# ATT&CK yourself before someone else does

Dave Herrald, John Stoner, and Ryan Kovar
Principal Strategists @ Splunk

# Forward-Looking Statements

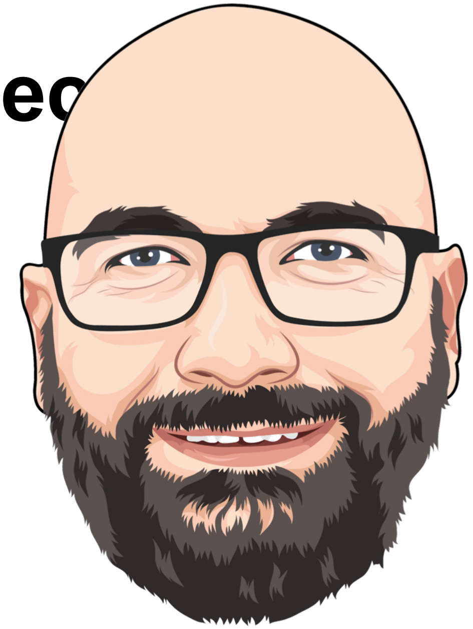
During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. 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, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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 functionalities described or to include any such feature or functionality in a future release.

# System Owner/User Discovery (T1033)

## Dave Herrald (🐦 @daveherrald)

- Principal Security Strategist at Splunk
- CISSP, GIAC G*, GSE #79
- 25+ years IT and Security
- Information security officer, security architec pen tester, consultant, SE, system/network engineer
- Former SANS mentor
- Co-Creator of Splunk Boss of the SOC



# System Owner/User Discovery (T1033)

## John Stoner ( @stonerpsu)

- Principal Security Strategist at Splunk
- 20+ years kicking around databases, ISPs, and Cyber
- 4.5 years at Splunk
- Creator of SA-Investigator
- Co-Editor and author of Hunting with Splunk
- Assist in steering the BOTS ship
- Developed APT Scenario for BOTS IV
- Developed workshops on hunting and investiga
  with Splunk

# System Owner/User Discovery (T1033)

## Ryan Kova🐦 @meansec)

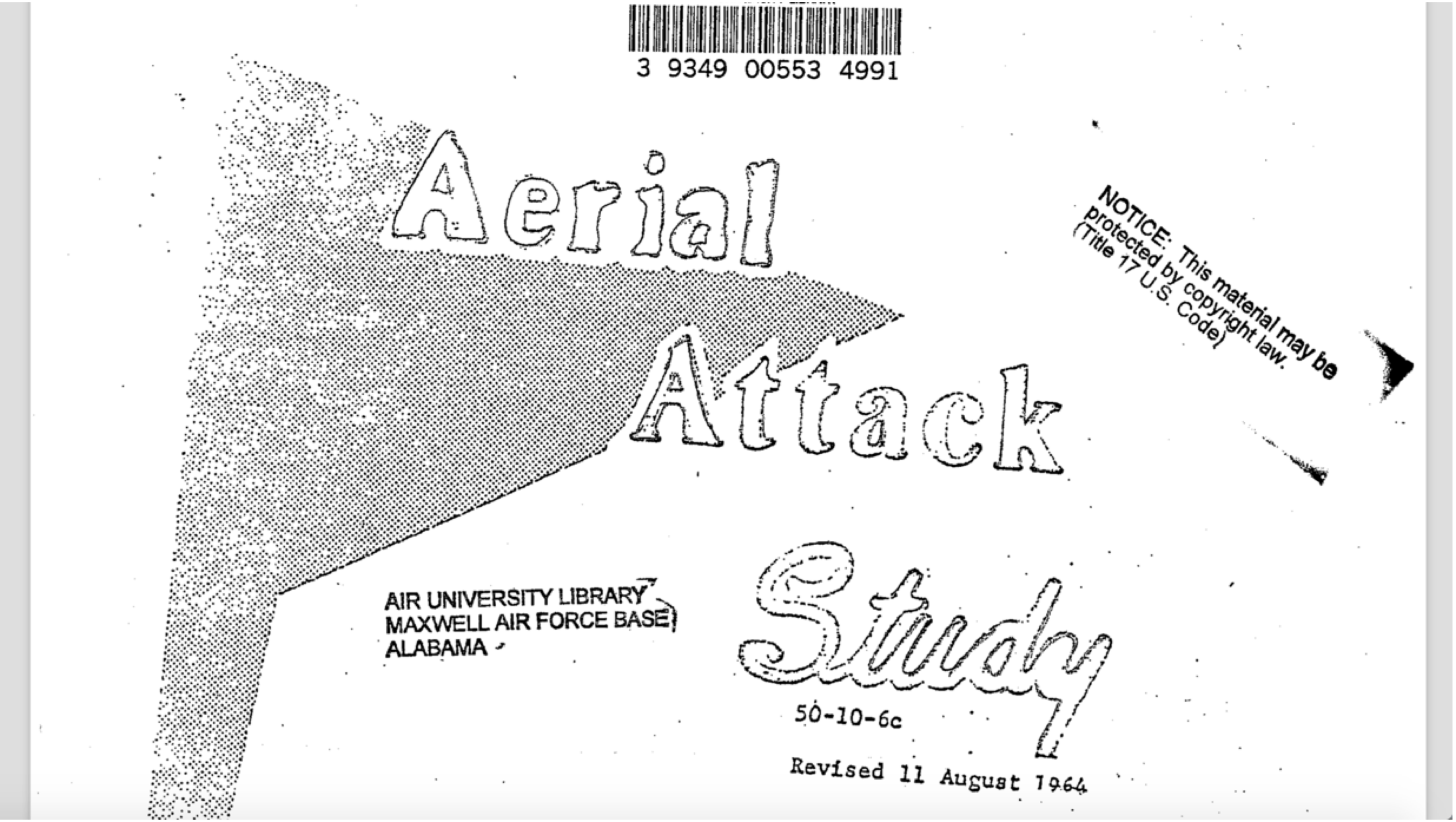
- Principal Security Strategist at Splunk
- Black Hat and Def Con Village Speaker
- MSc(Dist) Information Security
- Minister of OODAlooping at Splunk
- US/UK  DoD/PubSec Nation State Hunting Re
- Enough white in beard to speak authoritative
- Co-Creator of Boss of the SOC C F
- Hates printers and trilobites

# Agenda

1. What **we** think att&ck means to network defenders
2. How you can **hunt** with ATT&CK
3. Dance number
4. How you can **operationalize** ATT&CK with Splunk
5. **Conclusion**

# What we think ATT&CK means to network defenders

# Colonel John Boyd

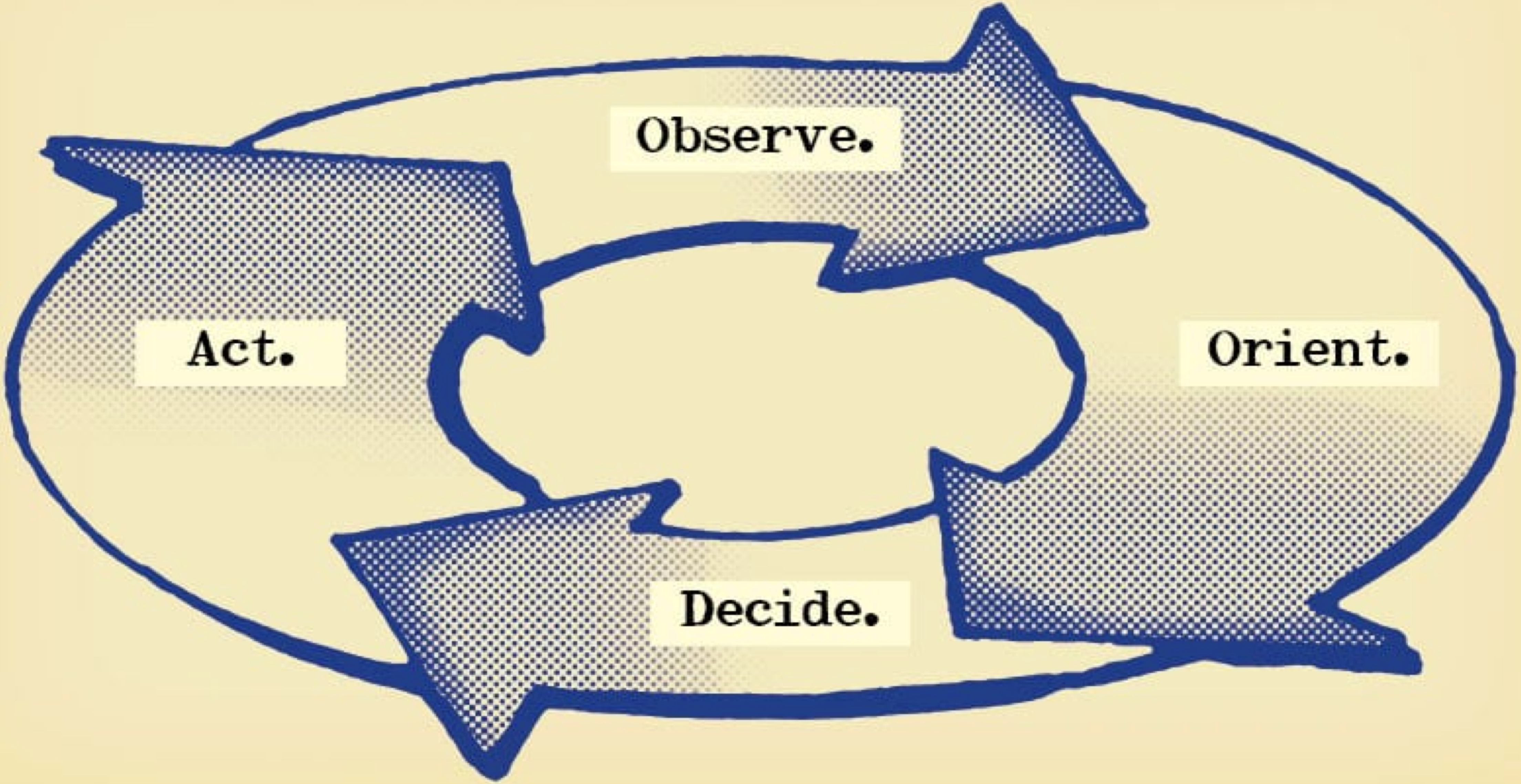


# Aerial Attack Study

50-10-6c

Revised 11 August 1964

# O.O.D.A. Loop.



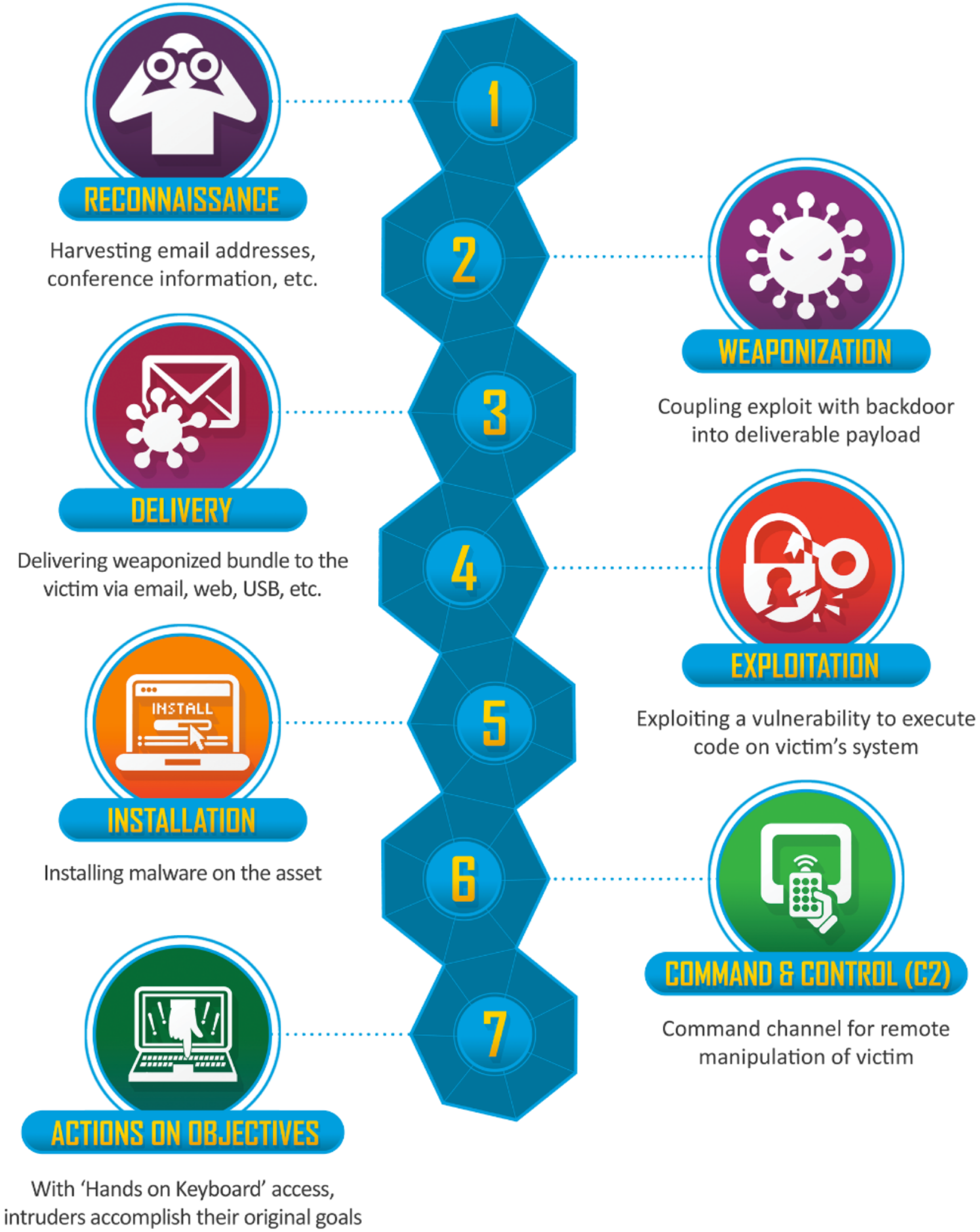
Observe.

Orient.

Decide.

Act.

# Lockheed Martin Cyber Kill Chain



1 RECONNAISSANCE

Harvesting email addresses, conference information, etc.

2 WEAPONIZATION

Coupling exploit with backdoor into deliverable payload

3 DELIVERY

Delivering weaponized bundle to the victim via email, web, USB, etc.

4 EXPLOITATION

Exploiting a vulnerability to execute code on victim's system

5 INSTALLATION

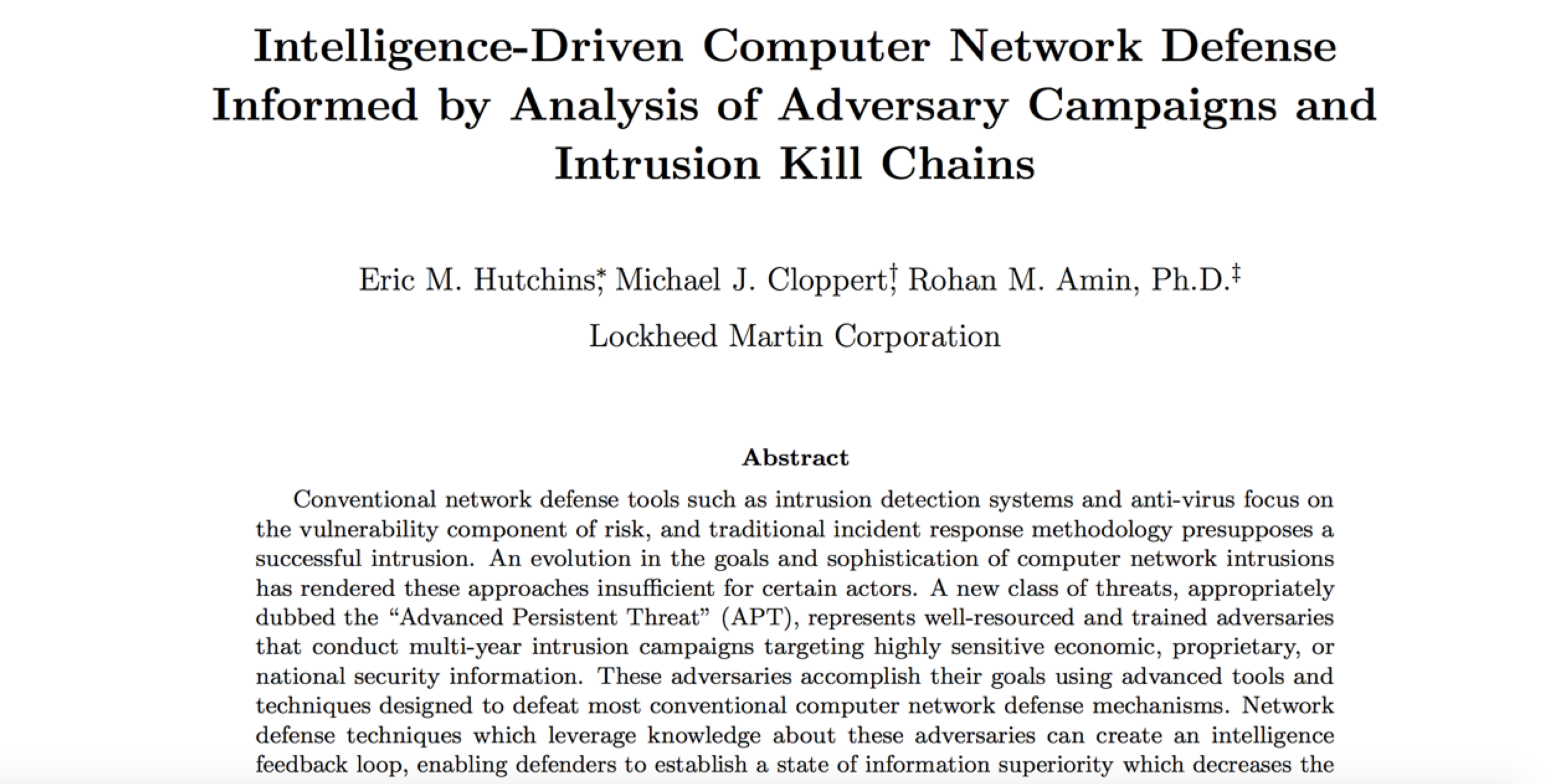
Installing malware on the asset

6 COMMAND & CONTROL (C2)

Command channel for remote manipulation of victim

7 ACTIONS ON OBJECTIVES

With 'Hands on Keyboard' access, intruders accomplish their original goals



# Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains

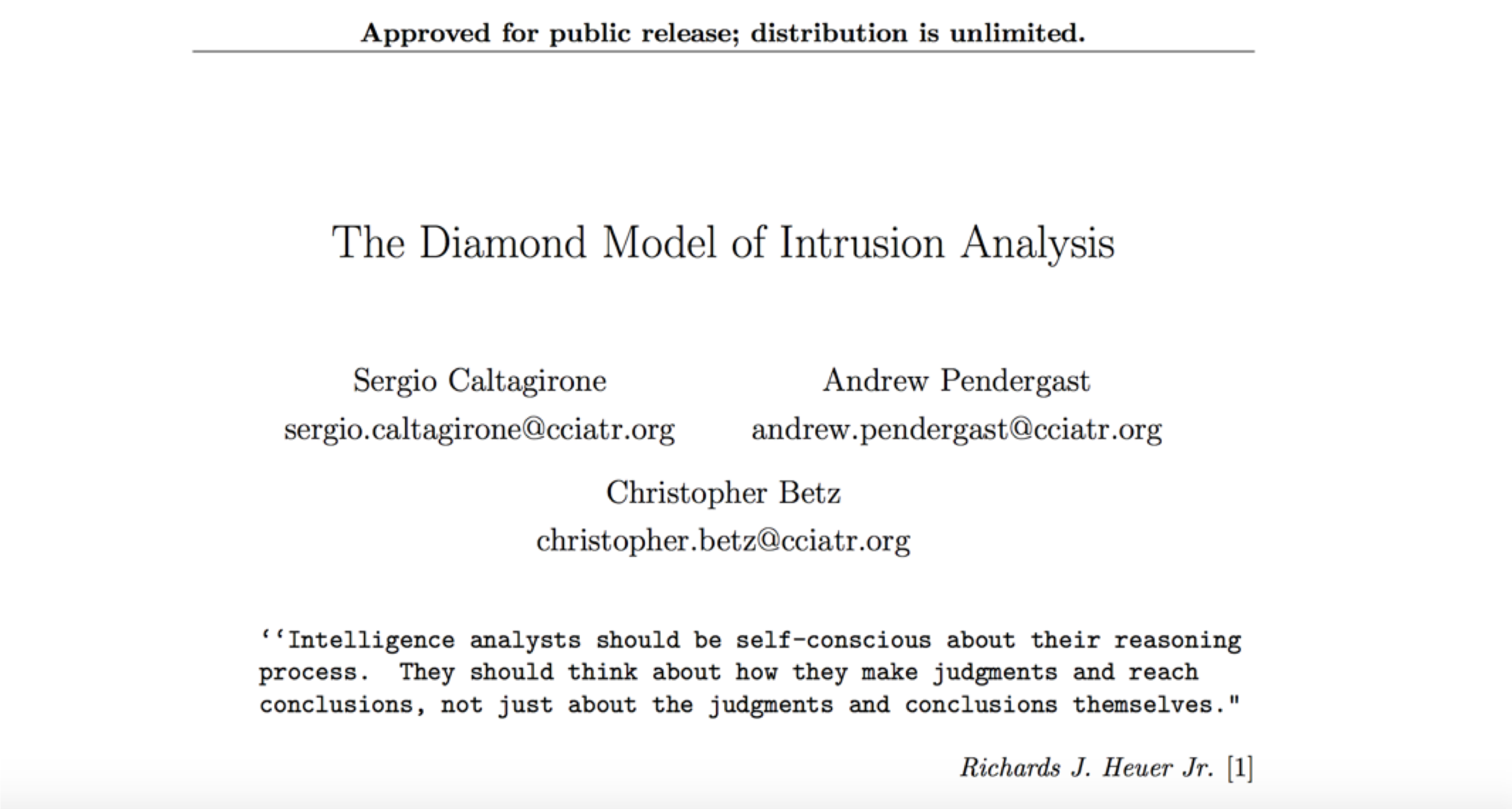
Eric M. Hutchins[*] Michael J. Cloppert[†] Rohan M. Amin, Ph.D.[‡]

Lockheed Martin Corporation

## Abstract

Conventional network defense tools such as intrusion detection systems and anti-virus focus on the vulnerability component of risk, and traditional incident response methodology presupposes a successful intrusion. An evolution in the goals and sophistication of computer network intrusions has rendered these approaches insufficient for certain actors. A new class of threats, appropriately dubbed the "Advanced Persistent Threat" (APT), represents well-resourced and trained adversaries that conduct multi-year intrusion campaigns targeting highly sensitive economic, proprietary, or national security information. These adversaries accomplish their goals using advanced tools and techniques designed to defeat most conventional computer network defense mechanisms. Network defense techniques which leverage knowledge about these adversaries can create an intelligence feedback loop, enabling defenders to establish a state of information superiority which decreases the

# Diamond Model



**Approved for public release; distribution is unlimited.**

# The Diamond Model of Intrusion Analysis

Sergio Caltagirone
sergio.caltagirone@cciatr.org

Andrew Pendergast
andrew.pendergast@cciatr.org

Christopher Betz
christopher.betz@cciatr.org

``Intelligence analysts should be self-conscious about their reasoning process. They should think about how they make judgments and reach conclusions, not just about the judgments and conclusions themselves."

*Richards J. Heuer Jr.* [1]

## 1 SOCIO-POLITICAL AXIS

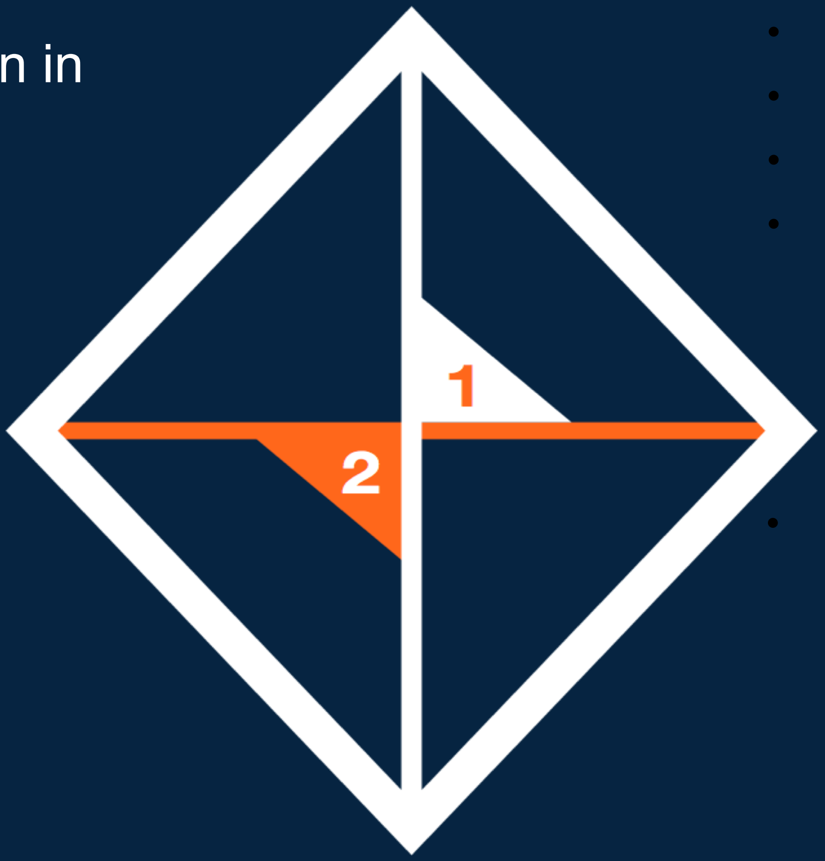
- Seeking to obtain high end Western Beers for production in their breweries

## ADVERSARY

- Nation-state sponsored adversary
- Located (+8.5 timezone)
- Uses Korean encoded language
- Uses Hancom Thinkfree Office

## CAPABILITIES

- PowerShell Empire
- Spearphishing



## INFRASTRUCTURE

- European VPS servers

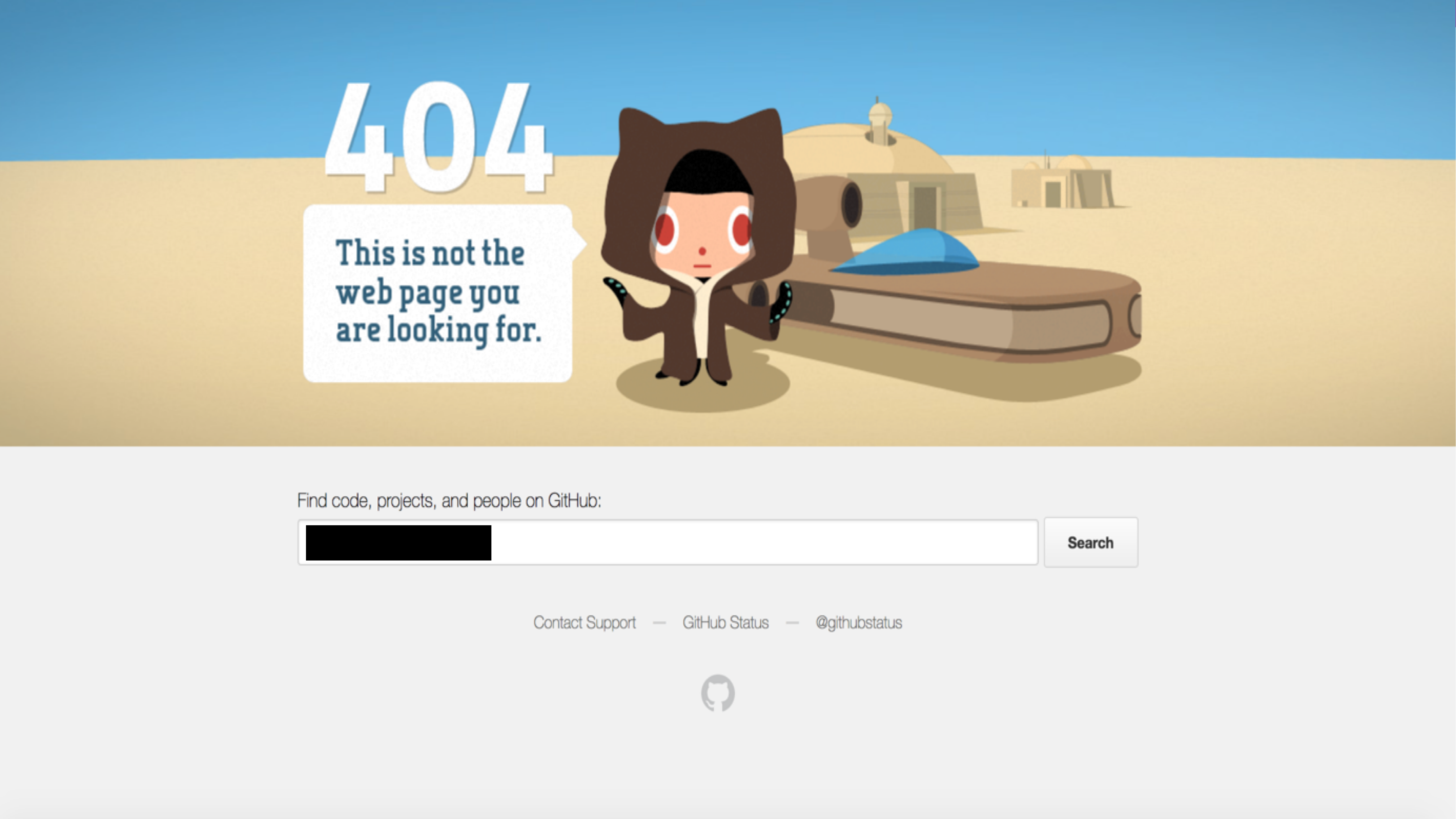
## 2 TECHNICAL AXIS

- Documents with .hwp suffix
- PS exec lateral movement
- YMLP
- Self signed SSL/TLS certificates
- +8.5 hour time zone
- Korean fonts for English
- Korean text google translated to English
- Naenara useragent string

## VICTIMS

- Western innovative Brewers and Home Brewing companies

*A special thanks to* THREATCONNECT



404

This is not the web page you are looking for.

Find code, projects, and people on GitHub:

[redacted]

Contact Support — GitHub Status — @githubstatus

USA MEX
ONE SIZE DOES NOT FIT ALL
30°C
Von links bügeln/
repasser

A different time for a specific use case

# Inflexible

RESEARCHER
KNOWLEDGE
CIRCUMSTANCES
CASE STUDY
CRITERIA
CASE
DATA
ANALYZING

CYBER
KILL CHAIN

MAHA

So cyber looked for something different

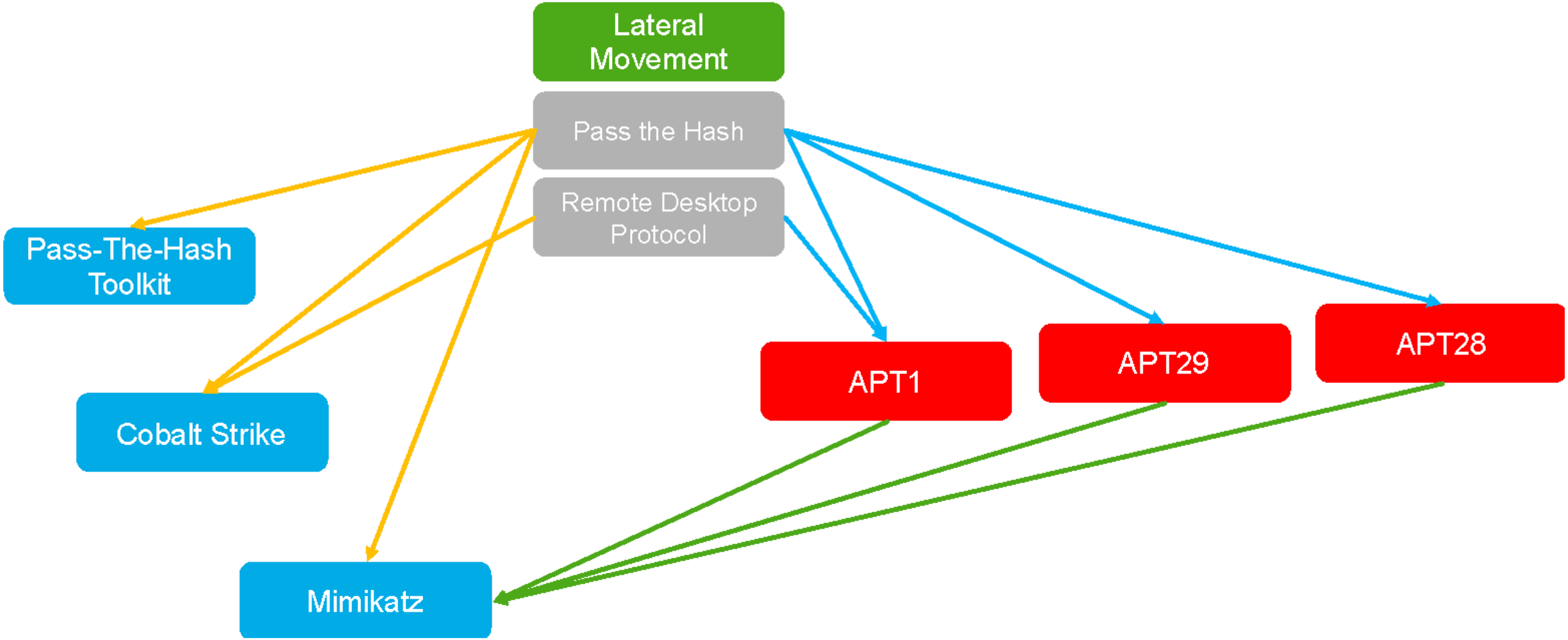
# MITRE

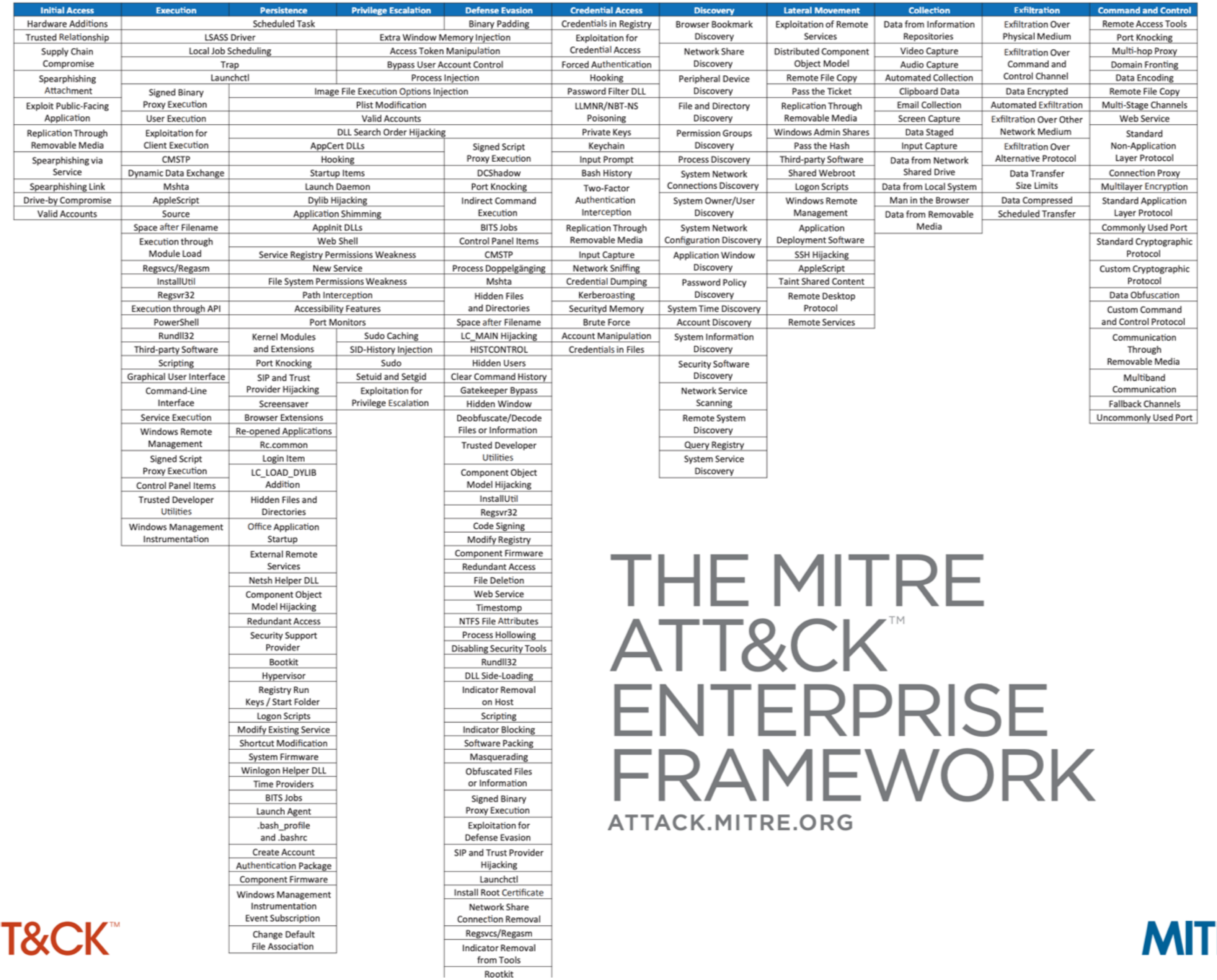
# ATTACK!!!

# MITRE | ATT&CK™

# How you can hunt with MITRE ATT&CK

# Tactic, Techniques, Adversaries and Software





| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control |
|---|---|---|---|---|---|---|---|---|---|---|
| Hardware Additions | Scheduled Task | Scheduled Task | Scheduled Task | Binary Padding | Credentials in Registry | Browser Bookmark Discovery | Exploitation of Remote Services | Data from Information Repositories | Exfiltration Over Physical Medium | Remote Access Tools |
| Trusted Relationship | LSASS Driver | LSASS Driver | Extra Window Memory Injection | Extra Window Memory Injection | Exploitation for Credential Access | Network Share Discovery | Distributed Component Object Model | Video Capture | Exfiltration Over Command and Control Channel | Port Knocking |
| Supply Chain Compromise | Local Job Scheduling | Local Job Scheduling | Access Token Manipulation | Access Token Manipulation | Forced Authentication | Peripheral Device Discovery | Remote File Copy | Audio Capture | Data Encrypted | Multi-hop Proxy |
| Spearphishing Attachment | Trap | Trap | Bypass User Account Control | Bypass User Account Control | Hooking | File and Directory Discovery | Pass the Ticket | Automated Collection | Automated Exfiltration | Domain Fronting |
| Exploit Public-Facing Application | Launchctl | Launchctl | Process Injection | Process Injection | Password Filter DLL | Permission Groups Discovery | Replication Through Removable Media | Clipboard Data | Exfiltration Over Other Network Medium | Data Encoding |
| Replication Through Removable Media | Signed Binary Proxy Execution | Image File Execution Options Injection | Image File Execution Options Injection | Image File Execution Options Injection | LLMNR/NBT-NS Poisoning | Process Discovery | Windows Admin Shares | Email Collection | Exfiltration Over Alternative Protocol | Remote File Copy |
| Spearphishing via Service | User Execution | Plist Modification | Plist Modification | Plist Modification | Private Keys | System Network Connections Discovery | Pass the Hash | Screen Capture | Data Transfer Size Limits | Multi-Stage Channels |
| Spearphishing Link | Exploitation for Client Execution | Valid Accounts | Valid Accounts | Valid Accounts | Keychain | System Owner/User Discovery | Third-party Software | Data Staged | Data Compressed | Web Service |
| Drive-by Compromise | CMSTP | DLL Search Order Hijacking | DLL Search Order Hijacking | DLL Search Order Hijacking | Input Prompt | System Network Configuration Discovery | Shared Webroot | Input Capture | Scheduled Transfer | Standard Non-Application Layer Protocol |
| Valid Accounts | Dynamic Data Exchange | AppCert DLLs | AppCert DLLs | Signed Script Proxy Execution | Bash History | Application Window Discovery | Logon Scripts | Data from Network Shared Drive | | Connection Proxy |
| | Mshta | Hooking | Hooking | DCShadow | Two-Factor Authentication Interception | Password Policy Discovery | Windows Remote Management | Data from Local System | | Multilayer Encryption |
| | AppleScript | Startup Items | Startup Items | Port Knocking | Replication Through Removable Media | System Time Discovery | Application Deployment Software | Man in the Browser | | Standard Application Layer Protocol |
| | Source | Launch Daemon | Launch Daemon | Indirect Command Execution | Input Capture | Account Discovery | SSH Hijacking | Data from Removable Media | | Commonly Used Port |
| | Space after Filename | Dylib Hijacking | Dylib Hijacking | BITS Jobs | Network Sniffing | System Information Discovery | AppleScript | | | Standard Cryptographic Protocol |
| | Execution through Module Load | Application Shimming | Application Shimming | Control Panel Items | Credential Dumping | Security Software Discovery | Taint Shared Content | | | Custom Cryptographic Protocol |
| | Regsvcs/Regasm | AppInit DLLs | AppInit DLLs | CMSTP | Kerberoasting | Network Service Scanning | Remote Desktop Protocol | | | Data Obfuscation |
| | InstallUtil | Web Shell | Web Shell | Process Doppelgänging | Securityd Memory | Remote System Discovery | Remote Services | | | Custom Command and Control Protocol |
| | Regsvr32 | Service Registry Permissions Weakness | Service Registry Permissions Weakness | Mshta | Brute Force | Query Registry | | | | Communication Through Removable Media |
| | Execution through API | New Service | New Service | Hidden Files and Directories | Account Manipulation | System Service Discovery | | | | Multiband Communication |
| | PowerShell | File System Permissions Weakness | File System Permissions Weakness | Space after Filename | Credentials in Files | | | | | Fallback Channels |
| | Rundll32 | Path Interception | Path Interception | LC_MAIN Hijacking | | | | | | Uncommonly Used Port |
| | Third-party Software | Accessibility Features | Accessibility Features | HISTCONTROL | | | | | | |
| | Scripting | Port Monitors | Port Monitors | Hidden Users | | | | | | |
| | Graphical User Interface | Kernel Modules and Extensions | Sudo Caching | Clear Command History | | | | | | |
| | Command-Line Interface | Port Knocking | SID-History Injection | Gatekeeper Bypass | | | | | | |
| | Service Execution | SIP and Trust Provider Hijacking | Sudo | Hidden Window | | | | | | |
| | Windows Remote Management | Screensaver | Setuid and Setgid | Deobfuscate/Decode Files or Information | | | | | | |
| | Signed Script Proxy Execution | Browser Extensions | Exploitation for Privilege Escalation | Trusted Developer Utilities | | | | | | |
| | Control Panel Items | Re-opened Applications | | Component Object Model Hijacking | | | | | | |
| | Trusted Developer Utilities | Rc.common | | InstallUtil | | | | | | |
| | Windows Management Instrumentation | Login Item | | Regsvr32 | | | | | | |
| | | LC_LOAD_DYLIB Addition | | Code Signing | | | | | | |
| | | Hidden Files and Directories | | Modify Registry | | | | | | |
| | | Office Application Startup | | Component Firmware | | | | | | |
| | | External Remote Services | | Redundant Access | | | | | | |
| | | Netsh Helper DLL | | File Deletion | | | | | | |
| | | Component Object Model Hijacking | | Web Service | | | | | | |
| | | Redundant Access | | Timestomp | | | | | | |
| | | Security Support Provider | | NTFS File Attributes | | | | | | |
| | | Bootkit | | Process Hollowing | | | | | | |
| | | Hypervisor | | Disabling Security Tools | | | | | | |
| | | Registry Run Keys / Start Folder | | Rundll32 | | | | | | |
| | | Logon Scripts | | DLL Side-Loading | | | | | | |
| | | Modify Existing Service | | Indicator Removal on Host | | | | | | |
| | | Shortcut Modification | | Scripting | | | | | | |
| | | System Firmware | | Indicator Blocking | | | | | | |
| | | Winlogon Helper DLL | | Software Packing | | | | | | |
| | | Time Providers | | Masquerading | | | | | | |
| | | BITS Jobs | | Obfuscated Files or Information | | | | | | |
| | | Launch Agent | | Signed Binary Proxy Execution | | | | | | |
| | | .bash_profile and .bashrc | | Exploitation for Defense Evasion | | | | | | |
| | | Create Account | | SIP and Trust Provider Hijacking | | | | | | |
| | | Authentication Package | | Launchctl | | | | | | |
| | | Component Firmware | | Install Root Certificate | | | | | | |
| | | Windows Management Instrumentation Event Subscription | | Network Share Connection Removal | | | | | | |
| | | Change Default File Association | | Regsvcs/Regasm | | | | | | |
| | | | | Indicator Removal from Tools | | | | | | |
| | | | | Rootkit | | | | | | |

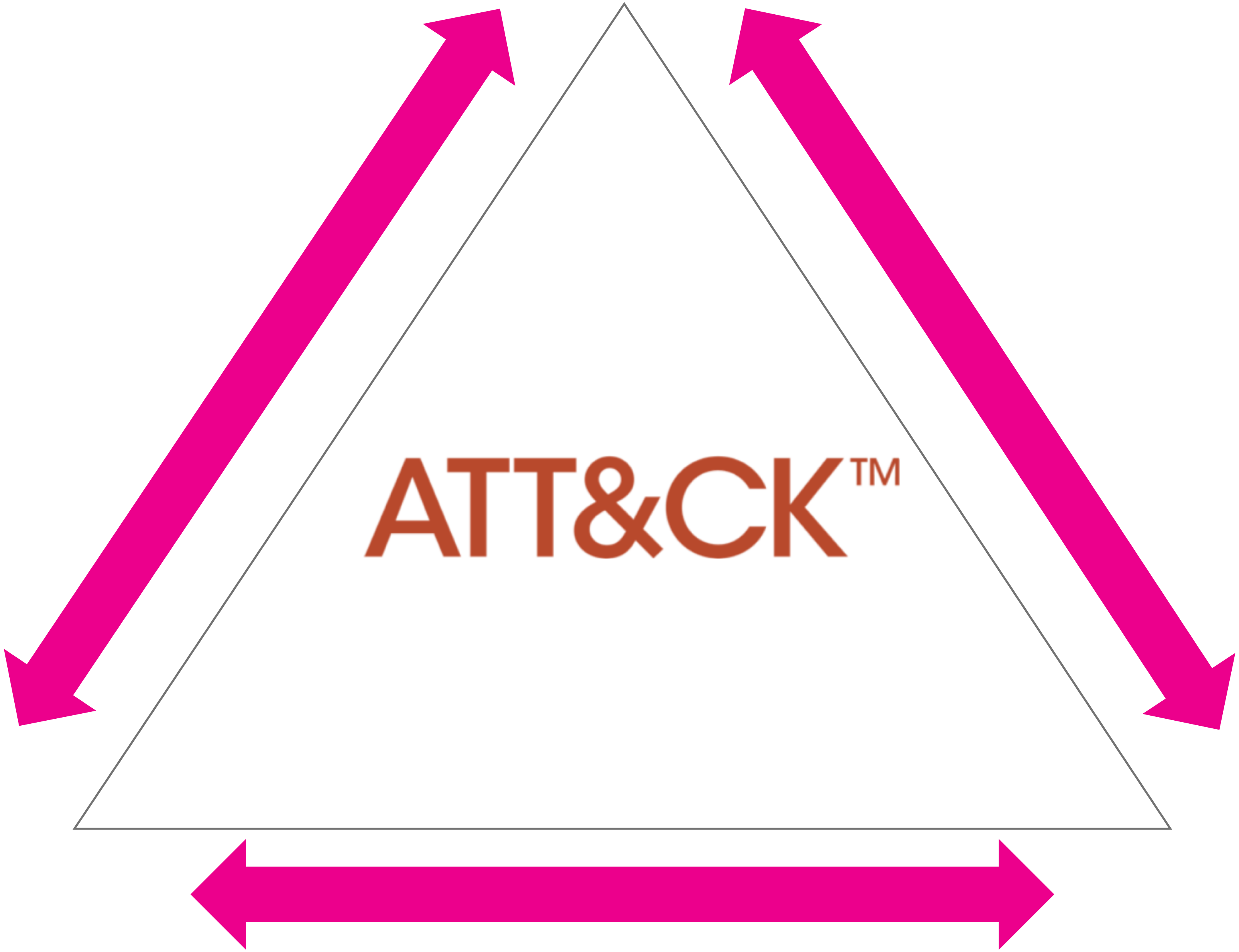
# THE MITRE ATT&CK™ ENTERPRISE FRAMEWORK

ATTACK.MITRE.ORG

ATT&CK™

MITRE

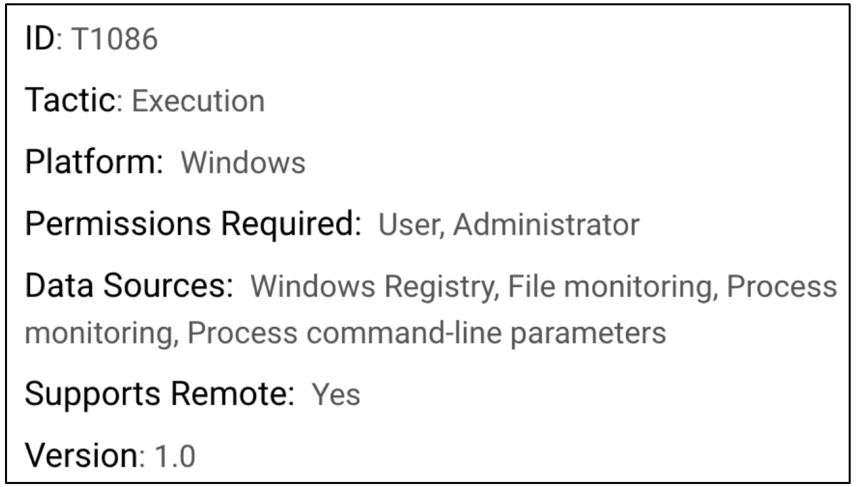
Threat Hunting



Threat Intelligence

Security Operations

# Using ATT&CK Techniques To Build Our Hypothesis - PowerShell



ID: T1086

Tactic: Execution

Platform: Windows

Permissions Required: User, Administrator

Data Sources: Windows Registry, File monitoring, Process monitoring, Process command-line parameters

Supports Remote: Yes

Version: 1.0

**https://attack.mitre.org/wiki/Technique/T1086**

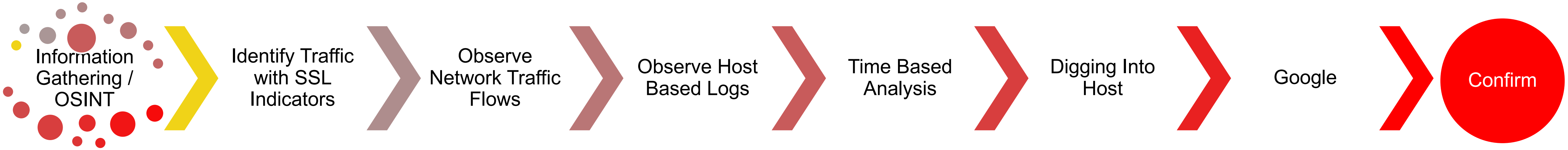
Adversaries will use PowerShell Empire to establish a foothold and carry out attacks

# How Might We Confirm or Refute Our Hypothesis?

- What is PowerShell?
- Where can I learn more about PowerShell Empire?
- Does PowerShell Empire have default settings that I could hunt for?
- What do data flows look like between sources and destinations?
- What user accounts are being used?
- What ports are being used?
- When did events occur?
- Are we able to see the contents of the scripts PowerShell is running to gain greater understanding?

Would you classify that as a launch problem, or a design problem?

# Notional Flow of PSE Hunt



Information Gathering / OSINT

Indicators in SSL

Identify Traffic with SSL Indicators

Pivot to Find Internal/External IPs

Observe Network Traffic Flows

- Firewall/IDS/ Wire
- User Agent Strings
- Domains

Observe Host Based Logs

- Network Indicators
- Host attributes (User, Event Descriptions)

Time Based Analysis

- Unique combinations of user/systems
- Pivot into specific users/systems of interest

Digging Into Host

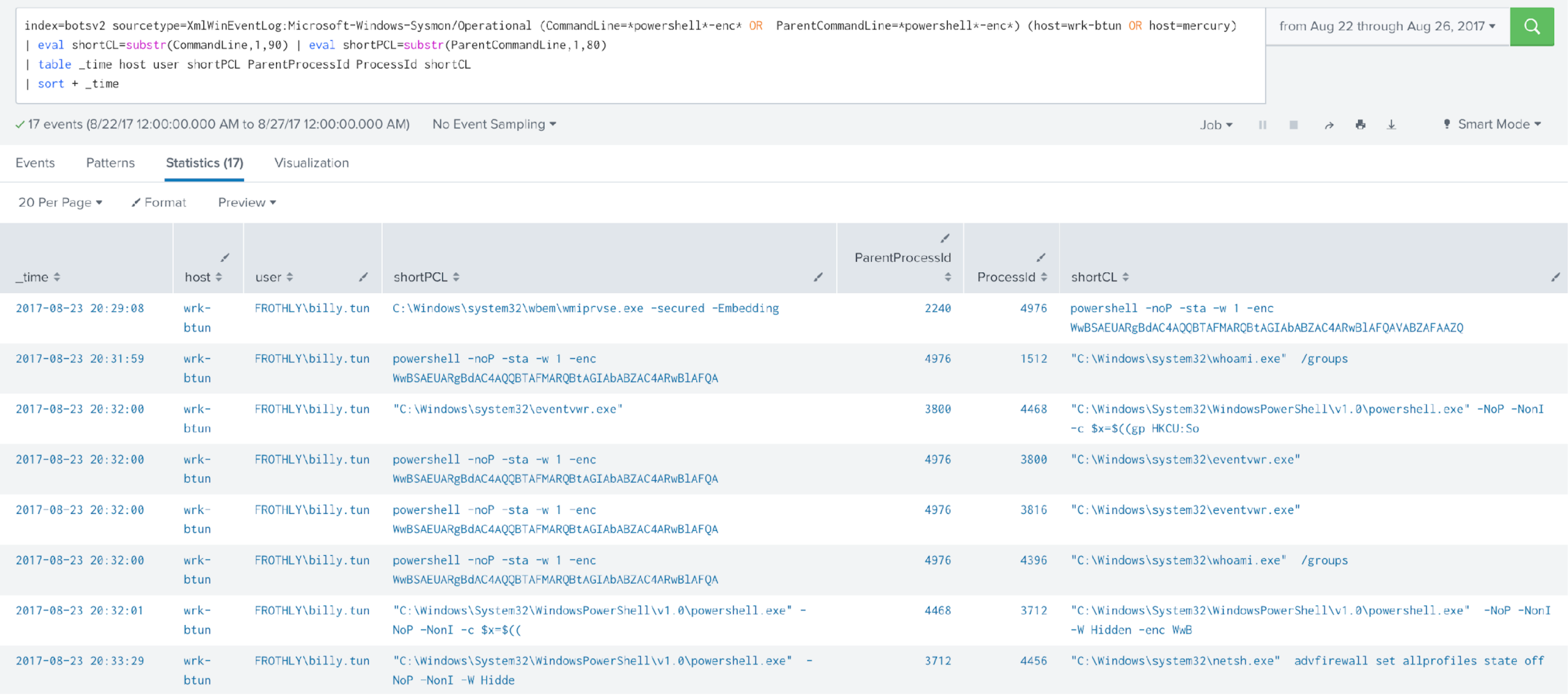
- Map interesting processes
- Additional attributes: Parent Processes, Encoding, accounts used, sequencing of commands

Google

- Research commands uncovered
- Compare commands executed on systems

Confirm

# Chaining Events Together

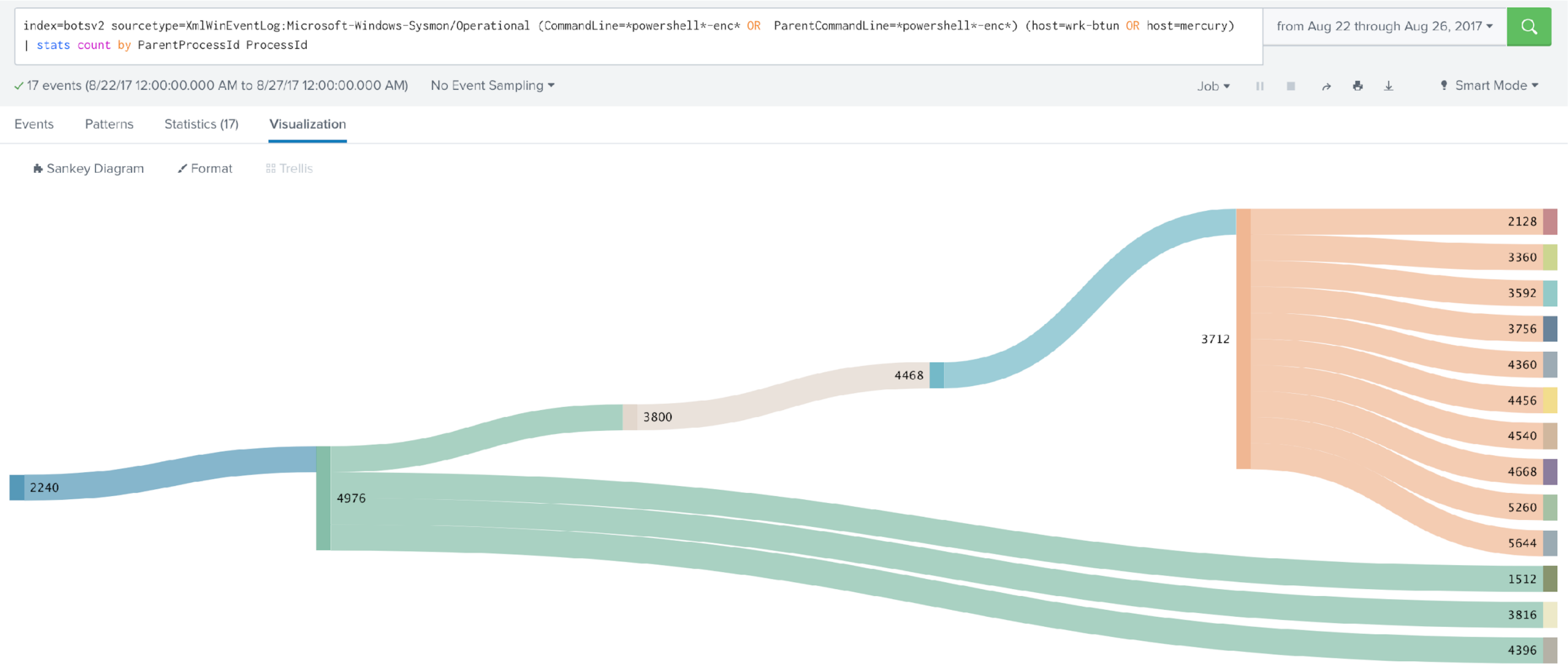


```
index=botsv2 sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational (CommandLine=*powershell*-enc* OR  ParentCommandLine=*powershell*-enc*) (host=wrk-btun OR host=mercury)
| eval shortCL=substr(CommandLine,1,90) | eval shortPCL=substr(ParentCommandLine,1,80)
| table _time host user shortPCL ParentProcessId ProcessId shortCL
| sort + _time
```

| _time | host | user | shortPCL | ParentProcessId | ProcessId | shortCL |
|---|---|---|---|---|---|---|
| 2017-08-23 20:29:08 | wrk-btun | FROTHLY\billy.tun | C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding | 2240 | 4976 | powershell -noP -sta -w 1 -enc WwBSAEUARgBdAC4AQQBTAFMARQBtAGIAbABZAC4ARwBlAFQAVABZAFAAZQ |
| 2017-08-23 20:31:59 | wrk-btun | FROTHLY\billy.tun | powershell -noP -sta -w 1 -enc WwBSAEUARgBdAC4AQQBTAFMARQBtAGIAbABZAC4ARwBlAFQA | 4976 | 1512 | "C:\Windows\system32\whoami.exe" /groups |
| 2017-08-23 20:32:00 | wrk-btun | FROTHLY\billy.tun | "C:\Windows\system32\eventvwr.exe" | 3800 | 4468 | "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoP -NonI -c $x=$((gp HKCU:So |
| 2017-08-23 20:32:00 | wrk-btun | FROTHLY\billy.tun | powershell -noP -sta -w 1 -enc WwBSAEUARgBdAC4AQQBTAFMARQBtAGIAbABZAC4ARwBlAFQA | 4976 | 3800 | "C:\Windows\system32\eventvwr.exe" |
| 2017-08-23 20:32:00 | wrk-btun | FROTHLY\billy.tun | powershell -noP -sta -w 1 -enc WwBSAEUARgBdAC4AQQBTAFMARQBtAGIAbABZAC4ARwBlAFQA | 4976 | 3816 | "C:\Windows\system32\eventvwr.exe" |
| 2017-08-23 20:32:00 | wrk-btun | FROTHLY\billy.tun | powershell -noP -sta -w 1 -enc WwBSAEUARgBdAC4AQQBTAFMARQBtAGIAbABZAC4ARwBlAFQA | 4976 | 4396 | "C:\Windows\system32\whoami.exe" /groups |
| 2017-08-23 20:32:01 | wrk-btun | FROTHLY\billy.tun | "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoP -NonI -c $x=$(( | 4468 | 3712 | "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoP -NonI -W Hidden -enc WwB |
| 2017-08-23 20:33:29 | wrk-btun | FROTHLY\billy.tun | "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoP -NonI -W Hidde | 3712 | 4456 | "C:\Windows\system32\netsh.exe" advfirewall set allprofiles state off |

# Visualizing the Chaining of Events

## Parent Process IDs and Process IDs



```
index=botsv2 sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational (CommandLine=*powershell*-enc* OR  ParentCommandLine=*powershell*-enc*) (host=wrk-btun OR host=mercury)
| stats count by ParentProcessId ProcessId
```

from Aug 22 through Aug 26, 2017

✓ 17 events (8/22/17 12:00:00.000 AM to 8/27/17 12:00:00.000 AM)

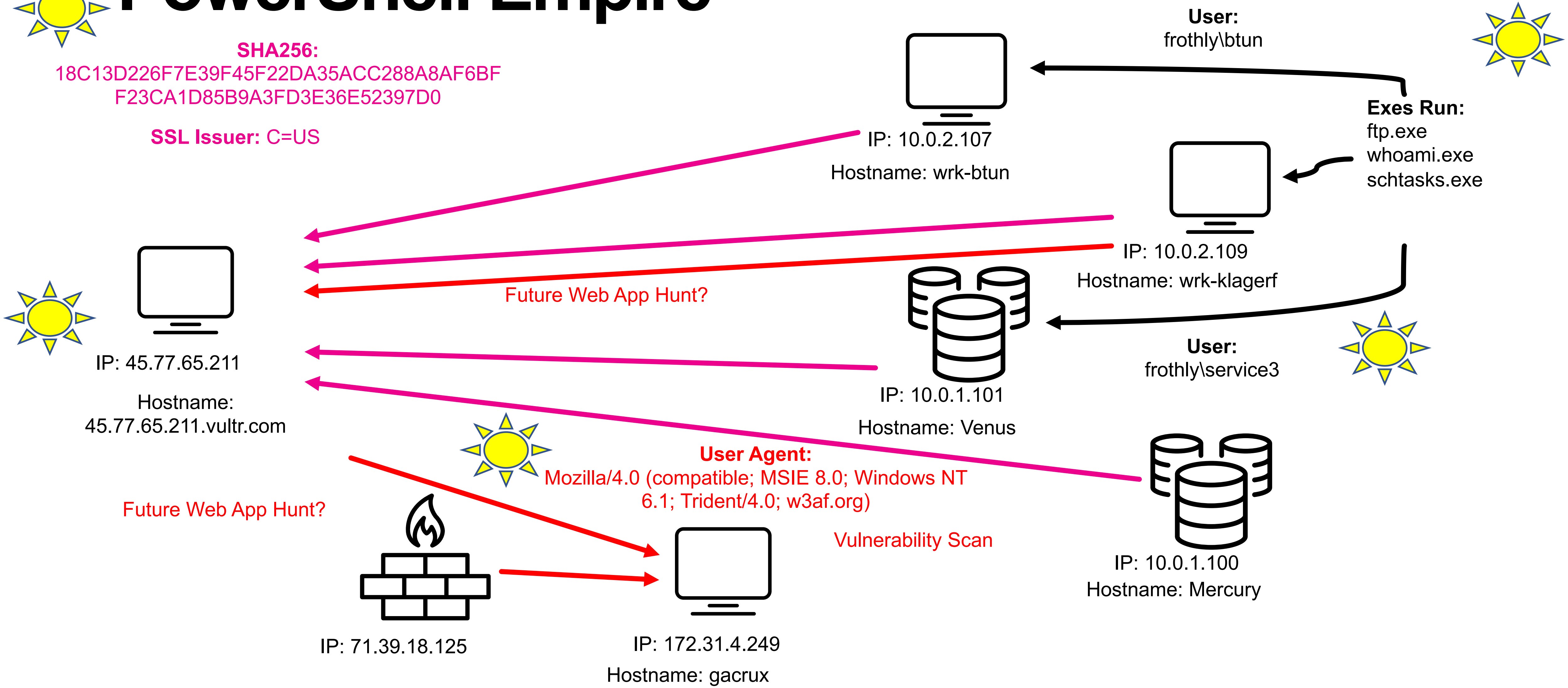
No Event Sampling

Smart Mode

# PowerShell Empire

**SHA256:**
18C13D226F7E39F45F22DA35ACC288A8AF6BF
F23CA1D85B9A3FD3E36E52397D0

**SSL Issuer:** C=US



**User:**
frothly\btun

IP: 10.0.2.107
Hostname: wrk-btun

**Exes Run:**
ftp.exe
whoami.exe
schtasks.exe

IP: 10.0.2.109
Hostname: wrk-klagerf

IP: 45.77.65.211
Hostname:
45.77.65.211.vultr.com

Future Web App Hunt?

IP: 10.0.1.101
Hostname: Venus

**User:**
frothly\service3

**User Agent:**
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; w3af.org)

Future Web App Hunt?

Vulnerability Scan

IP: 10.0.1.100
Hostname: Mercury

IP: 71.39.18.125

IP: 172.31.4.249
Hostname: gacrux

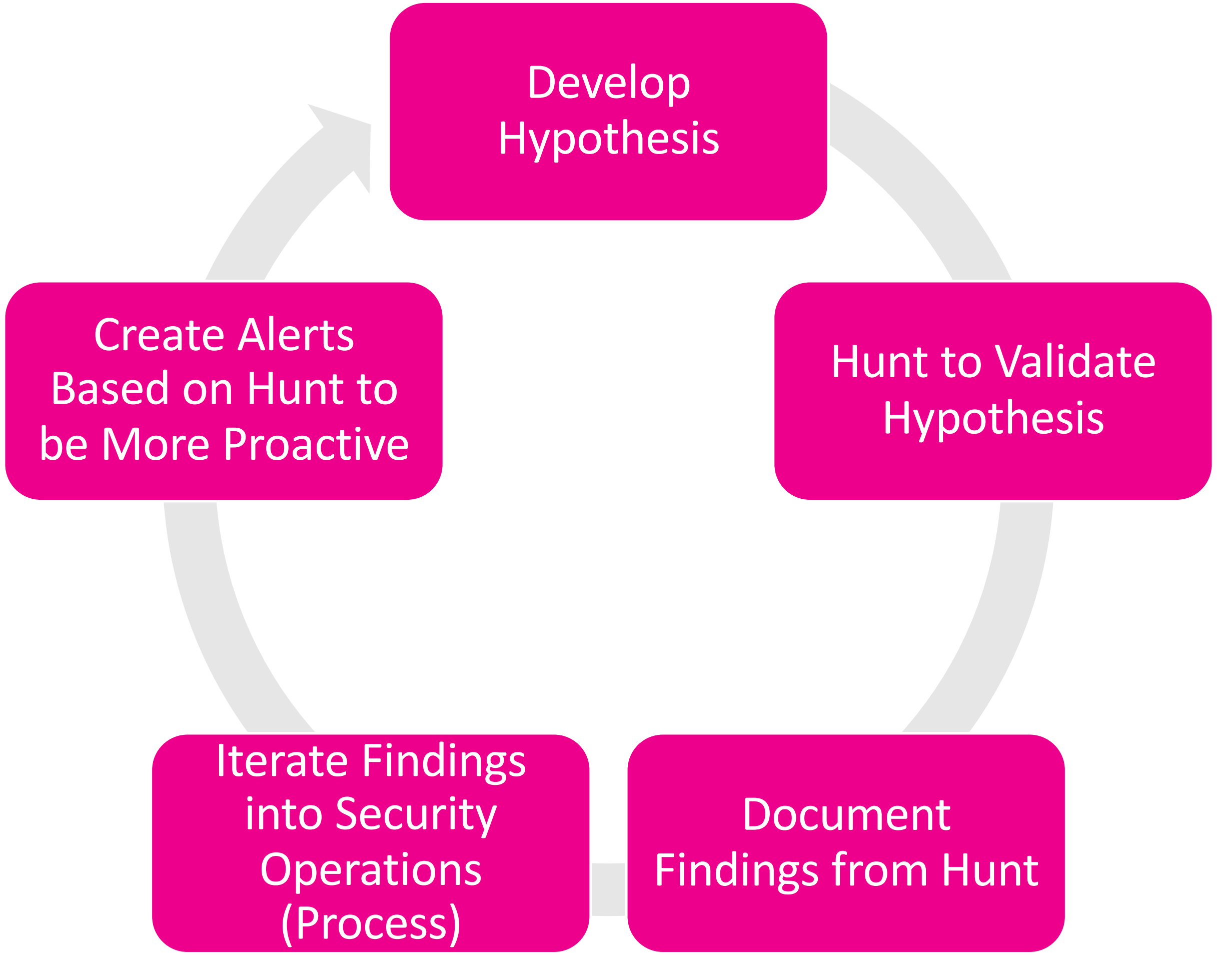
# Operationalizing ATT&CK with Splunk

# Operationalize Your Findings

Create Feedback Loop from Hunting to Incident Response

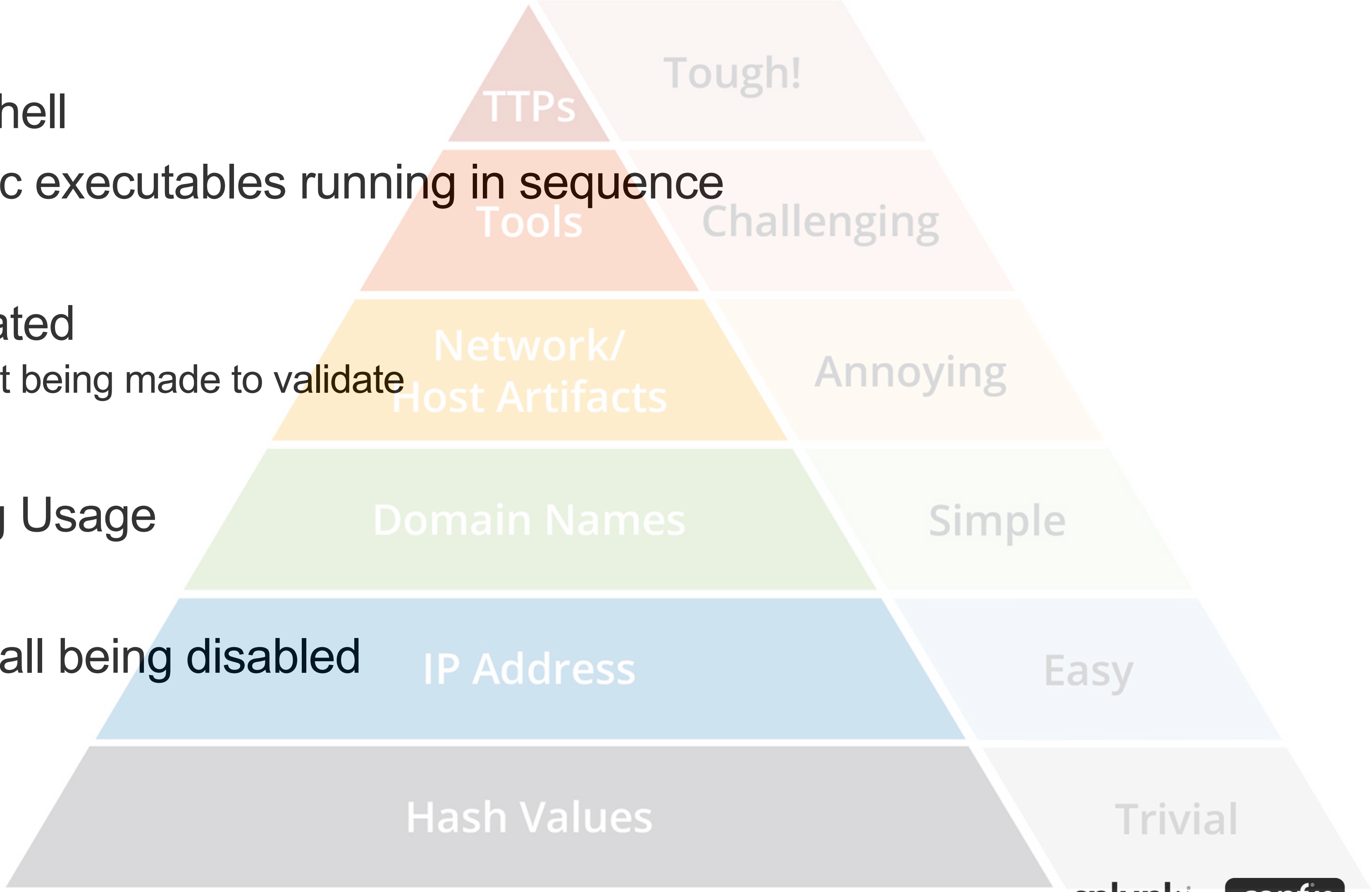
“End goal of hunting should be a change in policy or procedure - operationalization, don’t do the same thing over and over again”

- Threat Hunting Webshells with Splunk, James Bower


Develop Hypothesis
Hunt to Validate Hypothesis
Document Findings from Hunt
Iterate Findings into Security Operations (Process)
Create Alerts Based on Hunt to be More Proactive

# What Could We Operationalize?

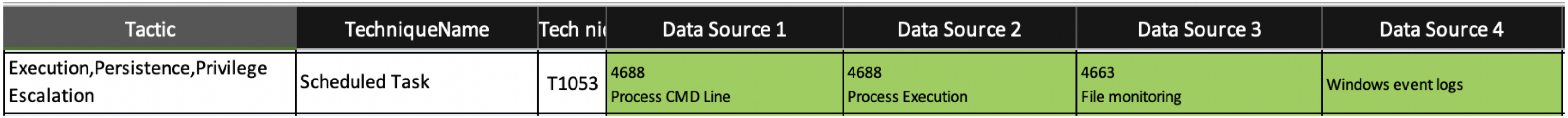
- Alert on encoded Powershell
- Alert when we see specific executables running in sequence
- Alert on SSL Issuer
- Detect new accounts created
  - Have a ticket to reference it being made to validate
- Blacklist IP Address
- Monitor User Agent String Usage
- Monitor for URIs
- Monitor and alert on firewall being disabled



Source: David J. Bianco, personal blog

# Considerations when operationalizing ATT&CK

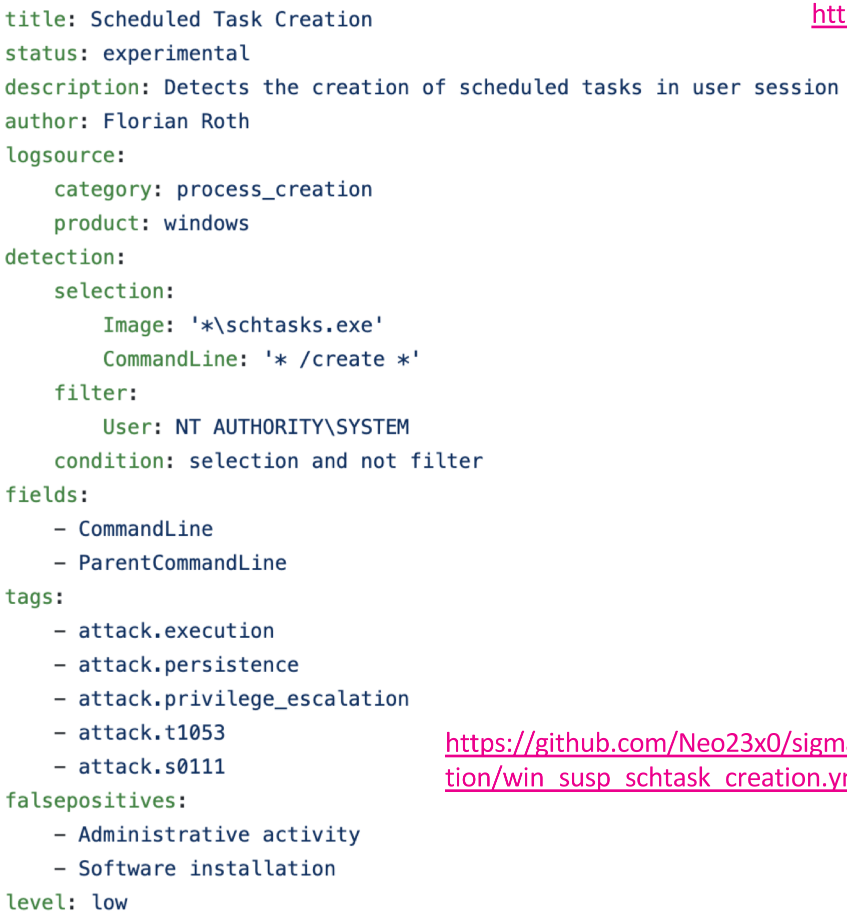
# Example: Scheduled Task (T1053)



| Tactic | TechniqueName | Tech ni | Data Source 1 | Data Source 2 | Data Source 3 | Data Source 4 |
|---|---|---|---|---|---|---|
| Execution,Persistence,Privilege Escalation | Scheduled Task | T1053 | 4688<br>Process CMD Line | 4688<br>Process Execution | 4663<br>File monitoring | Windows event logs |

"Monitor scheduled task creation from common utilities using command-line invocation. Legitimate scheduled tasks may be created during installation of new software or through system administration functions. Monitor process execution from the svchost.exe in Windows 10 and the Windows Task Scheduler taskeng.exe for older versions of Windows."

https://attack.mitre.org/techniques/T1053/



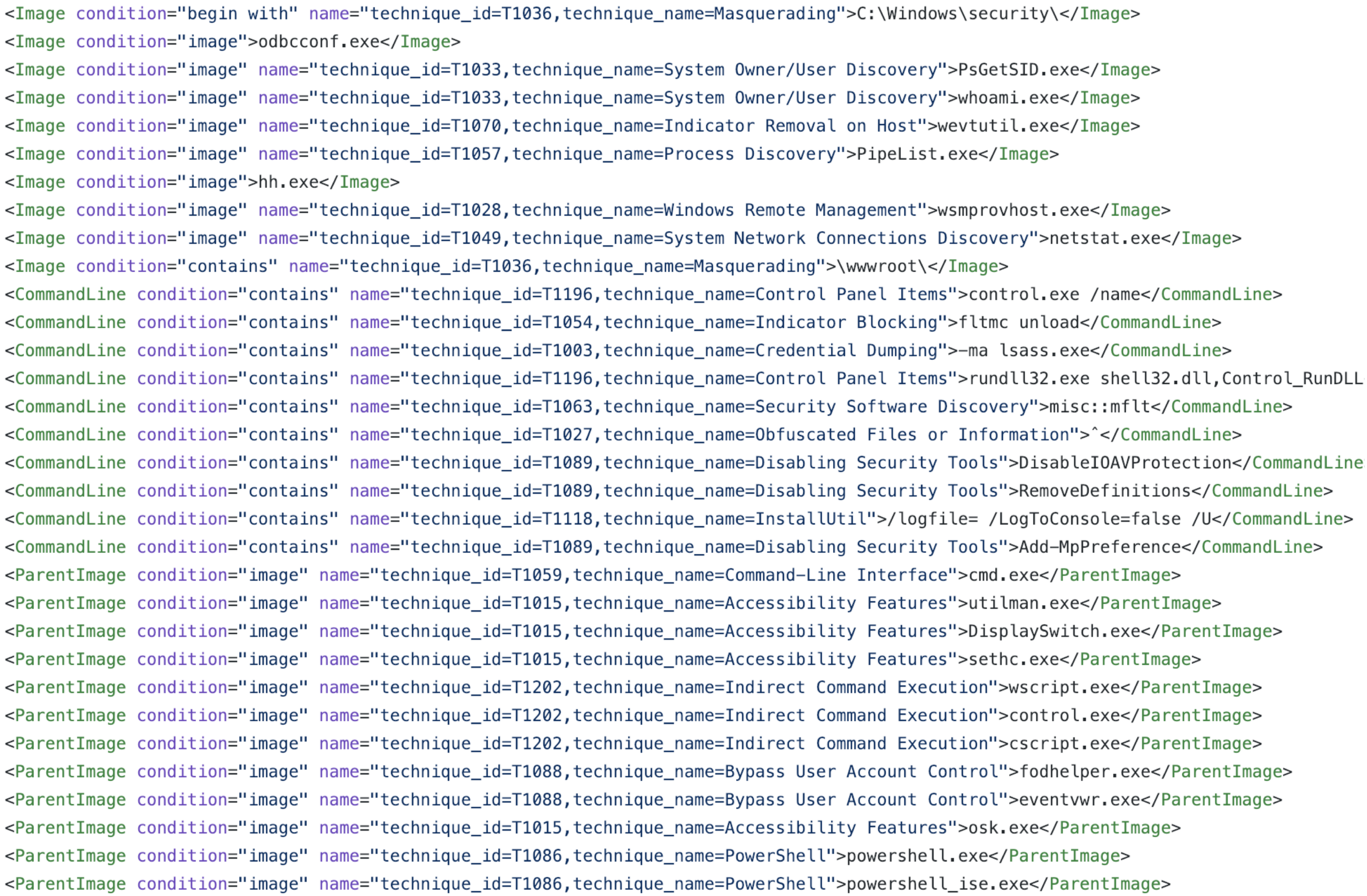
```
title: Scheduled Task Creation
status: experimental
description: Detects the creation of scheduled tasks in user session
author: Florian Roth
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        Image: '*\schtasks.exe'
        CommandLine: '* /create *'
    filter:
        User: NT AUTHORITY\SYSTEM
    condition: selection and not filter
fields:
    - CommandLine
    - ParentCommandLine
tags:
    - attack.execution
    - attack.persistence
    - attack.privilege_escalation
    - attack.t1053
    - attack.s0111
falsepositives:
    - Administrative activity
    - Software installation
level: low
```

https://www.malwarearchaeology.com/cheat-sheets

https://github.com/Neo23x0/sigma/blob/master/rules/windows/process_creation/win_susp_schtask_creation.yml

# Operationalizing Technique (Scheduled Tasks)

- Monitor for
  - Schtasks.exe that deviate from an IT baseline
    - Need excellent coordination with IT to build lookup of standard tasks to look for outliers
    - Could be noisy depending on the frequency
  - Scheduled task names that don’t match with the IT standard
    - Compromised system could be using an IT standard and this would not be seen
  - Scheduled tasks running under unexpected users
    - Should tasks run as system or as a named user?
  - Scheduled tasks that have command strings out of the normal
    - Should PowerShell scripts be running as scheduled tasks, for some organizations yes, for others no



```
<Image condition="begin with" name="technique_id=T1036,technique_name=Masquerading">C:\Windows\security\</Image>
<Image condition="image">odbcconf.exe</Image>
<Image condition="image" name="technique_id=T1033,technique_name=System Owner/User Discovery">PsGetSID.exe</Image>
<Image condition="image" name="technique_id=T1033,technique_name=System Owner/User Discovery">whoami.exe</Image>
<Image condition="image" name="technique_id=T1070,technique_name=Indicator Removal on Host">wevtutil.exe</Image>
<Image condition="image" name="technique_id=T1057,technique_name=Process Discovery">PipeList.exe</Image>
<Image condition="image">hh.exe</Image>
<Image condition="image" name="technique_id=T1028,technique_name=Windows Remote Management">wsmprovhost.exe</Image>
<Image condition="image" name="technique_id=T1049,technique_name=System Network Connections Discovery">netstat.exe</Image>
<Image condition="contains" name="technique_id=T1036,technique_name=Masquerading">\wwwroot\</Image>
<CommandLine condition="contains" name="technique_id=T1196,technique_name=Control Panel Items">control.exe /name</CommandLine>
<CommandLine condition="contains" name="technique_id=T1054,technique_name=Indicator Blocking">fltmc unload</CommandLine>
<CommandLine condition="contains" name="technique_id=T1003,technique_name=Credential Dumping">-ma lsass.exe</CommandLine>
<CommandLine condition="contains" name="technique_id=T1196,technique_name=Control Panel Items">rundll32.exe shell32.dll,Control_RunDLL
<CommandLine condition="contains" name="technique_id=T1063,technique_name=Security Software Discovery">misc::mflt</CommandLine>
<CommandLine condition="contains" name="technique_id=T1027,technique_name=Obfuscated Files or Information">^</CommandLine>
<CommandLine condition="contains" name="technique_id=T1089,technique_name=Disabling Security Tools">DisableIOAVProtection</CommandLine
<CommandLine condition="contains" name="technique_id=T1089,technique_name=Disabling Security Tools">RemoveDefinitions</CommandLine>
<CommandLine condition="contains" name="technique_id=T1118,technique_name=InstallUtil">/logfile= /LogToConsole=false /U</CommandLine>
<CommandLine condition="contains" name="technique_id=T1089,technique_name=Disabling Security Tools">Add-MpPreference</CommandLine>
<ParentImage condition="image" name="technique_id=T1059,technique_name=Command-Line Interface">cmd.exe</ParentImage>
<ParentImage condition="image" name="technique_id=T1015,technique_name=Accessibility Features">utilman.exe</ParentImage>
<ParentImage condition="image" name="technique_id=T1015,technique_name=Accessibility Features">DisplaySwitch.exe</ParentImage>
<ParentImage condition="image" name="technique_id=T1015,technique_name=Accessibility Features">sethc.exe</ParentImage>
<ParentImage condition="image" name="technique_id=T1202,technique_name=Indirect Command Execution">wscript.exe</ParentImage>
<ParentImage condition="image" name="technique_id=T1202,technique_name=Indirect Command Execution">control.exe</ParentImage>
<ParentImage condition="image" name="technique_id=T1202,technique_name=Indirect Command Execution">cscript.exe</ParentImage>
<ParentImage condition="image" name="technique_id=T1088,technique_name=Bypass User Account Control">fodhelper.exe</ParentImage>
<ParentImage condition="image" name="technique_id=T1088,technique_name=Bypass User Account Control">eventvwr.exe</ParentImage>
<ParentImage condition="image" name="technique_id=T1015,technique_name=Accessibility Features">osk.exe</ParentImage>
<ParentImage condition="image" name="technique_id=T1086,technique_name=PowerShell">powershell.exe</ParentImage>
<ParentImage condition="image" name="technique_id=T1086,technique_name=PowerShell">powershell_ise.exe</ParentImage>
```

```
<Image condition="begin with" name="technique_id=T1036,technique_name=Masquerading">C:\Windows\security\</Image>
<Image condition="image">odbcconf.exe</Image>
<Image condition="image" name="technique_id=T1033,technique_name=System Owner/User Discovery">PsGetSID.exe</Image>
<Image condition="image" name="technique_id=T1033,technique_name=System Owner/User Discovery">whoami.exe</Image>
<Image condition="image" name="technique_id=T1070,technique_name=Indicator Removal on Host">wevtutil.exe</Image>
<Image condition="image" name="technique_id=T1057,technique_name=Process Discovery">PipeList.exe</Image>
<Image condition="image">hh.exe</Image>
```

```
<Image condition="image" name="technique_id=T1070,technique_name=Indicator Removal on Host">wevtutil.exe</Image>
```

```
<Image condition="image" name="technique_id=T1049,technique_name=System Network Connections Discovery">netstat.exe</Image>
<Image condition="contains" name="technique_id=T1036,technique_name=Masquerading">\wwwroot\</Image>
<CommandLine condition="contains" name="technique_id=T1196,technique_name=Control Panel Items">control.exe /name</CommandLine>
<CommandLine condition="contains" name="technique_id=T1054,technique_name=Indicator Blocking">fltmc unload</CommandLine>
<CommandLine condition="contains" name="technique_id=T1003,technique_name=Credential Dumping">-ma lsass.exe</CommandLine>
<CommandLine condition="contains" name="technique_id=T1196,technique_name=Control Panel Items">rundll32.exe shell32.dll,Control_RunDLL
```

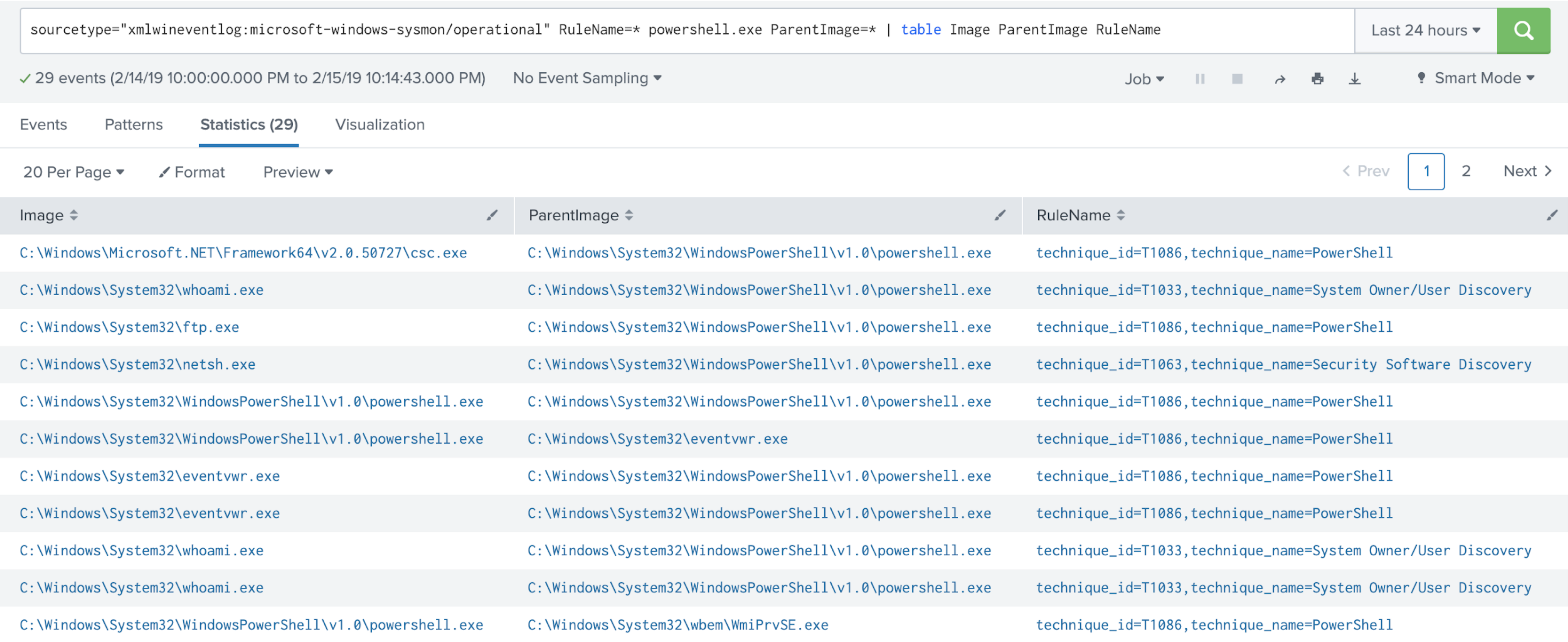
```
<CommandLine condition="contains" name="technique_id=T1089,technique_name=Disabling Security Tools">RemoveDefinitions</CommandLine>
```

```
<CommandLine condition="contains" name="technique_id=T1027,technique_name=Obfuscated Files or Information">^</CommandLine>
<CommandLine condition="contains" name="technique_id=T1089,technique_name=Disabling Security Tools">DisableIOAVProtection</CommandLine
<CommandLine condition="contains" name="technique_id=T1089,technique_name=Disabling Security Tools">RemoveDefinitions</CommandLine>
<CommandLine condition="contains" name="technique_id=T1118,technique_name=InstallUtil">/logfile= /LogToConsole=false /U</CommandLine>
<CommandLine condition="contains" name="technique_id=T1089,technique_name=Disabling Security Tools">Add-MpPreference</CommandLine>
<ParentImage condition="image" name="technique_id=T1059,technique_name=Command-Line Interface">cmd.exe</ParentImage>
```

```
<ParentImage condition="image" name="technique_id=T1086,technique_name=PowerShell">powershell.exe</ParentImage>
```

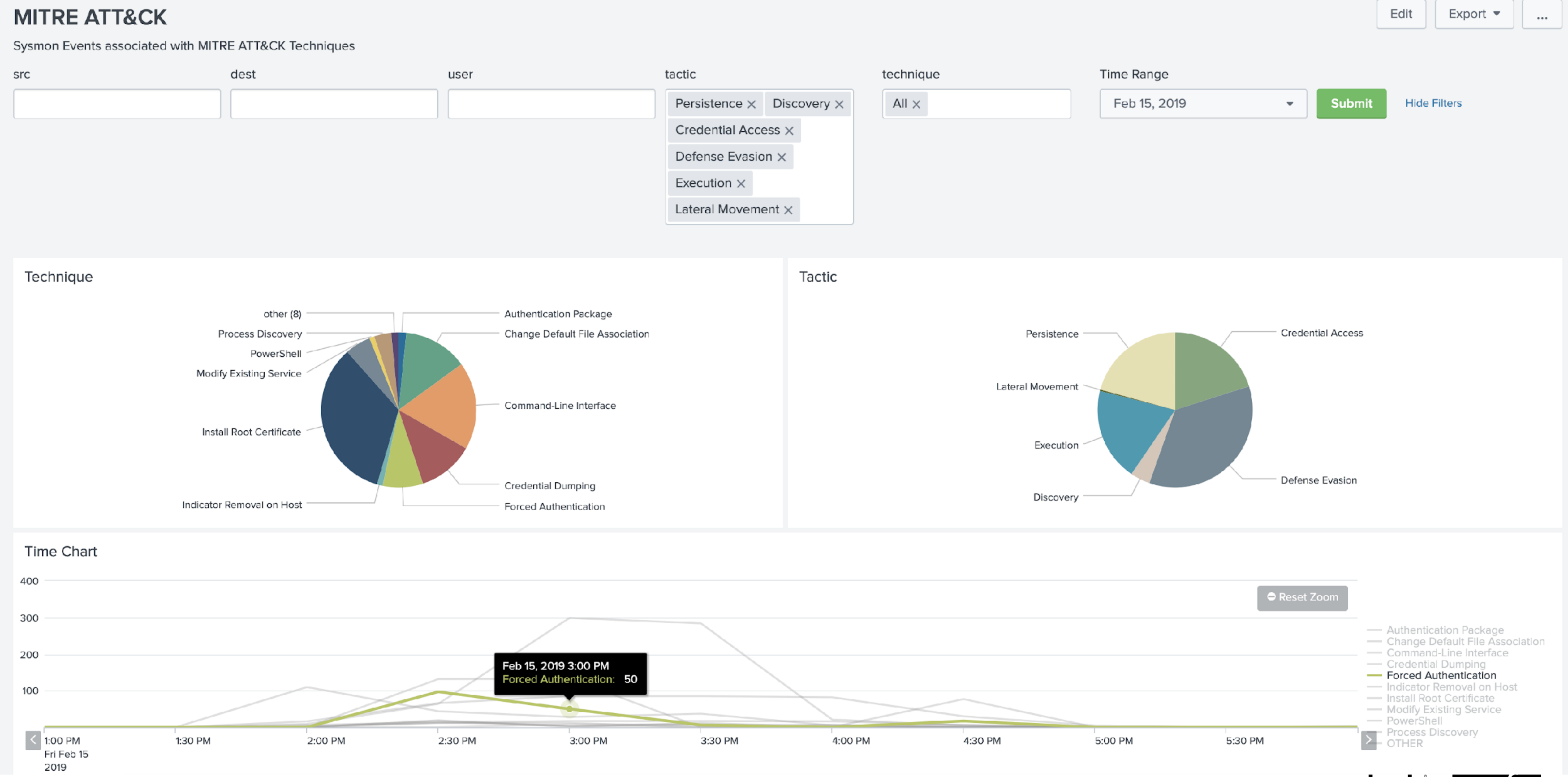
```
<ParentImage condition="image" name="technique_id=T1015,technique_name=Accessibility Features">DisplaySwitch.exe</ParentImage>
<ParentImage condition="image" name="technique_id=T1015,technique_name=Accessibility Features">sethc.exe</ParentImage>
<ParentImage condition="image" name="technique_id=T1202,technique_name=Indirect Command Execution">wscript.exe</ParentImage>
<ParentImage condition="image" name="technique_id=T1202,technique_name=Indirect Command Execution">control.exe</ParentImage>
<ParentImage condition="image" name="technique_id=T1202,technique_name=Indirect Command Execution">cscript.exe</ParentImage>
<ParentImage condition="image" name="technique_id=T1088,technique_name=Bypass User Account Control">fodhelper.exe</ParentImage>
<ParentImage condition="image" name="technique_id=T1088,technique_name=Bypass User Account Control">eventvwr.exe</ParentImage>
<ParentImage condition="image" name="technique_id=T1015,technique_name=Accessibility Features">osk.exe</ParentImage>
<ParentImage condition="image" name="technique_id=T1086,technique_name=PowerShell">powershell.exe</ParentImage>
<ParentImage condition="image" name="technique_id=T1086,technique_name=PowerShell">powershell_ise.exe</ParentImage>
```

https://github.com/olafhartong/sysmon-modular



```
sourcetype="xmlwineventlog:microsoft-windows-sysmon/operational" RuleName=* powershell.exe ParentImage=* | table Image ParentImage RuleName
```

| Image | ParentImage | RuleName |
|---|---|---|
| C:\Windows\Microsoft.NET\Framework64\v2.0.50727\csc.exe | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe | technique_id=T1086,technique_name=PowerShell |
| C:\Windows\System32\whoami.exe | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe | technique_id=T1033,technique_name=System Owner/User Discovery |
| C:\Windows\System32\ftp.exe | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe | technique_id=T1086,technique_name=PowerShell |
| C:\Windows\System32\netsh.exe | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe | technique_id=T1063,technique_name=Security Software Discovery |
| C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe | technique_id=T1086,technique_name=PowerShell |
| C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe | C:\Windows\System32\eventvwr.exe | technique_id=T1086,technique_name=PowerShell |
| C:\Windows\System32\eventvwr.exe | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe | technique_id=T1086,technique_name=PowerShell |
| C:\Windows\System32\eventvwr.exe | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe | technique_id=T1086,technique_name=PowerShell |
| C:\Windows\System32\whoami.exe | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe | technique_id=T1033,technique_name=System Owner/User Discovery |
| C:\Windows\System32\whoami.exe | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe | technique_id=T1033,technique_name=System Owner/User Discovery |
| C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe | C:\Windows\System32\wbem\WmiPrvSE.exe | technique_id=T1086,technique_name=PowerShell |



# MITRE ATT&CK

Sysmon Events associated with MITRE ATT&CK Techniques

src

dest

user

tactic

Persistence × Discovery × Credential Access × Defense Evasion × Execution × Lateral Movement ×

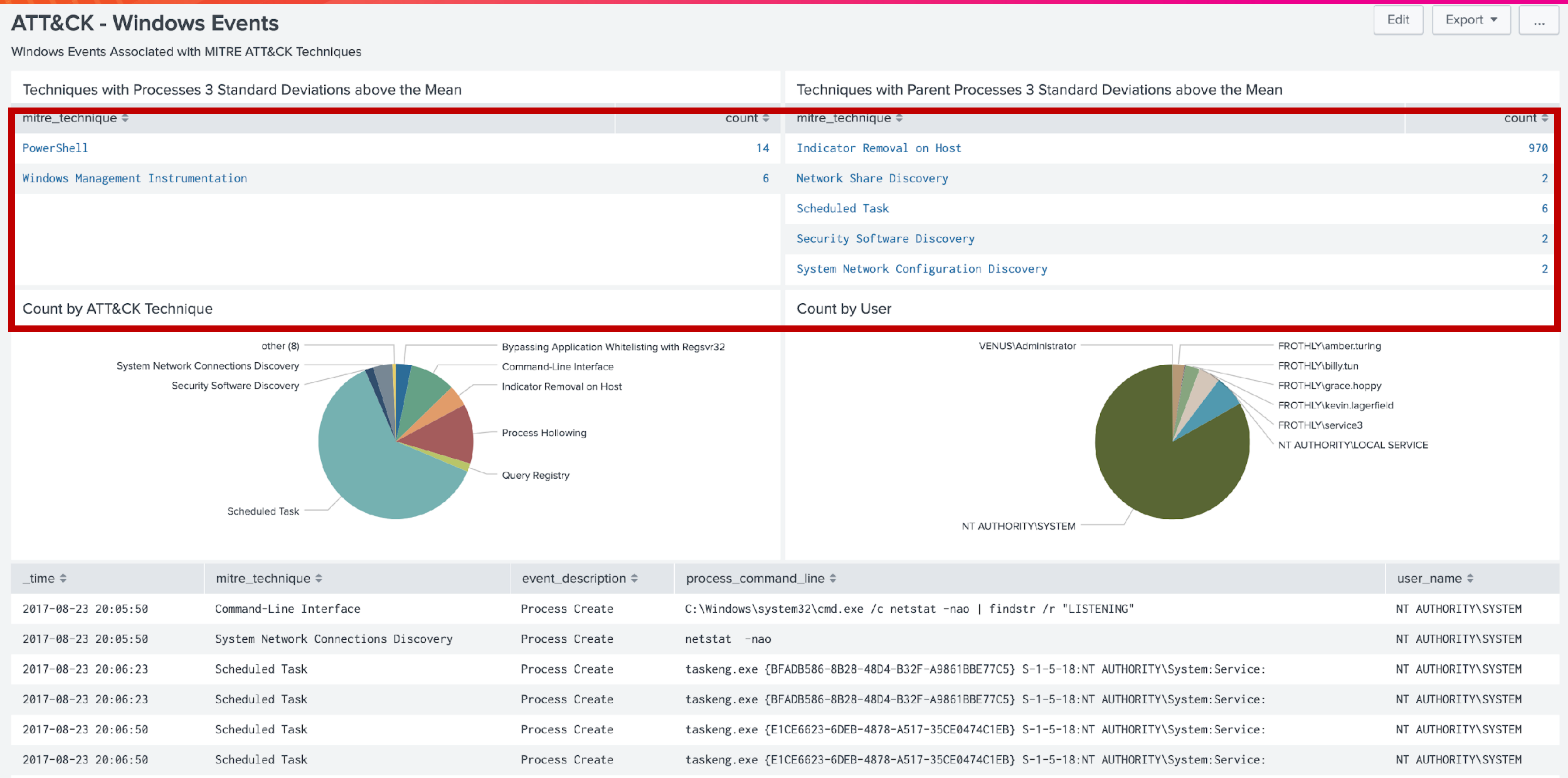
technique

All ×

Time Range

Feb 15, 2019

Feb 15, 2019 3:00 PM
Forced Authentication: 50



# ATT&CK - Windows Events

Windows Events Associated with MITRE ATT&CK Techniques

## Techniques with Processes 3 Standard Deviations above the Mean

| mitre_technique ⇕ | count ⇕ |
|---|---|
| PowerShell | 14 |
| Windows Management Instrumentation | 6 |

## Techniques with Parent Processes 3 Standard Deviations above the Mean

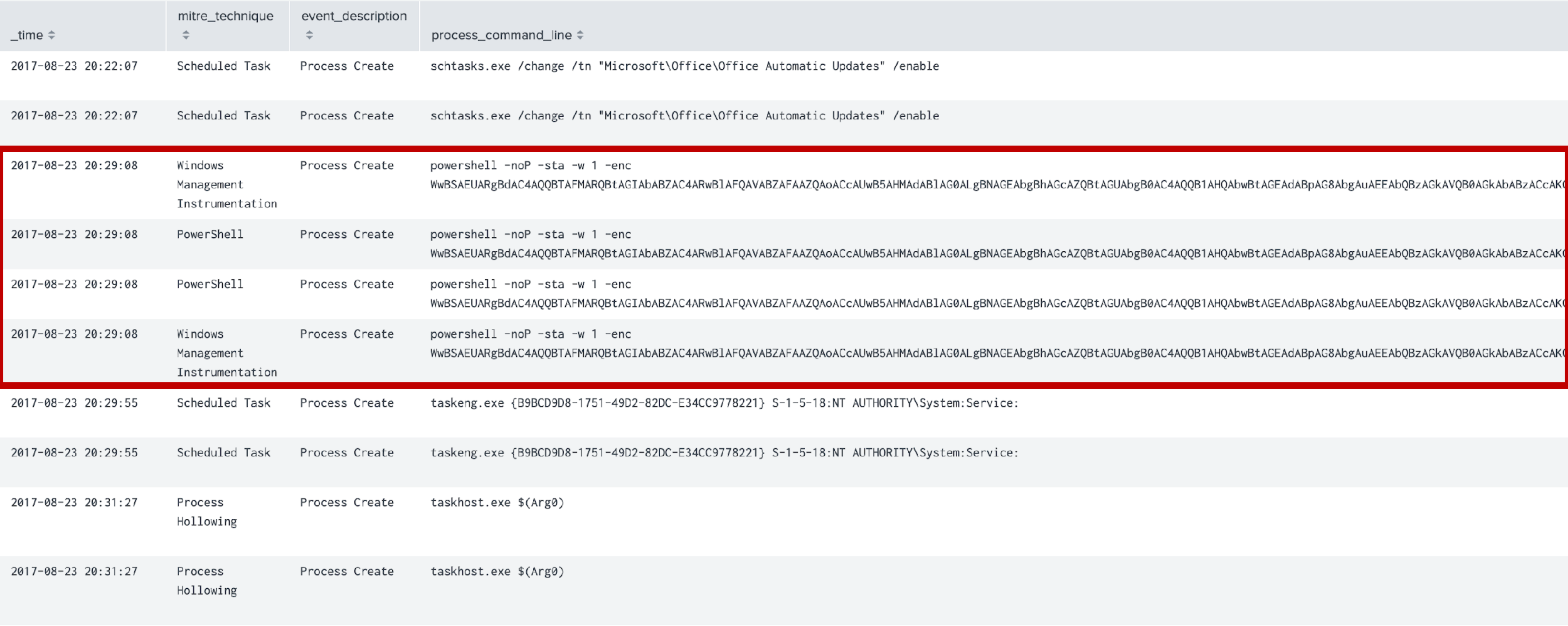
| mitre_technique ⇕ | count ⇕ |
|---|---|
| Indicator Removal on Host | 970 |
| Network Share Discovery | 2 |
| Scheduled Task | 6 |
| Security Software Discovery | 2 |
| System Network Configuration Discovery | 2 |

## Count by ATT&CK Technique

other (8)
System Network Connections Discovery
Security Software Discovery
Scheduled Task
Bypassing Application Whitelisting with Regsvr32
Command-Line Interface
Indicator Removal on Host
Process Hollowing
Query Registry

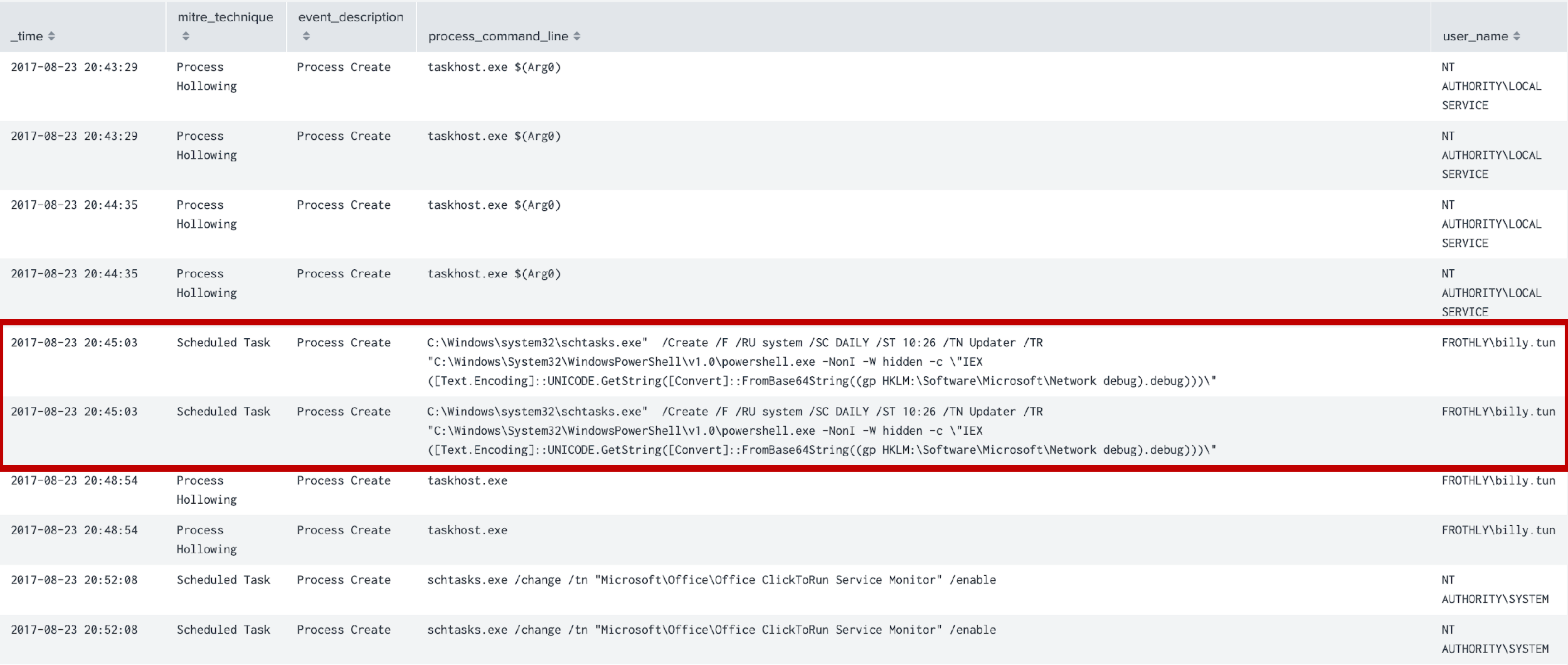
## Count by User

| _time ⇕ | mitre_technique ⇕ | event_description ⇕ | process_command_line ⇕ | user_name ⇕ |
|---|---|---|---|---|
| 2017-08-23 20:05:50 | Command-Line Interface | Process Create | C:\Windows\system32\cmd.exe /c netstat -nao \| findstr /r "LISTENING" | NT AUTHORITY\SYSTEM |
| 2017-08-23 20:05:50 | System Network Connections Discovery | Process Create | netstat  -nao | NT AUTHORITY\SYSTEM |
| 2017-08-23 20:06:23 | Scheduled Task | Process Create | taskeng.exe {BFADB586-8B28-48D4-B32F-A9861BBE77C5} S-1-5-18:NT AUTHORITY\System:Service: | NT AUTHORITY\SYSTEM |
| 2017-08-23 20:06:23 | Scheduled Task | Process Create | taskeng.exe {BFADB586-8B28-48D4-B32F-A9861BBE77C5} S-1-5-18:NT AUTHORITY\System:Service: | NT AUTHORITY\SYSTEM |
| 2017-08-23 20:06:50 | Scheduled Task | Process Create | taskeng.exe {E1CE6623-6DEB-4878-A517-35CE0474C1EB} S-1-5-18:NT AUTHORITY\System:Service: | NT AUTHORITY\SYSTEM |
| 2017-08-23 20:06:50 | Scheduled Task | Process Create | taskeng.exe {E1CE6623-6DEB-4878-A517-35CE0474C1EB} S-1-5-18:NT AUTHORITY\System:Service: | NT AUTHORITY\SYSTEM |



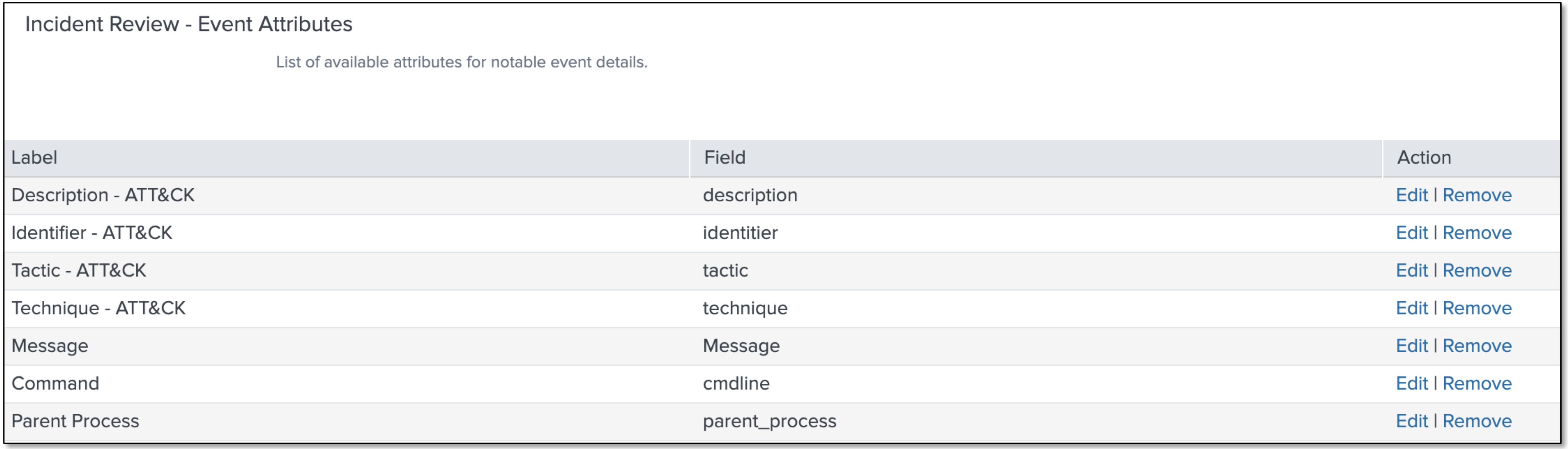
| _time | mitre_technique | event_description | process_command_line |
|---|---|---|---|
| 2017-08-23 20:22:07 | Scheduled Task | Process Create | schtasks.exe /change /tn "Microsoft\Office\Office Automatic Updates" /enable |
| 2017-08-23 20:22:07 | Scheduled Task | Process Create | schtasks.exe /change /tn "Microsoft\Office\Office Automatic Updates" /enable |
| 2017-08-23 20:29:08 | Windows Management Instrumentation | Process Create | powershell -noP -sta -w 1 -enc WwBSAEUARgBdAC4AQQBTAFMARQBtAGIAbABZAC4ARwBlAFQAVABZAFAAZQAoACcAUwB5AHMAdABlAG0ALgBNAGEAbgBhAGcAZQBtAGUAbgB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbgAuAEEAbQBzAGkAVQB0AGkAbABzACcAK |
| 2017-08-23 20:29:08 | PowerShell | Process Create | powershell -noP -sta -w 1 -enc WwBSAEUARgBdAC4AQQBTAFMARQBtAGIAbABZAC4ARwBlAFQAVABZAFAAZQAoACcAUwB5AHMAdABlAG0ALgBNAGEAbgBhAGcAZQBtAGUAbgB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbgAuAEEAbQBzAGkAVQB0AGkAbABzACcAK |
| 2017-08-23 20:29:08 | PowerShell | Process Create | powershell -noP -sta -w 1 -enc WwBSAEUARgBdAC4AQQBTAFMARQBtAGIAbABZAC4ARwBlAFQAVABZAFAAZQAoACcAUwB5AHMAdABlAG0ALgBNAGEAbgBhAGcAZQBtAGUAbgB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbgAuAEEAbQBzAGkAVQB0AGkAbABzACcAK |
| 2017-08-23 20:29:08 | Windows Management Instrumentation | Process Create | powershell -noP -sta -w 1 -enc WwBSAEUARgBdAC4AQQBTAFMARQBtAGIAbABZAC4ARwBlAFQAVABZAFAAZQAoACcAUwB5AHMAdABlAG0ALgBNAGEAbgBhAGcAZQBtAGUAbgB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbgAuAEEAbQBzAGkAVQB0AGkAbABzACcAK |
| 2017-08-23 20:29:55 | Scheduled Task | Process Create | taskeng.exe {B9BCD9D8-1751-49D2-82DC-E34CC9778221} S-1-5-18:NT AUTHORITY\System:Service: |
| 2017-08-23 20:29:55 | Scheduled Task | Process Create | taskeng.exe {B9BCD9D8-1751-49D2-82DC-E34CC9778221} S-1-5-18:NT AUTHORITY\System:Service: |
| 2017-08-23 20:31:27 | Process Hollowing | Process Create | taskhost.exe $(Arg0) |
| 2017-08-23 20:31:27 | Process Hollowing | Process Create | taskhost.exe $(Arg0) |

splunk> .conf19



| _time | mitre_technique | event_description | process_command_line | user_name |
|---|---|---|---|---|
| 2017-08-23 20:43:29 | Process Hollowing | Process Create | taskhost.exe $(Arg0) | NT AUTHORITY\LOCAL SERVICE |
| 2017-08-23 20:43:29 | Process Hollowing | Process Create | taskhost.exe $(Arg0) | NT AUTHORITY\LOCAL SERVICE |
| 2017-08-23 20:44:35 | Process Hollowing | Process Create | taskhost.exe $(Arg0) | NT AUTHORITY\LOCAL SERVICE |
| 2017-08-23 20:44:35 | Process Hollowing | Process Create | taskhost.exe $(Arg0) | NT AUTHORITY\LOCAL SERVICE |
| 2017-08-23 20:45:03 | Scheduled Task | Process Create | C:\Windows\system32\schtasks.exe"  /Create /F /RU system /SC DAILY /ST 10:26 /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))\" | FROTHLY\billy.tun |
| 2017-08-23 20:45:03 | Scheduled Task | Process Create | C:\Windows\system32\schtasks.exe"  /Create /F /RU system /SC DAILY /ST 10:26 /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))\" | FROTHLY\billy.tun |
| 2017-08-23 20:48:54 | Process Hollowing | Process Create | taskhost.exe | FROTHLY\billy.tun |
| 2017-08-23 20:48:54 | Process Hollowing | Process Create | taskhost.exe | FROTHLY\billy.tun |
| 2017-08-23 20:52:08 | Scheduled Task | Process Create | schtasks.exe /change /tn "Microsoft\Office\Office ClickToRun Service Monitor" /enable | NT AUTHORITY\SYSTEM |
| 2017-08-23 20:52:08 | Scheduled Task | Process Create | schtasks.exe /change /tn "Microsoft\Office\Office ClickToRun Service Monitor" /enable | NT AUTHORITY\SYSTEM |

# Adding Fields to Incident Review

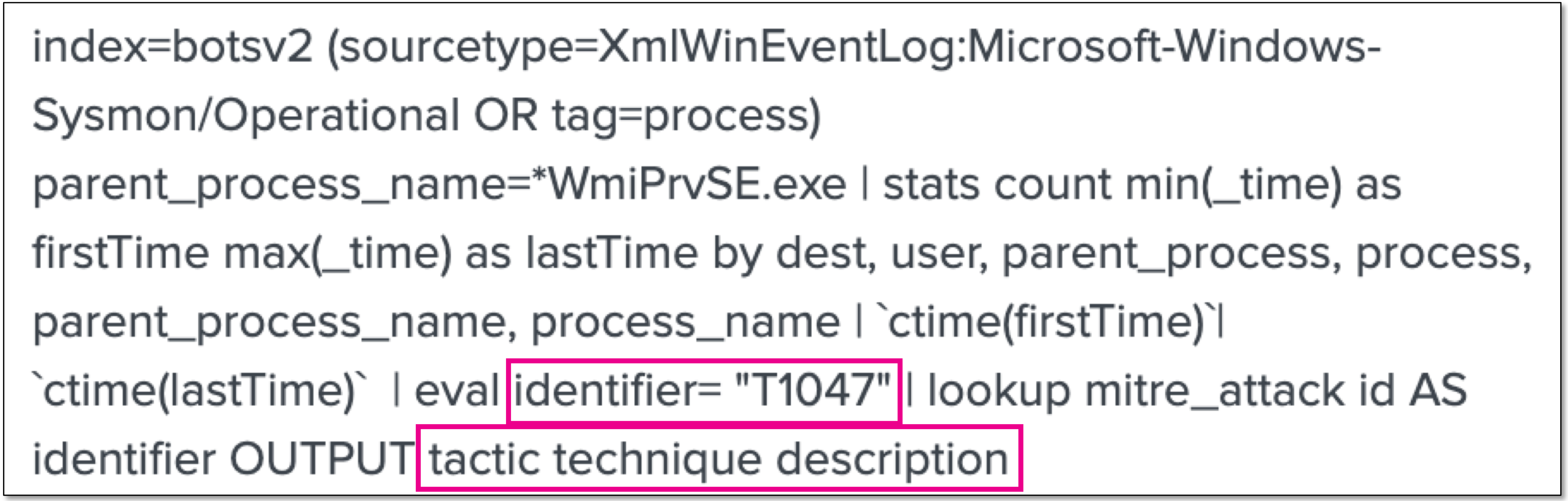


Incident Review - Event Attributes

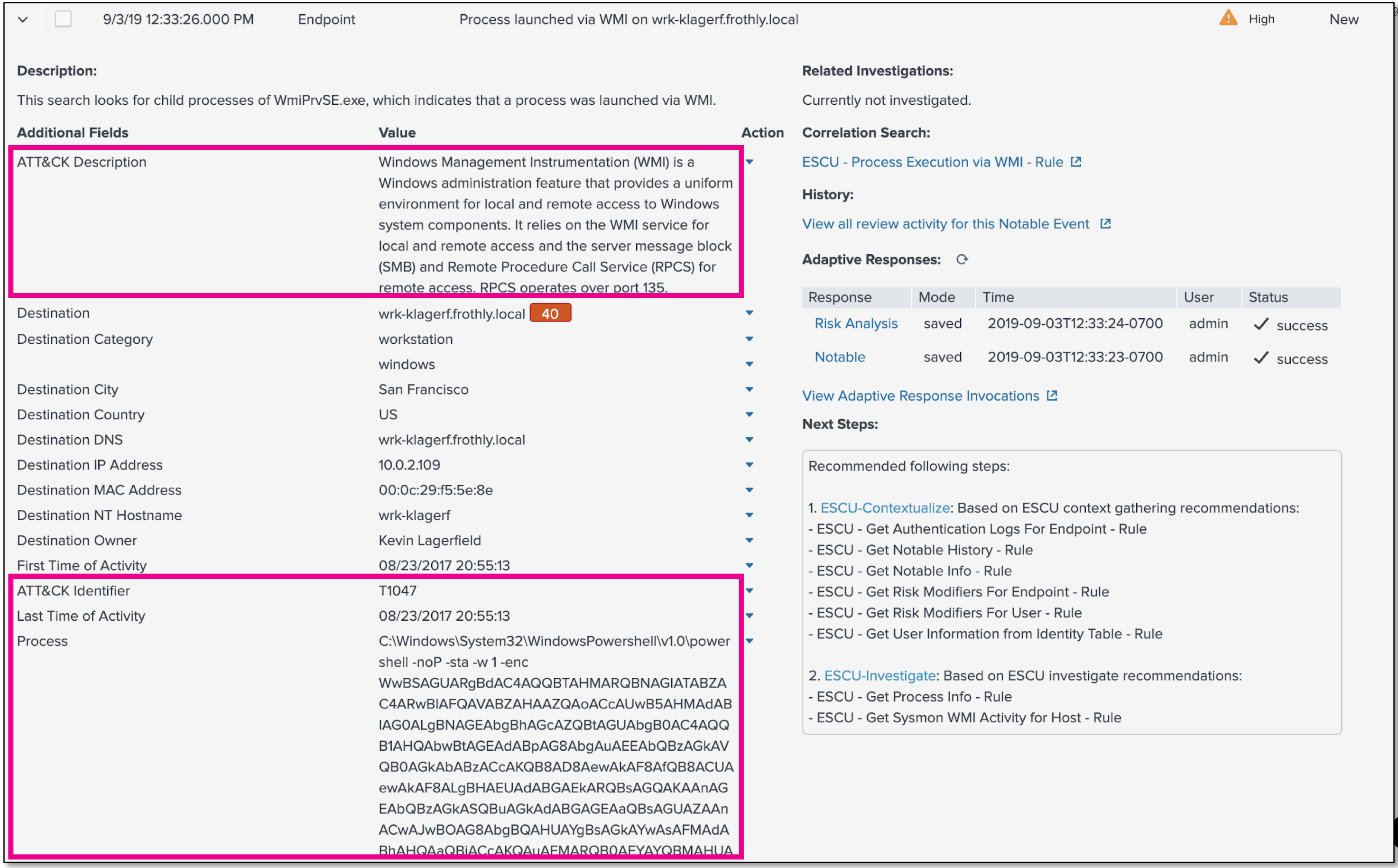
List of available attributes for notable event details.

| Label | Field | Action |
|---|---|---|
| Description - ATT&CK | description | Edit \| Remove |
| Identifier - ATT&CK | identitier | Edit \| Remove |
| Tactic - ATT&CK | tactic | Edit \| Remove |
| Technique - ATT&CK | technique | Edit \| Remove |
| Message | Message | Edit \| Remove |
| Command | cmdline | Edit \| Remove |
| Parent Process | parent_process | Edit \| Remove |

# Correlation Search Example



```
index=botsv2 (sourcetype=XmlWinEventLog:Microsoft-Windows-
Sysmon/Operational OR tag=process)
parent_process_name=*WmiPrvSE.exe | stats count min(_time) as
firstTime max(_time) as lastTime by dest, user, parent_process, process,
parent_process_name, process_name | `ctime(firstTime)`|
`ctime(lastTime)`  | eval identifier= "T1047"| lookup mitre_attack id AS
identifier OUTPUT tactic technique description
```



9/3/19 12:33:26.000 PM | Endpoint | Process launched via WMI on wrk-klagerf.frothly.local | High | New

**Description:**

This search looks for child processes of WmiPrvSE.exe, which indicates that a process was launched via WMI.

| Additional Fields | Value | Action |
|---|---|---|
| ATT&CK Description | Windows Management Instrumentation (WMI) is a Windows administration feature that provides a uniform environment for local and remote access to Windows system components. It relies on the WMI service for local and remote access and the server message block (SMB) and Remote Procedure Call Service (RPCS) for remote access. RPCS operates over port 135. | ▾ |
| Destination | wrk-klagerf.frothly.local 40 | ▾ |
| Destination Category | workstation | ▾ |
| | windows | ▾ |
| Destination City | San Francisco | ▾ |
| Destination Country | US | ▾ |
| Destination DNS | wrk-klagerf.frothly.local | ▾ |
| Destination IP Address | 10.0.2.109 | ▾ |
| Destination MAC Address | 00:0c:29:f5:5e:8e | ▾ |
| Destination NT Hostname | wrk-klagerf | ▾ |
| Destination Owner | Kevin Lagerfield | ▾ |
| First Time of Activity | 08/23/2017 20:55:13 | ▾ |
| ATT&CK Identifier | T1047 | ▾ |
| Last Time of Activity | 08/23/2017 20:55:13 | ▾ |
| Process | C:\Windows\System32\WindowsPowershell\v1.0\powershell -noP -sta -w 1 -enc WwBSAGUARgBdAC4AQQBTAHMARQBNAGIATABZAC4ARwBIAFQAVABZAHAAZQAoACcAUwB5AHMAdABlAG0ALgBNAGEAbgBhAGcAZQBtAGUAbgB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbgAuAEEAbQBzAGkAVQB0AGkAbABBzACcAKQB8AD8AewAkAF8AfQB8ACUAewAkAF8ALgBHAEUAdABGAEkARQBsAGQAKAAnAGEAbQBzAGkASQBuAGkAdABGAGEAaQBsAGUAZAAnACwAJwBOAG8AbgBQAHUAYgBsAGkAYwAsAFMAdABhAHQAaQBiACcAKQAuAFMARQB0AFYAYQBMAHUA | ▾ |

**Related Investigations:**

Currently not investigated.

**Correlation Search:**

ESCU - Process Execution via WMI - Rule

**History:**

View all review activity for this Notable Event

**Adaptive Responses:**

| Response | Mode | Time | User | Status |
|---|---|---|---|---|
| Risk Analysis | saved | 2019-09-03T12:33:24-0700 | admin | ✓ success |
| Notable | saved | 2019-09-03T12:33:23-0700 | admin | ✓ success |

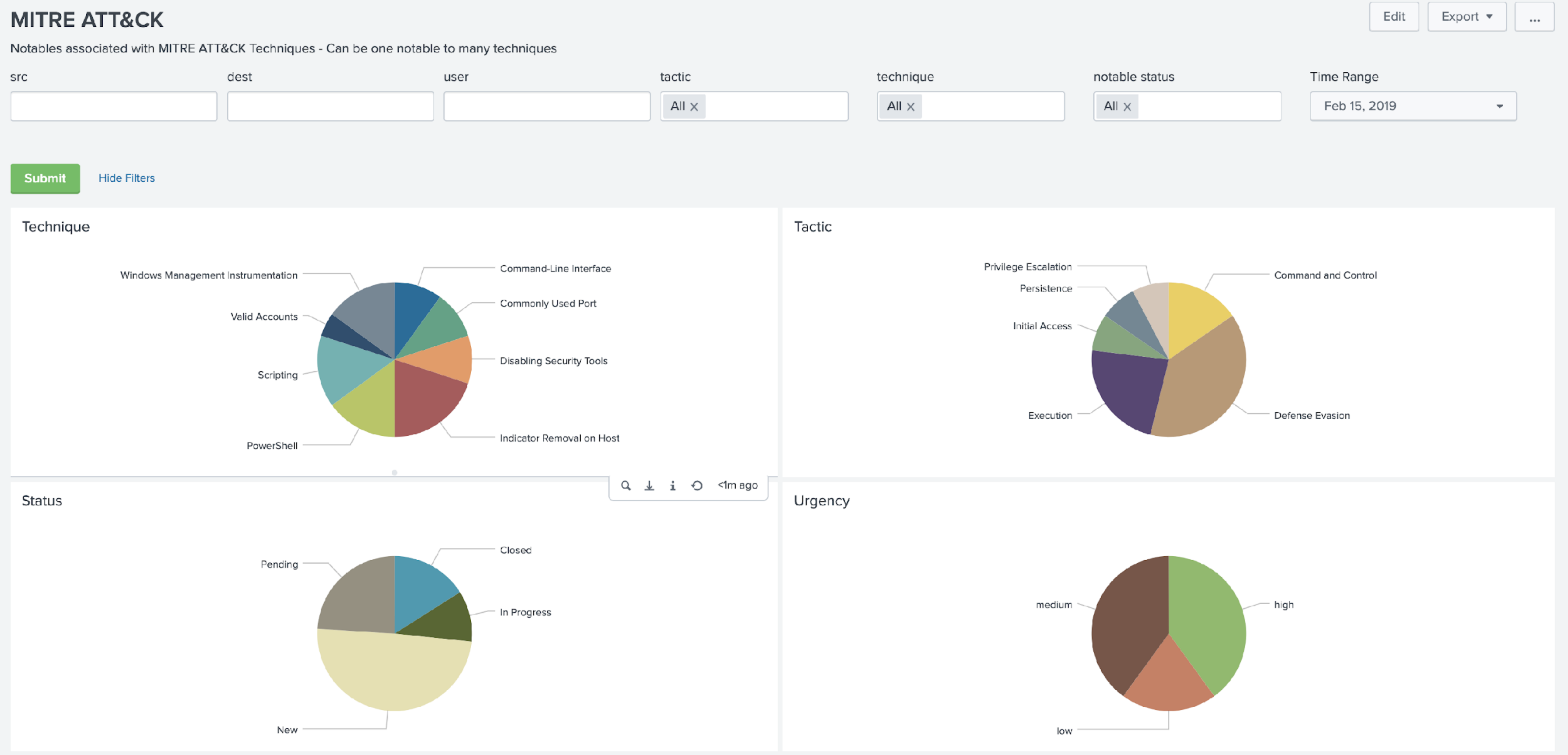
View Adaptive Response Invocations

**Next Steps:**

Recommended following steps:

1. ESCU-Contextualize: Based on ESCU context gathering recommendations:
- ESCU - Get Authentication Logs For Endpoint - Rule
- ESCU - Get Notable History - Rule
- ESCU - Get Notable Info - Rule
- ESCU - Get Risk Modifiers For Endpoint - Rule
- ESCU - Get Risk Modifiers For User - Rule
- ESCU - Get User Information from Identity Table - Rule

2. ESCU-Investigate: Based on ESCU investigate recommendations:
- ESCU - Get Process Info - Rule
- ESCU - Get Sysmon WMI Activity for Host - Rule



## MITRE ATT&CK

Notables associated with MITRE ATT&CK Techniques - Can be one notable to many techniques

src

dest

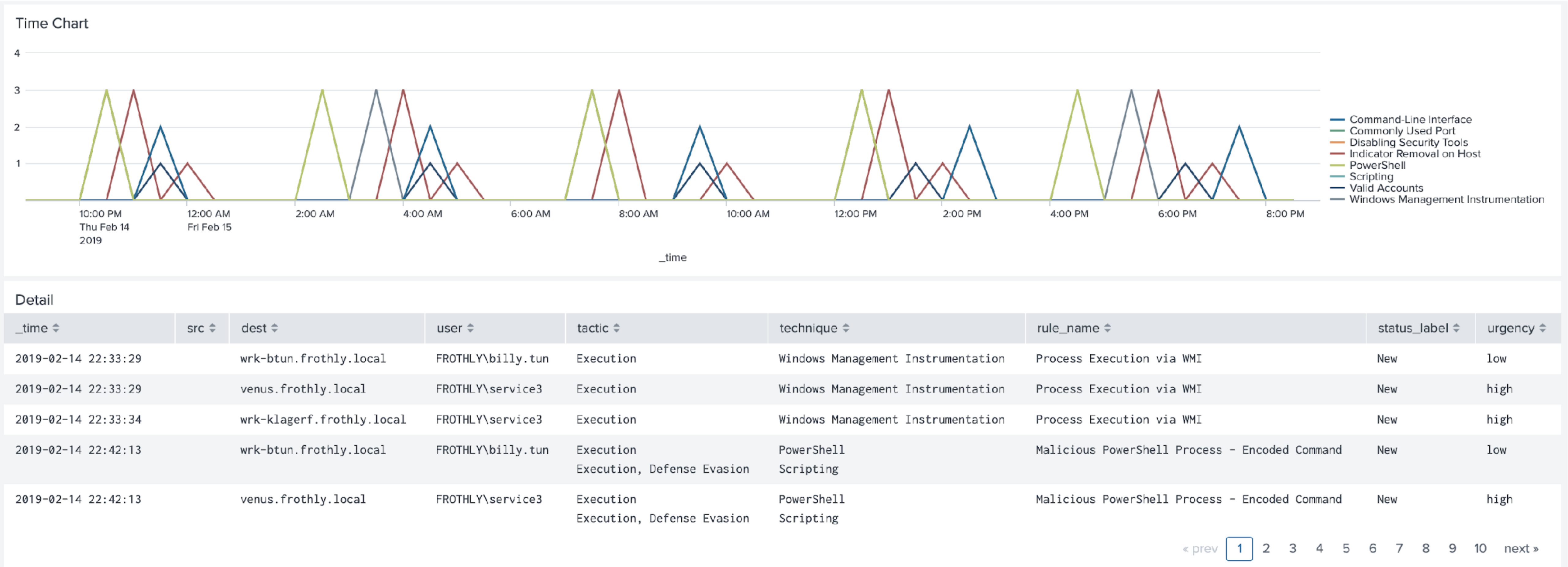
user

tactic
All ×

technique
All ×

notable status
All ×

Time Range
Feb 15, 2019

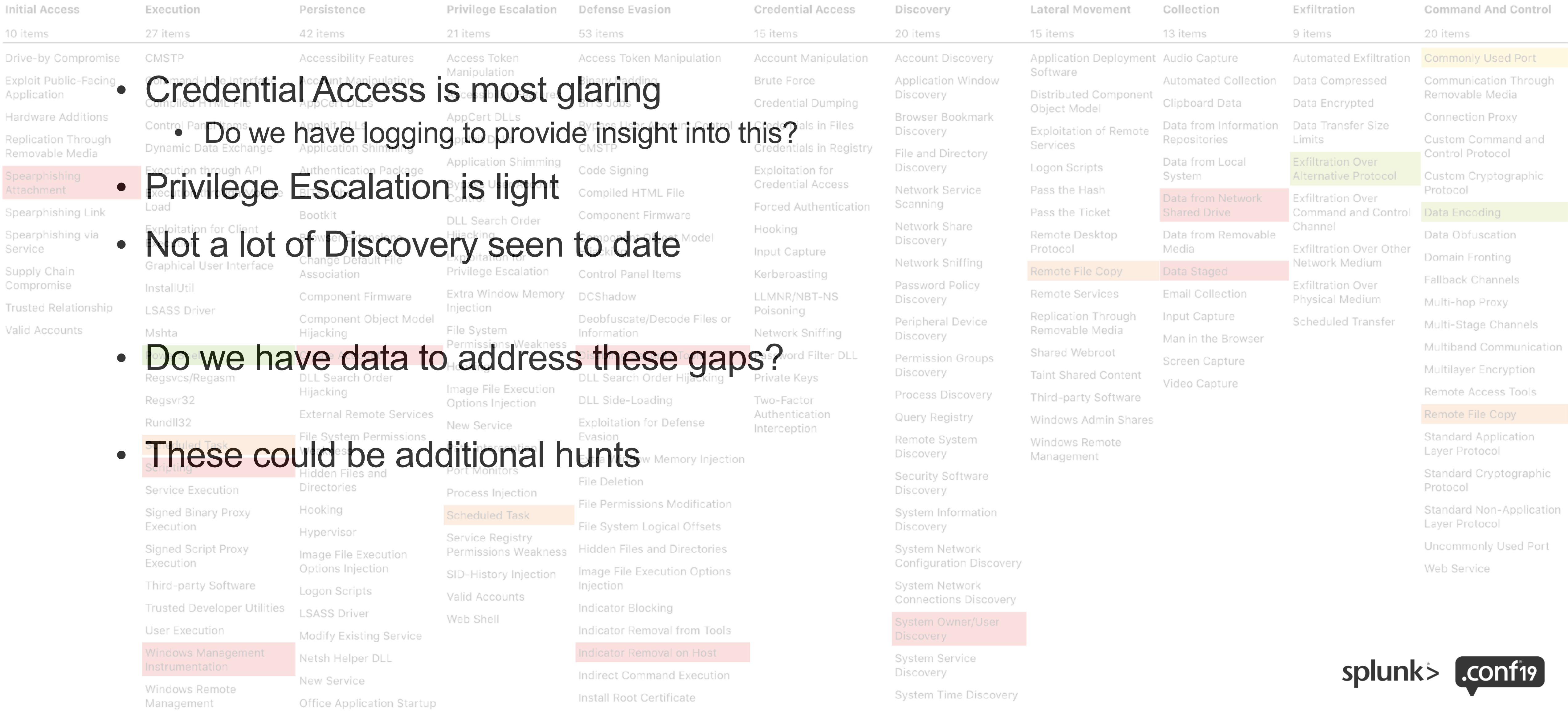


Detail

| _time | src | dest | user | tactic | technique | rule_name | status_label | urgency |
|---|---|---|---|---|---|---|---|---|
| 2019-02-14 22:33:29 | | wrk-btun.frothly.local | FROTHLY\billy.tun | Execution | Windows Management Instrumentation | Process Execution via WMI | New | low |
| 2019-02-14 22:33:29 | | venus.frothly.local | FROTHLY\service3 | Execution | Windows Management Instrumentation | Process Execution via WMI | New | high |
| 2019-02-14 22:33:34 | | wrk-klagerf.frothly.local | FROTHLY\service3 | Execution | Windows Management Instrumentation | Process Execution via WMI | New | high |
| 2019-02-14 22:42:13 | | wrk-btun.frothly.local | FROTHLY\billy.tun | Execution<br>Execution, Defense Evasion | PowerShell<br>Scripting | Malicious PowerShell Process - Encoded Command | New | low |
| 2019-02-14 22:42:13 | | venus.frothly.local | FROTHLY\service3 | Execution<br>Execution, Defense Evasion | PowerShell<br>Scripting | Malicious PowerShell Process - Encoded Command | New | high |

# Where Are Our Gaps?

- Credential Access is most glaring
  - Do we have logging to provide insight into this?
- Privilege Escalation is light
- Not a lot of Discovery seen to date
- Do we have data to address these gaps?
- These could be additional hunts



Initial Access
10 items
Drive-by Compromise
Exploit Public-Facing Application
Hardware Additions
Replication Through Removable Media
Spearphishing Attachment
Spearphishing Link
Spearphishing via Service
Supply Chain Compromise
Trusted Relationship
Valid Accounts

Execution
27 items
CMSTP
Command-Line Interface
Compiled HTML File
Control Panel Items
Dynamic Data Exchange
Execution through API
Execution through Module Load
Exploitation for Client Execution
Graphical User Interface
InstallUtil
LSASS Driver
Mshta
PowerShell
Regsvcs/Regasm
Regsvr32
Rundll32
Scheduled Task
Scripting
Service Execution
Signed Binary Proxy Execution
Signed Script Proxy Execution
Third-party Software
Trusted Developer Utilities
User Execution
Windows Management Instrumentation
Windows Remote Management

Persistence
42 items
Accessibility Features
Account Manipulation
AppCert DLLs
AppInit DLLs
Application Shimming
Authentication Package
BITS Jobs
Bootkit
Browser Extensions
Change Default File Association
Component Firmware
Component Object Model Hijacking
Create Account
DLL Search Order Hijacking
External Remote Services
File System Permissions Weakness
Hidden Files and Directories
Hooking
Hypervisor
Image File Execution Options Injection
Logon Scripts
LSASS Driver
Modify Existing Service
Netsh Helper DLL
New Service
Office Application Startup

Privilege Escalation
21 items
Access Token Manipulation
Accessibility Features
AppCert DLLs
AppInit DLLs
Application Shimming
Bypass User Account Control
DLL Search Order Hijacking
Exploitation for Privilege Escalation
Extra Window Memory Injection
File System Permissions Weakness
Hooking
Image File Execution Options Injection
New Service
Path Interception
Port Monitors
Process Injection
Scheduled Task
Service Registry Permissions Weakness
SID-History Injection
Valid Accounts
Web Shell

Defense Evasion
53 items
Access Token Manipulation
Binary Padding
BITS Jobs
Bypass User Account Control
CMSTP
Code Signing
Compiled HTML File
Component Firmware
Component Object Model Hijacking
Control Panel Items
DCShadow
Deobfuscate/Decode Files or Information
Disabling Security Tools
DLL Search Order Hijacking
DLL Side-Loading
Exploitation for Defense Evasion
Extra Window Memory Injection
File Deletion
File Permissions Modification
File System Logical Offsets
Hidden Files and Directories
Image File Execution Options Injection
Indicator Blocking
Indicator Removal from Tools
Indicator Removal on Host
Indirect Command Execution
Install Root Certificate

Credential Access
15 items
Account Manipulation
Brute Force
Credential Dumping
Credentials in Files
Credentials in Registry
Exploitation for Credential Access
Forced Authentication
Hooking
Input Capture
Kerberoasting
LLMNR/NBT-NS Poisoning
Network Sniffing
Password Filter DLL
Private Keys
Two-Factor Authentication Interception

Discovery
20 items
Account Discovery
Application Window Discovery
Browser Bookmark Discovery
File and Directory Discovery
Network Service Scanning
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery
Process Discovery
Query Registry
Remote System Discovery
Security Software Discovery
System Information Discovery
System Network Configuration Discovery
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
System Time Discovery

Lateral Movement
15 items
Application Deployment Software
Distributed Component Object Model
Exploitation of Remote Services
Logon Scripts
Pass the Hash
Pass the Ticket
Remote Desktop Protocol
Remote File Copy
Remote Services
Replication Through Removable Media
Shared Webroot
Taint Shared Content
Third-party Software
Windows Admin Shares
Windows Remote Management

Collection
13 items
Audio Capture
Automated Collection
Clipboard Data
Data from Information Repositories
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged
Email Collection
Input Capture
Man in the Browser
Screen Capture
Video Capture

Exfiltration
9 items
Automated Exfiltration
Data Compressed
Data Encrypted
Data Transfer Size Limits
Exfiltration Over Alternative Protocol
Exfiltration Over Command and Control Channel
Exfiltration Over Other Network Medium
Exfiltration Over Physical Medium
Scheduled Transfer

Command And Control
20 items
Commonly Used Port
Communication Through Removable Media
Connection Proxy
Custom Command and Control Protocol
Custom Cryptographic Protocol
Data Encoding
Data Obfuscation
Domain Fronting
Fallback Channels
Multi-hop Proxy
Multi-Stage Channels
Multiband Communication
Multilayer Encryption
Remote Access Tools
Remote File Copy
Standard Application Layer Protocol
Standard Cryptographic Protocol
Standard Non-Application Layer Protocol
Uncommonly Used Port
Web Service
]

# Conclusions

# Takeaways

1. Pick a model, any model
2. ATT&CK is great but is APT focused
3. Wonderful way to focus defenses, find gaps, and write detections
4. Several Splunk tools that incorporate ATT&CK today

# Thank you!

Dave Herrald
@daveherrald

John Stoner
@stonerPSU

Ryan Kovar
@meansec