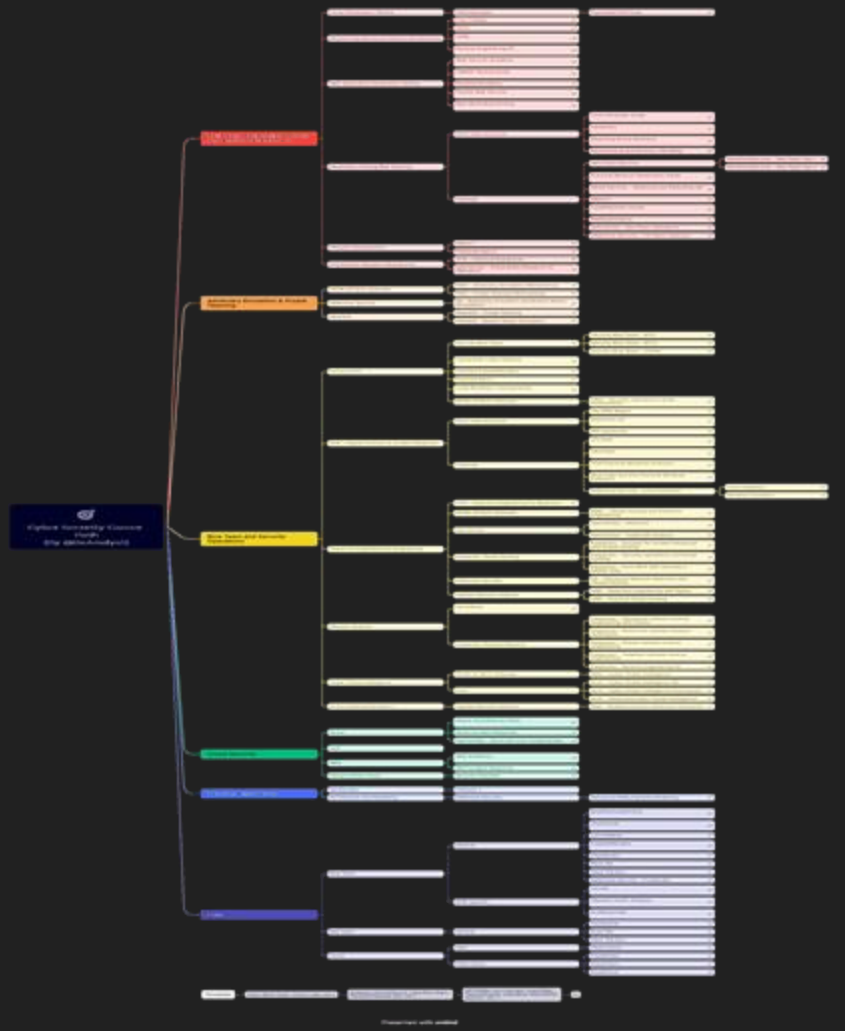
CANCEL YOUR PENTEST AND PURPLE THIS INSTEAD

Adversary Village Live-streaming series #5

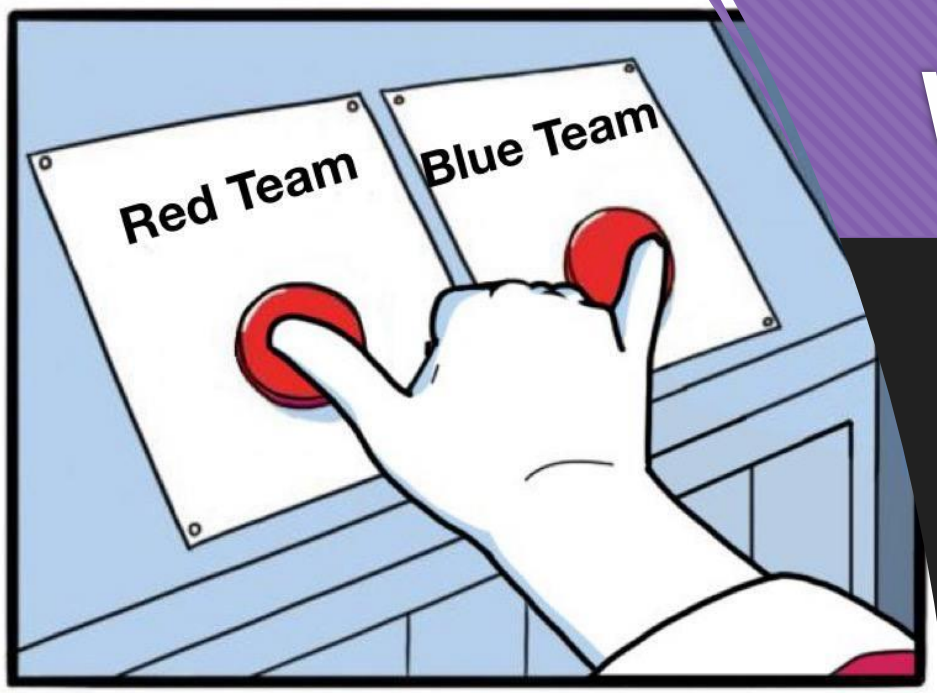
Samuel Rossier

~~whoami.exe~~ motivation.exe

- I'm Sam 
- I studied economics, I'm now in a SOC
- If I can do it, anyone can do it



https://github.com/0xAnalyst/Cyber_Security_Career_Path



Why this talk?

- Success story
- Lower barrier to entry
- Automation <3 Manual

What's in it for you?

1. Learning resources
2. Demystifying purple terminology
3. Simulation plan to take-away
4. Quick wins to improve

Introduction

Introduction – Learning resources

Methodology

- Scythe Purple Team Exercise Framework (link)
- Purple Team Strategies (link)

Training

- AttackIQ Academy
- Mitre ATT&CK Defender – MAD20 (free on Cybrary)
- Defensive Security
- Specter Ops
- SANS SEC599, SEC699, SEC565

Introduction – Purple flavors

Introduction – Purple flavors

Purple

Adv Emulation

Threat-Informed Defense

Purple

Simulation

Purple

Continuous Security Testing

Introduction – Purple flavors

Threat-Informed Defense

Purple Teaming

Continuous Security Testing

Adversary Simulation

Adversary Emulation

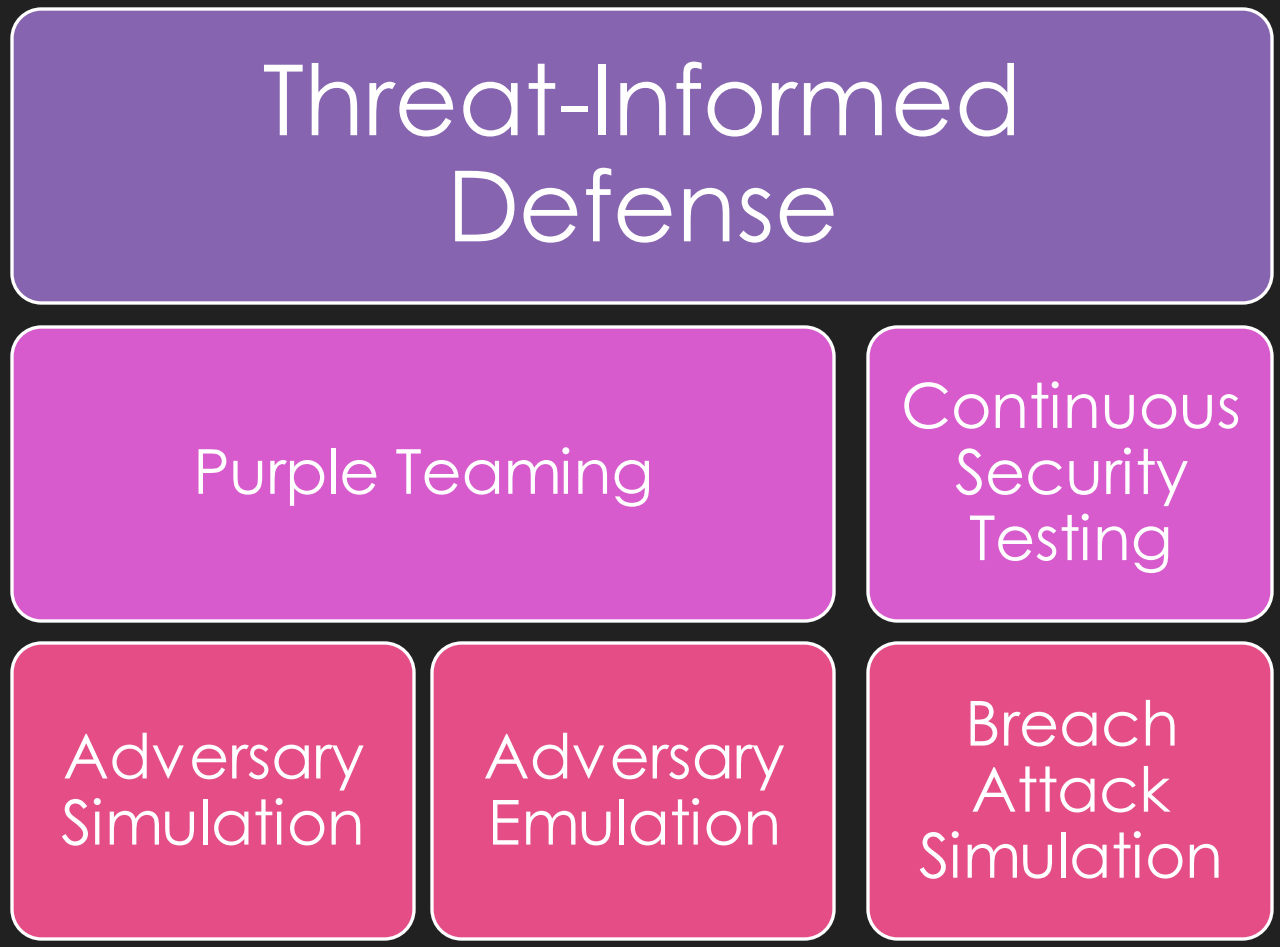
Breach Attack Simulation

Introduction – Purple flavors

Simulation: Performing steps that a threat actor could do

Emulation: Mimicking steps a threat actor would do (did)

Does it matter?



Introduction – Purple flavors

Simulation: Performing steps that a threat actor could do

Emulation: Mimicking steps a threat actor would do (did)

Does it matter?

Threat-Informed Defense

Purple Teaming

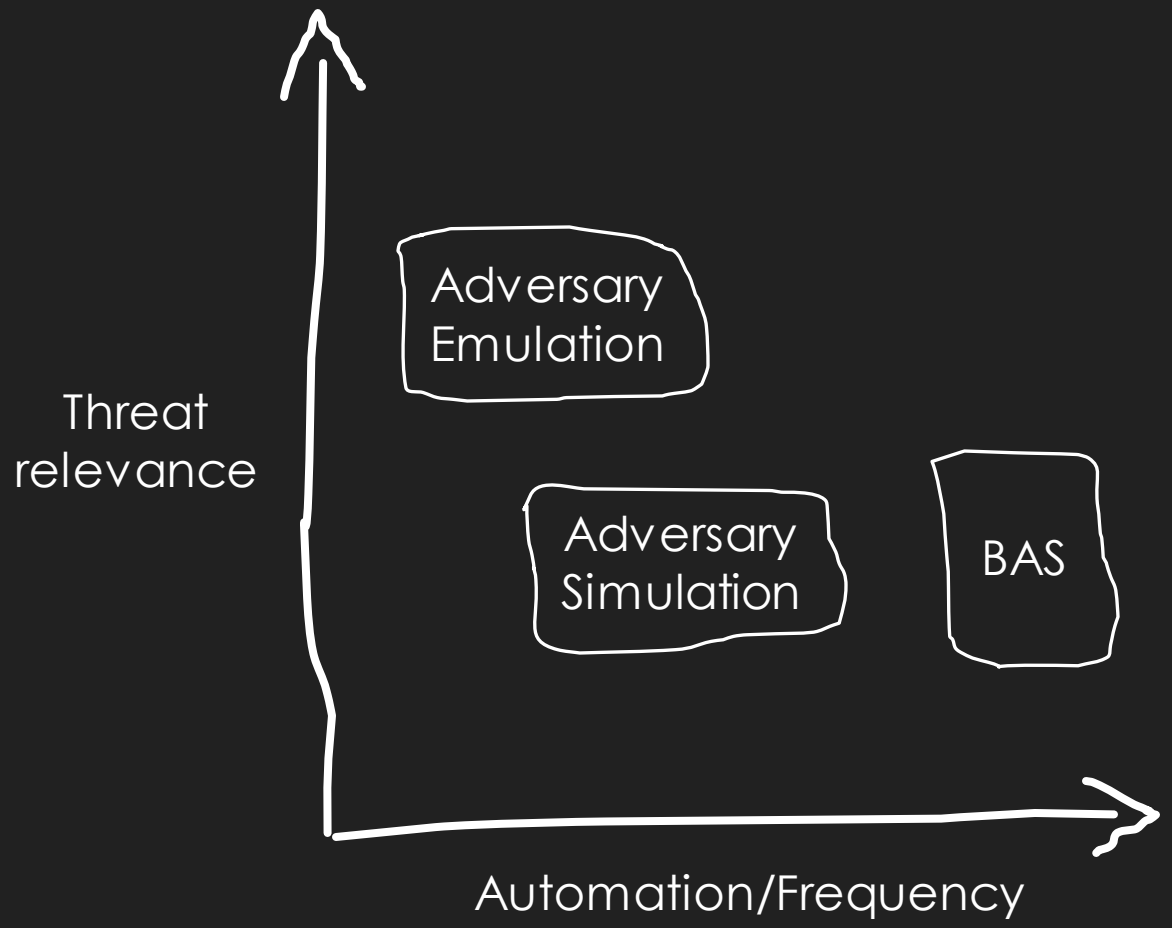
Continuous Security Testing

Adversary Simulation

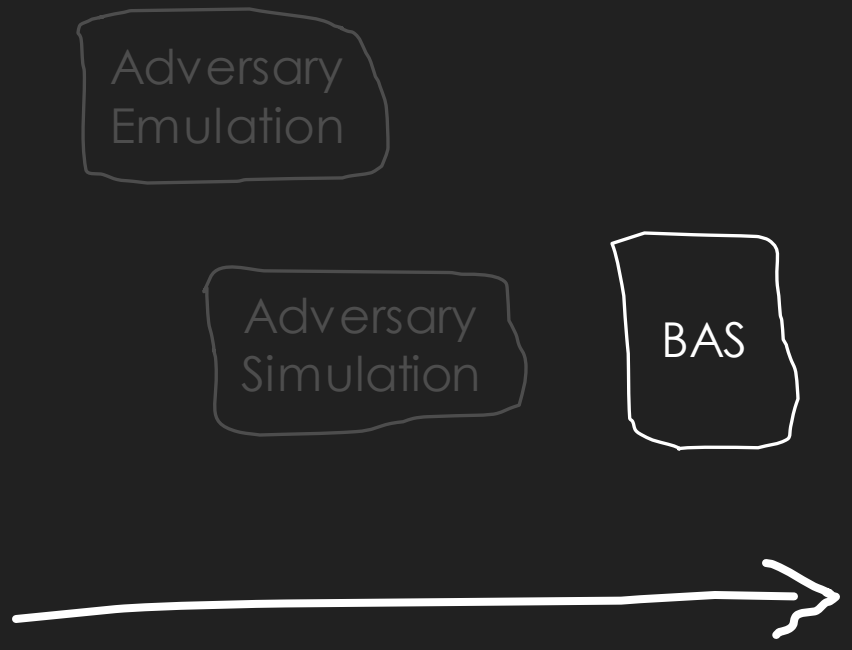
Adversary Emulation

Breach Attack Simulation

Introduction – Sophisticated study



Introduction – Automation <3 Manual



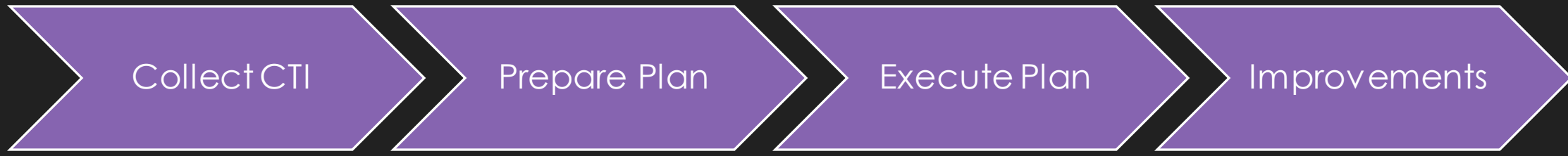
Objective:
Ensure security controls are ready against a wide variety of threats

Introduction – Automation <3 Manual

Objective:
Grow analysts experience, attack understanding and improve detection and response capabilities

Adversary Simulation

Adversary Simulation – Where are we?



Adversary Simulation – Where are we?

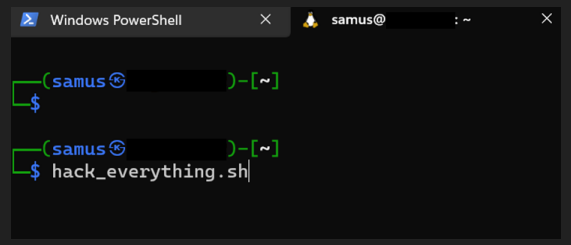
Collect CTI → Prepare Plan → Execute Plan → Improvements

- Done
- Done

Adversary Simulation – Where are we?

Collect CTI → Prepare Plan → Execute Plan → Improvements

- Done
- Done
- **Now**
- **Now**



Adversary Simulation – Walkthrough

Grab the plan!

https://github.com/Sam0x90/CTI/tree/main/Adversary%20Emulation%20Plans/2022_Top35_Mitre

WMI – Prevention

Prevention – Attack Surface Reduction

Block persistence through WMI event subscription

This rule prevents malware from abusing WMI to attain persistence on a device.

> **Important**
>
> File and folder exclusions don't apply to this attack surface reduction rule.

Fileless threats employ various tactics to stay hidden, to avoid being seen in the file system, and to gain periodic execution control. Some threats can abuse the WMI repository and event model to stay hidden.

Intune name: `Persistence through WMI event subscription`

Configuration Manager name: Not available

GUID: `e6db77e5-3df2-4cf1-b95a-636979351e5b`

Advanced hunting action type:

- AsrPersistenceThroughWmiAudited
- AsrPersistenceThroughWmiBlocked

Dependencies: Microsoft Defender Antivirus, RPC

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?view=o365-worldwide#block-persistence-through-wmi-event-subscription

Prevention – Disabling the service

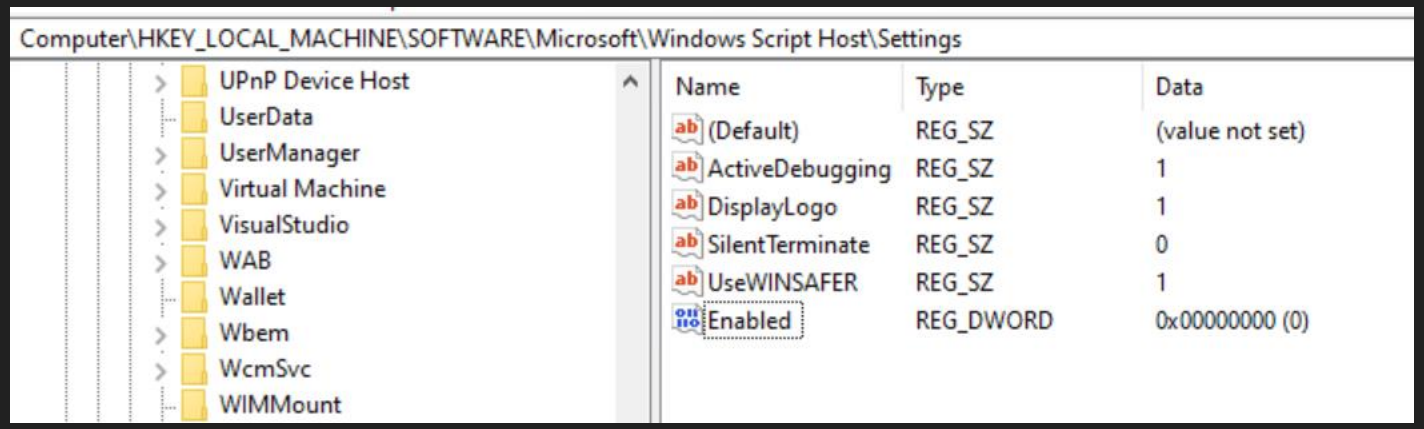
Windows Remote Management (WS-Management)

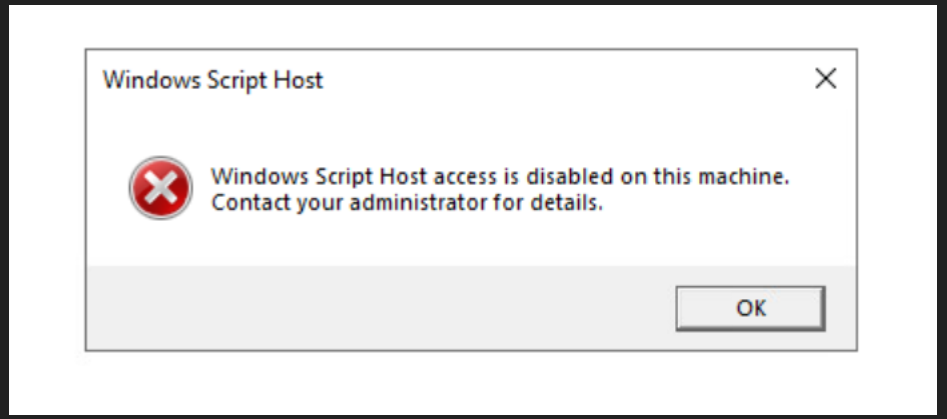
Name	Description
Service name	WinRM
Description	Windows Remote Management (WinRM) service implements the WS-Management protocol for remote management. WS-Management is a standard web services protocol used for remote software and hardware management. The WinRM service listens on the network for WS-Management requests and processes them. The WinRM Service needs to be configured with a listener using winrm.cmd command line tool or through Group Policy in order for it to listen over the network. The WinRM service provides access to WMI data and enables event collection. Event collection and subscription to events require that the service is running. WinRM messages use HTTP and HTTPS as transports. The WinRM service does not depend on IIS but is preconfigured to share a port with IIS on the same machine. The WinRM service reserves the /wsman URL prefix. To prevent conflicts with IIS, administrators should ensure that any websites hosted on IIS do not use the /wsman URL prefix.
Installation	Always installed
Startup type	Automatic
Recommendation	Do not disable
Comments	Needed for remote management

https://github.com/MicrosoftDocs/windowsserverdocs/blob/main/WindowsServerDocs/security/windows-services/security-guidelines-for-disabling-system-services-in-windows-server.md

Prevention – Bonus: Prevent (w|c)script.exe execution

- Create a DWORD 'Enabled', set to 0 in the registry key '*(HKLM|HKCU)\Software\Microsoft\Windows Script Host\Settings*'



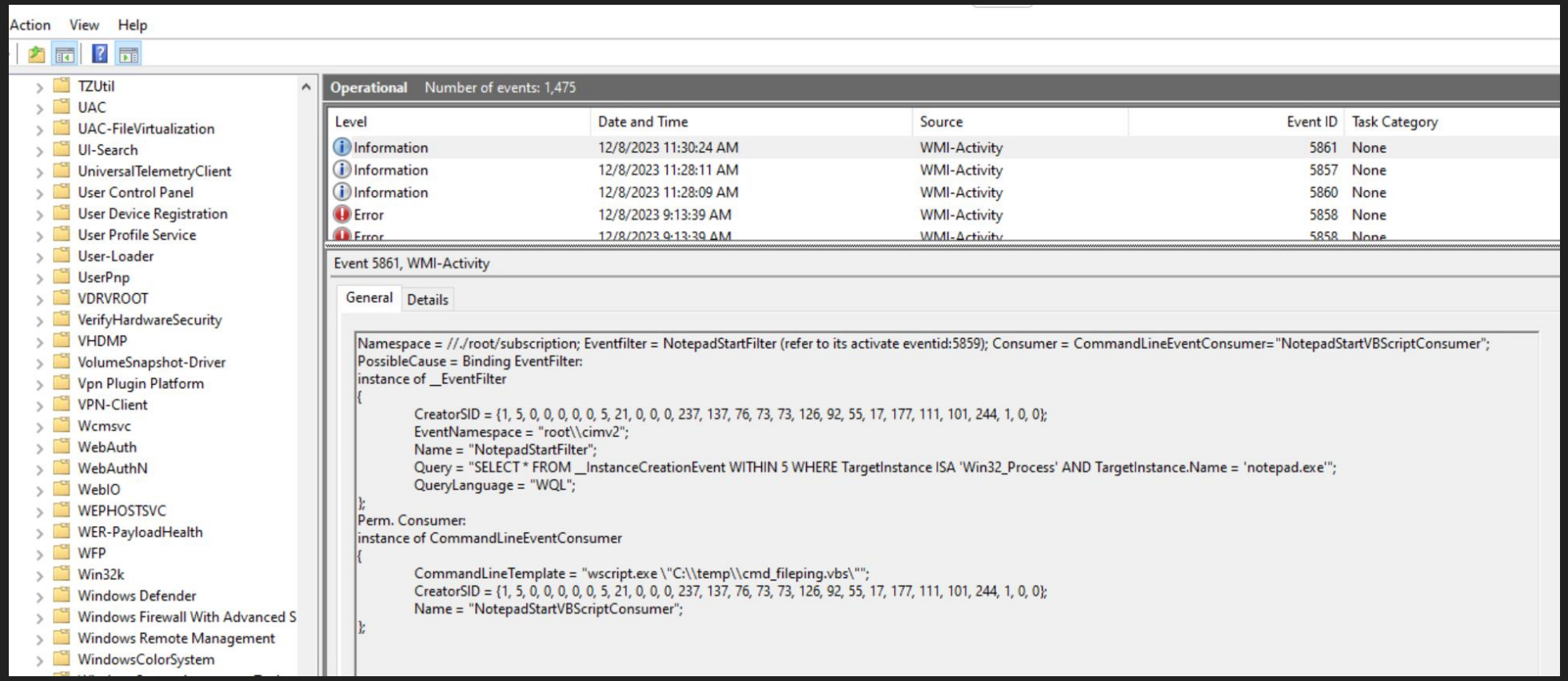



```
PS C:\Users\Administrator\Desktop\Purple\wmi> cscript.exe .\cmd_fileping.vbs
CScript Error: Windows Script Host access is disabled on this machine. Contact your administrator for details.
```

WMI – Telemetry

Telemetry – WMI activity

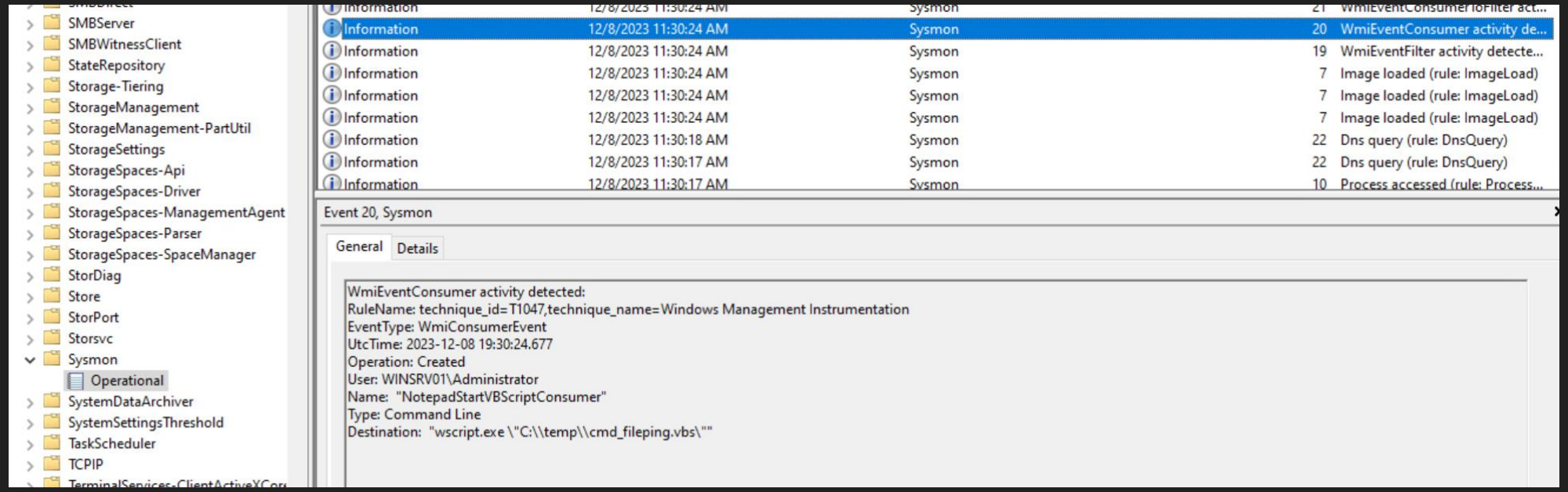
- Microsoft-Windows-WMI-Activity/Operational



Telemetry – Sysmon WMI Activity

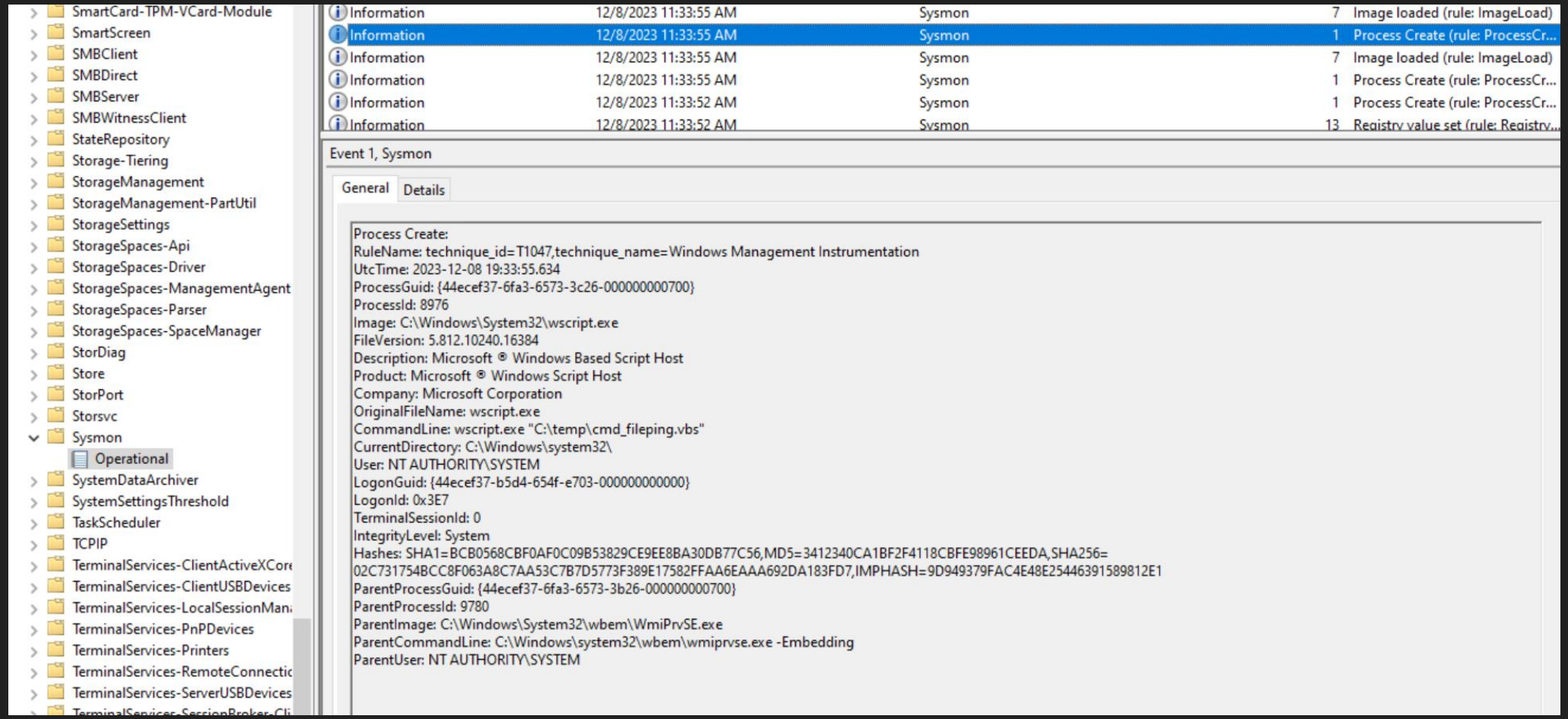
- Sysmon event ID 19, 20 and 21

```
<!-- Event ID 19,20,21, == WmiEvent. Log all WmiEventFilter, WmiEventConsumer, WmiEventConsumerToFilter activity - Includes -->
<RuleGroup groupRelation="or">
  <WmiEvent onmatch="include">
    <Operation name="technique_id=T1047,technique_name=Windows Management Instrumentation" condition="is">Created</Operation>
  </WmiEvent>
</RuleGroup>
```



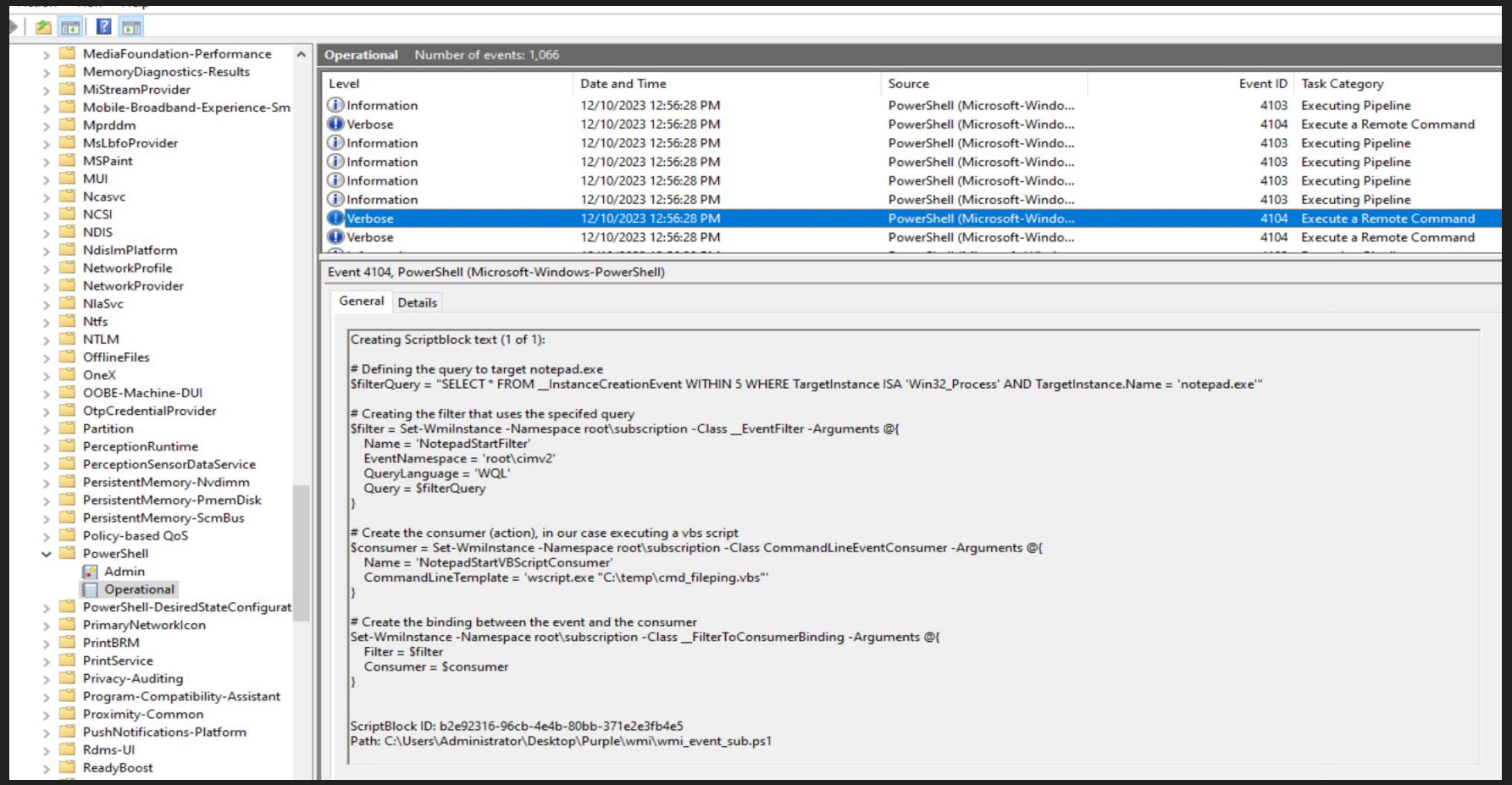
Telemetry – Process Creation Parent WMIPrvSE

- Sysmon event ID 1



Telemetry – Powershell logging

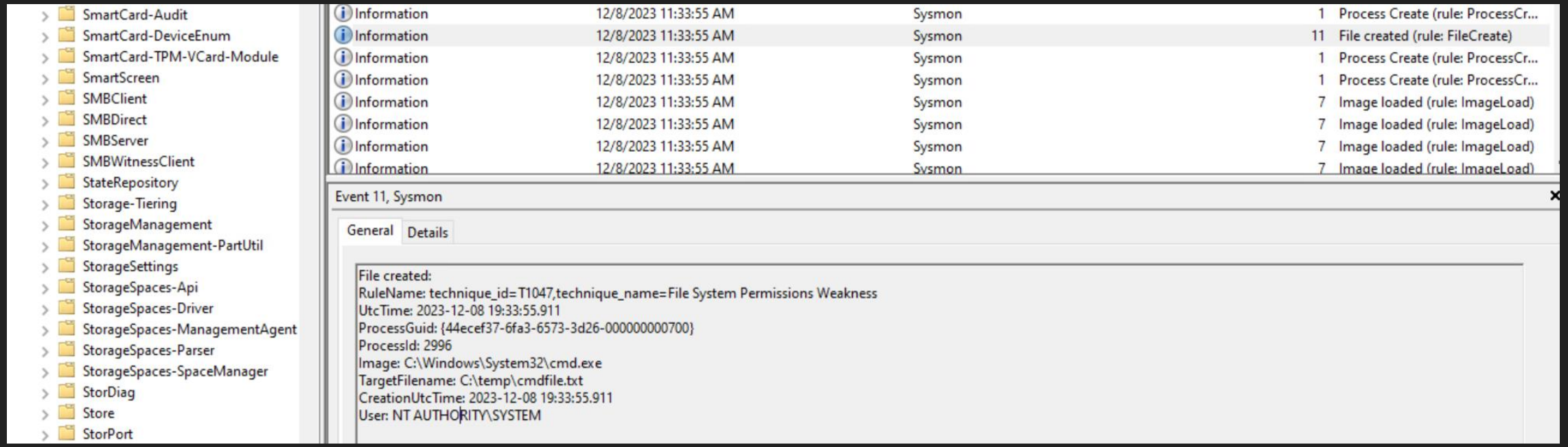
- Microsoft-Windows-PowerShell/Operational



Telemetry – Sysmon File Creation

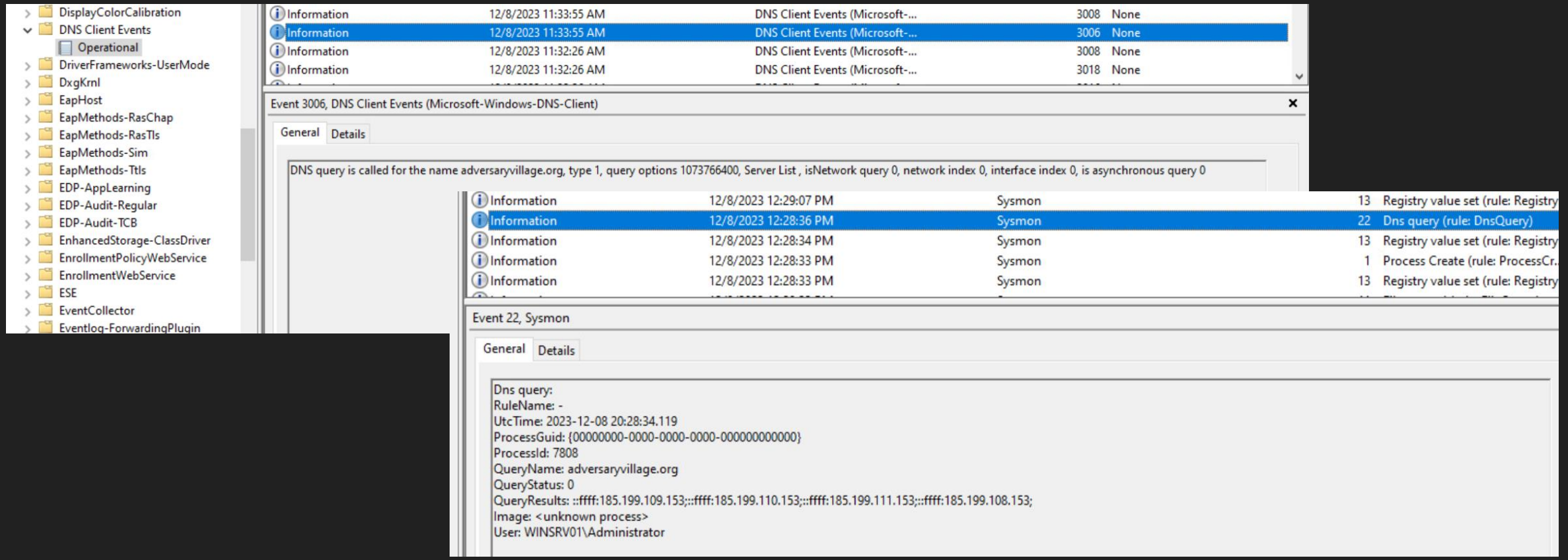
- Sysmon event ID 11

```
<TargetFilename name="technique_id=T1546.008,technique_name=Services File Permissions Weakness" condition="begin with">C:\Windows\Temp\</TargetFilename
<TargetFilename name="technique_id=T1546.008,technique_name=Services File Permissions Weakness" condition="begin with">C:\Program\</TargetFilename>
<TargetFilename name="technique_id=T1047,technique_name=File System Permissions Weakness" condition="begin with">C:\Temp\</TargetFilename>
<TargetFilename name="technique_id=T1047,technique_name=File System Permissions Weakness" condition="begin with">C:\PerfLogs\</TargetFilename>
<TargetFilename name="technique_id=T1047,technique_name=File System Permissions Weakness" condition="begin with">C:\Users\Public\</TargetFilename>
```



Telemetry – DNS Query

- Sysmon event ID 22
- Microsoft-Windows-DNS Client Events/Operational



Telemetry – Others

- EDR Telemetry
- Object access (4662)
- NGFW, IDS on DNS query (network)
- Prioritize telemetry collection

Sigma Log Source	Channel and EID	Default Settings	Rules	Percent
process_creation	Microsoft-Windows-Sysmon/Operational 1 or Security 4688	non-default	804	49.36%
security	Security	partial	139	8.53%
ps_script	Microsoft-Windows-PowerShell/Operational 4104	partial	125	7.67%
registry_set	Microsoft-Windows-Sysmon/Operational 13	sysmon	109	6.69%
file_event	Microsoft-Windows-Sysmon/Operational 11	sysmon	96	5.89%
system	System	default	50	3.07%
image_load	Microsoft-Windows-Sysmon/Operational 7	sysmon	39	2.39%
registry_event	Microsoft-Windows-Sysmon/Operational 12/13/14	sysmon	37	2.27%
ps_module	Microsoft-Windows-PowerShell/Operational 4103	non-default	30	1.84%
network_connection	Microsoft-Windows-Sysmon/Operational 3	sysmon	29	1.78%
process_access	Microsoft-Windows-Sysmon/Operational 10	sysmon	25	1.53%
pipe_created	Microsoft-Windows-Sysmon/Operational 17/18	sysmon	14	0.86%
application	Application	default	13	0.80%
dns_query	Microsoft-Windows-Sysmon/Operational 22	sysmon	12	0.74%
ps_classic_start	Windows PowerShell 400	default	10	0.61%
create_remote_thread	Microsoft-Windows-Sysmon/Operational 8	sysmon	10	0.61%

ent logs to collect the telemetry)

enabled easily as part of the EDR product but is not ON by default.)

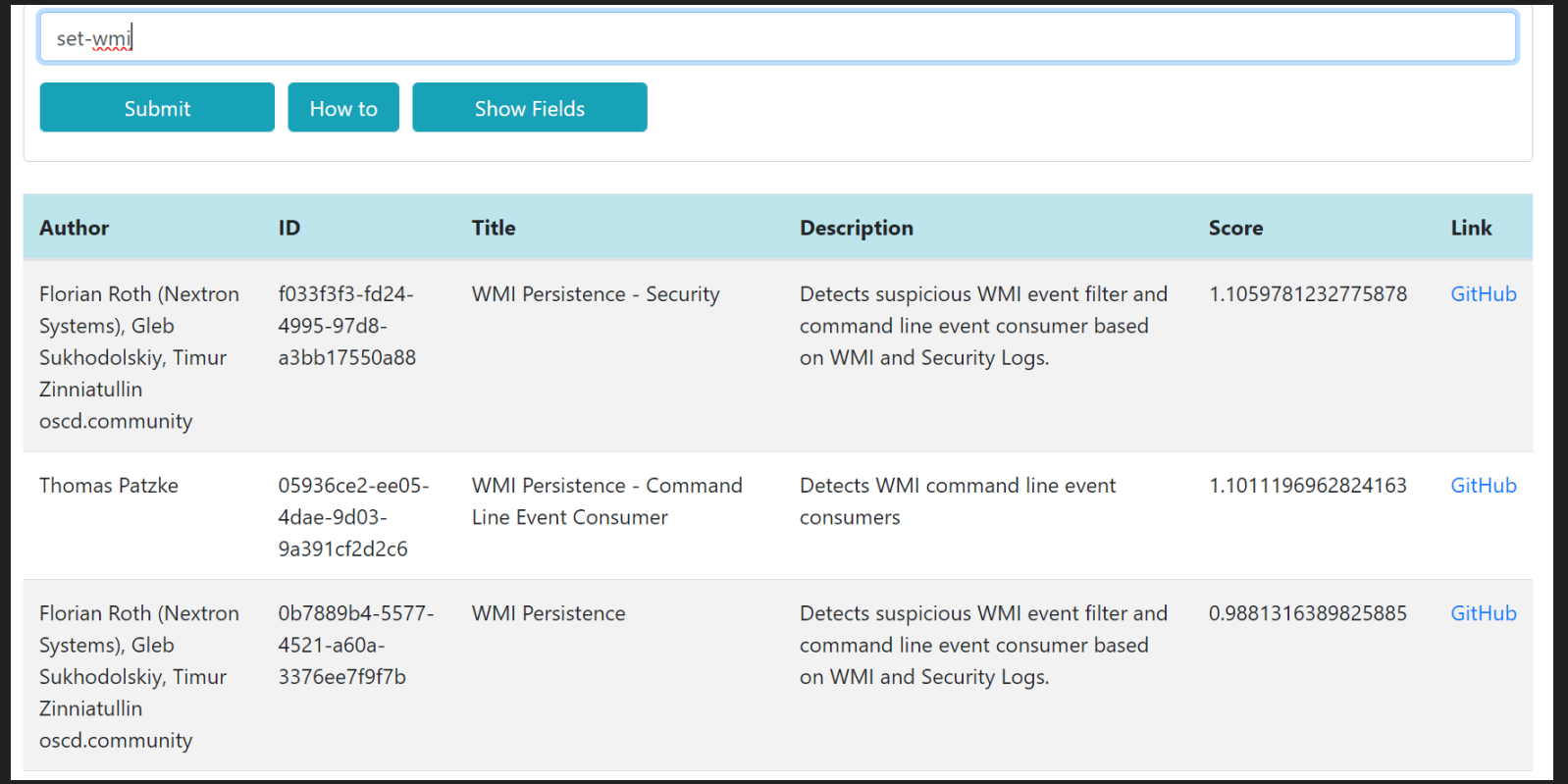
Cybereason	ESET Inspect	Elastic	LimaCharlie	MDE

WMI – Detection

AKA Don’t reinvent the wheel

Detection – Sigma

- https://sigmasearchengine.com/
- Search for 'set-wmi'



Author	ID	Title	Description	Score	Link
Florian Roth (Nextron Systems), Gleb Sukhodolskiy, Timur Zinniatullin oscd.community	f033f3f3-fd24-4995-97d8-a3bb17550a88	WMI Persistence - Security	Detects suspicious WMI event filter and command line event consumer based on WMI and Security Logs.	1.1059781232775878	GitHub
Thomas Patzke	05936ce2-ee05-4dae-9d03-9a391cf2d2c6	WMI Persistence - Command Line Event Consumer	Detects WMI command line event consumers	1.1011196962824163	GitHub
Florian Roth (Nextron Systems), Gleb Sukhodolskiy, Timur Zinniatullin oscd.community	0b7889b4-5577-4521-a60a-3376ee7f9f7b	WMI Persistence	Detects suspicious WMI event filter and command line event consumer based on WMI and Security Logs.	0.9881316389825885	GitHub

Detection – Sigma

```yaml
title: WMI Persistence
id: 0b7889b4-5577-4521-a60a-3376ee7f9f7b
status: test
description: Detects suspicious WMI event filter and command line event consumer based on WMI and Security Logs.
references:
    - https://twitter.com/mattifestation/status/899646620148539397
    - https://www.eideon.com/2018-03-02-THL03-WMIBackdoors/
author: Florian Roth (Nextron Systems), Gleb Sukhodolskiy, Timur Zinniatullin oscd.community
date: 2017/08/22
modified: 2022/02/10
tags:
    - attack.persistence
    - attack.privilege_escalation
    - attack.t1546.003
logsource:
    product: windows
    service: wmi
    definition: 'WMI Namespaces Auditing and SACL should be configured, EventID 5861 and 5859 detection requires Windows 10, 2012 and higher'
detection:
    wmi_filter_to_consumer_binding:
        EventID: 5861
    consumer_keywords:
        - 'ActiveScriptEventConsumer'
        - 'CommandLineEventConsumer'
        - 'CommandLineTemplate'
        # - 'Binding EventFilter'  # too many false positive with HP Health Driver
    wmi_filter_registration:
        EventID: 5859
    filter_scmevent:
        Provider: 'SCM Event Provider'
        Query: 'select * from MSFT_SCMEventLogEvent'
        User: 'S-1-5-32-544'
        PossibleCause: 'Permanent'
    condition: ( (wmi_filter_to_consumer_binding and consumer_keywords) or (wmi_filter_registration) ) and not filter_scmevent
falsepositives:
    - Unknown (data set is too small; further testing needed)
level: medium
```

Detection – Sigma

```yaml
title: WMI Event Subscription
id: 0f06a3a5-6a09-413f-8743-e6cf35561297
status: test
description: Detects creation of WMI event subscription persistence method
author: Tom Ueltschi (@c_APT_ure)
date: 2019/01/12
modified: 2021/11/27
tags:
    - attack.persistence
    - attack.t1546.003
logsource:
    product: windows
    category: wmi_event
detection:
    selection:
        EventID:
            - 19
            - 20
            - 21
    condition: selection
falsepositives:
    - Exclude legitimate (vetted) use of WMI event subscription in your network
level: medium
```

Detection – Sigma

- https://sigmasearchengine.com/
- Search for the technique 'T546.003'

T1546.003

Submit | How to | Show Fields

Author	ID	Title	Description	Score	Link
frack113	9e07f6e7-83aa-45c6-998e-0af26efd0a85	Powershell WMI Persistence	Adversaries may establish persistence and elevate privileges by executing malicious content triggered by a Windows Management Instrumentation (WMI) event subscription.	1.3294814157170132	GitHub

Thanks to: https://github.com/SigmaHQ/sigma & https://blevesearch.com/

Detection – Sigma

```yaml
title: Powershell WMI Persistence
id: 9e07f6e7-83aa-45c6-998e-0af26efd0a85
status: test
description: Adversaries may establish persistence and elevate privileges by executing malicious content triggered by a Windows Management Instrumentation (WMI) event subscription.
references:
    - https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1546.003/T1546.003.md
    - https://github.com/EmpireProject/Empire/blob/08cbd274bef78243d7a8ed6443b8364acd1fc48b/data/module_source/persistence/Persistence.psm1#L545
author: frack113
date: 2021/08/19
modified: 2022/12/25
tags:
    - attack.privilege_escalation
    - attack.t1546.003
logsource:
    product: windows
    category: ps_script
    definition: 'Requirements: Script Block Logging must be enabled'
detection:
    selection_ioc:
        - ScriptBlockText|contains|all:
            - 'New-CimInstance '
            - '-Namespace root/subscription '
            - '-ClassName __EventFilter '
            - '-Property ' # is a variable name
        - ScriptBlockText|contains|all:
            - 'New-CimInstance '
            - '-Namespace root/subscription '
            - '-ClassName CommandLineEventConsumer '
            - '-Property ' # is a variable name
    condition: selection_ioc
falsepositives:
    - Unknown
level: medium
```

Detection – MITRE CAR

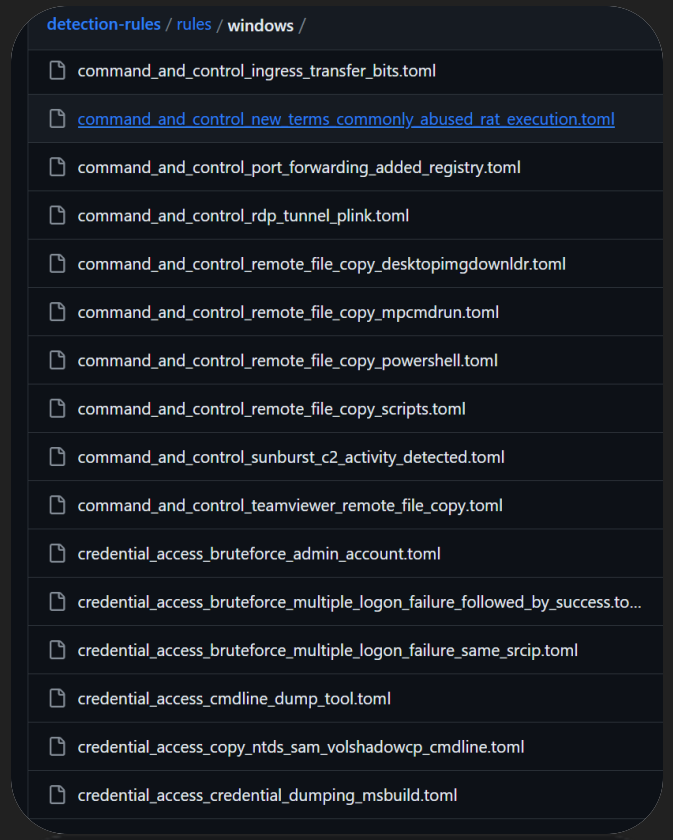
- https://car.mitre.org/analytics/by_technique

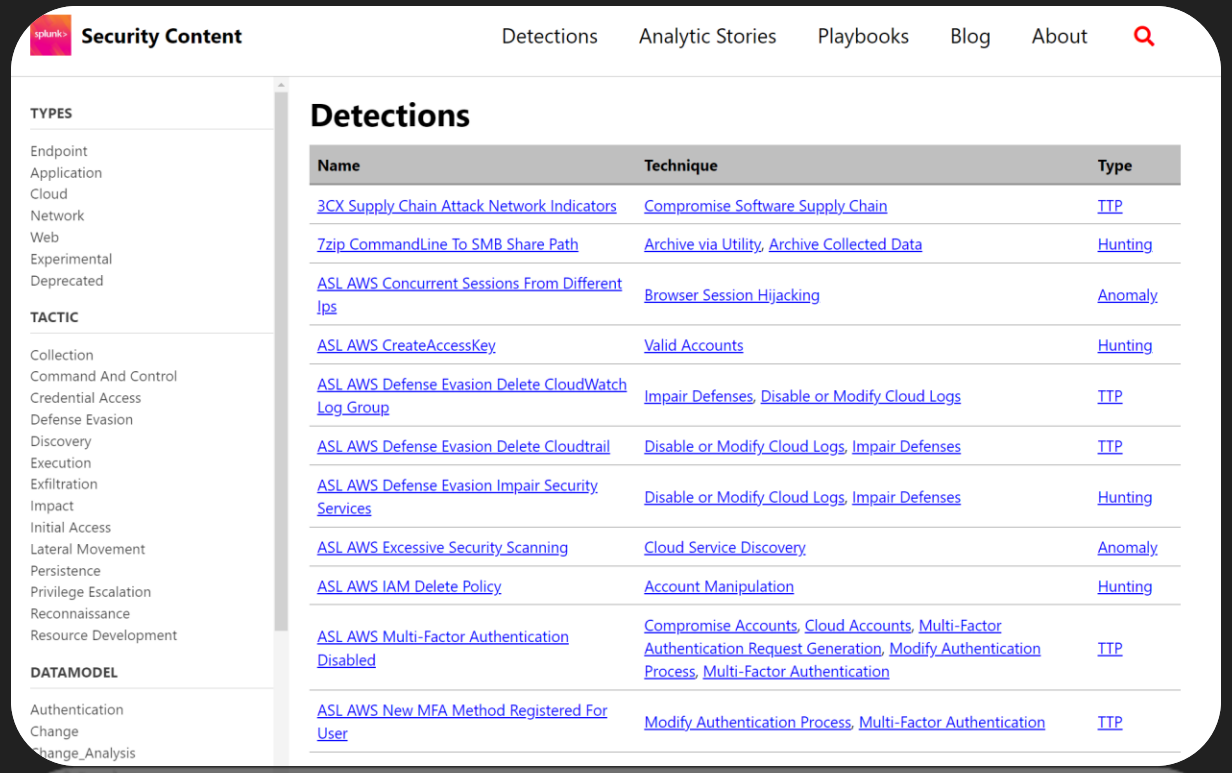
	T1546.001: Change Default File Association	• CAR-2013-01-002: Autorun Differences
T1546: Event Triggered Execution	T1546.003: Windows Management Instrumentation Event Subscription	• CAR-2013-01-002: Autorun Differences
		• CAR-2013-01-002: Autorun Differences

- Ok not a detection but it is an interesting hunt to run periodically!

Detection – Others

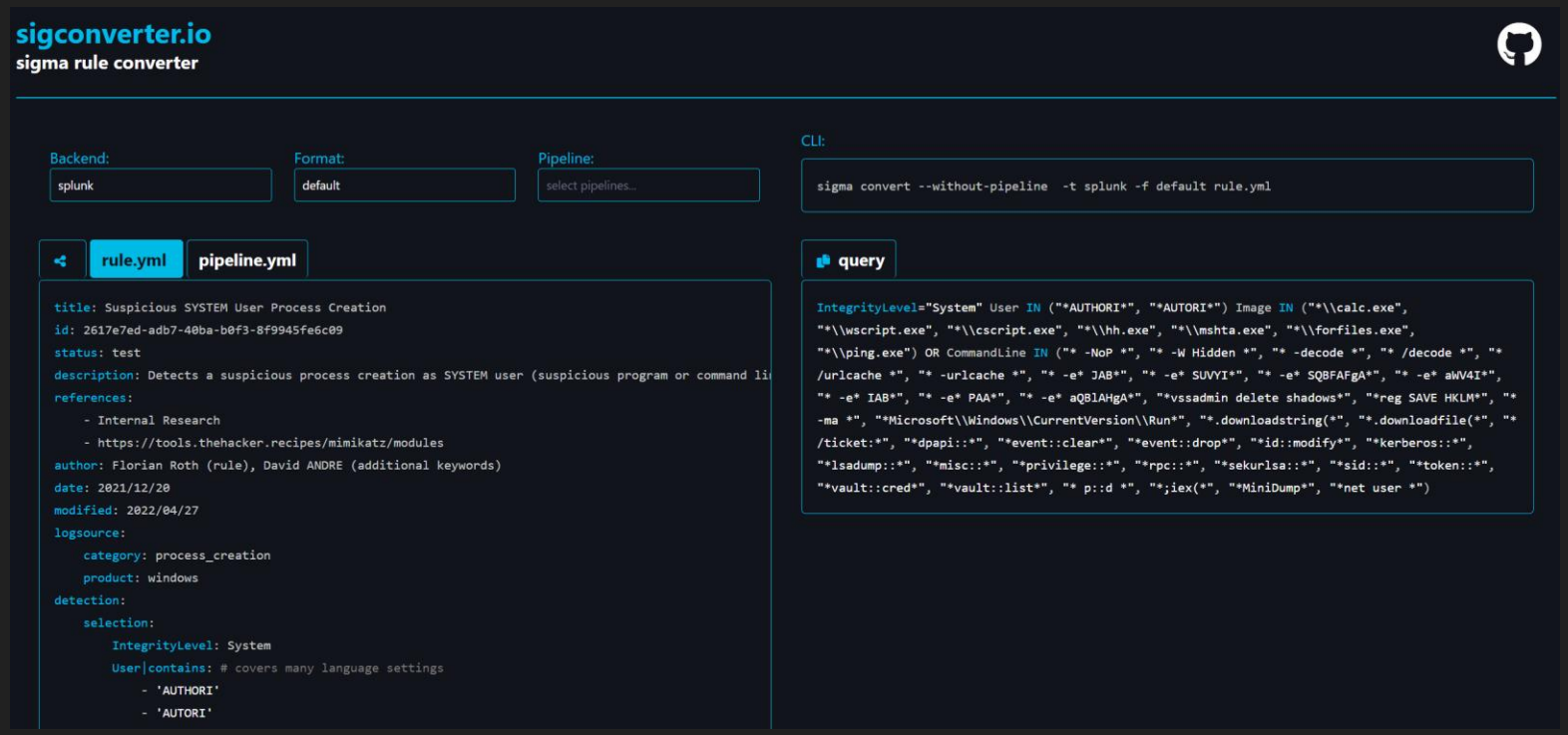
- Elastic, Splunk, Microsoft, Google, Joe, TheDFIRReport, etc.



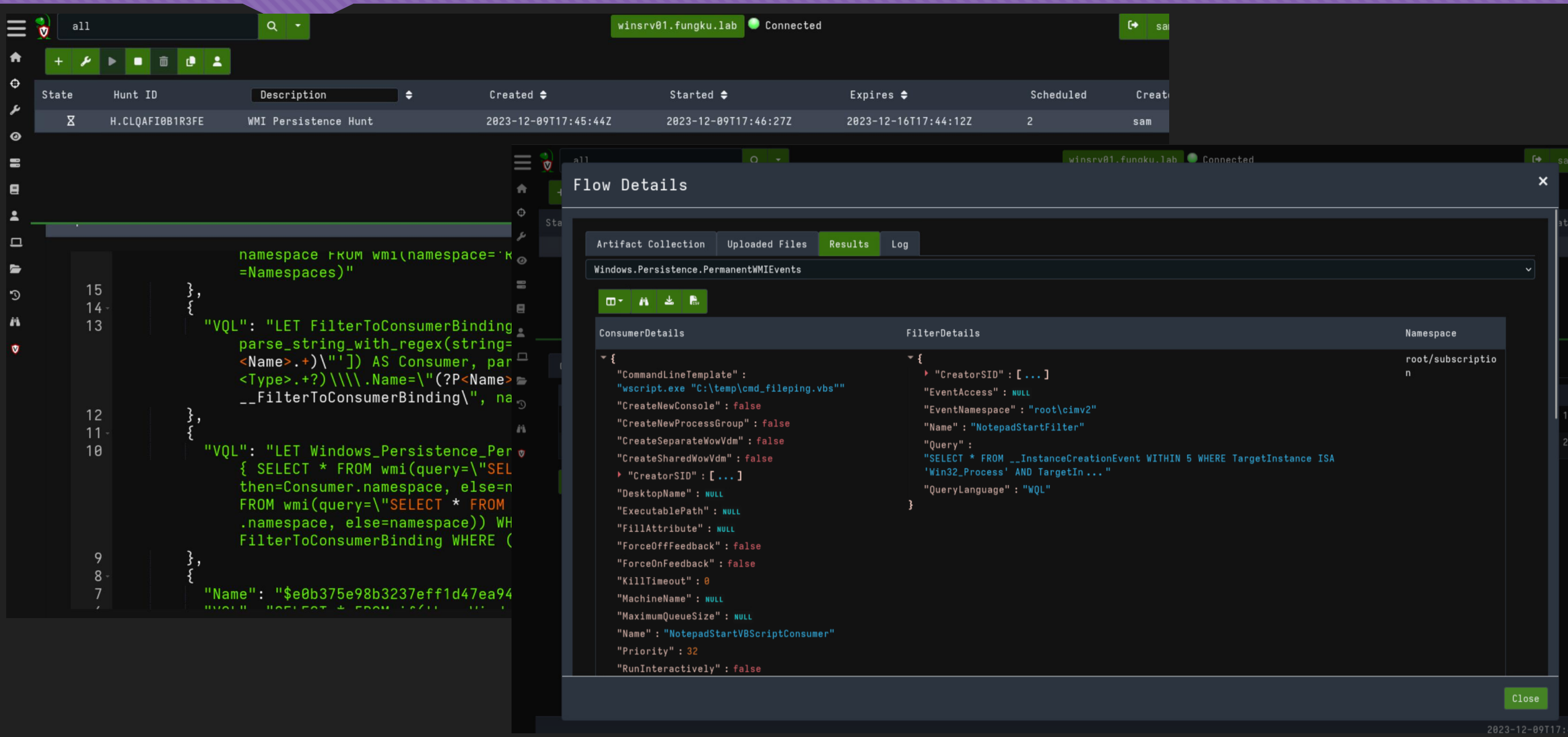


Detection – Translation

- https://sigconverter.io/
- https://uncoder.io/
- ChatGPT
- Manual fine-tuning



Detection – Bonus: Velociraptor Hunt



Conclusion

Conclusion

- Purple is awesome!
- Improve CTI and Red
- Take-aways:
  - Learning resources
  - Simulation plan
    - https://github.com/Sam0x90/CTI/tree/main/Adversary%20Emulation%20Plans/2022_Top35_Mitre
  - Quick wins resources
    - https://github.com/Sam0x90/CTI/blob/main/PurpleTeamResourceCollection.md

Thank you

@sam0x90