TALOS THREAT RESEARCH SUMMIT

Defending Cisco

Mike Scheck

Director, Cisco CSIRT

Cisco live!

Agenda

- CSIRT in Action
- What is CSIRT
- Arming a CSIRT for Success
- Secrets of the Playbook
- CSIRT Lessons learned

CSIRT in action

CSIRT to the Rescue
Detecting and Mitigating Covert Malware

Situation

- Non Managed IT software has a backdoor installed that allows remote access into the Cisco network through multiple covert channels.

Detection

- Leverage multiple flow based technologies to determine systems making connections to known C2. Anyconnect and NVM gives insight into not only system, but process making calls. Can look for additional connections from malicious processes

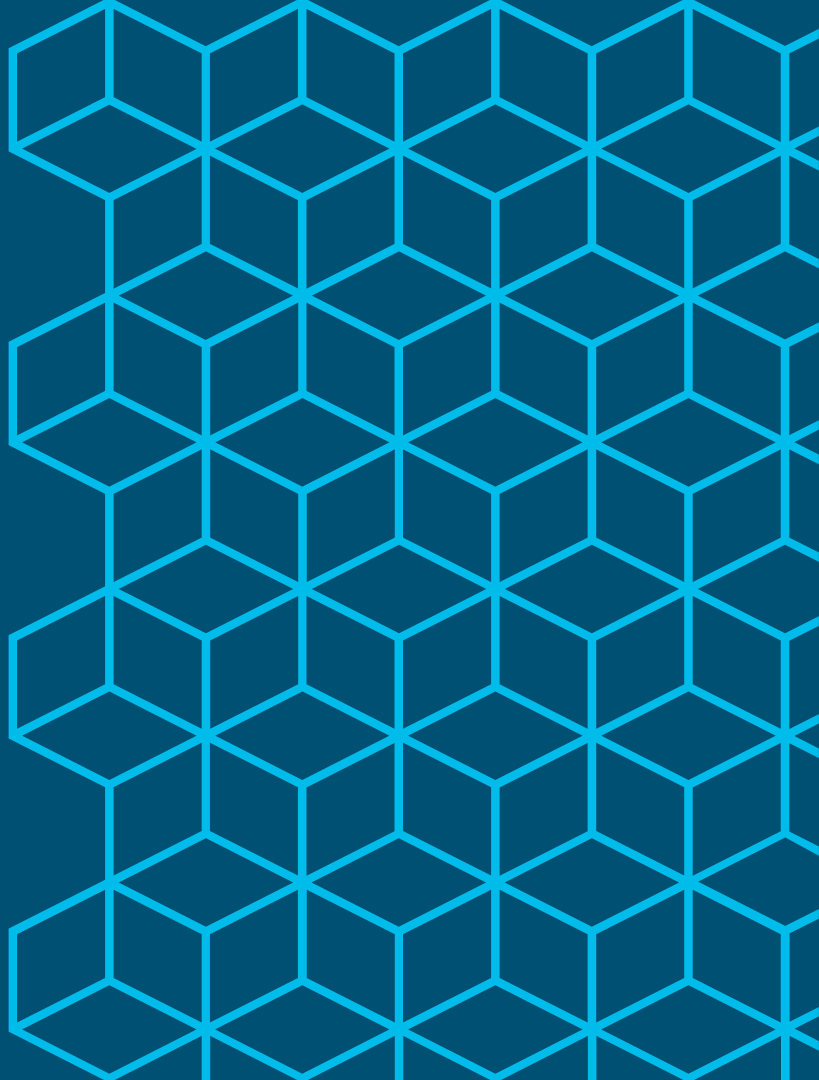
Mitigation

- Implement blocks at the multiple layers, Network/IPS, host based, and file based AMP. Block process execution as well as C2. Umbrella DNS blocks allow blocking on and off prem.

Statement

- Multiple layers of visibility and defense allow CSIRT to detect and mitigate at a level that wasn't possible until convergence of our security portfolio.

What exactly is a CSIRT, and why do you need one?



Defending CISCO

CSIRT: OUR MISSION & TEAM STRUCTURE

CSIRT

Reduces the risk of loss as a result of security incidents for Cisco-owned business. CSIRT regularly engages in proactive threat assessment, mitigation planning, incident trending with analysis, security architecture, and incident detection and response.

+

- Device Deployment & Operations
- Solution Design & Development
- Acquisition integration
- Consulting
- Purple Teaming
- Vulnerability Scanning
- Data Management
- Data Leakage Monitoring
- Legal/HR Support
- Operations Support
- Malware Reverse Engineering
- Product Testing
- Sales Support

The Evolution of the Cyber Criminal

Now a sophisticated business focused on ROI

Old School Threats

- Cyber-punks/Hackers
- Individual's Data
- Opportunistic
- Unsophisticated
- Notoriety/Political
- Nation State

Modern Threats

- Professional organized crime
- Trusted Insiders
- Multi-Billon $$ Business
- Targeted/ROI
- Sophisticated Supply Chains
- Nation State

Arming a CSIRT for success

Defending CISCO

WHAT IS AN INCIDENT RESPONSE TEAM?

MGT SUPPORT + TECHNOLOGY + PEOPLE + PROCESSES = IR

Defending CISCO

WHAT IS AN INCIDENT RESPONSE TEAM?

MGT SUPPORT + TECHNOLOGY + PEOPLE + PROCESSES = IR

- Understand Impact of a breach.
- Willing to investment.
- Willing to drive change through org.
- Implement and enforce policies.
- Support of best practice sharing and training.

Defending CISCO

Sometimes against itself…

Defending CISCO

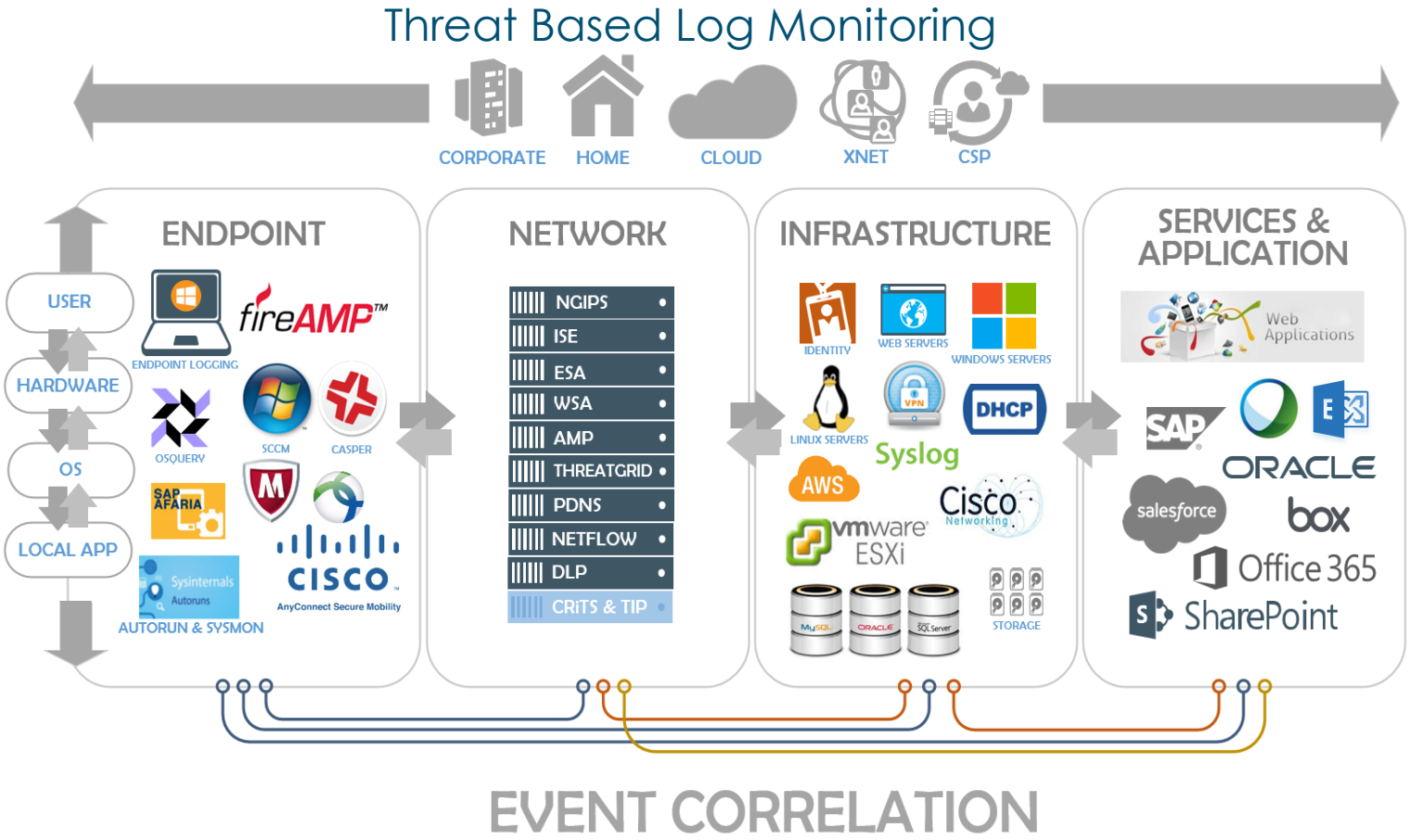
WHAT IS AN INCIDENT RESPONSE TEAM?

- Have a layered defense model.
- Perimeter | network | infra | endpoint | Application.
- Signature + Private/Shared Intel + Machine Learning + Org.

MGT SUPPORT + TECHNOLOGY + PEOPLE + PROCESSES = IR

Defending CISCO 2018

DATA COLLECTION & CORRELATION – END GOAL



PROTECTING CISCO

WHAT DATA SHOULD I COLLECT FOR IR: CORE DATA SET

CISCO

- Web Security Appliance
- Email Security Appliance
- Stealthwatch | SLN | Tetration | NVM
- AMP | FireAMP
- Adaptive Security Appliance
- ThreatGrid
- NGIPS
- Identity Services Engine
- Cognitive Threat Analytics
- Process Orchestrator
- GIR | DCE | RMS | Krieger | iCAM
- MalSpider | NetSarlacc | GOSINT

ADDITIONAL

Cisco Corporate OpenDNS deployment

Additional Network Security/Visibility

Planning and change management for 90 Days

30 Minutes to implement

166k Malware events detected in the first 24 hours

Acquisition process updated to include 0-day rollout of OpenDNS providing immediate security and visibility with no hardware requirements

Network, Web, Email Security Integrated File Analysis

AMP
Advanced Malware Protection

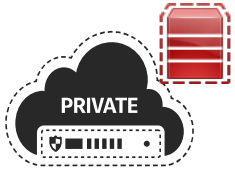
AMP for Networks
IDS / IPS

AMP on Web Security Appliance

AMP on Email Security Appliance

AMP Endpoint Agents

AMP File Analysis



AMP Private Cloud

AMP ThreatGrid Sandbox

Threat Intelligence Engine

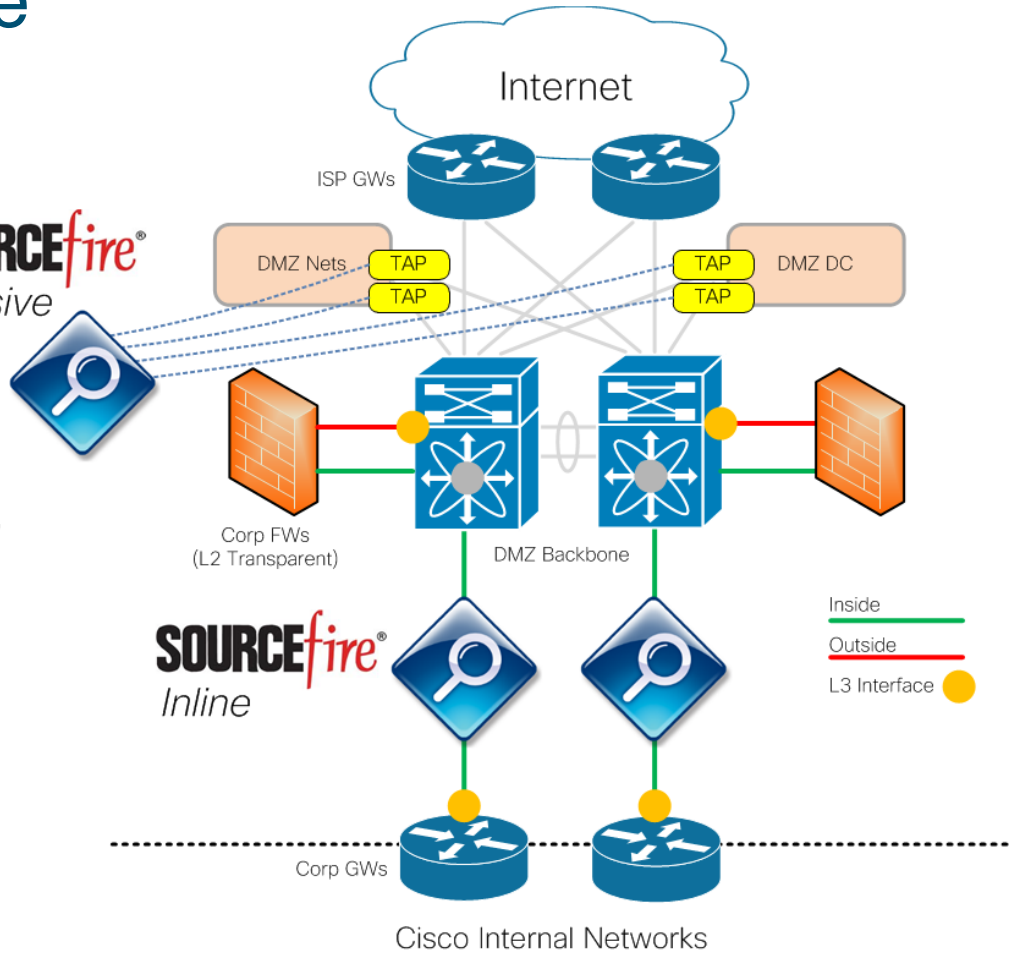
Process names
Registry Keys
IP Addresses
DNS Names

splunk>

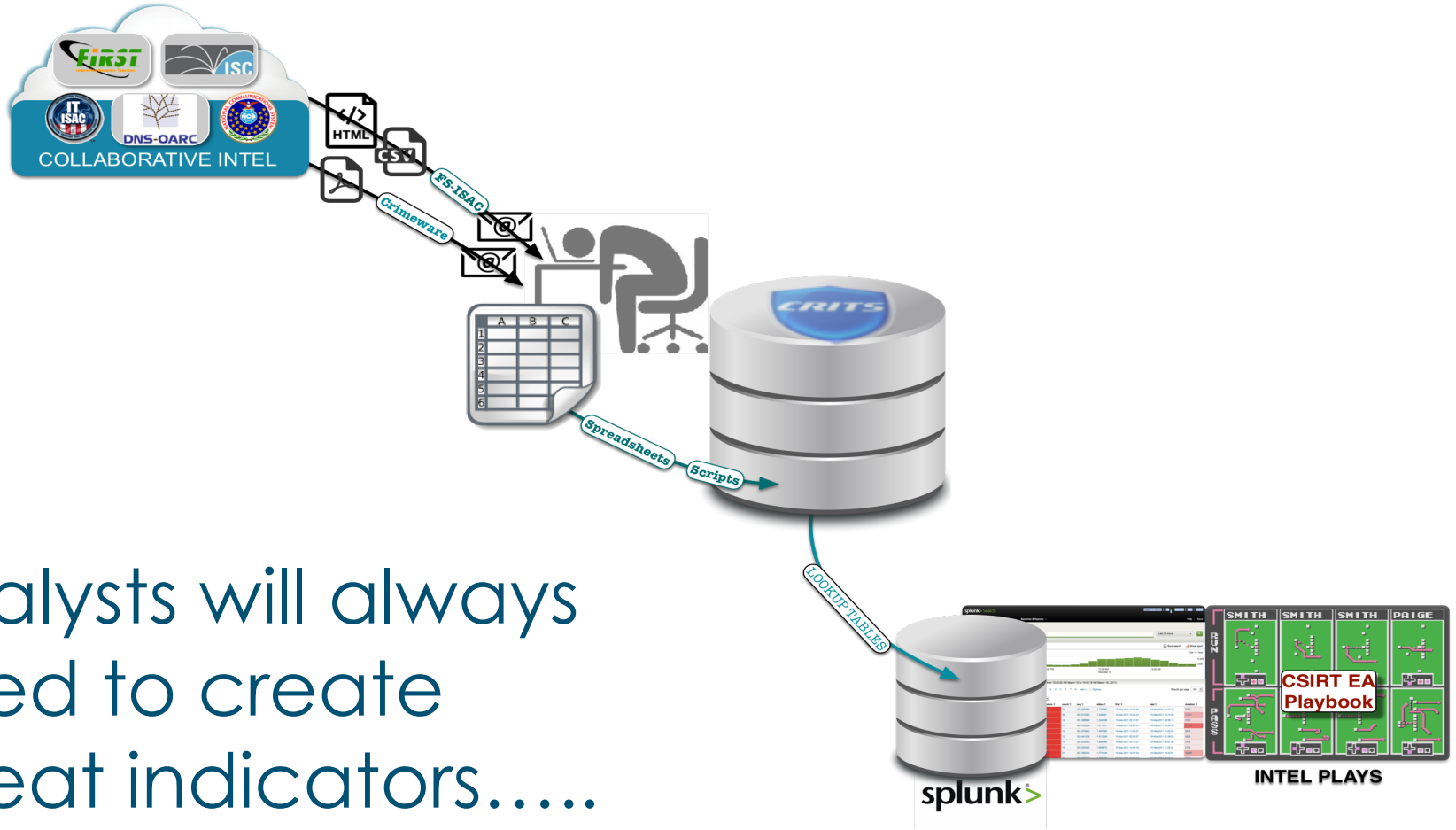
FirePower IPS Architecture

Both Inline and Passive

- Deploy inline/blocking only at iPoPs with user transit to the Internet
- Real time, proactive network-based threat detection and prevention
- Reduction in time-to-contain from hours to “didn’t happen”
- Inline redundancy
- Supports up to 20Gb/s of throughput
- Deploy passive for all other monitoring
- Plays used to determine compromise
- Efficacy of plays tracked to determine potential sigs for blocking



Preparing Threat Intel for Plays

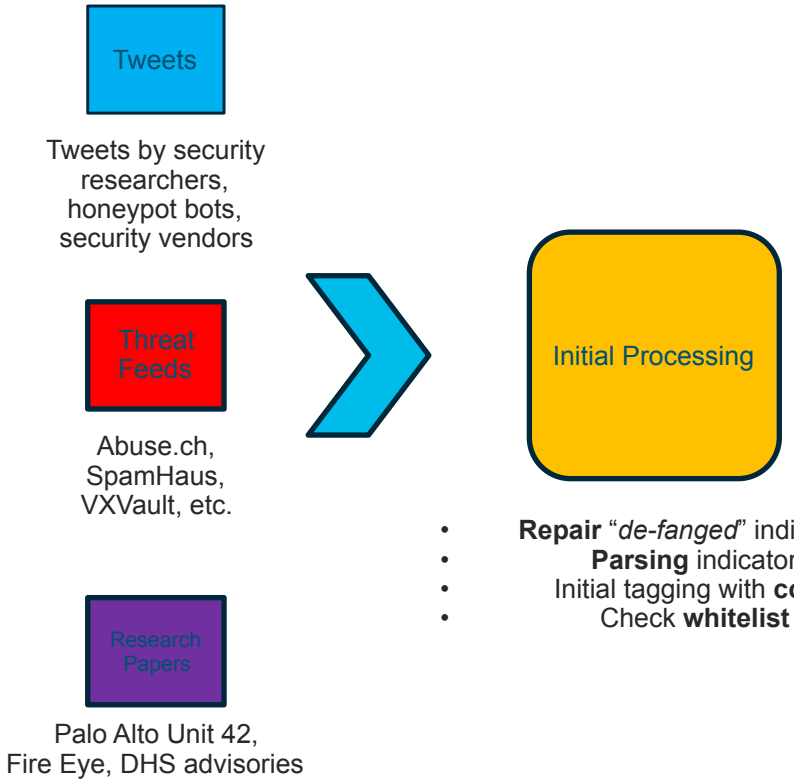


Analysts will always need to create threat indicators…..

GOSINT

Open source intelligence – in Go

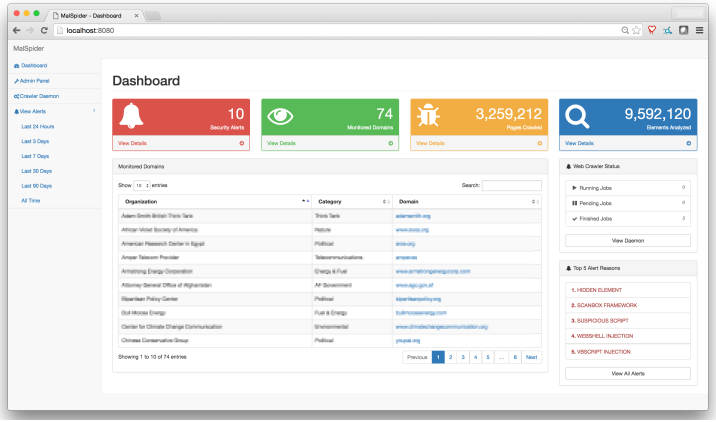
- Convert unstructured IOCs into a common schema
- Export to multiple industry standard formats
- Sanitize and validate indicators
- Automate tasks and reduce analyst time spent manually gathering and researching OSINT
- Mitigate costly errors by properly vetting all indicators while reducing the overhead of such a task
- Zero loss queuing so no vital intel is lost

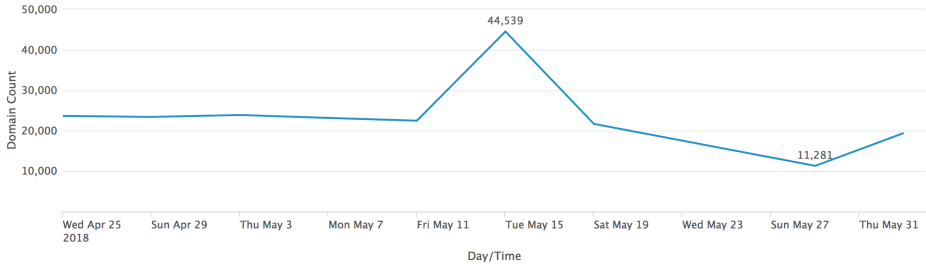


We ***proactively*** monitor websites

Using MalSpider to find interesting behavior

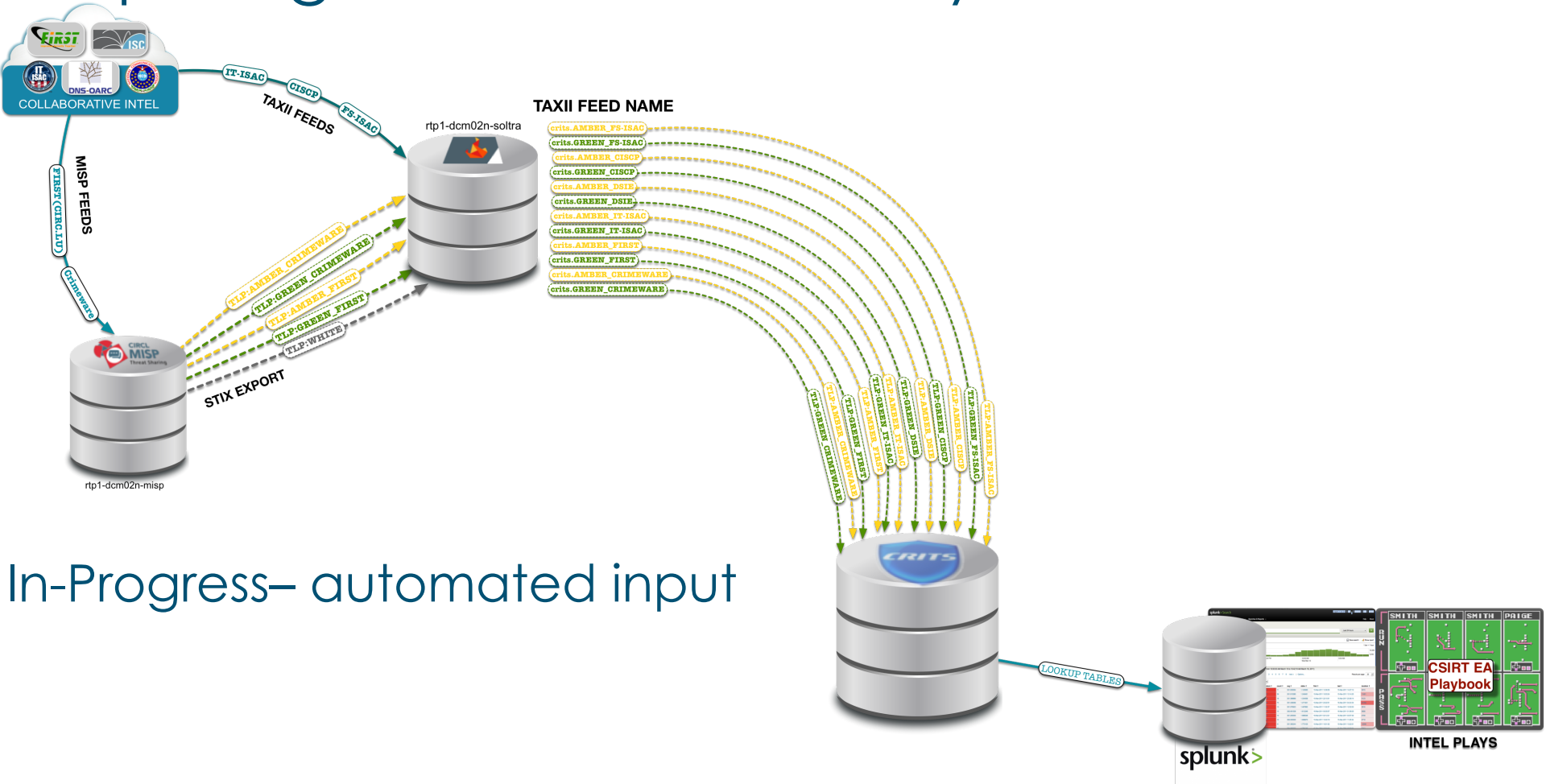
- **Websites** for Characteristics of Compromise
- **CDN/Third Party Javascript Resources** for Malicious Modifications





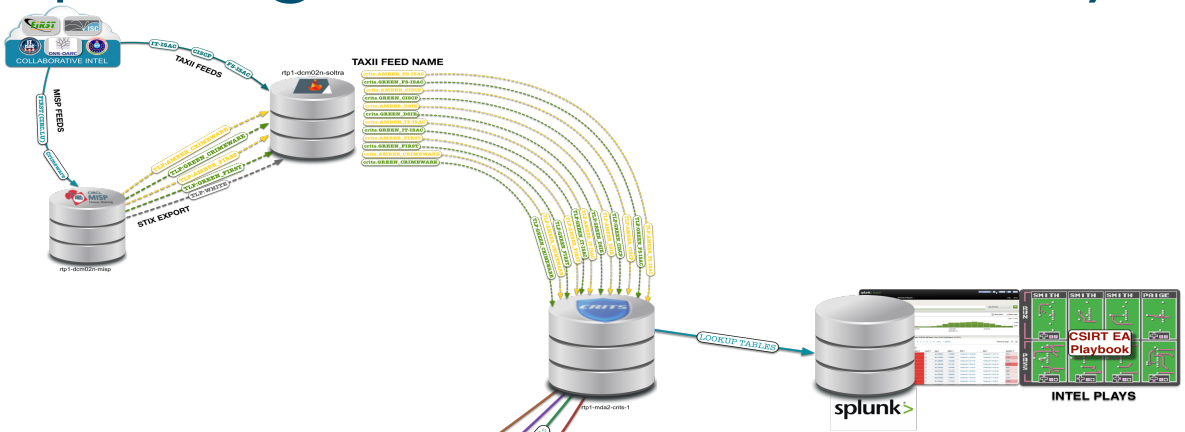
Domains w/ JavaScript cryptominers

Preparing Threat Intel for Plays

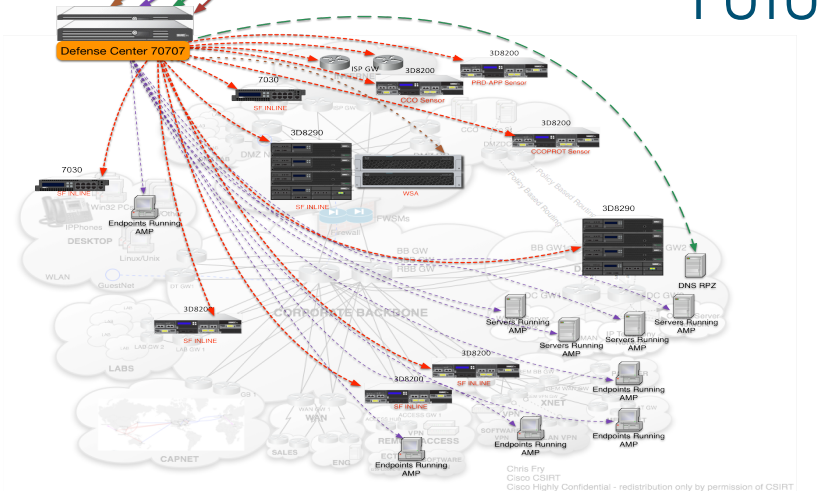


In-Progress– automated input

Preparing Threat Intel for Plays

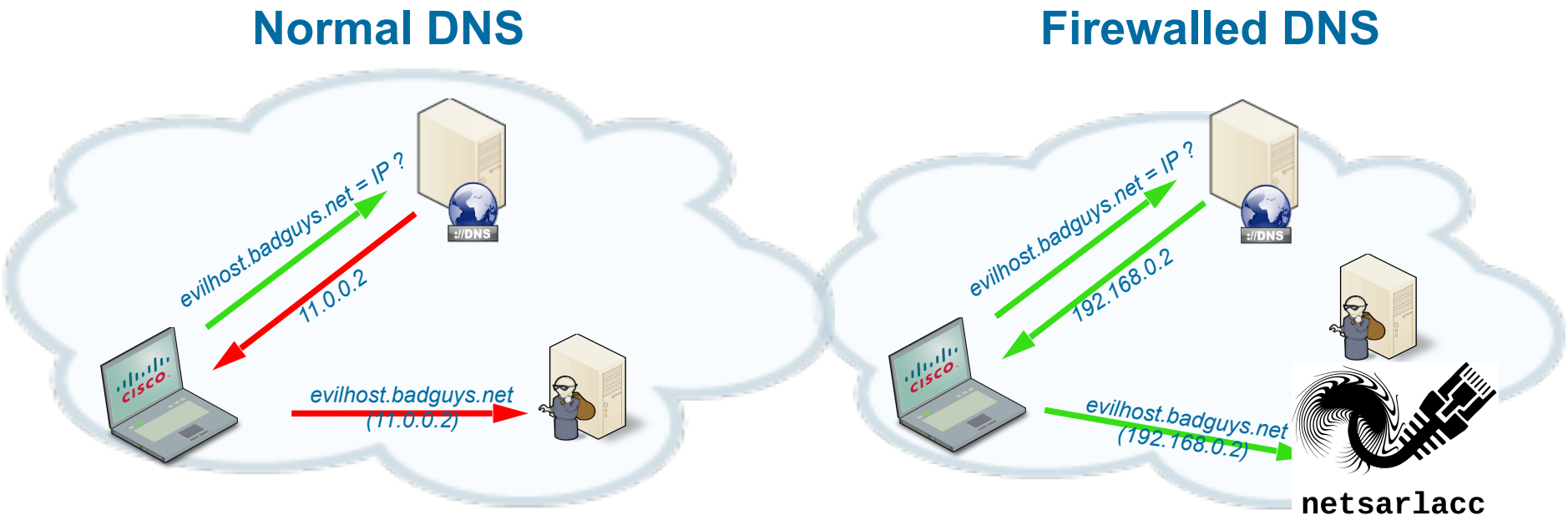


Future – full automation



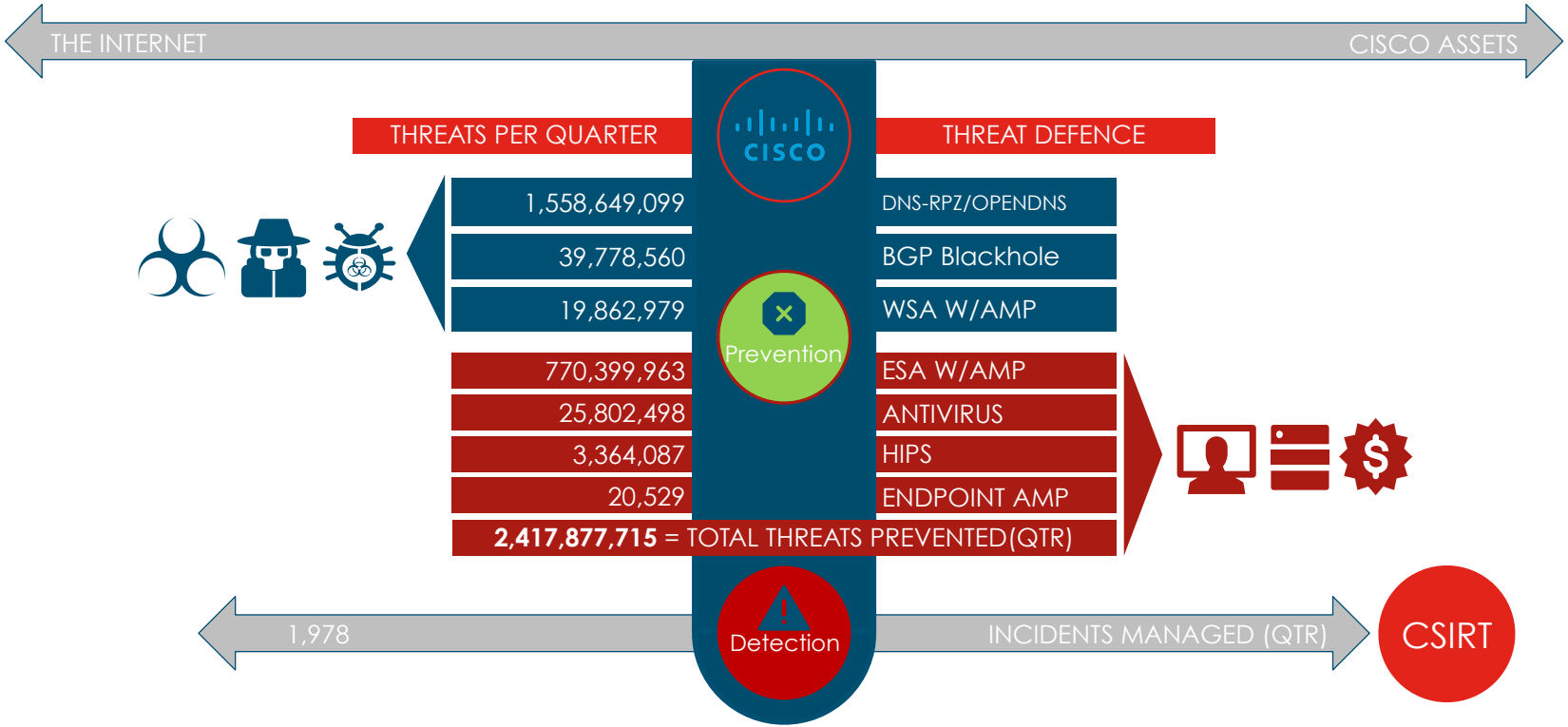
Mitigate: DNS Firewall

CSIRT deployment of netsarlacc



PROTECTING CISCO

PREVENTATIVE SOLUTIONS vs MANAGED INCIDENTS



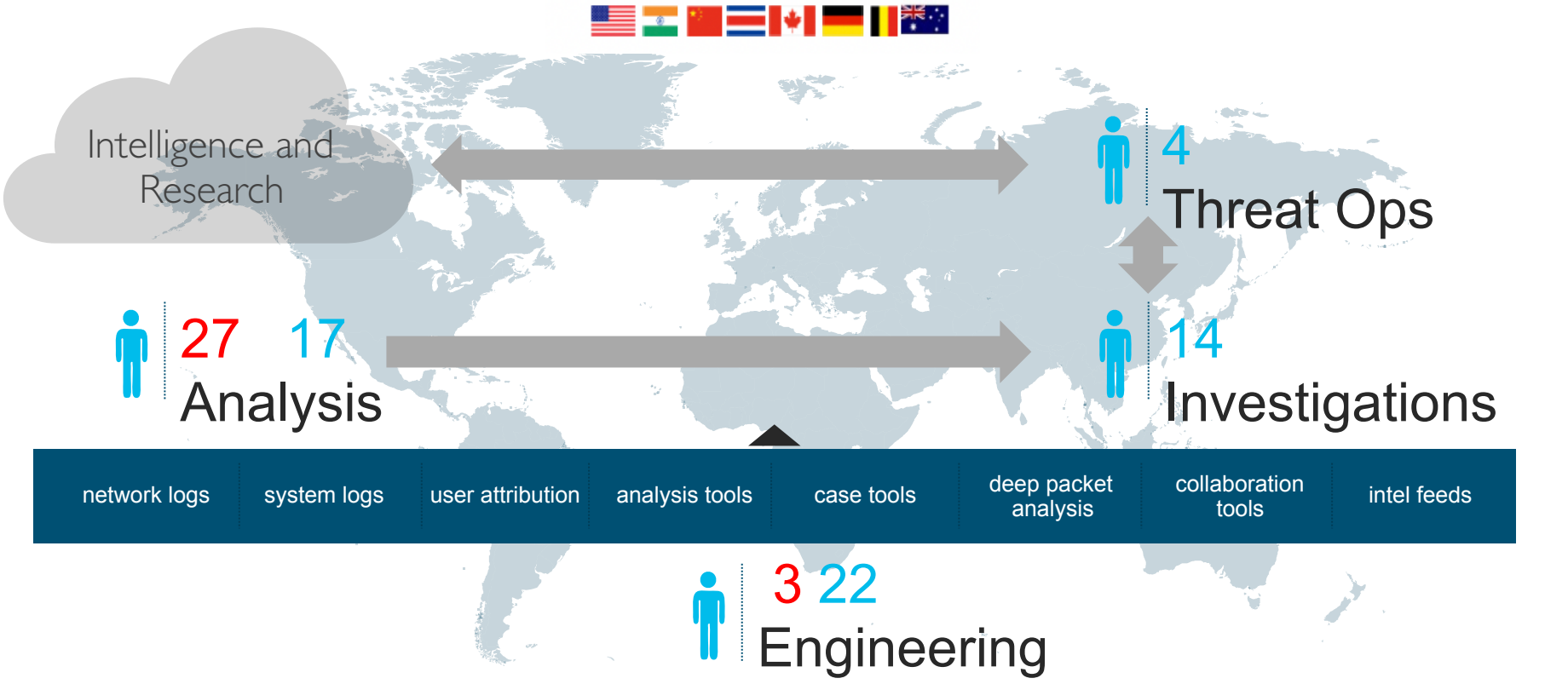
Defending CISCO

WHAT IS AN INCIDENT RESPONSE TEAM?

MGT SUPPORT + TECHNOLOGY + PEOPLE + PROCESSES = IR

- Specialized technology backgrounds.
- Understand the environment.
- Recognize tech | business | people | process gaps.
- Able to drive & influence change.
- Develop partnerships.

Global 24/7 Staff



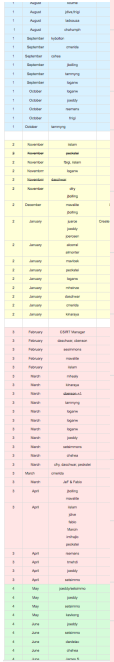
The heart of a CSIRT

How do you create a culture of fun and friendship?

CSIRT Skills

How do you make sure they have the right s

- Join an group like FIRST to collaborate and learn
- Encourage senior staff to present at security events (it's good for them as well as your team)
- Help management understand the importance of travel and training budget
- Track training year/year quarter/quarter to make sure everyone is give an opportunity
- Don't be afraid to let people have fun while they develop



3	February	CSIRT Manager		RTP, NC	Strategy Workshop	Team Strategy
3	February	daschwar, cbenson		San Juan, Puerto Rico	FIRST 2017 Planning Meeting	Support
3	February	sesimmons		Amsterdam	NG-DMZ implementation	Support
3	February	mavalite		Berlin	Cisco Live	Presenter
3	February	iislam		Berlin	Cisco Live	Team Meeting
3	March	mhealy		New Zealand	NSIE Multi-Lateral	Attendee
3	March	kinaraya		Shanghai	CRDC team visit	Team Meeting
3	March	~~cbenson +1~~		~~Kiawah Island, SC~~	~~CEO Leadership Council~~	~~Support~~
3	March	tammyng		Tucson, AZ	Women in Cybersecurity	Support/Recruitment
3	March	loganw	020-048868	Toronto	Cisco Security Week	Presenter
3	March	loganw	020-048868	New York	Cisco Security Week	Presenter
3	March	loganw		Bangalore	SOC Visit, NG DMZ Deployment	
3	March	joeddy		Bangalore	NG-DMZ implementation	Support
3	March	setsimmons		Netanya	NG-DMZ implementation	Support
3	March	chshea		San Jose		Team meeting
3	March	cfry, daschwar, peckstei		San Jose	Cisco Internet Office Workshop (Split Tunneling / DIA in-person meetings)	Meetings with IT & Infosec
3	March	cmerida		San Jose	SJC Site Visit/ Splunk	
3	March	JeF & Fabio		RTP	AWS Hackathon	Participants

Defending CISCO

WHAT IS AN INCIDENT RESPONSE TEAM?

- Have actionable processes.
- Automate recurring problems.
- Ability to measure & report on impact.

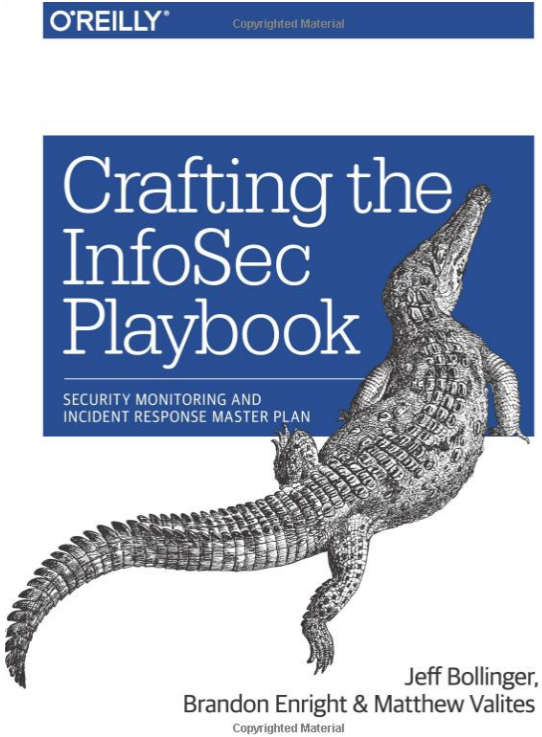
MGT SUPPORT + TECHNOLOGY + PEOPLE + PROCESSES = IR

Playbook Secrets

PROTECTING CISCO

I HAVE THE DATA, NOW WHAT: PLAYBOOK OBJECTIVES

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



Playbooks – Active response to threats

What are we trying to protect?	What are the threats?	How do we detect them?	How do we respond?
Cisco.com	DoS attack SQL Injection Directory traversal	NetFlow monitoring IPS/IDS detection System logs	Engage ISP Investigate
Active directory servers	Lateral movement Account compromise Malware	NetFlow alerts User activity HIPS logs	P1 incident Investigate
End user laptop	Malware Phishing attacks Drive-by download	HIPS/AV logs ESA logs WSA logs	Reimage Investigate

Playbook Example #1:
Sourcefire IPS Detection for Wannacry

Bug 12963 - 110093-INV-IPS-HOT_THREAT: Microsoft Security Bulletin MS17-010 & WannaCry ransomware (edit) Save Changes

Status: DEPLOYED (edit)

Product: CSIRT Playbook
Component: Investigative
Version: 2.0
Hardware: Other / All

Importance: P3 / major
Assigned To: csirt-analysts-qa@cisco.com (edit) (take)
QA Contact: csirt-analysts-qa@cisco.com (edit) (take)

URL:
Keywords: proactive_threat
Tags:

Depends on:
Blocks:
Show dependency tree / graph

Reported: 2017-05-12 19:15 UTC by Joey Rosen (joerosen)
Modified: 2017-05-19 18:16 UTC (History)
CC List: Add me to CC list
3 users (edit)

Tier Assignment: Tier 1
Incident Severity: High
Play Context: General
Play Search Scope: Cisco Corp
US Only: No - Outside of the US
Hot Threat: Yes
Play Search Source: Splunk

Objective:
```
This report is leveraging several Talos signatures to detect
activity for the recent Microsoft Windows vulnerability,
also known as MS17-010.  The report will also detect
activity related to ETERNALCHAMPION and ETERNALBLUE.
```

Analysis:
```
EA T1:
- Check relevant IPS events
- Identify traffic source and target
- Use CSIRT tools to get Cisco internal host information: IP
```

Splunk Query (Long):
```
index=ips NOT src_description=IN_VULNERABILITY_SCANNER
earliest=-4h rec_type_simple=PACKET OR rec_type_simple="IPS
event"
[search index=ips earliest=-4h (sid=41978 OR sid=42255 OR
sid=42256 OR sid=42329 OR sid=42330 OR sid=42331 OR
sid=42332 OR sid=42340) | fields event_id, event_sec,
|transaction event_id
```

Playbook Example #2
Lookup Query Play with Threat Intel

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

index=wsa earliest=-24h [inputlookup intel-url-green |
    where like(confidence, "medium") |
    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

Playbook Efficacy

How do you know you have the right plays?

As we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don't know we don't know.

PROTECTING CISCO

Understanding the threats with ATT&CK

PLAYBOOK EFFICACY

Completed Date: Previous quarter

NON-EMPTY PLAYS

600041 700017 600051 700006 600056

Play		# of Runs	Total # of Events	Avg. Run Time	# of True Positives	# of True Positives Duplicate	# of False Positives	# of Undetermined Hosts
600041	Files dropped by MS Office	366	36	14 mins	0	0	17	0
600051	USB/External_drive infections o..	534	46	31 mins	3	0	0	0
600056	To detect host suspected to be i..	534	12	28 mins	2	0	1	0
700004	TLP:GREEN Domain Indicators	77	230	85 mins	7	6	52	0
700006	DNS resolution requests for kno..	64	82	59 mins	0	6	17	0
700012	Gamarue malware activity	534	122	18 mins	14	75	0	0
700	f DNS lookups	534	54	44 mins	7	9	5	0
700	S lookups	534	85,436	31 mins	27	72	1,014	0
700017	DNS Lookups to Bad Reputation..	535	18,168	54 mins	156	1,288	4,446	0
700	HP panel posts	534	5	18 mins	0	0	2	0
700	s to Gamarue Malw..	178	365	27 mins	30	91	2	2
700021	Monitoring of Pirrit DNS Indicati..	534	7	9 mins	1	4	0	0
710000	Sustained, egregious high volu..	11	291	130 mins	2	0	0	0
800	SH Brute Force	179	2,008	311 mins	0	0	0	2
850	ser still able to VP..	30	7,391	71 mins	0	0	2	0
860005	Detection of emerging Hashes ..	12	211	182 mins	5	0	0	0
860006	Detection of suspicious Microso..	11	27	56 mins	1	0	0	0
900015	Sality Virus	534	48	31 mins	3	13	2	0

EMPTY PLAYS

Play Id	Title	Owner	# of Runs	Total # of Events
100004	CCO Monitoring	QIACHEN	178	9,416
100008	CMS Targetted Monitoring	FPARRALE	178	0
100027	CxO VIP Monitoring	FPARRALE	178	0
100034	Outbound connections from spe..	JKUMARR2	178	0
100046	IRC from unexpected location	JUARCE	534	0
100058	CRDC UPLOAD-IPS-Sig	KEVKONG	178	0
100063	MFE One Attacker to Many Targ..	FPARRALE	178	0
100065	MFE One Attacker Firing Many ..	FPARRALE	178	4
100066	MFE One Signature Against Ma..	FPARRALE	178	111
100067	MFE Many Attackers to One Tar..	FPARRALE	178	43
100068	WebEx MFE Many Attackers to ..	JUMANA	178	729
100069	WebEx MFE One Signature Agai..	SANATASO	178	270
100070	WebEx MFE One Attacker Firing..	JUMANA	178	60
100071	WebEx MFE One Attacker to Ma..	SRER	178	845
100076	Multi-victim SMB brute forcing	JKUMARR2	534	0
100080	TLP:GREEN IPV4 Indicators	PORTEGAU	92	71
100082	SQL Injections	JUARCE	114	704
100083	Windows Worm Sweep	JUARCE	178	5

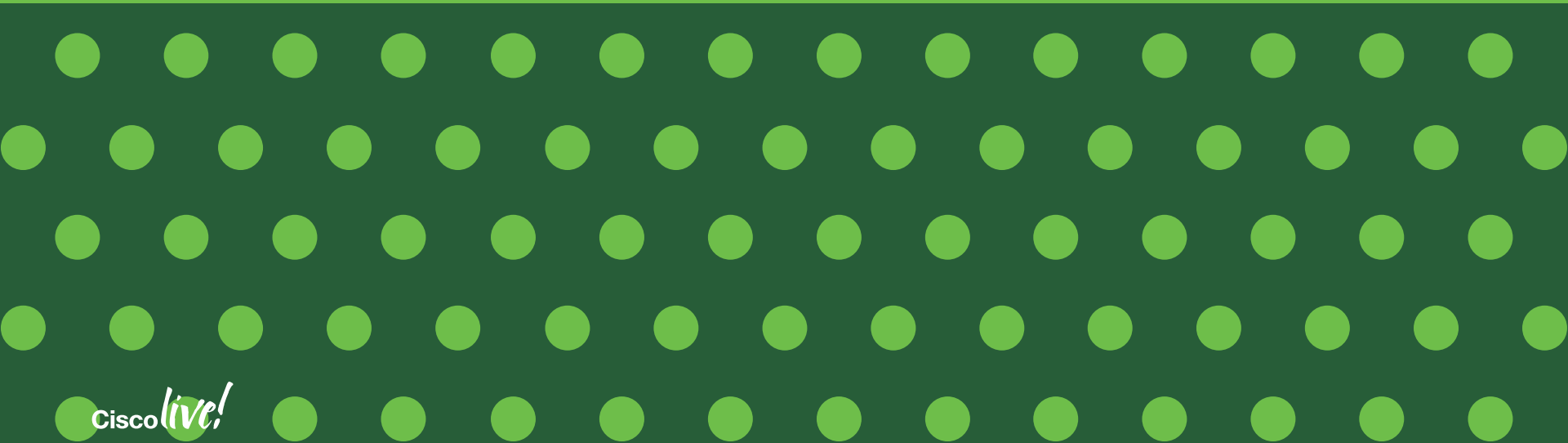
Defending CISCO

WHAT IS AN INCIDENT RESPONSE TEAM?

MGT SUPPORT + TECHNOLOGY + PEOPLE + PROCESSES = IR

- To be effective you need all of the ingredients.

CSIRT Lessons Learned



Defending CISCO

What's the difference between good and great

- Top down support for IR
- Attract and retain the right talent
- Invest tools to enable (not replace) staff
- Have process and methodology to scale to threats
- Collect the right data to detect and report
- Collaborate with other Incident Response teams
- Share your success stories

Defending CISCO

References

- High performance HTTP/SMTP sinkhole:
  https://github.com/ciscocsirt/netsarlacc
- Analyst tools for IOC handling/extraction:
  https://github.com/ciscocsirt/GOSINT
- Website compromise monitor:
  https://github.com/ciscocsirt/malspider
- Forum of Incident Response & Security Teams:
  https://www.first.org/

TALOS
THREAT RESEARCH
SUMMIT

Thank you!

Mike Scheck

@mike_scheck
mscheck@cisco.com

Learn more about Talos at
talosintelligence.com

Cisco live!

INTUITIVE