Homebrew Incident Response

@mimeframe - Manager, Incident Response

@mtmcgrew - Engineer, Incident Response

@cmccsec - Engineer, Incident Response

https://facebook.com/protectthegraph

State of affairs (the good)

Companies are...

- Investing in intrusion detection
- Developing data breach response plans (PR, insurance, BCP, …)
- Told to expect and prepare for breach

State of affairs (the bad)

Companies are...

- Rarely investing in incident response (IR) playbooks
  - how do you isolate an infected laptop in a remote office?
    - what about a production server that serves customers?

- Rarely investing in incident response (IR) tooling or infrastructure
  - logs necessary for analyzing an incident (for you or whomever you are outsourcing to)
  - semi-automated containment or eradication
  - local and remote forensics (memory or disk)

- Rarely following incident response (IR) guidelines or models
  - evidence is often timestomped or destroyed by accident
  - remediation is often rushed and compromised hosts are missed, resulting in a direct notification to the attackers

Goals of this talk

1. Open source incident response (IR) playbooks
2. Open source tooling and infrastructure
3. Discuss IR model implementation details
4. Provide solutions, both technical and procedural,
   that improve mean-time-to-{identification, resolution}
5. Encourage companies to stop “winging it” when it comes to IR
6. Promote dialogue and learn how we can improve

Quick notes

- We are only presenting on portions of our IR plan where we have good defense-in-depth
    - We are not elevating others while drowning ourselves
    - This presentation should not be viewed as holistic

Quick notes

- We regularly do goal-oriented attack simulations (redteams)
- Redteams allow us to refine our incident response processes and iterate from experience
- Upcoming slides demonstrate some core takeaways from these exercises

Quick notes

- We are emphasizing open-source tools because we realize most companies have limited financial resources for commercial products
    - We have a passion for helping small and large security teams thrive
    - We partner with companies of all sizes on our platform

Why does ‘winging’ IR fail?

because preparation and procedure matter

Why IR is here to stay

(1) http://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf

500+ companies surveyed in 2014

verticals

(ag, defense, edu, energy, media, finance, health, retail, tech, transport, ...)

company sizes

(500, 1k, 5k, 25k, 75k+)

In 2 years...

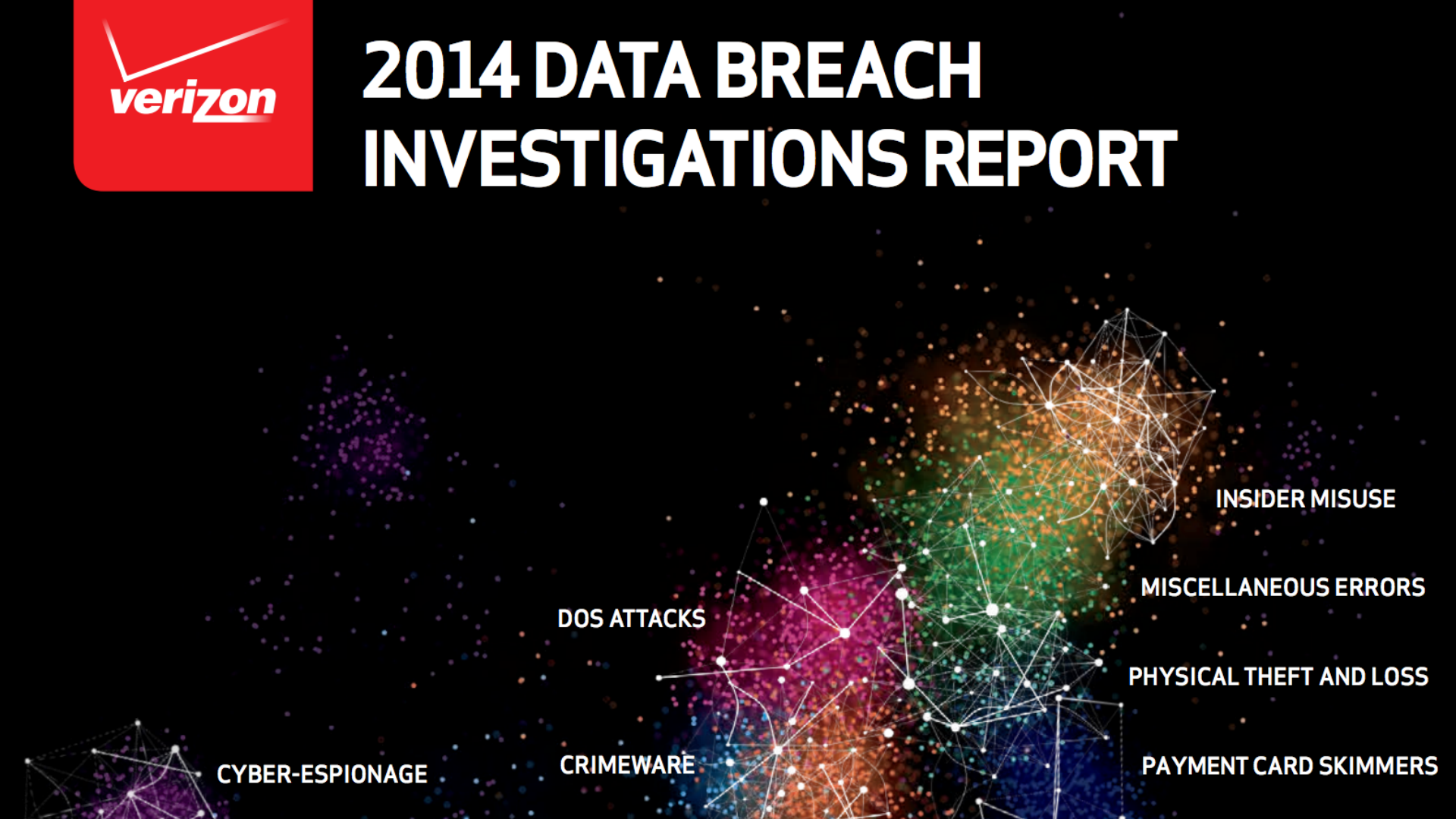
43% of companies had a breach that resulted in the loss of 1000+ sensitive/confidential records

Of those breached,

60% experienced another breach!

verizon

2014 DATA BREACH INVESTIGATIONS REPORT



1,367
CONFIRMED DATA BREACHES

63,437
SECURITY INCIDENTS

95
COUNTRIES REPRESENTED

Figure 3.
Number of security incidents with confirmed data loss by victim industry and organization size, 2013 dataset

Industry	Total	Small	Large	Unknown
Accommodation [72]	137	113	21	3
Administrative [56]	7	3	3	1
Construction [23]	2	1	0	1
Education [61]	15	1	9	5
Entertainment [71]	4	3	1	0
Finance [52]	465	24	36	405
Healthcare [62]	7	4	0	3
Information [51]	31	7	6	18
Management [55]	1	1	0	0
Manufacturing [31,32,33]	59	6	12	41
Mining [21]	10	0	7	3
Professional [54]	75	13	5	57
Public [92]	175	16	26	133
Real Estate [53]	4	2	0	2
Retail [44,45]	148	35	11	102
Trade [42]	3	2	0	1
Transportation [48,49]	10	2	4	4
Utilities [22]	80	2	0	78
Other [81]	8	6	0	2
Unknown	126	2	3	121
Total	**1,367**	**243**	**144**	**980**

Small = organizations with less than 1,000 employees,
Large = organization with 1,000+ employees

Keep in mind

these statistics only include companies that noticed and reported a breach

So, lets start with the basics

triage by example

Exercise #1

has anyone talked to evil.com?

Exercise #1

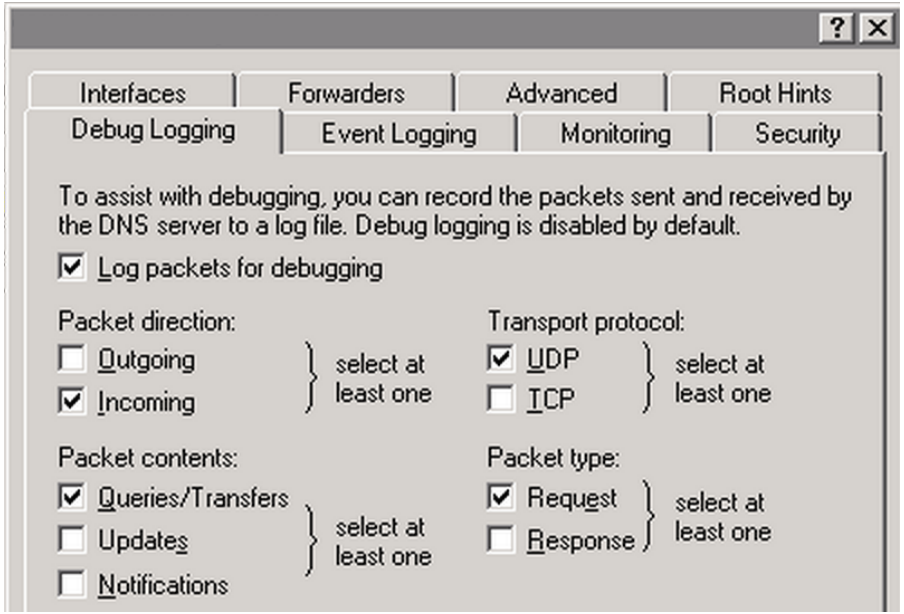
(has anyone talked to evil.com?)

- Native options:
  - DNS server logs
  - Firewall egress logs

- Foreign:
  - Proxy
  - Host agents
  - NSM platform (we'll discuss later)

DNS logs from a Microsoft © DNS Server

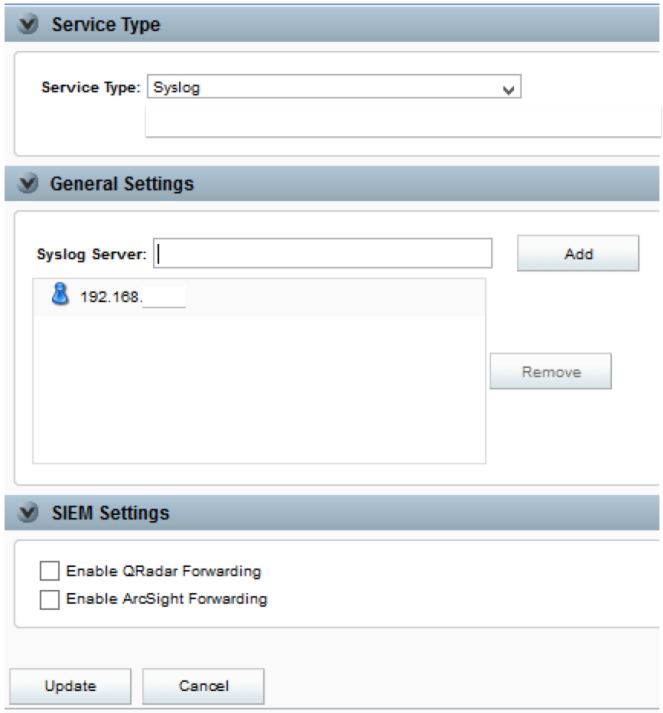
- Enable packet logging (1)
- Log location:
  - *c:\windows\system32\dns\dns.log*
- Collect and transport data via an agent
  - LogStash
  - FluentD
  - Splunk Universal Forwarder
  - ...



(1) http://technet.microsoft.com/en-us/library/cc759581(v=ws.10).aspx

DNS logs from a BlueCat © DNS Server

Use *Proteus*
to configure syslog



Firewall egress logs

syslog and forward to ElasticSearch/Splunk/SIEM

(1) https://live.paloaltonetworks.com/docs/DOC-6603
(2) https://apps.splunk.com/app/491/#/documentation
(3) https://live.paloaltonetworks.com/docs/DOC-6593

Result

we have the internal ip that queried evil.com

Exercise #2

what machine held that internal ip address?

Exercise #2

(what machine held that ip address?)

- Native options:
  - DHCP server logs
- Foreign:
  - Proxy (w/auth enabled)
  - NSM platform (we'll discuss later)

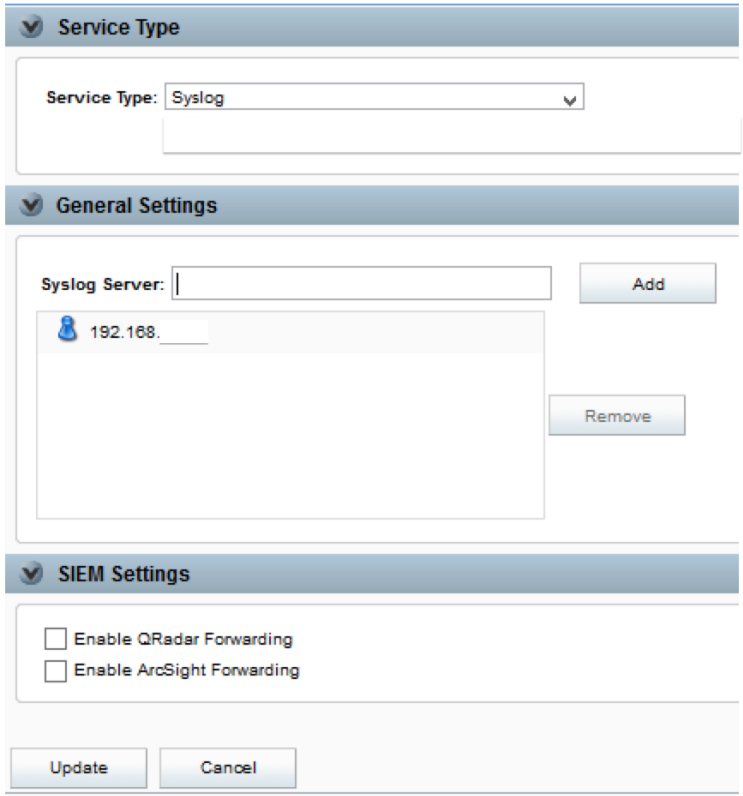
DHCP logs from a Microsoft © DHCP Server

- Enable `DHCP audit logging` (1)
- Log location: *c:\windows\system32*
  - Filenames: *DhcpSrvLog-{Mon, … ,Sun}.log*
- Collect data via LogStash, FluentD, Splunk UF, or ...

(1) http://technet.microsoft.com/en-us/library/dd183684(v=ws.10).aspx

DHCP logs from a BlueCat © DHCP Server

Use *Proteus*
to configure syslog



Result

we have the host that resolved evil.com

Exercise #3

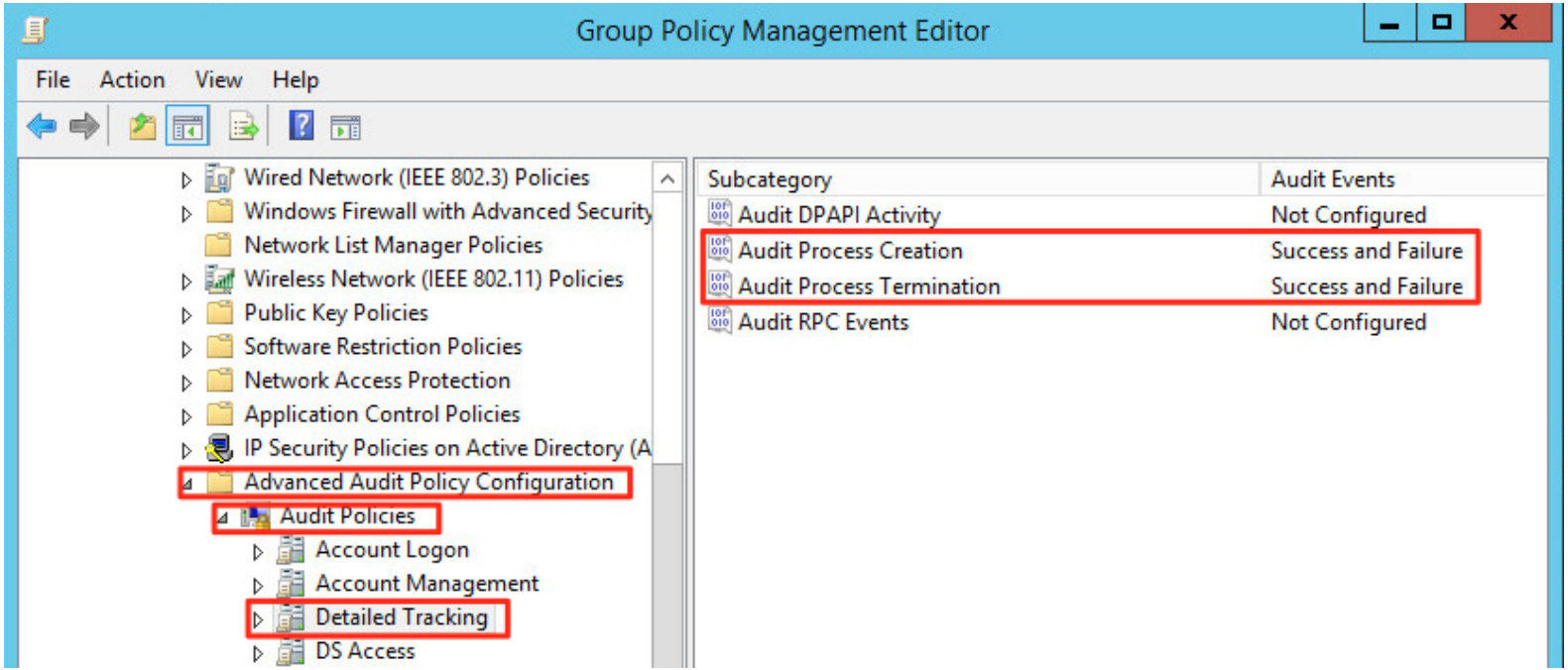
have we seen a particular process
on our Windows hosts?

Exercise #3

(have we seen this file on our Windows hosts?)

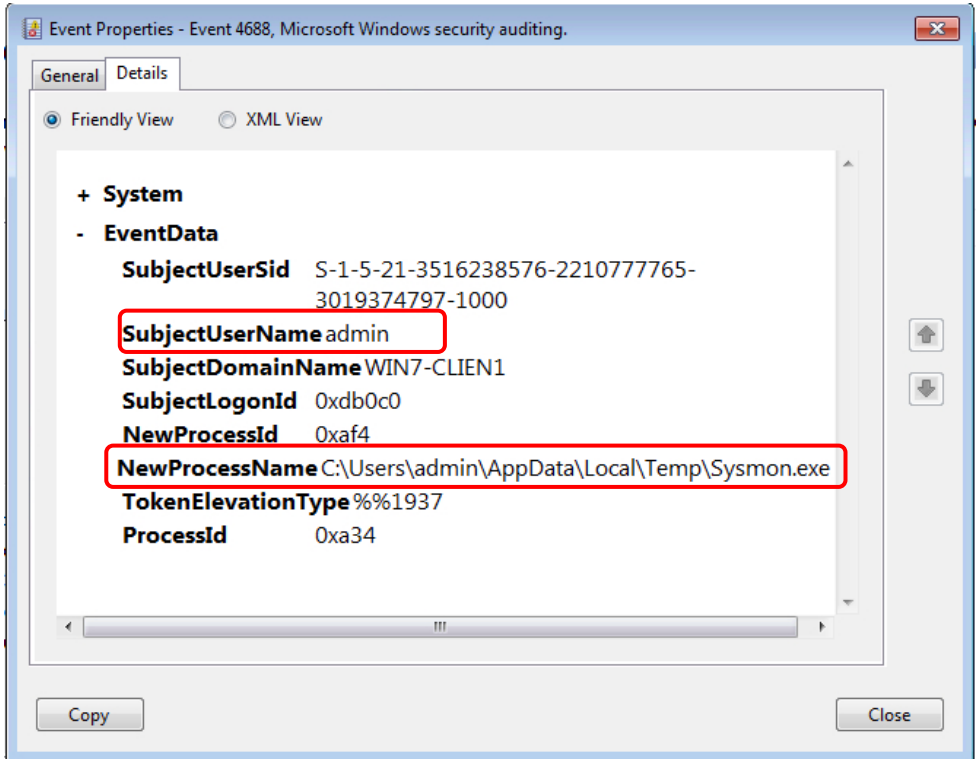
- Native Options:
  - `Audit process` feature
- Foreign:
  - Sysmon
  - Commercial ($)

`Audit process` feature



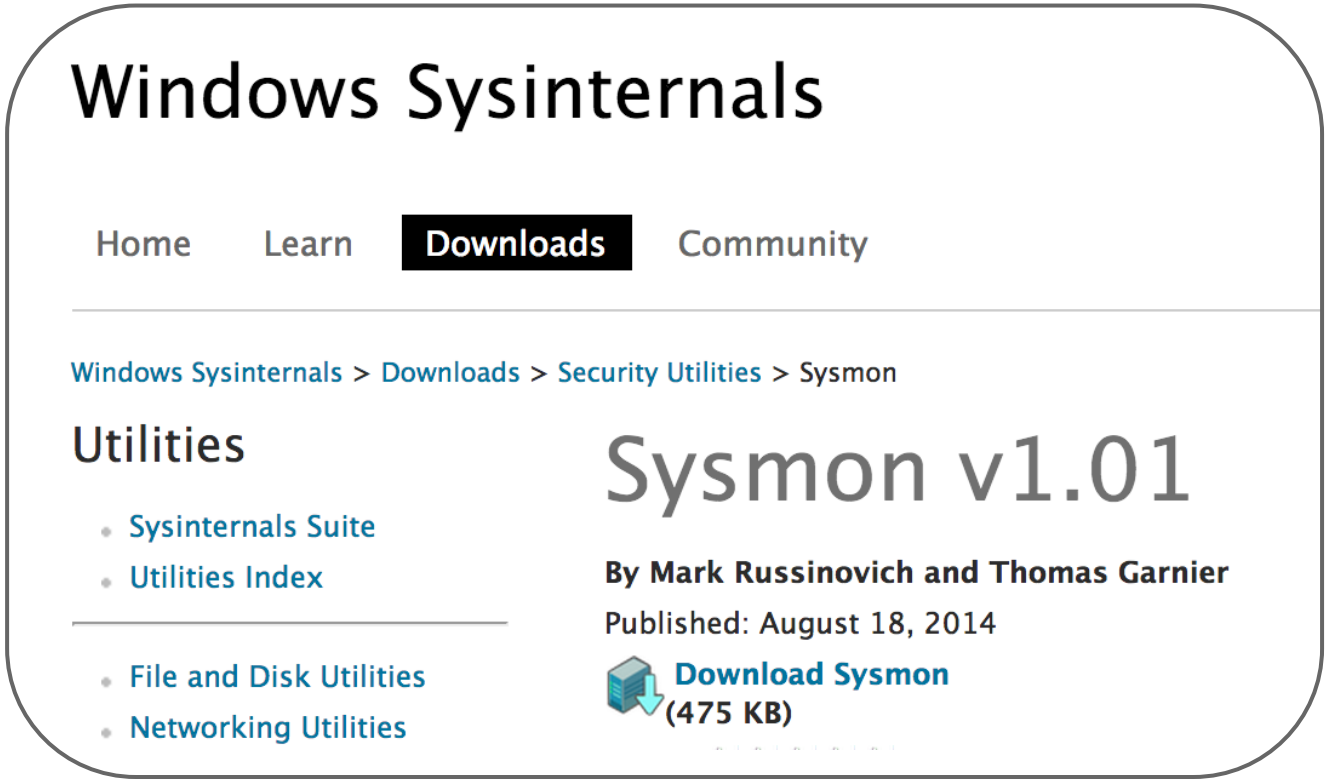
http://www.darkoperator.com/blog/2014/8/8/sysinternals-sysmon

`Audit process` feature

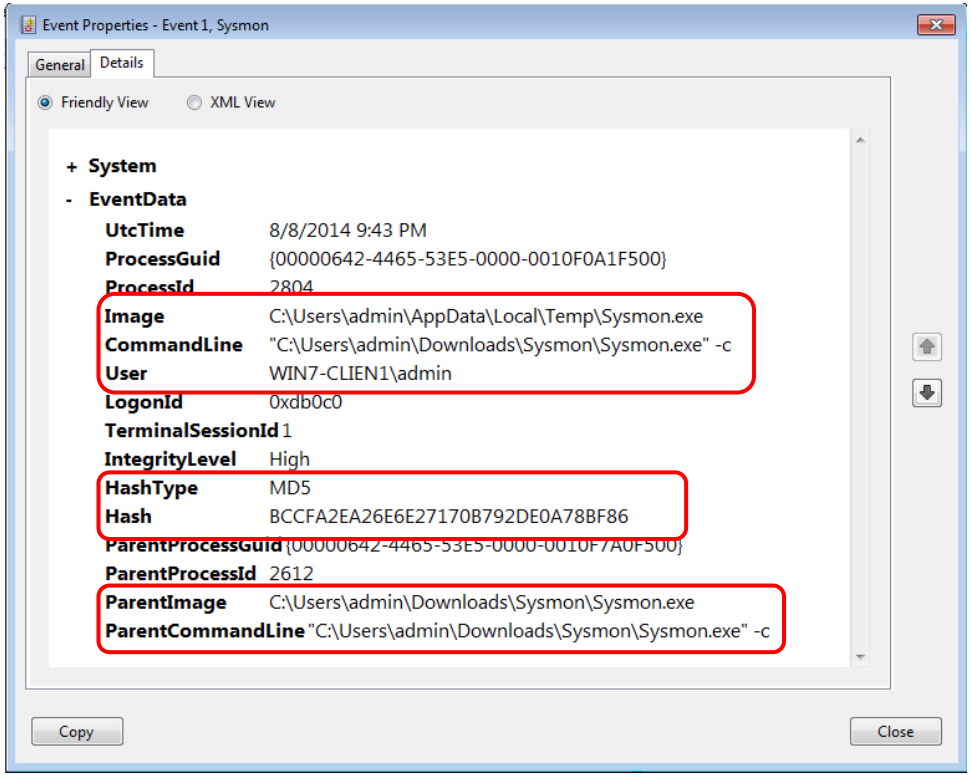


http://www.darkoperator.com/blog/2014/8/8/sysinternals-sysmon

Sysmon


Windows Sysinternals
Home
Learn
Downloads
Community
Windows Sysinternals > Downloads > Security Utilities > Sysmon
Utilities
Sysinternals Suite
Utilities Index
File and Disk Utilities
Networking Utilities
Sysmon v1.01
By Mark Russinovich and Thomas Garnier
Published: August 18, 2014
Download Sysmon
(475 KB)

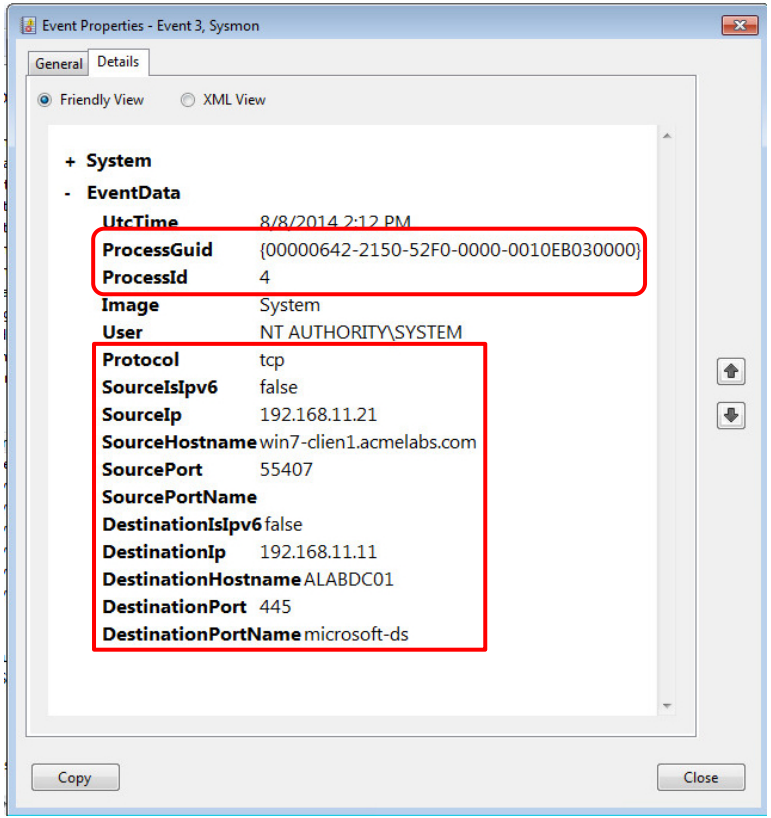
Sysmon



- *file-name*
- *file-path*
- *file-hash*
- *arguments*
- *...*

http://www.darkoperator.com/blog/2014/8/8/sysinternals-sysmon

Sysmon (there's more)



network connection to process details!

http://www.darkoperator.com/blog/2014/8/8/sysinternals-sysmon

Commercial vs. Sysmon

- It completely depends on your company culture, the availability/skillset of your team, and if you require additional features

- Pros:
  - Commercial can abstract away the need for you to worry about
    - log forwarding
    - log searching
    - log alerting

- Cons:
  - $$$
  - The filter driver is written by someone other than M$
    - There’s potential stability or performance concerns

Exercise #4

what resources did the attacker access on our local network?

Exercise #4

(what resources did the attacker access?)

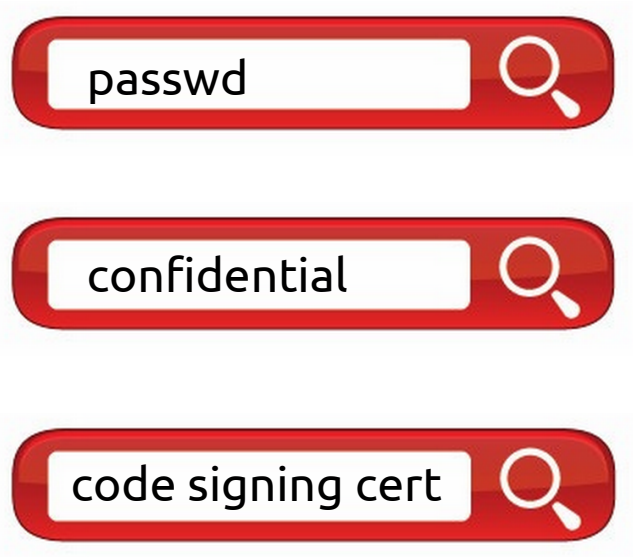
- “Native” options:
  - Configure logging on existing services
  - Netflow from switches and routers

- Foreign:
  - Add logging capabilities to existing services
  - Proxy
  - NSM platform (we’ll discuss later)

Code UI’s, DB UI’s, Wiki’s, Tasks

Verify you are logging:

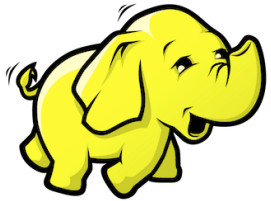
- Searches
- Page loads



Datasources

Verify you are logging:

- Connections
- Queries



Exercise #5

who broke into our office
and planted a malicious device?

Collect Badge logs

Attack vectors:

- Tailgating
- Badge cloning
- Badge theft

https://www.defcon.org/images/defcon-22/dc-22-presentations/Smith-Perrymon/DEFCON-22-Smith-Perrymon-All-Your-Badges-Are-Belong-To-Us-UPDATED.pdf

Resulting Capabilities

Have we seen traffic to domain X?

Have we seen traffic to IP X?

What IP in my network is responsible for this traffic?

What machine did that IP resolve to?

Have we seen a particular process?

What resources did the attacker access?

Who physically broke in and planted a device?

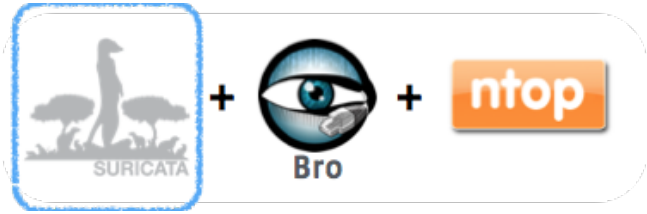
We’re evolving...

Network Security Monitoring (NSM)

a non-native stack

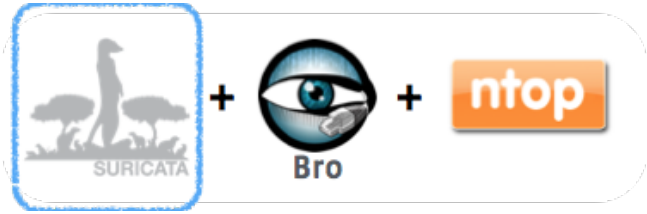
Our NSM for our Corporate (employee) network

Suricata



- Open source (http://suricata-ids.org/)
- Known for being detection-driven
  - Great for network signatures and IOCs
- Some protocol logging capabilities since v2.0

Suricata is detection-driven



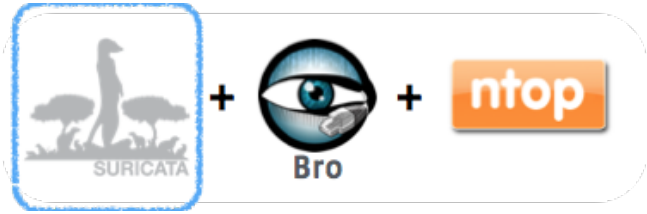
You can alert on anything in an

- HTTP request header
- HTTP request body
- HTTP response header
- HTTP response body

```
POST /update?product=windows HTTP/1.1
Accept: */*
X-Session: 0
X-Status: 0
X-Size: 61456
X-Sn: 1
User-Agent: Mozilla/4.0 (compatible; MSIE
6.0; Windows NT 5.1;SV1;
Host: update.alyac.org
Content-Length: 0
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: VisitorID=c2a4b456-e11e-4c37-88d8-
e770aa88058d&Exp=9/25/2014 6:14:17 AM
```

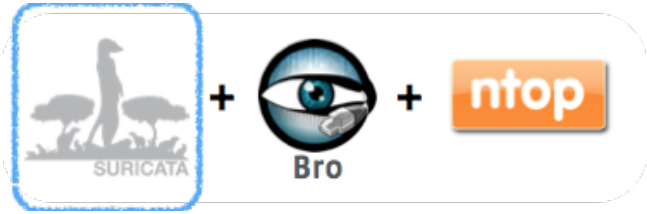
Note: HTTP is an example of one of the many available protocol dissectors

Ex: Detecting a CnC beacon




```
#
alert http $HOME_NET any -> $EXTERNAL_NET any
(
  msg:"ET TROJAN W32/BaneChant.APT Initial CnC Beacon";
  flow:established,to_server;
  content:"/adserv/logo.jpg"; fast_pattern:only; http_uri;
  content:"User-Agent|3A 20|Mozilla/4.0 (compatible|3B| MSIE 6.0|3B| Windows NT 5.1|3B| SV2)|0D 0A|"; http_header;
  reference:url,www.fireeye.com/blog/technical/<snip>.html;
  classtype:trojan-activity;
  sid:2016728;
  rev:2;
)
```

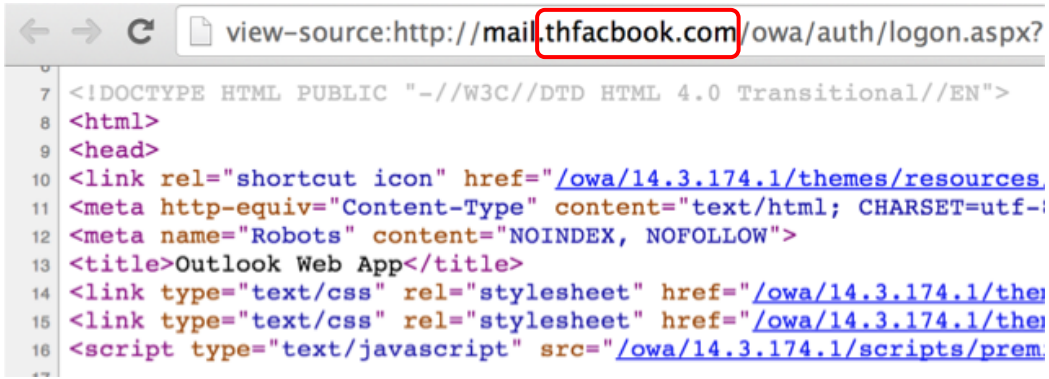
Ex: Detecting exfiltration




```
#
alert http $HOME_NET any -> $EXTERNAL_NET any
(
  msg:"ET TROJAN W32/BaneChant.APT Data Exfiltration POST to CnC";
  flow:established,to_server;
  content:"POST";
  http_method;
  content:"/adserv/get.php"; fast_pattern:only; http_uri;
  content:"User-Agent|3A 20|Mozilla/4.0 (compatible|3B| MSIE 6.0|3B| Windows NT 5.1|3B| SV2)|0D 0A|"; http_header;
  reference:url,www.fireeye.com/blog/technical/<snip>.html;
  classtype:trojan-activity;
  sid:2016727;
  rev:2;
)
```

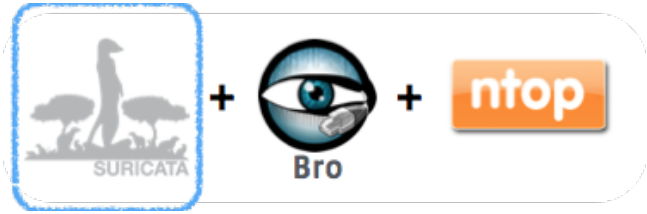
Ex: Thinking outside of the box

(catching an OWA phishing page)




```
alert ip any any -> any any
(
  msg:"Text 'Outlook Web App' (Gzip Deflated, title) detected in HTTP stream";
  flow:established,to_client;
  content:"Outlook Web App";
  http_server_body;
  sid:1601005; rev:1;
)
```

Scaling your intelligence



Daily Ruleset Update Summary 09/24/2014 EMERGING THREATS

[***] Summary: [***]

10 new Open rules, 17 new Pro (10 + 17). CVE-2014-6271 Bash Vuln, SolarWinds Storage Manager, AutoSMS.BF, Pushdo V3.

Thanks: Jake Warren and @jaimeblascob

[+++] Added rules: [+++]

Open:

2019226 – ET CURRENT_EVENTS DRIVEBY Nuclear EK 2013-3918 (current_events.rules)
2019227 – ET CURRENT_EVENTS Win32/Spy.Zbot.ACB SSL Cert Sept 24 2014 (current_events.rules)
2019228 – ET MALWARE Win32/SoftPulse.H Checkin (malware.rules)
2019229 – ET TROJAN Linux/Yangji.A Checkin (trojan.rules)
2019230 – ET TROJAN Possible Tinba DGA NXDOMAIN Responses (trojan.rules)
2019231 – ET WEB_SERVER Possible CVE-2014-6271 Attempt in URI (web_server.rules)
2019232 – ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers (web_server.rules)
2019233 – ET WEB_SERVER Possible CVE-2014-6271 Attempt in Client Body (web_server.rules)
2019234 – ET WEB_SERVER Possible CVE-2014-6271 Attempt in Client Body 2 (web_server.rules)
2019235 – ET TROJAN Pushdo v3 Checkin (trojan.rules)

Pro:

2808879 – ETPRO TROJAN Win32/Spy.Banker.AAHF Checkin (trojan.rules)
2808880 – ETPRO EXPLOIT SolarWinds Storage Manager Authentication Bypass (exploit.rules)
2808881 – ETPRO TROJAN Flooder.LYI Checkin (trojan.rules)
2808882 – ETPRO MOBILE_MALWARE Android.Trojan.AutoSMS.BF Checkin (mobile_malware.rules)
2808883 – ETPRO MOBILE_MALWARE Android.Trojan.AutoSMS.BF Checkin 2 (mobile_malware.rules)

Bro

- Open source (https://github.com/bro/bro)
- Framework for network logging and detection

Bro informs response

- We use Bro to create detailed logs for
  - **DHCP**
  - **DNS** (answers)
  - **HTTP** (URI, User-Agent, Content-Type, …)
  - **HTTPS** (certificate details)
  - **SSH** (banner)
  - **SMB**, IRC, ...

- Raw connection logs

Bro informs detection

- We use the ***Intelligence Framework*** (1) for domain alerting

- You can also alert on
  - IPs
  - URLs
  - File names and hashes
  - Certificate hashes
  - ...

(1) https://www.bro.org/sphinx-git/frameworks/intel.html

Example intel config


```
@load policy/frameworks/intel/seen
```

```
redef Intel::read_files += { "/somewhere/yourdata.txt" };
```

```
#fields indicator       indicator_type  meta.source     meta.desc
1.2.3.4 Intel::ADDR     source1 Sending phishing email  http://source1.
a.b.com Intel::DOMAIN   source2 Name used for data exfiltration -
```

ntop

- Developed PF_RING DNA
- Enables 0% CPU usage when moving packets from the network adapter to user-space
- Useful for Suricata and Bro on a 10Gbps link

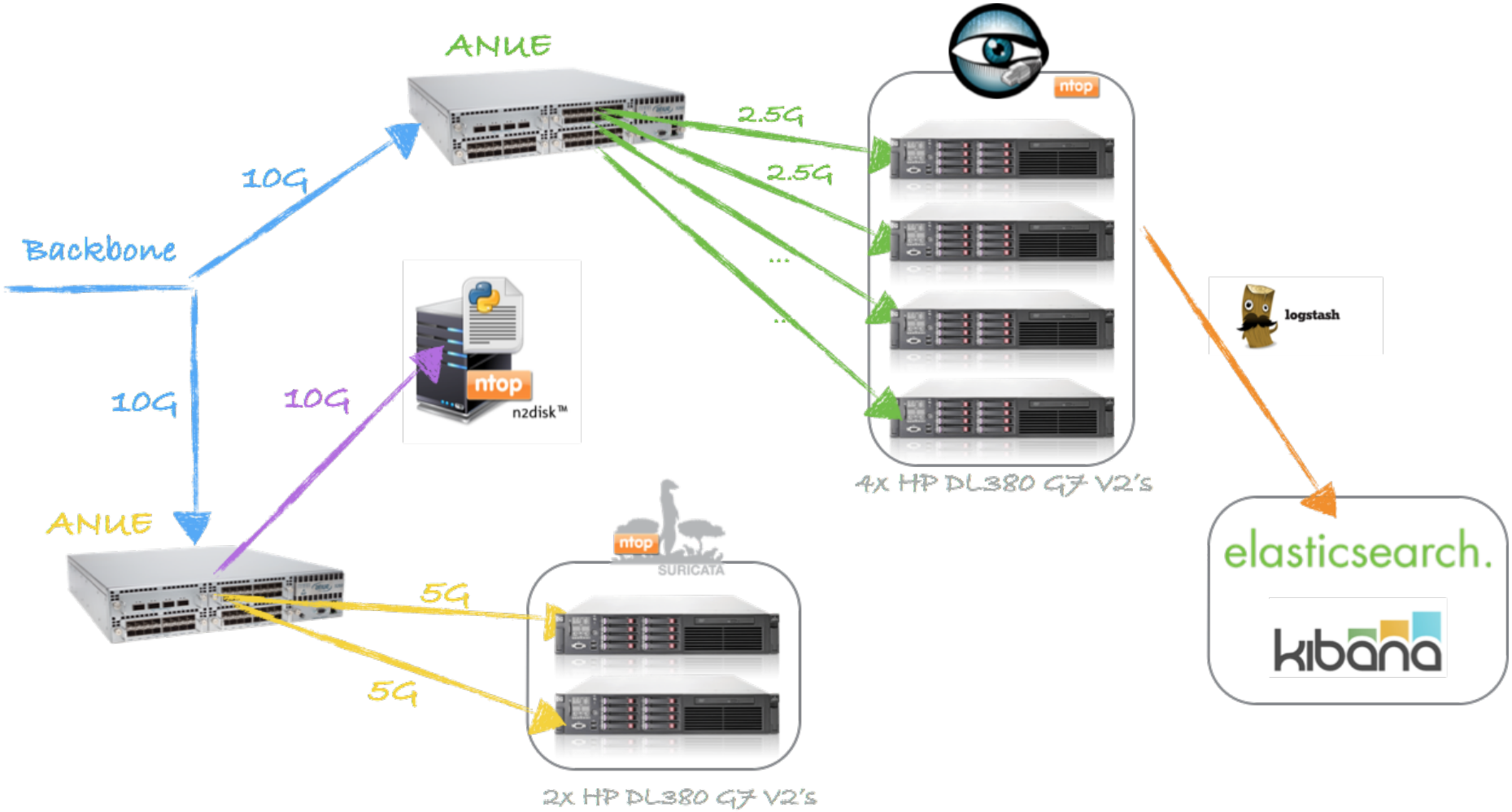
Note on ntop & bro

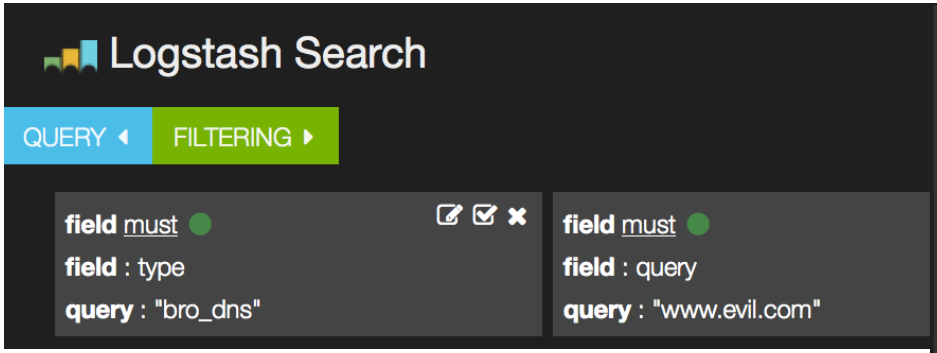
- PF_Ring DNA was not playing well with Bro
- We worked with the Bro team and a fix was committed upstream! (1)

(1) https://github.com/bro/broctl/commit/418f4cd535c4162a0b559e0a2bea99a6dfc3a9e4

Network Security Monitoring (NSM)

infrastructure and performance


ANUE
10G
Backbone
10G
10G
ANUE
2.5G
2.5G
...
..
ntop
n2disk™
4x HP DL380 G7 V2's
logstash
elasticsearch.
kibana
5G
5G
ntop
SURICATA
2x HP DL380 G7 V2's



id.orig_h		172.66.254.83
id.orig_p		63611
id.resp_h		204.232.231.46
id.resp_p		53
path		/usr/local/bro/logs/current/dns.log
proto		udp
qclass		1
qclass_name		C_INTERNET
qtype		1
qtype_name		A
query		www.evil.com

We're currently using a commercial datastore for Bro logs

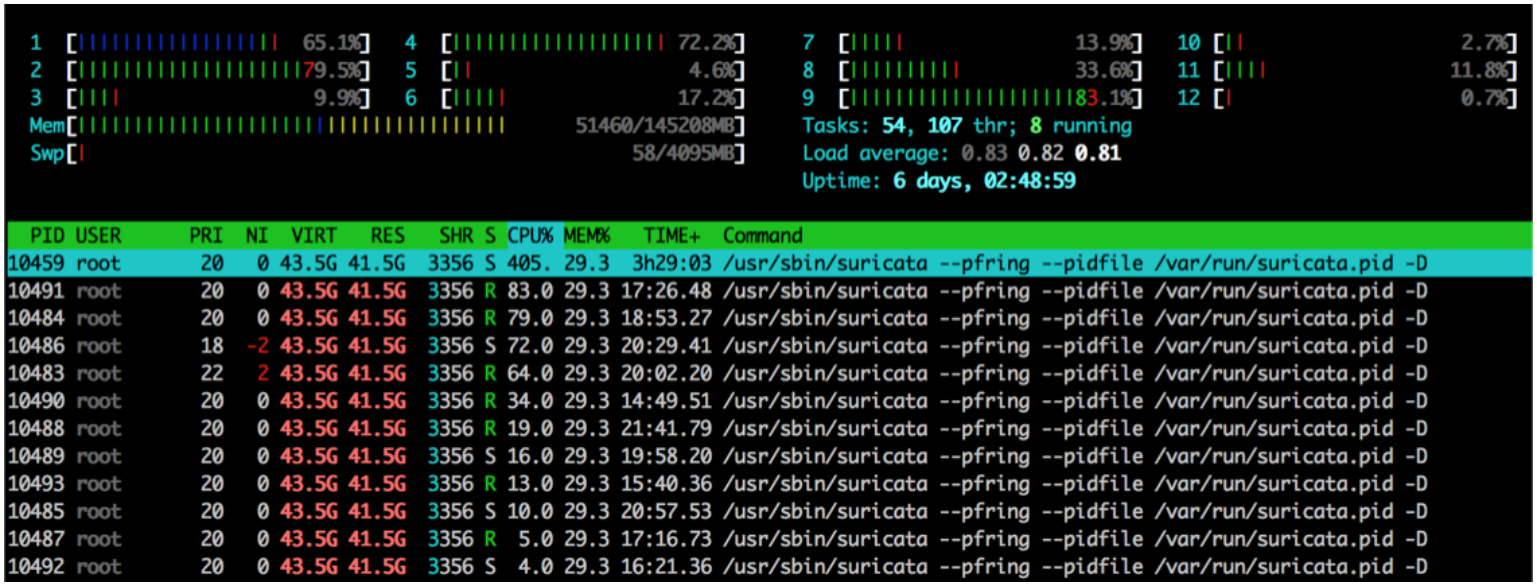
However, we're testing the ELK stack
(ElasticSearch(ES), Logstash, Kibana)
and we're finding that it performs beautifully.

4 hosts meet our scaling requirements

They have great deployment and production support:
http://www.elasticsearch.com/support/

elasticsearch.

kibana



~200k IPs

~21k Signatures

up to 5Gbps throughput

```
[BroControl] > netstats
worker-1-1: 1395266649.323261 recvd=0 dropped=0 link=0
worker-1-10: 1395266649.523218 recvd=820164569 dropped=0 link=820164569
worker-1-11: 1395266649.724149 recvd=845288997 dropped=0 link=845288997
worker-1-12: 1395266649.924162 recvd=816802857 dropped=0 link=816802857
worker-1-2: 1395266650.125102 recvd=749664073 dropped=0 link=749664073
worker-1-3: 1395266650.325134 recvd=743454781 dropped=0 link=743454781
worker-1-4: 1395266650.526182 recvd=922560492 dropped=0 link=922560492
worker-1-5: 1395266650.726161 recvd=778845182 dropped=0 link=778845182
worker-1-6: 1395266650.927157 recvd=657023129 dropped=0 link=657023129
worker-1-7: 1395266651.127302 recvd=768923551 dropped=0 link=768923551
worker-1-8: 1395266651.327221 recvd=716990695 dropped=0 link=716990695
worker-1-9: 1395266651.528271 recvd=732617517 dropped=0 link=732617517
```

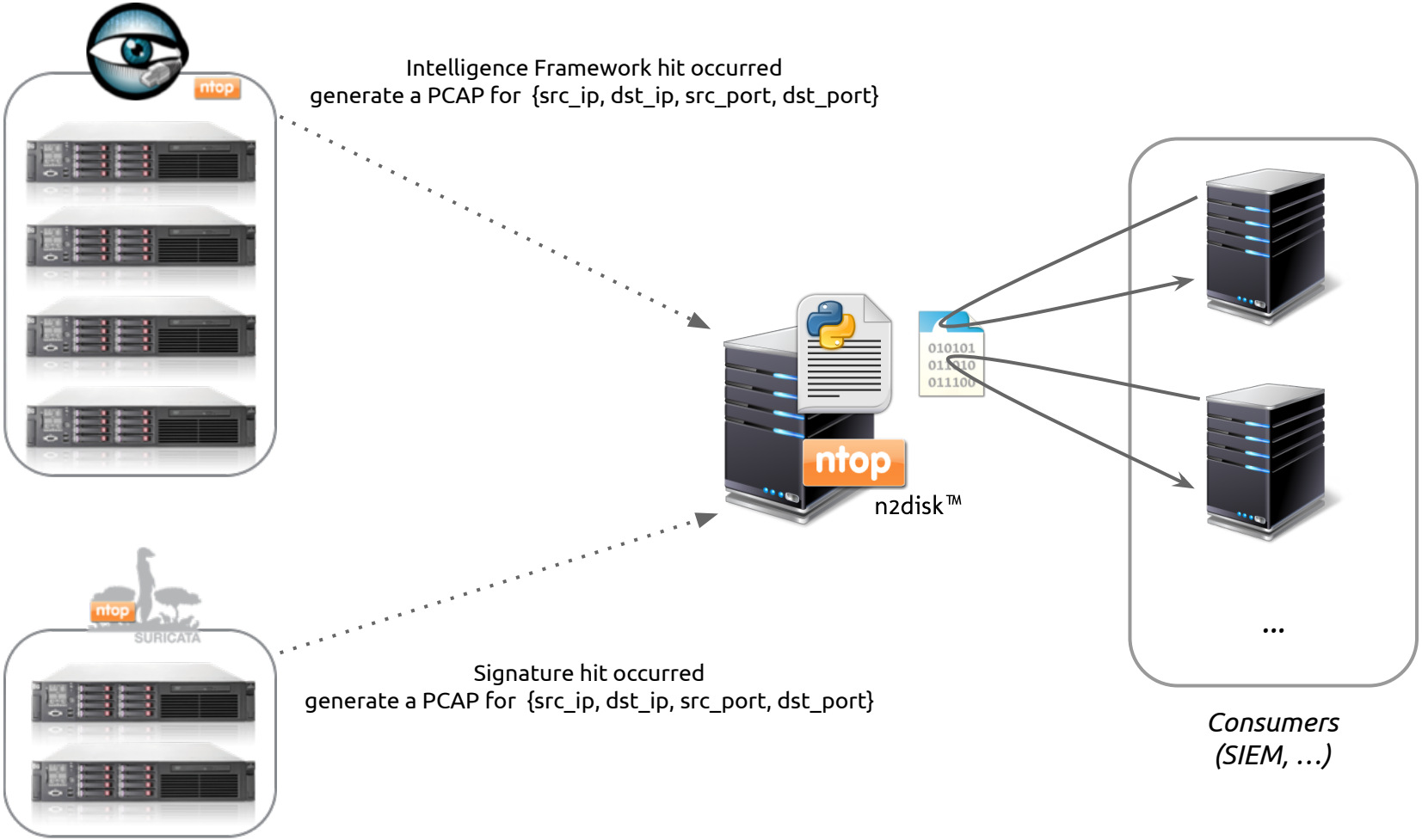
~0 packets dropped

~200k domains in Intelligence Framework

up to 2.5Gbps throughput

pcap-rpc service

- https://github.com/pcap-rpc
  - available by end of October
- A Python XML RPC service that wraps n2disk or TimeMachine
  - http://www.ntop.org/products/n2disk/ ($$)
  - https://github.com/bro/time-machine
- It allows any consumer (HIDS, NIDS, SIEM) to ask for a PCAP slice
- unified2 produces something similar, but is only for Suricata and Snort


Intelligence Framework hit occurred
generate a PCAP for {src_ip, dst_ip, src_port, dst_port}
ntop
ntop
n2disk™
010101
011010
011100
...
Signature hit occurred
generate a PCAP for {src_ip, dst_ip, src_port, dst_port}
ntop
SURICATA
Consumers
(SIEM, …)

We’re evolving...

Incident Response

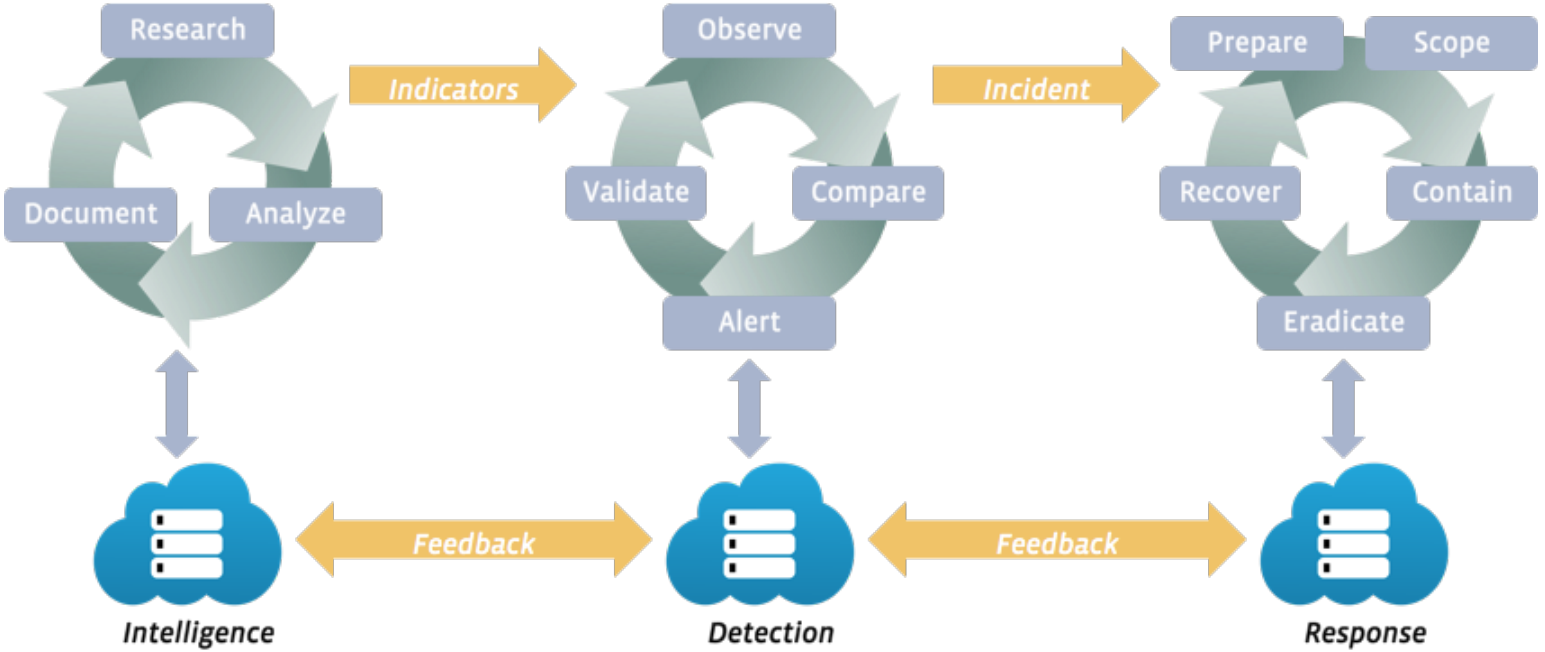
looking at the lifecycle

National Institute of
Standards and Technology
U.S. Department of Commerce

Special Publication 800-61
Revision 2

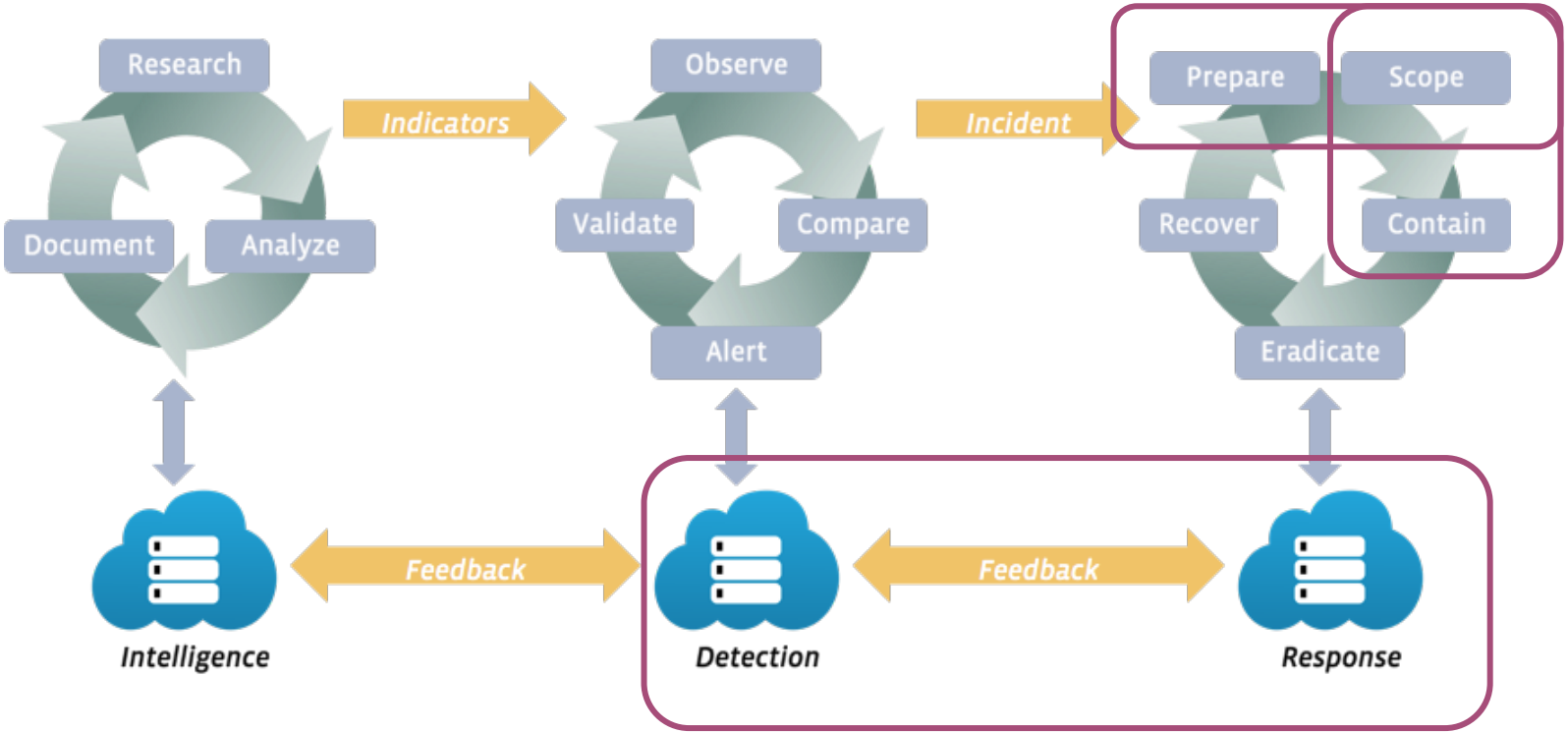
Computer Security Incident Handling Guide

IR Lifecycle



IR Lifecycle

Areas we'll be diving into



Prepare

Terminology

- An event is an observable occurrence on your network/systems
- The criticality of an adverse event determines if it is an incident
- Honoring this terminology in verbal or written dialogue is important
  - Failing to do so will result in confusion or assumptions
- When an event becomes an incident, you start to *Scope*

Communications

- We use an IRC server for out-of-band communications
- The server is not bound to a central authentication service
  - The central authentication service (KRB, LDAP, …) may be compromised
- The server runs on dedicated infrastructure
  - only accessible to incident responders
  - SSH requires local accounts using 2 factor-auth
- A bouncer is used for chat history / channel buffering

- The [IRC] server is <u>not</u> bound to a central authentication service
  - The central authentication service (KRB, LDAP, …) may be compromised

Our first redteam made us suffer for not honoring this

PROD Forensics Infrastructure

Goals:

Remote

- Remotely acquire and analyze forensic images
- Remote hands shouldn't be a requirement

Timely

- Fast read, write, and transfer speeds

Integrity

- Preserve the state of the machine

Secure

- Introduce as little additional risk as possible

Idempotent

- Achieve the same result, every time

One size fits all

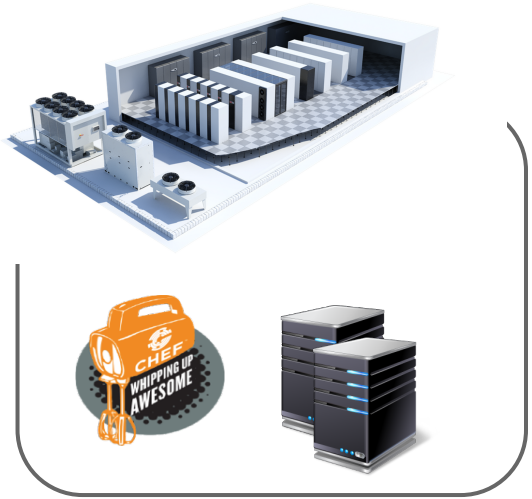
- Should work for any production Linux host

Open source

PROD Forensics Infrastructure

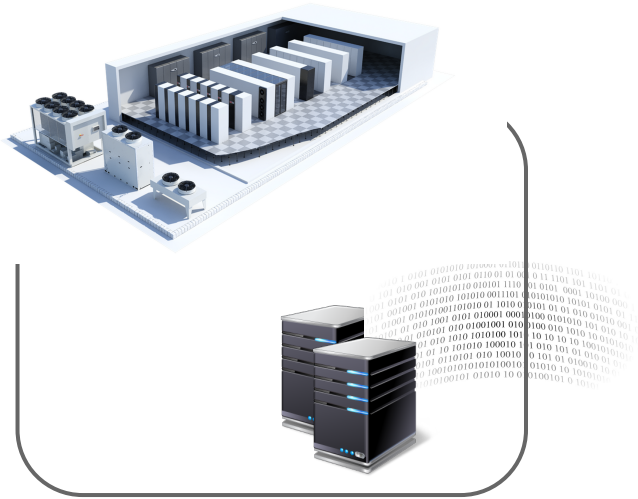
CPU	Intel, 6-8 Cores
HDD	30-36TB (12-16 disks in RAID 6 with XFS filesystem)
RAM	48-64GB
NIC	10G

PROD Forensics Infrastructure



- 2 forensic hosts in each datacenter (dc)
  - Area of compromise determines which dc is used
- Chef lets us spin up new, pre-configured forensic hosts when we need them
  - Sleuthkit, LiME, Volatility, Plaso, bulk_extractor, etc are easily accessible

PROD Forensics Infrastructure



Disk throughput and latency on 10G link:

- 4.5 hours to transfer a 1TB root partition
- 2.6 hrs with SSH compression!

CORP Forensics

CORP Forensics

Use evidence bags for compromised devices

(prepare for multiple compromised devices)

CORP Forensics

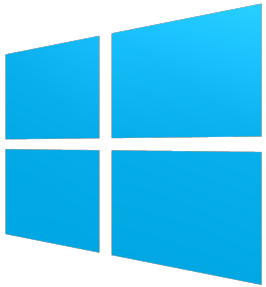
Use a safe to store physical, original evidence

Safes:

- reduce the likelihood of device damage
- are fire-proof up to a given temperature
- help with chain-of-custody

CORP Forensics Infrastructure

We have dedicated forensics examiners
in our large offices (HQ, remote)



F-Response
X-Ways
Autopsy

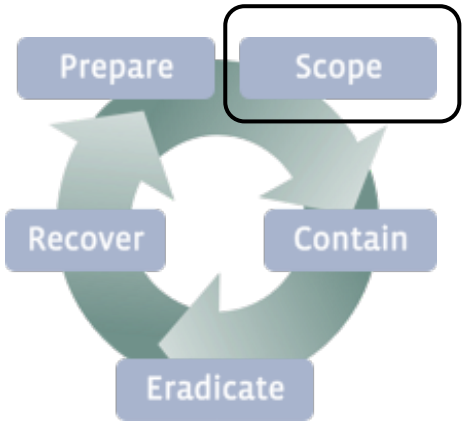
F-Response
Macquisition
Blacklight

Sift3

CORP Forensics Infrastructure

A NAS (network attached storage) is used
for long-term storage of forensic images.

Examiners use a *working-copy* of the original



Scope

Scope

- Do not touch attacker infrastructure!
  - dns queries
  - scanning (ports, services, …)
  - wget/curl'ing
  - sandboxing malware with internet

- Do not touch your compromised assets

- Gain insight from your existing logs
  (host, network, email, …) before taking any actions

practice good opsec!

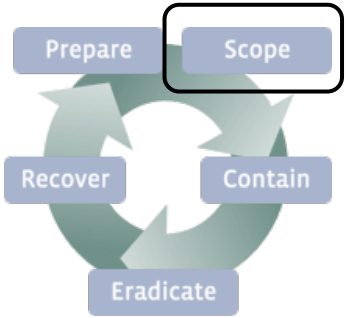
“There is no exception to the rule… that every rule has an exception”

- *James Thurber*

active exfiltration

(to containment)

Scope



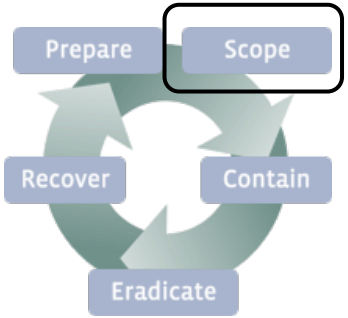
- Notify relevant internal stakeholders

  CISO, PR, Legal, …

- Perform OSINT (open source intelligence) on initial IOCs
  - WHOIS
  - Passive DNS
  - VirusTotal (no uploads)
  - Google

Depending on your risk tolerance, you may want to do this on a non-attributable network

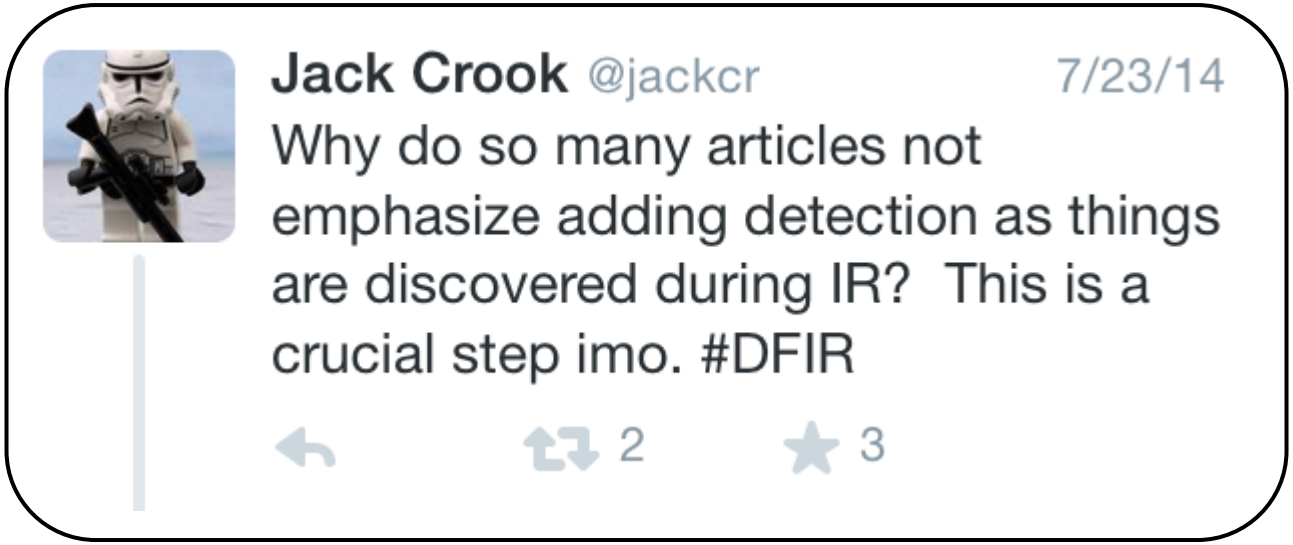
Scope



- Document initial IOCs (indicators of compromise)
  - File name, file hash, domain, IP, …
- Document secondary IOCs identified from OSINT
- Add IOCs to your IDS (intrusion detection systems) to identify current and soon-to-be compromised assets

No blocking actions yet (IPS)

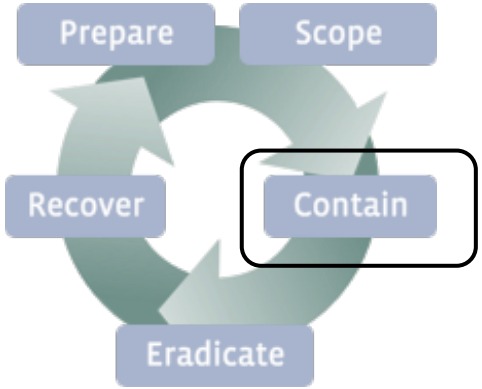
- Search your logs for these IOCs to identify additional compromised hosts
- Build a timeline (attack vector, lateral movement, …)



Chasing down IOCs may lead to additional IOCs or compromised assets.

Ensure there is a continuous feedback loop that is having every IOC searched-for and utilized in your IDS'

Don’t forget to triage alerts during an incident



Contain

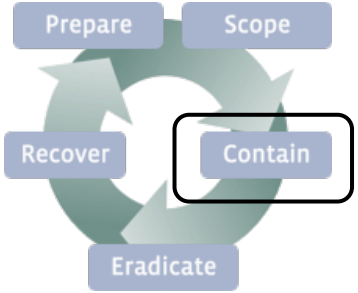

Avoid this

Containment

Sean Mason @SeanAMason 2d

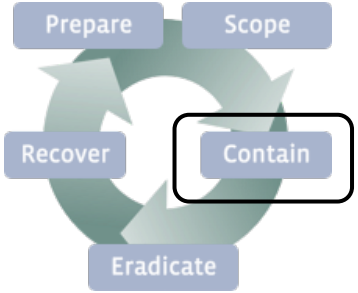
@jackcr Fair enough. My pet peeve is the lack of thinking through containment ahead of time. It's not simple and always seems glossed over.

Containment



- You want to try and contain all compromised assets <u>at the same time</u>
    - Failure to do so may result in the attacker pivoting (whack-a-mole)
    - This is why the *Scoping* phase is so important

Containment

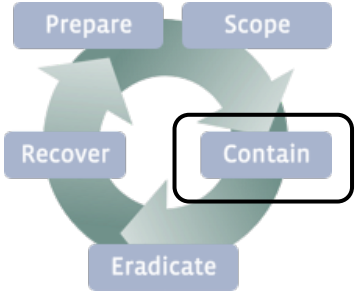


How you contain an asset depends on its:

- **Network requirements**
  - RFC1918 and/or internet egress?
- **Availability requirements**
  - 24/7 or what level of down-time is ok?
- **Business criticality**
  - User impact, revenue, …
- **Locale**
  - Corporate or Production environment?
  - HQ or remote office?

WiFi Network ACLs

(one of many containment options)

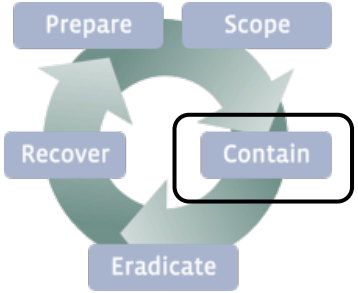


Before we discuss how we can use WiFi network ACLs for containment, lets quickly go over how our WiFi authentication works:

- Client authenticates to a wireless controller via EAP-TLS
- After certificate validation, the username is pulled from the certificate and used to look up AD group memberships via LDAP
- Based on group memberships, the RADIUS server assigns the client a Role
- The Role is returned to the wireless controller, which applies the ACLs associated with that Role

WiFi Network ACLs

(one of many containment options)



Create 2 new ROLES (ACLs) and distribute to Controllers

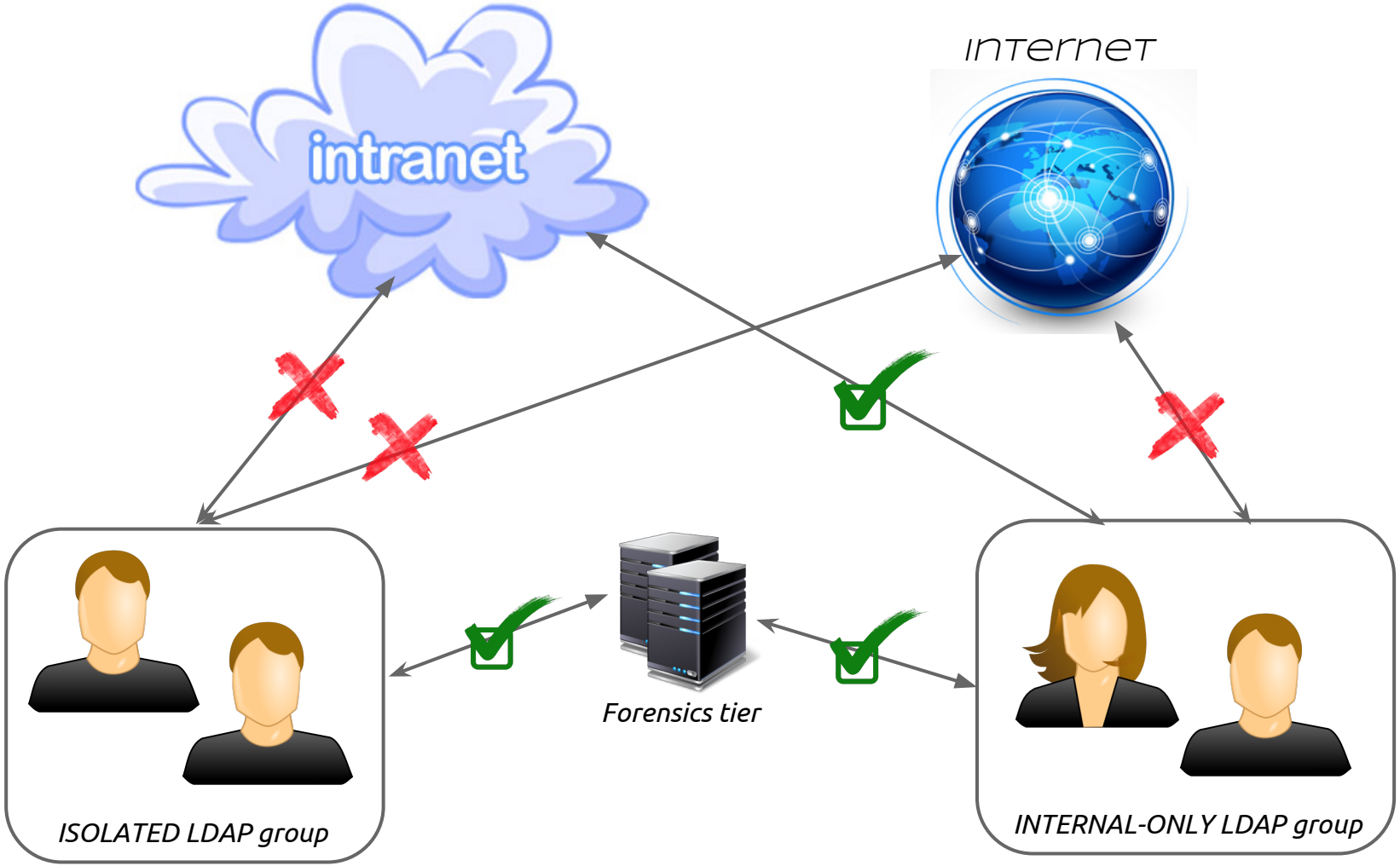
"**ISOLATED**"

- Only allows network communications to the forensics tier
- Prevents the asset from talking to anything else

"**INTERNAL-ONLY**"

- Only allows intranet network communications
  - This includes the forensics tier
- Internet egress is blocked

Associate an LDAP group to each ROLE

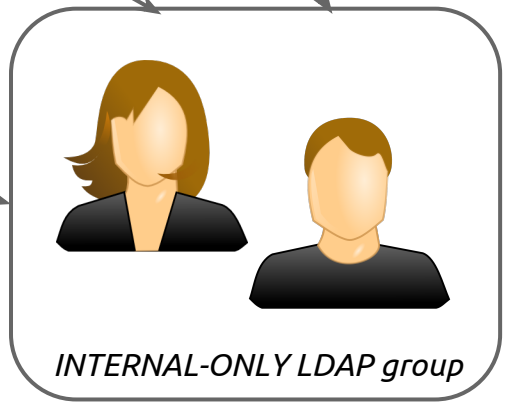

intranet
Internet
Forensics tier
ISOLATED LDAP group
INTERNAL-ONLY LDAP group

This is useful for blocking command-and-control (CnC/C2) communications

while

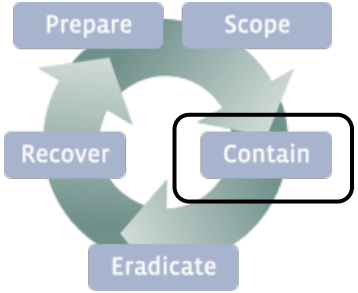
reducing employee friction

Forensics tier



* Which ROLE you use depends on incident severity and your company culture.

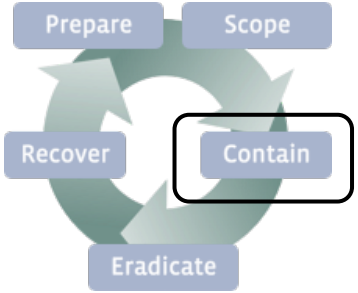
Sinkhole via DNS Zones



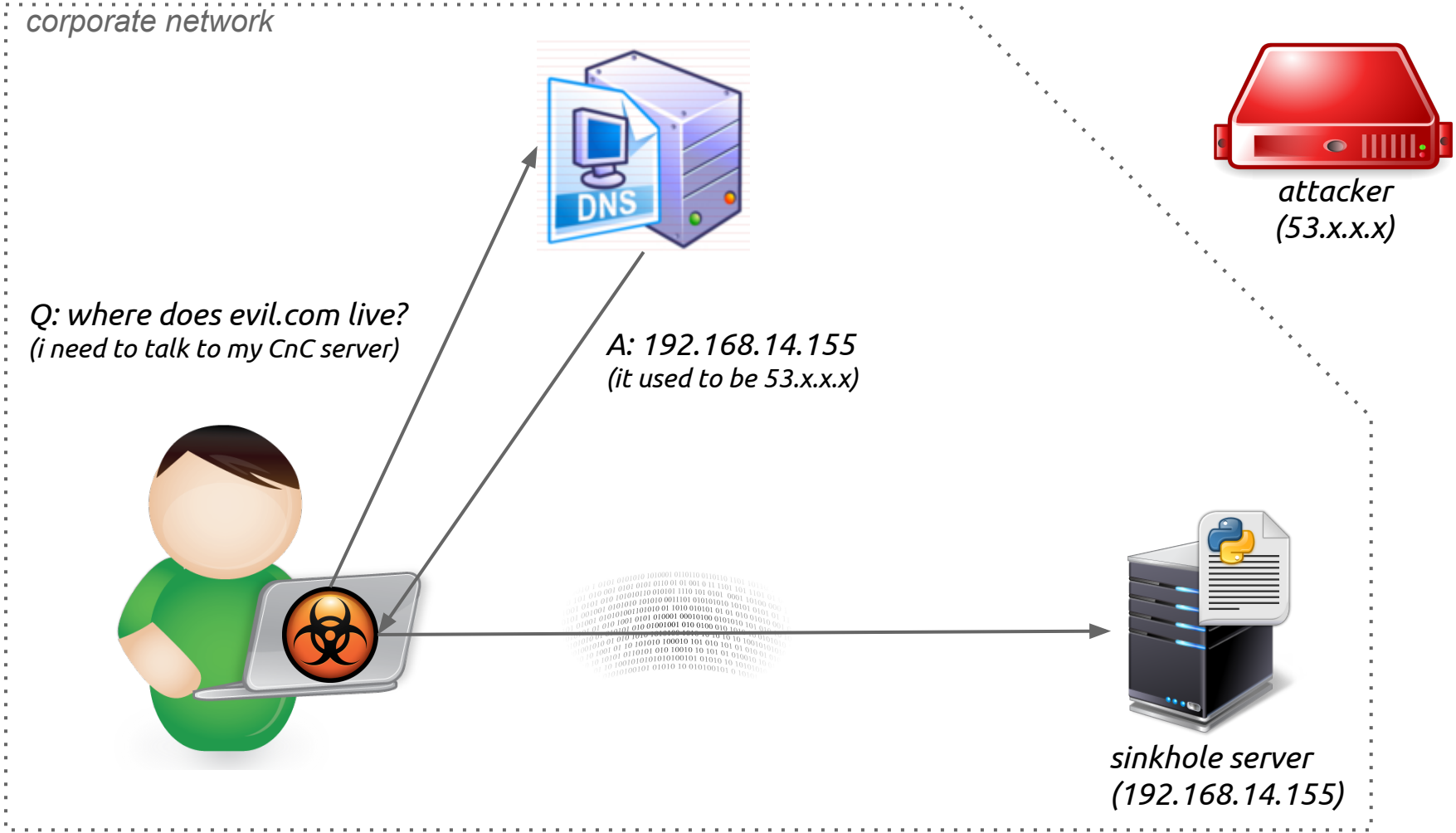
- Build 2 servers, each with a dedicated IP
  - *CRITICAL* - One for security incidents
  - *CATCH-ALL* - Another for everything-else

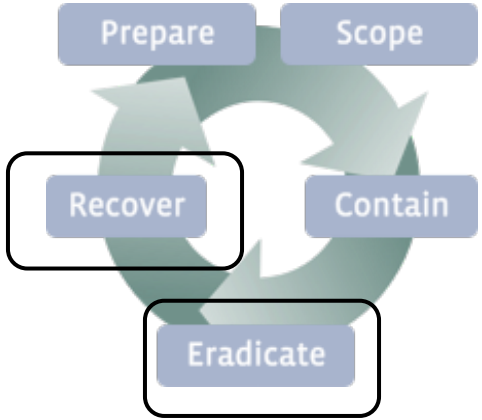
- When you want to block a domain on your network,
  add a forward-lookup DNS zone on your
  primary DNS server to point to the IP of CRITICAL or CATCH-ALL

Sinkhole Logging



- https://github.com/sinkhole-logger/
  - available by end of October
- It’s a python service that utilizes libpcap and scapy
- Features
  - completes TCP 3-way handshakes
  - logs all TCP and UDP connections (configurable)
  - produces detailed logs for http, https, irc, and ssh (configurable)
- Developed by our intern, Mitchell Grenier (@jedi22)


corporate network
DNS
attacker
(53.x.x.x)
Q: where does evil.com live?
(i need to talk to my CnC server)
A: 192.168.14.155
(it used to be 53.x.x.x)
sinkhole server
(192.168.14.155)



Eradicate & Recover

(maybe another time...)

New open-source product coming October 29th
(stay tuned!)

https://github.com/facebook

Questions?

(mimeframe@fb.com)

Appendix

Redteam
- http://en.wikipedia.org/wiki/Red_team

Sinkhole Logger:
- https://github.com/sinkhole-logger

PCAP-slice RPC service:
- https://github.com/pcap-rpc

NIST Incident Handling Guide
- http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

Our page
- https://www.facebook.com/protectthegraph


PROTECT
THE GRAPH