

CANCEL YOUR PENTEST AND PURPLE THIS INSTEAD

Adversary Village Live-streaming series #5

Samuel Rossier

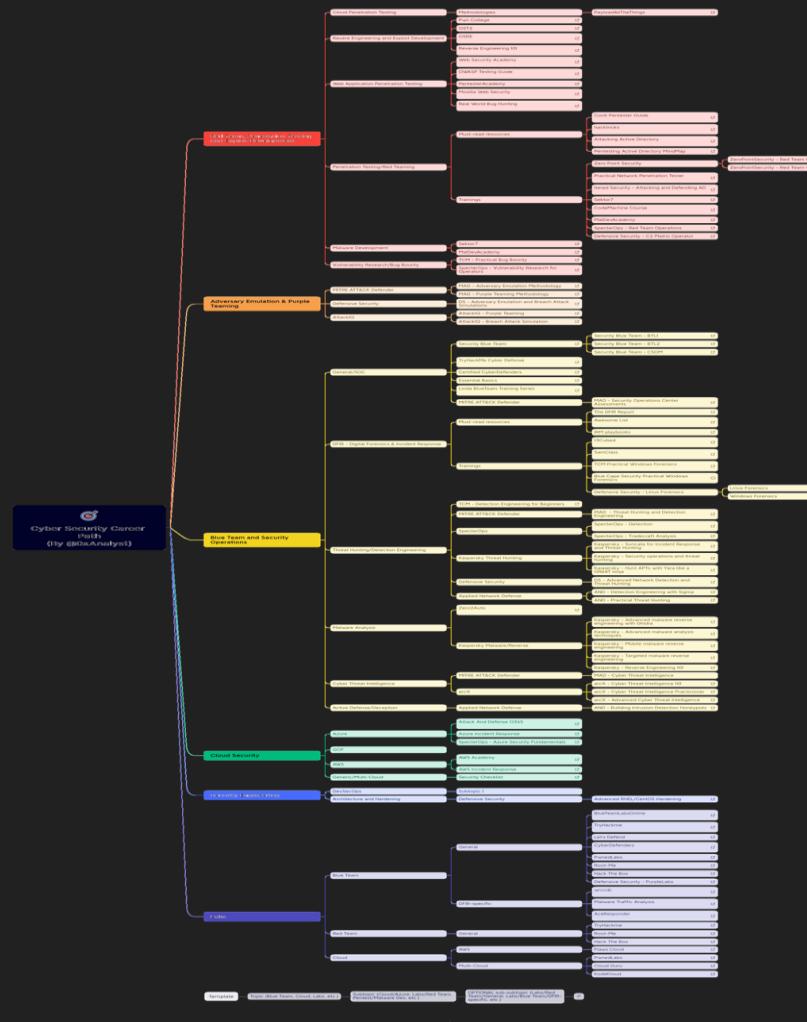
whoami.exe motivation.exe

- 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

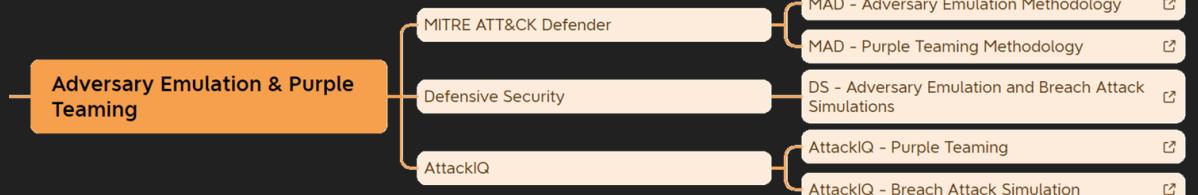
Methodology

- 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

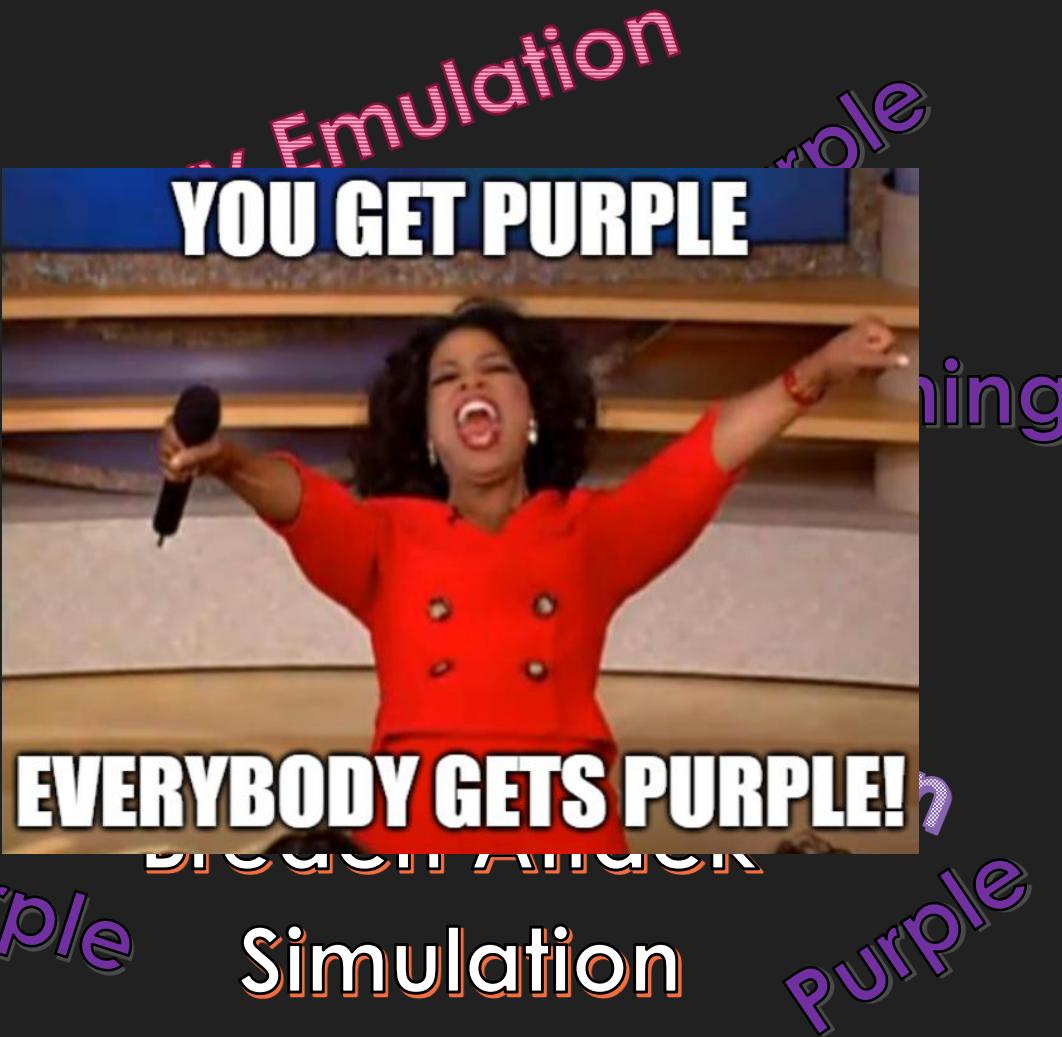


Introduction – Purple flavors



Introduction – Purple flavors

Purple
Threat-Informed Defense



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?

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?



Threat-Informed
Defense

Purple Teaming

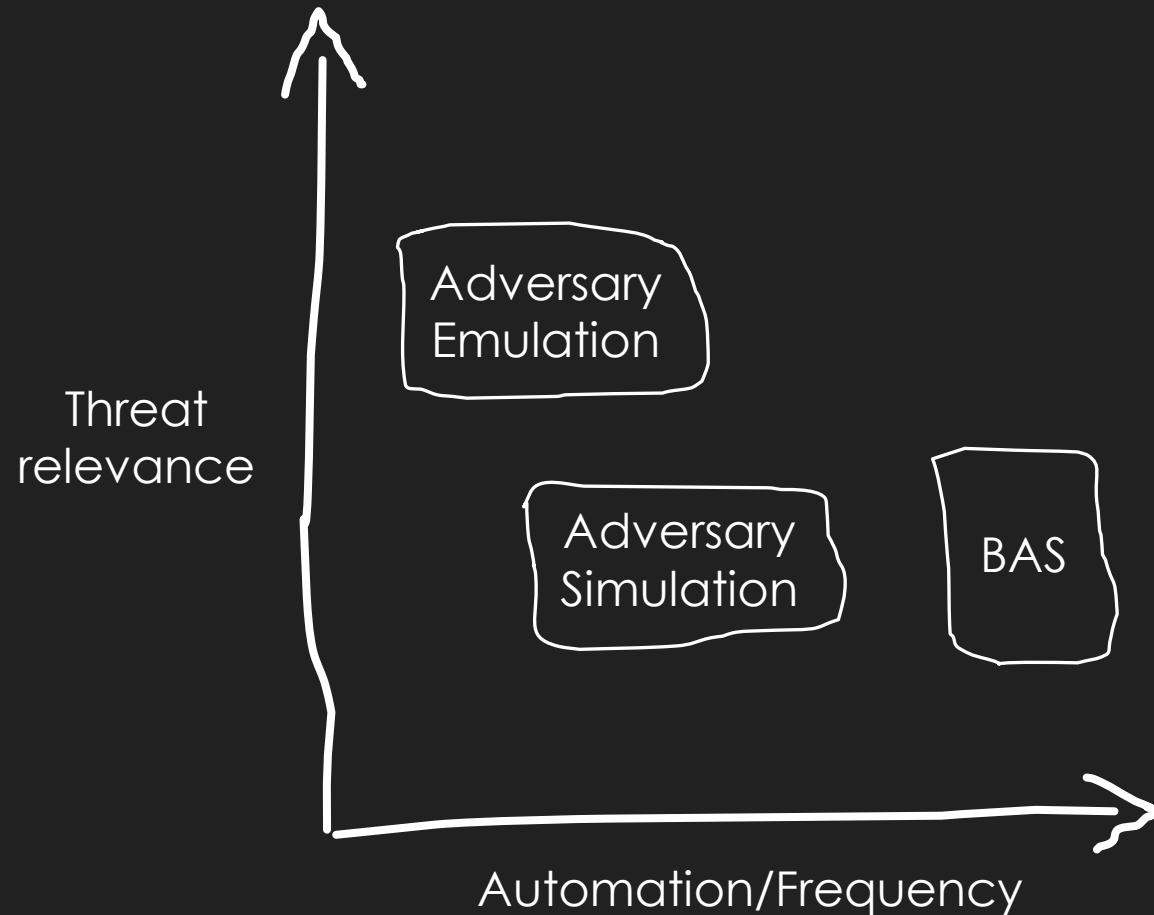
Continuous
Security
Testing

Adversary
Simulation

Adversary
Emulation

Breach
Attack
Simulation

Introduction – Sophisticated study



Introduction – Automation <3 Manual

Adversary
Emulation

Adversary
Simulation

BAS



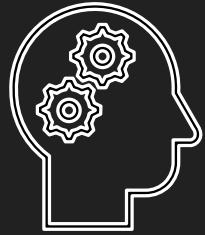
Objective:

Ensure security controls are
ready against a wide
variety of threats



Automation/Frequency

Introduction – Automation <3 Manual



Objective:

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

Adversary
Emulation

Adversary
Simulation

BAS



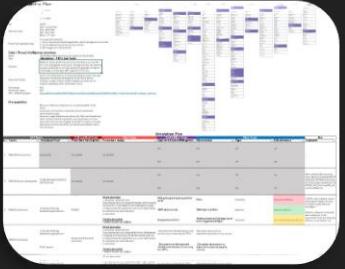
Automation/Frequency

Adversary Simulation

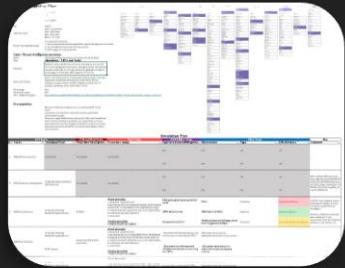
Adversary Simulation – Where are we?



Adversary Simulation – Where are we?



Adversary Simulation – Where are we?

A screenshot of a Windows PowerShell window. The command being typed is '\$ hack_everything.sh'. The terminal shows a standard Windows command-line interface with a blue header bar.

Adversary Simulation – Walkthrough

Grab the plan!

https://github.com/Sam0x90/CTI/tree/main/Adversary%20Emulation%20Plans/2022_Top3_5_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)

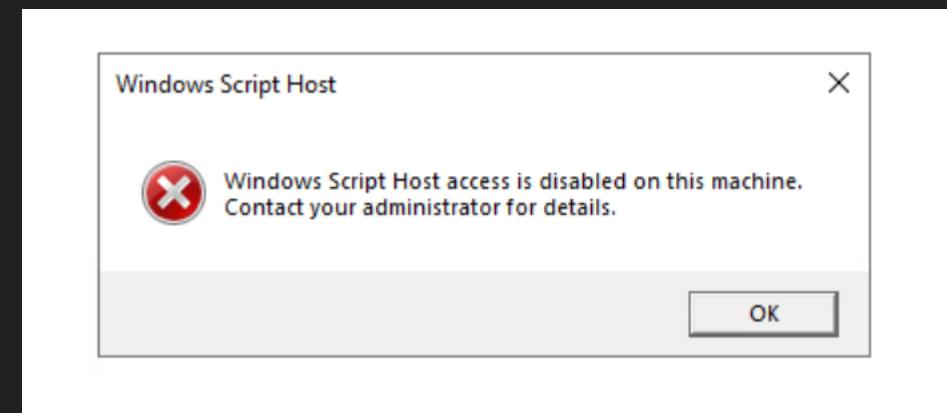
Name	Description
Service name	WinRM
Description	Windows Remote Management (WinRM) service implements the WS-Management protocol for remote management. WS-Management is a standard web services protocol used for remote software and hardware management. The WinRM service listens on the network for WS-Management requests and processes them. The WinRM Service needs to be configured with a listener using <code>winrm.cmd</code> 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 <code>/wsman</code> URL prefix. To prevent conflicts with IIS, administrators should ensure that any websites hosted on IIS do not use the <code>/wsman</code> 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’

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Script Host\Settings		
	Name	Type
UPnP Device Host	(Default)	REG_SZ
UserData	ActiveDebugging	REG_SZ
UserManager	DisplayLogo	REG_SZ
Virtual Machine	SilentTerminate	REG_SZ
VisualStudio	UseWINSAFER	REG_SZ
WAB	Enabled	REG_DWORD



```
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.
PS C:\Users\Administrator\Desktop\Purple\wmi>
```

WMI – Telemetry

Telemetry – WMI activity

○ Microsoft-Windows-WMI-Activity/Operational

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of event sources, and the right pane shows a list of events under the "Operational" category.

Event Viewer Screenshot:

- Action View Help**
- Operational Number of events: 1,475**
- Level Date and Time Source Event ID Task Category**
- Information 12/8/2023 11:30:24 AM WMI-Activity 5861 None
- Information 12/8/2023 11:28:11 AM WMI-Activity 5857 None
- Information 12/8/2023 11:28:09 AM WMI-Activity 5860 None
- Error 12/8/2023 9:13:39 AM WMI-Activity 5858 None
- Error 12/8/2023 9:13:39 AM WMI-Activity 5858 None

Event 5861, WMI-Activity

General Details

```
Namespace = //./root/subscription; Eventfilter = NotepadStartFilter (refer to its activate eventid:5859); Consumer = CommandLineEventConsumer="NotepadStartVBScriptConsumer";
PossibleCause = Binding EventFilter;
instance of _EventFilter
{
    CreatorSID = {1, 5, 0, 0, 0, 0, 5, 21, 0, 0, 0, 237, 137, 76, 73, 73, 126, 92, 55, 17, 177, 111, 101, 244, 1, 0, 0};
    EventNamespace = "root\\cimv2";
    Name = "NotepadStartFilter";
    Query = "SELECT * FROM __InstanceCreationEvent WITHIN 5 WHERE TargetInstance ISA 'Win32_Process' AND TargetInstance.Name = 'notepad.exe'";
    QueryLanguage = "WQL";
}
Perm. Consumer:
instance of CommandLineEventConsumer
{
    CommandLineTemplate = "wscript.exe \"C:\\temp\\cmd_fileping.vbs\"";
    CreatorSID = {1, 5, 0, 0, 0, 0, 5, 21, 0, 0, 0, 237, 137, 76, 73, 73, 126, 92, 55, 17, 177, 111, 101, 244, 1, 0, 0};
    Name = "NotepadStartVBScriptConsumer";
}
```

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>
```

The screenshot shows the Sysmon WMI Activity log interface. On the left is a navigation pane with a tree view of system components like SMBServer, StorageManagement, and Sysmon. The main area displays a table of events:

Event ID	Time	User	Source	Description
21	12/8/2023 11:30:24 AM	Sysmon		WmiEventConsumerToFilter activity detected
20	12/8/2023 11:30:24 AM	Sysmon		WmiEventConsumer activity detected
19	12/8/2023 11:30:24 AM	Sysmon		WmiEventFilter activity detected
7	12/8/2023 11:30:24 AM	Sysmon		Image loaded (rule: ImageLoad)
7	12/8/2023 11:30:24 AM	Sysmon		Image loaded (rule: ImageLoad)
7	12/8/2023 11:30:24 AM	Sysmon		Image loaded (rule: ImageLoad)
22	12/8/2023 11:30:18 AM	Sysmon		Dns query (rule: DnsQuery)
22	12/8/2023 11:30:17 AM	Sysmon		Dns query (rule: DnsQuery)
10	12/8/2023 11:30:17 AM	Sysmon		Process accessed (rule: ProcessAccess)

A context menu is open over the first event (ID 21), showing options like "Copy", "Paste", "Delete", and "Details". The "Details" tab is selected, displaying the following information:

WmiEventConsumer activity detected:
RuleName: technique_id=T1047,technique_name=Windows Management Instrumentation
EventType: WmiConsumerEvent
UtcTime: 2023-12-08 19:30:24.677
Operation: Created
User: WINSRV01\Administrator
Name: "NotepadStartVBScriptConsumer"
Type: Command Line
Destination: "wscript.exe \"C:\\temp\\cmd_fileping.vbs\""

Telemetry – Process Creation Parent WMIPrvSE

○ Sysmon event ID 1

The screenshot shows a Windows application window titled "Event 1, Sysmon". On the left is a tree view of system components, with "Sysmon" expanded to show "Operational" and other sub-components. The main pane displays a table of log entries. One entry is highlighted in blue, corresponding to the event shown in the details pane below.

Type	Date	User	Source	Message
Information	12/8/2023 11:33:55 AM	Sysmon		7 Image loaded (rule: ImageLoad)
Information	12/8/2023 11:33:55 AM	Sysmon		1 Process Create (rule: ProcessCr...
Information	12/8/2023 11:33:55 AM	Sysmon		7 Image loaded (rule: ImageLoad)
Information	12/8/2023 11:33:55 AM	Sysmon		1 Process Create (rule: ProcessCr...
Information	12/8/2023 11:33:52 AM	Sysmon		1 Process Create (rule: ProcessCr...
Information	12/8/2023 11:33:52 AM	Sysmon		13 Registry value set (rule: Registry...

Event 1, Sysmon

General Details

Process Create:

RuleName: technique_id=T1047,technique_name=Windows Management Instrumentation
UtcTime: 2023-12-08 19:33:55.634
ProcessGuid: {44ecef37-6fa3-6573-3c26-000000000700}
ProcessId: 8976
Image: C:\Windows\System32\wscript.exe
FileVersion: 5.812.10240.16384
Description: Microsoft ® Windows Based Script Host
Product: Microsoft ® Windows Script Host
Company: Microsoft Corporation
OriginalFileName: wscript.exe
CommandLine: wscript.exe "C:\temp\cmd_fileping.vbs"
CurrentDirectory: C:\Windows\system32\
User: NT AUTHORITY\SYSTEM
LogonGuid: {44ecef37-b5d4-654f-e703-000000000000}
LogonId: 0x3E7
TerminalSessionId: 0
IntegrityLevel: System
Hashes: SHA1=BCB0568CBF0AF0C09B53829CE9EE8BA30DB77C56,MD5=3412340CA1BF2F4118CBFE98961CEEDA,SHA256=02C731754BC8F063A8C7AA53C7B7D5773F389E17582FFAA6EAAA692DA183FD7,IMPHASH=9D949379FAC4E48E25446391589812E1
ParentProcessGuid: {44ecef37-6fa3-6573-3b26-000000000700}
ParentProcessId: 9780
ParentImage: C:\Windows\System32\wbem\WmiPrvSE.exe
ParentCommandLine: C:\Windows\system32\wbem\wmiprvse.exe -Embedding
ParentUser: NT AUTHORITY\SYSTEM

Telemetry – Powershell logging

○ Microsoft-Windows-PowerShell/Operational

The screenshot shows the Windows Event Viewer interface. On the left, a navigation pane lists various Windows services and components. In the center, a main pane displays a table of events under the 'Operational' category. The table has columns for Level, Date and Time, Source, Event ID, and Task Category. Several events are listed, with one specific event highlighted in blue. Below the table, a detailed view of event 4104 is shown, titled 'Event 4104, PowerShell (Microsoft-Windows-PowerShell)'. This view includes tabs for 'General' and 'Details'. The 'Details' tab contains a large block of PowerShell script code, which defines a WMI query to target 'notepad.exe', creates a filter, a consumer, and a binding between them. The script also specifies a command-line template to execute a VBScript file. At the bottom of the details pane, it shows the 'ScriptBlock ID' and the 'Path' where the script was saved.

Level	Date and Time	Source	Event ID	Task Category
Information	12/10/2023 12:56:28 PM	PowerShell (Microsoft-Windo...	4103	Executing Pipeline
Verbose	12/10/2023 12:56:28 PM	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Information	12/10/2023 12:56:28 PM	PowerShell (Microsoft-Windo...	4103	Executing Pipeline
Information	12/10/2023 12:56:28 PM	PowerShell (Microsoft-Windo...	4103	Executing Pipeline
Information	12/10/2023 12:56:28 PM	PowerShell (Microsoft-Windo...	4103	Executing Pipeline
Information	12/10/2023 12:56:28 PM	PowerShell (Microsoft-Windo...	4103	Executing Pipeline
Information	12/10/2023 12:56:28 PM	PowerShell (Microsoft-Windo...	4103	Executing Pipeline
Information	12/10/2023 12:56:28 PM	PowerShell (Microsoft-Windo...	4103	Executing Pipeline
Verbose	12/10/2023 12:56:28 PM	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Verbose	12/10/2023 12:56:28 PM	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command

Event 4104, PowerShell (Microsoft-Windows-PowerShell)

General Details

Creating Scriptblock text (1 of 1):

```
# Defining the query to target notepad.exe
$filterQuery = "SELECT * FROM __InstanceCreationEvent WITHIN 5 WHERE TargetInstance ISA 'Win32_Process' AND TargetInstance.Name = 'notepad.exe'"
```

```
# Creating the filter that uses the specified query
$filter = Set-WmiInstance -Namespace root\subscription -Class __EventFilter -Arguments @{
    Name = 'NotepadStartFilter'
    EventNamespace = 'root\cimv2'
    QueryLanguage = 'WQL'
    Query = $filterQuery
}
```

```
# Create the consumer (action), in our case executing a vbs script
$consumer = Set-WmiInstance -Namespace root\subscription -Class CommandLineEventConsumer -Arguments @{
    Name = 'NotepadStartVBSConsumer'
    CommandLineTemplate = 'wscript.exe "C:\temp\cmd_fileping.vbs"'
}
```

```
# Create the binding between the event and the consumer
Set-WmiInstance -Namespace root\subscription -Class __FilterToConsumerBinding -Arguments @{
    Filter = $filter
    Consumer = $consumer
}
```

ScriptBlock ID: b2e92316-96cb-4e4b-80bb-371e2e3fb4e5
Path: C:\Users\Administrator\Desktop\Purple\wmi\wmi_event_sub.ps1

Telemetry – Sysmon File Creation

○ Sysmon event ID 11

```
<Image Name="technique_id=T1047,technique_name=Windows Management Instrumentation Condition begin with >C:\Windows\System32\wbem\services.exe> /Image>
<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>
```

> SmartCard-Audit	Information	12/8/2023 11:33:55 AM	Sysmon	1 Process Create (rule: ProcessCr...
> SmartCard-DeviceEnum	Information	12/8/2023 11:33:55 AM	Sysmon	11 File created (rule: FileCreate)
> SmartCard-TPM-VCard-Module	Information	12/8/2023 11:33:55 AM	Sysmon	1 Process Create (rule: ProcessCr...
> SmartScreen	Information	12/8/2023 11:33:55 AM	Sysmon	1 Process Create (rule: ProcessCr...
> SMBClient	Information	12/8/2023 11:33:55 AM	Sysmon	7 Image loaded (rule: ImageLoad)
> SMBDirect	Information	12/8/2023 11:33:55 AM	Sysmon	7 Image loaded (rule: ImageLoad)
> SMBServer	Information	12/8/2023 11:33:55 AM	Sysmon	7 Image loaded (rule: ImageLoad)
> SMBWitnessClient	Information	12/8/2023 11:33:55 AM	Sysmon	7 Image loaded (rule: ImageLoad)
> StateRepository	Information	12/8/2023 11:33:55 AM	Sysmon	7 Image loaded (rule: ImageLoad)
> Storage-Tiering	Information	12/8/2023 11:33:55 AM	Sysmon	7 Image loaded (rule: ImageLoad)
> StorageManagement	Information	12/8/2023 11:33:55 AM	Sysmon	7 Image loaded (rule: ImageLoad)
> StorageManagement-PartUtil	Information	12/8/2023 11:33:55 AM	Sysmon	7 Image loaded (rule: ImageLoad)
> StorageSettings	Information	12/8/2023 11:33:55 AM	Sysmon	7 Image loaded (rule: ImageLoad)
> StorageSpaces-Api	Information	12/8/2023 11:33:55 AM	Sysmon	7 Image loaded (rule: ImageLoad)
> StorageSpaces-Driver	Information	12/8/2023 11:33:55 AM	Sysmon	7 Image loaded (rule: ImageLoad)
> StorageSpaces-ManagementAgent	Information	12/8/2023 11:33:55 AM	Sysmon	7 Image loaded (rule: ImageLoad)
> StorageSpaces-Parser	Information	12/8/2023 11:33:55 AM	Sysmon	7 Image loaded (rule: ImageLoad)
> StorageSpaces-SpaceManager	Information	12/8/2023 11:33:55 AM	Sysmon	7 Image loaded (rule: ImageLoad)
> StorDiag	Information	12/8/2023 11:33:55 AM	Sysmon	7 Image loaded (rule: ImageLoad)
> Store	Information	12/8/2023 11:33:55 AM	Sysmon	7 Image loaded (rule: ImageLoad)
> StorPort	Information	12/8/2023 11:33:55 AM	Sysmon	7 Image loaded (rule: ImageLoad)

Event 11, Sysmon

General Details

File created:
RuleName: technique_id=T1047,technique_name=File System Permissions Weakness
UtcTime: 2023-12-08 19:33:55.911
ProcessGuid: {44ecf37-6fa3-6573-3d26-000000000700}
ProcessId: 2996
Image: C:\Windows\System32\cmd.exe
TargetFilename: C:\temp\cmdfile.txt
CreationUtcTime: 2023-12-08 19:33:55.911
User: NT AUTHORITY\SYSTEM

Telemetry – DNS Query

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

The screenshot shows the Windows Event Viewer interface. On the left, a navigation pane lists various Windows services and components. The main pane displays two separate log entries.

Event 3006, DNS Client Events (Microsoft-Windows-DNS-Client)

Time	Type	Source	Message
12/8/2023 11:33:55 AM	Information	DNS Client Events (Microsoft-Windows-DNS-Client)	DNS Client Events (Microsoft-Windows-DNS-Client) 3008 None
12/8/2023 11:33:55 AM	Information	DNS Client Events (Microsoft-Windows-DNS-Client)	DNS Client Events (Microsoft-Windows-DNS-Client) 3006 None
12/8/2023 11:32:26 AM	Information	DNS Client Events (Microsoft-Windows-DNS-Client)	DNS Client Events (Microsoft-Windows-DNS-Client) 3008 None
12/8/2023 11:32:26 AM	Information	DNS Client Events (Microsoft-Windows-DNS-Client)	DNS Client Events (Microsoft-Windows-DNS-Client) 3018 None

Event 22, Sysmon

Time	Type	Source	Message
12/8/2023 12:29:07 PM	Information	Sysmon	13 Registry value set (rule: Registry)
12/8/2023 12:28:36 PM	Information	Sysmon	22 Dns query (rule: DnsQuery)
12/8/2023 12:28:34 PM	Information	Sysmon	13 Registry value set (rule: Registry)
12/8/2023 12:28:33 PM	Information	Sysmon	1 Process Create (rule: ProcessCr.)
12/8/2023 12:28:33 PM	Information	Sysmon	13 Registry value set (rule: Registry)

Event Details:

```
Dns query:  
RuleName: -  
UtcTime: 2023-12-08 20:28:34.119  
ProcessGuid: {00000000-0000-0000-0000-000000000000}  
ProcessId: 7808  
QueryName: adversaryvillage.org  
QueryStatus: 0  
QueryResults: ::ffff:185.199.109.153;::ffff:185.199.110.153;::ffff:185.199.111.153;::ffff:185.199.108.153;  
Image: <unknown process>  
User: WINSRV01\Administrator
```

- 4
5
6
7
8
9
- Not Implemented
 - Partially Implemented
 - ? Pending Response
 - Via Windows EventLogs (EDR is inspecting windows event logs to collect the telemetry)
 - Via EnablingTelemetry (Additional telemetry that can be enabled easily as part of the EDR product but is not ON by default.)

Telemetry – Others

○ EDR Telemetry

Device Operations

○ Object access (4662)

Other Relevant Events

○ NGFW, IDS on DNS query (network)

Named Pipe Activity

○ 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%

Tele	Event	Feature	Category	Sub-Cat	Carbon Black	CrowdStrike	Cybereason	ESET Inspect	Elastic	LimaCharlie	MDE
43	Service Deletion				■	■	■	■	■	?	■
44	Driver Loaded				■	■	■	■	■	■	■
45	Driver/Module Activity	Driver Modification			■	■	■	■	■	■	■
46	Driver Unloaded				■	■	■	■	■	■	■
47	Virtual Disk Mount				■	■	■	■	■	■	■
48	USB Device Unmount				■	■	■	■	■	■	■
49	Mount				■	■	■	■	■	■	■
50	Group Policy Modification				■	■	■	■	■	■	■
51	Pipe Creation				■	■	■	■	■	■	■
52	Pipe Completion				■	■	■	■	■	■	■
53	Agent Start				■	■	■	■	■	■	■
54	Agent Stop				■	■	■	■	■	■	■
55	Agent Installed				■	■	■	■	■	■	■
56					■	■	■	■	■	■	■
57					■	■	■	■	■	■	■
58					■	■	■	■	■	■	■
59					■	■	■	■	■	■	■
60					■	■	■	■	■	■	■
61					■	■	■	■	■	■	■
62					■	■	■	■	■	■	■
63					■	■	■	■	■	■	■
64					■	■	■	■	■	■	■

WMI – Detection

AKA Don't reinvent the wheel

Detection – Sigma

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

The screenshot shows a web-based search interface for Sigma detection rules. At the top, there is a search bar containing the query 'set-wmi'. Below the search bar are three buttons: 'Submit', 'How to', and 'Show Fields'. The main area displays a table of search results with the following columns: Author, ID, Title, Description, Score, and Link.

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

```
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

```
1  title: WMI Event Subscription
2  id: 0f06a3a5-6a09-413f-8743-e6cf35561297
3  status: test
4  description: Detects creation of WMI event subscription persistence method
5  author: Tom Ueltschi (@c_APT_ure)
6  date: 2019/01/12
7  modified: 2021/11/27
8  tags:
9    - attack.persistence
10   - attack.t1546.003
11  logsource:
12    product: windows
13    category: wmi_event
14  detection:
15    selection:
16      EventID:
17        - 19
18        - 20
19        - 21
20    condition: selection
21  falsepositives:
22    - Exclude legitimate (vetted) use of WMI event subscription in your network
23  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

```
1  title: Powershell WMI Persistence
2  id: 9e07f6e7-83aa-45c6-998e-0af26efd0a85
3  status: test
4  description: Adversaries may establish persistence and elevate privileges by executing malicious content triggered by a Windows Management Instrumentation (WMI) event subscription.
5  references:
6      - https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1546.003/T1546.003.md
7      - https://github.com/EmpireProject/Empire/blob/08cbd274bef78243d7a8ed6443b8364acd1fc48b/data/module_source/persistence/Persistence.psm1#L545
8  author: frack113
9  date: 2021/08/19
10 modified: 2022/12/25
11 tags:
12     - attack.privilege_escalation
13     - attack.t1546.003
14 logsource:
15     product: windows
16     category: ps_script
17     definition: 'Requirements: Script Block Logging must be enabled'
18 detection:
19     selection_ioc:
20         - ScriptBlockText|contains|all:
21             - 'New-CimInstance '
22             - '-Namespace root/subscription '
23             - '-ClassName __EventFilter '
24             - '-Property ' # is a variable name
25         - ScriptBlockText|contains|all:
26             - 'New-CimInstance '
27             - '-Namespace root/subscription '
28             - '-ClassName CommandLineEventConsumer '
29             - '-Property ' # is a variable name
30     condition: selection_ioc
31 falsepositives:
32     - Unknown
33 level: medium
```

Detection – MITRE CAR

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

T1546: Event Triggered Execution	T1546.001: Change Default File Association T1546.003: Windows Management Instrumentation Event Subscription	CAR-2013-01-002: Autorun Differences
		<ul style="list-style-type: none">• 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.

A screenshot of a file browser interface titled "detection-rules / rules / windows /". The list contains 24 entries, each with a small icon and a file name:

- command_and_control_ingress_transfer_bits.toml
- command_and_control_new_terms_commonly_abused_rat_execution.toml
- command_and_control_port_forwarding_added_registry.toml
- command_and_control_rdp_tunnel_plink.toml
- command_and_control_remote_file_copy_desktopimgdownldr.toml
- command_and_control_remote_file_copy_mpcmdrun.toml
- command_and_control_remote_file_copy_powershell.toml
- command_and_control_remote_file_copy_scripts.toml
- command_and_control_sunburst_c2_activity_detected.toml
- command_and_control_teamviewer_remote_file_copy.toml
- credential_access_bruteforce_admin_account.toml
- credential_access_bruteforce_multiple_logon_failure_followed_by_success.toml
- credential_access_bruteforce_multiple_logon_failure_same_srcip.toml
- credential_access_cmdline_dump_tool.toml
- credential_access_copy_ntds_sam_volshadowcp_cmdline.toml
- credential_access_credential_dumping_msbuild.toml

A screenshot of the Splunk Security Content detections page. The top navigation bar includes links for Detections, Analytic Stories, Playbooks, Blog, and About, along with a search icon.

The main content area is titled "Detections" and displays a table of 15 detected incidents. Each row includes the Name, Technique, and Type of the detection.

Name	Technique	Type
3CX Supply Chain Attack Network Indicators	Compromise Software Supply Chain	TTP
Zip CommandLine To SMB Share Path	Archive via Utility, Archive Collected Data	Hunting
ASL AWS Concurrent Sessions From Different Ips	Browser Session Hijacking	Anomaly
ASL AWS CreateAccessKey	Valid Accounts	Hunting
ASL AWS Defense Evasion Delete CloudWatch Log Group	Impair Defenses, Disable or Modify Cloud Logs	TTP
ASL AWS Defense Evasion Delete Cloudtrail	Disable or Modify Cloud Logs, Impair Defenses	TTP
ASL AWS Defense Evasion Impair Security Services	Disable or Modify Cloud Logs, Impair Defenses	Hunting
ASL AWS Excessive Security Scanning	Cloud Service Discovery	Anomaly
ASL AWS IAM Delete Policy	Account Manipulation	Hunting
ASL AWS Multi-Factor Authentication Disabled	Compromise Accounts, Cloud Accounts, Multi-Factor Authentication Request Generation, Modify Authentication Process, Multi-Factor Authentication	TTP
ASL AWS New MFA Method Registered For User	Modify Authentication Process, Multi-Factor Authentication	TTP

Detection – Translation

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

sigconverter.io
sigma rule converter

Backend: splunk Format: default Pipeline: select pipelines...

CLI:
sigma convert --without-pipeline -t splunk -f default rule.yml

rule.yml pipeline.yml

```
title: Suspicious SYSTEM User Process Creation
id: 2617e7ed-adb7-40ba-0ff3-8f9945fe6c09
status: test
description: Detects a suspicious process creation as SYSTEM user (suspicious program or command line references)
references:
- Internal Research
- https://tools.thehacker.recipes/mimikatz/modules
author: Florian Roth (rule), David ANDRE (additional keywords)
date: 2021/12/20
modified: 2022/04/27
logsource:
category: process_creation
product: windows
detection:
selection:
IntegrityLevel: System
User|contains: # covers many language settings
- 'AUTHORI'
- 'AUTORI'
```

query

```
IntegrityLevel="System" User IN ("*AUTHORI*", "*AUTORI*") Image IN ("*\calc.exe",
"\wscript.exe", "*\cscript.exe", "*\hh.exe", "*\mshta.exe", "*\forfiles.exe",
"\ping.exe") OR CommandLine IN ("* -NoI", "* -W Hidden", "* -decode", "* /decode", "* /urlcache",
"-e* JAB*", "* -e* SUVYI*", "* -e* SQBFAGA*", "* -e* aWV4I",
"-e* IAB*", "* -e* PAA*", "* -e* aQ81AigA*", "*vssadmin delete shadows", "*reg SAVE HKLM",
"-ma", "*Microsoft\Windows\CurrentVersion\Run", ".downloadstring()", ".downloadfile()", "/ticket",
"dpapi:::", "event::clear", "event::drop", "id::modify", "Kerberos::",
"lsadump::", "misc::", "privilege::", "rpc::", "sekurlsa::", "sid::", "token::",
"vault::cred", "vault::list", "p::d", ";iex(", "MiniDump", "net user ")
```

Detection – Bonus: Velociraptor Hunt

The screenshot shows the Velociraptor interface with two main windows.

Hunt Configuration: The top window displays a list of hunts. One hunt is selected: "H.CLQAFI0B1R3FE" (WMI Persistence Hunt) created by "sam" on 2023-12-09T17:45:44Z, which is currently connected to "winsrv01.fungku.lab".

Flow Details: A modal window titled "Flow Details" is open, showing the configuration for the selected hunt. It includes tabs for "Artifact Collection", "Uploaded Files", "Results" (which is selected), and "Log".

ConsumerDetails: This section contains the configuration for the consumer. It includes fields like "Name": "NotepadStartFilter", "Query": "SELECT * FROM __InstanceCreationEvent WITHIN 5 WHERE TargetInstance ISA 'Win32_Process' AND TargetIn...", and "Namespace": "root\subscription".

FilterDetails: This section contains the WQL filter configuration. The query is defined as:

```
SELECT * FROM __InstanceCreationEvent WITHIN 5 WHERE TargetInstance ISA 'Win32_Process' AND TargetIn...
```

Code Preview: On the left side of the interface, there is a code editor showing a snippet of WQL or similar script. The code includes logic for handling namespaces and querying WMI events.

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