Operationalizing Hunt: Defensive Cyber Operations

Hunting Adversarial Behaviors

Anthony Talamantes | Manager, Defensive Cyber Operations

Todd Kight | Lead Cyber Threat Analyst

October 2018

Forward-Looking Statements

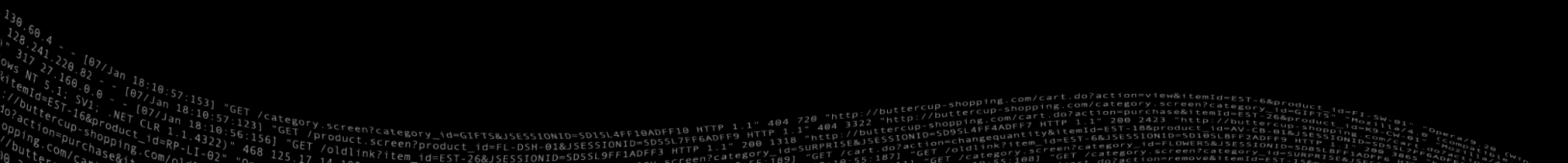
During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results 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

Summary

- Overview: Creating a Threat Based Cyber Team
- Use Cases & Data
  - Requirements
  - Access
- Traditional SOC
- Hunt Methodologies
- Hunt & Content Development



Overview: Building a Threat-Based Cyber Team

Review .conf17

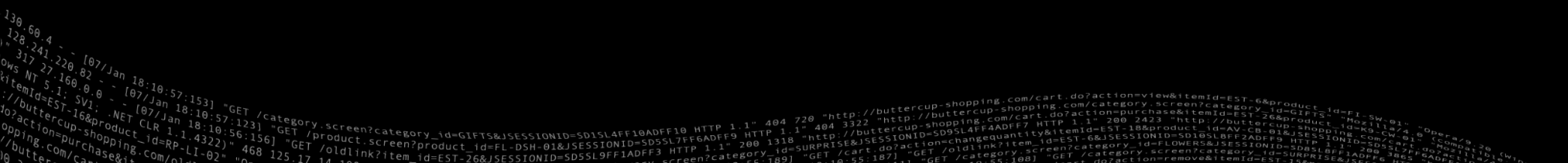
splunk> .conf18

Johns Hopkins University Applied Physics Lab

splunk> .conf18

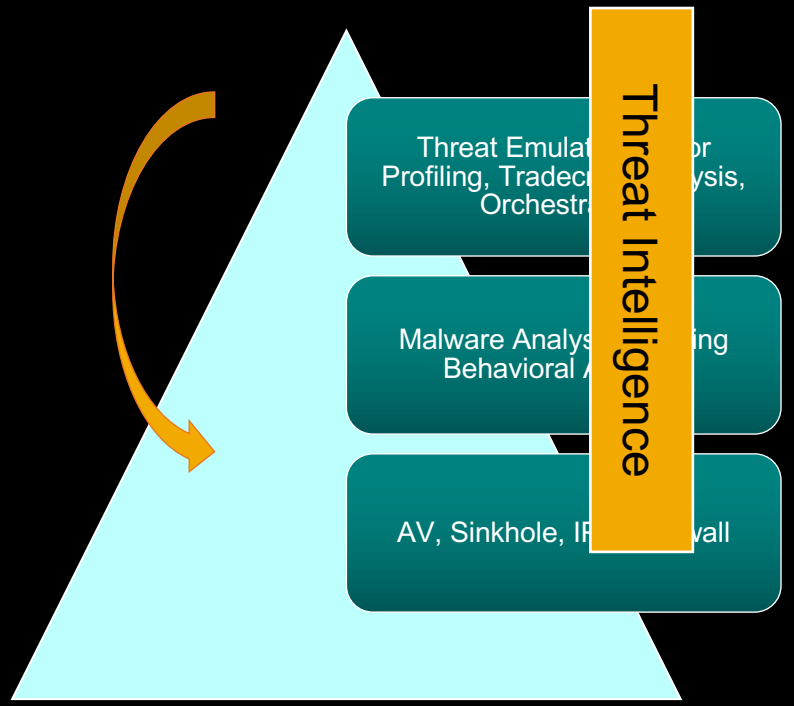
Defensive Cyber Operations

- JHUAPL cyber attack 2009
  - Focus on Security Posture
- Never let an Incident go to waste
  - Defense partners
- Change in Threat landscape
- Moved focus from Security Posture to Capability Posture
- Cyber maturity evolution
  - Response & Mitigation
  - Behaviors & Hunting
- Investment in Technology, People, and Process
- Change in Philosophy
- Change in Core competencies



Change in Philosophy

- Threat Focused Cyber Operations
  - Research and identify Threats targeting your organization
  - Target advanced tactics, techniques and procedures of adversary
  - Emulate threat in your environment
  - Develop hunting and analytics techniques
- Changes, Challenges & Culture
  - What is behavioral monitoring anyways?
  - Mitigation vs Detection
  - What is Threat Intelligence?
    - More than indicators of compromise



Defensive Cyber Operations Inception

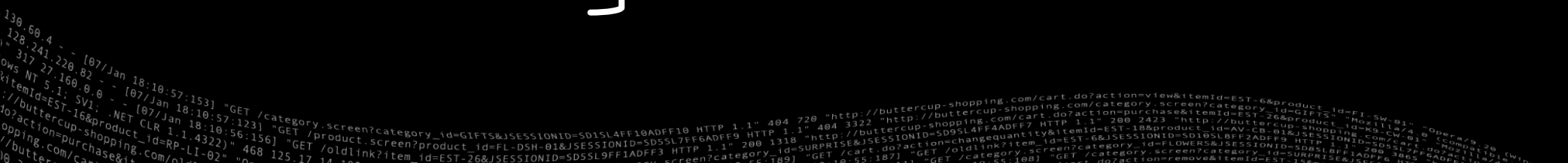
Philosophy

- Use Cases
- Data Analysis
- Behaviors
- Visibility based
- Agility
- Enrichment
- Automation
- Independence
- DevOps

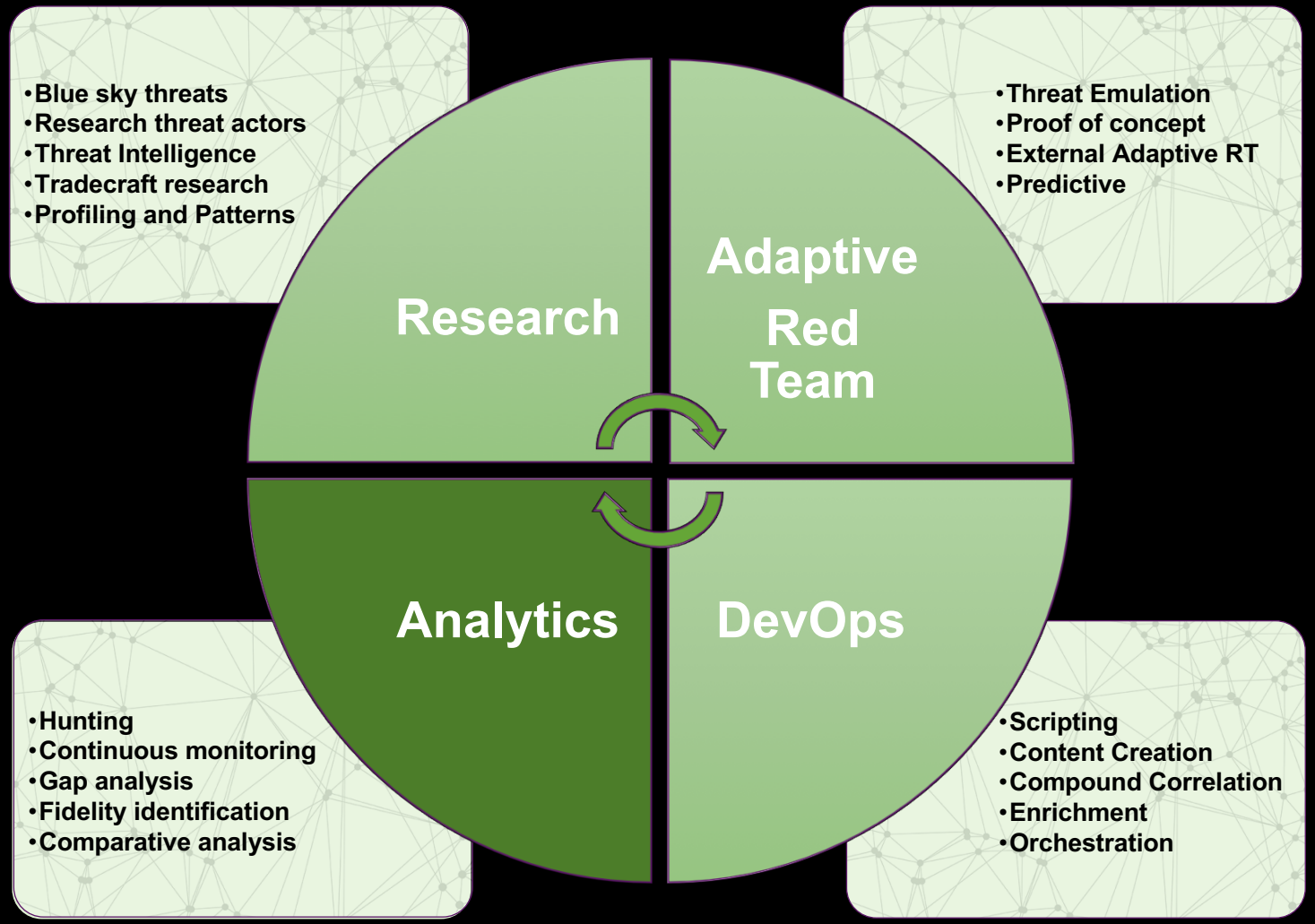
Capability Posture

- **Technology**
  - **Splunk**
  - **EDR**
- **People**
  - **New skillsets**
  - **New approach**
- **Process**
  - **Hunting**
  - **Agility**

Vehicle For Change



Defensive Cyber Operations Construct



Data

Requirements & Access

splunk> .conf18

MITRE ATT&CK™ model

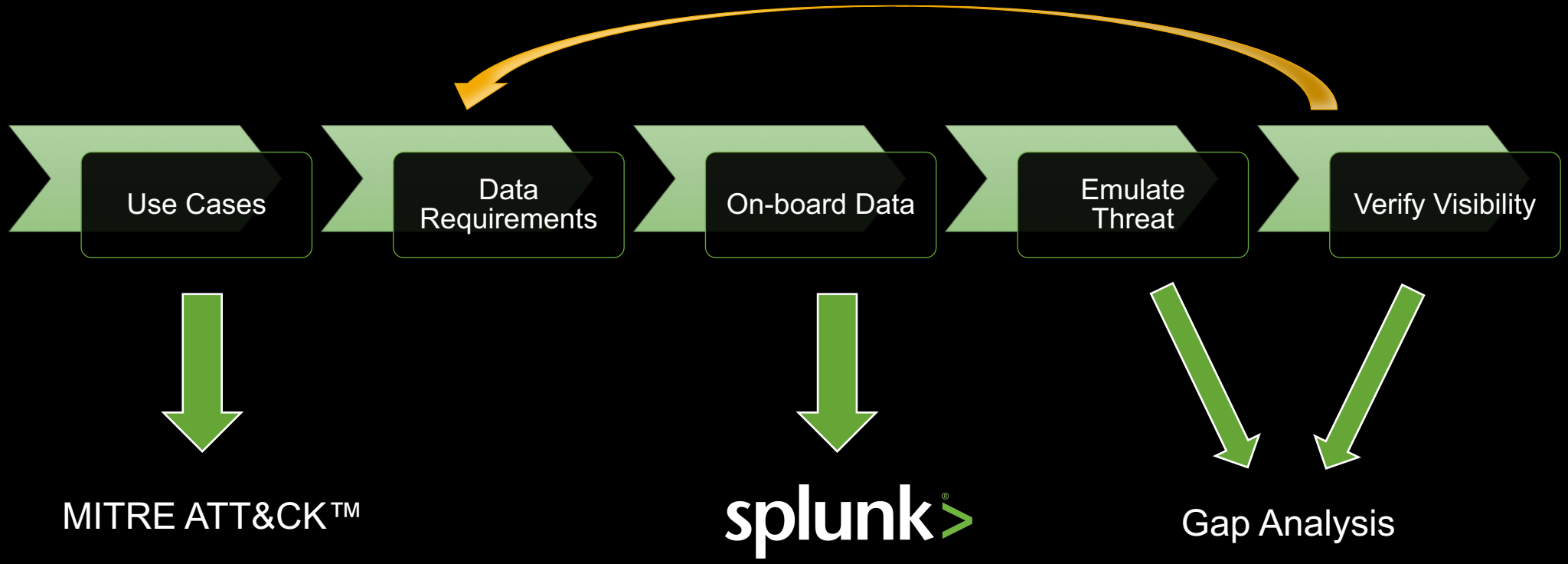
Starting Point in Defining Use Cases

- "We started ATT&CK almost five years ago as a way to categorize common adversary behavior for adversary emulation and intrusion detection research."
- MITRE ATT&CK Philosophy
  - 4.1 Conceptual
    - There are three conceptual ideas that are core to the philosophy behind ATT&CK:
      - It maintains the adversary's perspective;
      - It follows real-world use of activity through empirical use examples;
      - The level of abstraction is appropriate to bridge offensive action with possible defensive countermeasures.

https://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/the-philosophy-of-attck

https://www.mitre.org/sites/default/files/publications/pr-18-0944-11-mitre-attack-design-and-philosophy.pdf

Process For Defining Data Requirements



Use Cases & Data Requirements

- ATT&CK ID T1015

Examples

- APT29 used sticky-keys to obtain unauthenticated, privileged console access.[4][5]
- APT3 replaces the Sticky Keys binary `C:\Windows\System32\sethc.exe` for persistence. [6]
- Axiom actors have been known to use the Sticky Keys replacement within RDP sessions to obtain persistence.[7]
- Deep Panda has used the sticky-keys technique to bypass the RDP login screen on remote systems during intrusions.[8]

ATT&CK Matrix for Enterprise

The full ATT&CK Matrix below includes techniques spanning Windows, Mac, and Linux platforms and can be u

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evas
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	Binary Paddin

Accessibility Features

Technique

ID	T1015
Tactic	Persistence, Privilege Escalation
Platform	Windows
Permissions Required	Administrator
Effective Permissions	SYSTEM
Data Sources	Windows Registry, File monitoring, Process monitoring
CAPEC ID	CAPEC-558
Contributors	Paul Speulstra, AECOM Global Security Operations Center

splunk> .conf18

Use Cases & Data Requirements

- ATT&CK ID T1175

Discovery	Lateral Movement	Collection
Account Discovery	AppleScript	Audio Capture
Application Window Discovery	Application Deployment Software	Automated Collection
Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data
File and Directory Discovery	Exploitation of Remote Services	Data Staged

Distributed Component Object Model

Technique

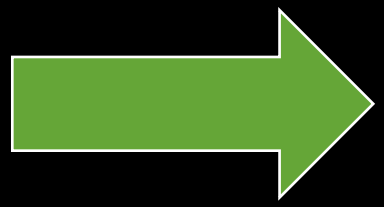
ID	T1175
Tactic	Lateral Movement
Platform	Windows
Permissions Required	Administrator, SYSTEM
Data Sources	API monitoring, Authentication logs, DLL monitoring, Packet capture, Process monitoring, Windows Registry, Windows event logs

Examples

- Cobalt Strike can deliver "beacon" payloads for lateral movement by leveraging remote COM execution.[10]
- POWERSTATS can use DCOM (targeting the 127.0.0.1 loopback address) to execute additional payloads on compromised hosts.[11]

Use Cases & Data Requirements

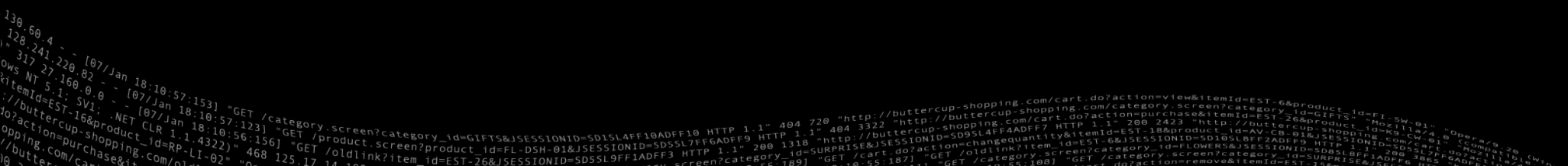
- Data needed to support Use Cases
  - Windows registry
  - File monitoring
  - Process monitoring
  - DLL monitoring
  - Process monitoring
  - Authentication logs
  - API monitoring
  - Windows Event logs
  - Packet Capture



splunk>

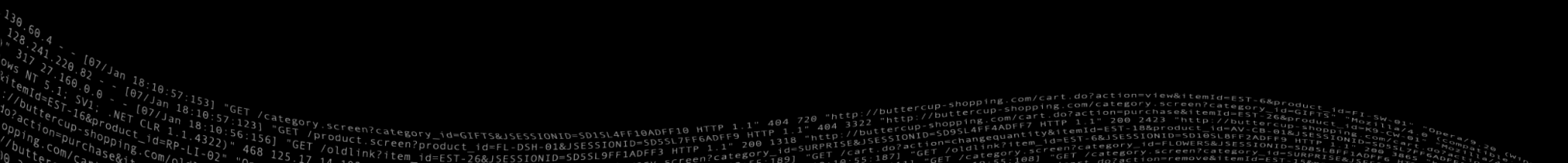
Use Cases & Data Requirements

- In addition – we also leverage
  - Process to network enumeration
  - Command line arguments
  - Module loads
  - Analytic data



Getting to Data Fast

- Lower cost of entry
- Google-like query language supporting all analysts
- Language to support advanced queries
- Normalization
- Buckets
  - Raw
  - Supplemental
  - Interesting
  - Actionable
- Focus areas



Traditional SOC

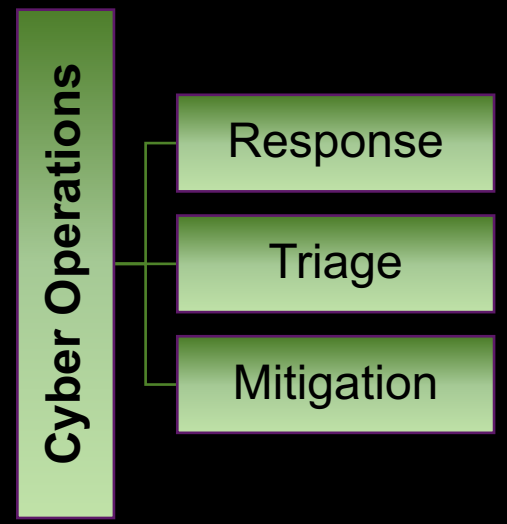
Discussion on Reactive Approach

Traditional SOC

- Matching Atomic IOCs
  - IP Addresses
  - Email addresses
  - Domains
  - File Hashes

Hunting?

- Reactive Based
  - Mitigating indicators of someone else's compromise



Hunt Methodologies

A few approaches to get things started

Hunt Methodologies

Pivoting

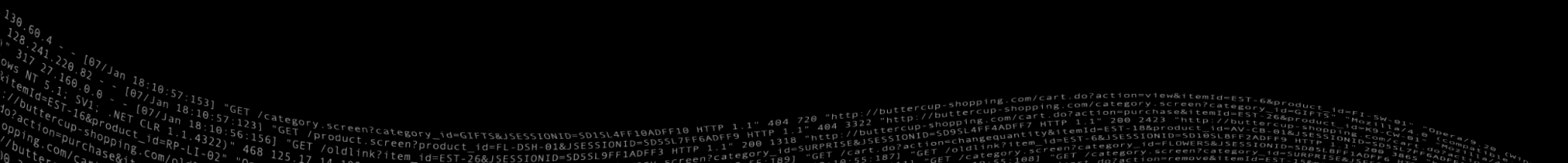
- Use reference point as a start

Referential Hunting

- Stacking
  - Content (use cases/signatures)
  - Pre-determined data (metered execs)
- Baseline Drift
  - Expected ports unexpected processes
  - Uniqueness / Newness / Rareness
    - Lateral
    - C2
    - Account Usage
- Compound Correlation
  - <develop threat model>
  - <combine above methods to reach a conclusion>
  - This + that + the other thing = interesting

Rabbit-holing

Pivot Points	
Email	Infrastructure IP X-Header Sender Name
Malware Analysis	PDB path Certificate Behavior Other Strings
Web	User-Agent
Domain	Registrant Infrastructure

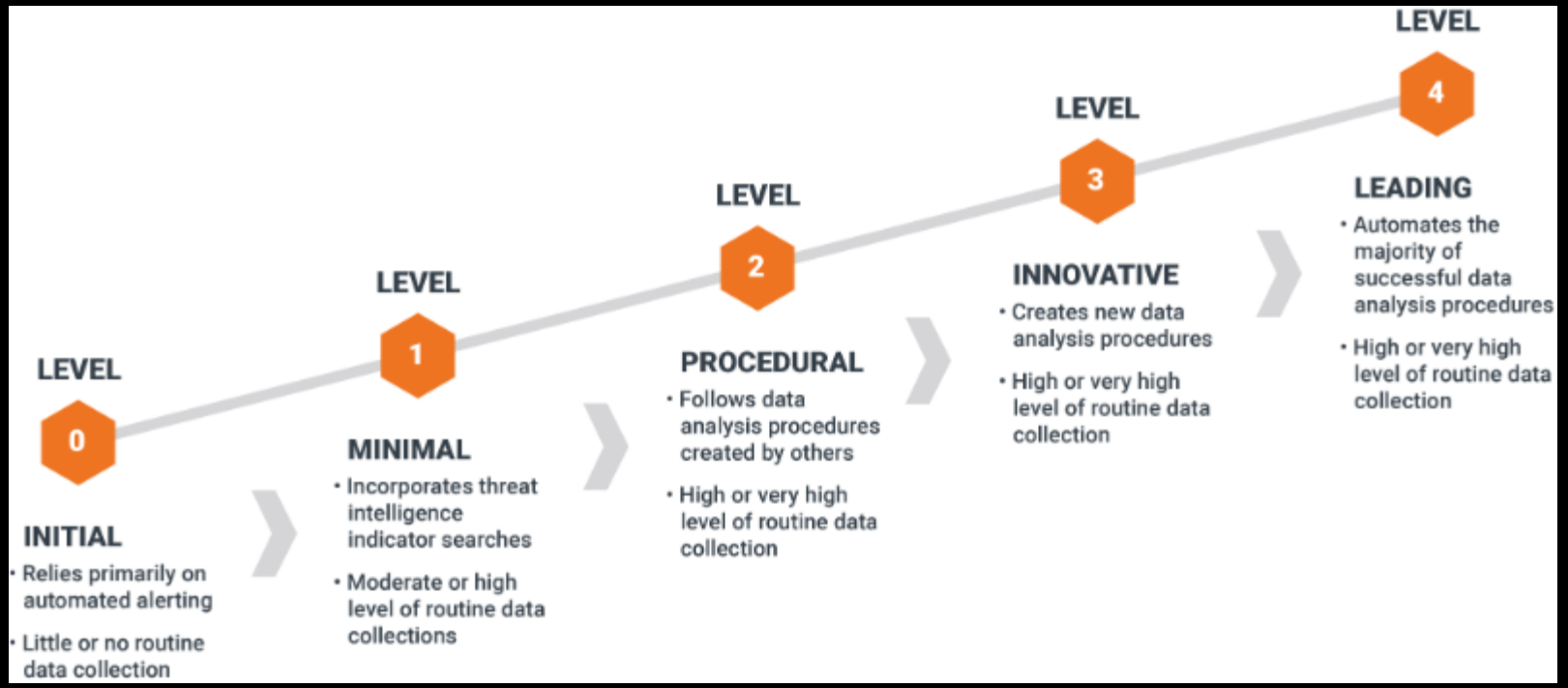


splunk> .conf18

Measuring Progress – Hunting Maturity Model

What level are you?

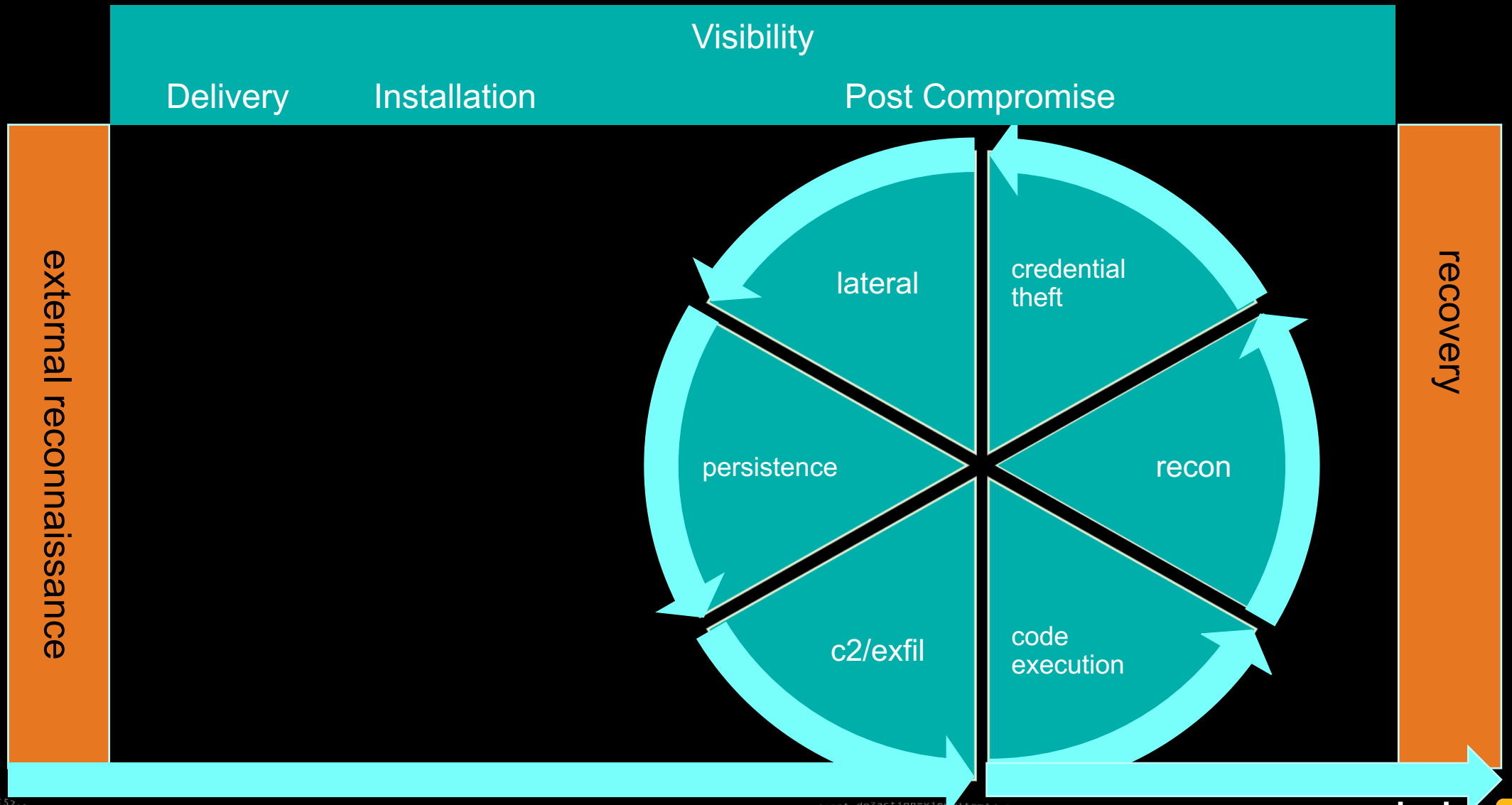
- Know your data
- Understand the threat
- Avoid reliance on vendor generated alerts
- Use threat intelligence differently
- Research
- Emulate
- Create
- Utilize varying hunt methodologies



Ref:
https://www.linkedin.com/pulse/threat-hunting-maturity-model-ely-kahn
https://sqrll.com

splunk> .conf18

Measuring Progress - Attack Lifecycle

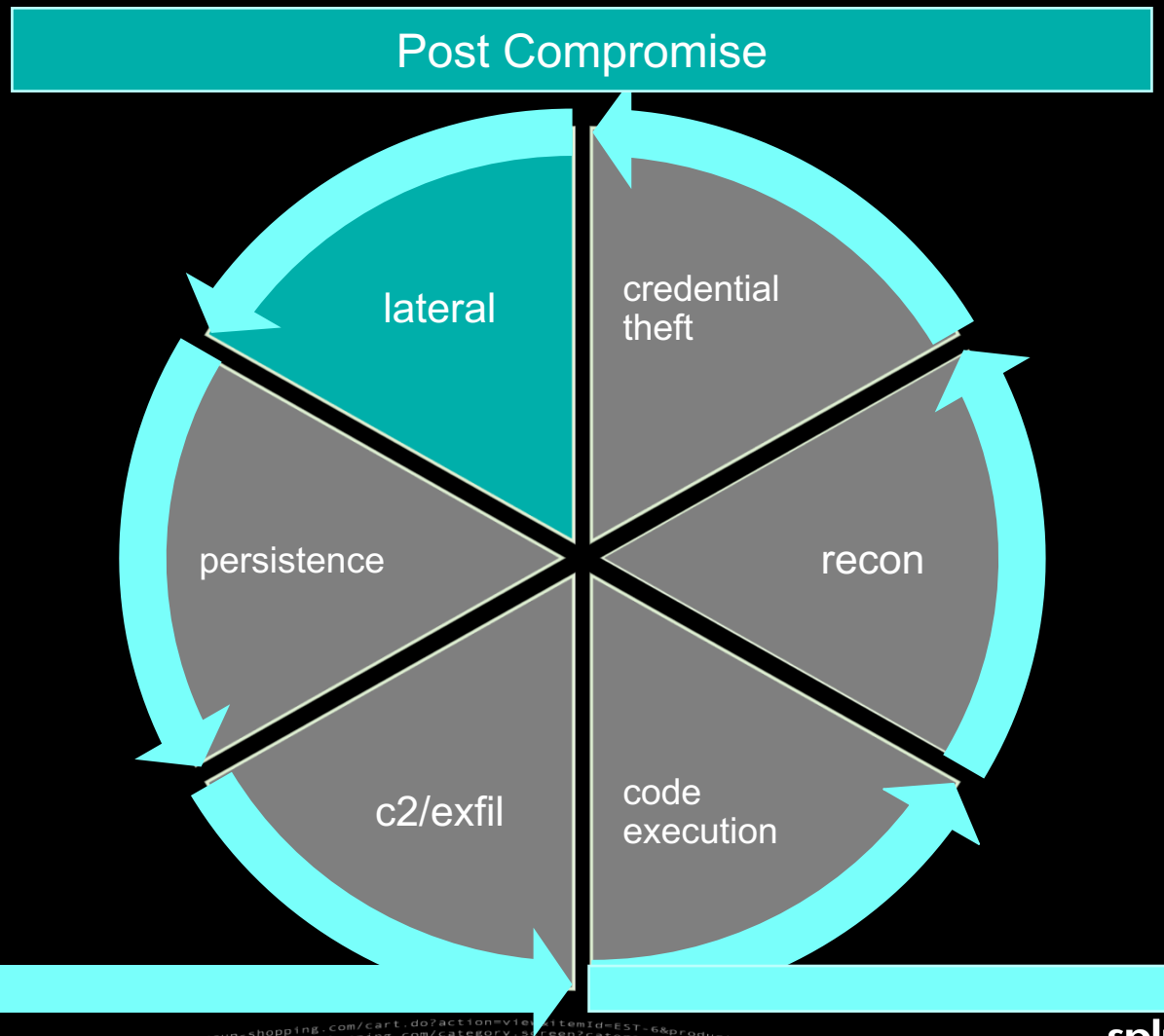


Measuring Progress - Attack Lifecycle

FOCUS ON LATERAL

Potential Technologies

- EDR
- Sysmon
- Netflow
- IDS
- Firewall (host)
- …

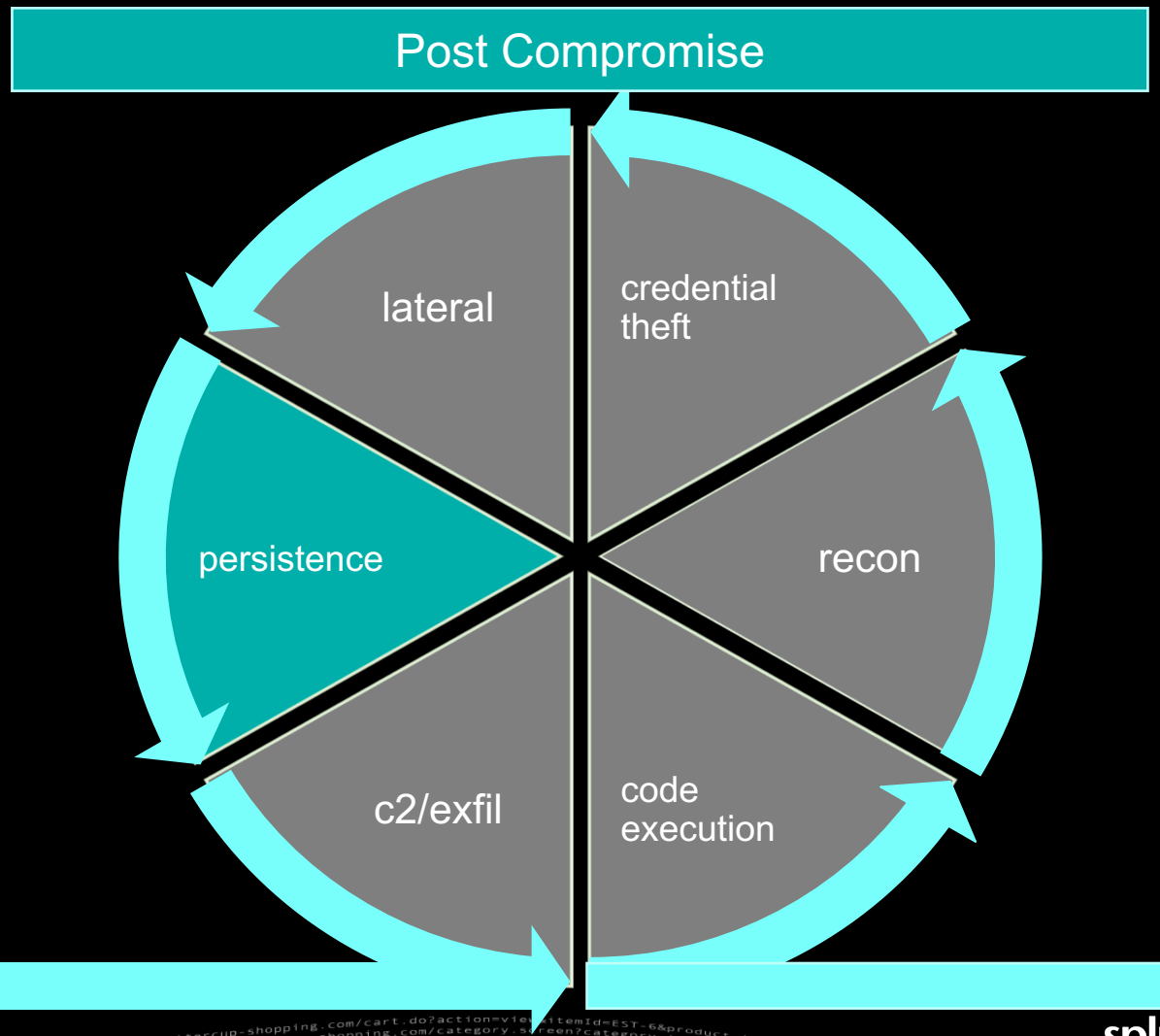


Measuring Progress - Attack Lifecycle

FOCUS ON PERSISTENCE

Potential Technologies

- EDR
- Sysmon
- Regmon
- …



Hunt & Content Development

Building more meaningful signatures

splunk> .conf18

Hunt & Content Development

Building more meaningful signatures

Sources of Information

- Threat Intelligence
- MITRE's ATT&CK™ model
- Independent research

Process

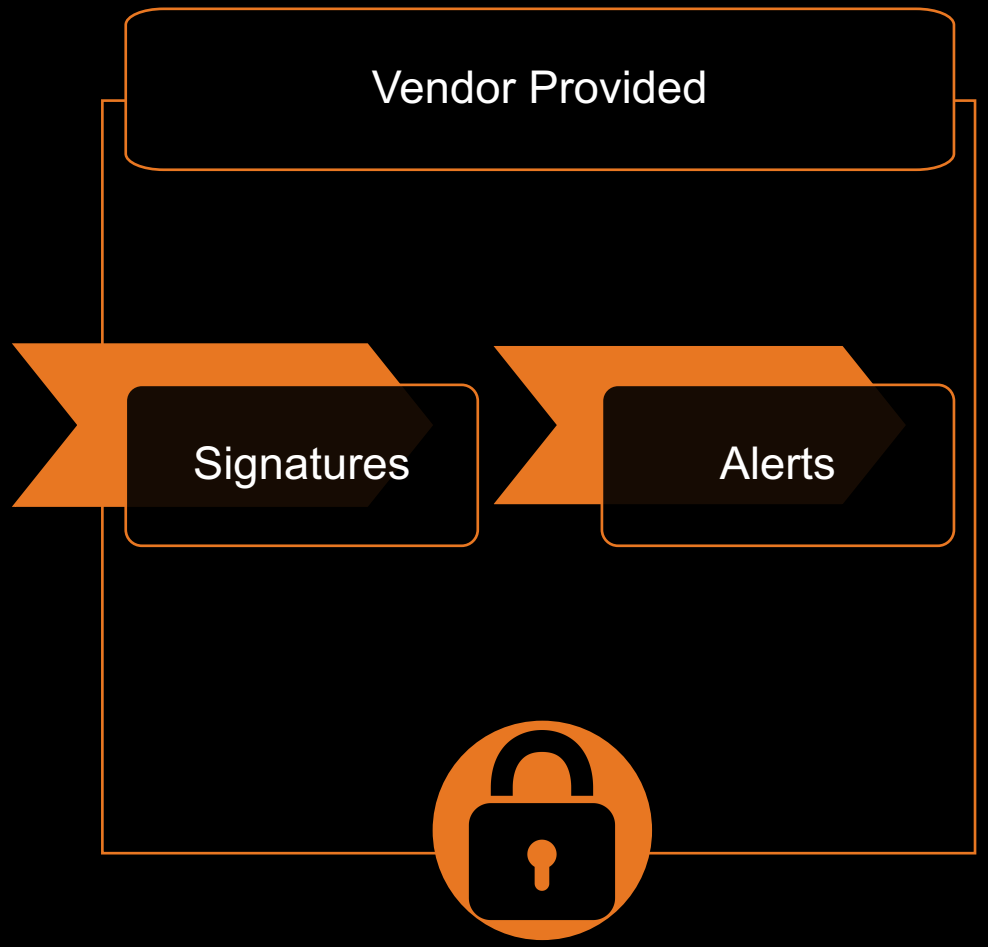
- Threat Emulation
- Walkthrough – let's build a use case
- High fidelity content development frees up time to Hunt!

Hunt & Content Development

Evolving towards something more useful

Historically…

- SOC responded to vendor provided alerts from vendor provided signatures
- This was a black box approach
- We needed something more



Hunt & Content Development

Using MITRE's ATT&CK™ model

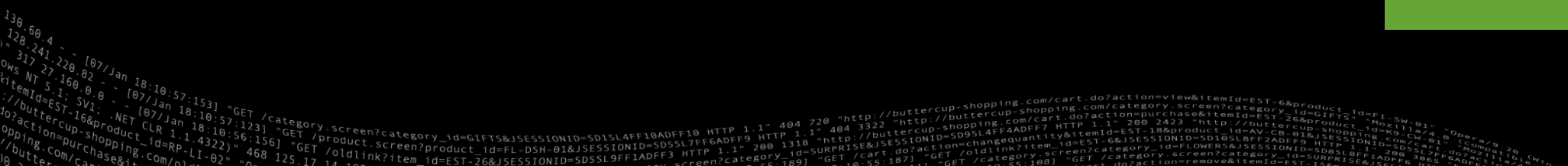
Pros

- Excellent starting point for content development
- Extensive list of well defined tactics and techniques
- Maps tactics and techniques to adversary
- Validates existing data and identifies gaps in visibility

Cons

- Opportunities exist for inclusion of detection signatures

MITRE's Adversarial Tactics, Techniques, and Common Knowledge ATT&CK™ is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's lifecycle and the platforms they are known to target. ATT&CK is useful for understanding security risk against known adversary behavior, for planning security improvements, and verifying defenses work as expected.

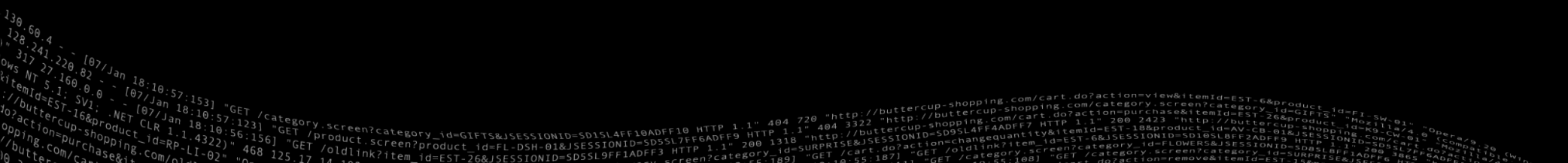


Hunt & Content Development

Using additional research and bright shiny ideas

- Credential Theft – Golden ticket
- Lateral – DCOM <extended research beyond ATT&CK>
- Persistence – WMI

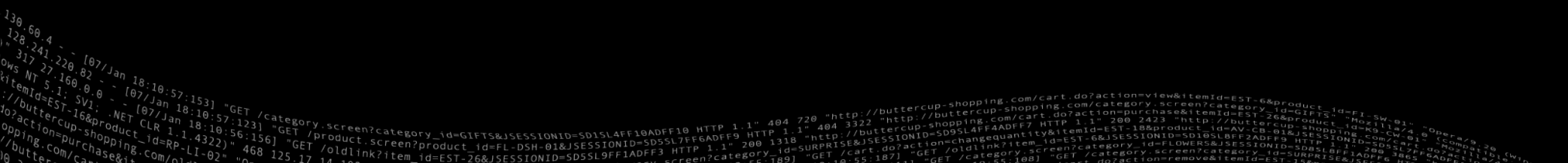
- Bloggers
  - enigma0x3
  - mattifestation
  - Cyb3rWard0g



Hunt & Content Development

Using Threat Intelligence

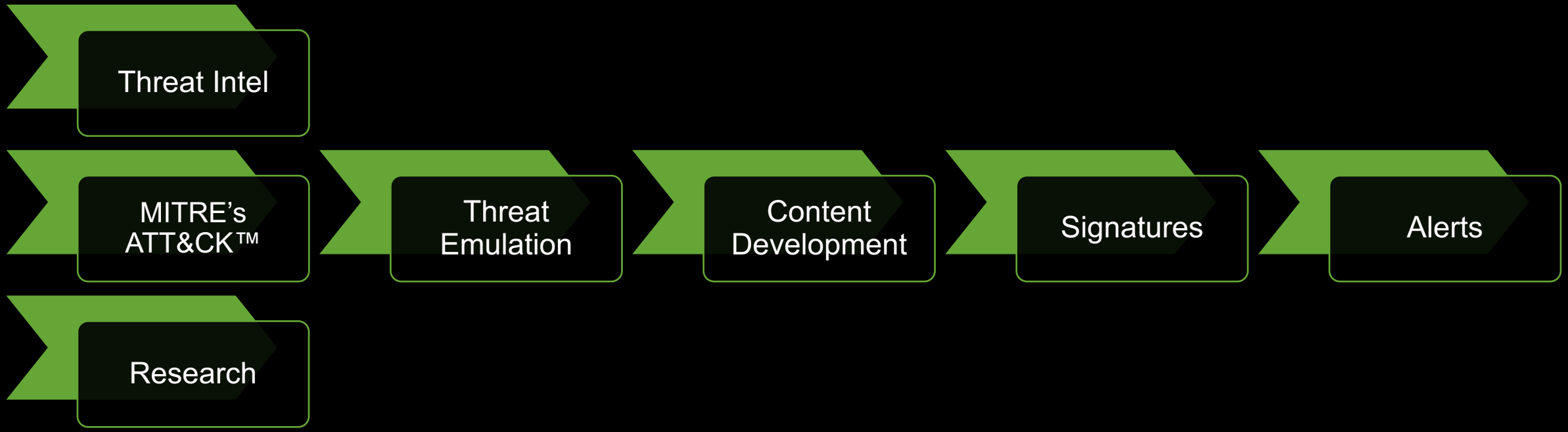
- Indicators of Compromise (IOCs)
  - Matching (not hunt)
- Threat Intelligence Reports
  - Understanding TTPs
  - Understanding Threat



splunk> .conf18

Hunt & Content Development

Let's build a use case (signature)



Hunt & Content Development - Easy

T1015 – Accessibility Features

Accessibility Features	
Technique	
ID	T1015
Tactic	Persistence, Privilege Escalation
Platform	Windows
Permissions Required	Administrator
Effective Permissions	SYSTEM
Data Sources	Windows Registry, File monitoring, Process monitoring
CAPEC ID	CAPEC-558

- Great starting point
- Limited data needed for detection
- Easy to emulate
- Easy to detect

Hunt & Content Development - Easy

T1015 – Accessibility Features / Our Take

Data Sources	EDR, Sysmon, EventID 4688, Application Whitelisting, Splunk Regmon
Use Cases	Staging (binary replacement and/or registry modification) Execution (parent child mismatch)
Emulation (Staging)	replace any of the 'sticky keys' executables with the program you want to run (c:\windows\system32\cmd.exe)
Emulation (Staging)	reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\#{target_executable}" /v "Debugger" /t REG_SZ /d "C:\windows\system32\cmd.exe" /f
Emulation (Execution)	Shift key …

Hunt & Content Development - Easy

T1015 – Accessibility Features / Our Take

Detection (Staging)	(regmod:"\registry\machine\software\microsoft\windows nt\currentversion\image file execution options\sethc.exe\debugger") OR (regmod:"\registry\machine\software\microsoft\windows nt\currentversion\image file execution options\utilman.exe\debugger") OR (regmod:"\registry\machine\software\microsoft\windows nt\currentversion\image file execution options\osk.exe\debugger") OR (regmod:"\registry\machine\software\microsoft\windows nt\currentversion\image file execution options\magnify.exe\debugger") OR (regmod:"\registry\machine\software\microsoft\windows nt\currentversion\image file execution options\narrator.exe\debugger") OR (regmod:"\registry\machine\software\microsoft\windows nt\currentversion\image file execution options\displayswitch.exe\debugger") OR (regmod:"\registry\machine\software\microsoft\windows nt\currentversion\image file execution options\atbroker.exe\debugger")

Hunt & Content Development - Easy

T1015 – Accessibility Features / Our Take

Detection (Execution)	((parent_name:winlogon.exe username:SYSTEM AND (process_name:cmd.exe OR process_name:explorer.exe)) OR (process_name:sethc.exe AND cmdline:211 AND -(file_desc:"Accessibility shortcut keys")) OR (process_name:osk.exe AND -file_desc:"Accessibility On-Screen Keyboard") OR (process_name:magnify.exe AND -file_desc:"Microsoft Screen Magnifier") OR (process_name:narrator.exe AND -(file_desc:"Narrator" OR file_desc:"Screen Reader")) OR (process_name:displayswitch.exe AND -file_desc:"Display Switch") OR (process_name:atbroker.exe AND -(file_desc:"Windows Assistive Technology Manager" OR file_desc:"Transitions Accessible technologies between desktops"))) AND username:SYSTEM

Hunt & Content Development - Challenging

T1175 – Distributed Component Object Model

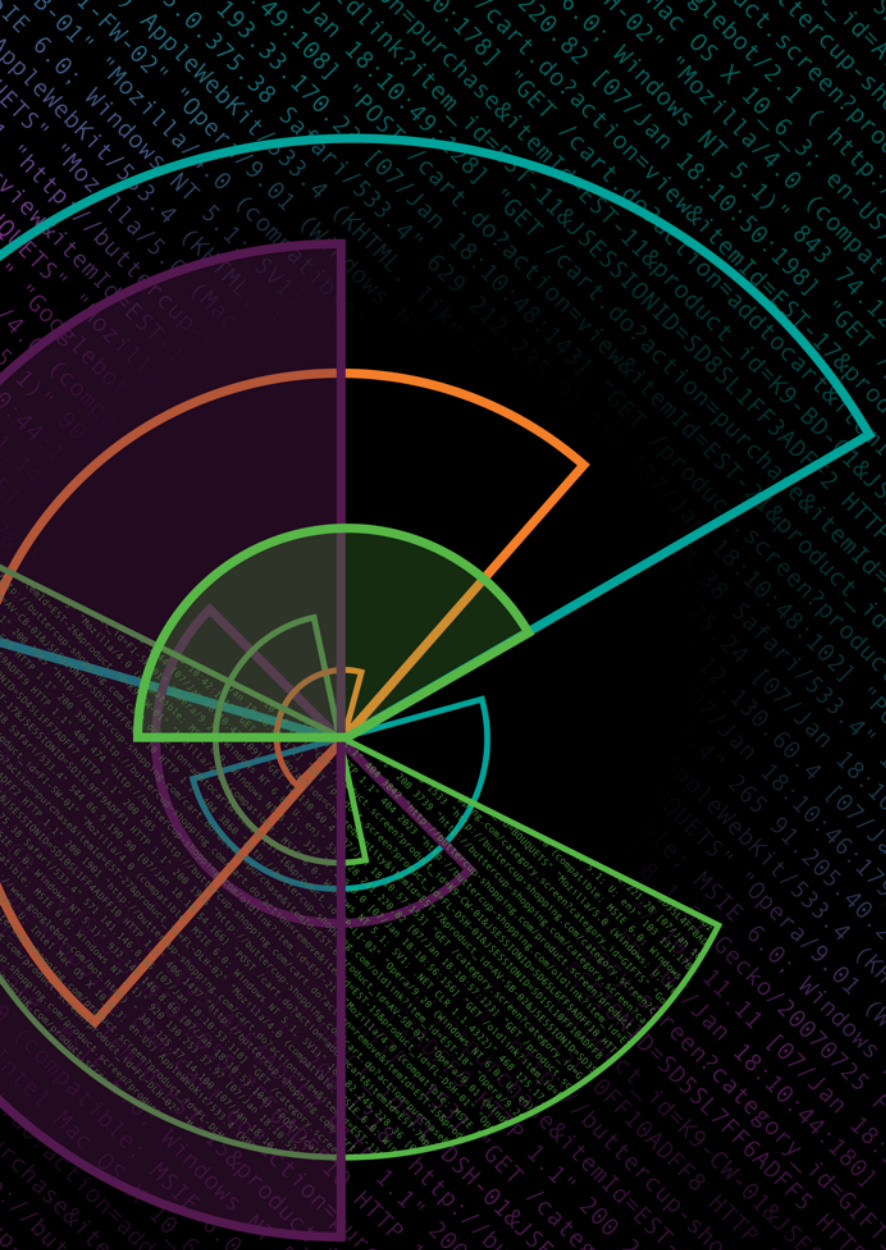
Distributed Component Object Model	
Technique	
ID	T1175
Tactic	Lateral Movement
Platform	Windows
Permissions Required	Administrator, SYSTEM
Data Sources	API monitoring, Authentication logs, DLL monitoring, Packet capture, Process monitoring, Windows Registry, Windows event logs

- A little more challenging to detect
- Emulated threat
- Identified additional data sources (process-to-netconn)
- Result: successful detection of technique and identification of attacker and victim hosts

Key Takeaways

Our story

1. Catalyst for change
2. Building the team
3. Value of data
4. Research and Threat Intelligence
5. Hunt methodologies
6. Hunt & Content development
7. Measure progress



Q&A

splunk> .conf18