.183
10.5.11.8
10.3.4.51
10.5.60.66

Events: Transfer, Block, Create, Move, Execute, Scan, Retrospective, Quarantine

Dispositions: Unknown, Malware, Clean, Custom, Unavailable

Events

Time	Event Type	Sending IP
2013-12-06 10:57:13	Retrospectiv...	
2013-12-06 17:40:28	Transfer	10.4.10.183
2013-12-06 18:06:03	Transfer	10.5.11.8
2013-12-06 18:10:03	Transfer	10.5.11.8
2013-12-06 18:14:10	Retrospectiv...	
2013-12-06 18:14:23	File Quaranti...	
2013-12-06 18:17:27	Transfer	10.4.10.183

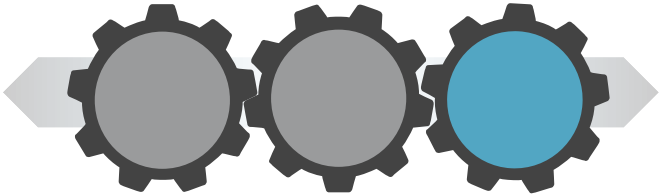
Time	2013-12-06 18:17:27
Event Type	File Sent
IP Address	10.4.10.183
Blocked Recipient	10.5.11.8
File Name	WindowsMediaInstaller.exe
Disposition	Malware
Action	Malware Block
Application Protocol	HTTP
Client	Firefox

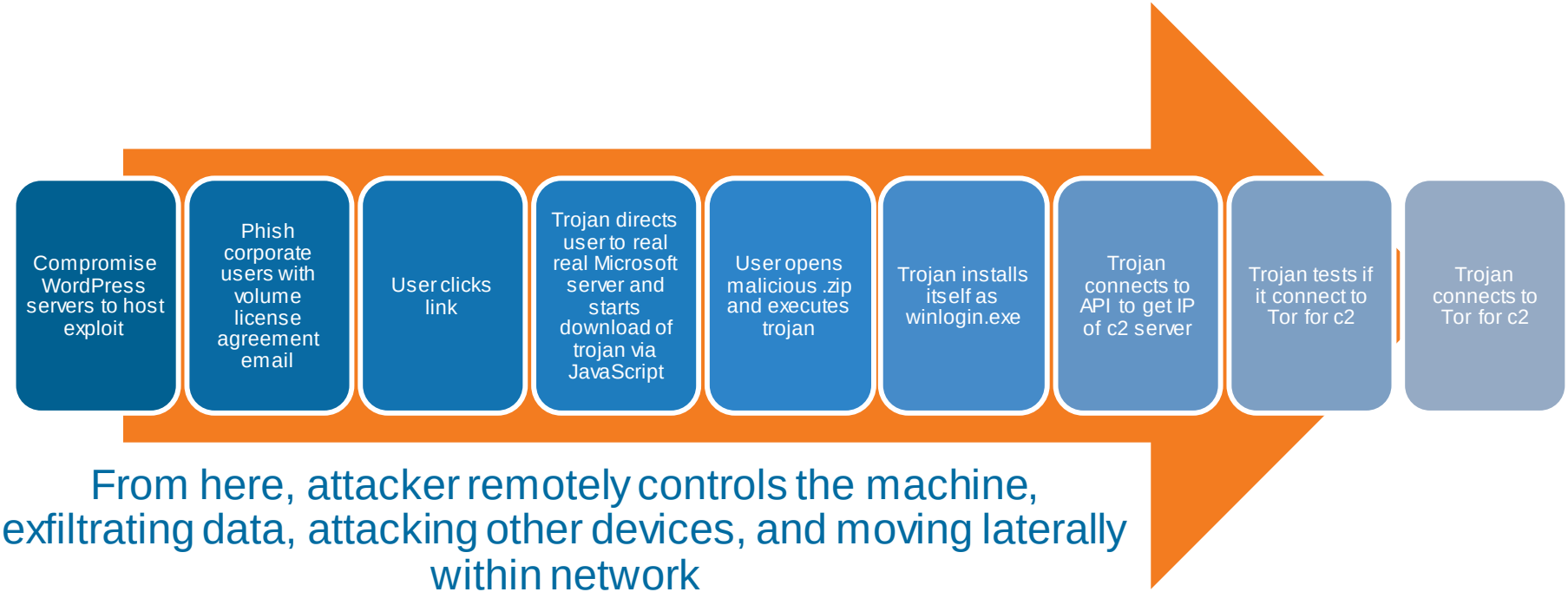
8 hours after the first attack, the Malware tries to re-enter the system through the original point of entry but is recognised and blocked.

Case Study - MTD

Investigation Case Study

Trojaned WordPress servers + “Chanitor” malware





From here, attacker remotely controls the machine, exfiltrating data, attacking other devices, and moving laterally within network

Investigation Case Study

1. Attacker Sent User Phishing Email

"Congratulations…to begin registration please download…"

Real user's email address in both To: field and URL, to look more legitimate

-------- Original Message --------
Subject: Welcome to the Microsoft Volume Licensing Service Center (VLSC)91643303:3
From: Microsoft Volume <notice_message@microsoft.com>
Date: Thu, January 15, 2015 10:13 am
To: [redacted]

Welcome [redacted]!

Congratulations on your newly accepted Open License with Microsoft, ending in 92044. You have been assigned Administrator permissions on the Microsoft Volume Licensing Service Center (VLSC) site.

To begin registration, please download details from link below. When prompted, enter your business e-mail as shown below:

VLSC Registration details:
https://www.microsoft.com/licensing/servicecenter/registration.aspx?e=[redacted]

Required Business E-mail:[redacted]
Type of new Licensing ID: OPEN

Once VLSC registration is complete, you will be able to:

- Download licensed software
- Retrieve keys for Volume Licensing software
- View Microsoft licensing details for your organization
- Manage Software Assurance benefits
- Manage subscriptions, including MSDN and/or TechNet
- Assign others in your organization to do any of the above tasksâ€"or to also be an Administrator.
- Also, within selected regions, VLSC enables the direct purchase of media kits from the Software Download Catalog.

Once you are registered, you may add any individual to your VLSC account to help manage your licenses or perform other tasks at any time. To do so, please visit the My Permissions link to view all details related to your VLSC permissions settings. Also visit Frequently Asked Questions in the Help section to learn more about what you can do in the Volume Licensing Service Center. Your new access permissions to VLSC may take up to 2 hours to become effective.

Thank you,

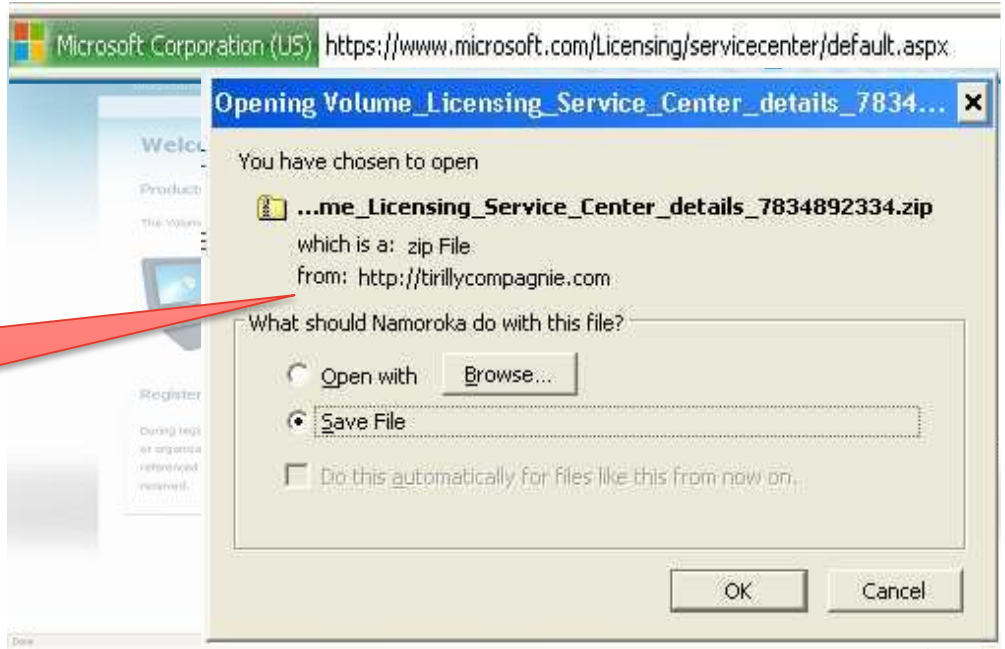
The Microsoft Volume Licensing Service Center Team

Investigation Case Study

2. Victim Clicked Link and Received Malware Download

Opens real, SSL-verified Microsoft site

Malware downloaded from a different site via JavaScript trick



Investigation Case Study

3. Analyst Observed Retrospective Alert for 1.php

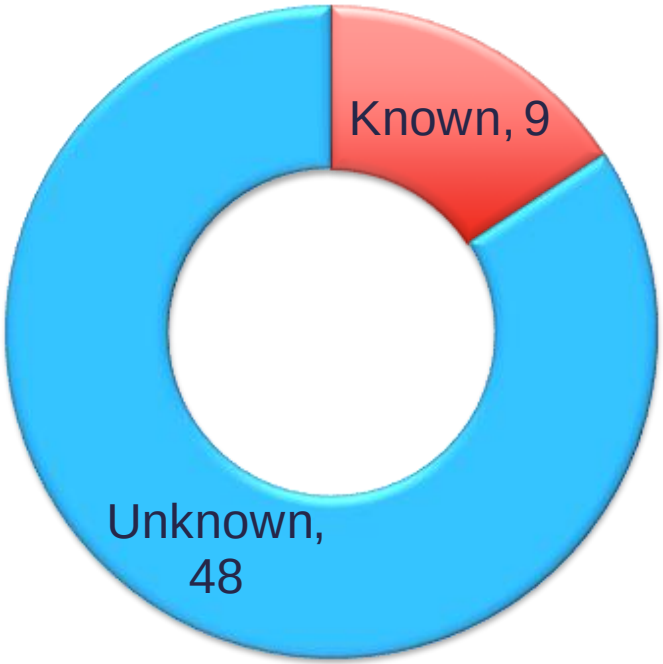
Time	Sending IP	Sending Country	Receiving IP	Sending Port	Receiving Port	Event Type	Threat Name	File Name	File SHA256
2015-01-15 16:21:10	46.105.47.143	FRA	[redacted]	[redacted]	54120	Threat Detected in Network File Transfer (Retrospective)	GenericKD:TR-tpd	Laha	53365e66...0d58fdd0
2015-01-15 16:54:16	46.105.47.139	FRA	[redacted]	80	35769	Threat Detected in Network File Transfer (Retrospective)	GenericKD:TR-tpd	Laha	53365e66...0d58fdd0
2015-01-15 17:14:28	95.211.34.220	NLD	[redacted]	80	33519	Threat Detected in Network File Transfer (Retrospective)	GenericKD:TR-tpd	Laha	53365e66...0d58fdd0
2015-01-15 17:25:10	95.211.34.220	NLD	[redacted]	80	33892	Threat Detected in Network File Transfer (Retrospective)	GenericKD:TR-tpd	Laha	53365e66...0d58fdd0
2015-01-15 20:29:54	46.105.47.139	FRA	[redacted]	80	37084	Threat Detected in Network File Transfer (Retrospective)	GenericKD:TR-tpd	Laha	53365e66...0d58fdd0
2015-01-15 20:32:27	92.243.0.157	FRA	[redacted]	80	37166	Threat Detected in Network File Transfer (Retrospective)	GenericKD:TR-tpd	Laha	53365e66...0d58fdd0

Threat Detected in Network File Transfer (Retrospective) GenericKD:TR-tpd 1.php 53365e66...0d58fdd0

Investigation Case Study

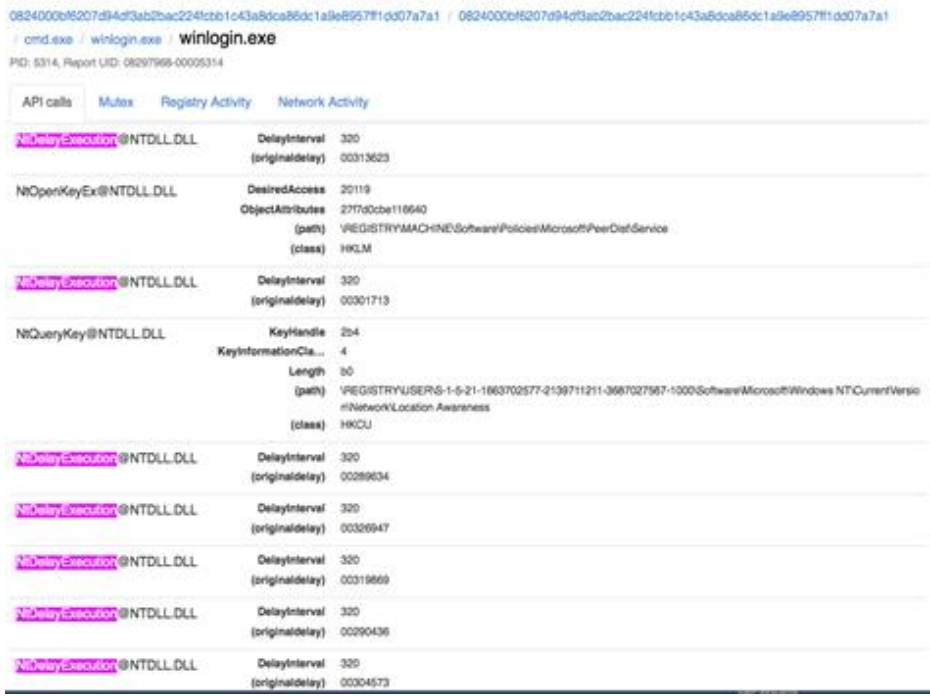
4. Analyst Researched Threat

- Virus detection 9/57
- Sandbox execution failed
- Escalated to MTD Investigator



Investigation Case Study

- All sandboxes initially called file clean
- Ran file on physical box with network and memory capture, file system monitoring



Investigation Case Study

- All sandboxes initially called file clean
- Ran file on physical box with network and memory capture, file system monitoring

Malware programmed sleep function to fool sandbox analysis

NtDelayExecution@NTDLL.DLL	DelayInterval	320
	(originaldelay)	00289634
NtDelayExecution@NTDLL.DLL	DelayInterval	320
	(originaldelay)	00326947
NtDelayExecution@NTDLL.DLL	DelayInterval	320
	(originaldelay)	00319869
NtDelayExecution@NTDLL.DLL	DelayInterval	320
	(originaldelay)	00290436
NtDelayExecution@NTDLL.DLL	DelayInterval	320
	(originaldelay)	00304573

- Investigator Conducted Forensic Analysis
  Discovered malware as “Chanitor”; uses sandbox evasion

Investigation Case Study

6. Investigator Determined Malware C2 Servers

Online service to learn C2 IP address

DNS Queries	IP Resolution at Time of Analysis
api.ipify.org	50.16.221.126, 54.225.211.214, 54.235.186.52
o3qz25zwu4or5mak.tor2web.org	194.150.168.70, [illegible]
o3qz25zwu4or5mak.tor2web.ru	166.78.1[illegible]

Tor servers; malware tested for connectivity before sending data

Investigation Case Study

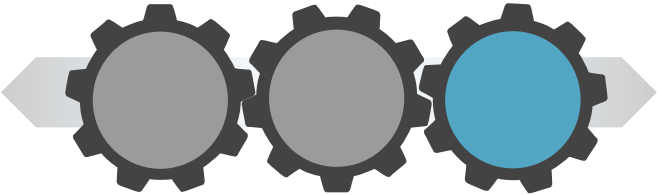
7. Investigator Searched for C2 Traffic

MTD Investigator searched NetFlow traffic.

Objective: Determine whether the victim was compromised and under remote control ?

Result: No evidence found.

Investigation Case Study



8. Investigator requested to Block Domains
No successful exfiltration; malicious sites blocked

Customer guided to block the file by hash on email and web gateways, and block 3 domains used to serve the malicious files

Key Takeaways

Observation	Conclusion
Attack targeted corporate users by phishing with corporate-licensed software	Attackers after more than just personal data
Malware examination required physical forensic analysis due to sandbox evasion techniques	Sandbox technology useful but only part of solution
Attacker used Tor for C2 traffic	Tor connections should raise suspicion on corporate networks
Malware domains quickly discovered and blocked	Monitoring by senior security investigators key to protect against advanced attacks

Q & A

Complete Your Online Session Evaluation

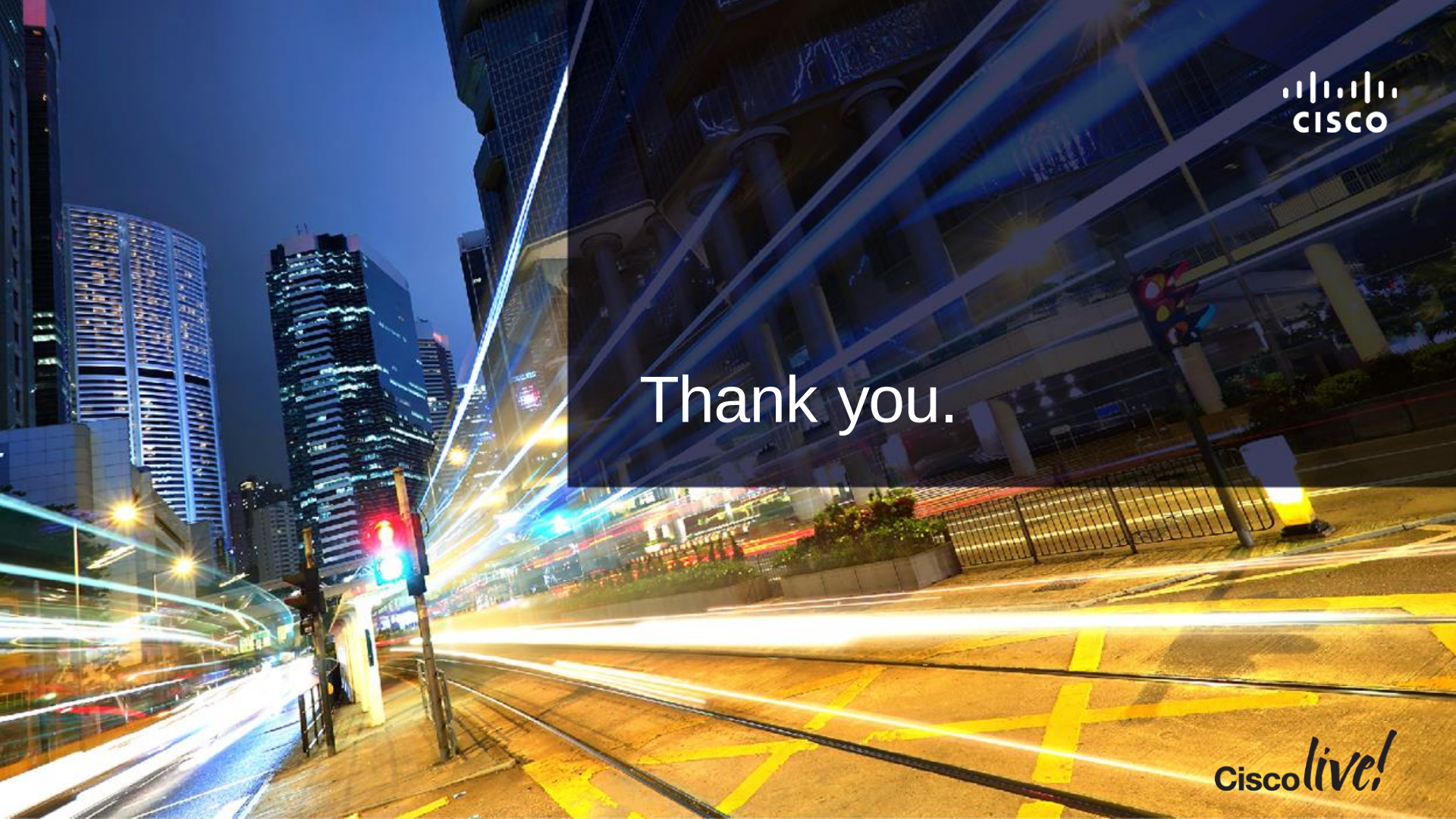
Give us your feedback and receive a Cisco Live 2015 T-Shirt!

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