



PURPLE
PROTOCOL
LAB MANUAL

Lab 1

Threat Intelligence

The first step to emulating an adversary is to identify and understand that adversary. As famously quoted in Sun Tzu's Art of War "If you know the enemy and know yourself, you need not fear the result of a hundred battles." This lab covers the "Know the enemy" part.

In this lab, we will dive into understanding how to recognize and analyze the Tactics, Techniques, and Procedures (TTPs) used by Advanced Persistent Threats (APTs). As cyber threats become more sophisticated, it's essential for security professionals to not only detect attacks but also understand the methods adversaries use to infiltrate and navigate systems.

By the end of the lab, you should be able to do the following:

- Identify an Adversary relevant to your organization
- Recognize the Tactics Techniques and Procedures (TTPs) utilized by the adversary
- Utilize MITRE ATT&CK Navigator to map attack chains per APT



1) On your lab VM's desktop, double click the MITRE ATT&CK® Icon

MITRE | ATT&CK®

Matrices ▾ Tactics ▾ Techniques ▾ Defenses ▾ CTI ▾ Search Q

This is a custom instance of the ATT&CK Website built from source code published by ATT&CK on GitHub. It is not affiliated with ATT&CK in any official capacity. The official instance of the ATT&CK website can be found at attack.mitre.org.

ATT&CK Matrix for Enterprise

layout: side ▾ show sub-techniques hide sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	44 techniques	17 techniques	32 techniques	9 techniques	17 techniques	18 techniques	9 techniques	14 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (7)	Abuse Elevation Control Mechanism (8)	Abuse Elevation Control Mechanism (8)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (4)	Application Layer Protocol (3)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (11)	BITS Jobs	Access Token Manipulation (3)	Access Token Manipulation (3)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (2)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction (1)
Gather Victim Identity Information (2)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Services	Boot or Logon Autostart Execution (14)	Account Manipulation (7)	Account Manipulation (7)	Credentials from Password Stores (4)	Browser Information Discovery	Automated Collection	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (4)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (3)	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	Build Image on Host	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Content Injection	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (3)	Boot or Logon Initialization Scripts (3)	Debugger Evasion	Cloud Service Dashboard	Remote Services (3)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Host Software Binary	Create or Modify System Process (3)	Create or Modify System Process (3)	Deobfuscate/Decode Files or Information	Cloud Storage Object Discovery	Replication Through Removable Media	Data from Cloud Storage	Data Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Native API	Create Account (3)	Domain or Tenant Policy Modification (2)	Domain or Tenant Policy Modification (2)	Deploy Container	Cloud Service Discovery	Software Deployment Tools	Data from Configuration Repositories (3)	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Financial Theft
Search Open Technical Databases (3)	Stage Capabilities (8)	Supply Chain Compromise (3)	Scheduled Task/Job (3)	Event Triggered Execution (17)	Exploitation for Defense Evasion	Exploitation for Defense Evasion	Direct Volume Access	Debugger Evasion	Taint Shared Content	Data from Information Repositories (3)	Encrypted Channels	Exfiltration Over Web Service (4)	Firmware Corruption
Search Open Websites/Domains (3)	Trusted Relationship	Valid Accounts (4)	Serverless Execution	Shared Modules	Escape to Host	Escape to Host	Execution Guardrails (2)	Device Driver Discovery	Use Alternate Authentication Material (4)	Data from Local System	Failback Channels	Inhibit System Recovery	Network Denial of Service (2)
Search Victim-Owned Websites			Software Deployment Tools	System Services (2)	Event Triggered Execution (17)	Event Triggered Execution (17)	File and Directory Permissions Modification (2)	Domain Trust Discovery		Data from Network Shared Drive	Ingress Tool Transfer	Scheduled Transfer	Resource Hijacking (4)
			User Execution (3)	Hijack Execution Flow (13)	Hijack Execution Flow (13)	Hijack Execution Flow (13)	Hide Artifacts (12)	File and Directory Discovery		Data from Removable Media	Multi-Stage Channels	Transfer Data to Cloud Account	Service Stop
			Windows Management Instrumentation	Implant Internal Image	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	Hijack Execution Flow (13)	Group Policy Discovery		Protocol Tunneling	Non-Application Layer Protocol		System Shutdown/Reboot
				Modify Authentication Process (9)	Process Injection (12)	Process Injection (12)	Impair Defenses (11)	Log Enumeration		Proxy (4)	Remote Access Software		
				Office Application Startup (8)	Scheduled Task/Job (3)	Scheduled Task/Job (3)	Indicator Removal (10)	Network Service Discovery		Email Collection (3)	Traffic Signaling (2)		
				Power Settings	Valid Accounts (4)	Valid Accounts (4)	Masquerading (10)	Network Share Discovery		Input Capture (4)	Web Service (2)		
				Pre-OS Boot (3)			Modify Authentication Process (9)	OS Credential Dumping (8)		Screen Capture			
				Scheduled Task/Job (3)			Modify Cloud Compute Infrastructure (3)	Steal Application Access Token		Video Capture			
				Server Software Component (3)			Modify Cloud Resource Hierarchy	Steal or Forge Authentication Request Certificates					
				Traffic Signaling (2)			Modify Registry	Steal or Forge Kerberos Tickets (5)					
				Valid Accounts (4)			Network Boundary Bridging (1)	Steal Web Session Cookie					
							Obfuscated Files or Information (14)	Unsecured Credentials (8)					
							Plist File Modification						
							Pre-OS Boot (3)						
							Process Injection (12)						
							Reflective Code Loading						
							Rogue Domain Controller						
							Rootkit						
							Subvert Trust Controls (4)						
							System Binary Proxy Execution (14)						
							System Script Proxy Execution (2)						
							Template Injection						
							Traffic Signaling (2)						
							Trusted Developer Utilities Proxy						

2) Click "CTI > Groups"

MITRE | ATT&CK®

Matrices ▾ Tactics ▾ Techniques ▾ Defenses ▾ CTI ▾ Search Q

This is a custom instance of the MITRE ATT&CK Website. The official website can be found at attack.mitre.org

GROUPS ▾

- Groups
- Software
- Campaigns

Take a moment to scroll through this page. At the time of creating this workshop, MITRE had 163 APTs listed here with all of their associated groups alongside it. These groups are either the same group with the same name or a spin-off group that have very similar TTPs due to the actual hands-on-keyboard threat actors being some of the

same people. The description also may tell you what countries they typically target and/or what industries they are known to target. For example:

APT17 is a China-based threat group that has conducted network intrusions against U.S. government entities, the defense industry, law firms, information technology companies, mining companies, and non-government organizations.

The purpose of this Cyber Threat Intelligence (CTI) is to be able to identify adversaries that are known to attack organizations similar to your own, whether that is your company’s HQ location or industry. These are the threat actors most likely to attack your organization. Try to find an APT that is known to target your industry and organizations where your company is headquartered and take note of that APT for later.

3) Select G0007 (APT28).

G0007	APT28	IRON TWILIGHT, SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn	APT28 is a threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS) military unit 26165. This group has been active since at least 2004.
-------	-------	---	--

Scroll Down to see the "Techniques Used" for this threat actor.

Techniques Used				ATT&CK® Navigator Layers ▾
Domain	ID	Name	Use	

Here you can see all the techniques that APT28 has been known to use against other organizations.

MITRE has a great, open-source application called “MITRE ATT&CK Navigator” to help visualize the known TTPs of Threat Actors in their database.



4) On the desktop of your Lab VM, double click:

5) Click on Create New Layer > Enterprise ATT&CK:

MITRE ATT&CK® Navigator

The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more.

[help](#) [changelog](#) [theme](#)

Create New Layer

Create a new empty layer

Enterprise ATT&CK

Mobile ATT&CK

ICS ATT&CK

More Options

Open Existing Layer

Load a layer from your computer or a URL

Create Layer from Other Layers

Select layers to inherit properties from

Create Customized Navigator

Create a hyperlink to a customized ATT&CK Navigator

6) Click on the Magnifying Glass at the top right, scroll to “Threat Groups” and select “APT 28”:

layer x +

Selection Controls Layer Controls Technique Controls

Search

Search Settings
☐ name ☐ ATT&CK ID ☐ description ☐ data sources

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 44 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques
Active Scanning (0/3)	Acquire Access (0/8)	Content Injection (0/10)	Cloud Administration Command (0/14)	Account Manipulation (0/20)	Abuse Elevation Control Mechanism (0/14)	Abuse Elevation Control Mechanism (0/44)	Adversary-in-the-Middle (0/17)	Account Discovery (0/32)	Exploitation of Remote Services (0/9)	Adversary-in-the-Middle (0/17)	Application Layer Protocol (0/18)
Gather Victim Host Information (0/4)	Acquire Infrastructure (0/8)	Drive-by Compromise (0/10)	Command and Scripting Interpreter (0/14)	BITS Jobs (0/20)	Access Token Manipulation (0/14)	Access Token Manipulation (0/44)	Brute Force (0/17)	Application Window Discovery (0/32)	Internal Spearphishing (0/9)	Archived Collected Data (0/17)	Communications Through Removable Media (0/18)
Gather Victim Identity Information (0/3)	Compromise Accounts (0/8)	Exploit Public-Facing Application (0/10)	Container Administration Command (0/14)	Boot or Logon Initialization Scripts (0/20)	Access Token Manipulation (0/14)	Build Image on Host (0/44)	Credentials from Password Stores (0/17)	Browser Information Discovery (0/32)	Lateral Tool Transfer (0/9)	Audio Capture (0/17)	Content Injection (0/18)
Gather Victim Network Information (0/5)	Compromise Infrastructure (0/8)	External Remote Services (0/10)	Deploy Container (0/14)	Boot or Logon Initialization Scripts (0/20)	Account Manipulation (0/14)	Debugger Evasion (0/44)	Exploitation for Credential Access (0/17)	Cloud Infrastructure Discovery (0/32)	Remote Service Session Hijacking (0/9)	Automated Collection (0/17)	Data Encoding (0/18)
Gather Victim Org Information (0/4)	Develop Capabilities (0/8)	Hardware Additions (0/10)	Exploitation for Client Execution (0/14)	Browser Extensions (0/20)	Boot or Logon Initialization Scripts (0/14)	Deploy Container (0/44)	Forced Authentication (0/17)	Cloud Service Dashboard (0/32)	Remote Services (0/9)	Browser Session Hijacking (0/17)	Data Obfuscation (0/18)
Pushing for Information (0/4)	Establish Accounts (0/8)	Phishing (0/10)	Inter-Process Communication (0/14)	Compromise Host Software Binary (0/20)	Boot or Logon Initialization Scripts (0/14)	Direct Volume Access (0/44)	Forge Web Credentials (0/17)	Cloud Storage Object Discovery (0/32)	Replication Through Removable Media (0/9)	Clipboard Data (0/17)	Dynamic Resolution (0/18)
Search Closed Sources (0/2)	Obtain Capabilities (0/8)	Replication Through Removable Media (0/10)	Native API (0/14)	Create Account (0/20)	Boot or Logon Initialization Scripts (0/14)	Domain or Tenant Policy Modification (0/44)	Input Capture (0/17)	Container and Resource Discovery (0/32)	Software Deployment Tools (0/9)	Data from Cloud Storage (0/17)	Encrypted Channel (0/18)
Search Open Technical Databases (0/3)	Stage Capabilities (0/8)	Supply Chain Compromise (0/10)	Scheduled Task/Job (0/14)	Create or Modify System Process (0/20)	Create or Modify System Process (0/14)	Execution Guardrails (0/44)	Modify Authentication Process (0/17)	Debugger Evasion (0/32)	Taint Shared Content (0/9)	Data from Configuration Repository (0/17)	Fallback Channels (0/18)
Search Open Websites/Domains (0/3)	Trusted Relationship (0/8)	Serverless Execution (0/10)	Shared Modules (0/14)	Event Triggered Execution (0/20)	Domain or Tenant Policy Modification (0/14)	File and Directory Permissions Modification (0/44)	Multi-Factor Authentication Interception (0/17)	Device Driver Discovery (0/32)	Use Alternate Authentication Material (0/9)	Data from Information Repositories (0/17)	Ingress Tool Transfer (0/18)
Search Victim-Owned Websites (0/4)	Valid Accounts (0/8)	Software Deployment Tools (0/10)	External Remote Services (0/14)	Escape to Host (0/20)	Hide Artifacts (0/14)	Hijack Execution Flow (0/44)	Multi-Factor Authentication Request Generation (0/17)	File and Directory Discovery (0/32)	Group Policy Discovery (0/9)	Data from Local System (0/17)	Multi-Stage Channels (0/18)
	System Services (0/8)	Hijack Execution Flow (0/10)	Event Triggered Execution (0/14)	Impair Defenses (0/20)	Impersonation (0/14)	Indicator Removal (0/44)	OS Credential Dumping (0/17)	Log Enumeration (0/32)	Network Service Discovery (0/9)	Data from Network Shared Drive (0/17)	Non-Application Layer Protocol (0/18)
	User Execution (0/8)	Implant Internal Image (0/10)	Exploitation for Privilege Escalation (0/14)	Indirect Command Execution (0/20)	Masquerading (0/14)	Masquerading (0/44)	Steal Application Access Token (0/17)	Network Share Discovery (0/32)	Network Sniffing (0/9)	Data from Removable Media (0/17)	Non-Standard Port (0/18)
	Windows Management Instrumentation (0/8)	Modify Authentication Process (0/10)	Hijack Execution Flow (0/14)	Office Automation (0/20)	Office Automation (0/14)	Office Automation (0/44)	Steal or Forge Authentication Credentials (0/17)	Password Policy Discovery (0/32)	Proxy (0/9)	Data Staged (0/17)	Protocol Tunneling (0/18)
										Email Collection (0/17)	Remote Access Software (0/18)

Techniques (556)

select all deselect all

Abuse Elevation Control Mechanism [view](#) [select](#) [deselect](#)

Abuse Elevation Control Mechanism : Bypass User Account Control [view](#) [select](#) [deselect](#)

Abuse Elevation Control Mechanism : Elevated Execution [view](#) [select](#) [deselect](#)

Threat Groups (160)

select all deselect all

APT17 [view](#) [select](#) [deselect](#)

APT18 [view](#) [select](#) [deselect](#)

APT19 [view](#) [select](#) [deselect](#)

APT28 [view](#) [select](#) [deselect](#)

APT29 [view](#) [select](#) [deselect](#)

7) Under “Layer Controls” select “Expand Subtechniques”:

The screenshot shows the MITRE ATT&CK framework interface. The 'Layer Controls' tab is selected, and the 'Expand Subtechniques' button is highlighted. The interface displays a grid of techniques categorized by layer (e.g., Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control). The right sidebar shows search settings and a list of techniques.

Layer	Techniques
Defense Evasion	44 techniques
Credential Access	17 techniques
Discovery	32 techniques
Lateral Movement	9 techniques
Collection	17 techniques
Command and Control	18 techniques


8) Click on “Technique Controls” > Background Color > Red (because red means bad)

The screenshot shows the MITRE ATT&CK framework interface. The 'Technique Controls' tab is selected, and the 'Background Color' dropdown menu is open, showing the 'Red' color selected. The interface displays a grid of techniques categorized by layer (e.g., Execution, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control). The right sidebar shows search settings and a list of techniques.

Layer	Techniques
Execution	14 techniques
Defense Evasion	44 techniques
Credential Access	17 techniques
Discovery	32 techniques
Lateral Movement	9 techniques
Collection	17 techniques
Command and Control	18 techniques

[illegible]

- Industry
 - Finance
 - Critical Infrastructure
 - Healthcare
 - Government
 - Etc.
- Country or Region
 - USA based organization
 - Foreign based organization
 - Which countries are considered an adversary of the country the organization is based?



The screenshot shows the Metasploit console with a session named 'layer1' and a red box highlighting a '+' icon, indicating the addition of a new session.

Note any overlaps in Techniques used as well as any differences. These Tactics Techniques and Procedures (TTPs) are what we emulate in order to understand what our adversary is likely to do when attacking our organization. By understanding these TTPs we can emulate them in order to test our defenses and understand where our visibility gaps are. TTPs are interesting. As you mature as a hacker, you slowly develop what is often referred to as a “Methodology”. These are the steps you take when enumerating machines you are testing, the tools you become comfortable with and gravitate to, the path you take to dump credentials or laterally move, etc. You will develop a “fingerprint” of your own in the same way any Threat Actor does. That is essentially what TTPs are, the fingerprint of a Threat Actor. This is typically how Threat Actors are identified and categorized post breach.

Lab 2

Atomic Red Team Framework

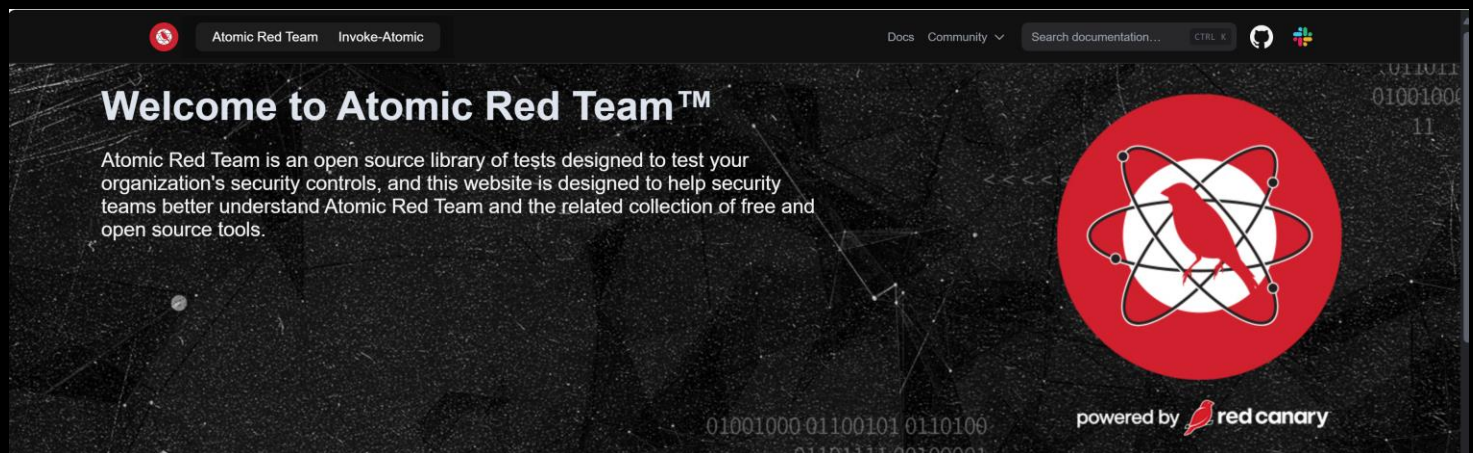
This lab will go over Red Canary's Atomic Red Team Framework. Atomic Red Team is a library of techniques, scripts, and test case execution automation, all mapped to MITRE ATT&CK's Technique Numbers. These tests built for each Technique are referred to as "atomics". This makes it easy to cross reference MITRE ATT&CK CTI Threat Actors and their Techniques to Atomic Red Team's Atomics.

By the end of this lab you should be able to do the following:

- Navigate Atomic Red Team's Library of atomics
- Cross Reference a MITRE ATT&CK Technique Number with the Atomic Red Team's atomic
- Execute test cases based on atomics

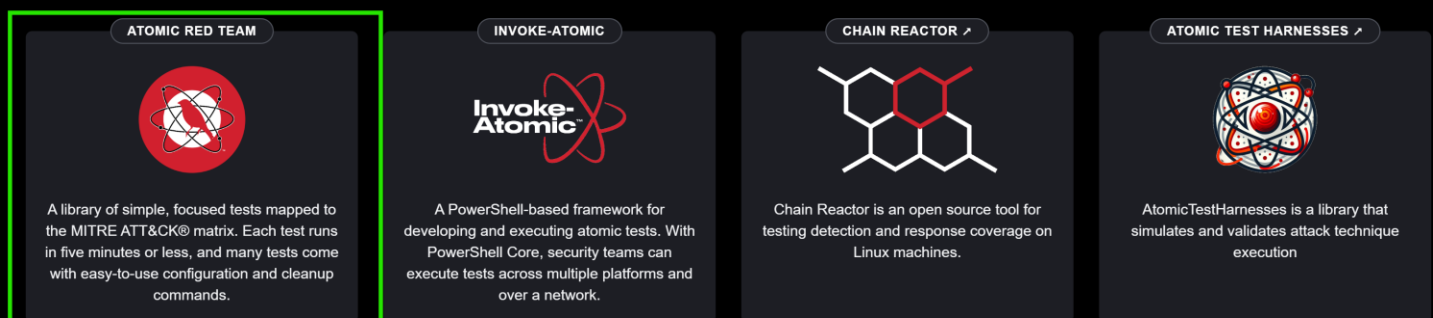
If network connectivity allows start at "1)", otherwise skip to "2)"

1) Navigate to <https://AtomicRedTeam.io/>



Scroll to "Projects" and click on "ATOMIC RED TEAM"

Projects



This is the library of Techniques, Test Cases for the Techniques, and how to execute them. Red Canary labels these tests as "Atomics". There are often many Atomics per technique and sub-technique allowing for a wide variety of ways to test any given technique or situation. You can search for the MITRE ATT&CK Technique number in the search bar to find a specific Atomic matching that technique.

Atomic Red Team

[Get started](#)
[View all atomics](#)

Atomic Red Team is an open source library of tests that security teams can use to simulate adversarial activity in their environments.



Fast

Atomic tests run in five minutes or less and require minimal setup. Spend less time configuring and more time testing!



Focused

Security teams don't want to operate with a "hopes and prayers" attitude towards detection. Atomic tests are mapped to the MITRE ATT&CK matrix, so you always know which techniques you do and don't detect.



Community-driven

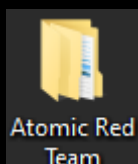
Atomic Red Team is open source and community developed. By working together, we can develop a fuller picture of the security landscape.

1720

Tactic Platforms Executors Elevation

ID	GUID	Name	Tactic	Platform(s)	Executor	Elevation	
T1001.002	c7921449-8b62-4c4d-8a83-d9281ac0190b	Steganographic Tarball Embedding	command-and-control	Windows	Powercat	None	</>
T1001.002	04bb8e3d-1670-46ab-a3f1-5cee64da29b6	Embedded Script in Image Execution via Extract-Invoke-PSImage	command-and-control	Windows	Powercat	None	</>
T1001.002	4ff61684-ad91-405c-9fbc-048354ff1d07	Execute Embedded Script in Image via Steganography	command-and-control	Linux	Powercat	None	</>
T1003	96345bfc-8ae7-4b6a-80b7-223200f24ef9	Gsecdump	credential-access	Windows	Gsecdump	System	</>

2) Due to past experiences with network connectivity issues at DEF CON during workshops, we decided to locally import all of the test cases from the Atomic Red Team framework onto the VM directly to mitigate any potential network issues getting in the way of the workshop.



3) On the Desktop of your VM you should see an icon: **Atomic Red Team** Double click this icon to open the folder.

Inside of this are all the Atomics stored locally inside of the VM. We will demonstrate how to utilize these Atomics in this lab.

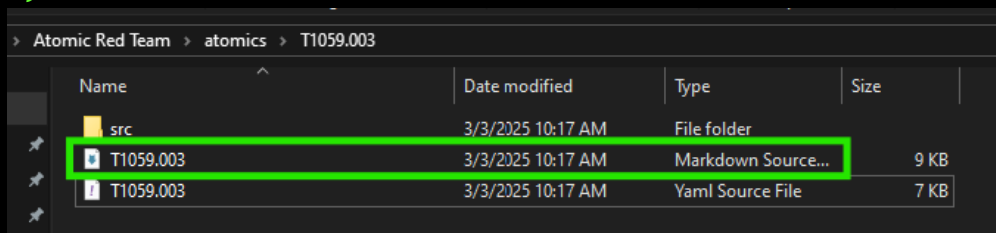
4) Scroll to T1059.003 and double click to open:

ard
Organize
New
Open

Atomic Red Team > atomics >

Name	Date modified	Type	Size
T1059.002	3/3/2025 10:17 AM	File folder	
T1059.003	3/3/2025 10:17 AM	File folder	
T1059.004	3/3/2025 10:17 AM	File folder	
T1059.005	3/3/2025 10:17 AM	File folder	
T1059.006	3/3/2025 10:17 AM	File folder	

5) Double click on the Markdown Source File:



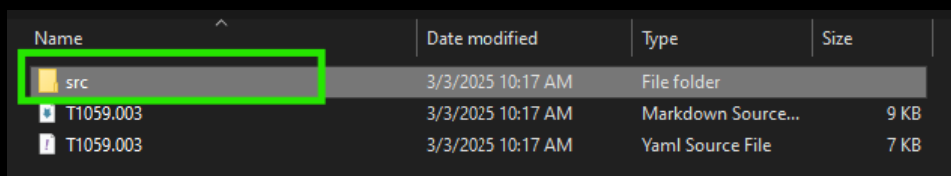
Name	Date modified	Type	Size
src	3/3/2025 10:17 AM	File folder	
T1059.003	3/3/2025 10:17 AM	Markdown Source...	9 KB
T1059.003	3/3/2025 10:17 AM	Yaml Source File	7 KB

Here you will see Atomic Red Team's explanation of the technique. In this case, it is "Command and Scripting Interpreter: Windows Command Shell"

```
C: > Users > hacker > Desktop > Atomic Red Team > atomics > T1059.003 > T1059.003.md > T1059.003 - Command and Scripting Interpreter: Windows Command Shell > ## Atomic Test #5 - Command Prompt read contents from CMD
1 # T1059.003 - Command and Scripting Interpreter: Windows Command Shell
205 ## Atomic Test #5 - Command Prompt read contents from CMD file and execute
206 Simulate Raspberry Robin using the "standard-in" command prompt feature cmd `/R <` to read and execute a file via cmd.exe
207 See https://redcanary.com/blog/raspberry-robin/.
208
209 **Supported Platforms:** Windows
210
211
212 **auto_generated_guid:** df81db1b-066c-4802-9bc8-b6d030c3ba8e
213
214
215
216
217
218 #### Inputs:
219 | Name | Description | Type | Default Value |
220 |-----|-----|-----|-----|
221 | input_file | CMD file that is read by Command Prompt and execute, which launches calc.exe | path | PathToAtomicsFolder&#92;T1059.003&#92;src&#92;t1059.003_cmd.cmd|
222
223
224 #### Attack Commands: Run with `command_prompt`! |
225
226
227 ```cmd
228 cmd /r cmd<"{input_file}"
229 ```
230
231
232
233
234 #### Dependencies: Run with `powershell`!
235 ##### Description: CMD file must exist on disk at specified location ({input_file})
236 ##### Check Prereq Commands:
237 ```powershell
238 if (Test-Path "{input_file}") {exit 0} else {exit 1}
239 ```
240 ##### Get Prereq Commands:
241 ```powershell
242 New-Item -Type Directory (split-path "{input_file}") -ErrorAction ignore | Out-Null
243 Invoke-WebRequest "https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/T1059.003/src/t1059.003_cmd.cmd" -OutFile "{input_file}"
244 ```
245
```

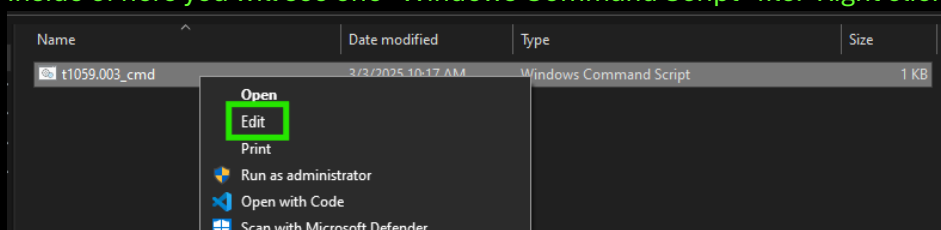
Atomic Red Team has features that allow for automation of test case execution. We will not be going over the automation portion of Atomic Red Team in this workshop, we will be executing test cases manually.

6) Back inside the previous T1059.003 folder, open the SRC folder:



Name	Date modified	Type	Size
src	3/3/2025 10:17 AM	File folder	
T1059.003	3/3/2025 10:17 AM	Markdown Source...	9 KB
T1059.003	3/3/2025 10:17 AM	Yaml Source File	7 KB

Inside of here you will see one "Windows Command Script" file. Right click and edit this file:



Name	Date modified	Type	Size
t1059.003_cmd	3/3/2025 10:17 AM	Windows Command Script	1 KB

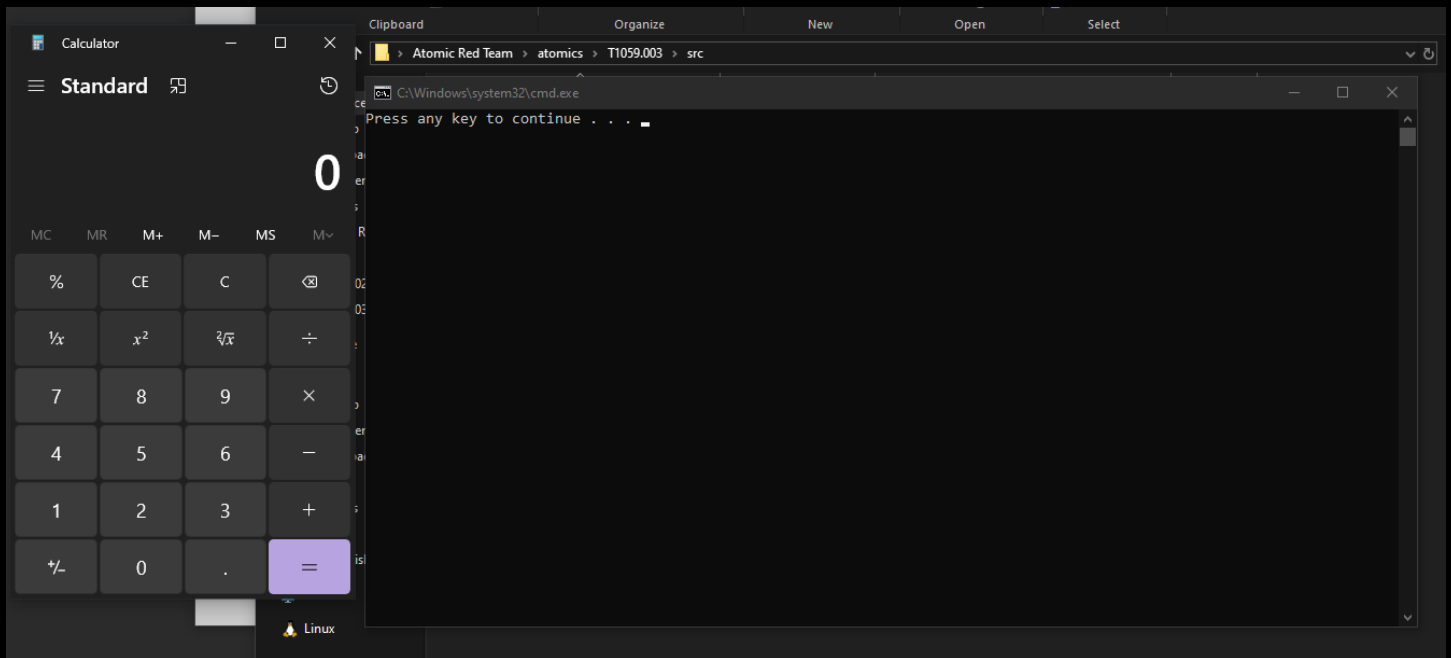
- Open
- Edit
- Print
- Run as administrator
- Open with Code
- Scan with Microsoft Defender...

This is a very basic script. This is essentially just a script that calls command prompt to execute a binary “calc.exe”. While calc.exe is not malicious, the behavior of executing a binary in this roundabout way is suspicious and Threat Actors have been known to do this during their attack chains. Malicious executables can be built in a few minutes that can bypass AV/EDR (ask me how I know). Therefore, we want to detect this type of suspicious behavior as opposed to the executable itself.

7) Open Powershell and copy/paste the following command into PowerShell:

```
Start-Process "C:\Users\hacker\Desktop\Atomic Red Team\atomics\T1059.003\src\t1059.003_cmd.cmd"
```

Command prompt should have opened and then executed the command to launch calc.exe from system32:



Now we will use another technique that is meant to dump the memory from Local Security Authority Subsystem Service (LSASS). My dumping the memory of the LSASS process, we can extract the cached passwords of users who have logged into the machine. This technique is specifically relating to the dump itself though so we won't go beyond that.

8) Open PowerShell as Admin

9) Use the following command to change directory to the Atomic folder:

```
cd 'C:\users\hacker\Desktop\Atomic Red Team\atomics\T1003.001\src'
```

10) Use the following command to bypass the execution policy for PowerShell:

```
Set-ExecutionPolicy bypass
```

11) When it asks if you want to change policy type “Y”

12) Run the following commands:

```
Import-Module .\Out-Minidump.ps1
```

```
get-process lsass
```

```
get-process lsass | Out-Minidump
```

If this works and is not blocked, it will create a file called lsass_[Id Number].dmp in the same folder as the Out-Minidump.ps1 file:

```
PS C:\Windows\system32> cd 'C:\users\hacker\Desktop\Atomic Red Team\atomics\T1003.001\src'
PS C:\users\hacker\Desktop\Atomic Red Team\atomics\T1003.001\src> Set-ExecutionPolicy bypass

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
https://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): y
PS C:\users\hacker\Desktop\Atomic Red Team\atomics\T1003.001\src> Import-Module .\Out-Minidump.ps1
PS C:\users\hacker\Desktop\Atomic Red Team\atomics\T1003.001\src> get-process lsass

Handles   NPM(K)    PM(K)      WS(K)      CPU(s)      Id  SI ProcessName
-----
1377      29      8396      20132       2.52      744  0 lsass

PS C:\users\hacker\Desktop\Atomic Red Team\atomics\T1003.001\src> get-process lsass | Out-Minidump



Directory: C:\users\hacker\Desktop\Atomic Red Team\atomics\T1003.001\src

Mode                LastWriteTime         Length Name
----                -
-a----            3/27/2025  10:37 AM         76205063 lsass_744.dmp

PS C:\users\hacker\Desktop\Atomic Red Team\atomics\T1003.001\src> get-process lsass | Out-Minidump

Directory: C:\users\hacker\Desktop\Atomic Red Team\atomics\T1003.001\src

Mode                LastWriteTime         Length Name
----                -
-a----            3/27/2025  10:45 AM         76359845 lsass_744.dmp
```

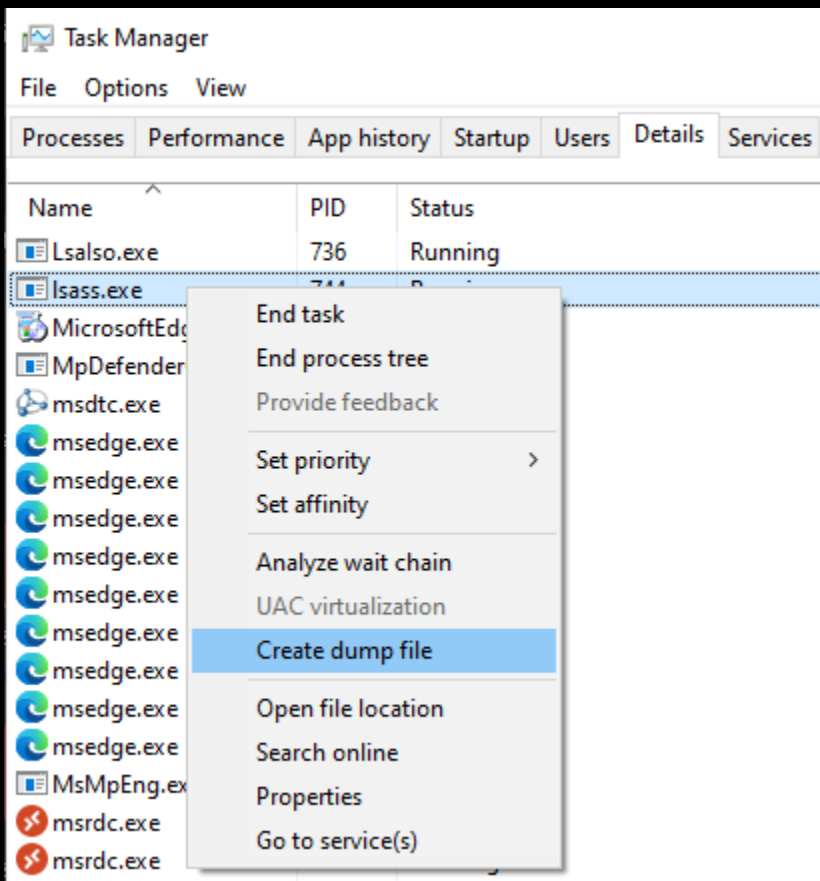
Name	Date modified	Type	Size
 lsass_744.dmp	3/27/2025 10:45 AM	DMP File	74,571 KB
 Out-Minidump.ps1	3/3/2025 10:17 AM	Windows PowerS...	4 KB

This .dmp file holds credential information because we took a snapshot of the portion of the memory that LSASS was using. Another way we can do the same thing is to dump it from Task Manager directly.

13) Open Task Manager

14) Navigate to the Details tab

15) Right click on LSASS and click “Create dump file”



This will effectively do the same thing, create a memory dump of LSASS that can be pulled off the machine and credentials stolen from the dump. The Windows Defender Antivirus may have triggered on either of these techniques.

For our next technique we'll be destroying evidence of our wrongdoing, but before we destroy the logs let's take a look at Event Viewer.

16) In the VM, either type “Event Viewer” in the start menu and open it, or press Windows+X then “V” (which is the 1337 way of opening event viewer)

17) Expand “Windows Logs”

Here you will see the 4 main categories of Windows Logs:

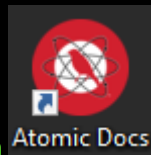
Application – Logs relating to applications like Microsoft Edge, Windows Management Instrumentation, .Net Runtime stuff, etc.

Security – Logs relating to authentication, file permissions, logons, etc.

Setup – Logs relating to installation, upgrades, and other OS related setup information

System – Logs related to Windows System Components, Drivers, and other critical Windows functions

Windows by default has most logs sent here. Your organization can customize other items to be sent here and may also send these logs to a centralized Security Information and Event Management server (SIEM). Incident Response and Threat Hunters may use logs like these to aid them in investigation. For this reason, Threat Actors often clear these to cover their tracks. This is suspicious behavior so we want to test to see if we have alerting set up for this situation.



18) On the desktop of the VM, open

19) Navigate to T1070.001:

T1070.001

src (7)

T1070.002

T1070.003

T1070.004

T1070.005

T1070.006

T1070.008

T1071

T1071.001

T1071.004

T1072

T1074.001

bin (1)

T1070.001 - Indicator Removal on Host: Clear Windows Event Logs

Description from ATT&CK

Adversaries may clear Windows Event Logs to hide the activity of an intrusion. Windows Event Logs are a record of a computer's alert Security, with five event types: Error, Warning, Information, Success Audit, and Failure Audit.

With administrator privileges, the event logs can be cleared with the following utility commands:

- `wevtutil cl system`
- `wevtutil cl application`
- `wevtutil cl security`

These logs may also be cleared through other mechanisms, such as the event viewer GUI or [PowerShell](#). For example, adversaries may clear the Security EventLog and after reboot, disable future logging. Note: events may still be generated and logged in the .evtx file between the time the logs are cleared and the system is rebooted.

Adversaries may also attempt to clear logs by directly deleting the stored log files within `C:\Windows\System32\winevt\logs\`.

Here you can see the explanation of how this technique is done:

With administrator privileges, the event logs can be cleared with the following utility commands:

- `wevtutil cl system`
- `wevtutil cl application`
- `wevtutil cl security`

20) Open Command Prompt as Administrator, and run these commands:

```
Administrator: Command Prompt

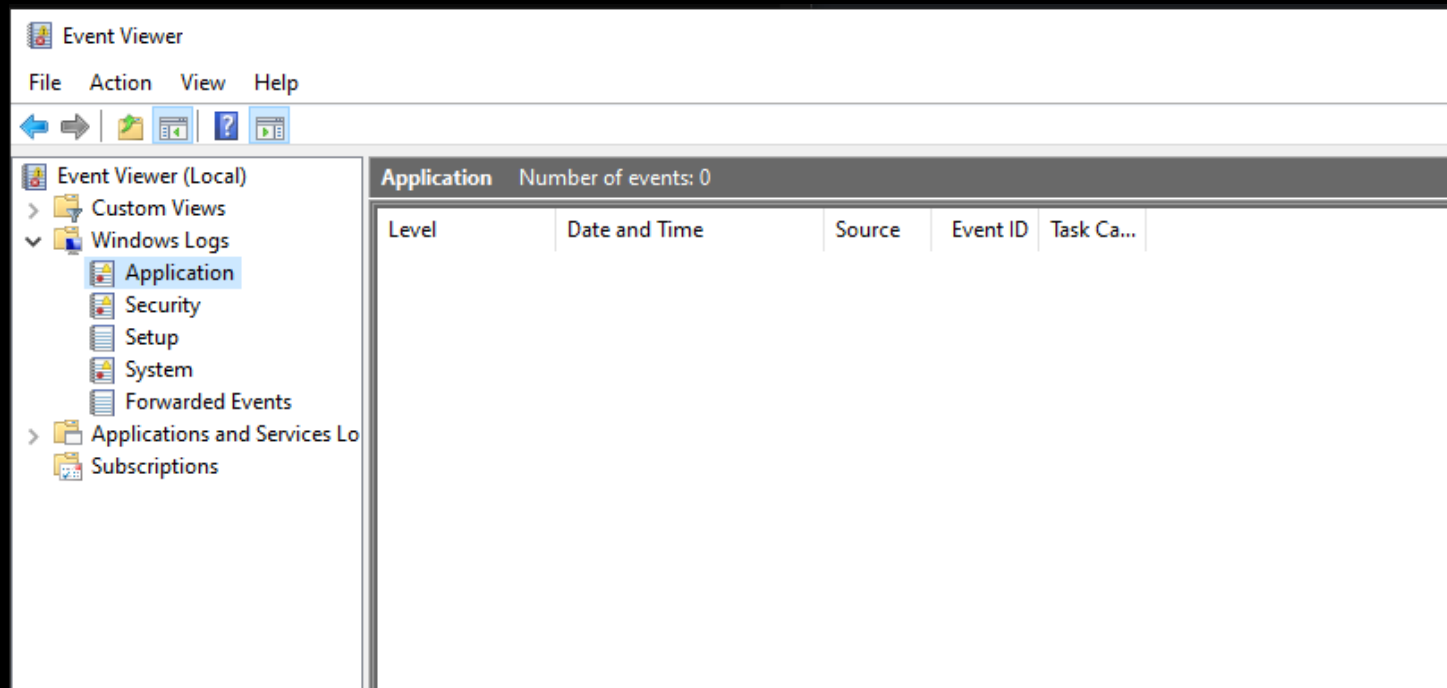
C:\Windows\system32>wevtutil cl system

C:\Windows\system32>wevtutil cl application

C:\Windows\system32>wevtutil cl security

C:\Windows\system32>
```

21) Open Event Viewer back up and navigate to Windows Logs. Click on Application, Security, and System to view the logs. You will see all of these have been cleared.



These are just three examples of common techniques that are executed by Threat Actors. As you can see, Red Canary's Atomic Red Team Framework spells out how to execute these Techniques in a way that is easy to follow. The Techniques we used in this lab are some of the easier ones to execute. These do get more complicated, but as you continue to do these, you will learn as you go and become more comfortable with the more complicated Techniques. As you execute future test cases, don't just copy and paste commands or execute pre-built binaries in Atomic Red Team. Open up scripts, read through them, do the necessary research to actually understand what is happening and how it works before you execute.

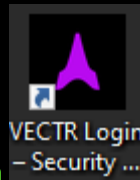
Lab 3

Purple Team Organization and Execution

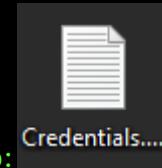
The other half of the equation is knowing your own organization's strengths and weaknesses during any phase of an adversary's chain of attacks. With this information you can understand where to prioritize remediation and fortification of defenses.

By the end of the lab, you should be able to do the following:

- Create a new Purple Team Assessment in Vectr
- Create a new Campaign within the Purple Team assessment
- Document test case results
- Generate reporting and trend metrics for stakeholders



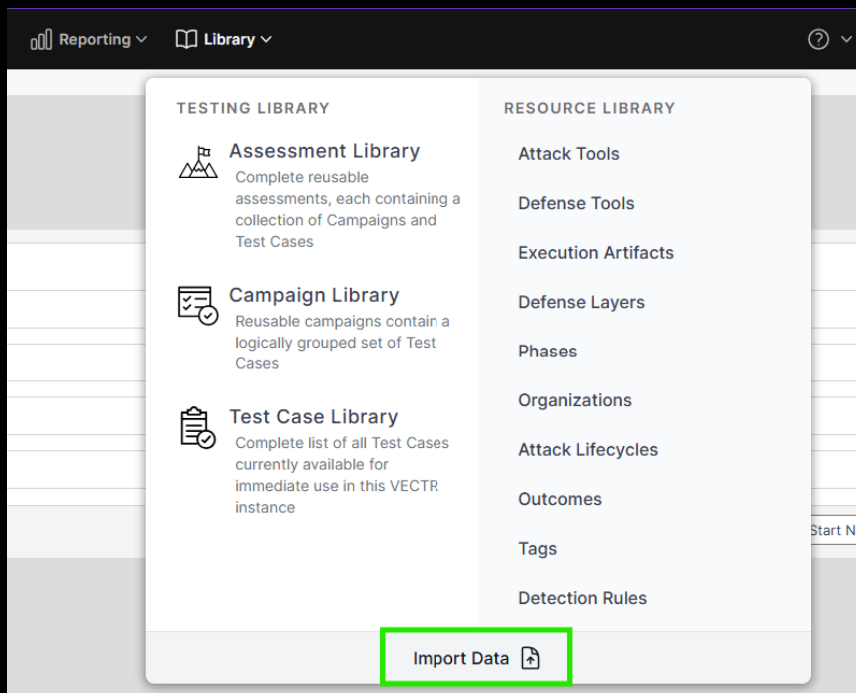
1) On the Desktop of your VM, click on



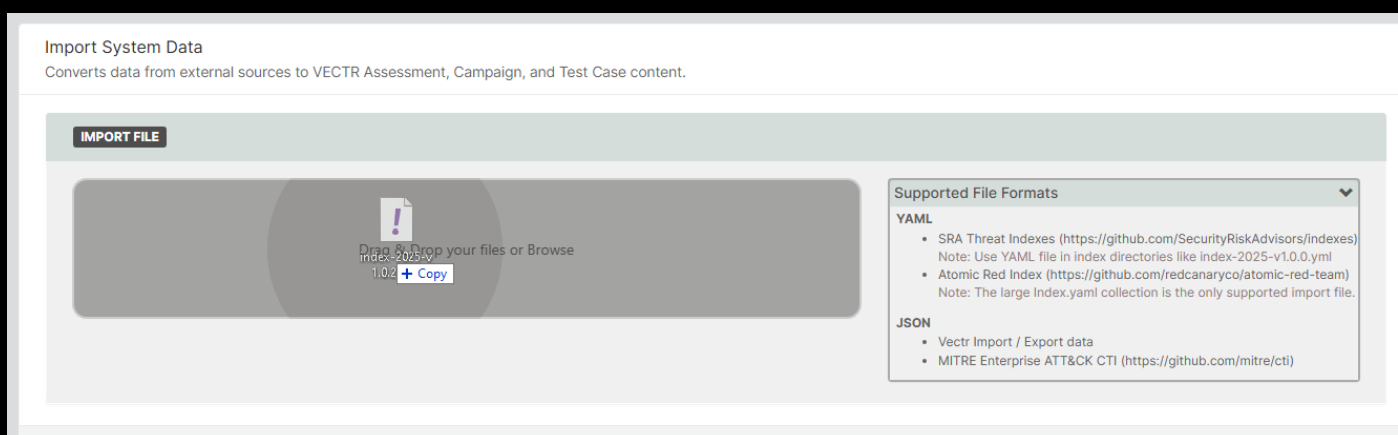
2) Log in using the credentials in the Credentials.txt file on the desktop:

It will ask for you to select an Active Environment. Select HEALTH_THREAT_INDEX.

3) Navigate to Library > Import Data



4) On the Desktop exists a file called index-2025-v1.0.2.yml, drag that file into the “import file” box



5) Click “Submit” on the bottom right

This .yml file is the newest Threat Simulation Index from Security Risk Advisors (SRA). This contains the most recent index (at the time of the Lab’s creation). These are the most common techniques used by 24 active Threat Actors. This index is curated by SRA and updated periodically.

3) At the top of the screen, Navigate to Testing > View All Assessments. On the bottom right of the Assessments screen, click “Start New Assessment”

ENVIRONMENT
HEALTH_THREAT_I...

Testing

Reporting

Library

ASSESSMENTS

2025 Q2: TSI - Threat Simulation I... >

Health Threat Index 2022 (Q1) >
Health Threat Simulation Index 2022 - January

Health Threat Index 2022 (Q2) >
Health Threat Simulation Index 2022 - April

Health Threat Index 2022 (Q3) >
Health Threat Simulation Index 2022 - July

Health Threat Index 2022 (Q4) >
Health Threat Simulation Index 2022 - October

+ Add an Assessment

View All Assessments

Health Threat Index 2022 (Q4)
Description: Health Threat Simulation Index 2022 - October

CAMPAIGNS

• Collection

• Command and Control

• Credential Access

• Defense Evasion

• Discovery

• Execution

• Exfiltration

+ Add a Campaign

View All Campaigns

Assessments

HEALTH INDEX

Name	Score	Status	
Health Threat Index 2022 (Q1)	34.62%	COMPLETED	...
Health Threat Index 2022 (Q2)	50.00%	COMPLETED	...
Health Threat Index 2022 (Q3)	61.54%	COMPLETED	...
Health Threat Index 2022 (Q4)	80.77%	COMPLETED	...

Metrics

Trending


+ Start New Assessment

4) Click on TSI – Threat Simulation Index 2025:


New Assessment

Get started quickly with a template curated by SRA, or [customize](#) from the ground up.


Security Risk Advisors Templates



Financial Services



Healthcare



Retail and Hospitality

Custom Templates

TSI - Threat Simulation Index 2025 v1.0....

5) Click on “Create” to create the assessment using this template:

New Custom Assessment

Name:

2025 Q2: TSI - Threat Simulation Index 2025 v1.0.2

Description:

Template:

Threat Simulation Index 2025 v1.0.2

X

▼

Exercise Date:

Apr 03, 2025

to

Apr 04, 2025

Advanced Options

⌵

Cancel

Create

6) Navigate to Reporting > MITRE ATT&CK Alignment:

The screenshot shows the Vectr interface with the 'Assessments' section. The 'HEALTH INDEX' is expanded, showing 'Health Threat Index 2022 (Q1)' through 'Q4'. The 'MITRE ATT&CK Alignment' report is highlighted in a green box. The 'Resilience Trending' chart is also visible. The 'Status' column shows 'COMPLETED' for all four quarters. The 'OTHER ASSESSMENTS' section shows '2025 Q2: TSI - Threat Simulation Index 2025 v1.0.2' with a status of 'NOT PERFORMED'.

7) Click on “Assessments” and check the box for 2025 Q2: TSI – Threat Simulation Index:

The screenshot shows the Vectr interface with the 'Assessments' section. The 'MITRE ATT&CK Alignment' report is highlighted in a green box. The '2025 Q2: TSI - Threat Simulation Index 2025 v1.0.2' assessment is checked in the 'OTHER ASSESSMENTS' section.

8) Click on the grey box for “No Test Coverage” to make it inactive:

The screenshot shows the MITRE ATT&CK Alignment report. The 'No Test Coverage' box is highlighted in a green box and labeled 'INACTIVE'. The report shows various attack techniques and their status.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
No Test Coverage INACTIVE	Phishing T1566 Valid Accounts T1078	Scheduled Task/Job T1053	Account Manipulation T1098	Account Manipulation T1098	Domain or Tenant Policy Modification T1484	Adversary-in-the-Middle T1557	Account Discovery T1087	Remote Services T1021	Adversary-in-the-Middle T1557	Application Layer Protocol T1071	Exfiltration Over Alternative Protocol T1048	Data Encrypted for Impact T1486	Inhibit 2

Here you will see the MITRE ATT&CK matrix for the index that was just imported. As you complete test cases and take note of the results, these cells will be color coded based on how strong or weak your organization’s detection/blocking capabilities are for any given test case.

MITRE ATT&CK Alignment												
Framework												
Display Mode												
ENTERPRISE												
Mitre Filters												
No Test Coverage												
Outcome TBD												
Weakest												
Minimal												
Lower												
Moderate												
Strong												
INACTIVE												
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
		Phishing T1566 4 1	Scheduled Task/Job T1053 1 0	Account Manipulation T1098 5 4	Account Manipulation T1098 5 4	Domain or Tenant Policy Modification T1484 3 1	Adversary-in-the-Middle T1557 1 0	Account Discovery T1087 1 0	Remote Services T1021 5 1	Adversary-in-the-Middle T1557 1 0	Application Layer Protocol T1071 3 0	Exfiltration Over Alternative Protocol T1048 1 0
	Valid Accounts T1078			Boot or Logon Autostart Execution T1547 1 0	Boot or Logon Autostart Execution T1547 1 0	Hide Artifacts T1564 1 0	Modify Authentication Process T1556 1 0	Network Service Discovery T1046 3 0	Use Alternative Authentication Material T1550 1 0	Data from Information Repositories T1213 2 0	Ingress Tool Transfer T1105 3 0	Inhibit System Recovery T1490 2 0
				Create Account T1136 1 0	Domain or Tenant Policy Modification T1484 3 1	Hijack Execution Flow T1574 1 0	Multi-Factor Authentication Request Generation T1621 1 0	System Information Discovery T1082 3 0			Remote Access Software T1219 3 0	Exfiltration Over C2 Channel T1041 1 0
				Hijack Execution Flow T1574 1 0	Hijack Execution Flow T1574 1 0	Impair Defenses T1562 2 0	OS Credential Dumping T1003 4 0					
				Modify Authentication Process T1556 1 0	Schedule Task/Job T1053 1 0	Indicator Removal T1070 1 0	Steal Application Access Token T1528 1 0					
				Scheduled Task/Job T1053 1 0	Valid Accounts T1078	Modify Authentication Process T1556 1 0	Steal or Forge Kerberos Tickets T1558 3 1					
				Valid Accounts T1078		Modify Registry T1112 1 0	Steal Web Session Cookie T1539 2 0					
						Obfuscate Files or Information T1027 1 0	Unsecured Credentials T1552 2 0					
						Rootkit T1014 1 0						
						System Binary Proxy Execution T1218 1 0						
						Use Alternative Authentication Material T1550 1 0						
						Valid Accounts T1078						


Now that we have created an Assessment, we will create a campaign inside of the assessment. A campaign is a smaller subset of an existing assessment to test against a more specific group of test cases, for example a campaign for AWS or Azure specifically. You could also create a campaign for one particular Threat Actor in an assessment with many Threat Actors. There are many ways you can utilize campaigns within an assessment.

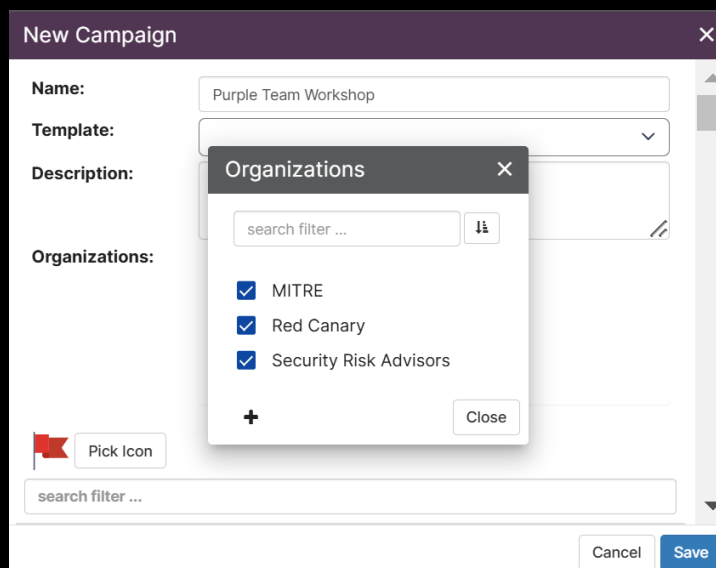
10) Navigate to Testing > 2025 Q2: TSI – Threat Simulation Index > View All Campaigns.

The screenshot shows the Vectr interface with the 'Testing' tab selected. A dropdown menu for 'ASSESSMENTS' is open, showing a list of assessments. The '2025 Q2: TSI - Threat Simulation Index' assessment is highlighted. Below the assessments, there is a section for 'CAMPAIGNS' with a list of campaigns: Impact, Purple Team Workshop, Lateral Movement, Discovery, Command and Control, Defense Evasion, and Credential Access. At the bottom of the campaigns list, there is a button labeled 'View All Campaigns' which is highlighted with a red box.

11) Click on **New Campaign**, name it "Purple Team Workshop"

The screenshot shows the Vectr interface with the 'Campaign Dashboard' for the '2025 Q1: TSI - Threat Simulation Index 2025 v1.0' assessment. The dashboard displays a table with columns for Name, Progress, Outcome, and Tags. The table lists three campaigns: Impact, Lateral Movement, and Discovery. The 'ASSESSMENT ACTIONS' dropdown menu is open, showing options: 'New Campaign', 'Edit Assessment', and 'Import Log'. The 'New Campaign' button is highlighted with a red box.

12) Click the **Organizations:**  button and Select **MITRE** and **Red Canary** as the organizations.



Filter to select relevant TTPs (see next).

TTPs for Documentation:

T1490 – HI – Delete Shadows with vssadmin

Pick Icon

T1490

↓ Include	Organizations	Phase	Category	Test Case Name	MITRE ID
<input checked="" type="checkbox"/>	SRA	Impact	Inhibit System Recovery	HI - Delete Shadows with vssadmin	T1490

T1070.001 – TSI - Clear Windows Event Log entries

Pick Icon


T1070.001

↓ Include	Organizations	Phase	Category	Test Case Name	MITRE ID
<input checked="" type="checkbox"/>	SRA	Defense Evasion	Clear Windows Event Logs	TSI - Clear Windows Event Log entries	T1070.001

T1003.001 – TSI – Dump LSASS memory using Task Manager

↓ Include	Organizations	Phase	Category	Test Case Name	MITRE ID
<input checked="" type="checkbox"/>	SRA	Credential Access	LSASS Memory	TSI - Dump LSASS memory using Task Manager	T1003.001

T1056 – HI - Keylogger


 Pick Icon

T1056

↓ Include	Organizations	Phase	Category	Test Case Name	MITRE ID
<input checked="" type="checkbox"/>	SRA	Collection	Keylogging	HI - Keylogger	T1056.001

13) Click “Save” to save your new campaign

14) Navigate to Reporting > MITRE ATT&CK Alignment and select the 2025 Q2: TSI – Threat Simulation index assessment.



ENVIRONMENT
DEFAULT

Testing

Reporting

Library

Reporting > Heat Map

Report Type

Assessments

Heat Map

2025 Q1: TSI - Threat Simulation Index 2025 v1.0.2

Assessment Heat Map

No Test Coverage

Outcome TBD

INACTIVE

Reconnaissance

Resource Development

Initial Access

Phishing

T1566

4


1

Spearphishing Attachment

T1566.001


GUIDED ANALYSIS

Threat Resilience Scoring



MITRE ATT&CK Alignment

Resilience Trending



SAVED REPORT VIEWS

2024 Heat Map

REPORT TYPES

Scorecard

Test Case Drilldown

Data Integrity

Occurrence Filter

No Filter

Mitre Filters

Moderate

Strong

Discovery

Account Discovery

T1087

1

0

Lateral Movement

Remote Services

T1021

5

1

Collection

Adversary Impersonation

T1557

Assessments

Filter Assessments

HEALTH INDEX

Health Threat Index 2022 (Q1)

Health Threat Index 2022 (Q2)

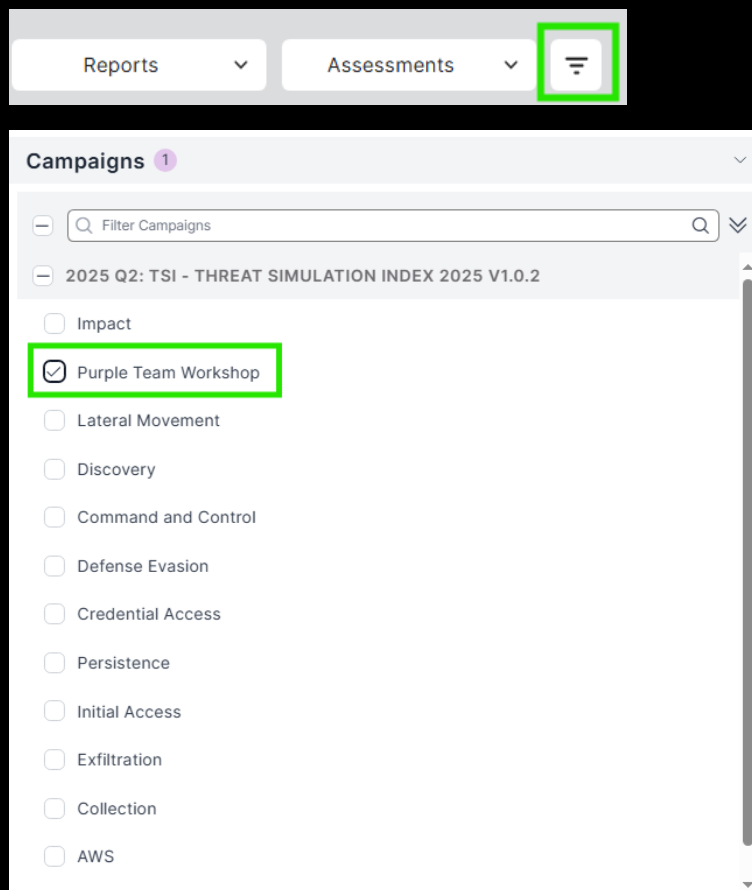
Health Threat Index 2022 (Q3)

Health Threat Index 2022 (Q4)

OTHER ASSESSMENTS

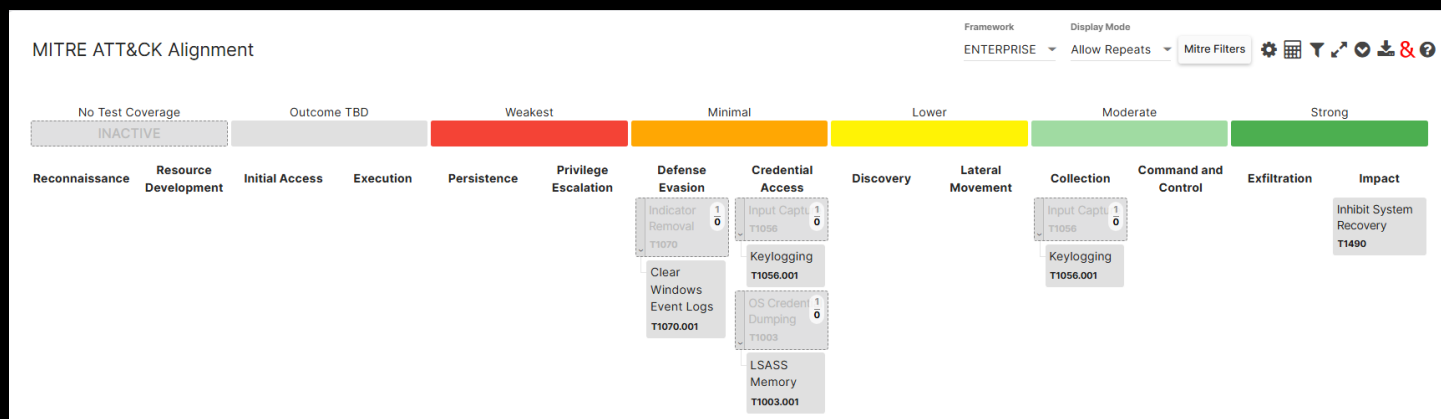
2025 Q2: TSI - Threat Simulation Index 2025 v1.0.2

15) Next to “Assessments” click on the Filter button and select the Purple Team Workshop campaign:

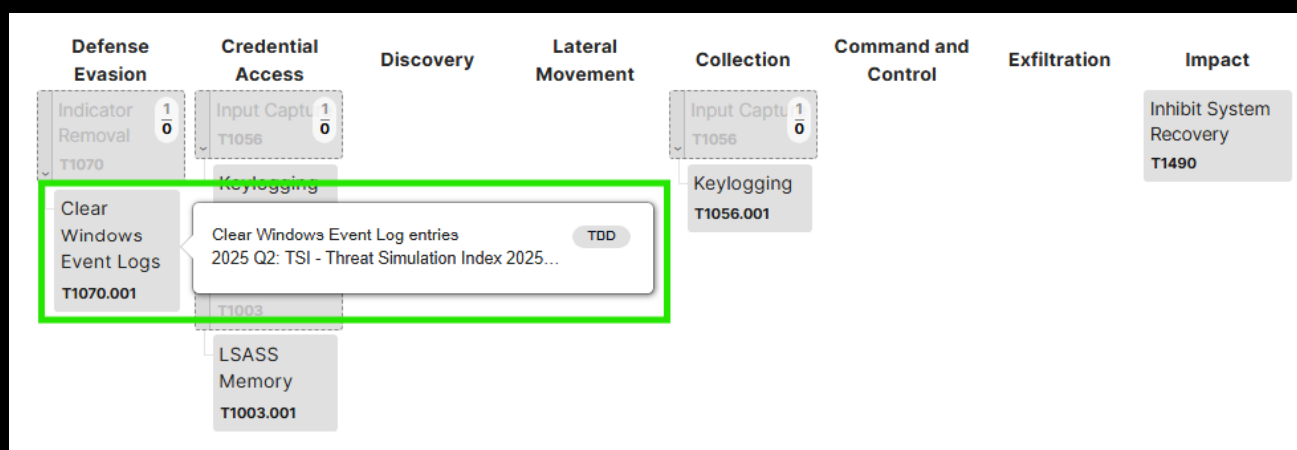


16) Click back into the MITRE ATT&CK Matrix to close the menu

You will now see the Purple Team Workshop campaign created under the TSI – Threat Simulation Index in the MITRE ATT&CK Alignment page:

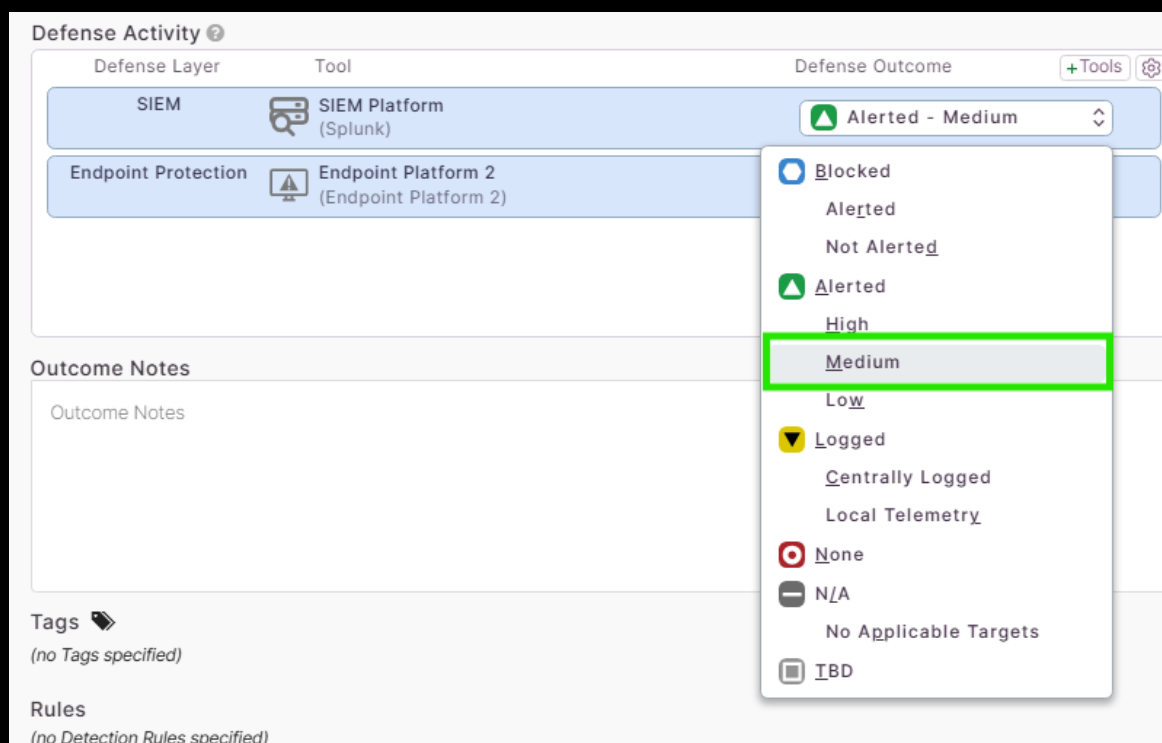


17) Click into “Clear Windows Event Logs”



This page is where all of the information for the test case resides. This keeps track of the Status of the test case, the Attack Timeline, the Name and Description of the test, the Operators Guidance, Detection Time, Outcome Notes, and Detection/Prevention guidance, as well as any evidence files such as screenshots of alerts or logs. It is a very well-organized means of tracking these test cases. We will simulate the test case outcome.

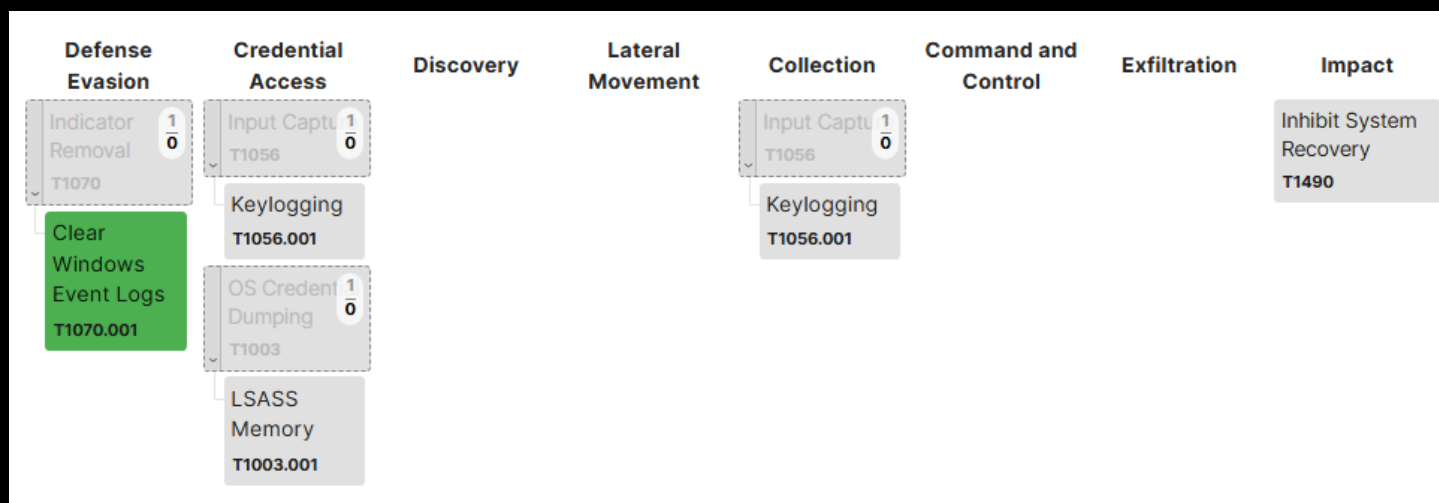
18) Under Defense Activity > SIEM dropdown, select the “Alerted – Medium” outcome



You will see the Test Case outcome at the top right switch to “Success” and Test Case Outcome will show the “Alerted – Medium” outcome that we selected in the dropdown.

19) In the Outcome Notes section, write “Alerted in SIEM” and then press Save at the bottom right of the page.

You will see the “Clear Windows Event Logs” test case turned green. This is an indication that the organization has passed this test case.



20) Open the Keylogging test case. Under Defense Activity > Endpoint Protection Dropdown, select Blocked – Alerted and then Save at the bottom right.

This will cause the Keylogging test case to turn green. You will also see that the Keylogging test case exists in two columns (two tactics or phases). This is because a Keylogger can be used for both Credential Access as well as Collection of data or other information that a threat actor may want to gather. It should be noted that some test cases may exist in more than one Tactic, but the test case when opened is the same singular test case.

21) Open the LSASS Memory test case. Under Defense Activity > Endpoint Protection dropdown, select “none” and Save at the bottom right.

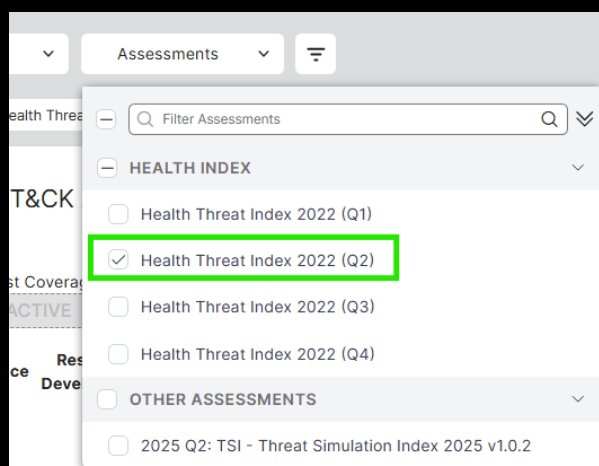
The LSASS Memory test case turned red due to this being a completely failed test case.

22) Open the Inhibit System Recovery test case. Under Defense Activity > SIEM drop down, select “Centrally Logged” and then Save at the bottom right.

This test case turned orange. This is still a failure, but it is not as bad as no logging at all as there are some artifacts left from the technique whereas the LSASS Memory technique indicates the organization was completely blind to the technique.

To visualize what a fully completed heat map would look like, we will navigate to a demo index that is pre-populated with results.

23) Navigate to Assessments and select “Health Threat Index 2022 (Q2)”

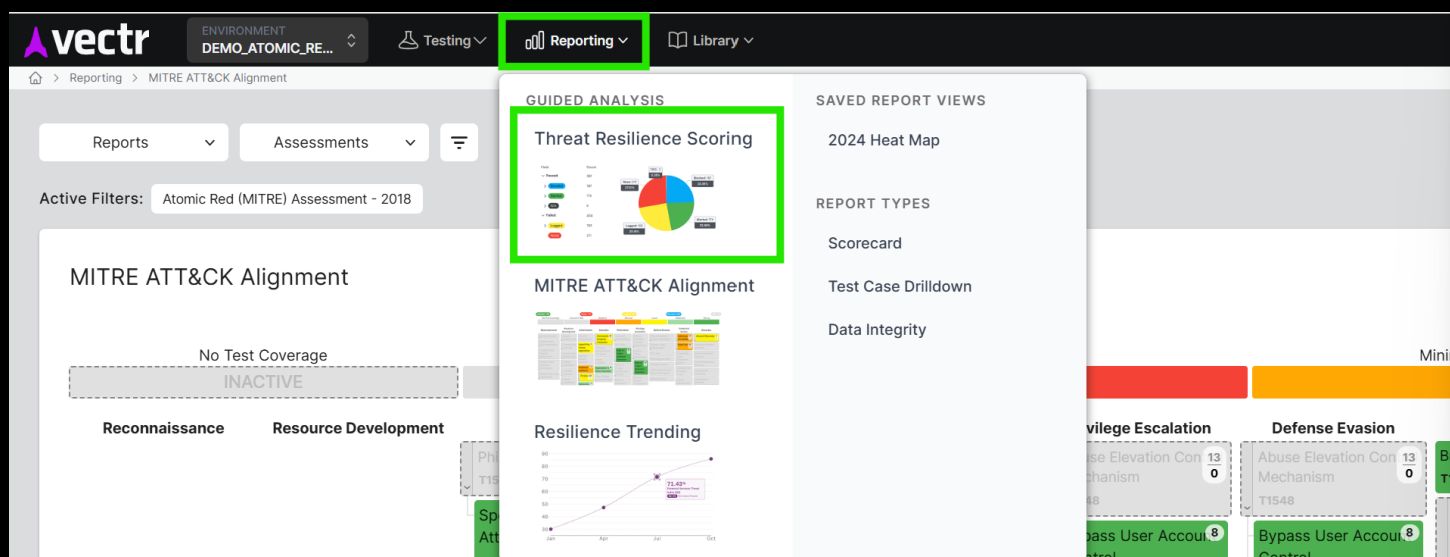


The idea behind all of this is to allow Incident Response a fighting chance at detecting and eradicating a threat before they are able to complete their objective. The more test cases you alert or block on, the better those chances become.

The heat map gives an easy means of visualizing which phase of a Threat Actor's attack chain we have strong defenses, and which need work.

After an Assessment is completed, the next step is to generate reports that can be disseminated to stakeholders.

24) Navigate to Reporting > Threat Resilience Scoring:



Here you can see the results of a completed assessment. The selected assessment had 52 test cases and passed 50% of them. For the test cases in this assessment, 50% of them were either blocked and/or alerted, while the other 50% were only logged or had no artifacts at all.

Scroll down and view the other charts. These are all breakdowns of Phases/Tactics along with the outcomes of the testing. There are several ways this data can be organized and reported upon. The idea is to show progression as you work with the Blue Team to build logs, alerts, and blocks as necessary to improve your resilience to the Threat Actor(s) you test against.

25) Navigate to Reports > Kill Chain Summary

The screenshot shows a navigation bar with three tabs: 'Reports', 'Assessments', and a filter icon. The 'Reports' tab is selected and highlighted with a red border. Below the navigation bar, there are three columns of report categories: 'GUIDED ANALYSIS', 'PERFORMANCE COMPARISON', and 'IN-DEPTH'. Under 'GUIDED ANALYSIS', there are three items: 'Threat Resilience Scoring', 'MITRE ATT&CK Alignment', and 'Scorecard'. Under 'PERFORMANCE COMPARISON', there is one item: 'Resilience Trending'. Under 'IN-DEPTH', there are three items: 'Toolset Summary', 'Test Case Drilldown', and 'Kill Chain Summary'. The 'Kill Chain Summary' item is highlighted with a red border. Below it is 'Data Integrity'.

Reports ▾ **Assessments** ▾

GUIDED ANALYSIS

- Threat Resilience Scoring**
Get a high-level summary of assessment performance
- MITRE ATT&CK Alignment**
Visualize your defense success against the MITRE Heatmap
- Scorecard**
Configure your dashboard of common reporting visualizations

PERFORMANCE COMPARISON

- Resilience Trending**
Track your assessment performance over time

IN-DEPTH

- Toolset Summary**
Evaluate your organization's defense tools and layers
- Test Case Drilldown**
Get detailed breakdowns per Test Case
- Kill Chain Summary**
Review your organization's defense posture by MITRE Tactic
- Data Integrity**
Improve your reporting accuracy by checking for common data mistakes

Here you can see the breakdown of individual phases within the attack in chart form in Pie Chart form.

26) Navigate to Reports > Resilience Trending

The screenshot shows the same navigation bar and report categories as the previous image. The 'Reports' tab is selected and highlighted with a red border. The 'Resilience Trending' item under the 'PERFORMANCE COMPARISON' column is highlighted with a red border.

Reports ▾ **Assessments** ▾

GUIDED ANALYSIS

- Threat Resilience Scoring**
Get a high-level summary of assessment performance
- MITRE ATT&CK Alignment**
Visualize your defense success against the MITRE Heatmap
- Scorecard**
Configure your dashboard of common reporting visualizations

PERFORMANCE COMPARISON

- Resilience Trending**
Track your assessment performance over time

IN-DEPTH

- Toolset Summary**
Evaluate your organization's defense tools and layers
- Test Case Drilldown**
Get detailed breakdowns per Test Case
- Kill Chain Summary**
Review your organization's defense posture by MITRE Tactic
- Data Integrity**
Improve your reporting accuracy by checking for common data mistakes

27) Under “Assessments” check all 4 boxes for Q1 – Q4:

Assessments

Filter Assessments

HEALTH INDEX

☒ Health Threat Index 2022 (Q1)

☒ Health Threat Index 2022 (Q2)

☒ Health Threat Index 2022 (Q3)

☒ Health Threat Index 2022 (Q4)

OTHER ASSESSMENTS

☐ 2025 Q2: TSI - Threat Simulation Index 2025 v1.0.2

As you periodically test your environment against particular indices, and of course have the blue team remediate failed test cases, you will generate a resilience trendline that can provide the feedback to leadership that the program is generating value. This trendline represents the improvement in your organization’s resilience to attacks from your adversaries.

Active Filters: Assessments 4

Resilience Trending

Score

100

80

60

40

20

0

Dec 2021

Jan 2022

Feb 2022

Mar 2022

Apr 2022

May 2022

Jun 2022

Jul 2022

Aug 2022

Sep 2022

Oct 2022

Nov 2022

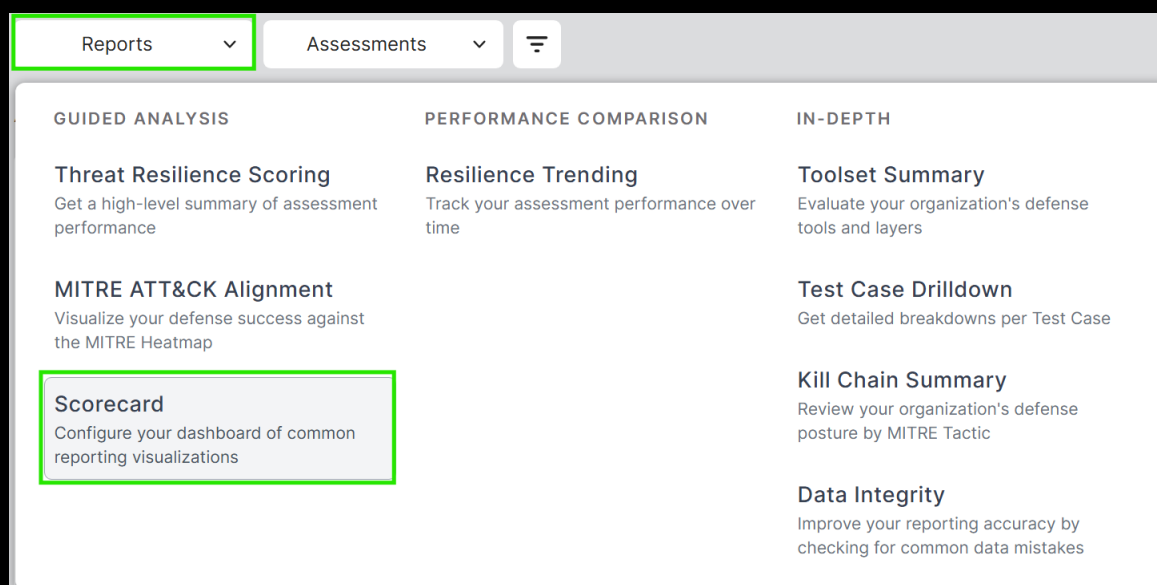
Date

Context Graph

Reset Zoom

Date	Score
Jan 2022	35
Apr 2022	50
Jul 2022	62
Oct 2022	81

28) Navigate to Reports > Scorecard:



This page provides breakdowns of the results of testing based on Outcome distribution/counts, which layers of your defense in depth are doing most of the heavy lifting, which phases of the attack chain are you strongest or weakest, as well as breaking down your most successful and least successful campaigns, phases, or techniques.

This data and these charts can be manipulated to fit the needs of your reporting or how stakeholders may want to ingest this information. Vectr provides a wide variety of reporting methods based on the results of your testing. This is often updated in new versions of Vectr.

This concludes the Lab portion of Purple Protocol. Write down any questions you may have and ask away during the review of this lab as well as the Q&A portion of the workshop (if time permits).