SAND2018-5977C

From Identification to Automated Response – Threat Profiling, Investigation and Mitigation in Today's Landscape

6 June 2018

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

#whoami

- Mike

Sandia National Laboratories

#whoami

- John

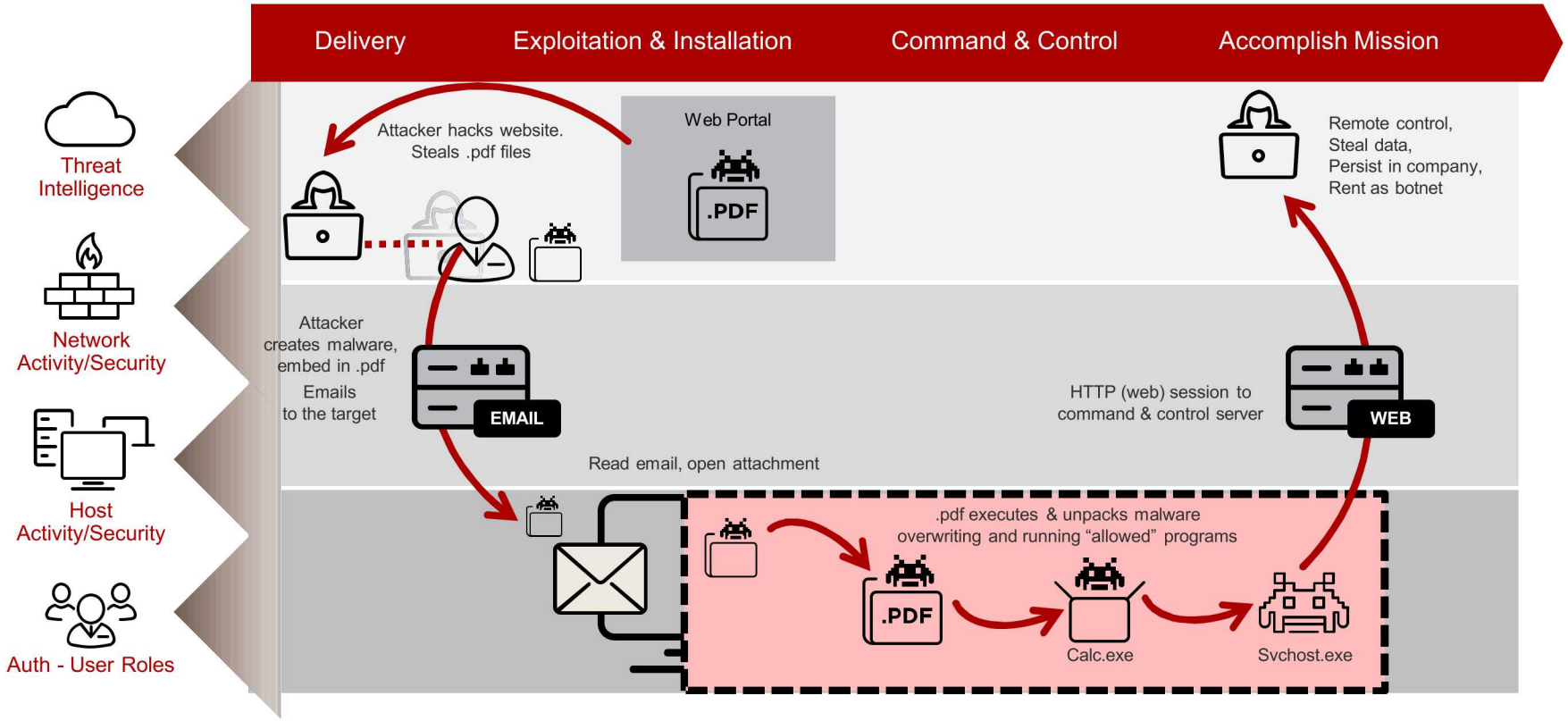
Sandia National Laboratories

Sandia National Laboratories

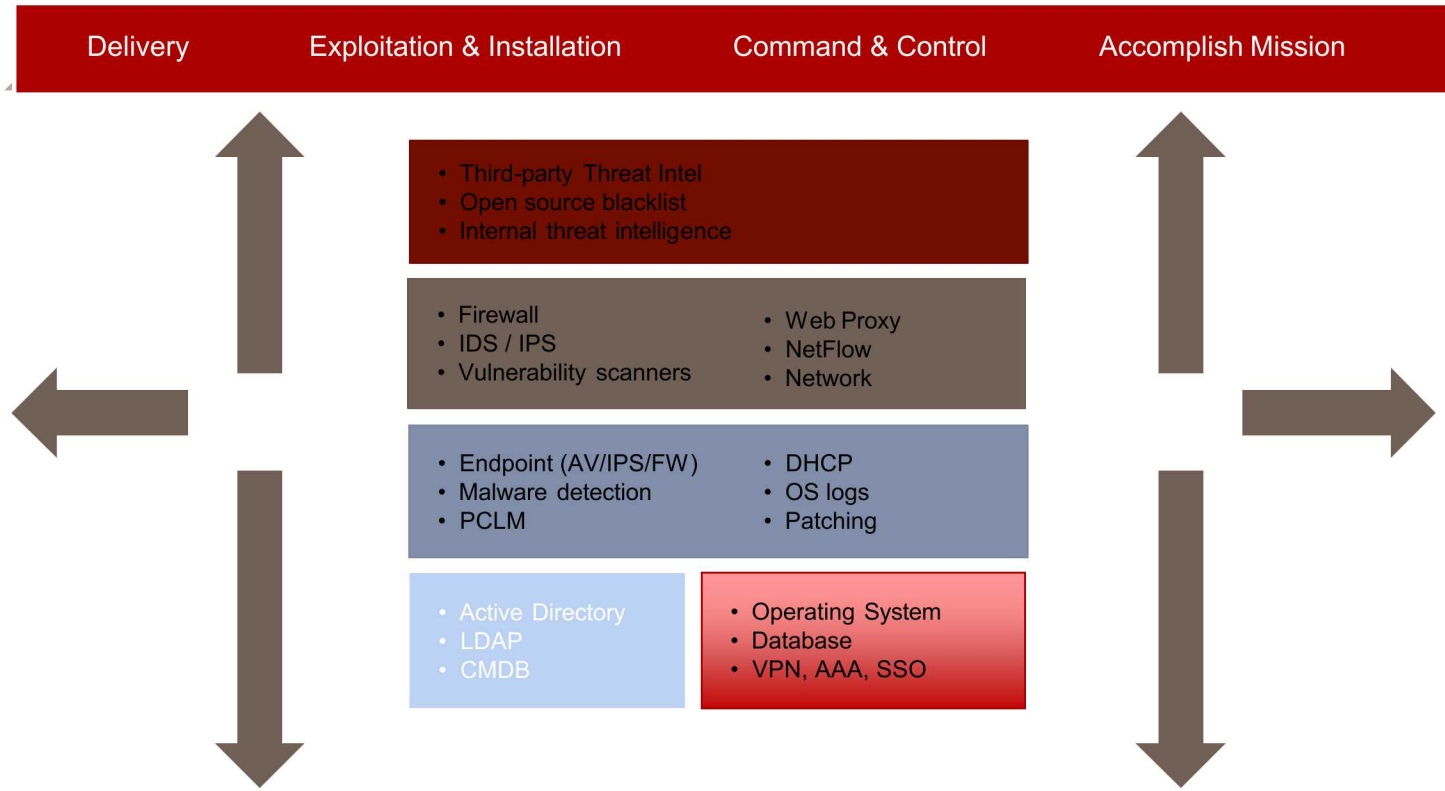
Threat hunters focus their search on adversaries...and who are already within the networks and systems of the threat hunters' organization"

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

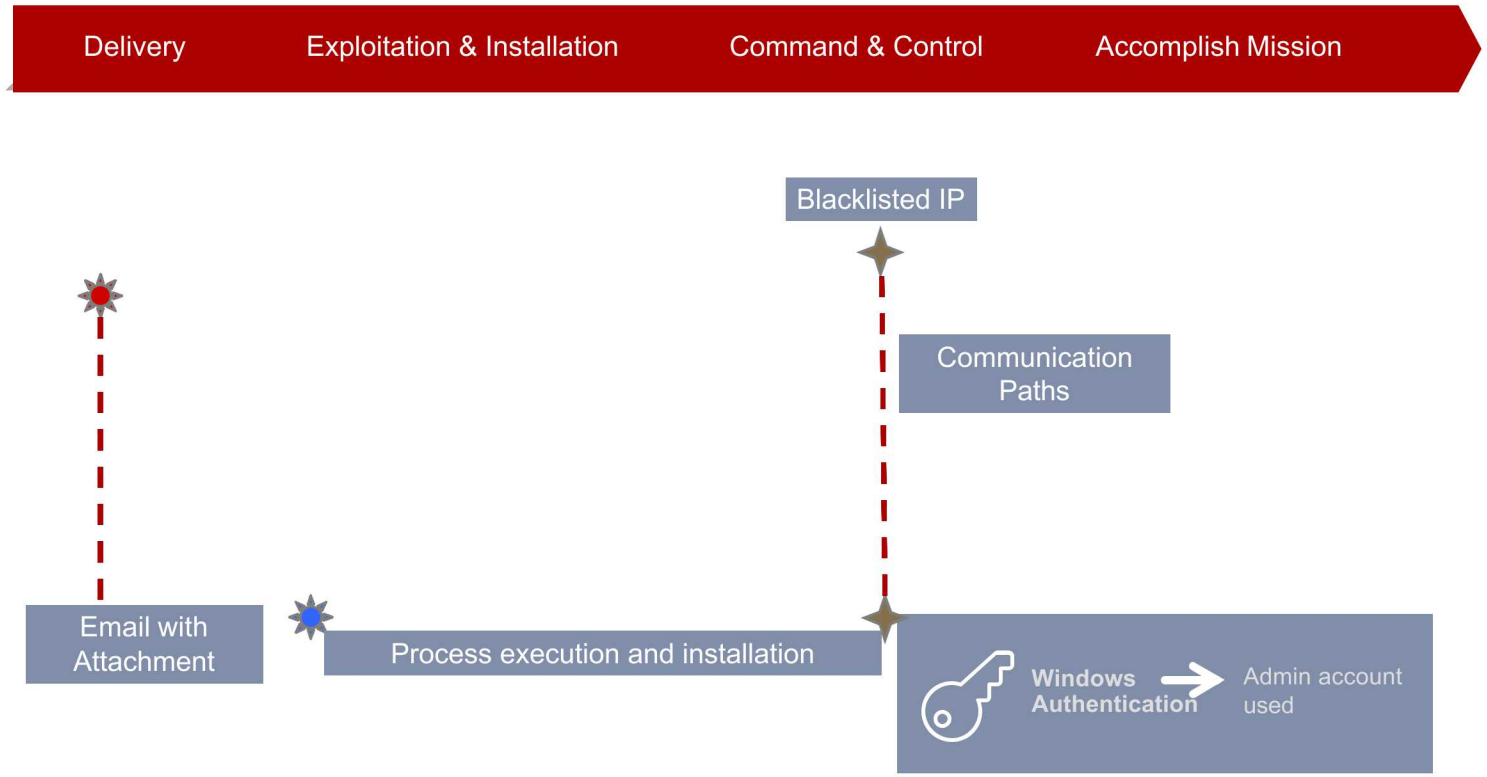
Example of an Advanced Threat



Data Sources Needed



Insights from Events Collected



Threat Hunting and Incident Response

Sandia National Laboratories

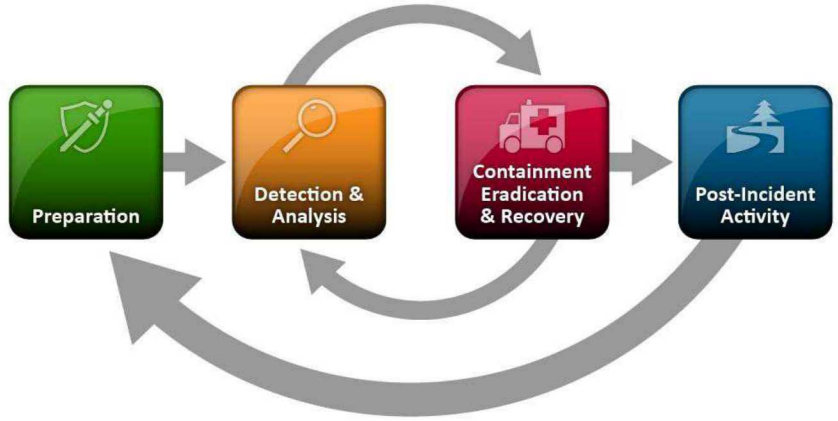
Threat Hunting

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 long
- Focus on containment and recovery
- Work with other teams to eradicate

- Hunting can still be performed!!!



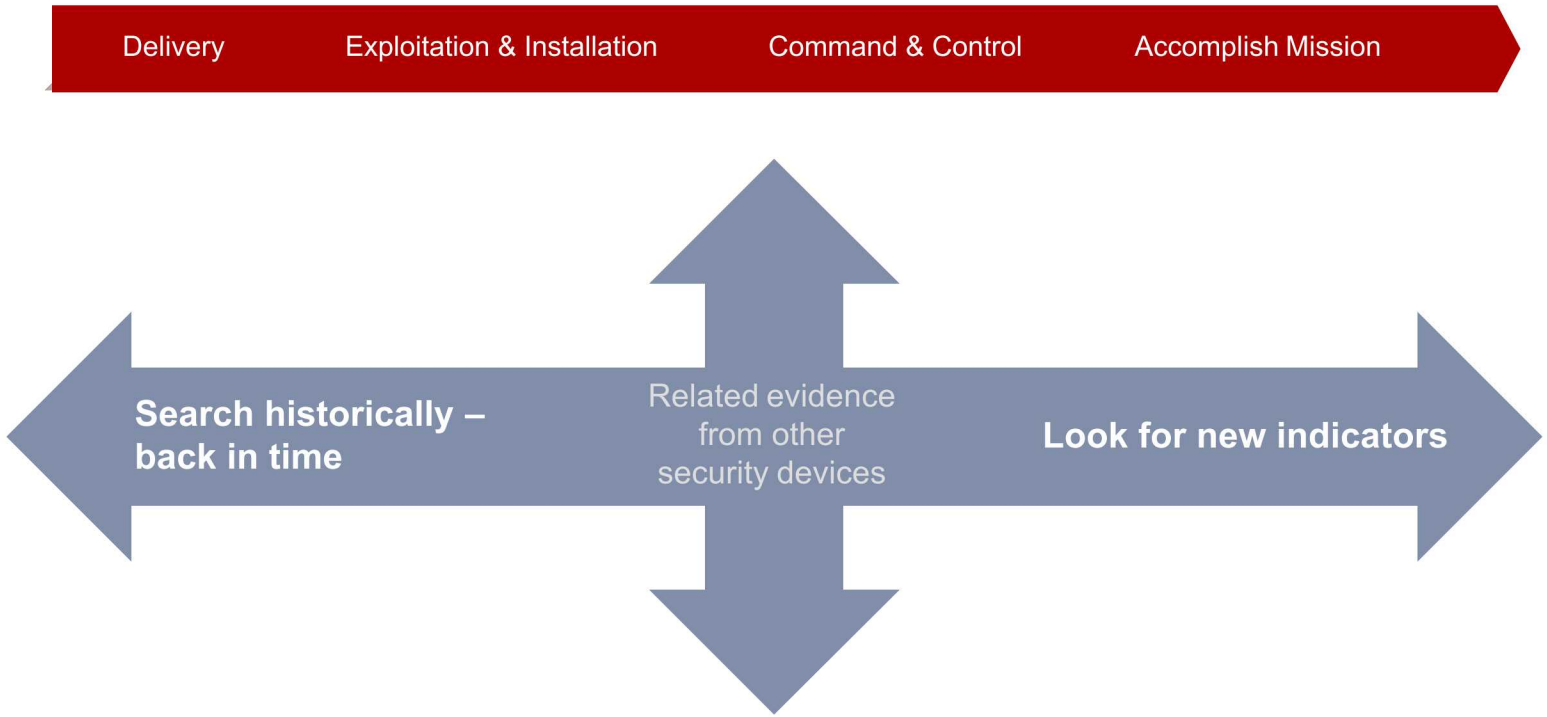
NIST SP800-61

Why Do We Hunt?

Sandia National Laboratories

Hunting Occurs In The Past and Present

Sandia National Laboratories



Sandia National Laboratories

"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

Where to start?

Lead Development

Think about taking an indicator and pulling on the string

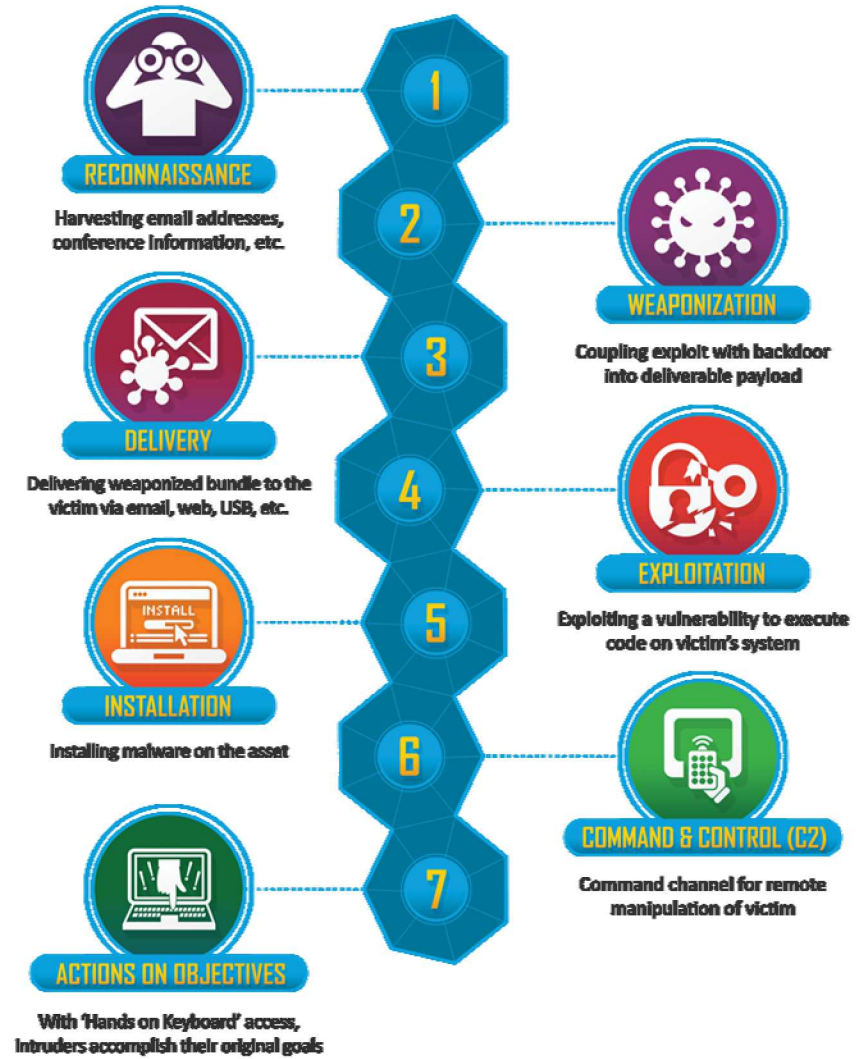
Brainstorming

- Past Performance May Not Be Indicative Of Future Results, but Previous Security Events/Incidents May Be Used To Identify Trends
  - Have past attackers commonly used spearphishing for delivery?
  - Did you read about SSL Certificates being a technique to identify attacker infrastructure?
- Activities considered to be out of the norm
    - Data Volumes, Directionality, Destinations, Sources, Apps, Time
- Testing Results
  - Why are adversary teams targeting systems?
  - If internal teams are targeting, maybe adversaries are too!

Lockheed Martin Kill Chain

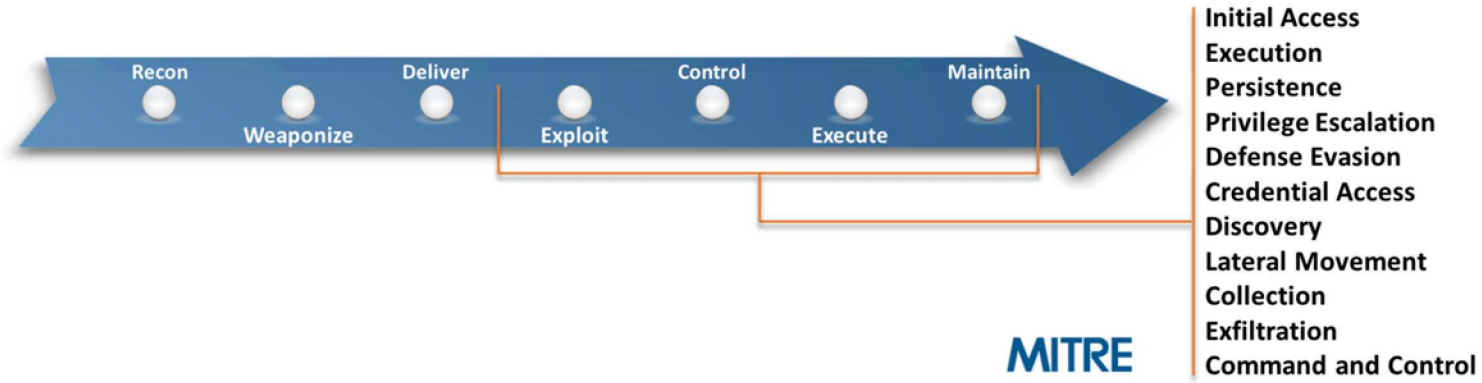
Sandia National Laboratories

- 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



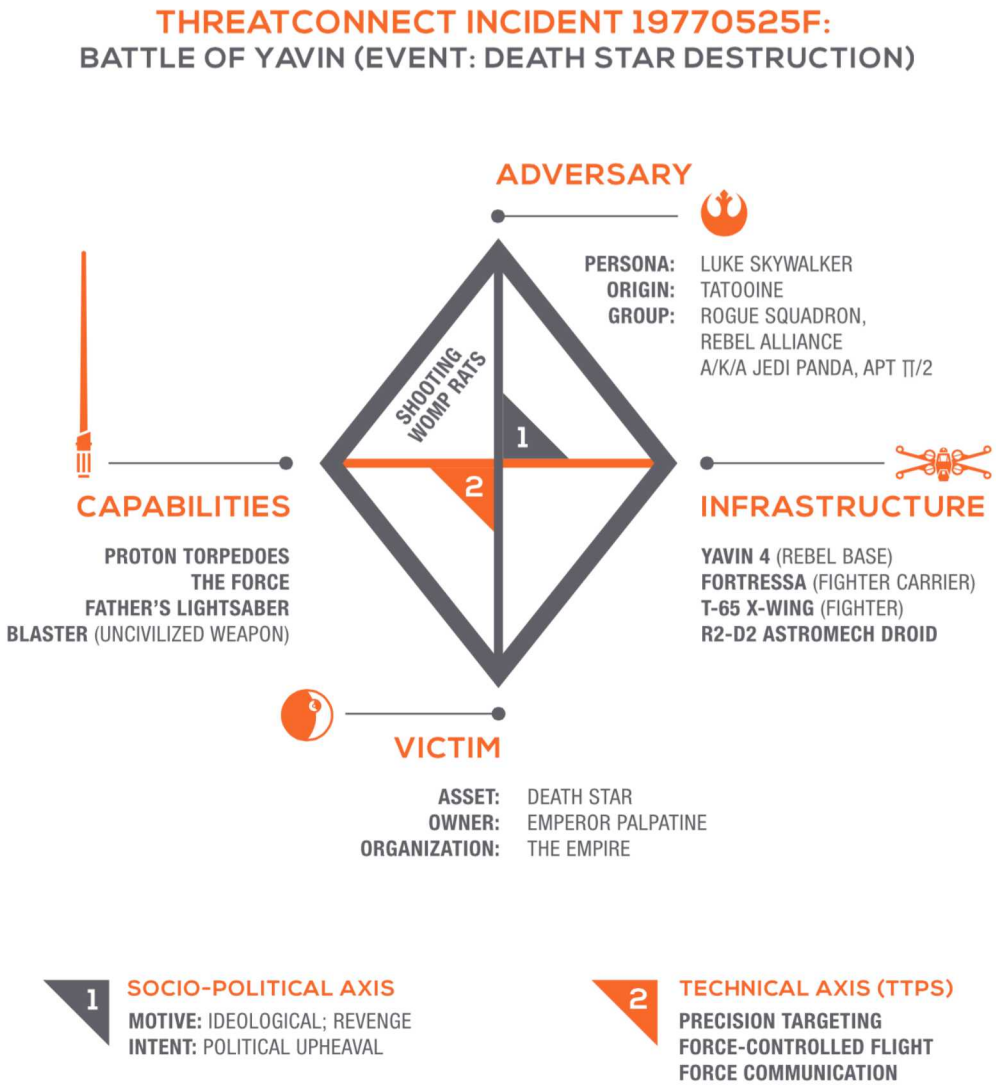
MITRE ATT&CK

- 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

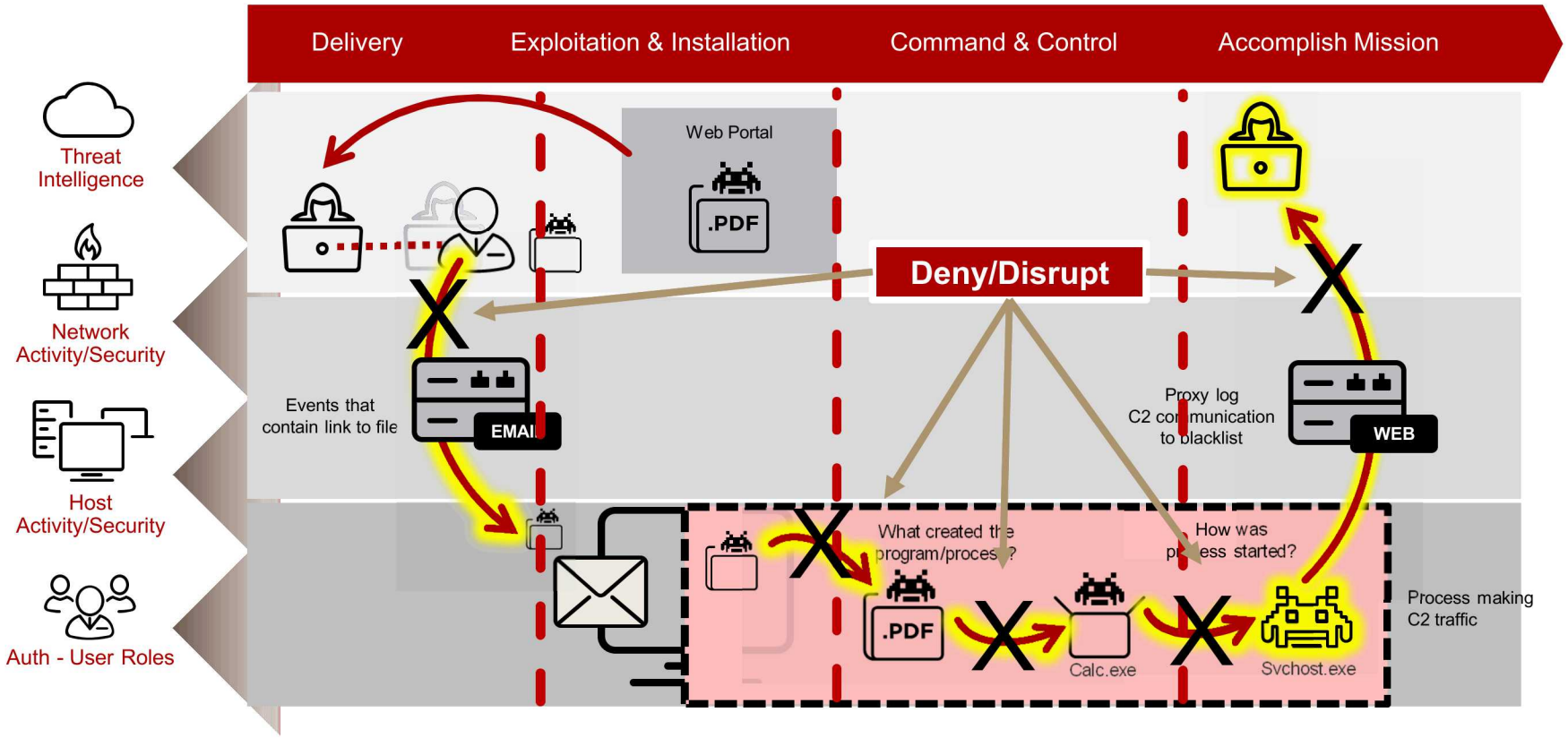


Diamond Model

- 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/



What Are We Trying To Accomplish?



How to detect bad people doing bad things

Sandia National Laboratories

- Current Methods
  - 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

How we should detect bad people doing bad things

Sandia National Laboratories

- Think more like attackers
- Embrace automation
- Train your tools to detect actions threat actors do, instead of looking for IOC's
- Validate your tools
- Encourage information sharing
- Don't punish the good guys

Why we do adversary emulation

Sandia National Laboratories

- Train the tools
- Test the tools
- Profile our attackers
- Enrich our data
- Extrapolate our data to fill in missing gaps
- Scope the threat landscape

Profiling your Attacker

Sandia National Laboratories

- Collect Data
  - Threat Reports
  - Conferences
  - Twitter
  - Blogs
  - Malware Activity
  - Information Sharing
  - CVE’s
  - Incident Response and Forensics
- Enrich your data
  - Building target environments
  - Building sample attacks based on threat actor actions
  - Correlate events to activities and actors

Enablers for APT3 Emulation

Sandia National Laboratories

- 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

Attack Walkthrough

Sandia National Laboratories

Summary: An attacker sets up a malicious webserver and a victim browses to the website. The website allows the attacker to take the control of the victim and gain access to other machines on the network.

Attack Emulation - Demo

Attack Emulation

Sandia National Laboratories

Detailed Attack Flow:

- The attacker uses Metasploit to stage an attack on a webserver
- The webserver hosts an exploit for Adobe Flash discovered by HackingTeam (CVE-2015-5119)
- When the exploit is successful, a beacon phones home to the attacker
- The victim browses to the website and the attacker silently takes control of their machine.
- The attacker migrates to an x64 process (explorer.exe) and gains system level privileges
- The attacker uploads kiwi and steals passwords from memory
- The attacker uploads met.exe a binary that will phone home when ran
- The attacker uploads two batch scripts and runs them
  - (persistence.bat) Which creates a backdoor scheduled task that runs at boot
  - (collect.bat) Which creates a list of .txt files on the machine and a list of running processes
- The attacker then uses credentials stolen from memory with kiwi to launch psexec to spread to other machines in the environment.
- The attacker repeats the post exploitation steps on the newly compromised machine

Leveraging Emulation to Enhance Detection

Sandia National Laboratories

- By building a variety of attacks and attack environments we are able to:
  - Fine tune tools
  - Evaluate our tools
  - Expect more than IOC's
  - Ability to develop new IOC's
  - Detect technique usage

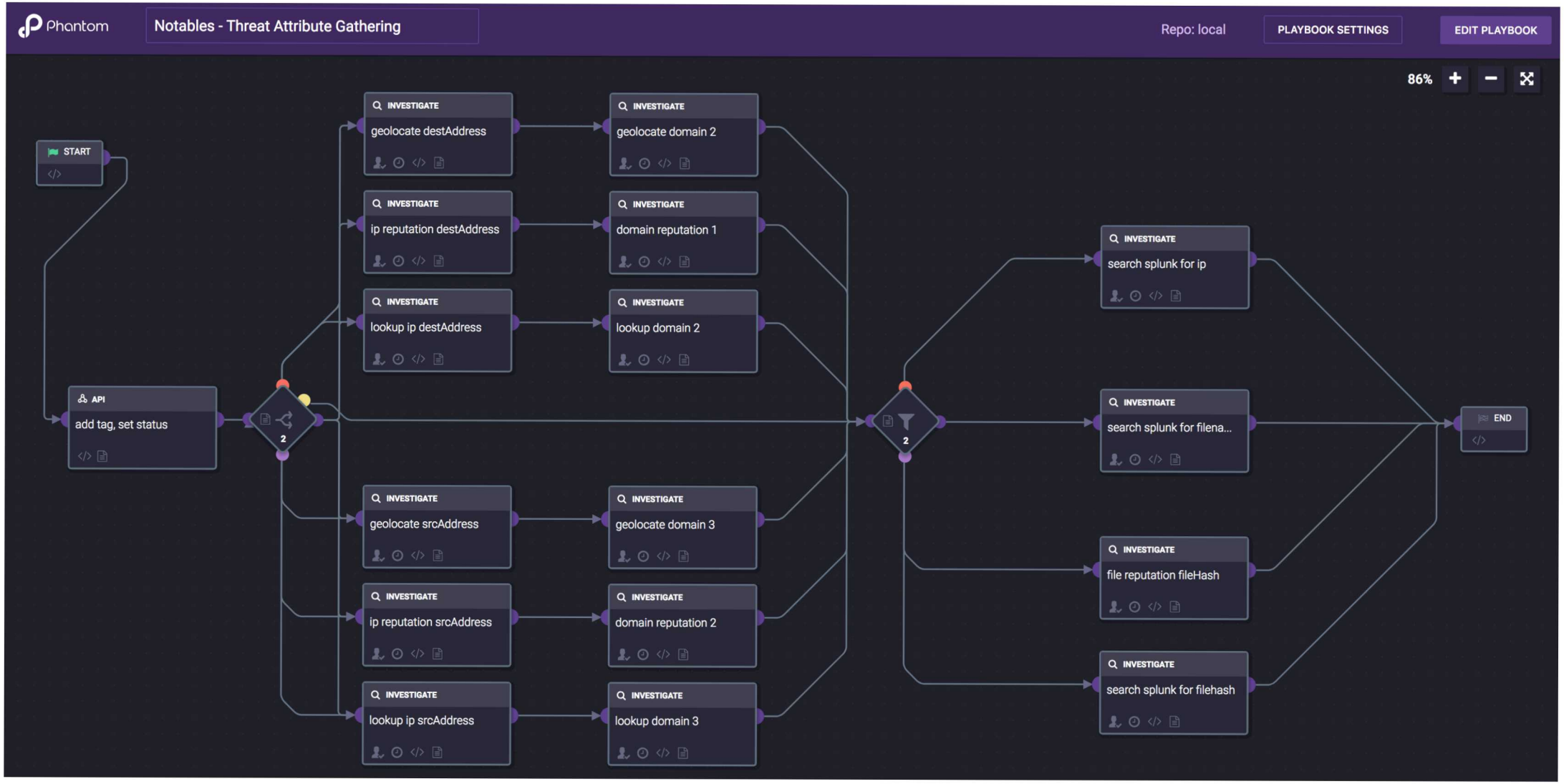
Automation Goals

Sandia National Laboratories

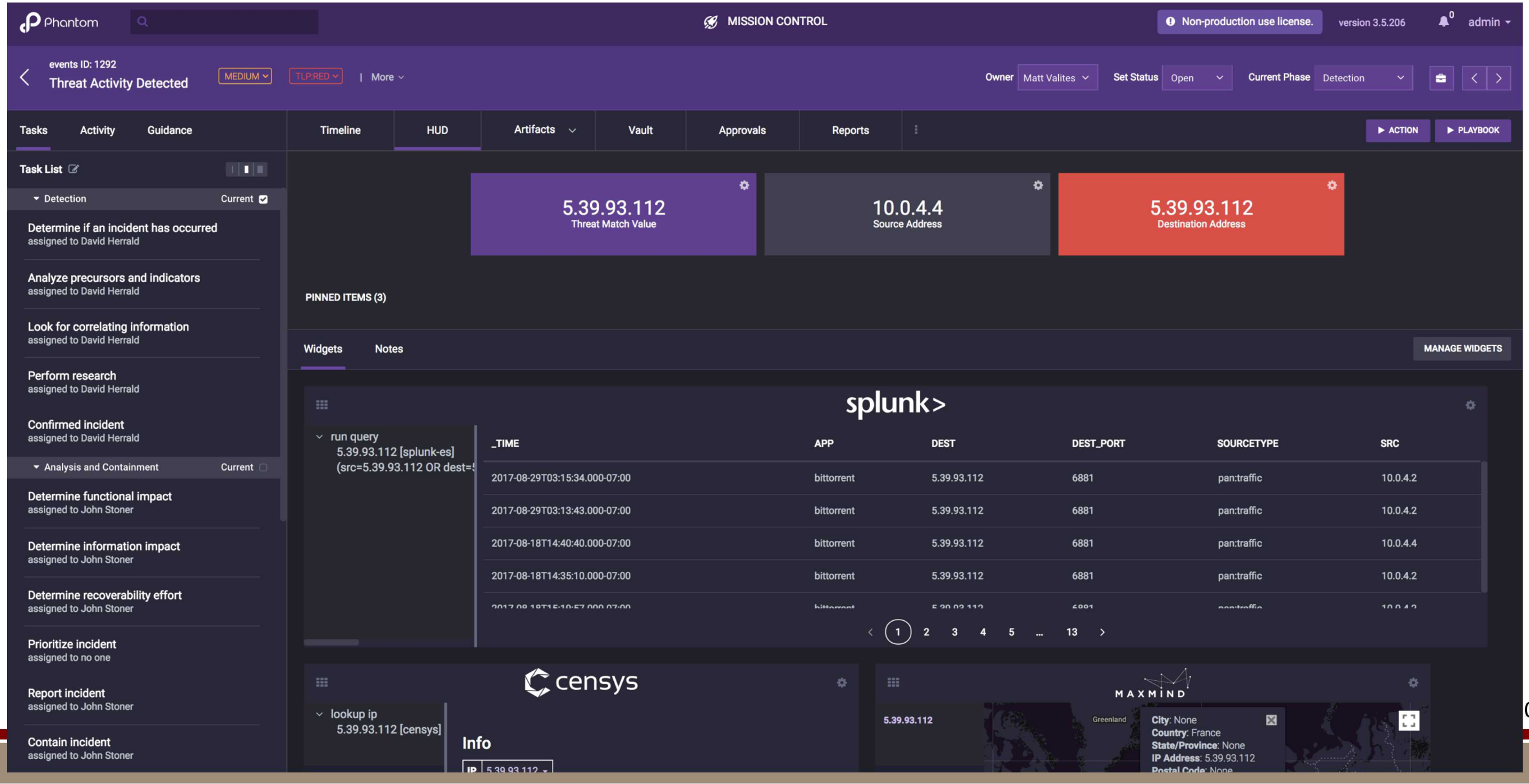
- Minimally
  - Detection
  - Containment
  - Fixing the issue
- Ideally
  - Active Defenses
  - Deception
  - Forensic Collection
  - IOC development
  - Information Sharing
  - Closing the hole elsewhere

Automating Threat Intel Gathering

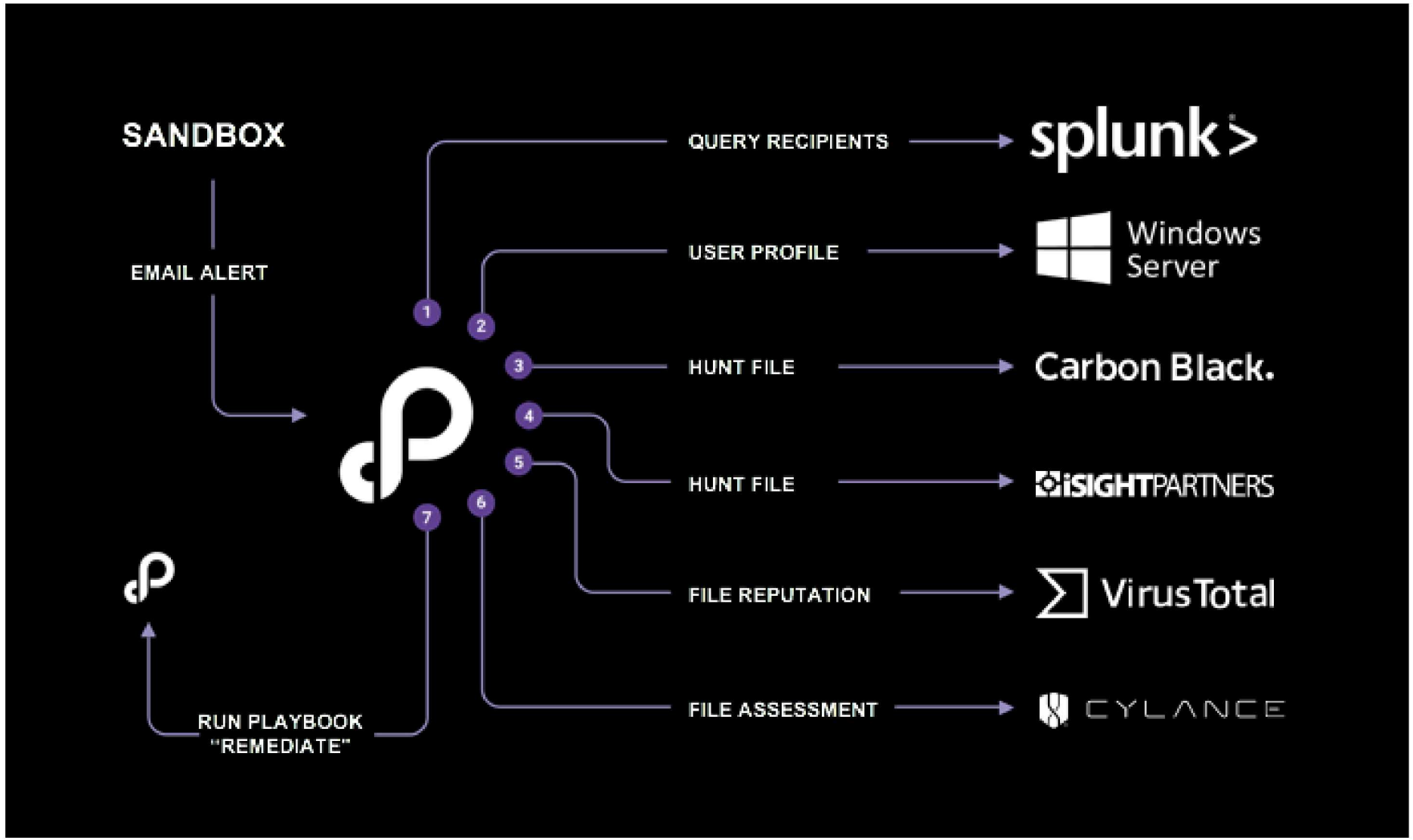
Sandia National Laboratories



Analyst View & Apply Process To Findings



Other Examples for Response



Testing & Refining

- Remember, Hunting is Hard!
- The first search is not the perfect search
- May end up with false positives like alerting
- Mitigation
  - Build your leads/hypothesis and test on a known good system
    - Reduce risk of returning lots of noise
  - Run data against sample data set
    - Ensure you won't get overrun on a monthly long search

Operationalize Your Findings

Sandia National Laboratories

- Create Feedback Loop from Hunting to Incident Response
- Hunting is proactive
- Develop a hypothesis
- “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