

---

---

# Enter Mordor

---

---

Pre-recorded Security Events from  
Simulated Adversarial Techniques

---

---

# | @Cyb3rWard0g

- Creator of
  - @HunterPlaybook
  - @THE\_HELK
  - ATTACK-Python-Client
  - @OSSEM\_Project
  - @Mordor\_Project
  - Blacksmith & More
- Founder:
  - @HuntersForge



# Agenda

- What is the goal of Purple Teaming?
- Purple Teaming Challenges?
  - Planning vs Execution
- Are we being effective at purple teaming?
- The Mordor Project
- Purple Teaming - Mordor Style
- Enabling the community!

# What is the Goal of Purple Teaming?

Or at least one of the goals! :)

# What can we do together?



# Remember: It is NOT a Competition!



Legolas! Two already!



I'm on seventeen!



I'll have no pointy-ear outscoring me!

# A Few Goals!

- Validate current detections
- Build new detections
- Brainstorm new tradecraft
- Map data to adversary actions
- Improve Telemetry
- **Learn from each other**
  - Red improves Blue



# A Few Goals!

- Validate current detections
- Build new detections
- Brainstorm new tradecraft
- Map data to adversary actions
- Improve Telemetry
- **Learn from each other**
  - Red improves Blue
  - Blue improves Red too!



Believe me! You will always learn something new..



# Rubeus

- Rubeus is a C# re-implementation of some of the functionality from Benjamin Delpy's Kekeo project
  - Kerberos structures built by hand...
  - Rubeus works nicely with execute-assembly
  - So why not use Kekeo? Because ASN.1!
    - Requires a commercial ASN.1 library to customize/rebuild the Kekeo codebase
- **Author: Will Schroeder @harmj0y**

# Rubeus: over-pass-the-hash

## Mimikatz pth

- "sacrificial" logon session that doesn't interact with the current logon session.
- Opens the LSASS process
- Patches associated logon session with hash/key.
- Normal Kerberos authentication process Kicks off (Hash->TGT)

## Rubeus asktgt (createnetonly)

- CreateProcessWithLogonW Function to create a sacrificial process/logon session
- Rubeus builds/crafts AS-REQ (w/ preauth)
- TGT request successful
- Imports TGT to logon session (Hash->TGT)

# Rubeus askTGT does NOT touch LSASS!

## Mimikatz pth

- "sacrificial" logon session that doesn't interact with the current logon session.
- **Opens the LSASS process**
- Patches associated logon session with hash/key.
- Normal Kerberos authentication process Kicks off (Hash->TGT)

## Rubeus asktgt (createnetonly)

- CreateProcessWithLogonW Function to create a sacrificial process/logon session
- Rubeus builds/crafts AS-REQ (w/ preauth)
- TGT request successful
- Imports TGT to logon session (Hash-TGT)

# Mimikatz & Rubeus - Kerberos Authentication

Event Properties - Event 5156, Microsoft Windows security auditing.

General Details

The Windows Filtering Platform has permitted a connection.

**Application Information:**

Process ID:	816
Application Name:	\device\harddiskvolume4\windows\system32\lsass.exe

**Network Information:**

Direction:	Outbound
Source Address:	192.168.64.137
Source Port:	50066
Destination Address:	192.168.64.147
Destination Port:	88
Protocol:	6

**Filter Information:**

Filter Run-Time ID:	72462
Layer Name:	Connect
Layer Run-Time ID:	48

Event Properties - Event 5156, Microsoft Windows security auditing.

General Details

The Windows Filtering Platform has permitted a connection.

**Application Information:**

Process ID:	7984
Application Name:	\device\harddiskvolume4\users\cbrown\rubeus.exe

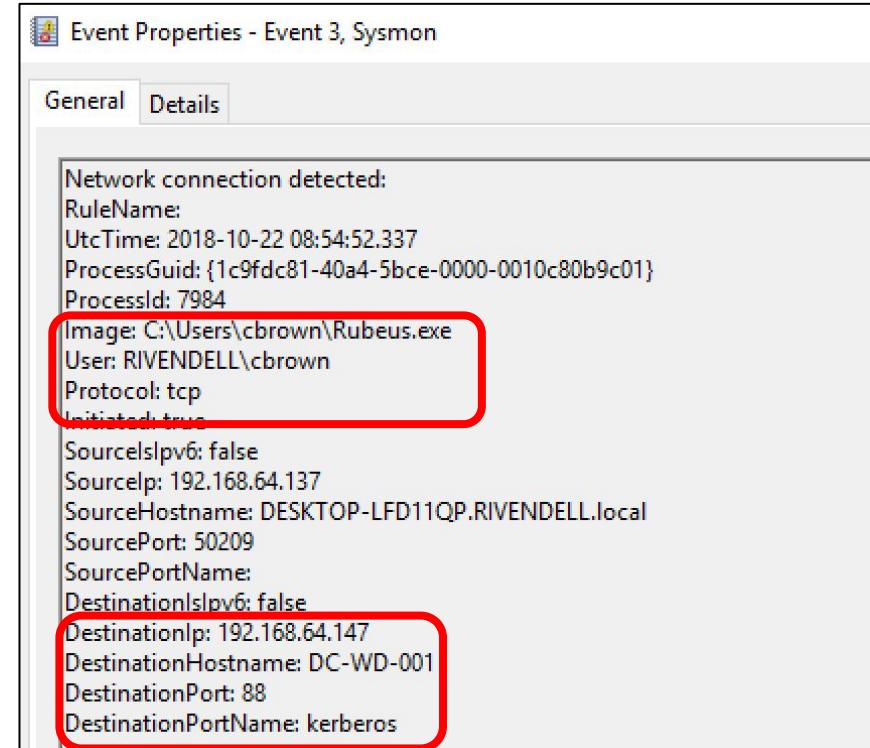
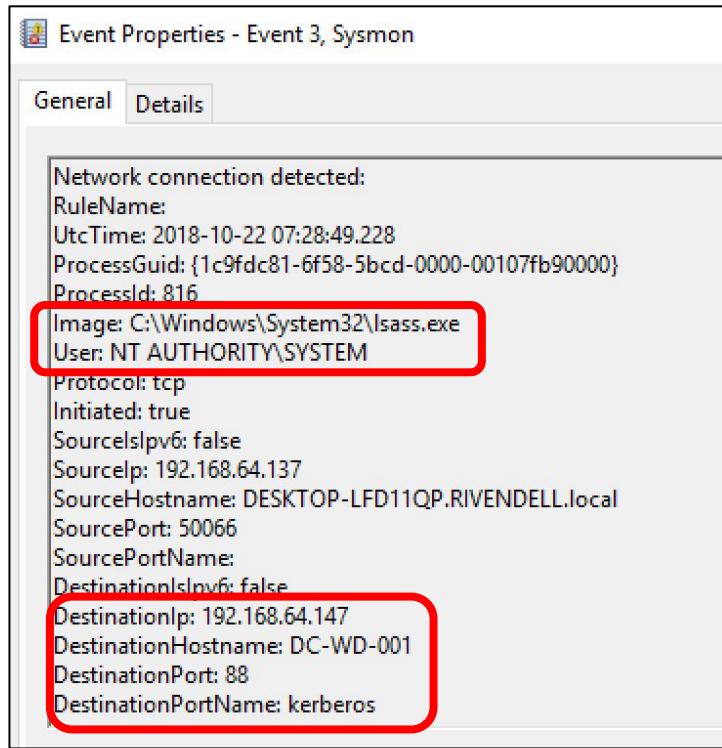
**Network Information:**

Direction:	Outbound
Source Address:	192.168.64.137
Source Port:	50209
Destination Address:	192.168.64.147
Destination Port:	88
Protocol:	6

**Filter Information:**

Filter Run-Time ID:	74536
Layer Name:	Connect
Layer Run-Time ID:	48

# Mimikatz & Rubeus - Kerberos Authentication



# Purple Teaming Challenges

# Purple Team Challenges?

- What techniques do we prioritize?
- What is the scope? (Production?)
- What is the risk?
- How long is it going to take?
- Do we use our own Tradecraft?
- How do we handle communications?
- What are the deliverables?
- How do we track findings?
- Who is in charge?
- How do we split the team?
- Do we need to update our audit policies?
- Are we collecting data from every endpoint in scope?
- Do we even know what events we are collecting?
- Do we write a report together?
- Do we do a tabletop exercise?
- What metrics can we use?
- Who else should be included?

# ■ Purple Team Challenges? (Strategy & Preparation)

- What techniques do we prioritize?
- What is the scope? (Production?)
- What is the risk?
- How long is it going to take?
- Do we use our own Tradecraft?
- How do we handle communications?
- What are the deliverables?
- How do we track findings?
- Who is in charge?
- How do we split the team?
- Do we need to update our audit policies?
- Are we collecting data from every endpoint in scope?
- Do we even know what events we are collecting?
- Do we write a report together?
- Do we do a tabletop exercise?
- What metrics can we use?
- Who else should be included?

# Purple Team Challenges? (Strategy & Preparation)

- **What techniques do we prioritize?**
- What is the scope? (Production?)
- What is the risk?
- How long is it going to take?
- **Do we use our own Tradecraft?**
- How do we handle communications?
- What are the deliverables?
- **How do we track findings?**
- Who is in charge?
- How do we split the team?
- **Do we need to update our audit policies?**
- Are we collecting data from every endpoint in scope?
- **Do we even know what events we are collecting?**
- Do we write a report together?
- Do we do a tabletop exercise?
- What metrics can we use?
- Who else should be included?

# Purple Teaming Challenges

What about during the execution?

# Purple Teaming: Ad-Hoc Execution! (I Love it!)

Lee Christensen @tifkin\_ Just adding to the list of autorun evasions. Having some fun back and forth with @Cyb3rWard0g :)

```
PS C:\> Get-ItemProperty 'HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Utilman.exe' | select Debugger
Debugger
\\.\C:\windows\system32\cmd.exe /c calc.exe

PS C:\> Get-ItemProperty 'HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe' | select Debugger
Debugger
C:\windows\system32\cmd.exe /c calc.exe
```

Autoruns [DESKTOP-8VASC5V]\ee - Sysinternals: www.sysinternals.com

File Entry Options User Help

Hide Empty Locations  Hide Microsoft Entries  Hide Windows Entries  Hide VirusTotal Clean Entries  Scan Options...  Font...

Filter:

Category	Description	Publisher
Windows NT\CurrentVersion\Image File Execution Options	sethc.exe	Windows Co., Microsoft Co.
Windows NT\CurrentVersion\Image File Execution Options	sethc.exe	Windows Co., Microsoft Co.
Windows NT\CurrentVersion\Image File Execution Options	Microsoft Command Processor\Autorun	Windows Co., Microsoft Co.
Windows NT\CurrentVersion\Image File Execution Options	Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	Windows Co., Microsoft Co.
Windows NT\CurrentVersion\Image File Execution Options	sethc.exe	Windows Co., Microsoft Co.
Windows NT\CurrentVersion\Image File Execution Options	Microsoft Command Processor\Autorun	Windows Co., Microsoft Co.
Windows NT\CurrentVersion\Image File Execution Options	Wow6432Node\Microsoft\Command Processor\Autorun	Windows Co., Microsoft Co.
Windows NT\CurrentVersion\Image File Execution Options	HCU\Software\Microsoft\Command Processor\Autorun	Windows Co., Microsoft Co.
Windows NT\CurrentVersion\Image File Execution Options	HKEY\Software\Classes\Exefile\ShellOpen\Command\(\Default)	Windows Co., Microsoft Co.
Windows NT\CurrentVersion\Image File Execution Options	HKEY\Software\Classes\Exefile\ShellOpen\Command\(\Default)	Windows Co., Microsoft Co.

Roberto Rodriguez @Cyb3rWard0g · Jan 17, 2018  
Replies to @tifkin\_ Slow down Brah! ❤️❤️❤️🍺😊

Event Properties - Event 13, Sysmon

General - Details	
Registry value set:	
EventID:	SetValue
UtcTime:	2018-01-17 18:01:27.530
ProcessId:	[a98268c1-8ecf-5a5f-0000-00101cc6801]
ThreadId:	704
Image:	C:\Windows\regedit.exe
TargetObject:	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\notepad.exe\Debugger
File Execution Options:	notepad.exe\Debugger
Details:	\\.\C:\Windows\System32\cmd.exe /c calc.exe

Event Log Name: Microsoft-Windows-Symon/Operational

Event Properties - Event 4088, Sysmon

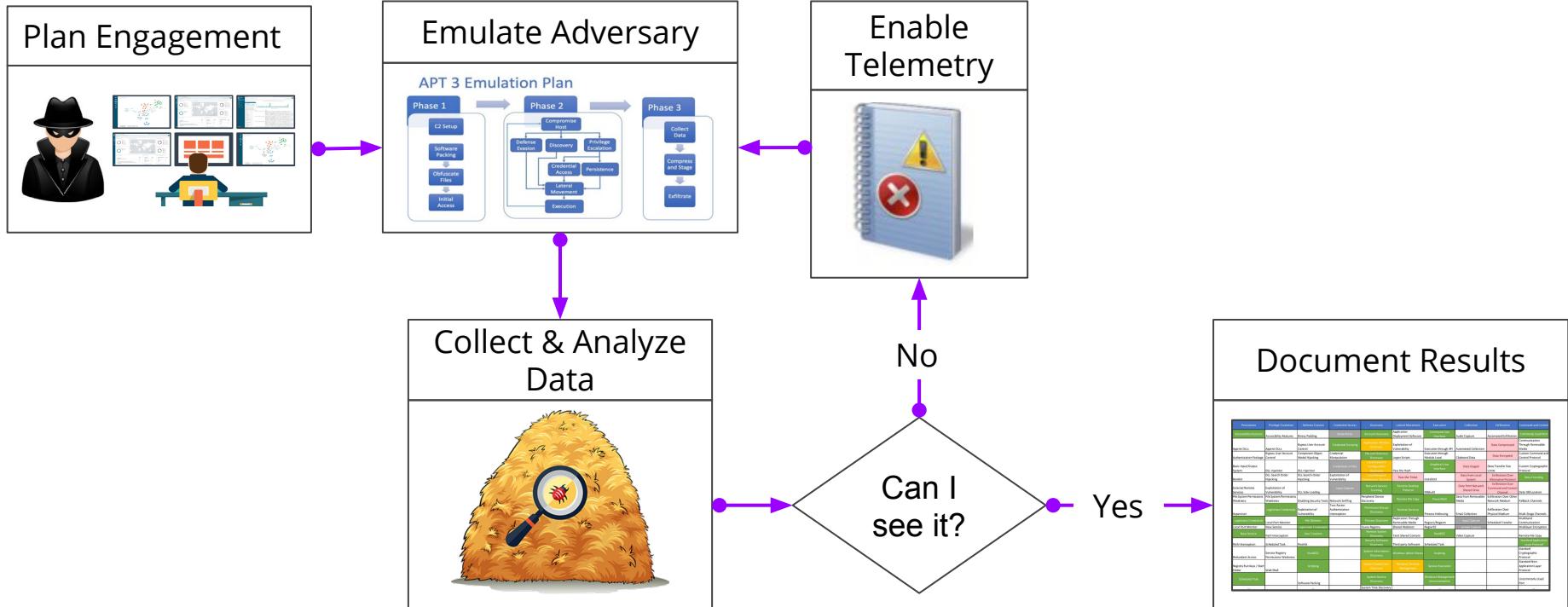
Security - Number of events: 17230   New events available	
EventID:	4088
Number of events:	17230   New events available
Keywords:	Event Type: SetValue
Date and Time:	2018-01-17 12:48:14.457
Source:	System
Processor ID:	[a98268c1-8ecf-5a5f-0000-00101cc6801]
Process ID:	704
Image:	C:\Windows\regedit.exe
TargetObject:	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\notepad.exe\Debugger
File Execution Options:	notepad.exe\Debugger
Details:	(Empty)

Event Log Name: Microsoft-Windows-Symon/Operational

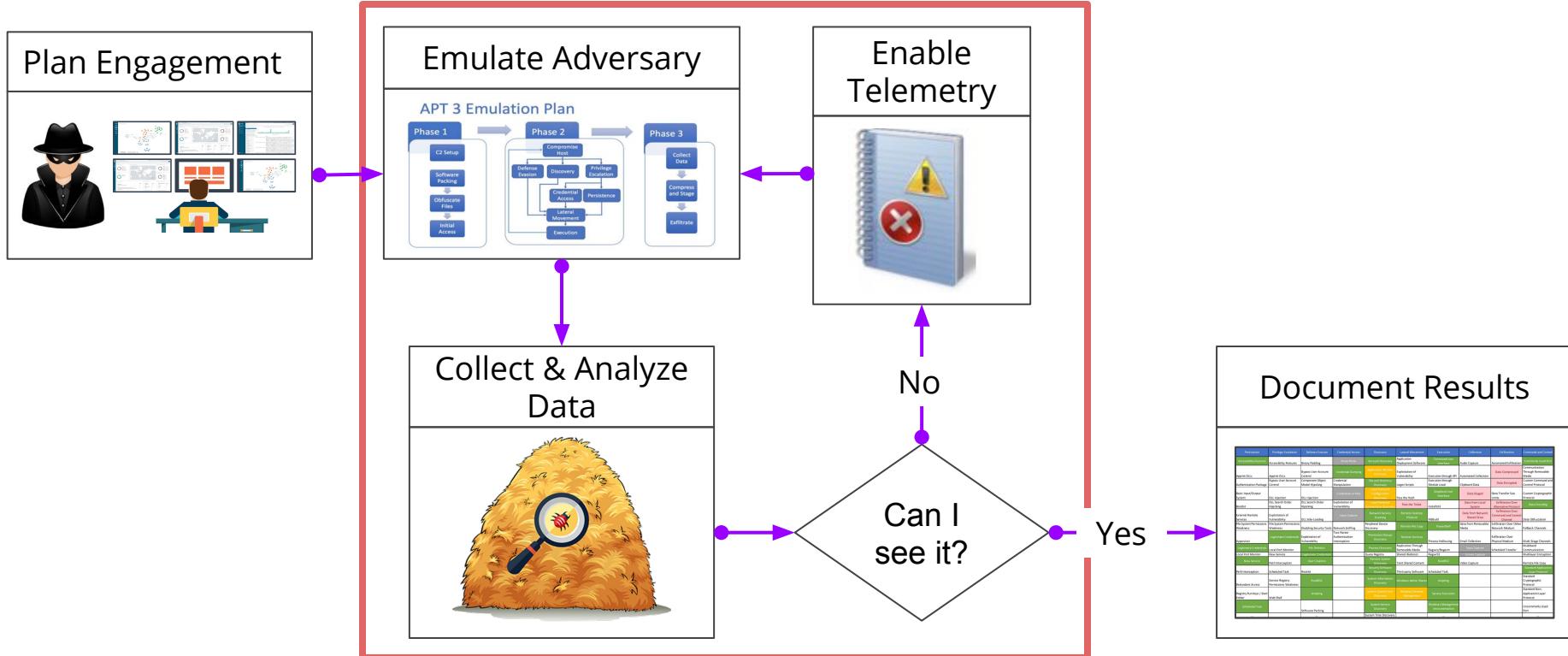
Event Properties - Event 4088, Sysmon

General - Details	
Process Information:	New Process ID: 13
New Process Name:	C:\Windows\System32\cmd.exe
Token Elevation Type:	9%198
Mandatory Label:	Mandatory Label: Medium Mandatory Level
Current Thread ID:	0
Creator Process Name:	C:\Windows\System32\winlogon.exe
Processor Command Line:	\\.\C:\Windows\System32\cmd.exe /c calc.exe utilman.exe /debug

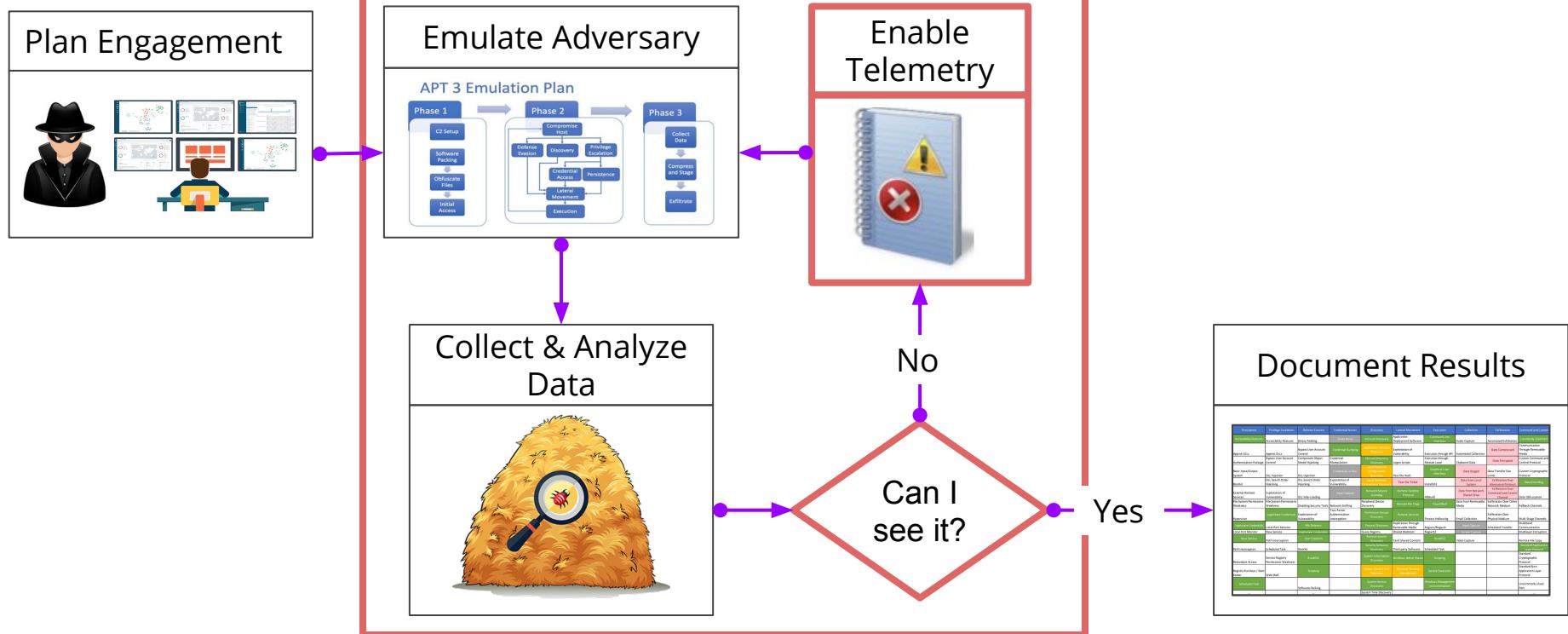
# Purple Teaming: Basic Planned Execution



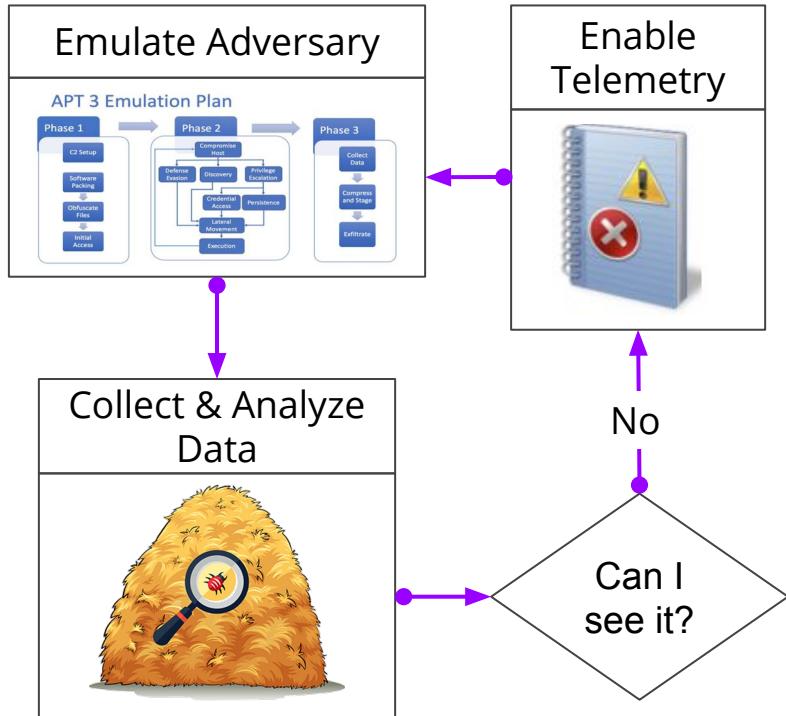
# Purple Teaming: Basic Planned Execution



# Purple Teaming: Basic Planned Execution

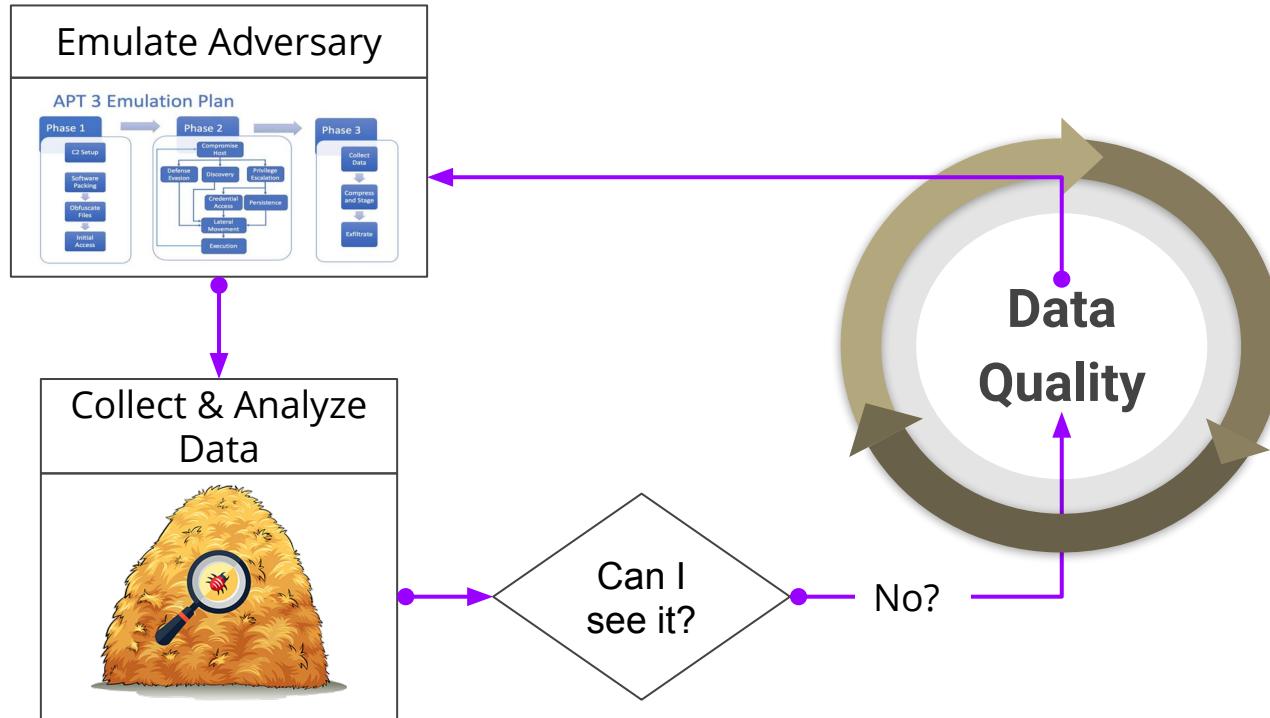


# Planned Execution: Production Challenges

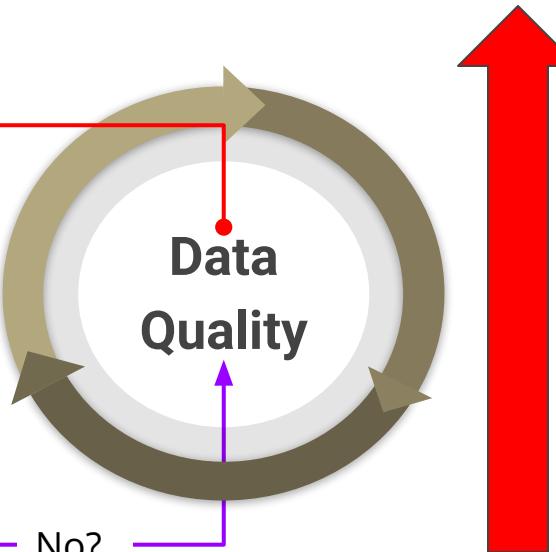
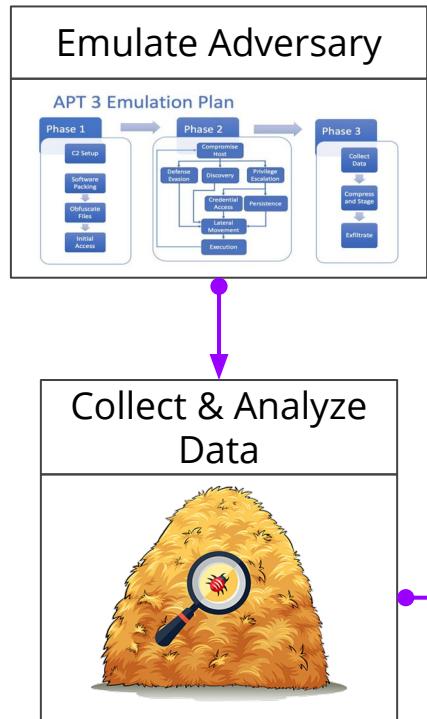


- How do you know what you need if you can't even see it?
- How long would it take to approve an audit policy change?
- How do you know the log volume that you are about to enable?
- How do you know it is not your data pipeline failing?
- What if your event logs are not parsed or standardized?

# Planned Execution: Production Challenges



# Planned Execution: Production Challenges



Impacts Time Scope



# Planned Execution: Production Challenges



Time Spent



Time Spent

# We all have busy schedules



# Purple Teaming: Ad-Hoc Execution! (I Love it!)



Lee Christensen  
@tifkin\_

Just adding to the list of autorun evasions. Having some fun back and forth with @Cyb3rWard0g :)

```
PS C:\> Get-ItemProperty 'HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Utilman.exe' | select Debugger
Debugger
\\.\C:\windows\system32\cmd.exe /c calc.exe

PS C:\> Get-ItemProperty 'HKLM:\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe' | select Debugger
Debugger
\\.\C:\windows\system32\cmd.exe /c calc.exe
```



Roberto Rodriguez @Cyb3rWard0g · Jan 17, 2018  
Replies to @tifkin\_  
Slow down Brah! ❤️❤️❤️🍺😊

```
Image: C:\Windows\System32\calc.exe
CommandLine: calc.exe "C:\WINDOWS\system32\notepad.exe"
CurrentDirectory: C:\Windows\system32
UserId: DESKTOP-29D84T
LogonGuid: {a98268c1-4a6e-5a5f-0000-002097580003}
LogonId: 0x4097
TerminalSessionId: 1
IntegrityLevel: Medium
Hasher: SHA1=823d0f89344c2c4f13a0b277202d5f58ea684
MD5=180469ae0239e313b4c65f02f070bc15ha256=8c92532a408056819c40091f5fa7afaa15625100e817806056
IMPHASH=1AC96822B8A1514C532728332921
ParentProcessGuid: {a98268c1-4a6e-5a5f-0000-00101cc68001}
ParentProcessId: 142
ParentImageName: C:\Windows\System32\cmd.exe
ParentCommandLine: \\.\C:\Windows\System32\cmd.exe /C calc.exe *C:\WINDOWS\system32\notepad.exe"
```

```
Log Name: Microsoft-Windows-Symon\Operational
Source: Symon
Event ID: 1
Level: Information
User: SYSTEM
Logged: 1/17/2018 10:01:35 AM
Task Category: Process Create (rule: ProcessCreate)
Keywords:
Computer: DESKTOP-29D84T
```

```
Registry value set:
EventID: SetValue
UtcTime: 2018-01-17 10:01:45.57
ProcessId: {a98268c1-4a6e-5a5f-0000-00101cc68001}
Process: Tmp
Image: C:\Windows\regedit.exe
TargetObject: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\notepad.exe\Debugger
Details: (Empty)
```

```
Log Name: Microsoft-Windows-Symon\Operational
Source: Symon
Event ID: 13
Level: Information
Logged: 1/17/2018 10:00:14 AM
Task Category: Registry value set (rule: RegistryEvent)
Keywords:
```

Event Properties - Event 13, Symon

General - Details

Registry value set:  
EventID: SetValue  
UtcTime: 2018-01-17 10:01:27.530  
ProcessId: {a98268c1-4a6e-5a5f-0000-00101cc68001}  
ProcessId: 704  
Image: C:\Windows\regedit.exe  
TargetObject: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\notepad.exe\Debugger  
Details: \\.\C:\Windows\System32\cmd.exe /C calc.exe

Event Properties - Event 4088, Microsoft Windows security auditing

General - Details

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	1/17/2018 12:48:14 PM	Microsoft Windows security auditing	4688	Process Creation
Audit Success	1/17/2018 12:48:13 PM	Microsoft Windows security auditing	4688	Process Creation
Audit Success	1/17/2018 12:48:13 PM	Microsoft Windows security auditing	4688	Process Creation
Audit Success	1/17/2018 12:46:45 PM	Microsoft Windows security auditing	4688	Process Creation
Audit Success	1/17/2018 12:46:45 PM	Microsoft Windows security auditing	4688	Process Creation

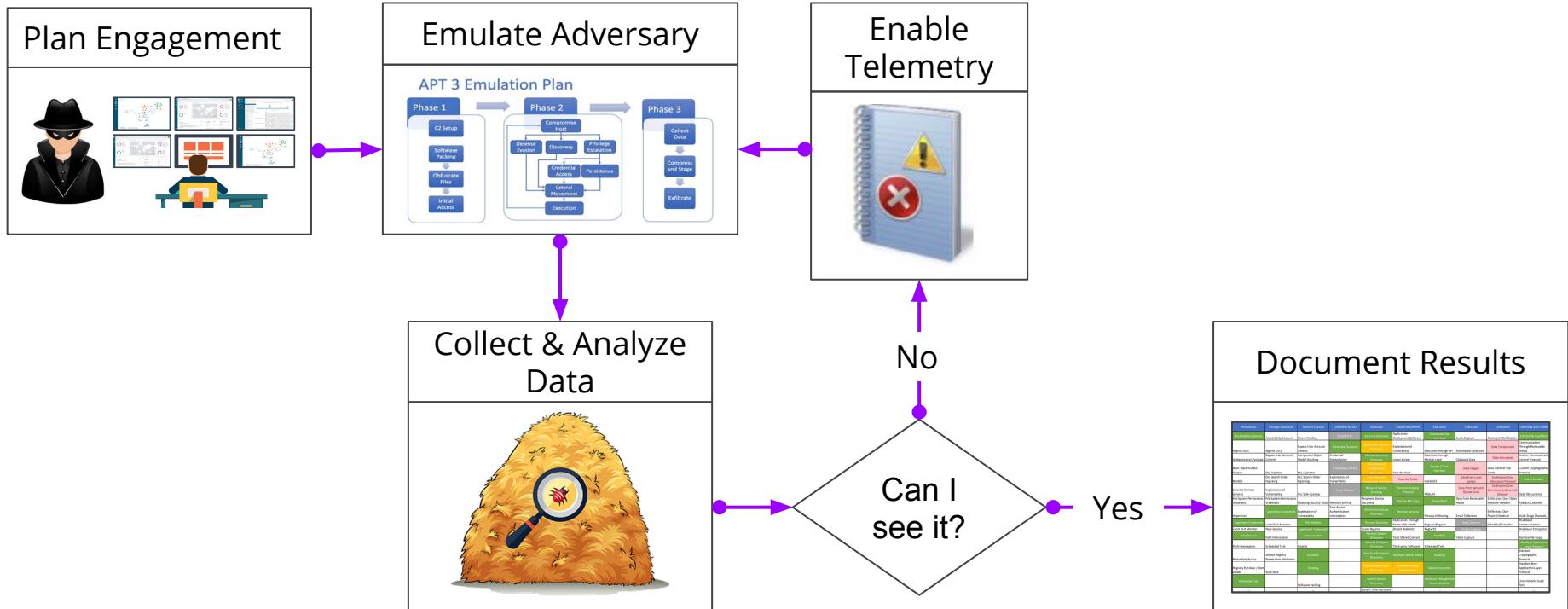
Event 4088, Microsoft Windows security auditing

General - Details

Process Information:  
Old Process ID: 0  
New Process ID: 0  
New Process Name: C:\Windows\System32\cmd.exe  
Token Elevation Type: 0  
Mandatory Label: Mandatory Label: Medium Mandatory Level  
Current Process ID: 0  
Creator Process Name: C:\Windows\System32\winlogon.exe  
Processor Command Line: \\.\C:\Windows\System32\cmd.exe /C calc.exe utilman.exe /debug



# Planned Execution: A Lab Before Production



# We can start improving this!



Time Spent

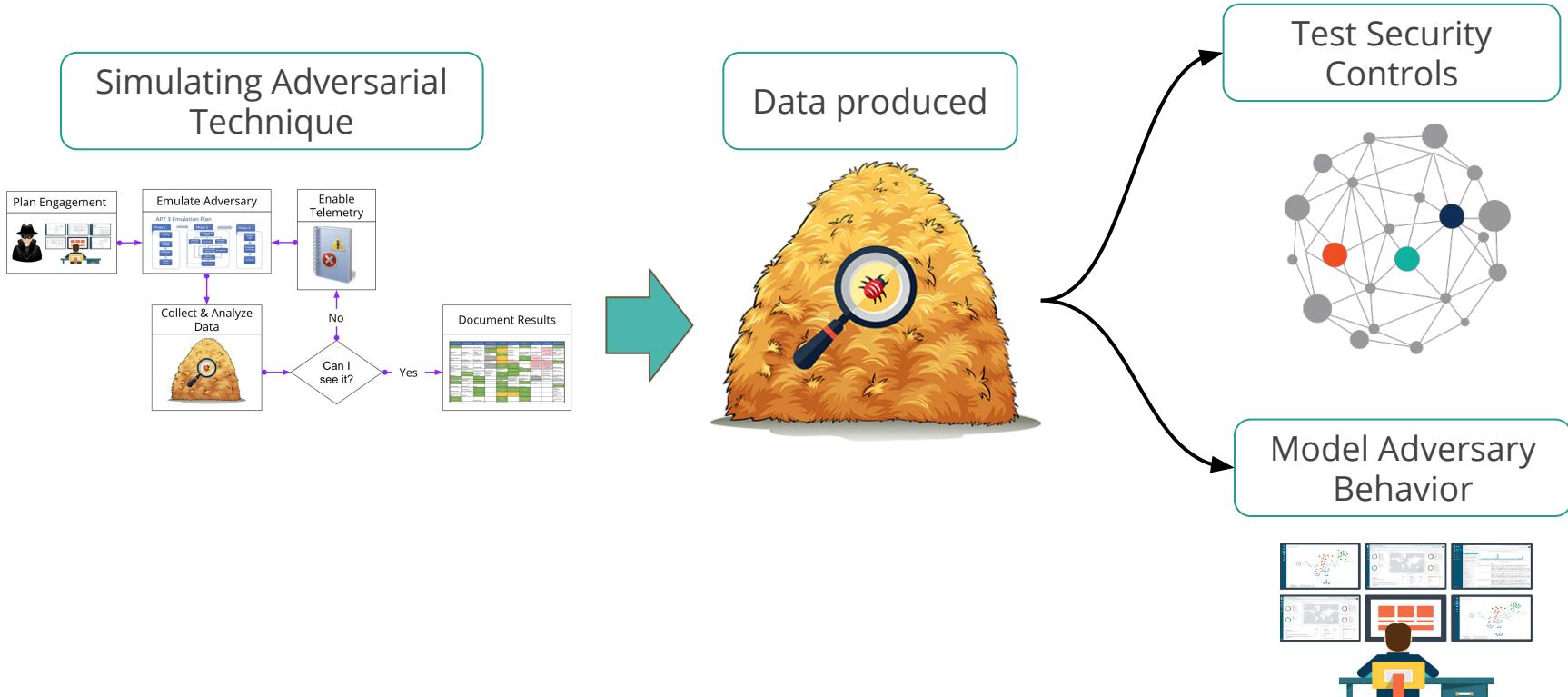


Time Spent

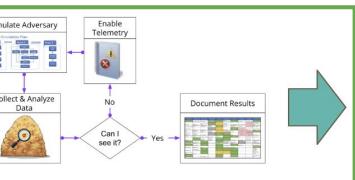
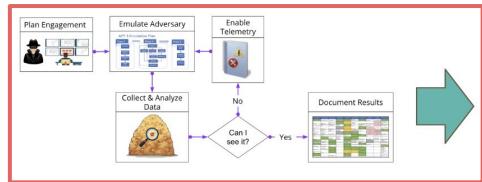
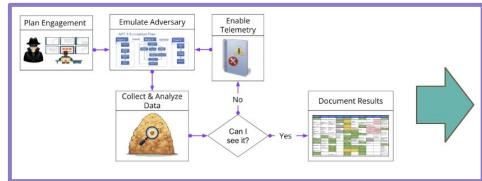
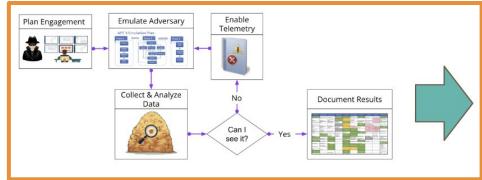
# Purple Teaming Challenges

Can you run this technique variation  
one more time?

# Execute -> Collect -> Analyze -> Repeat



# Same Technique + Some Variations



Data produced



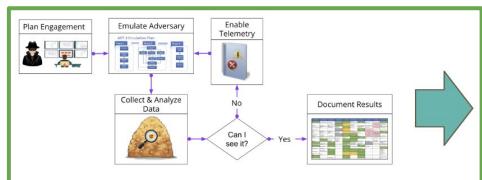
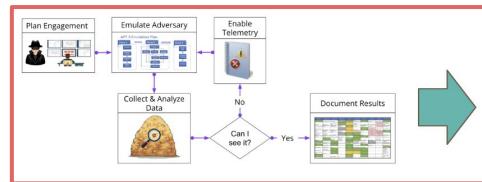
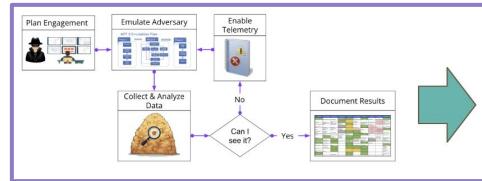
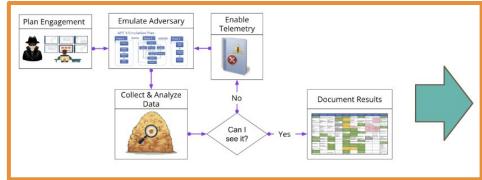
Test Security Controls



Model Adversary Behavior



# Same Technique + Some Variations



## Data produced



# Test Security Controls



# Model Adversary Behavior

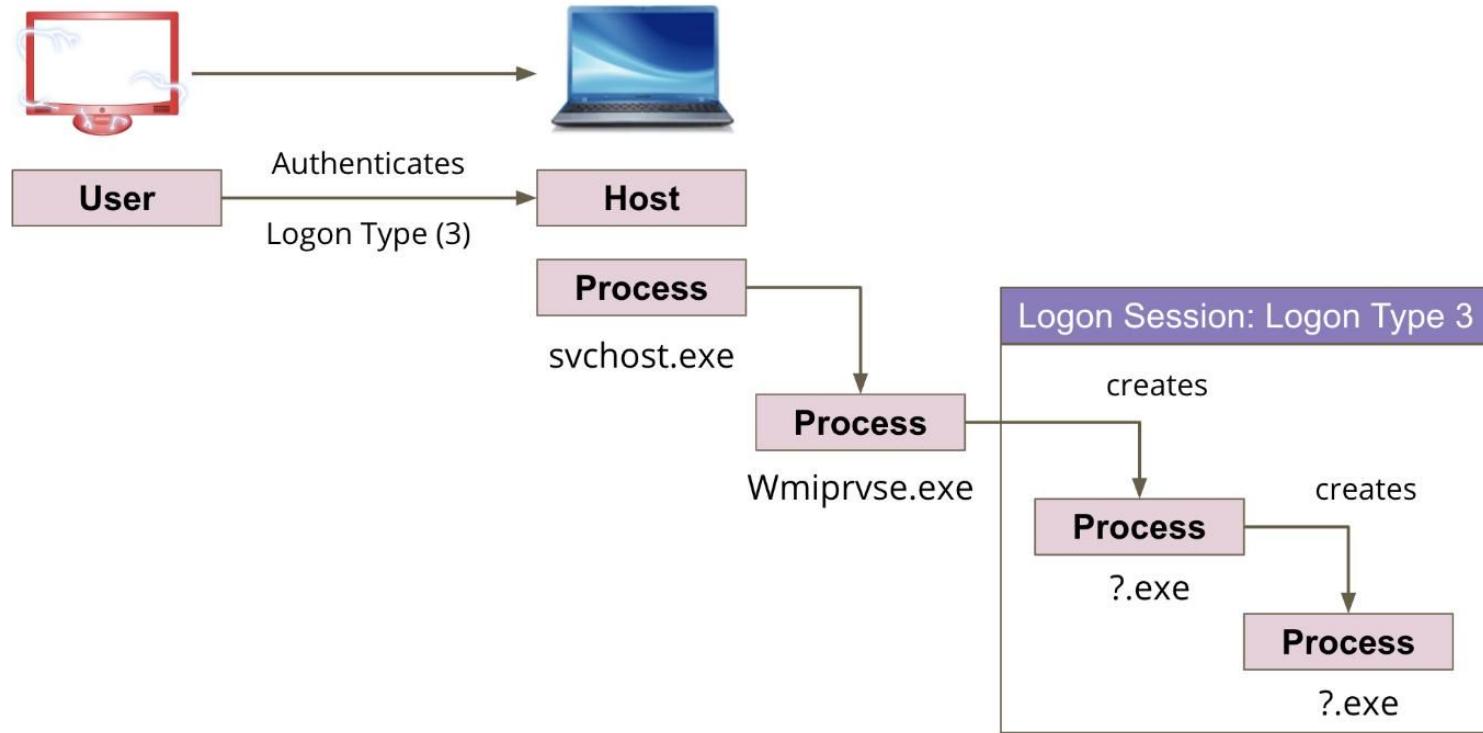


# Same Data? Similar Events?

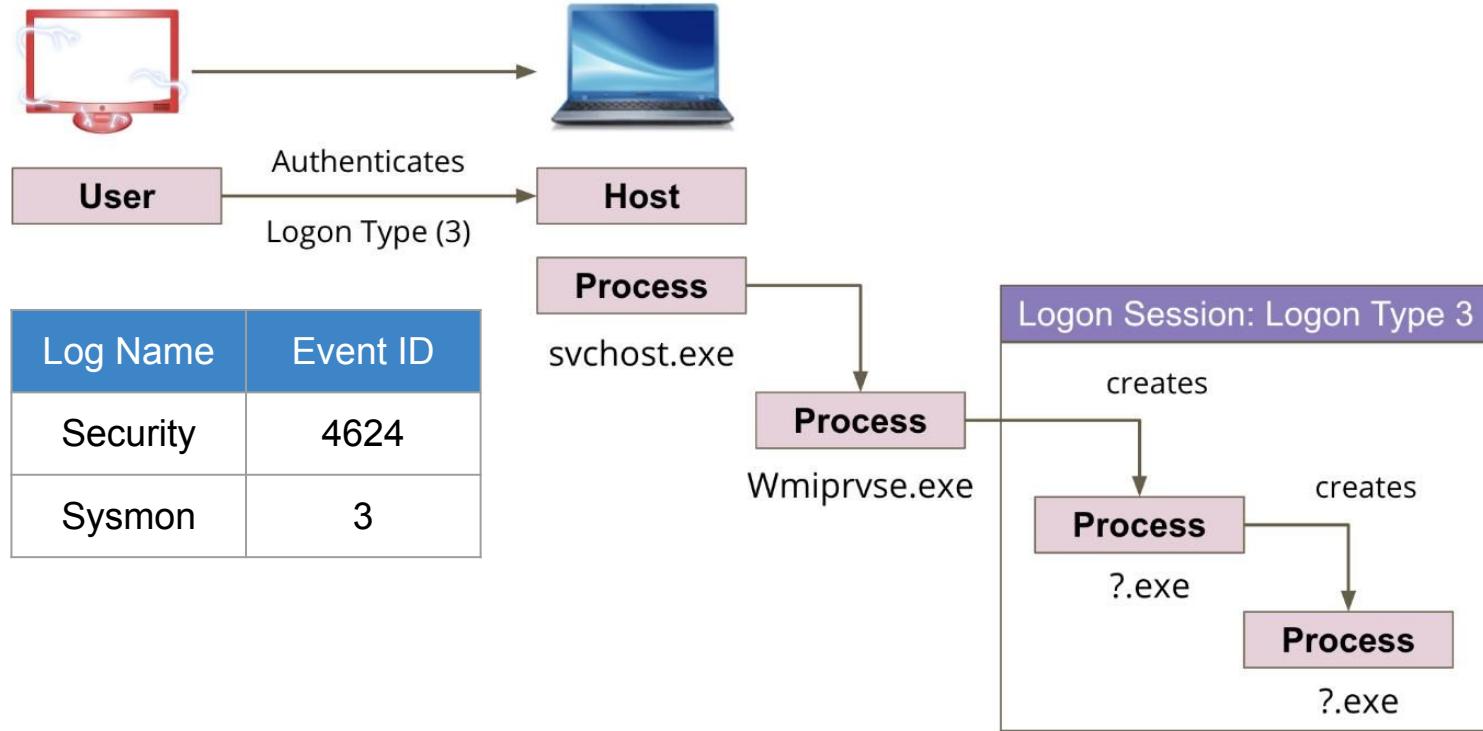
# Lateral Movement via WMI (Win32\_Process Create)

- **wmic** /node:172.18.39.106 /user:Administrator /password:P1ls3n! process call create cmd.exe
- **Invoke-WmiMethod** -ComputerName 172.18.39.106 -Credential Administrator -Class Win32\_Process -Name Create -ArgumentList notepad.exe
- **SharpWMI.exe** action=create computername=HR01.shire.com command="powershell.exe -enc ZQBj..."
- **./wmieexec** shire.com/pgustavo@172.18.39.106

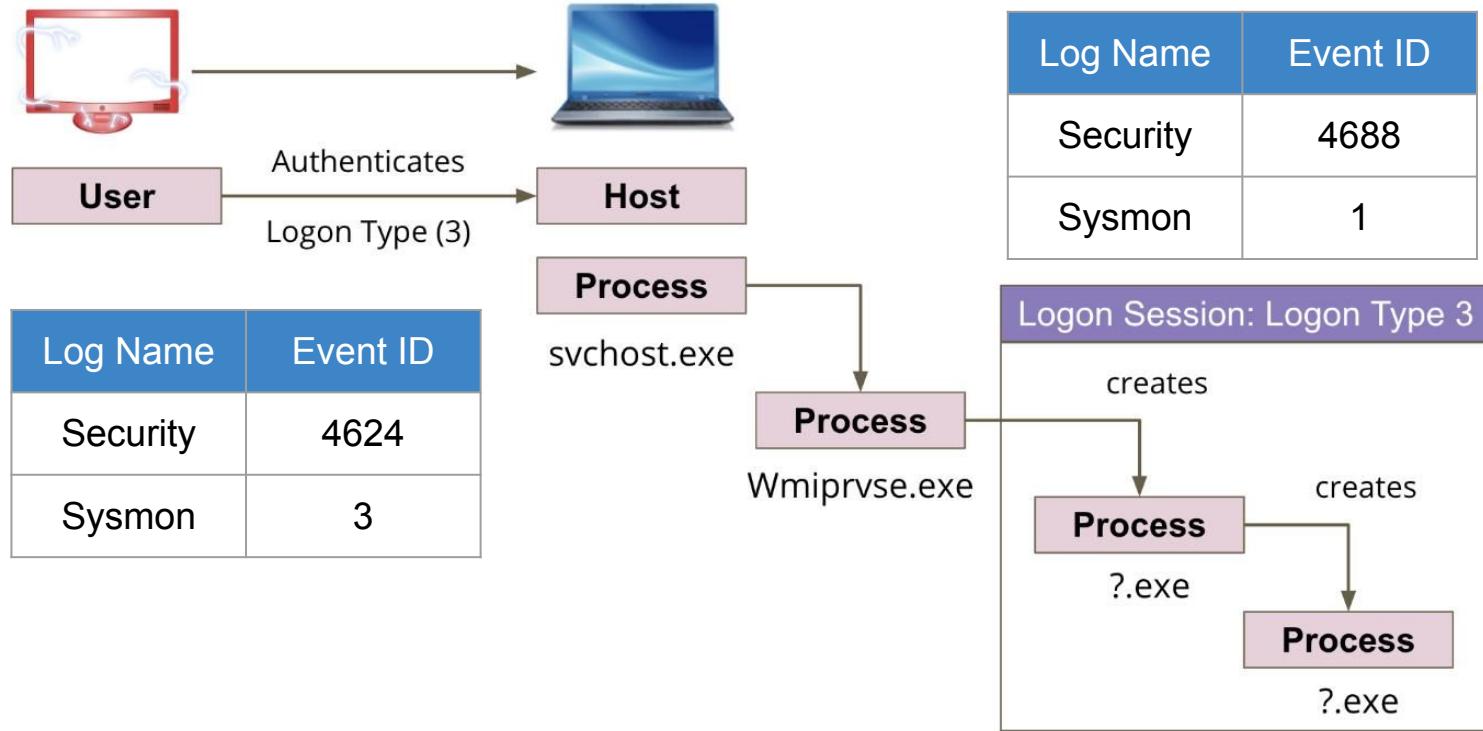
# Lateral Movement via WMI - Behavior



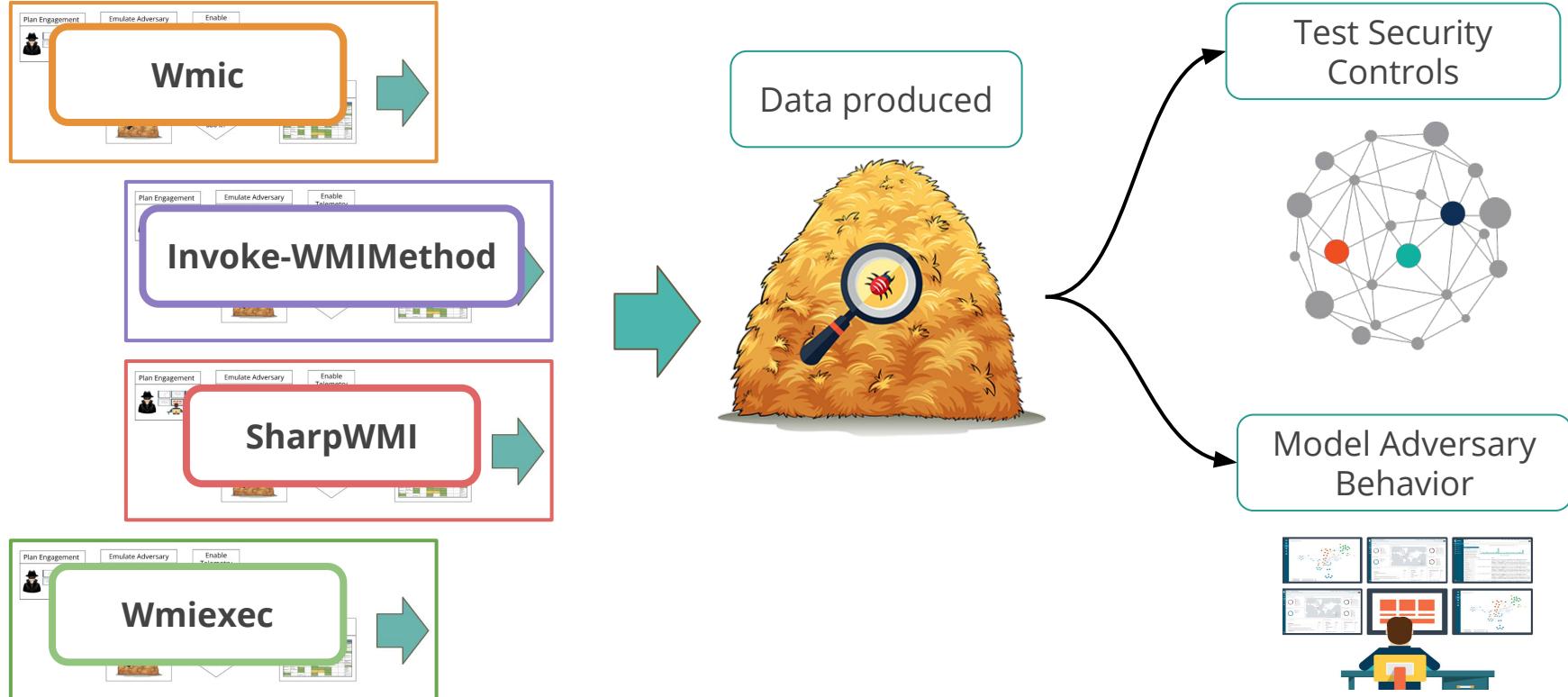
# Lateral Movement via WMI - Behavior



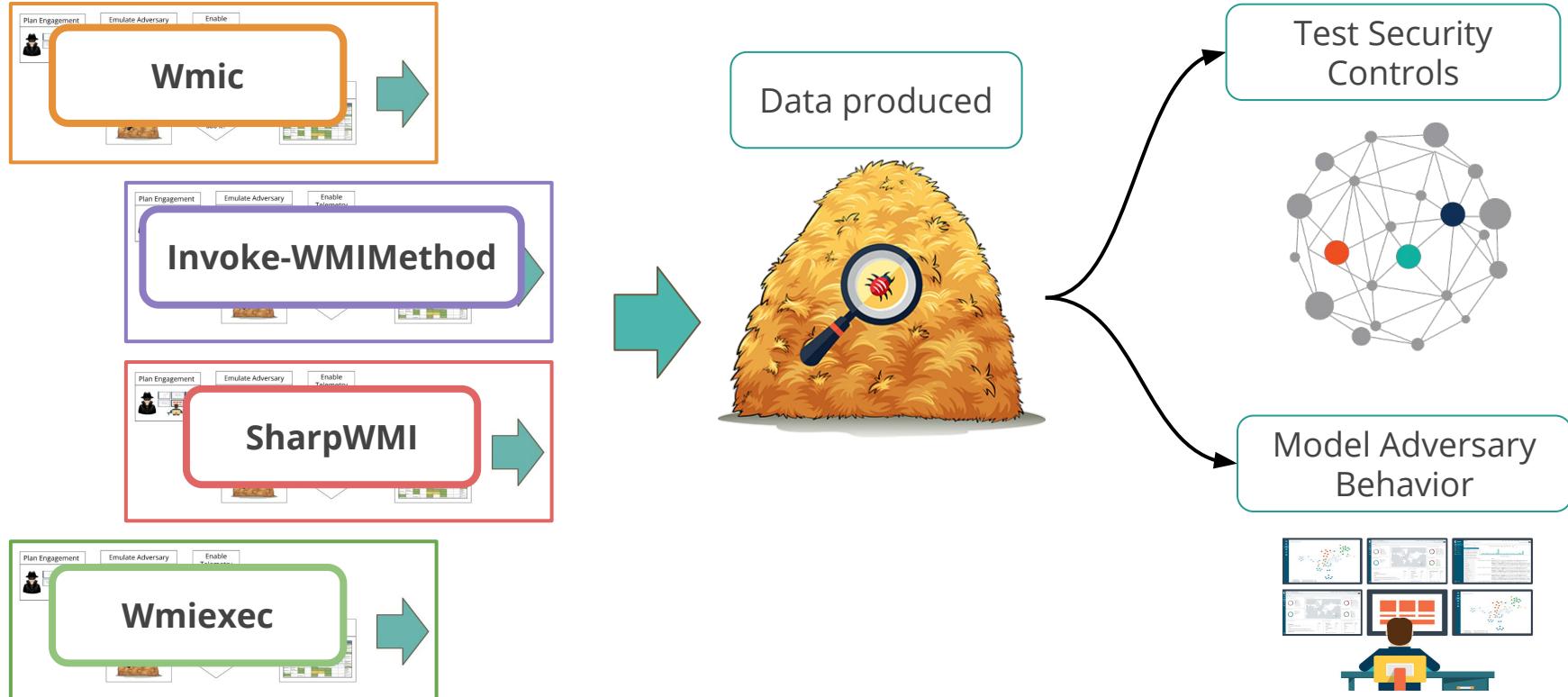
# Lateral Movement via WMI - Behavior



# Same Technique + Some Variations



# Can you run it again? Please!



# But... We are getting similar events...



Data produced

Log Name	Event ID
Security	4624
Sysmon	3
Security	4688
Sysmon	1

Test Security Controls



Model Adversary Behavior



# Are we being effective at purple teaming?

# I Effective or Efficient Purple Teaming?

Efficiency

Efficacy

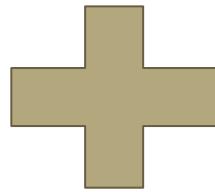


Effectiveness

# Efficiency



The way resources are used (or wasted), How can I make the most of the resources I have



# Efficacy



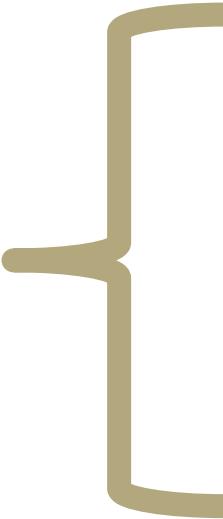
It doesn't matter how we do it,  
but only on what we accomplish

# Effectiveness

Accomplishes the goals (to be efficacious) employing the best and most economic methodology (to be efficient).

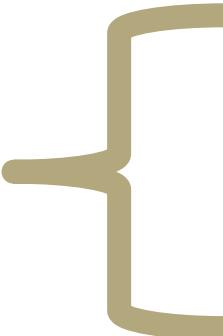


# Efficiency



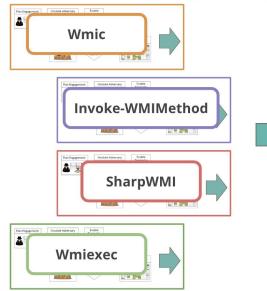
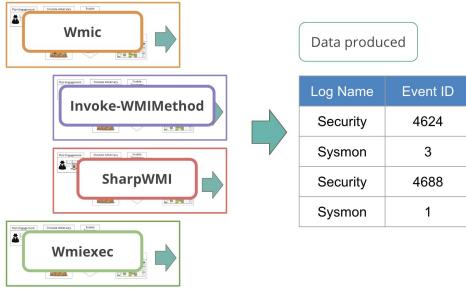
- Let's prioritize specific techniques
- Can we automate adversary emulation plans?
- How do we replicate results?
- How do we expedite unit testing?
- How do I reduce the number of times a technique is executed for research?

# Efficacy

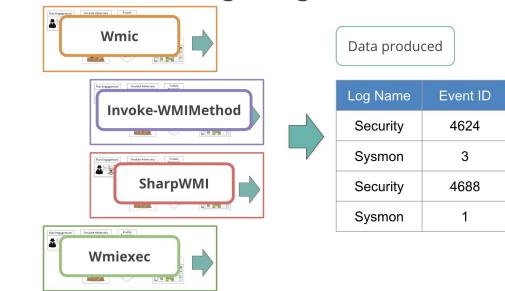
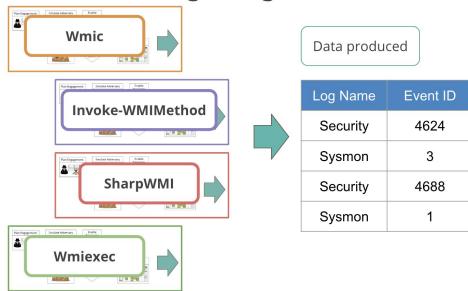
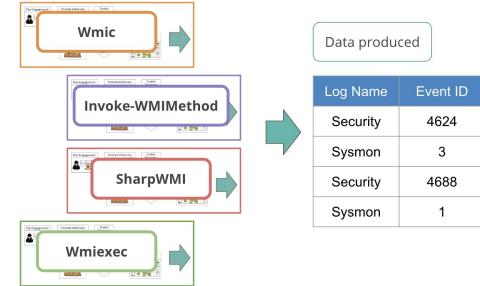


- Let's execute 5 techniques a week !
- At least 3 variations per technique!
- Let's emulate all APT groups!
- Let's test current security analytics!

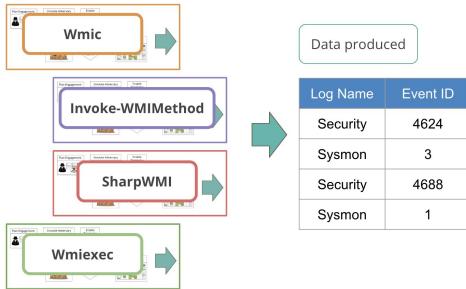
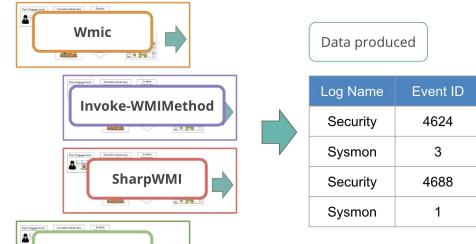
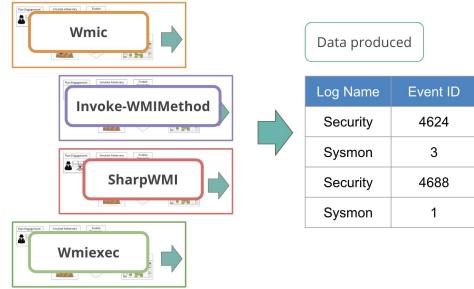
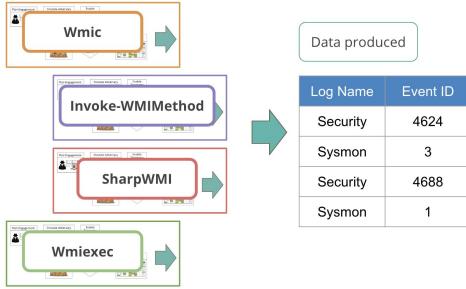
# We might be doing this over and over..



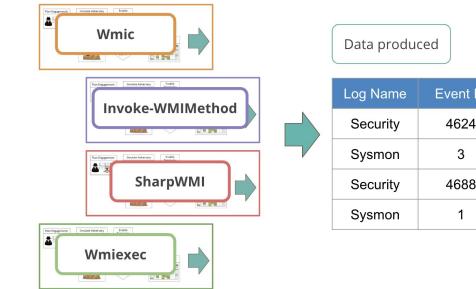
Log Name	Event ID
Security	4624
Sysmon	3
Security	4688
Sysmon	1



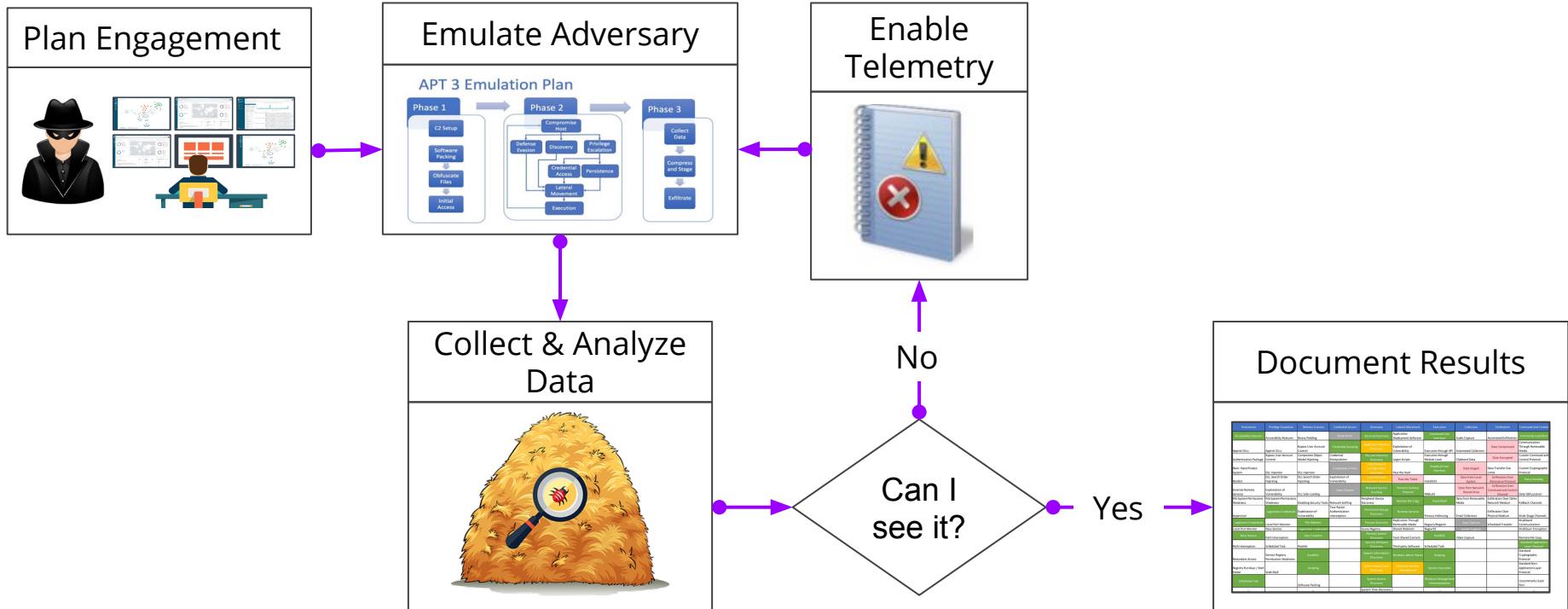
# And we still get similar events..



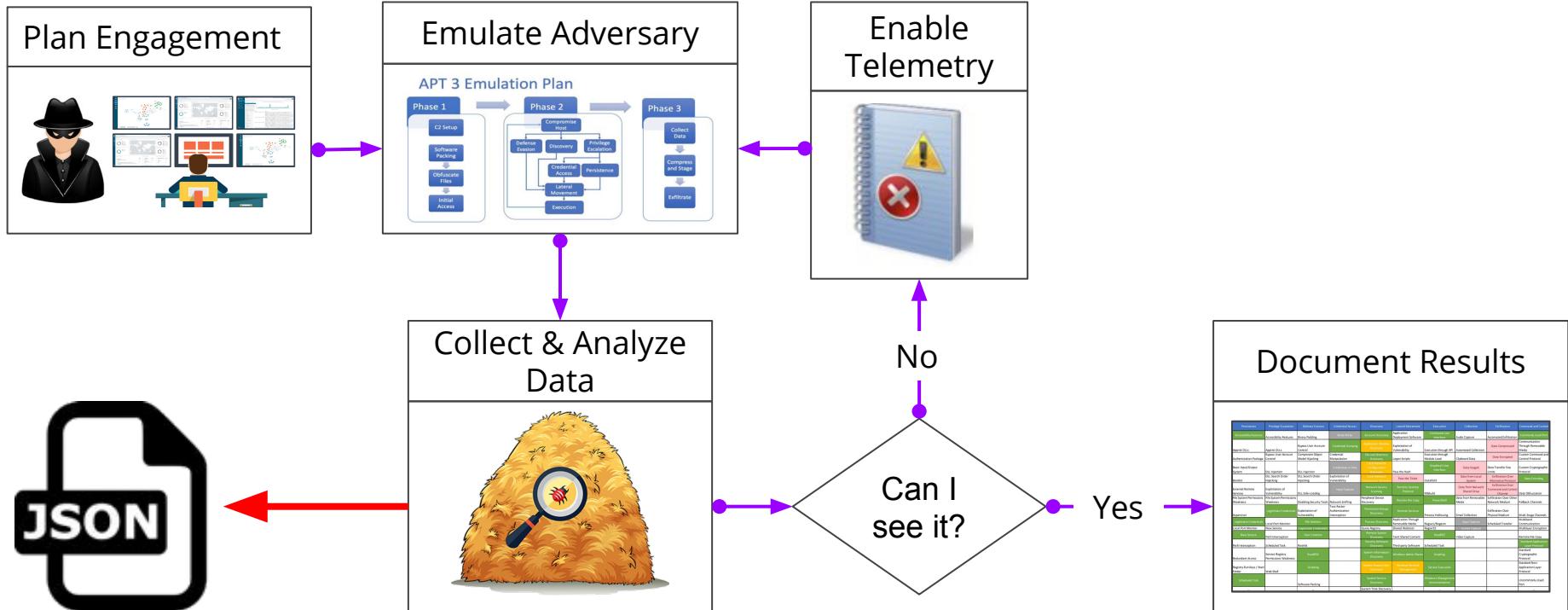
Log Name	Event ID
Security	4624
Sysmon	3
Security	4688
Sysmon	1



# What if we could save our output?



# What if we could save our output?



# We could keep the momentum!

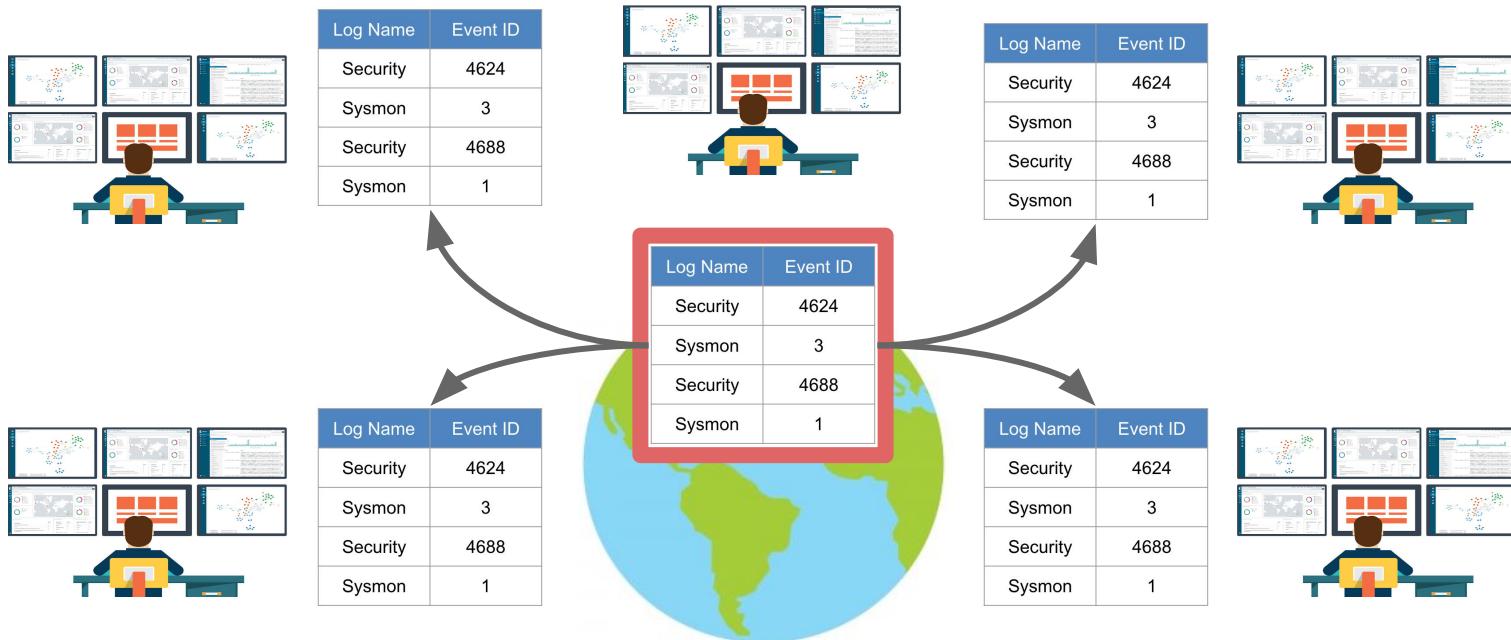


Time Spent

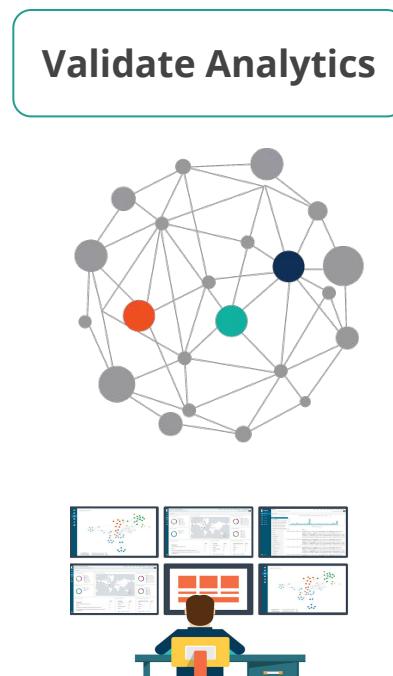
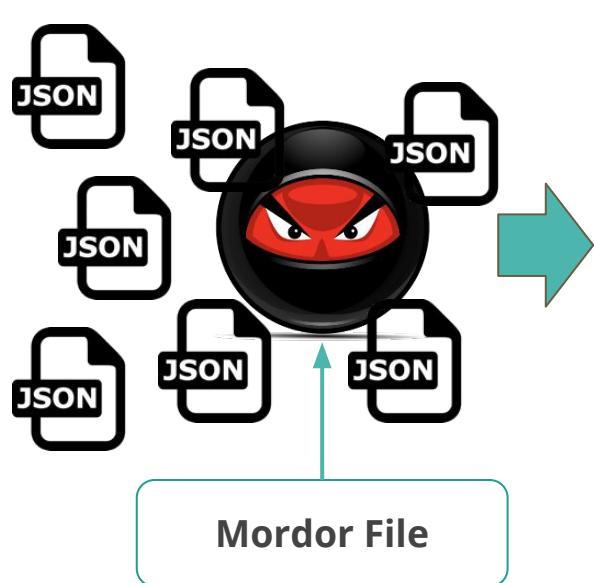


Time Spent

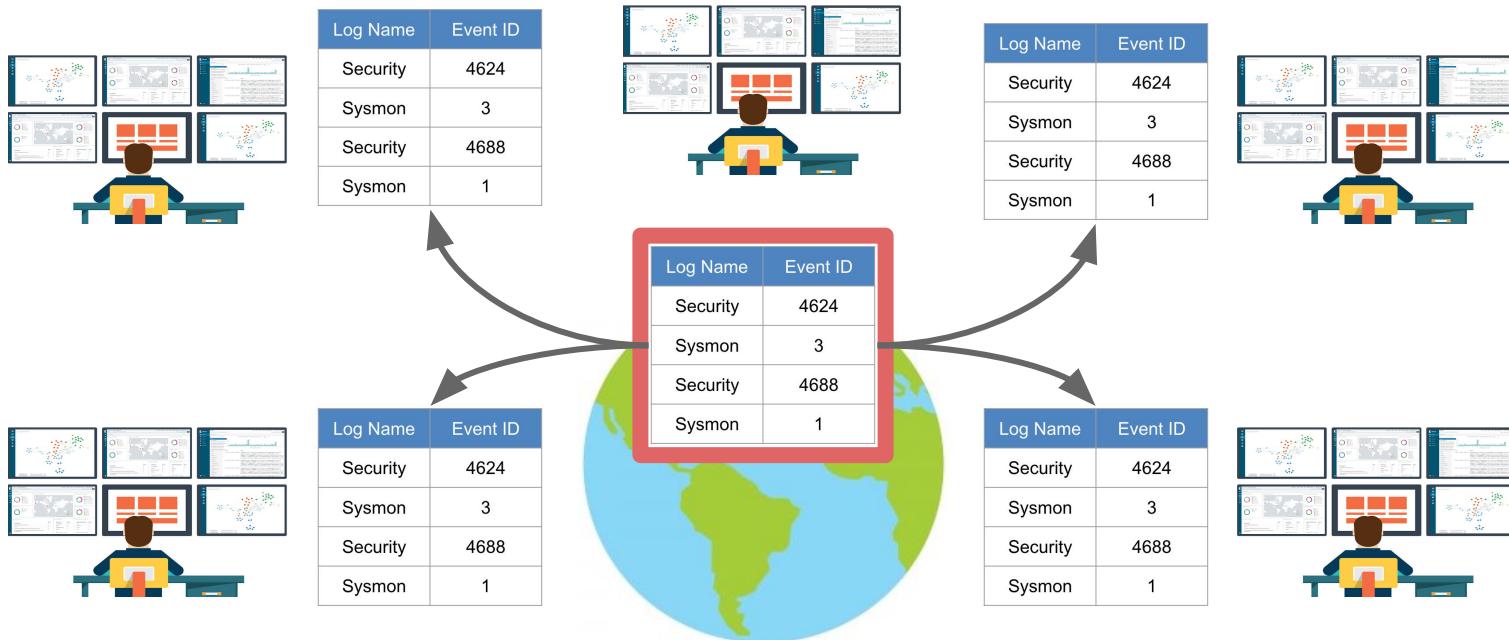
# We could also train future purple teamers!



# We could expedite analytic validation - Unit Testing



# We could also help the community!



# Enter Mordor

# Mordor Project @Mordor\_Project

- Pre-recorded security events generated by simulated adversarial techniques in the form of JavaScript Object Notation (JSON)
- Pre-recorded data categorized by platforms, adversary groups, tactics and techniques defined by the Mitre ATT&CK Framework.
- Data represents not only specific known malicious events but additional context/events that occur around it.



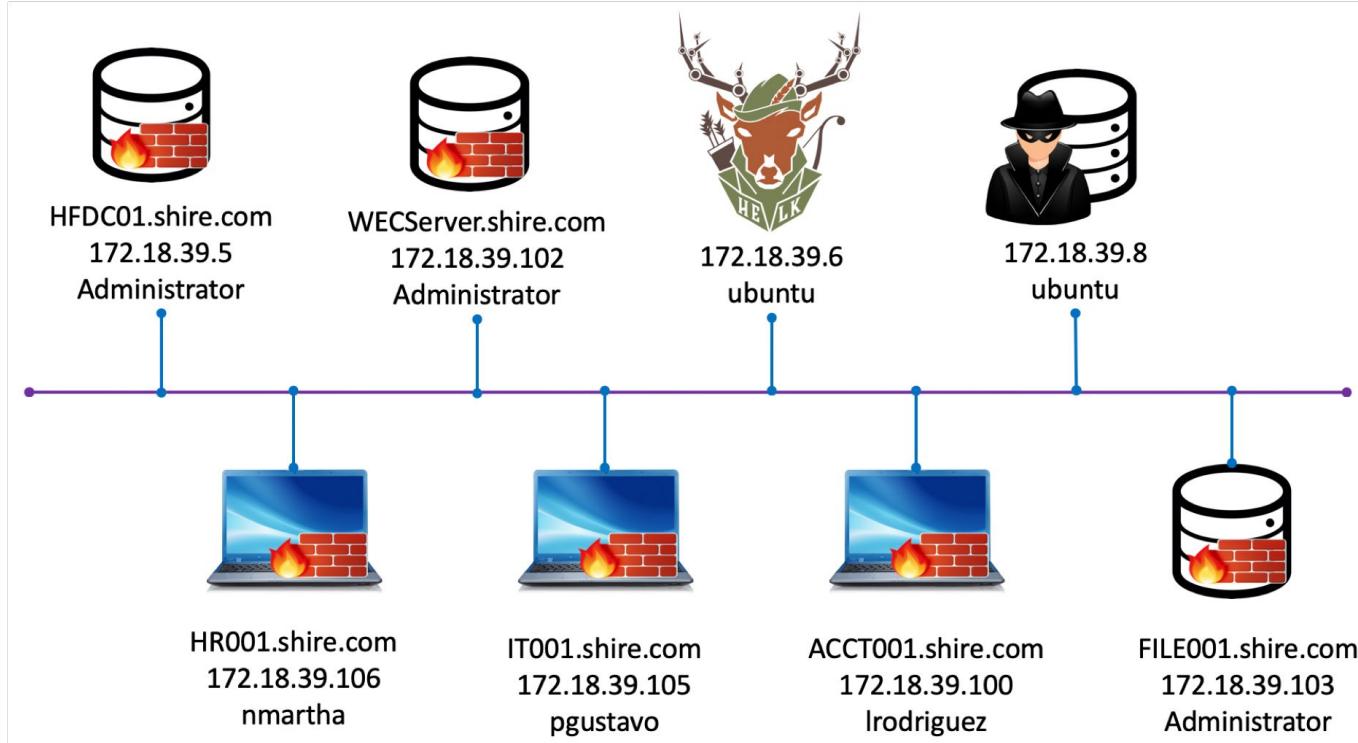
# Mordor Standard Environments

- Environment designed to replicate a small research network
- Standardized and documented setup
- Platforms
  - Windows
  - Linux
- Endpoints Telemetry
  - Windows Security Auditing
  - Event Tracing for Windows (ETW) (NEW!!)
- Network Telemetry
  - Network Logs
- Environments Available: Shire and Erebor deployed by **BlackSmith!**

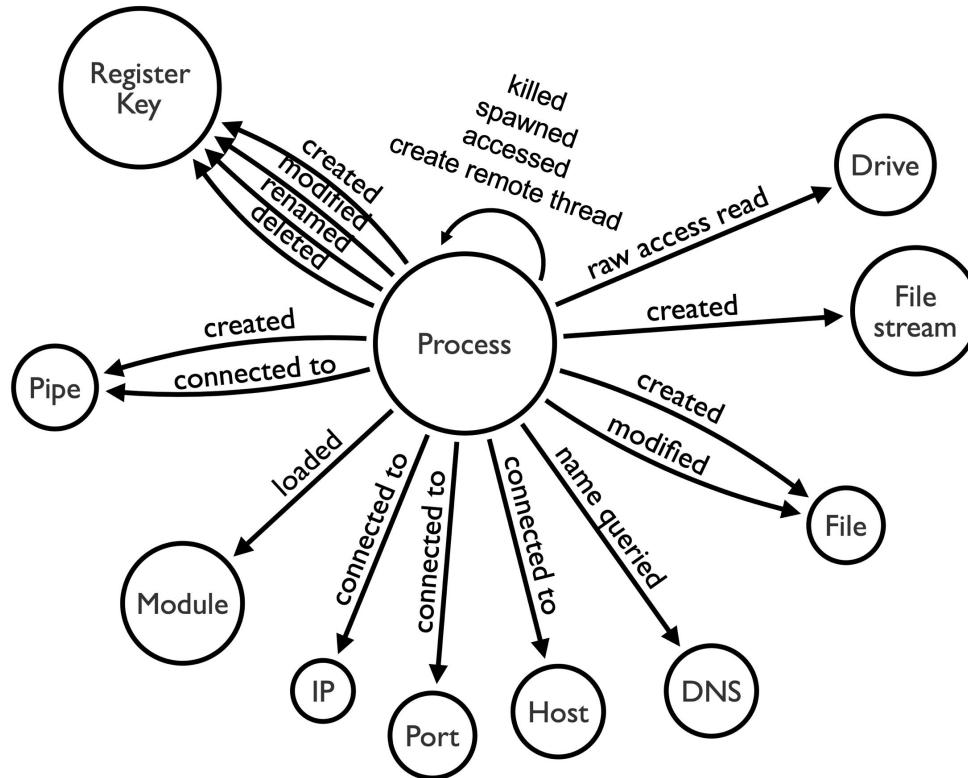
# Mordor Environments: The Shire



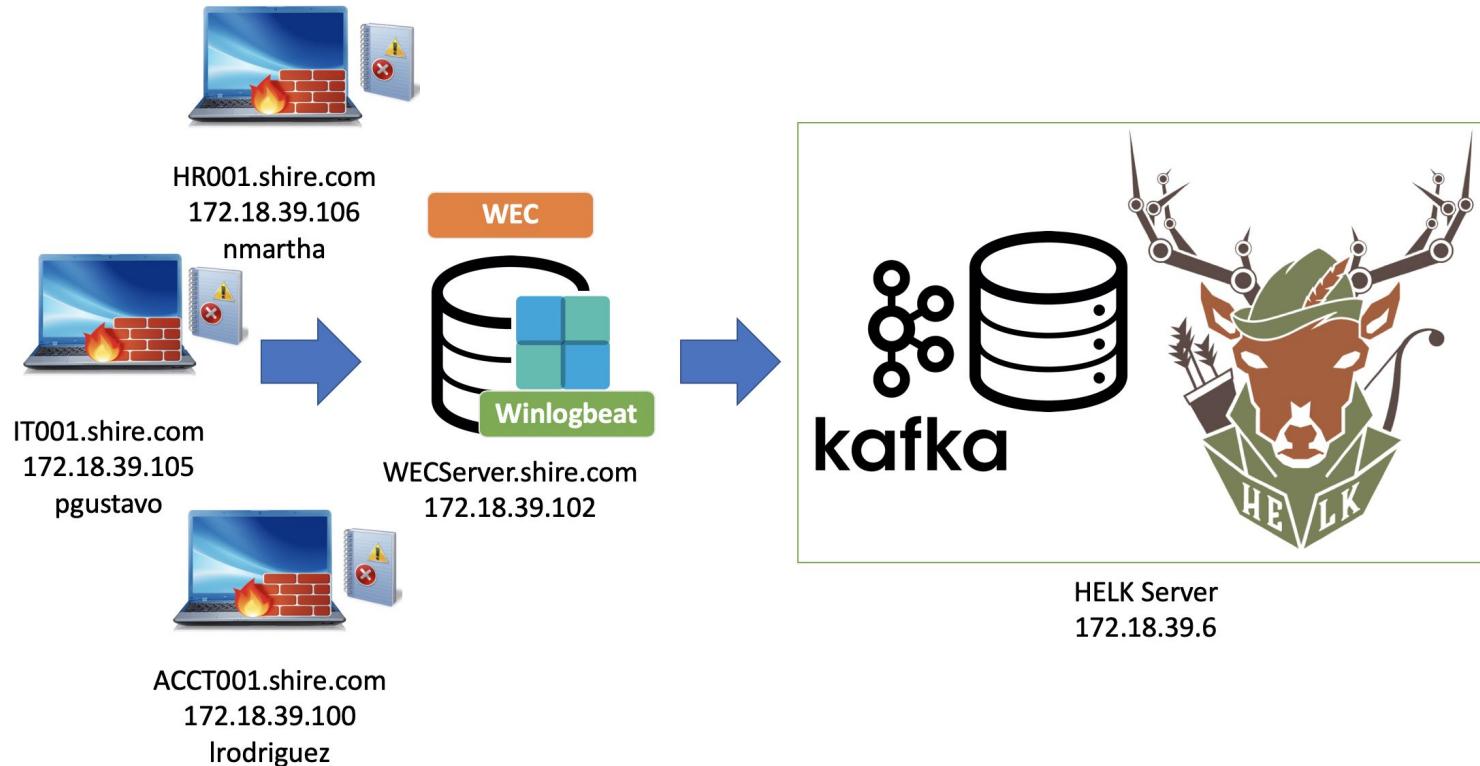
# The Shire Design



# The Shire Telemetry: Win Logs & Sysmon



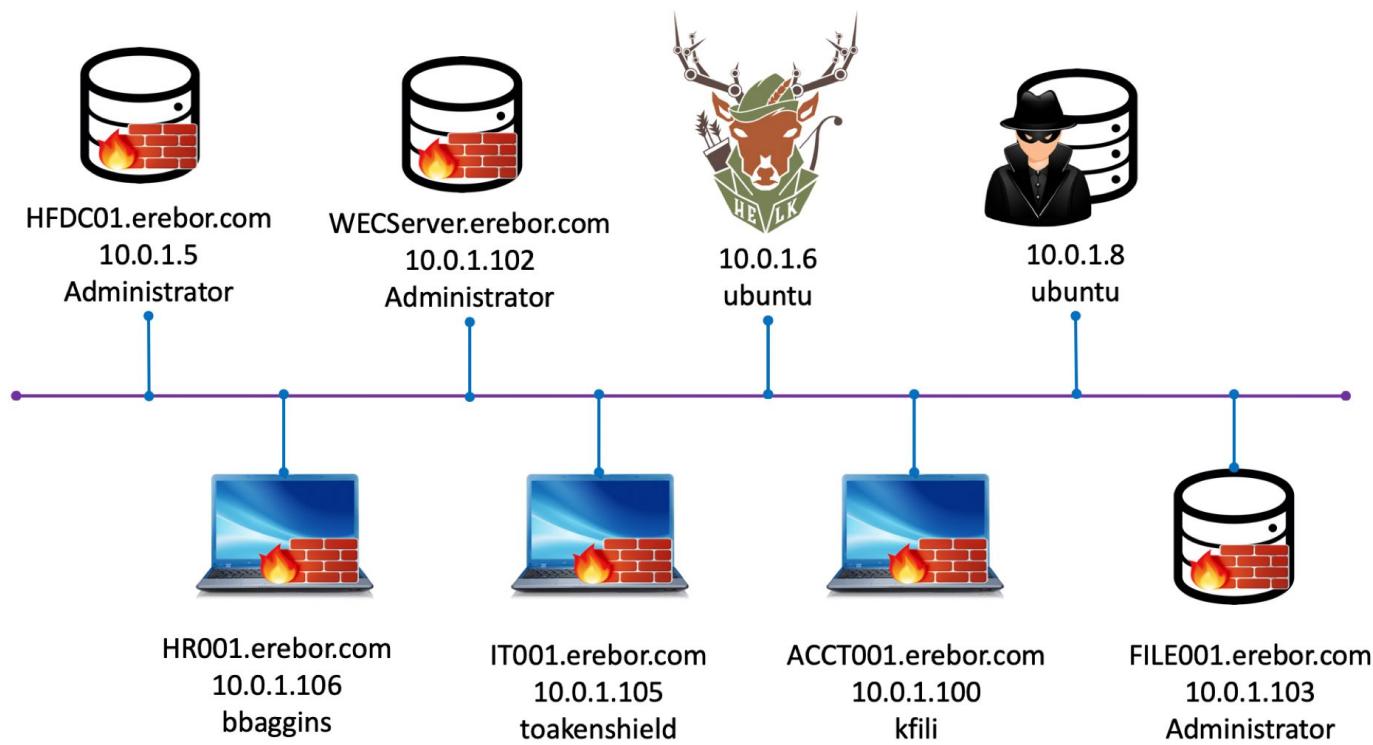
# The Shire: Event Log -> WEC -> HELK



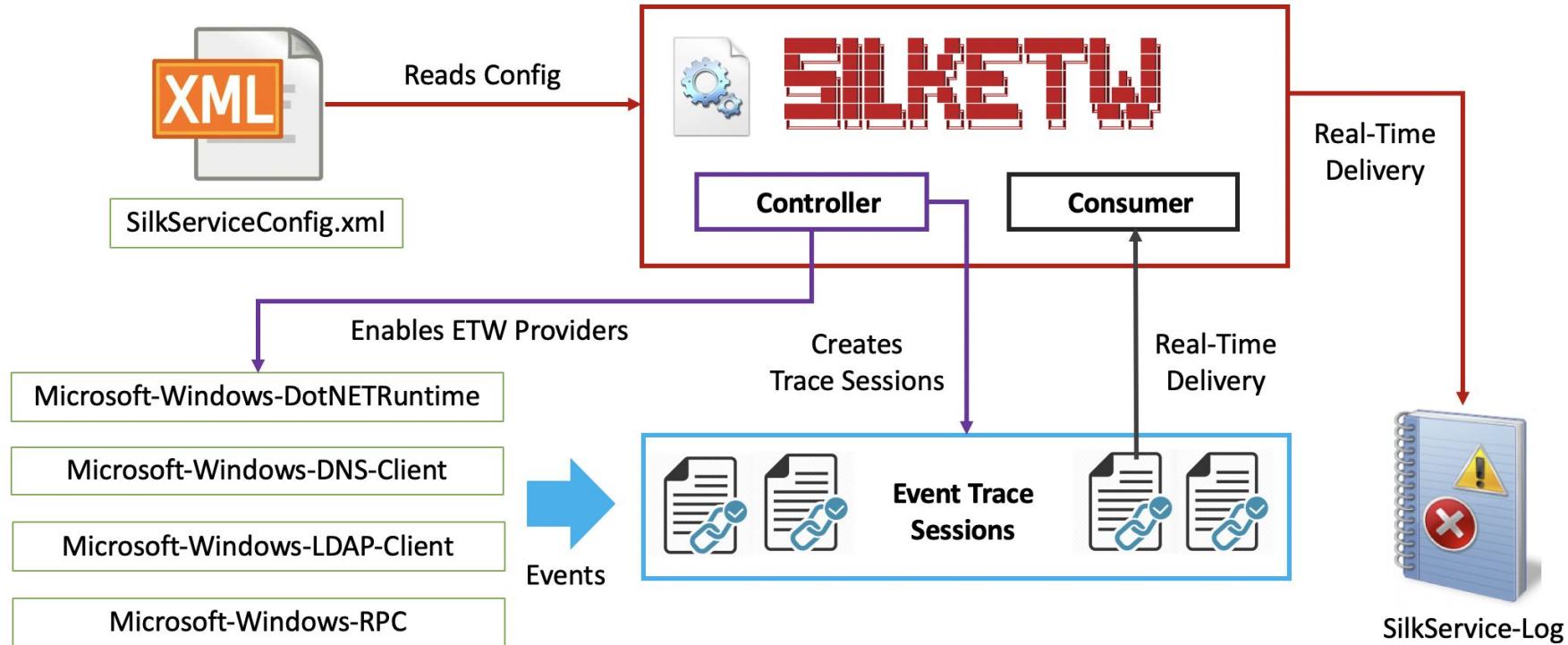
# Mordor Environments: Erebor (Lonely Mountain)



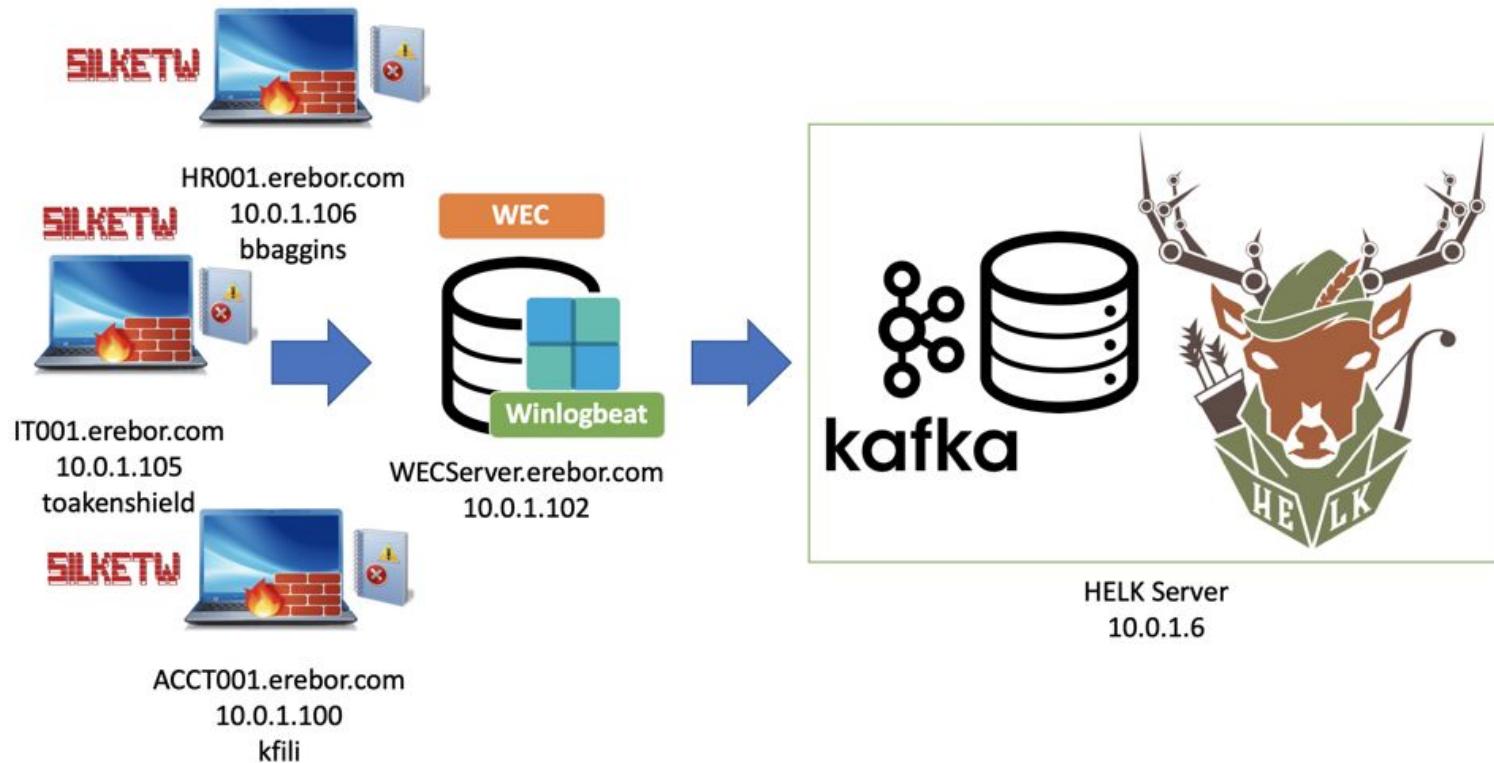
# Erebor Design



# Erebor Telemetry: ETW Events via SilkETW



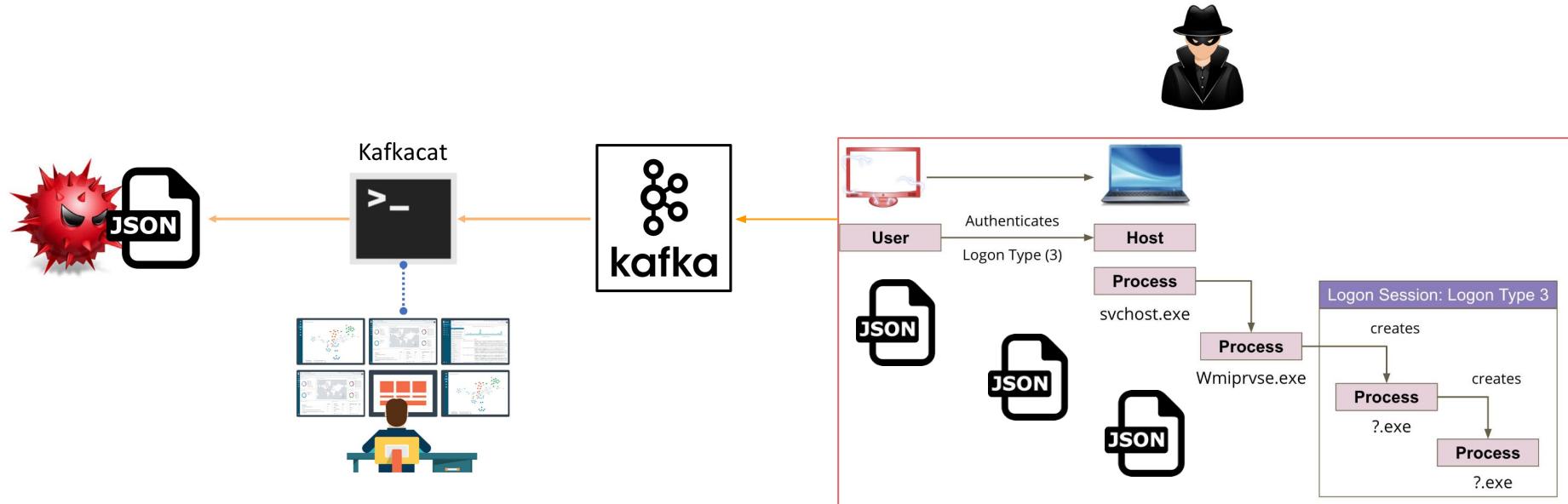
# Erebor: ETW Events -> Event Log -> WEC -> HELK



# How do you export (consume) data?

- I use **Kafkacat!**
- kafkacat is a generic non-JVM producer and consumer for Apache Kafka >=0.8, think of it as a netcat for Kafka.
- **In consumer mode**
  - Kafkacat reads messages from a topic and prints them to standard output (stdout). You can also redirect it to a file
- **In producer mode**
  - Kafkacat reads messages from standard input (stdin). You can also send data to kafkacat by adding data from a file.

# Consuming Data -> Creating Mordor File

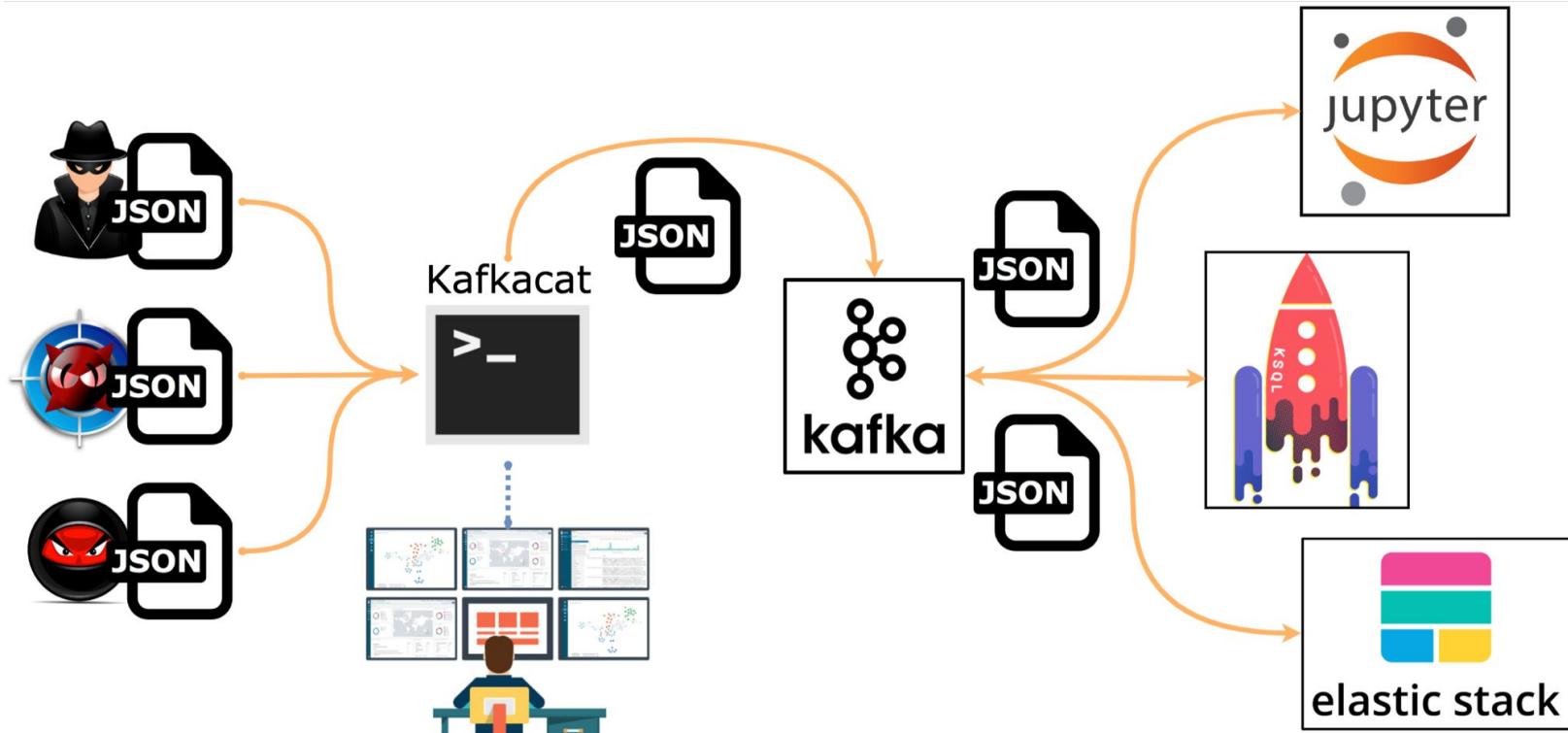


# Consuming Data (Taking a snapshot of data)

```
$ kafka-cat -b <Kafka-IP>:9092 -t  
<kafka-Topic> -C -o end > file.json
```

- **-b** : Kafka broker
- **-t** : Topic to consume from
- **-C** : Consumer Mode
- **-o** : Offset to start consuming from

# Producing Data (Injecting Adversary Dataset)



# Producing Data (Injecting Adversary Dataset)

```
$ kafka-cat -b <Kafka-IP>:9092 -t  
<kafka-Topic> -P -l file.json
```

- **-b** : Kafka broker
- **-t** : Topic to produce to
- **-P** : Producer Mode
- **-l** : Send messages from a file

# Can I download all the available Mordor datasets ?

```
$ git clone
```

```
https://github.com/hunters-forge/mordor.git
```

```
$ cd mordor/small_datasets/
```

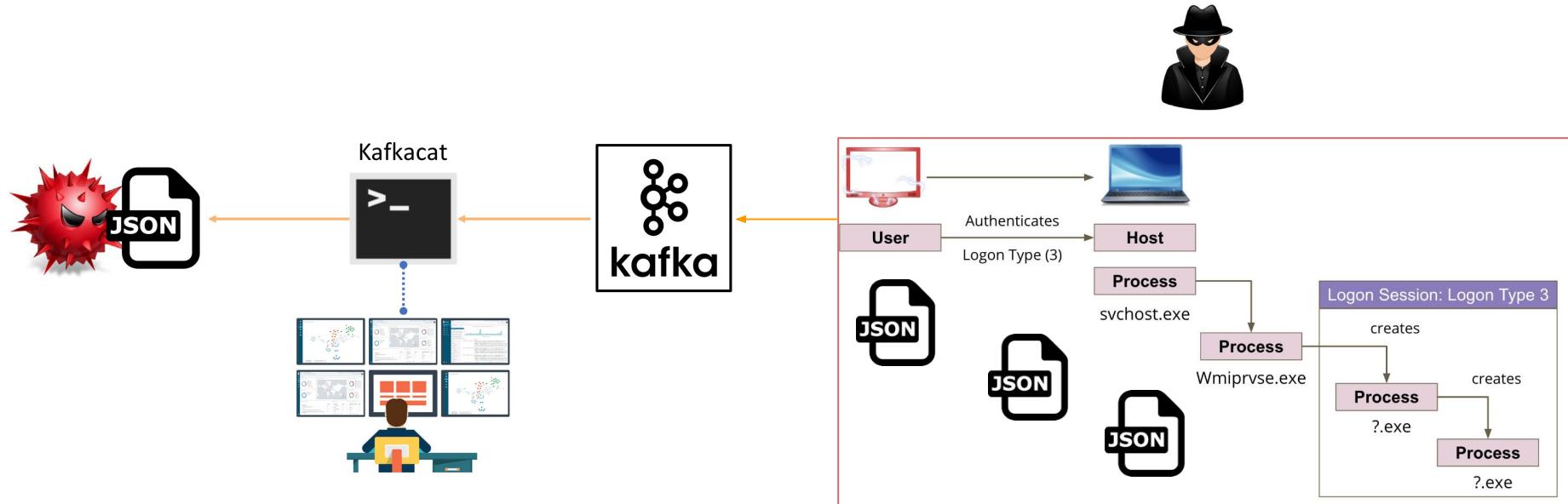
```
$ find . -type f -name "*.tar.gz" -print0
```

```
| sudo xargs -0 -I{} tar xf {} -C .
```

# Purple Teaming - Mordor Style

One Adversarial Technique at the time!

# Let's do it!



# Let's do it! (Demo)

The screenshot shows the COVENANT web application interface. On the left is a sidebar with navigation links: Dashboard, Listeners, Launchers, Grunts (selected), Templates, Tasks, Taskings, Graph, Data, and Users. The main area is titled "Grunt: b1bde3dbff". It has tabs for Info, Interact, Task (selected), and Taskings. Under the Task tab, there is a dropdown menu set to "Assembly". Below it are fields for "AssemblyName" (empty) and "EncodedAssembly" (with a "Choose File" button and "No file chosen"). A "Parameters" section is present but empty. At the bottom, a terminal window shows the following session:

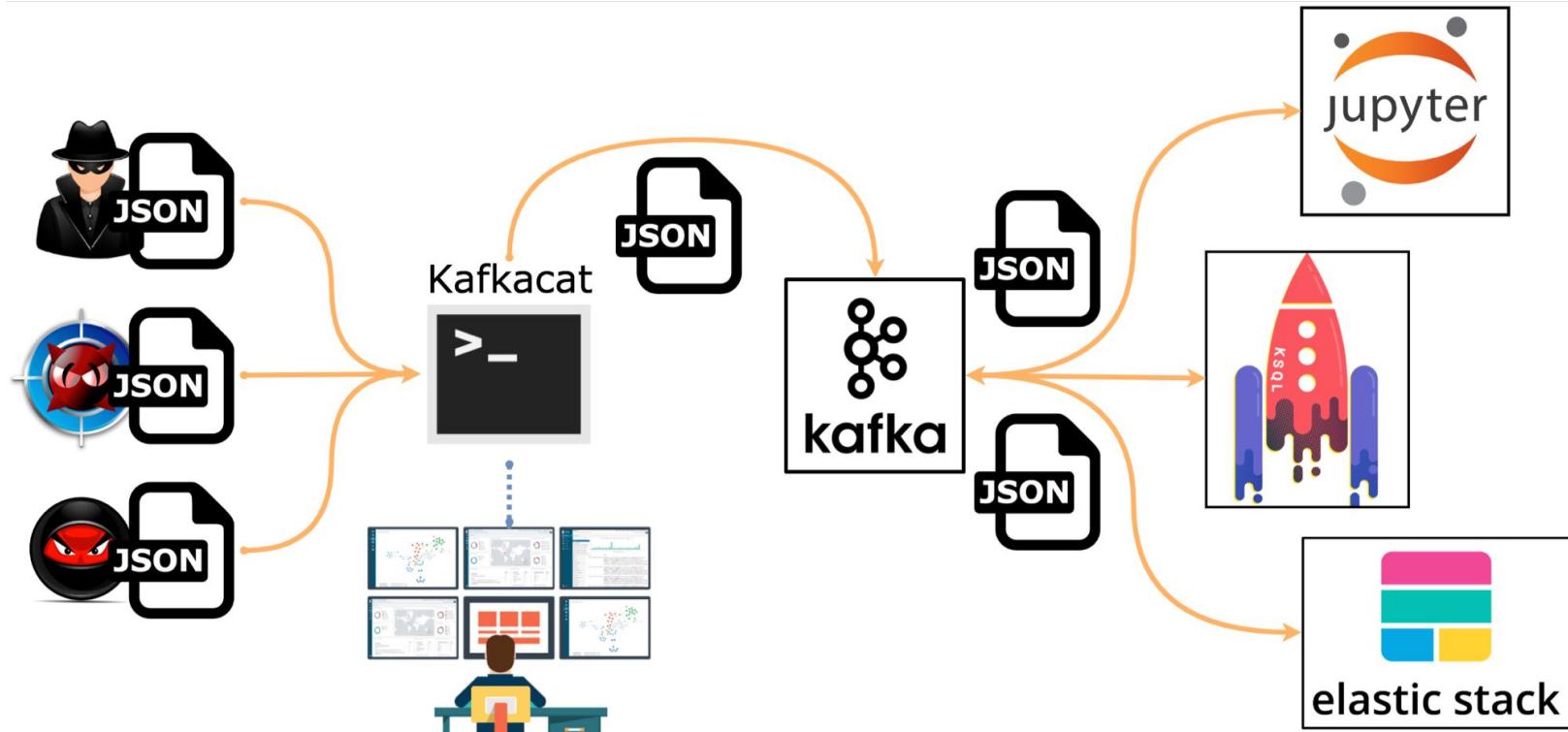
```
mordor_extras -- ubuntu@ip-172-18-39-6: ~ -- ssh -i ../../Documents/projects/keys/aws-ubuntu-key.pem ubuntu@34.226.121.87 -- 108x11
ubuntu@ip-172-18-39-6:~$ ls -lh
total 0
ubuntu@ip-172-18-39-6:~$ kafka-cat -b localhost:9092 -t winlogbeat -C -o end > covenant_wmigrunt_powershell_$(date +%%F%%H%%S).json
% Reached end of topic winlogbeat [0] at offset 1758940
% Reached end of topic winlogbeat [0] at offset 1758947
```

# What about this other thing? (Demo)

The screenshot shows the Covenant web application interface. On the left is a sidebar with navigation links: Dashboard, Listeners, Launchers, Grunts (selected), Templates, Tasks, Taskings, Graph, Data, and Users. The main content area has a title "Grunt: b1bde3dbff". Below it are tabs: Info, Interact, Task (selected), and Taskings. Under the Task tab, there is a dropdown menu set to "ReadTextFile" and a "Path" input field containing "\FILE001\secrets\ring.txt". A blue "Task" button is below these fields. At the bottom of the page is a terminal window showing the following command and its output:

```
mordor_extras — ubuntu@ip-172-18-39-6:~$ ssh -i ./Documents/projects/keys/aws-ubuntu-key.pem ubuntu@34.226.121.87 — 108x11
ubuntu@ip-172-18-39-6:~$ kafkacat -b localhost:9092 -t winlogbeat -C -o end > covenant_readtextfile_ring_$(date +%F%H%M%S).json
% Reached end of topic winlogbeat [0] at offset 1776178
% Reached end of topic winlogbeat [0] at offset 1776181
% Reached end of topic winlogbeat [0] at offset 1776214
```

# Import and Analyze Mordor dataset (Demo)



# Let's do it! (Demo)

The screenshot shows the COVENANT web application interface. On the left is a sidebar with navigation links: Dashboard, Listeners, Launchers, Grunts (selected), Templates, Tasks, Taskings, Graph, Data, and Users. The main area is titled "Grunt: b1bde3dbff". It has tabs for Info, Interact (selected), Task, and Taskings. Under the Task tab, there is a dropdown menu set to "Assembly". Below it is a field labeled "AssemblyName" which is empty. There is also a "EncodedAssembly" section with a "Choose File" button and a message "No file chosen". At the bottom, there is a "Parameters" section. A terminal window at the bottom displays the following command and output:

```
mordor_extras -- ubuntu@ip-172-18-39-6: ~ -- ssh -i ../../Documents/projects/keys/aws-ubuntu-key.pem ubuntu@34.226.121.87 -- 108x11
ubuntu@ip-172-18-39-6:~$ ls -lh
total 0
ubuntu@ip-172-18-39-6:~$ kafkacat -b localhost:9092 -t winlogbeat -C -o end > covenant_wmigrunt_powershell_$(date +%%F%%H%%S).json
% Reached end of topic winlogbeat [0] at offset 1758940
% Reached end of topic winlogbeat [0] at offset 1758947
```

# Purple Teaming - Mordor Style

Adversary Emulation Plans (Full Campaign)!

# Emulating Adversary APT3

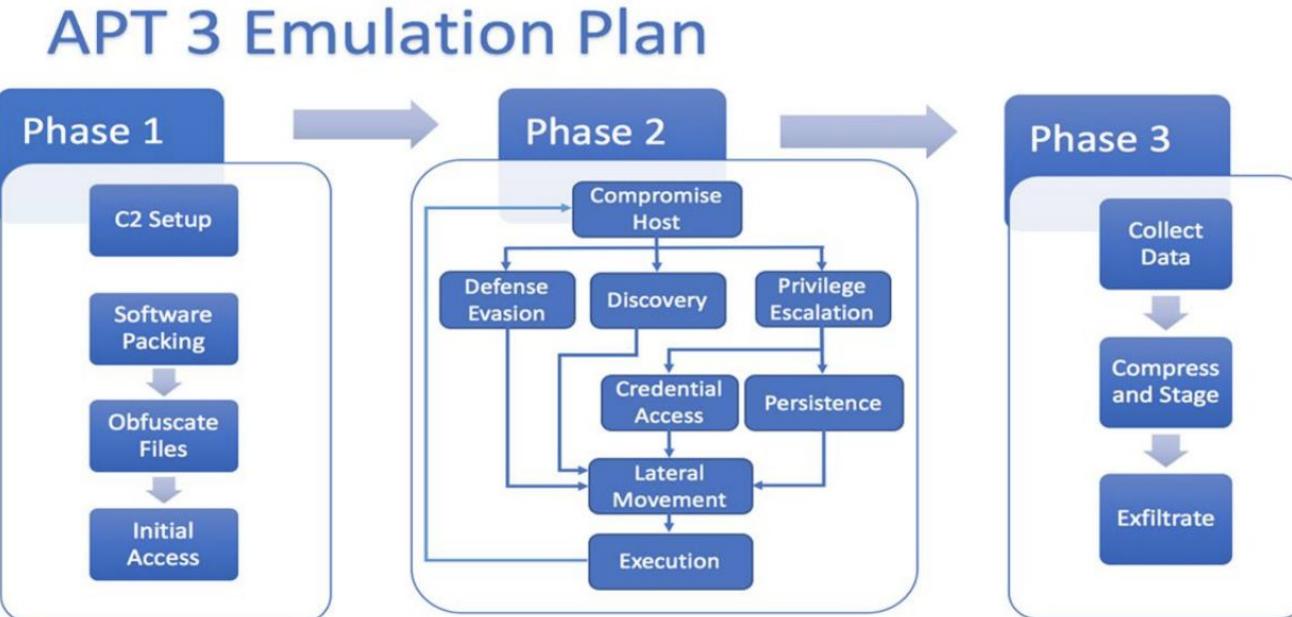


Figure 1 APT3's Three Phases of Action

# ATT&CK Evaluations: APT 3 Round 1

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Efiltration	Impact
Drive-by Compromise	CMSRPT	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Discovery	Application Deployment	Audio Capture	Automated User Port	Automated Extrusion	Data Destruction
Exploit/Public-Facing	Command-Line Interface	Account Manipulation	Accessibility Features	Binary Padding	Application Window	Distributed Component	Communication Through Shared Resource	Data Compressed	Data Encrypted for Impact	Data Loss
External Remote Services	Compiled .HME File	AppCart DLLs	AppCart DLLs	Blitze Force	Browser Beacons	Distributed Component	Automated Collection	Data Exfiltration	Data Exfiltration	Data Loss
Hardware Additions	Control Panel Items	AppInit DLLs	AppInit DLLs	Credential Dumping	Browser Beacons	Exploitation of Handle Leaking	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hopscotch Through Dynamic Data Exchange	Application Shimming	Application Shimming	Bypass User Account Control	Credentials in Registry	Cloud Trust Discovery	Logon Scripts	Data from Information Disclosure	Data Transfer Size Limits	Data Wipe	Data Loss
Spearmarking Attachment	Execution Through Authentication Package	Execution Through Authentication Package	ByPass User Account Control	Exploitation for Credential Theft	File and Directory	Hashes	Data from Local System	Exfiltration Over Alternative Channel	Data Content Wipe	Data Loss
Spearmarking Link	Execution Through Module	Execution Through Module	Code Signing	File and Directory	Hashes	Pass the Hash	Data from Network Shared Drives	Data Structure Wipe	Data Loss	Data Loss
Spearmarking via Service	Fileless JScript	Fileless JScript	Compile After Delivery	Forced Authentication	Network Share Discovery	Remote Desktop Protocol	Data from Removable Media	Data Encroachment	Data Loss	Data Loss
Supply Chain Compromise	Exploitation for Client Side Exploit	Exploitation for Client Side Exploit	Compiled HTML File	Hooking	Network Sniffing	Remote Desktop Protocol	Data from Removable Media	Data Loss	Data Loss	Data Loss
Trustless Relationship	Graphics User Interface	Browser Extensions	EVAS's Window Memory Hooking	Component Firmware	Input Capture	Password Policy Discovery	Data Staged	Data Loss	Data Loss	Data Loss
Valid Accounts	LSASS Driver	Componented Services	Component Model Object Hooking	Component Object Model Hooking	Input Prompt	Peripheral Device	Depacketization	Fallback Channels	File Encryption	File Encryption
Maha	Execution Object Model Hijacking	Execution Object Model Hijacking	Configurable File	Kerberos	Input Sniffing	Protocol Discovery	Main in the Browser	Filesystem Corruption	Filesystem Corruption	Filesystem Corruption
PowerShell	Create Account	New Service	Configure-Delete Files or Information	NFS	Keyboard Sniffing	Protocol Discovery	Multi-Stage Changes	Domain Fronting	Endpoint Denial of Service	Endpoint Denial of Service
RegAccess/RegRead	DLL Search Order Hijacking	Path Interception	Disabling Security Tools	NFS	Query Registry	Shared Content	Screen Capture	Exfiltration Over Different Channel	Exfiltration Over Different Channel	Exfiltration Over Different Channel
RegRead/2	External Remote Services	Port Monitors	Pluggable Filter DLL	Password Filter DLL	Remote File Copy	Third-party Software	Video Capture	Multi-thread Communication	Imbit System Recovery	Imbit System Recovery
Rundll32	WMI	Process Injection	Pluggable Filter DLL	Private Keys	Remote System Discovery	Windows Admin Shares	Web Service	Multi-layer Encryption	Network Denial of Service	Network Denial of Service
Runhook	WMI	Process Injection	Pluggable Filter DLL	Protocol Discovery	Windows Admin Shares	Windows Admin Shares	Web Service	Remote Access Tools	Resource Hijacking	Resource Hijacking
Runhooked Task	Windows Task Scheduler	Redundant Access	Protocol Discovery	Protocol Discovery	Windows Admin Shares	Windows Admin Shares	Web Service	Remote File Copy	Runtime Data Manipulator	Runtime Data Manipulator
Runhooked Task	Windows Task Scheduler	Redundant Access	Protocol Discovery	Protocol Discovery	Windows Admin Shares	Windows Admin Shares	Web Service	Remote File Copy	Service Stop	Service Stop
Runhooked Task	Windows Task Scheduler	Redundant Access	Protocol Discovery	Protocol Discovery	Windows Admin Shares	Windows Admin Shares	Web Service	Remote File Copy	Stored Data Manipulation	Stored Data Manipulation
Runhooked Task	Windows Task Scheduler	Redundant Access	Protocol Discovery	Protocol Discovery	Windows Admin Shares	Windows Admin Shares	Web Service	Remote File Copy	Transient Data Manipulation	Transient Data Manipulation
Runhooked Task	Windows Task Scheduler	Redundant Access	Protocol Discovery	Protocol Discovery	Windows Admin Shares	Windows Admin Shares	Web Service	Uncleanly Used Port	Uncleanly Used Port	Uncleanly Used Port
Runhooked Task	Windows Task Scheduler	Redundant Access	Protocol Discovery	Protocol Discovery	Windows Admin Shares	Windows Admin Shares	Web Service	Web Service	Web Service	Web Service
Trusted Developer Utilities	Modify Existing Service	Port Monitors	Protocol Modification	Protocol Modification	System Time Discovery	Virtualization-Sandbox Evasion				
Win32 Exec	Notch Helper DLL	Redundant Access	Protocol Modification	Protocol Modification	Virtualization-Sandbox Evasion					
Windows Management	New Service	Redundant Access	Protocol Modification	Protocol Modification						
Windows Remote Management	Office Application Startup	Redundant Access	Protocol Modification	Protocol Modification						
XSL Script Processing		Path Interception	Protocol Modification	Protocol Modification						
		Port Monitors	Protocol Modification	Protocol Modification						
		Redundant Access	Protocol Modification	Protocol Modification						
		Replay-Half Keys	Protocol Modification	Protocol Modification						
		Scheduled Task	Protocol Modification	Protocol Modification						
		SonScanner	Protocol Modification	Protocol Modification						
		Security Support Provider	Protocol Modification	Protocol Modification						
		Service Registration	Protocol Modification	Protocol Modification						
		Shrunkit Modification	Protocol Modification	Protocol Modification						
		SPF and Trust Provider	Protocol Modification	Protocol Modification						
		System Firmware	Protocol Modification	Protocol Modification						
		Time Providers	Protocol Modification	Protocol Modification						
		Valid Accounts	Protocol Modification	Protocol Modification						
		Web Shell	Protocol Modification	Protocol Modification						
		Windows API Hooking	Protocol Modification	Protocol Modification						
		Winlogon Helper DLL	Protocol Modification	Protocol Modification						

<https://attackevals.mitre.org/methodology/round1/scope.html>

# ATT&CK Evaluations: APT 3 Round 1 (Day 1 & 2)

## Cobalt Strike

- Step 1 - [Initial Compromise](#) ›
- Step 2 - [Initial Discovery](#) ›
- Step 3 - [Privilege Escalation](#) ›
- Step 4 - [Discovery for Lateral Movement](#) ›
- Step 5 - [Credential Access](#) ›
- Step 6 - [Lateral Movement](#) ›
- Step 7 - [Persistence](#) ›
- Step 8 - [Collection](#) ›
- Step 9 - [Exfiltration](#) ›
- Step 10 - [Execution of Persistence](#) ›

## Empire

- Step 11 - [Initial Compromise](#) ›
- Step 12 - [Initial Discovery](#) ›
- Step 13 - [Discovery for Lateral Movement](#) ›
- Step 14 - [Privilege Escalation](#) ›
- Step 15 - [Credential Access](#) ›
- Step 16 - [Lateral Movement](#) ›
- Step 17 - [Persistence](#) ›
- Step 18 - [Collection](#) ›
- Step 19 - [Exfiltration](#) ›
- Step 20 - [Execution of Persistence](#) ›

# ATT&CK Evaluations: APT 3 Round 1 Day 2

ATT&CK Eval Step	ATT&CK Eval Phase	Tactic	Technique Id	Technique Name	Empire Commands / Notes	Source Endpoint	Source Username	Target Endpoint	Target Username	ATT&CK Eval Scenario #2 Procedures
11.A.1	Initial Access	Defense Evasion Execution	T1064	Scripting	usestager windows/launcher_vbs set Listener https set OutFile /tmp/autoupdate.vbs execute user nmartha double clicks vbs script	HR001	nmartha	HR001	nmartha	Initial compromise was emulated via a malicious VBScript. A legitimate user executed a VBScript stager, which launched PowerShell to download and execute an Empire payload
11.B.1	Initial Access	Command and Control	T1043	Commonly Used Port	listeners uselistener http set Name https set Host 10.0.10.106 set Port 443 set CertPath /opt/Empire/data execute	HR001	nmartha	HR001	nmartha	The executed Empire payload established an encrypted C2 channel over HTTPS on TCP port 443
11.B.1	Initial Access	Command and Control	T1071	Standard Application Layer Protocol	listeners uselistener http set Name https set Host 10.0.10.106 set Port 443 set CertPath /opt/Empire/data execute	HR001	nmartha	HR001	nmartha	The executed Empire payload established an encrypted C2 channel over HTTPS on TCP port 443
11.B.1	Initial Access	Command and Control	T1032	Standard Cryptographic Protocol	listeners uselistener http set Name https set Host 10.0.10.106 set Port 443 set CertPath /opt/Empire/data execute	HR001	nmartha	HR001	nmartha	The executed Empire payload established an encrypted C2 channel over HTTPS on TCP port 443
12.A.1	Initial Discovery	Discovery	T1016	System Network Configuration Discovery	shell route print	HR001	nmartha	HR001	nmartha	The route utility was executed via PowerShell to enumerate the local routing table.
12.A.2	Initial Discovery	Discovery	T1016	System Network Configuration Discovery	shell ipconfig /all	HR001	nmartha	HR001	nmartha	The ipconfig utility was executed via PowerShell to enumerate local TCP/IP network configuration information.
12.B.1	Initial Discovery	Discovery	T1033	System Owner/User Discovery	shell whoami /all /fo list	HR001	nmartha	HR001	nmartha	The whoami utility was executed via PowerShell to enumerate information about the current user
12.C.1	Initial Discovery	Discovery	T1057	Process Discovery	shell qprocess *	HR001	nmartha	HR001	nmartha	The qprocess utility was executed via PowerShell to enumerate local running processes.
12.D.1	Initial Discovery	Discovery	T1007	System Service Discovery	shell net start	HR001	nmartha	HR001	nmartha	The net utility was executed via PowerShell to enumerate local active services.
12.E.1	Initial Discovery	Defense Evasion Execution	T1064	Scripting	usemodule situational_awareness/host/winenum	HR001	nmartha	HR001	nmartha	Empire: Built-in WinEnum module executed to programmatically execute a series of enumeration techniques
12.E.1.1	Initial Discovery	Discovery	T1033	System Owner/User Discovery	usemodule situational_awareness/host/winenum	HR001	nmartha	HR001	nmartha	WinEnum: Get-UserInfo
12.E.1.2	Initial Discovery	Discovery	T1069	Permission Groups Discovery	usemodule situational_awareness/host/winenum	HR001	nmartha	HR001	nmartha	WinEnum: "AD Group Memberships"
12.E.1.3	Initial Discovery	Discovery	T1201	Password Policy Discovery	usemodule situational_awareness/host/winenum	HR001	nmartha	HR001	nmartha	WinEnum: "Password Last Changed"

# Purple Teaming - Mordor Style

Automating Adversary Emulation Plans

# Caldera: Automated Adversary emulation (ATT&CK)

# CALDERA

Cyber Adversary Language and Decision Engine for Red Team Automation

## I am a **blue-teamer**

As a blue-team operator, you should start by deploying one or many 54ndc47 (Sandcat) agents on remote computers you want to test. Then move into Chain mode to create adversary profiles and run operations against the deployed hosts.

## I am a **researcher**

As a researcher, you should restart the server with the mock plugin, which deploys simulated agents. Then, go into Chain mode and run a few sample operations. Once familiar with how abilities link together, study the sequential.py module in the source code, which contains the automated decision-making logic.

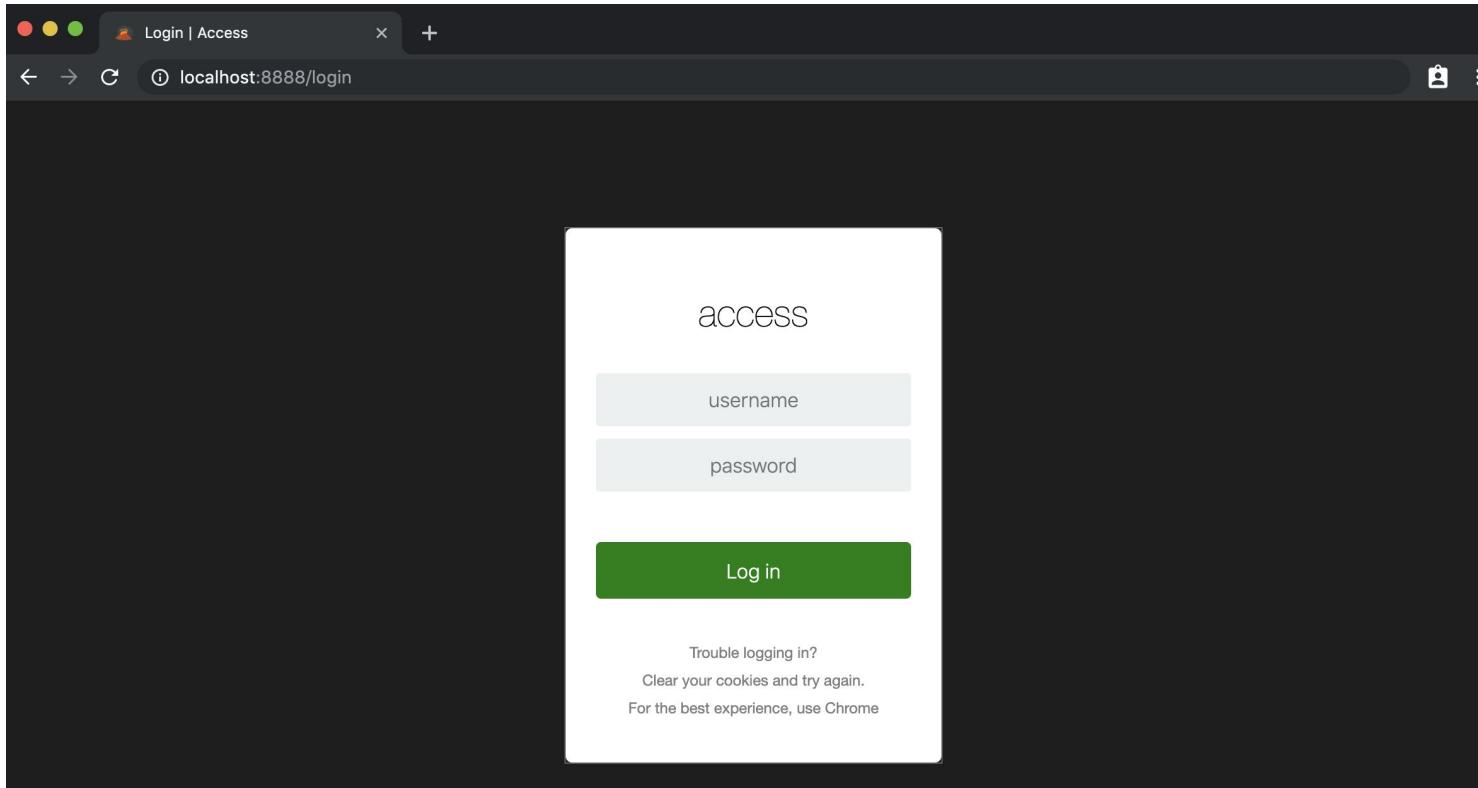
## I am a **red-teamer**

As a red-team operator, you should restart the server with the terminal plugin loaded. Then, deploy one or many 54ndc47 (Sandcat) agents on remote computers. Use the terminal to create and join reverse-shell sessions to manually compromise the hosts.

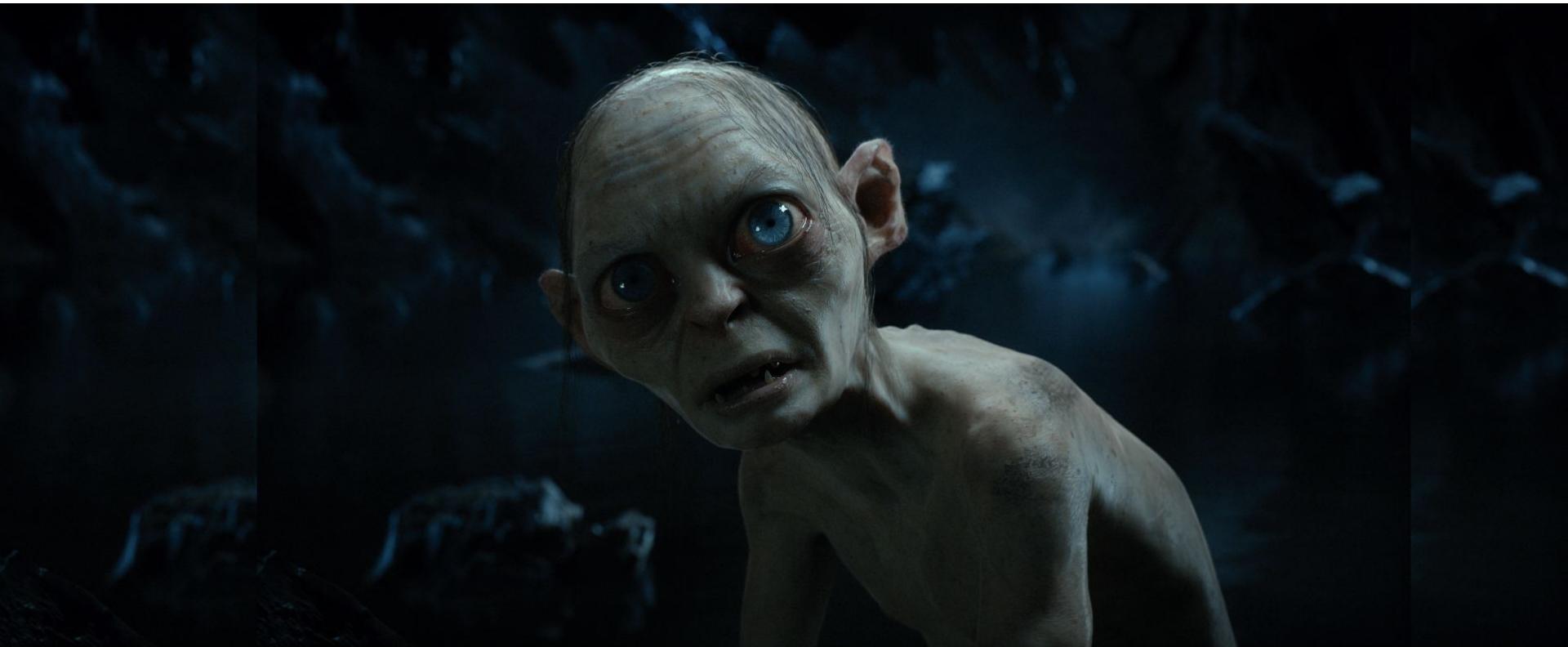
# Caldera Installation

- git clone --recursive  
<https://github.com/mitre/caldera.git>
- cd caldera/
- pip3 install -r requirements.txt
- python -u server.py
- git clone  
<https://github.com/Cyb3rWard0g/docker-caldera>
- cd docker-caldera/
- docker-compose -f docker-compose-caldera.yml up --build -d

# Caldera: Automated Adversary emulation (ATT&CK)



# Is there a plugin for the ATT&CK evals?



# Caldera ATT&CK Eval's Plugin (NEW!)

Home Sandcat Chain **Evals\_Caldera**

Docs Logout

## ATT&CK | Eval's

### Initial Compromise

Manually execute the Remote Access Tool (RAT) on target machine (see [Sandcat](#)). Automated delivery is out of scope of this exercise and must be executed manually.  
Once this is completed, begin the evaluation by starting the 'ATT&CK Eval APT3' operation using Chain mode and include the \*evals\* fact sheet (see [Chain](#)).

2.A.1 - System Network Configuration Discovery (T1016)

2.A.2 - System Network Configuration Discovery (T1016)

| Whaaat? You can just let the plugin do it all?



# Caldera: APT3 ATT&CK Eval Round 1 Day 1

## ATT&CK Eval APT3 - Full

full evaluation

### Phase 1 +

---

#### 2.A.2 - System Network Configuration Discovery (T1016)

The arp utility is executed via cmd to enumerate local ARP configuration information.

DISCOVERY | T1016 | SYSTEM NETWORK CONFIGURATION DISCOVERY



### Phase 2 +

---

#### 2.B.1 - System Owner / User Discovery (T1033)

The native echo command is executed via cmd to enumerate local environment variables associated with current user and domain.

DISCOVERY | T1033 | SYSTEM OWNER/USER DISCOVERY



# Caldera: APT3 ATT&CK Eval Round 1 Day 1

Phase 17 +

## 8.D.1 - Screen Capture (T1113)

Native API call(s) were used to collect a screenshot.

COLLECTION | T1113 | SCREEN CAPTURE



Phase 18 +

## 9.B.1 - Data from Network Shared Drive (T1039) and Exfiltration over C2 Channel (T1041)

Copy a target file from a remote file share through the existing C2 channel

EXFILTRATION | T1041 | EXFILTRATION OVER COMMAND AND CONTROL CHANNEL



Phase 19 +

## 10.A.1 – Registry Run Key / Startup Folder (T1060) from 1.B, 10.A.2 – Scheduled Task (T1053) from 7.C

EXECUTION | T1086 | POWERSHELL



# Caldera: ATT&CK Evals Plugin Installation

- cd caldera/plugins
- git clone  
[https://github.com/mitre-attack/evals\\_caldera.git](https://github.com/mitre-attack/evals_caldera.git)
- Modify caldera/conf/local.yml file and add  
“**- evals\_caldera**” under plugins

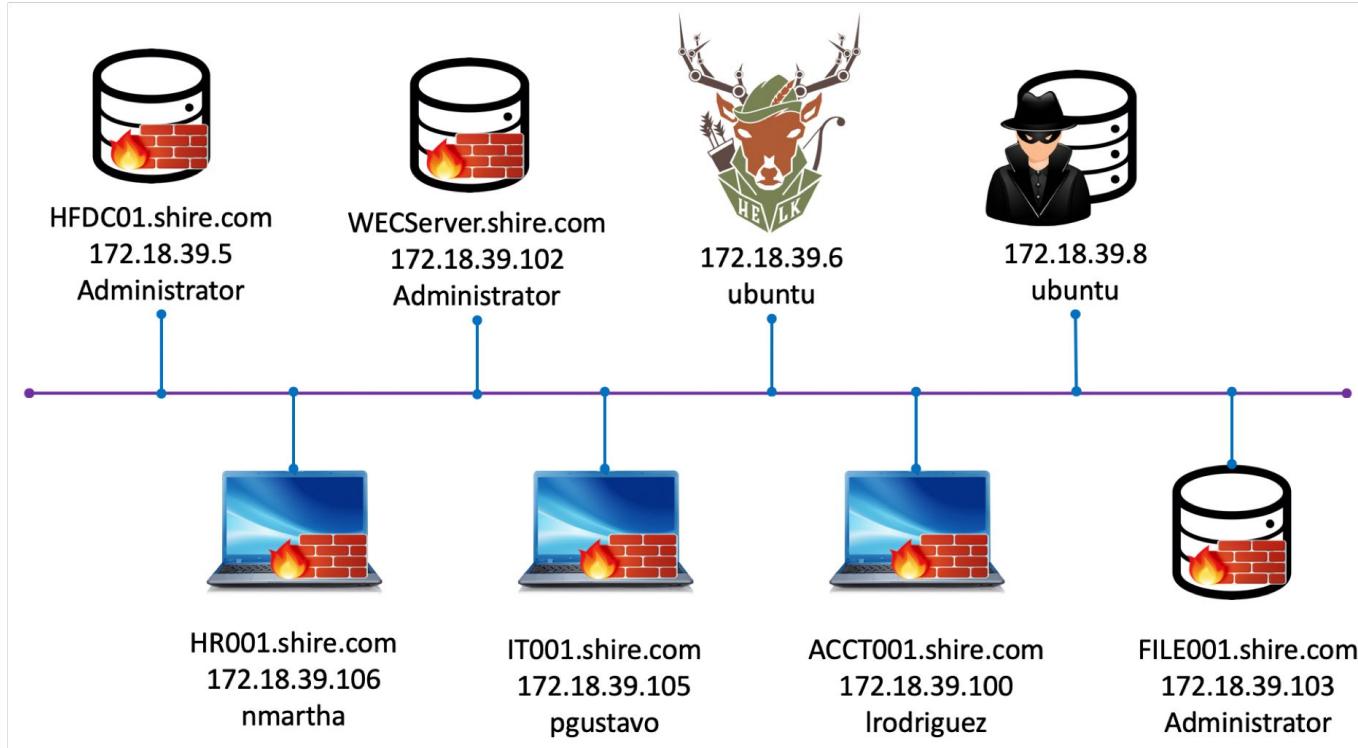
# Can I do it at home?



# Blacksmith Project & Mordor!

- git clone <https://github.com/hunters-forge/Blacksmith>
- Follow pre-requirements before deploying **Shire Environment**:  
[https://blacksmith.readthedocs.io/en/latest/mordor\\_shire.html](https://blacksmith.readthedocs.io/en/latest/mordor_shire.html)
- Update parameter **RTODefaultC2** to **caldera** in  
cfn-parameters/shire/c2-server-parameters.json
- Update parameter **RestrictLocation** in  
cfn-parameters/shire/ec2-network-parameters.json
- Run **./deploy.sh -e 'shire'**

# Blacksmith Project & Mordor!



# Thank you so much Daniel!



Follow

**Daniel Weiss**

@d4weiss Follows you

cyber. red. blue. purple. tweets are my own.

# Caldera: APT3 ATT&CK Eval Round 1 Day 1 (Video)

Home Sandcat Chain **Evals\_Caldera**

Docs Logout

## ATT&CK | Eval

### Initial Compromise

Manually execute the Remote Access Tool (RAT) on target machine (see [Sandcat](#)). Automated delivery is out of scope of this exercise and must be executed manually.  
Once this is completed, begin the evaluation by starting the 'ATT&CK Eval APT3' operation using Chain mode and include the \*evals\* fact sheet (see [Chain](#)).



2.A.1 - System Network Configuration Discovery (T1016)



2.A.2 - System Network Configuration Discovery (T1016)

# What did we learn today?

# Purple Teaming - Mordor Style

- Practice like you play before production!
- Be prepared and make sure you set rules of engagement!
- Keep the back and forth going and at the same time:
  - Take data snapshots of each technique or whole emulation plan (very very helpful and convenient!!)
  - Reuse pre-recorded data for additional deep research
  - Expedite analytic validations with the datasets
  - Train other purple teamers with re-recorded events
  - Learn from the data produced (Red & Blue)

# Purple Teaming - Mordor Style

- Practice like you play before production!
- Be prepared and make sure you set rules
- Keep the back and forth going and at the same time:
  - Take data snapshots of each technique or whole emulation plan (very very helpful and convenient!!)
  - Reuse pre-recorded data for additional deep research
  - Expedite analytic validations with the datasets
  - Train other purple teamers with re-recorded events
  - **Learn from the data produced (Red & Blue)**

# Purple Teaming - Mordor Style

- Practice like you play before production!
- Be prepared and make sure you set rules
- Keep the back and forth going and at the same time:
  - Take data snapshots of each technique or whole emulation plan (very very helpful and convenient!!)
  - Reuse pre-recorded data for additional deep research
  - Expedite analytic validations with the datasets
  - Train other purple teamers with re-recorded events
  - Learn from the data produced (Red & Blue)
- **Empower others and give back to the community!**

# | Threat Hunters Forge Community!



Threat Hunters Forge

Data Science, Threat Hunting & Open Source Projects

# Threat Hunters Forge Slack Community!



## ThreatHunting

Threat Hunters Forge

Join the Threat Hunters Forge Slack  
Community!

A community led effort to share detection  
strategies and to support open source  
projects to aid the development of security  
analytics and tooling for threat hunting!

Get access today!

FREE to join

Email

Join Now

<https://launchpass.com/threathunting>

# Goal: Share and Empower the Community!



# Let's do it together!



# Threat Hunters Forge References

- **GitHub:** <https://github.com/hunters-forge>
- **Python Library:** <https://github.com/Cyb3rPanda/openhunt>
- **Slack Invitation:** <https://launchpass.com/threathunting>
- **Official Blog:** <https://medium.com/threat-hunters-forge>
- **Founders:** @Cyb3rWard0g & @Cyb3rPandaH
- **Official Twitter:** @HuntersForge
- @HunterPlaybook
- @THE\_HELK
- @OSSEM\_Project, @Mordor\_Project & More

# Thank You! Muchas Gracias!