Improve your Threat Hunt with Adversary Emulation

Thomas V Fischer

202011191110000CET

I am @Fvt...

- Current focus is SecOps at <UNDISCLOSED>
- 25+ years experience in InfoSec
  - Security Advocate, Architect & Threat Researcher focused on Data Protection
  - Spent number years in corporate IR team positions

BSidesLondon Director

- Contact
  - tvfischer+sec@gmail.com tvfischer@pm.me
  - keybase.io/fvt

GCFA GNFA GCIH CISSP®

Challenges in Threat Hunting

Threat Hunting Defined

"the process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions" – Sqrrl, Framework for Threat Hunting

"Human act of looking for badness that is not yet detected successfully." -Sergio Caltagirone (Dragos)

https://sqrrl.com/media/Framework-for-Threat-Hunting-Whitepaper.pdf

Threat Hunting Challenges

- How to organize our program?

- Mapping gaps
  - Do I have the right data sources?
  - Are the right security controls in place?
  - Understanding adversary techniques is more than a checklist

- How effective is my program?
  - Can I detect actors, e.g APTXX

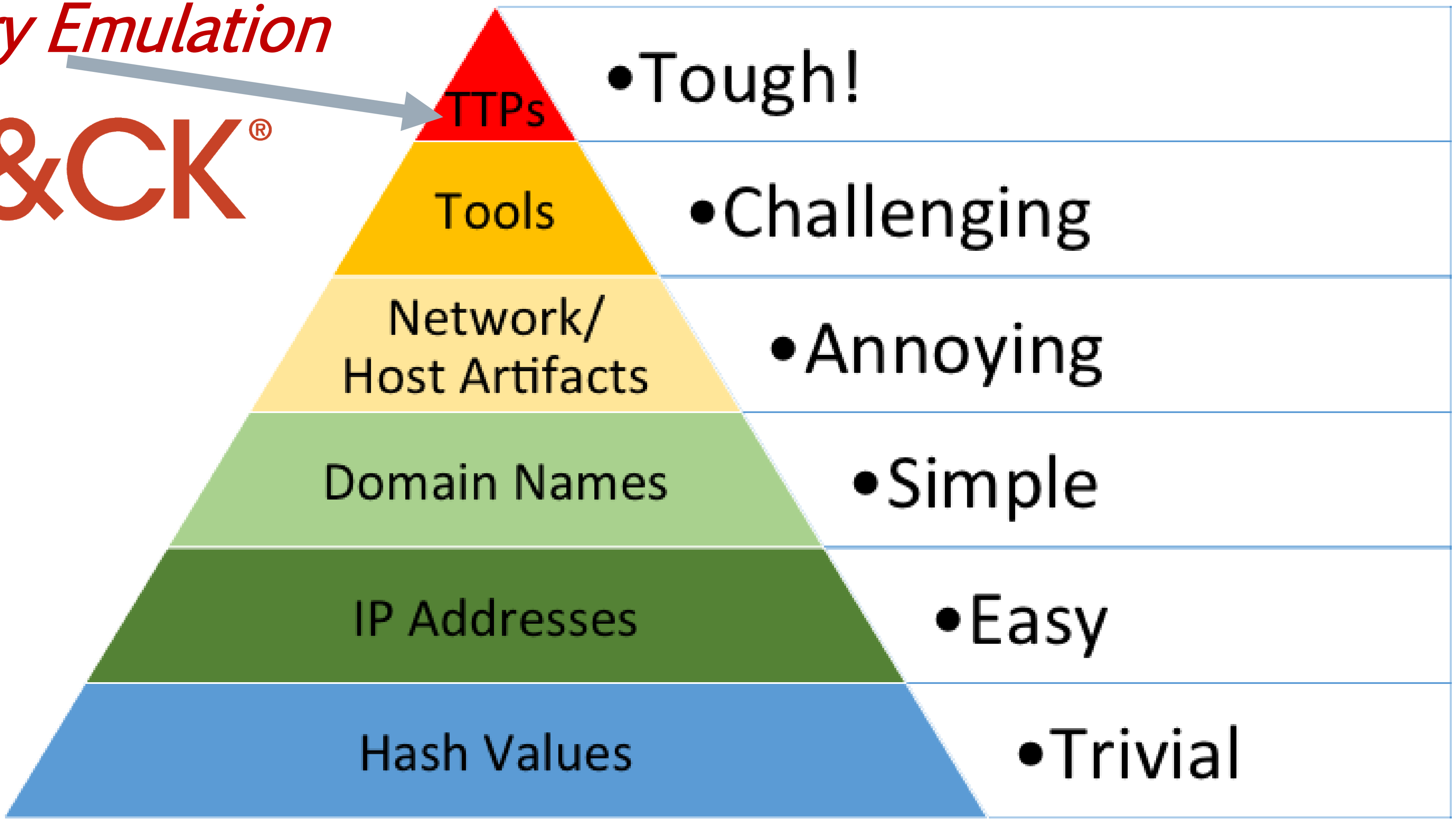
Key Characteristics of an Efficient Process

- What adversary model do we support?
- How we prioritize adversary techniques
- What about the data?
  - Understand the quality
  - Do we have the right data
- Technology
- People skills

The Pyramid of Pain

Adversary Emulation

ATT&CK®



David Bianco, https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Adversary Emulation

Adversary Emulation - Definition

- Activity where **how an adversary operates** is performed by a security team
- Benefit is to **improve the organization's defense posture** against adversary techniques
- *Red and Purple Teaming can be categorized as **Adversary Emulation***

Why Adversary Emulation?

- Prioritize results
- Validating defenses
- Gap identification

Adversary Activities

- Not IOCs
- Tactics, Techniques & Procedures
  - How the adversary operates at a high level
  - Basis of the adversary emulation
- Traditional tools, methods not applicable
  - Vulnerability scans
  - Penetration tests
- Use a structured approach
  - Kill chain or attack flow
  - e.g. MITRE ATT&CK

Key Differences Pentest vs. Adversary Emulation

Penetration Testing

- Assess security by identifying and exploiting vulnerabilities
- Focus on a scope or set of systems
- Focused on testing prevention not detection

Adversary Emulation

- Assess organization readiness versus certain threat actors
- Focus on execution of scenarios (how many flags)
- Tests both prevention and detection (blue team presence)

Key Differences in Teaming

Purple Team

- Real world threat actor emulated using TTPs
- Maximize the interaction/ collaboration with the blue team
- **Benefit**: improve the prevention and detection capabilities

Red Team

- Real world threat actor emulated using TTPs
- Little or no interaction with the blue team (red vs blue)
- **Benefit**: assess the blue team's performance

Tools for Adversary Emulation

MITRE Says it Best

> “MITRE’s Adversarial Tactics, Techniques and Common Knowledge (ATT&CK™) is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary’s lifecycle and the platforms they are known to target.
>
> ATT&CK is useful for understanding security risk against known adversary behavior, for planning security improvements, and verifying defenses work as expected.”

https://attack.mitre.org/

Tactics and Techniques

- Tactics describe high-level steps taken by adversary to attack
- Breach is assumed in ATT&CK
  - *Initial Intrusion* is “first”
- Techniques describe how a tactic is executed
  - Description, detection & recommended prevention
  - Known threat actor
  - Further broken down into sub-techniques

Procedures vs. Sub-techniques

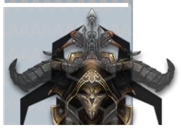
- Sub-techniques
  - More details on behaviour used to achieve goal
  - Lower-level than technique
  - Not on all techniques

- Procedures
  - A specific implementation used by adversary
  - Procedures section in
  - “observed in the wild”

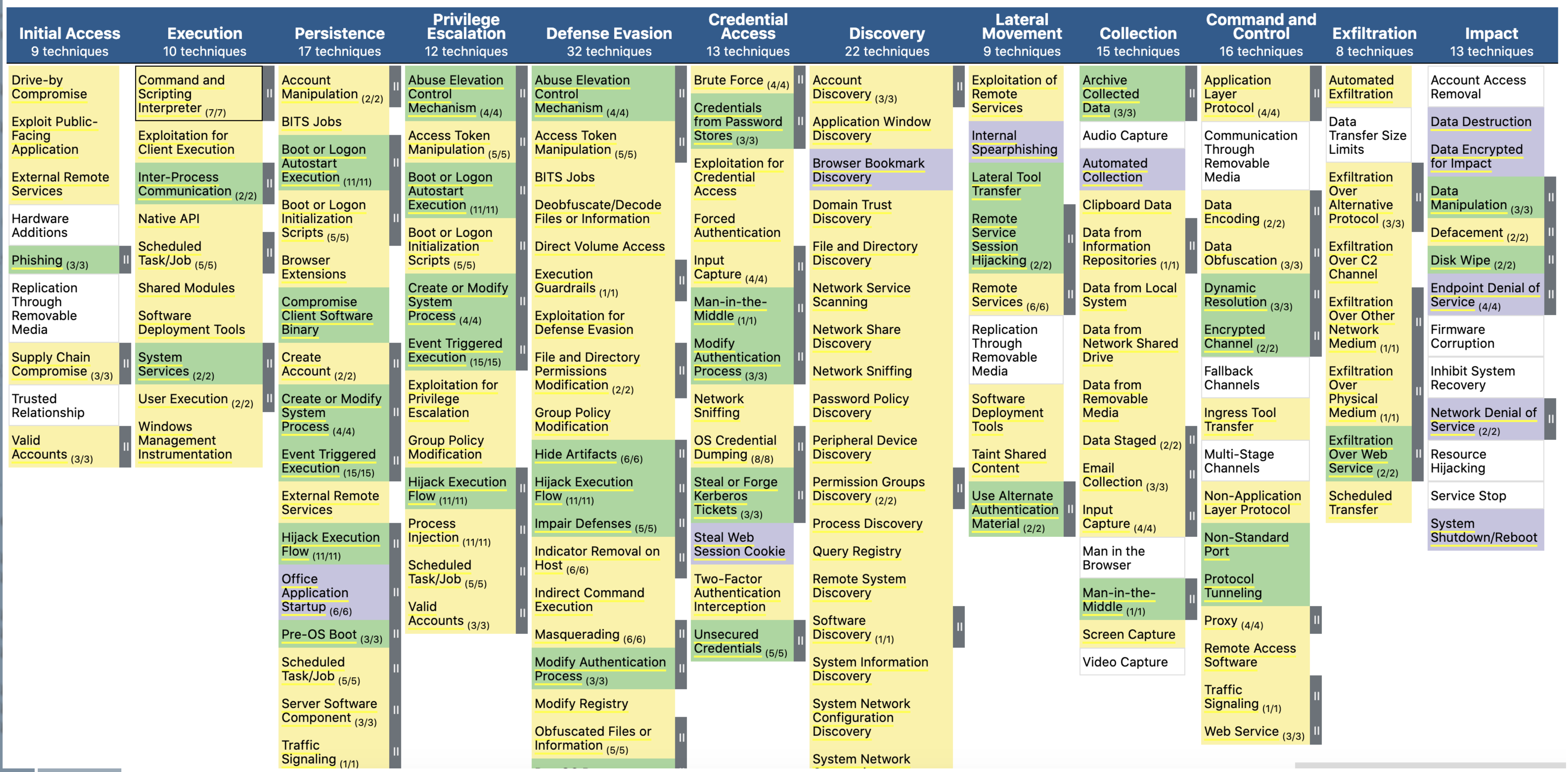
Procedures vs. Sub-techniques

- Sub-techniques
  - More details on behaviour used to achieve goal
  - Lower-level than technique
  - Not on all techniques
- Procedures
  - A specific implementation used by adversary
  - Procedures section in
  - “**observed in the wild**”

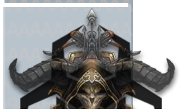
DEEPSEC
IN-DEPTH SECURITY



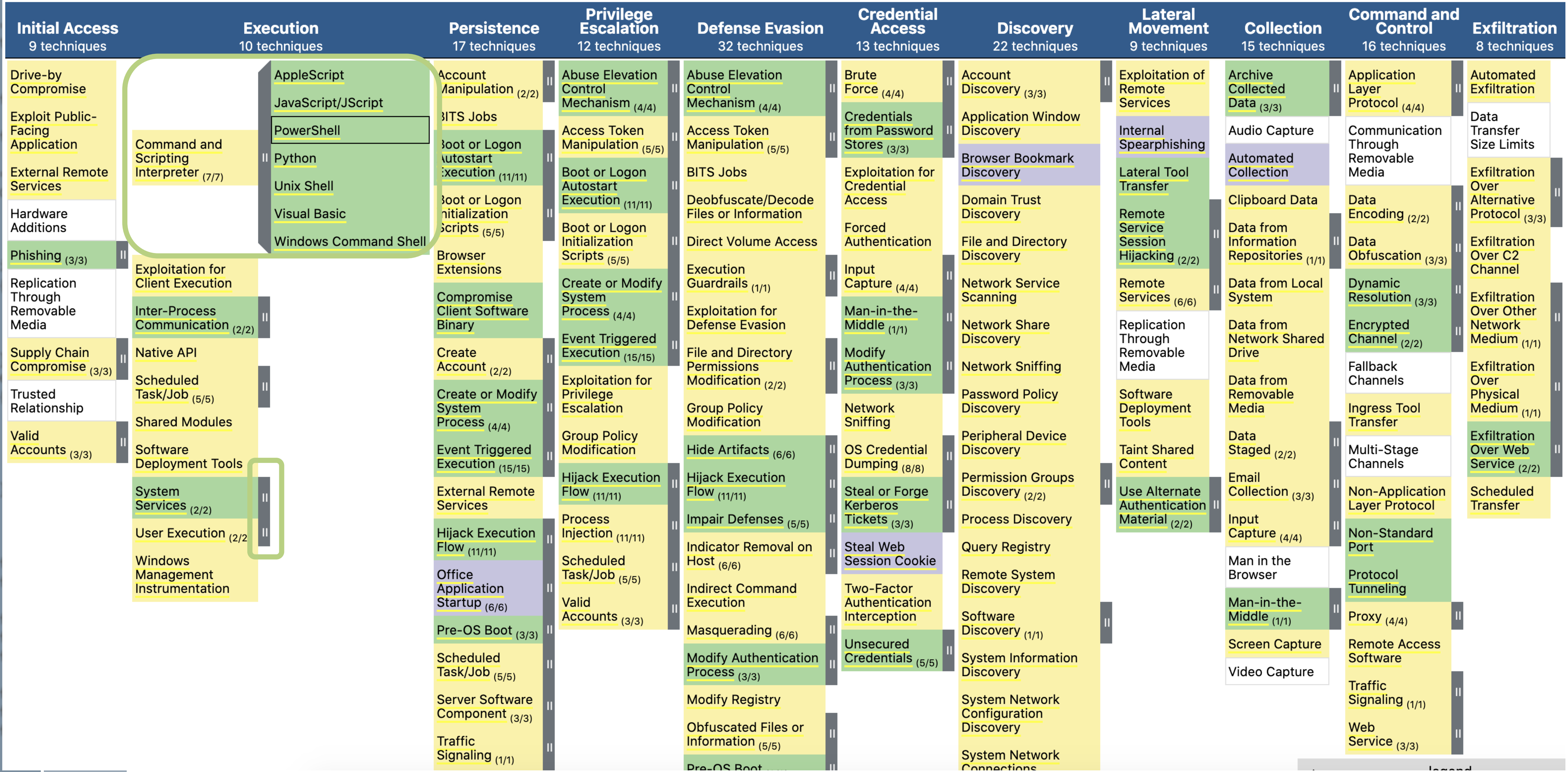
MITRE ATT&CK



Initial Access 9 techniques	Execution 10 techniques	Persistence 17 techniques	Privilege Escalation 12 techniques	Defense Evasion 32 techniques	Credential Access 13 techniques	Discovery 22 techniques	Lateral Movement 9 techniques	Collection 15 techniques	Command and Control 16 techniques	Exfiltration 8 techniques	Impact 13 techniques
Drive-by Compromise	Command and Scripting Interpreter (7/7)	Account Manipulation (2/2)	Abuse Elevation Control Mechanism (4/4)	Abuse Elevation Control Mechanism (4/4)	Brute Force (4/4)	Account Discovery (3/3)	Exploitation of Remote Services	Archive Collected Data (3/3)	Application Layer Protocol (4/4)	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5/5)	Access Token Manipulation (5/5)	Credentials from Password Stores (3/3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
External Remote Services	Inter-Process Communication (2/2)	Boot or Logon Autostart Execution (11/11)	Boot or Logon Autostart Execution (11/11)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2/2)	Exfiltration Over Alternative Protocol (3/3)	Data Encrypted for Impact
Hardware Additions	Native API	Boot or Logon Initialization Scripts (5/5)	Boot or Logon Initialization Scripts (5/5)	Deobfuscate/Decode Files or Information	Forced Authentication	Domain Trust Discovery	Remote Service Session Hijacking (2/2)	Clipboard Data	Data Obfuscation (3/3)	Exfiltration Over C2 Channel	Data Manipulation (3/3)
Phishing (3/3)	Scheduled Task/Job (5/5)	Browser Extensions	Create or Modify System Process (4/4)	Direct Volume Access	Input Capture (4/4)	File and Directory Discovery	Remote Services (6/6)	Data from Information Repositories (1/1)	Dynamic Resolution (3/3)	Exfiltration Over Other Network Medium (1/1)	Defacement (2/2)
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (15/15)	Execution Guardrails (1/1)	Man-in-the-Middle (1/1)	Network Service Scanning	Replication Through Removable Media	Data from Local System	Encrypted Channel (2/2)	Exfiltration Over Physical Medium (1/1)	Disk Wipe (2/2)
Supply Chain Compromise (3/3)	Software Deployment Tools	Create Account (2/2)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process (3/3)	Network Share Discovery	Software Deployment Tools	Data from Network Shared Drive	Fallback Channels	Exfiltration Over Web Service (2/2)	Endpoint Denial of Service (4/4)
Trusted Relationship	System Services (2/2)	Create or Modify System Process (4/4)	Group Policy Modification	File and Directory Permissions Modification (2/2)	Network Sniffing	Network Sniffing	Taint Shared Content	Data from Removable Media	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Valid Accounts (3/3)	User Execution (2/2)	Event Triggered Execution (15/15)	Hijack Execution Flow (11/11)	Group Policy Modification	OS Credential Dumping (8/8)	Password Policy Discovery	Use Alternate Authentication Material (2/2)	Data Staged (2/2)	Multi-Stage Channels		Inhibit System Recovery
	Windows Management Instrumentation	External Remote Services	Process Injection (11/11)	Hide Artifacts (6/6)	Steal or Forge Kerberos Tickets (3/3)	Peripheral Device Discovery		Email Collection (3/3)	Non-Application Layer Protocol		Network Denial of Service (2/2)
		Hijack Execution Flow (11/11)	Scheduled Task/Job (5/5)	Hijack Execution Flow (11/11)	Steal Web Session Cookie	Permission Groups Discovery (2/2)		Input Capture (4/4)	Non-Standard Port		Resource Hijacking
		Office Application Startup (6/6)	Valid Accounts (3/3)	Impair Defenses (5/5)	Two-Factor Authentication Interception	Process Discovery		Man in the Browser	Protocol Tunneling		Service Stop
		Pre-OS Boot (3/3)		Indicator Removal on Host (6/6)	Unsecured Credentials (5/5)	Query Registry		Man-in-the-Middle (1/1)	Proxy (4/4)		System Shutdown/Reboot
		Scheduled Task/Job (5/5)		Indirect Command Execution		Remote System Discovery		Screen Capture	Remote Access Software		
		Server Software Component (3/3)		Masquerading (6/6)		Software Discovery (1/1)		Video Capture	Traffic Signaling (1/1)		
		Traffic Signaling (1/1)		Modify Authentication Process (3/3)		System Information Discovery			Web Service (3/3)		
				Modify Registry		System Network Configuration Discovery					
				Obfuscated Files or Information (5/5)		System Network					

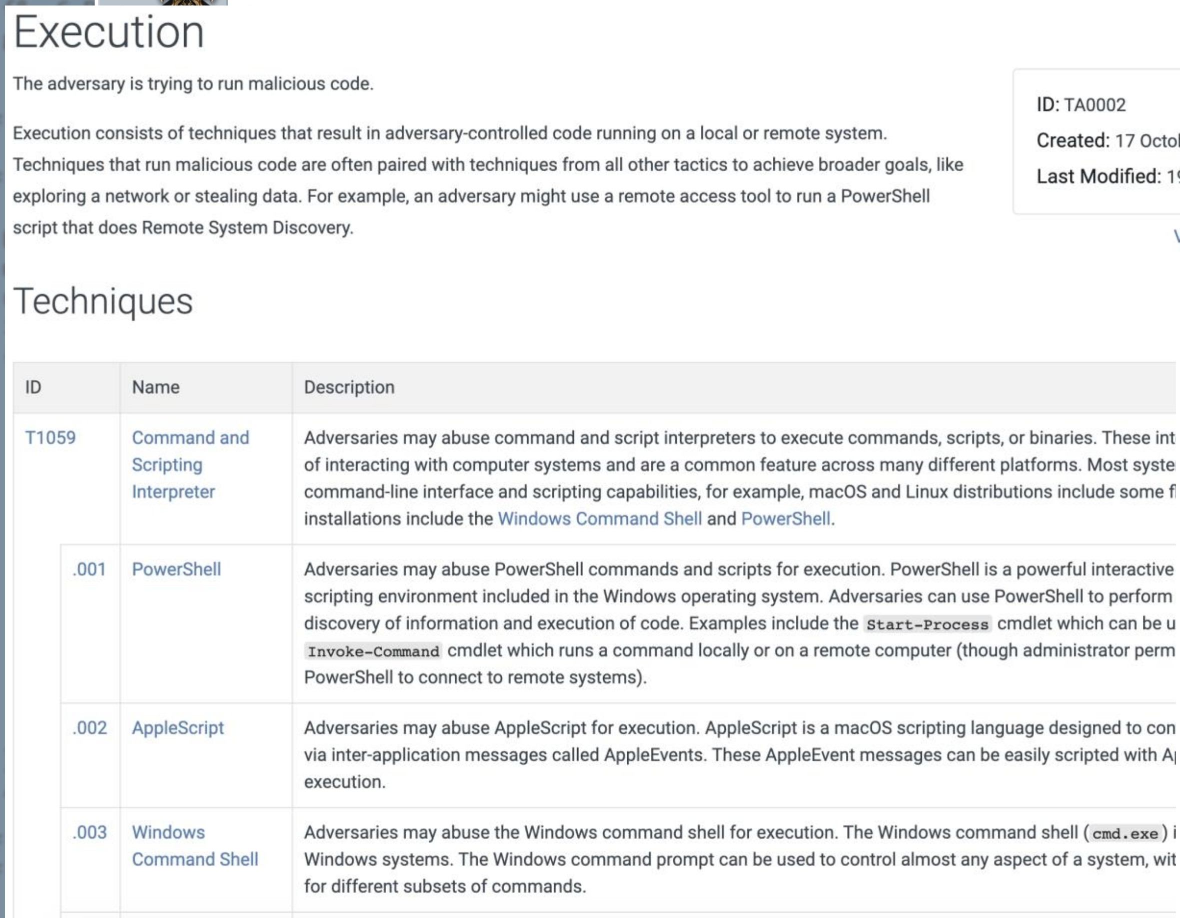


MITRE ATT&CK – Sub Techniques



Initial Access 9 techniques	Execution 10 techniques	Persistence 17 techniques	Privilege Escalation 12 techniques	Defense Evasion 32 techniques	Credential Access 13 techniques	Discovery 22 techniques	Lateral Movement 9 techniques	Collection 15 techniques	Command and Control 16 techniques	Exfiltration 8 techniques
Drive-by Compromise	Command and Scripting Interpreter (7/7) AppleScript JavaScript/JScript PowerShell Python Unix Shell Visual Basic Windows Command Shell	Account Manipulation (2/2)	Abuse Elevation Control Mechanism (4/4)	Abuse Elevation Control Mechanism (4/4)	Brute Force (4/4)	Account Discovery (3/3)	Exploitation of Remote Services	Archive Collected Data (3/3)	Application Layer Protocol (4/4)	Automated Exfiltration
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5/5)	Access Token Manipulation (5/5)	Credentials from Password Stores (3/3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits
External Remote Services	Inter-Process Communication (2/2)	Boot or Logon Autostart Execution (11/11)	Boot or Logon Autostart Execution (11/11)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2/2)	Exfiltration Over Alternative Protocol (3/3)
Hardware Additions	Native API	Boot or Logon Initialization Scripts (5/5)	Boot or Logon Initialization Scripts (5/5)	Deobfuscate/Decode Files or Information	Forced Authentication	Domain Trust Discovery	Remote Service Session Hijacking (2/2)	Clipboard Data	Data Obfuscation (3/3)	Exfiltration Over C2 Channel
Phishing (3/3)	Scheduled Task/Job (5/5)	Browser Extensions	Create or Modify System Process (4/4)	Direct Volume Access	Input Capture (4/4)	File and Directory Discovery	Remote Services (6/6)	Data from Information Repositories (1/1)	Dynamic Resolution (3/3)	Exfiltration Over Other Network Medium (1/1)
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (15/15)	Execution Guardrails (1/1)	Man-in-the-Middle (1/1)	Network Service Scanning	Replication Through Removable Media	Data from Local System	Encrypted Channel (2/2)	Exfiltration Over Physical Medium (1/1)
Supply Chain Compromise (3/3)	Software Deployment Tools	Create Account (2/2)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process (3/3)	Network Share Discovery	Software Deployment Tools	Data from Network Shared Drive	Fallback Channels	Exfiltration Over Web Service (2/2)
Trusted Relationship	System Services (2/2)	Create or Modify System Process (4/4)	Group Policy Modification	File and Directory Permissions Modification (2/2)	Network Sniffing	Network Sniffing	Taint Shared Content	Data from Removable Media	Ingress Tool Transfer	Scheduled Transfer
Valid Accounts (3/3)	User Execution (2/2	Event Triggered Execution (15/15)	Hijack Execution Flow (11/11)	Group Policy Modification	OS Credential Dumping (8/8)	Password Policy Discovery	Use Alternate Authentication Material (2/2)	Data Staged (2/2)	Multi-Stage Channels	
	Windows Management Instrumentation	External Remote Services	Process Injection (11/11)	Hide Artifacts (6/6)	Steal or Forge Kerberos Tickets (3/3)	Peripheral Device Discovery		Email Collection (3/3)	Non-Application Layer Protocol	
		Hijack Execution Flow (11/11)	Scheduled Task/Job (5/5)	Hijack Execution Flow (11/11)	Steal Web Session Cookie	Permission Groups Discovery (2/2)		Input Capture (4/4)	Non-Standard Port	
		Office Application Startup (6/6)	Valid Accounts (3/3)	Impair Defenses (5/5)	Two-Factor Authentication Interception	Process Discovery		Man in the Browser	Protocol Tunneling	
		Pre-OS Boot (3/3)		Indicator Removal on Host (6/6)	Unsecured Credentials (5/5)	Query Registry		Man-in-the-Middle (1/1)	Proxy (4/4)	
		Scheduled Task/Job (5/5)		Indirect Command Execution		Remote System Discovery		Screen Capture	Remote Access Software	
		Server Software Component (3/3)		Masquerading (6/6)		Software Discovery (1/1)		Video Capture	Traffic Signaling (1/1)	
		Traffic Signaling (1/1)		Modify Authentication Process (3/3)		System Information Discovery			Web Service (3/3)	
				Modify Registry		System Network Configuration Discovery				
				Obfuscated Files or Information (5/5)		System Network Connections				
				Pre-OS Boot						

MITRE ATT&CK – Tactic & Technique



Execution

The adversary is trying to run malicious code.

Execution consists of techniques that result in adversary-controlled code running on a local or remote system. Techniques that run malicious code are often paired with techniques from all other tactics to achieve broader goals, like exploring a network or stealing data. For example, an adversary might use a remote access tool to run a PowerShell script that does Remote System Discovery.

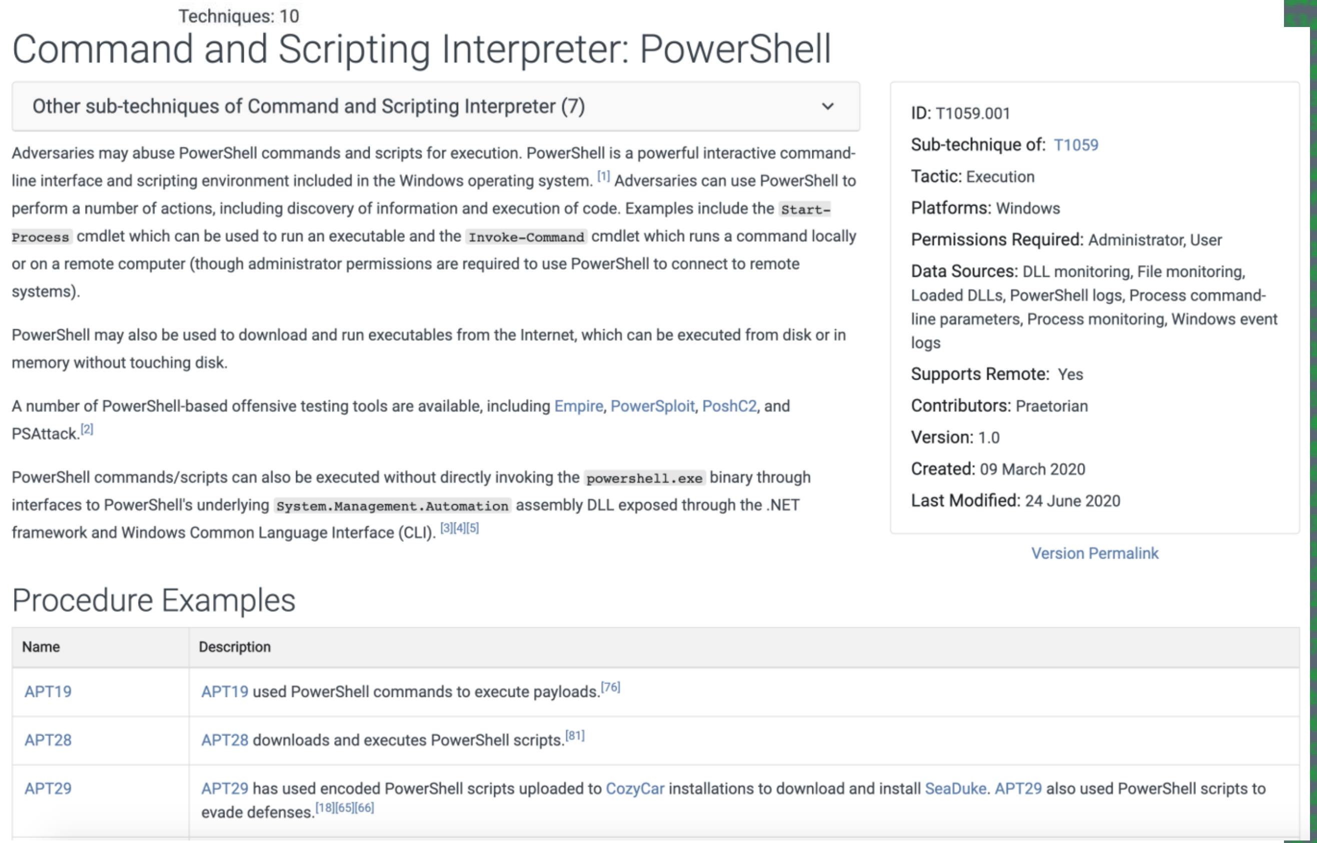
ID: TA0002
Created: 17 October 2018
Last Modified: 19 July 2019

Version Permalink

Techniques

ID		Name	Description
T1059		Command and Scripting Interpreter	Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These int of interacting with computer systems and are a common feature across many different platforms. Most syste command-line interface and scripting capabilities, for example, macOS and Linux distributions include some f installations include the Windows Command Shell and PowerShell.
	.001	PowerShell	Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive scripting environment included in the Windows operating system. Adversaries can use PowerShell to perform discovery of information and execution of code. Examples include the `Start-Process` cmdlet which can be u `Invoke-Command` cmdlet which runs a command locally or on a remote computer (though administrator perm PowerShell to connect to remote systems).
	.002	AppleScript	Adversaries may abuse AppleScript for execution. AppleScript is a macOS scripting language designed to con via inter-application messages called AppleEvents. These AppleEvent messages can be easily scripted with A execution.
	.003	Windows Command Shell	Adversaries may abuse the Windows command shell for execution. The Windows command shell (`cmd.exe`) i Windows systems. The Windows command prompt can be used to control almost any aspect of a system, wit for different subsets of commands.

Techniques: 10



Command and Scripting Interpreter: PowerShell

Other sub-techniques of Command and Scripting Interpreter (7)

Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system. [1] Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the `Start-Process` cmdlet which can be used to run an executable and the `Invoke-Command` cmdlet which runs a command locally or on a remote computer (though administrator permissions are required to use PowerShell to connect to remote systems).

PowerShell may also be used to download and run executables from the Internet, which can be executed from disk or in memory without touching disk.

A number of PowerShell-based offensive testing tools are available, including Empire, PowerSploit, PoshC2, and PSAttack.[2]

PowerShell commands/scripts can also be executed without directly invoking the `powershell.exe` binary through interfaces to PowerShell's underlying `System.Management.Automation` assembly DLL exposed through the .NET framework and Windows Common Language Interface (CLI). [3][4][5]

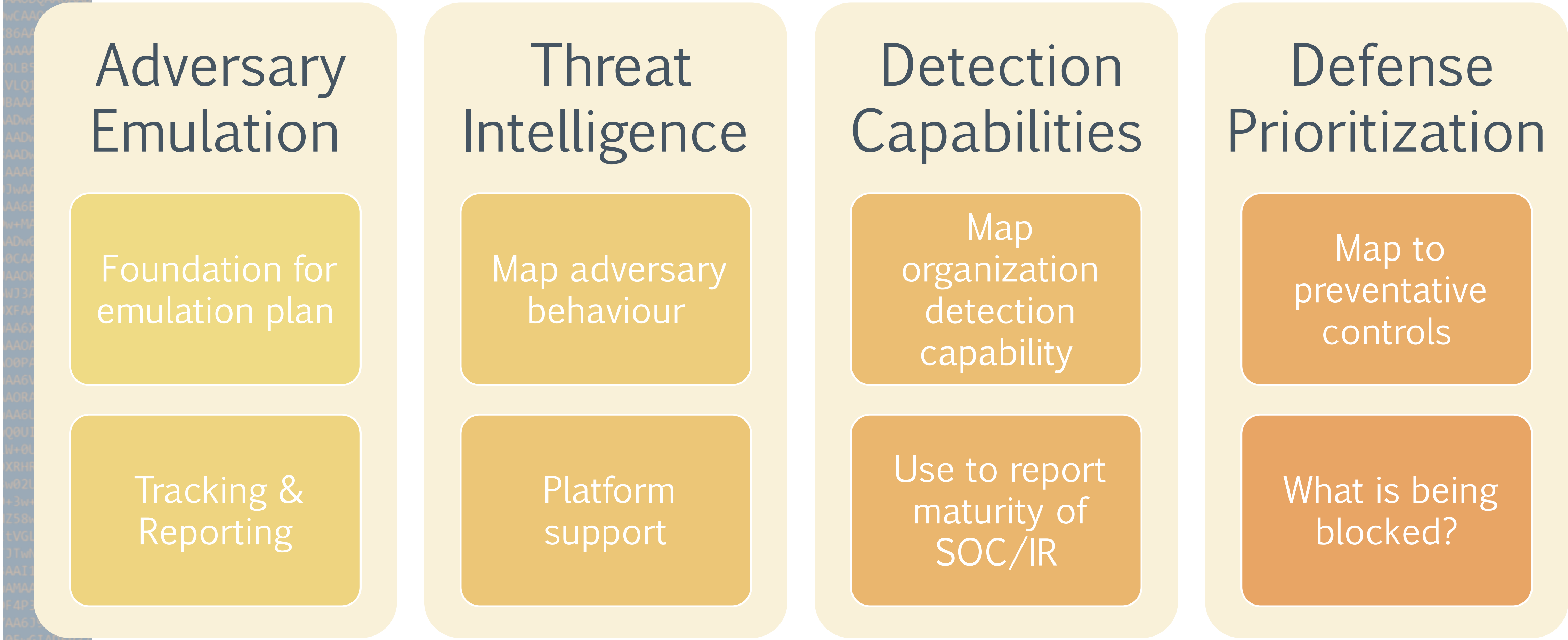
ID: T1059.001
Sub-technique of: T1059
Tactic: Execution
Platforms: Windows
Permissions Required: Administrator, User
Data Sources: DLL monitoring, File monitoring, Loaded DLLs, PowerShell logs, Process command-line parameters, Process monitoring, Windows event logs
Supports Remote: Yes
Contributors: Praetorian
Version: 1.0
Created: 09 March 2020
Last Modified: 24 June 2020

Version Permalink

Procedure Examples

Name	Description
APT19	APT19 used PowerShell commands to execute payloads.[76]
APT28	APT28 downloads and executes PowerShell scripts.[81]
APT29	APT29 has used encoded PowerShell scripts uploaded to CozyCar installations to download and install SeaDuke. APT29 also used PowerShell scripts to evade defenses.[18][65][66]

Leveraging ATT&CK



Adversary Emulation

- Foundation for emulation plan
- Tracking & Reporting

Threat Intelligence

- Map adversary behaviour
- Platform support

Detection Capabilities

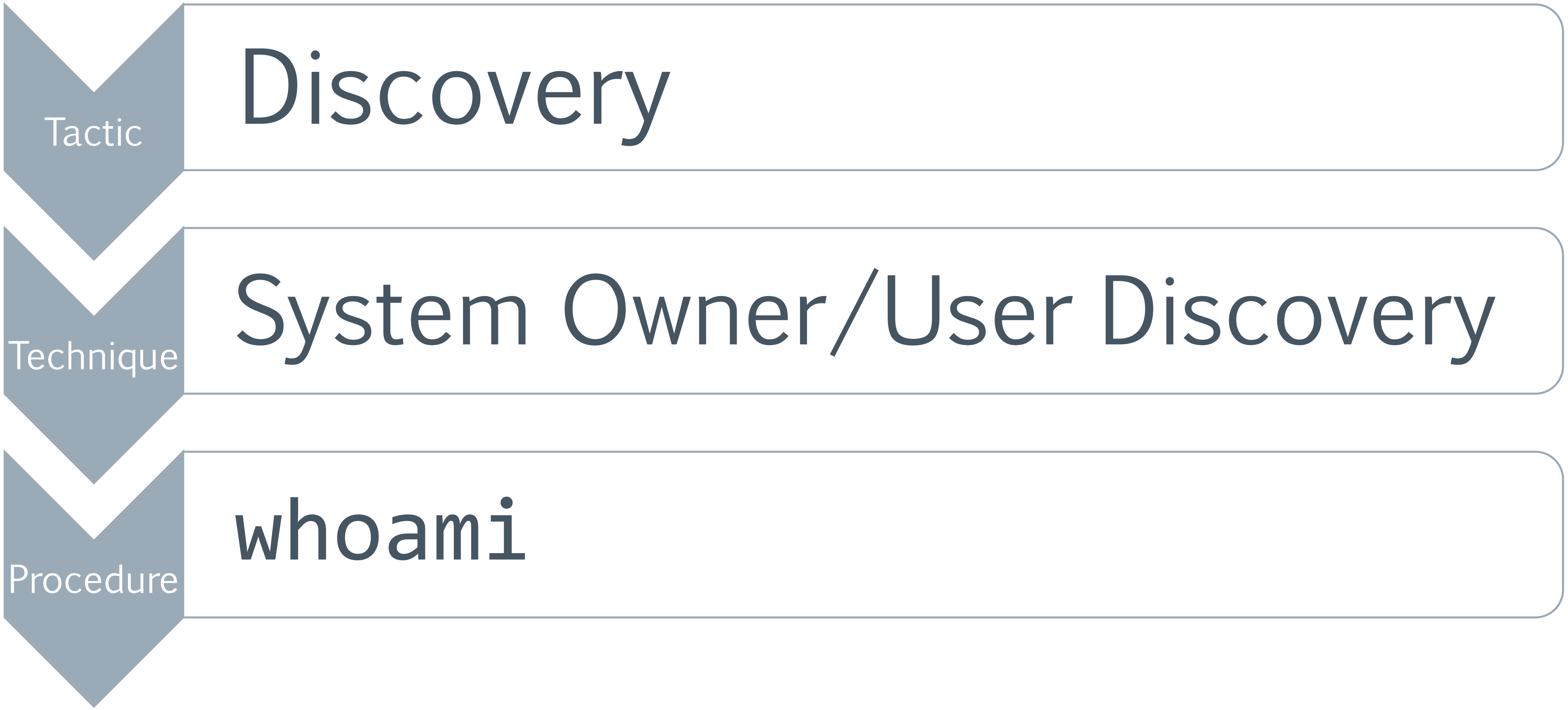
- Map organization detection capability
- Use to report maturity of SOC/IR

Defense Prioritization

- Map to preventative controls
- What is being blocked?

Common Reference Language

Example Adversary Emulation Breakdown

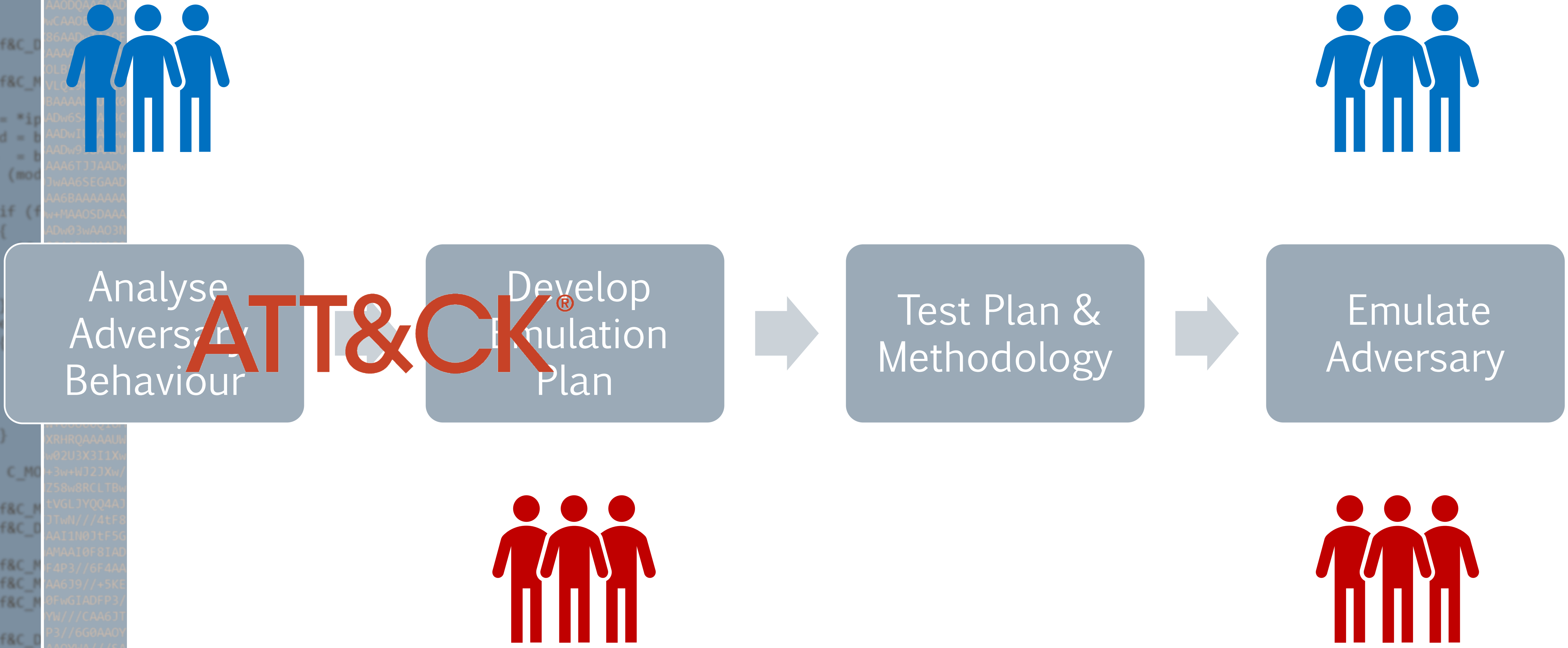


Tactic: Discovery

Technique: System Owner/User Discovery

Procedure: `whoami`

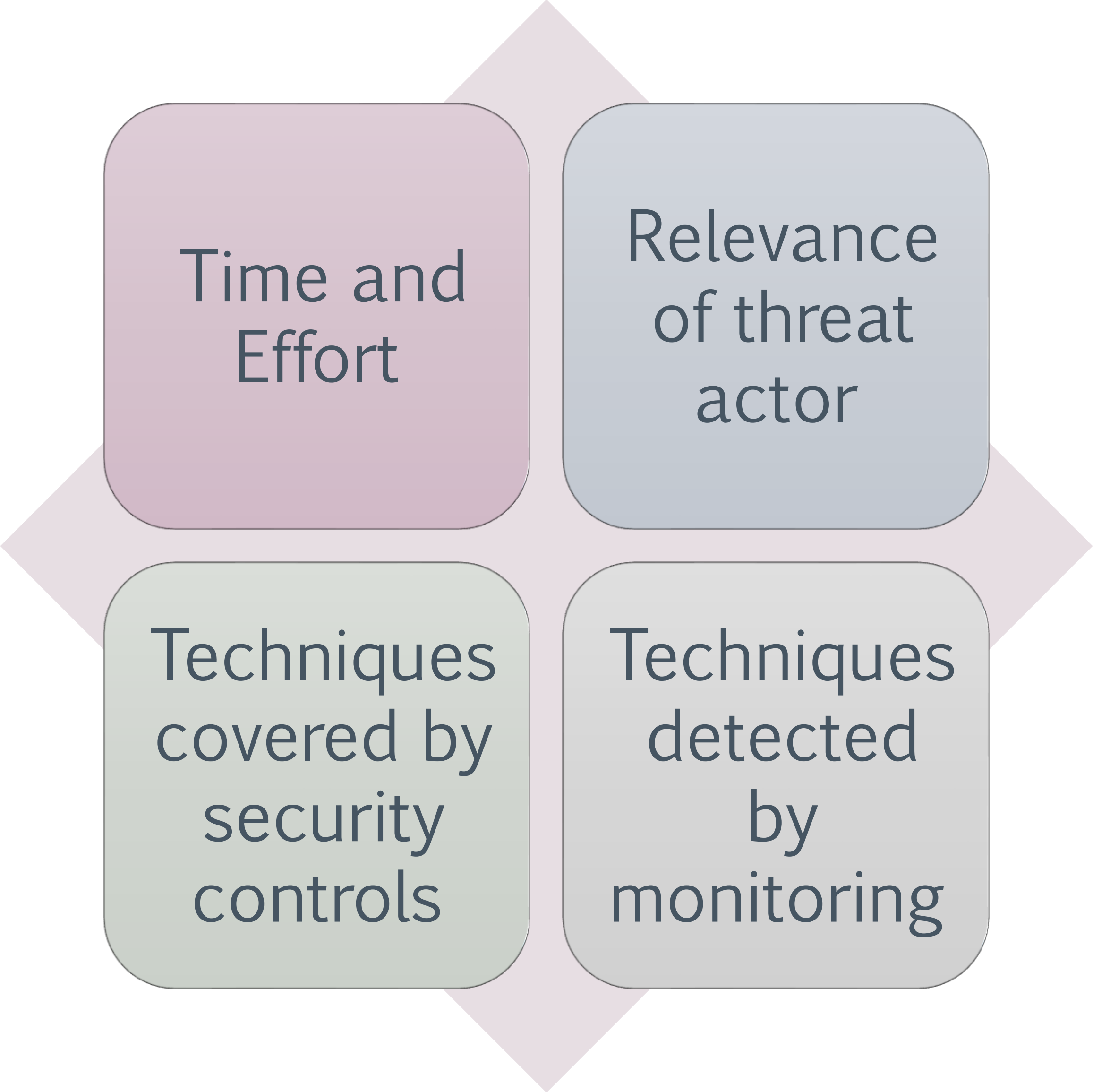
Building Adversary Emulation Process



Building an Adversary Emulation Plan

- **Good adversary emulation** plan is crucial for effectiveness
- Should include **distinct phases** to mimic a real-world adversary
- Every tactic is **NOT required**; change it up! *Improvise*
- Example phases in MITRE’s APT3
  - Implement infrastructure (C2)
  - Achieve initial execution (Initial Access)
  - Carry out internal discovery, privilege escalation and later movement (lateral movement)
  - Collect, stage and exfiltrate data (Action on Objectives)

Key Criteria for a Plan



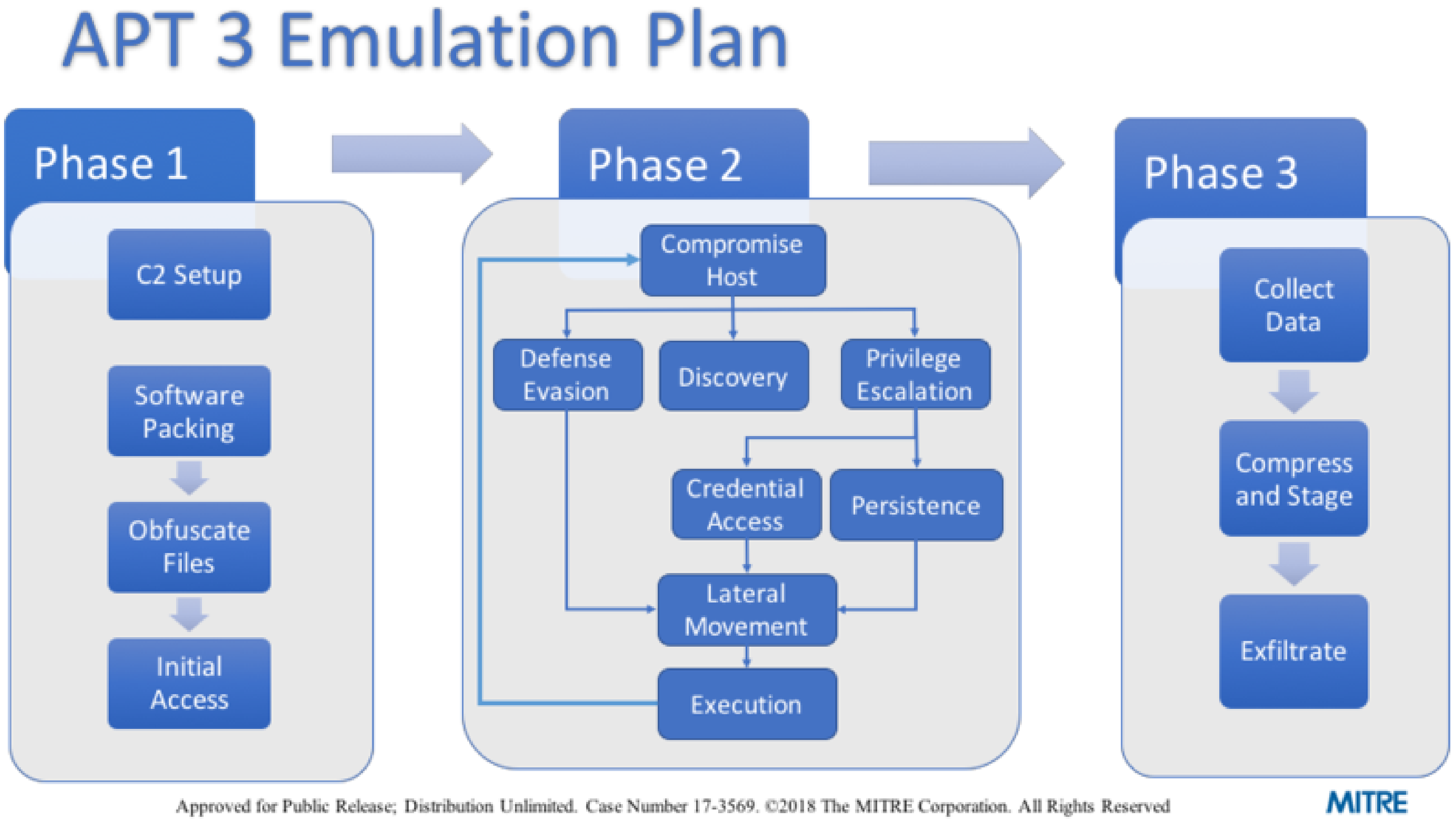
Time and Effort

Relevance of threat actor

Techniques covered by security controls

Techniques detected by monitoring

What is an Emulation Plan



APT 3 Emulation Plan

Approved for Public Release; Distribution Unlimited. Case Number 17-3569. ©2018 The MITRE Corporation. All Rights Reserved

https://attack.mitre.org/resources/adversary-emulation-plans/

APT28 Emulation Example

Phase 1

- Initial Access – Removable Media [T1091]
- Execution –Client Exploit [T1203]

Phase 2

- Persistence - Valid Accounts [T1078]
- Privilege Escalation – Exploitation [T1068]
- Defense Evasion – Obfuscate Files [T1027]
- Lateral Movement – Exploit Remove Services [T1210]

Phase 3

- Exfiltration – Exfil over C2 [T1041]

Supporting Tools

- Use an emulation stack
- Automated or scripted; supports specific set of ATT&CK techniques
- Full stack simulation based on adversary emulation plan; manual

Automated or Scripted Tools

RedHunt

Atomic Red Team

MITRE
Caldera

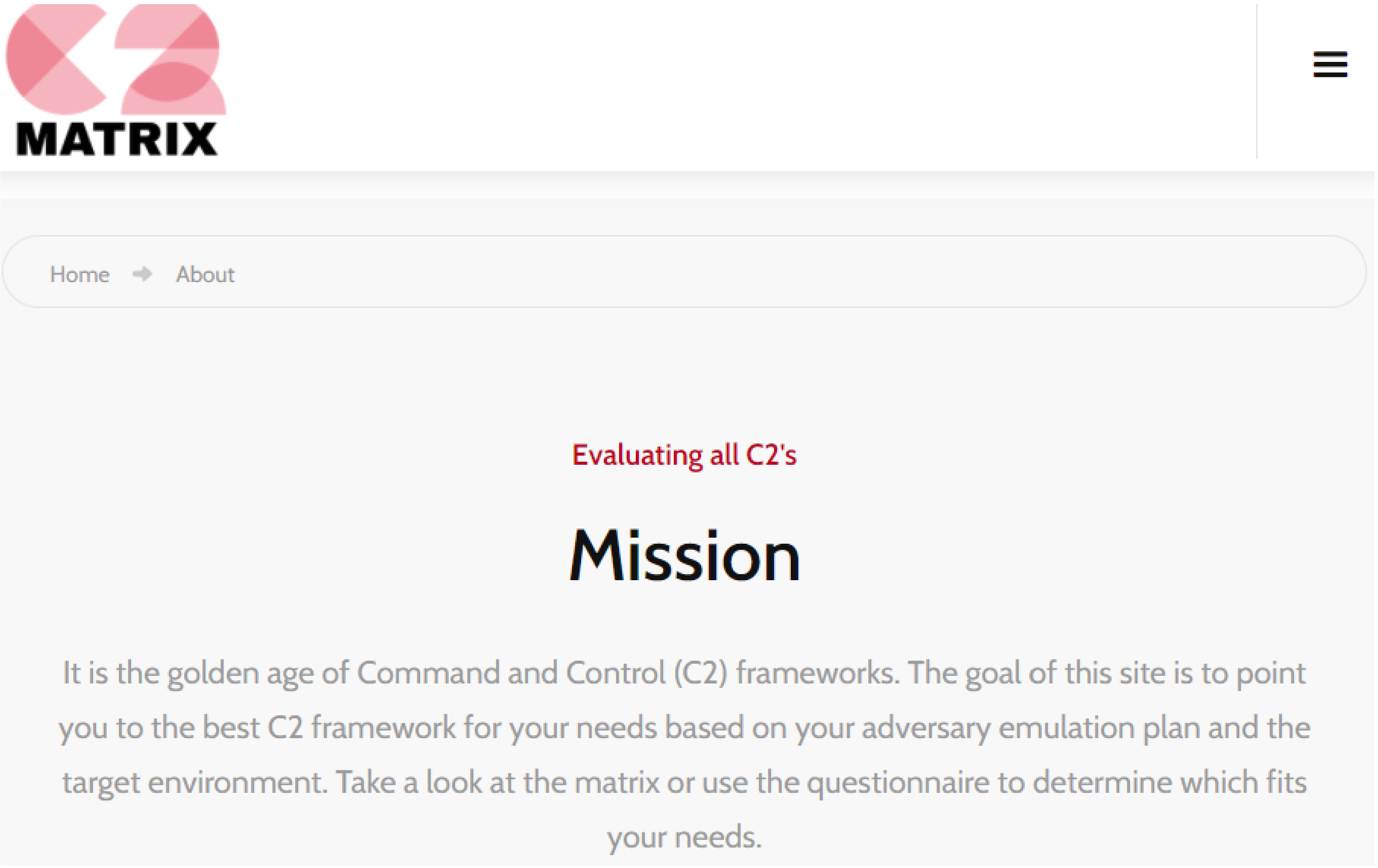
ATTACKIQ

SCYTHE

Metta (Uber)

Manual Adversary Emulation

- Red Team Automation (RTA)
- DumpsterFire Toolset
- Covenant



C2 MATRIX

Home ➜ About

Evaluating all C2's

Mission

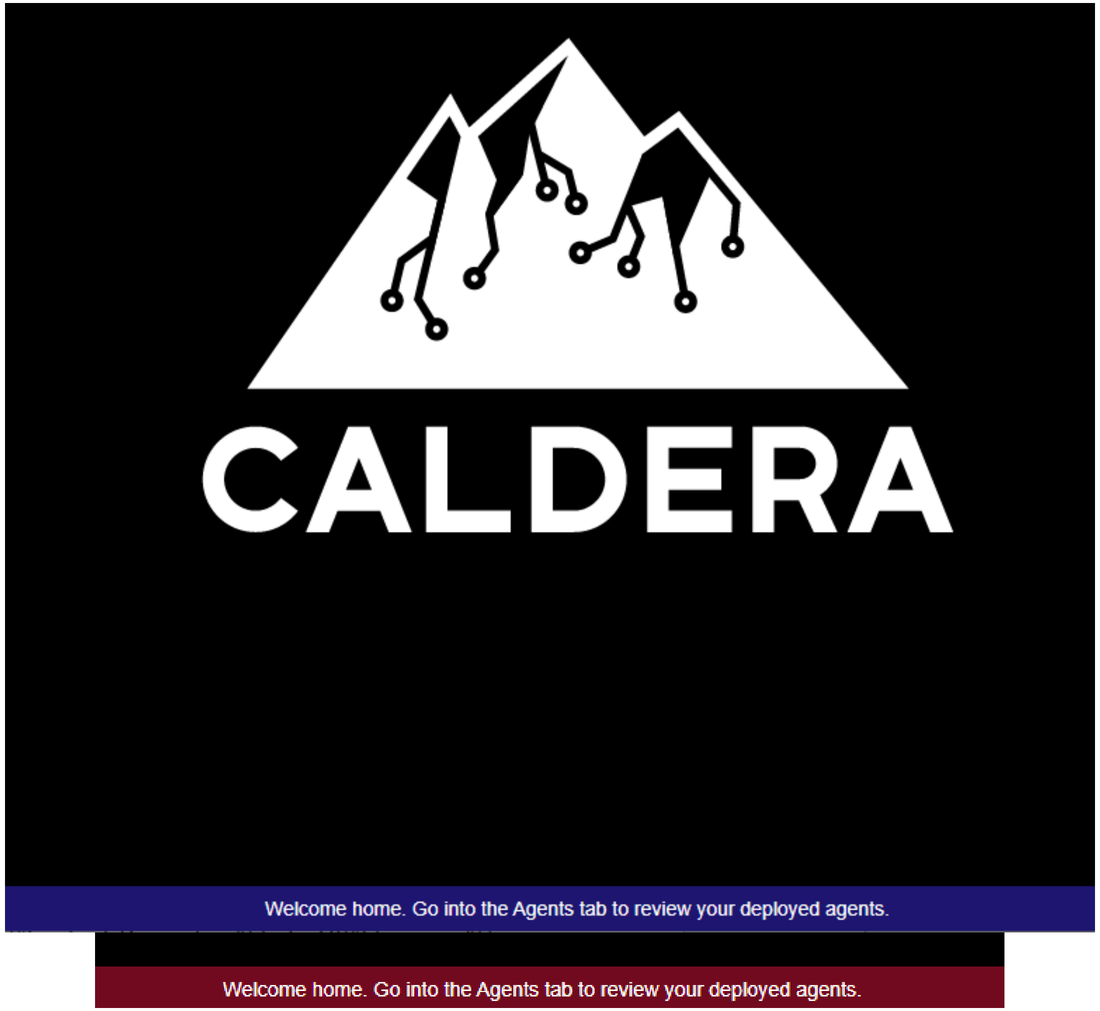
It is the golden age of Command and Control (C2) frameworks. The goal of this site is to point you to the best C2 framework for your needs based on your adversary emulation plan and the target environment. Take a look at the matrix or use the questionnaire to determine which fits your needs.

https://www.thec2matrix.com/

MITRE Caldera

Quick Intro

https://github.com/mitre/caldera



Welcome home. Go into the Agents tab to review your deployed agents.

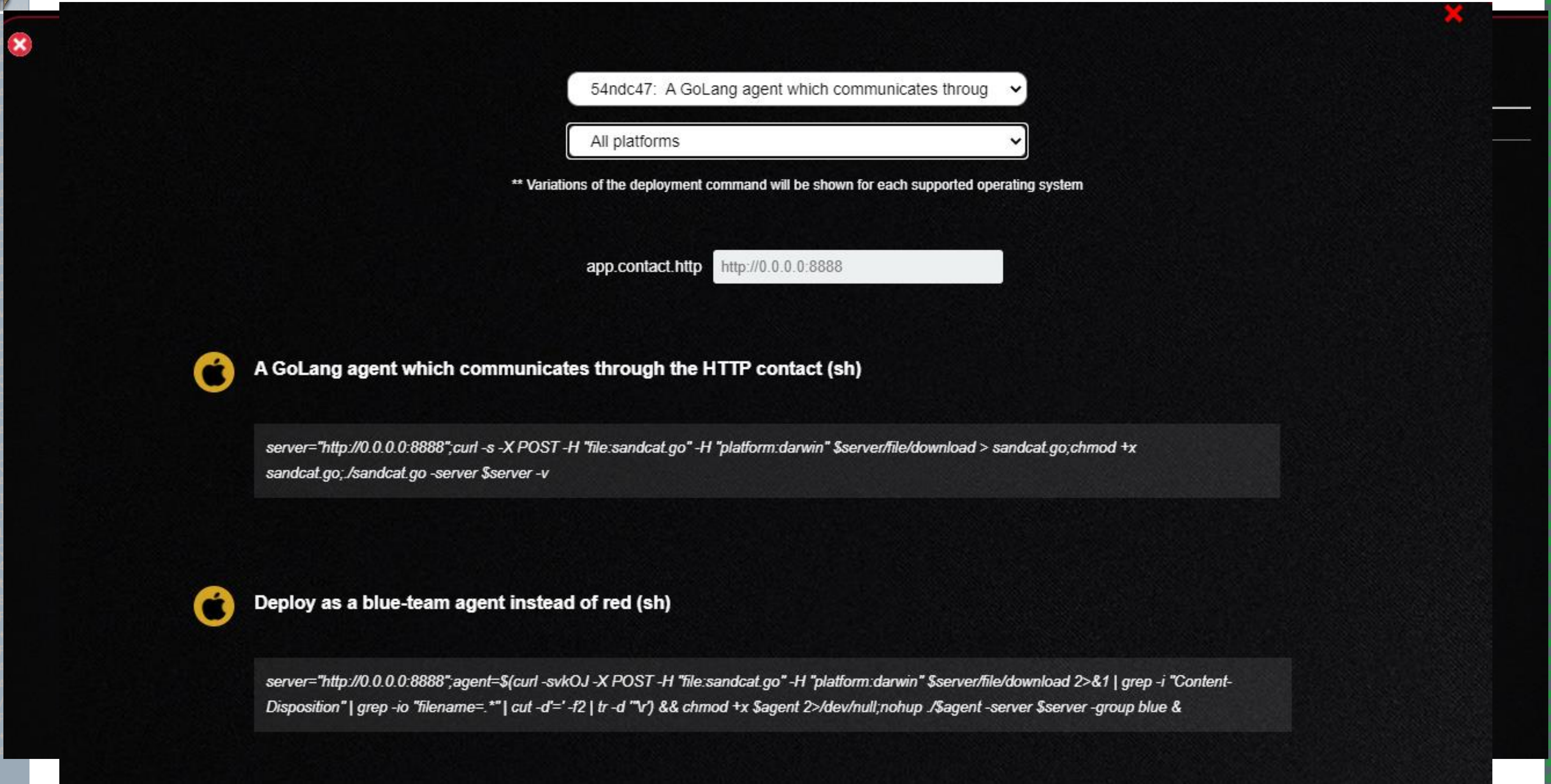
Welcome home. Go into the Agents tab to review your deployed agents.

MITRE Caldera Basics

- **Use Cases**
  - Red-Team Engagements
  - Autonomous Incident Response
  - Non-deterministically (decision making algos)

- **Terminology**
  - Agent
  - Group
  - Ability
  - Adversary
  - Operation
  - Fact
  - Source
  - Rule
  - Planner
  - Plugin

CALDERA – Deploy Agent



** Variations of the deployment command will be shown for each supported operating system

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

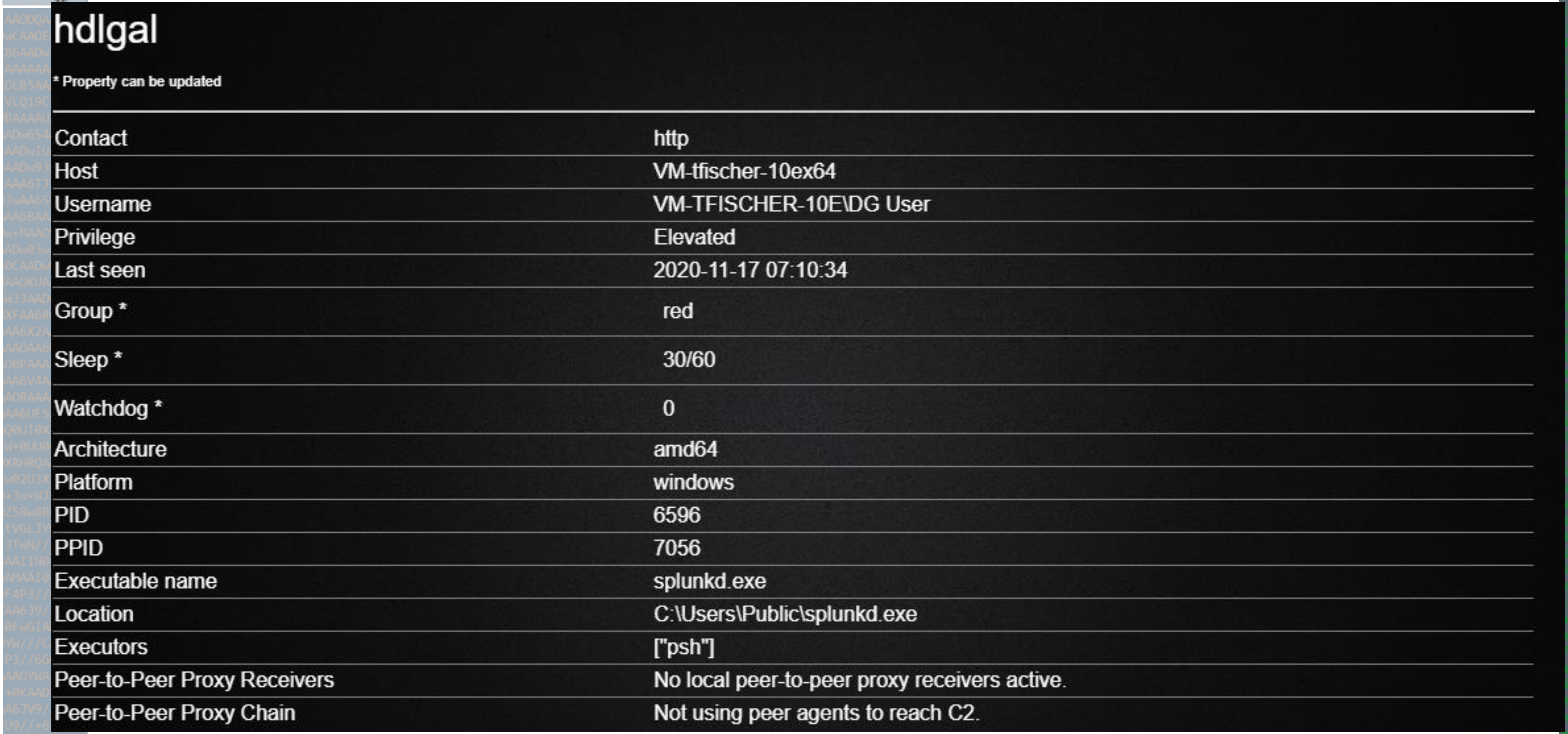
A GoLang agent which communicates through the HTTP contact (sh)

```
server="http://0.0.0.0:8888";curl -s -X POST -H "file:sandcat.go" -H "platform:darwin" $server/file/download > sandcat.go;chmod +x sandcat.go;./sandcat.go -server $server -v
```

Deploy as a blue-team agent instead of red (sh)

```
server="http://0.0.0.0:8888";agent=$(curl -svkOJ -X POST -H "file:sandcat.go" -H "platform:darwin" $server/file/download 2>&1 | grep -i "Content-Disposition" | grep -io "filename=.*" | cut -d'=' -f2 | tr -d '"\r') && chmod +x $agent 2>/dev/null;nohup ./$agent -server $server -group blue &
```

CALDERA – Agent Info

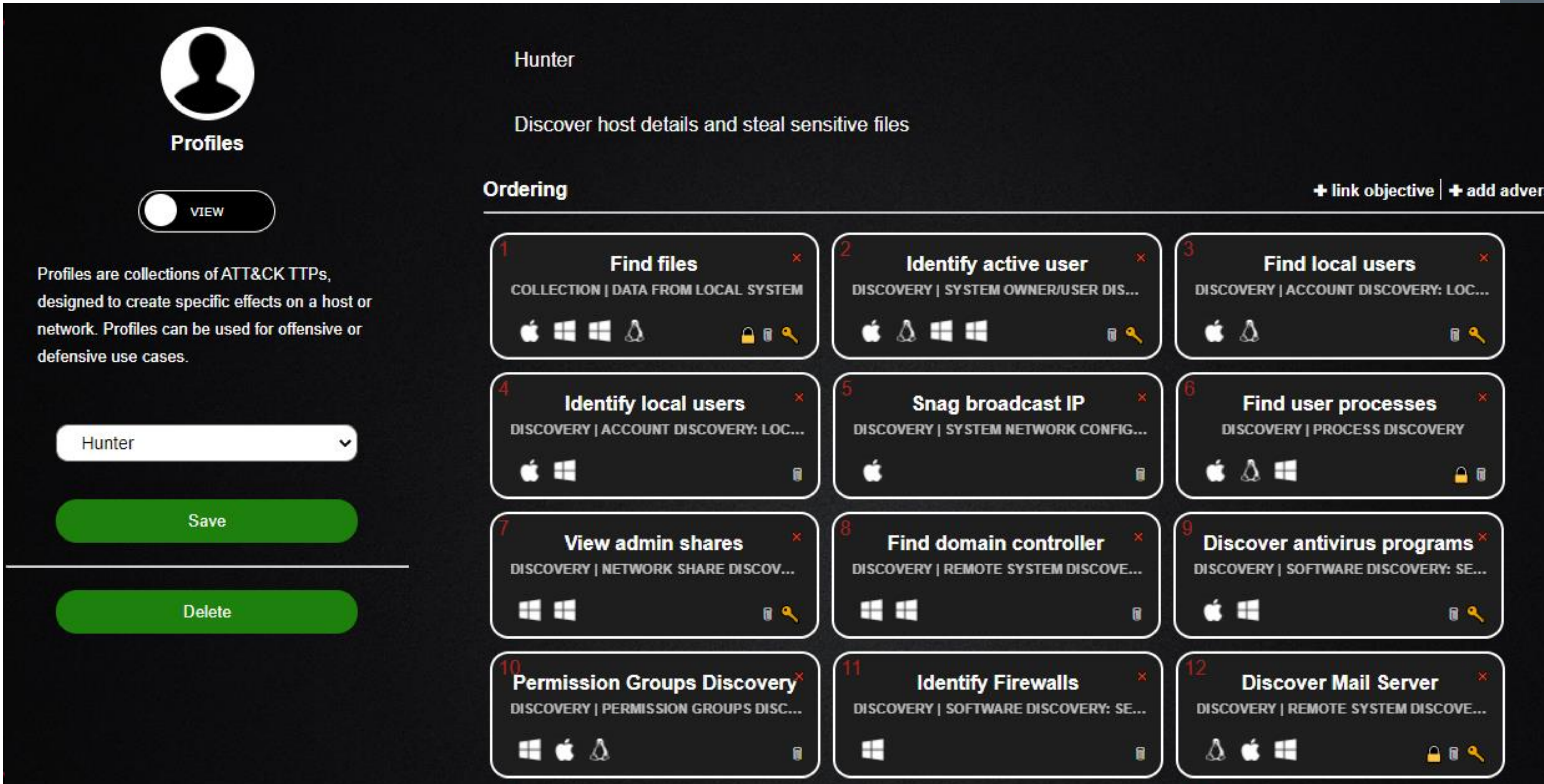


hdlgal

* Property can be updated

Contact	http
Host	VM-tfischer-10ex64
Username	VM-TFISCHER-10E\DG User
Privilege	Elevated
Last seen	2020-11-17 07:10:34
Group *	red
Sleep *	30/60
Watchdog *	0
Architecture	amd64
Platform	windows
PID	6596
PPID	7056
Executable name	splunkd.exe
Location	C:\Users\Public\splunkd.exe
Executors	["psh"]
Peer-to-Peer Proxy Receivers	No local peer-to-peer proxy receivers active.
Peer-to-Peer Proxy Chain	Not using peer agents to reach C2.

CALDERA – Adversary Profiles



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.

Hunter

Hunter

Discover host details and steal sensitive files

Ordering

1 Find files
COLLECTION | DATA FROM LOCAL SYSTEM

2 Identify active user
DISCOVERY | SYSTEM OWNER/USER DIS...

3 Find local users
DISCOVERY | ACCOUNT DISCOVERY: LOC...

4 Identify local users
DISCOVERY | ACCOUNT DISCOVERY: LOC...

5 Snag broadcast IP
DISCOVERY | SYSTEM NETWORK CONFIG...

6 Find user processes
DISCOVERY | PROCESS DISCOVERY

7 View admin shares
DISCOVERY | NETWORK SHARE DISCOV...

8 Find domain controller
DISCOVERY | REMOTE SYSTEM DISCOVE...

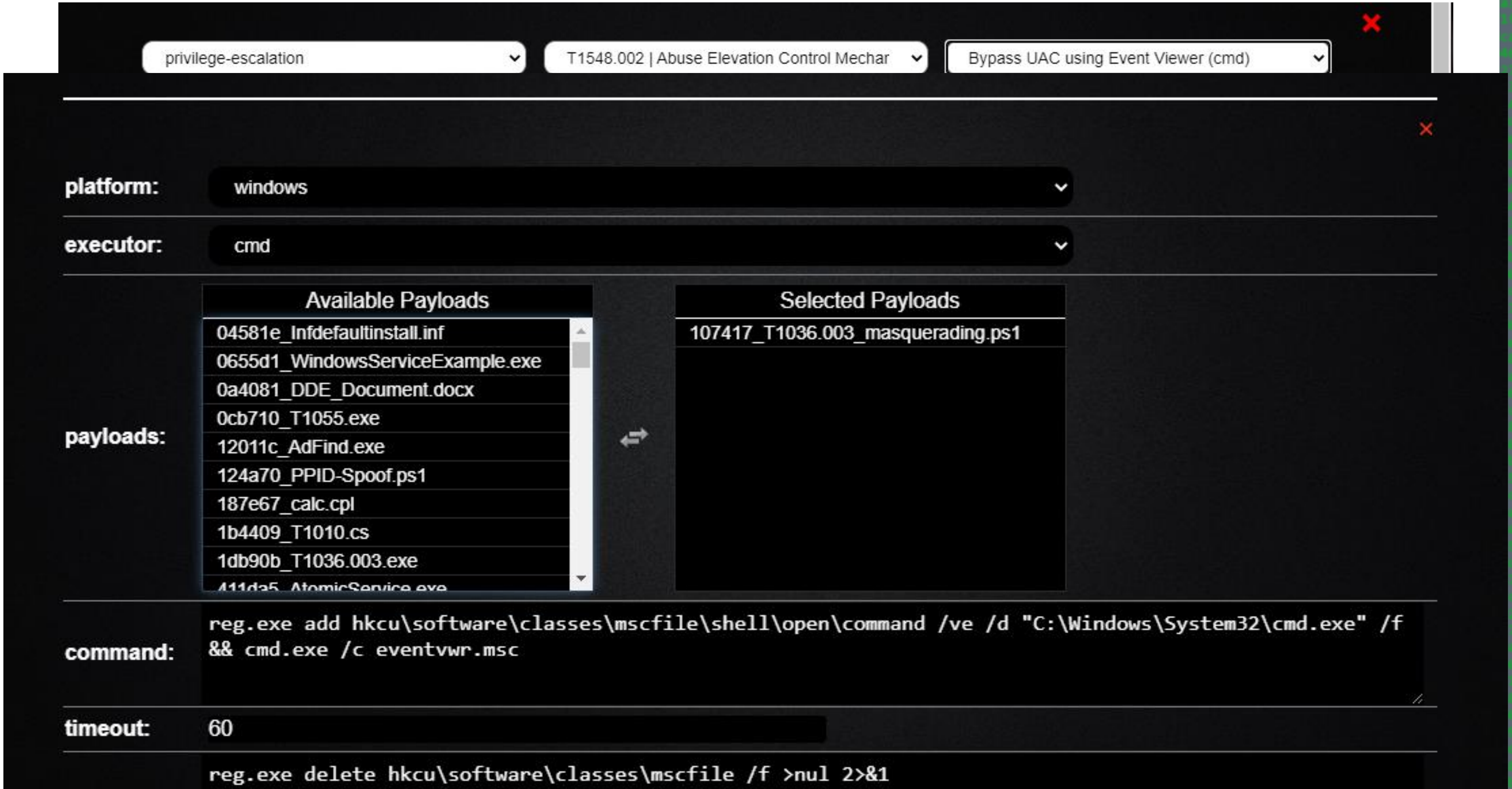
9 Discover antivirus programs
DISCOVERY | SOFTWARE DISCOVERY: SE...

10 Permission Groups Discovery
DISCOVERY | PERMISSION GROUPS DISC...

11 Identify Firewalls
DISCOVERY | SOFTWARE DISCOVERY: SE...

12 Discover Mail Server
DISCOVERY | REMOTE SYSTEM DISCOVE...

CALDERA – Adversary Profiles – Add Ability



privilege-escalation

T1548.002 | Abuse Elevation Control Mechar

Bypass UAC using Event Viewer (cmd)

platform: windows

executor: cmd

payloads:

Available Payloads
- 04581e_Infdefaultinstall.inf
- 0655d1_WindowsServiceExample.exe
- 0a4081_DDE_Document.docx
- 0cb710_T1055.exe
- 12011c_AdFind.exe
- 124a70_PPID-Spoof.ps1
- 187e67_calc.cpl
- 1b4409_T1010.cs
- 1db90b_T1036.003.exe
- 411da5_AtomicService.exe

Selected Payloads
- 107417_T1036.003_masquerading.ps1

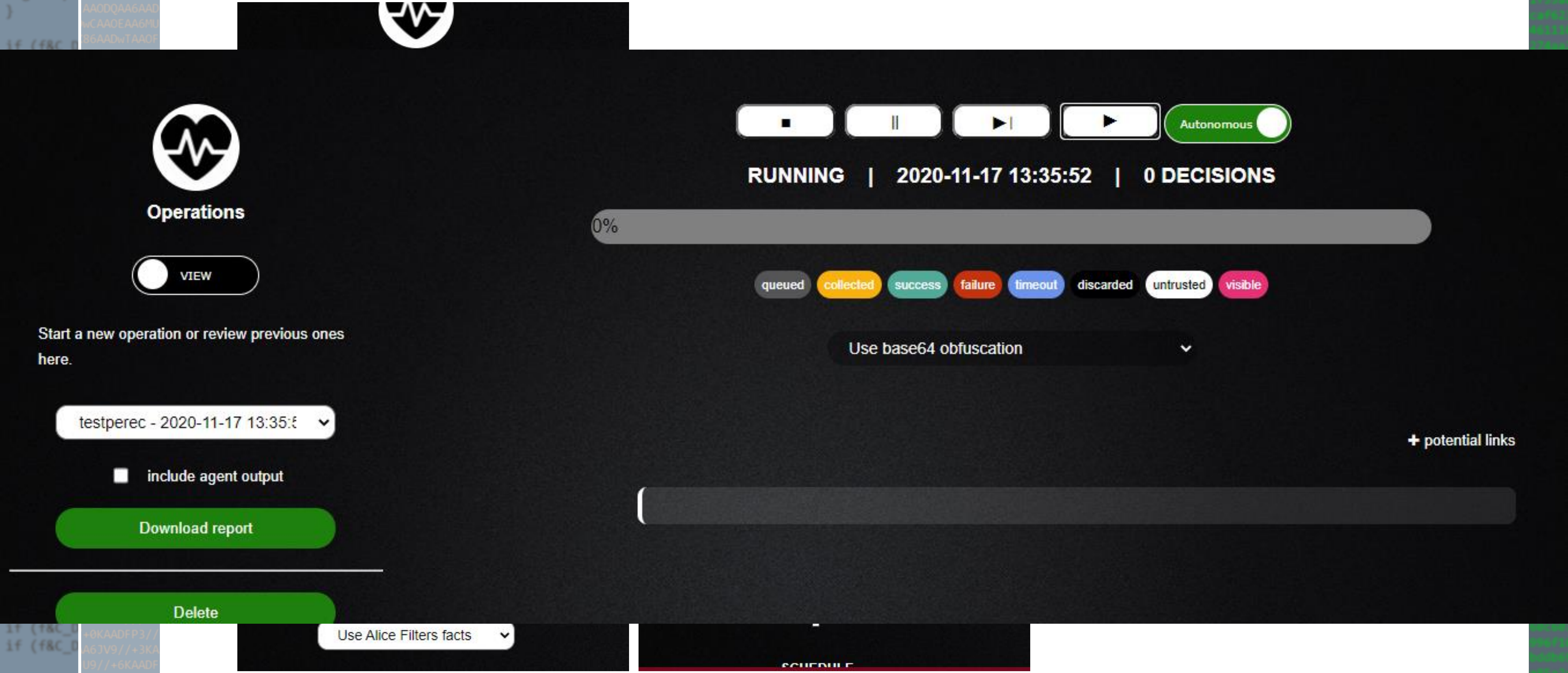
command:

```
reg.exe add hkcu\software\classes\mscfile\shell\open\command /ve /d "C:\Windows\System32\cmd.exe" /f
&& cmd.exe /c eventvwr.msc
```

timeout: 60

```
reg.exe delete hkcu\software\classes\mscfile /f >nul 2>&1
```

CALDERA – Run Operation



Operations

VIEW

Start a new operation or review previous ones here.

testperec - 2020-11-17 13:35:5

☐ include agent output

Download report

Delete

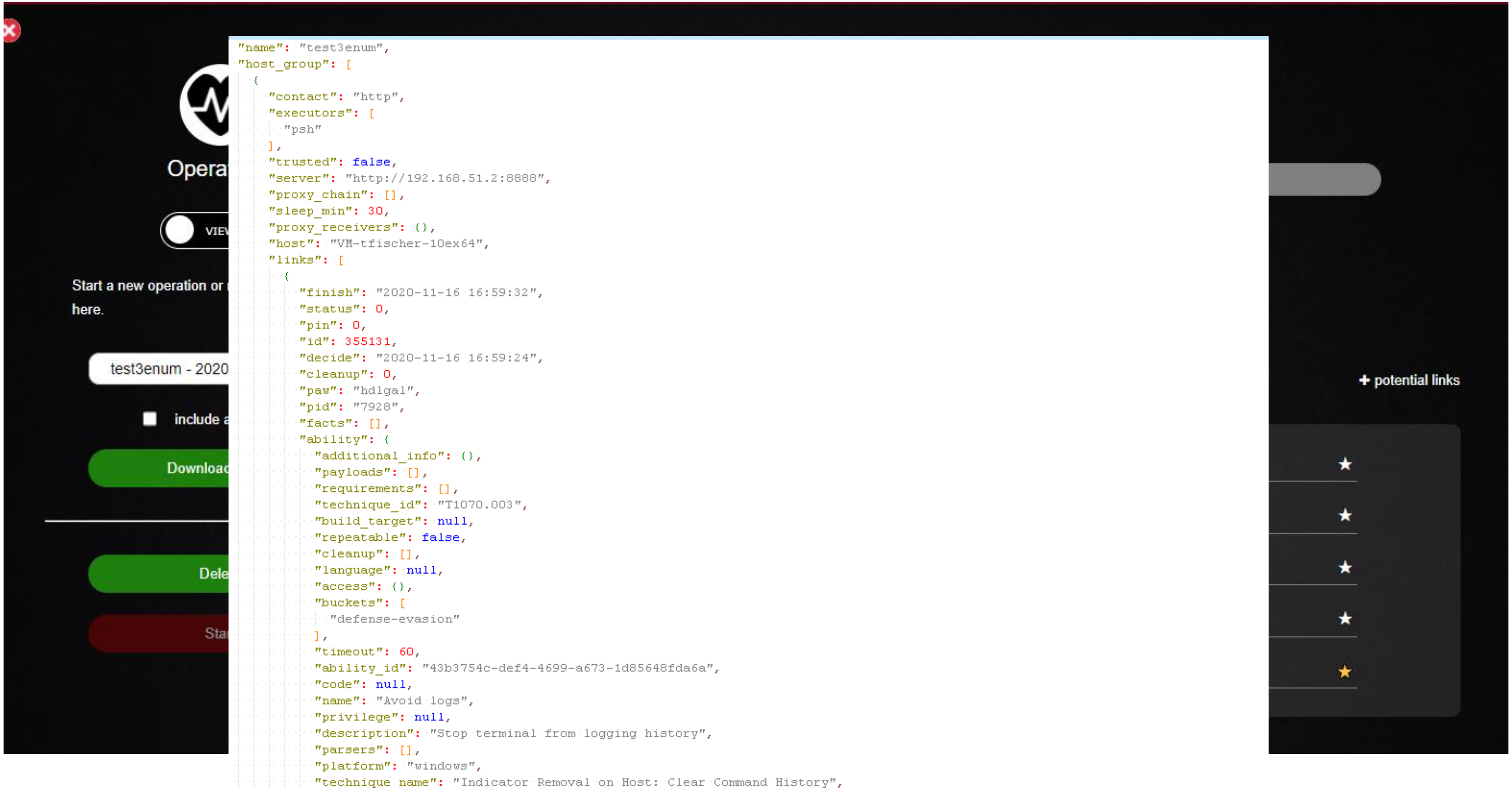
Use Alice Filters facts

RUNNING | 2020-11-17 13:35:52 | 0 DECISIONS

0%

Use base64 obfuscation

CALDERA – Run Operation



```
"name": "test3enum",
"host_group": [
  {
    "contact": "http",
    "executors": [
      "psh"
    ],
    "trusted": false,
    "server": "http://192.168.51.2:8888",
    "proxy_chain": [],
    "sleep_min": 30,
    "proxy_receivers": {},
    "host": "VM-tfischer-10ex64",
    "links": [
      {
        "finish": "2020-11-16 16:59:32",
        "status": 0,
        "pin": 0,
        "id": 355131,
        "decide": "2020-11-16 16:59:24",
        "cleanup": 0,
        "paw": "hdlgal",
        "pid": "7928",
        "facts": [],
        "ability": {
          "additional_info": {},
          "payloads": [],
          "requirements": [],
          "technique_id": "T1070.003",
          "build_target": null,
          "repeatable": false,
          "cleanup": [],
          "language": null,
          "access": {},
          "buckets": [
            "defense-evasion"
          ],
          "timeout": 60,
          "ability_id": "43b3754c-def4-4699-a673-1d85648fda6a",
          "code": null,
          "name": "Avoid logs",
          "privilege": null,
          "description": "Stop terminal from logging history",
          "parsers": [],
          "platform": "windows",
          "technique_name": "Indicator Removal on Host: Clear Command History",
```

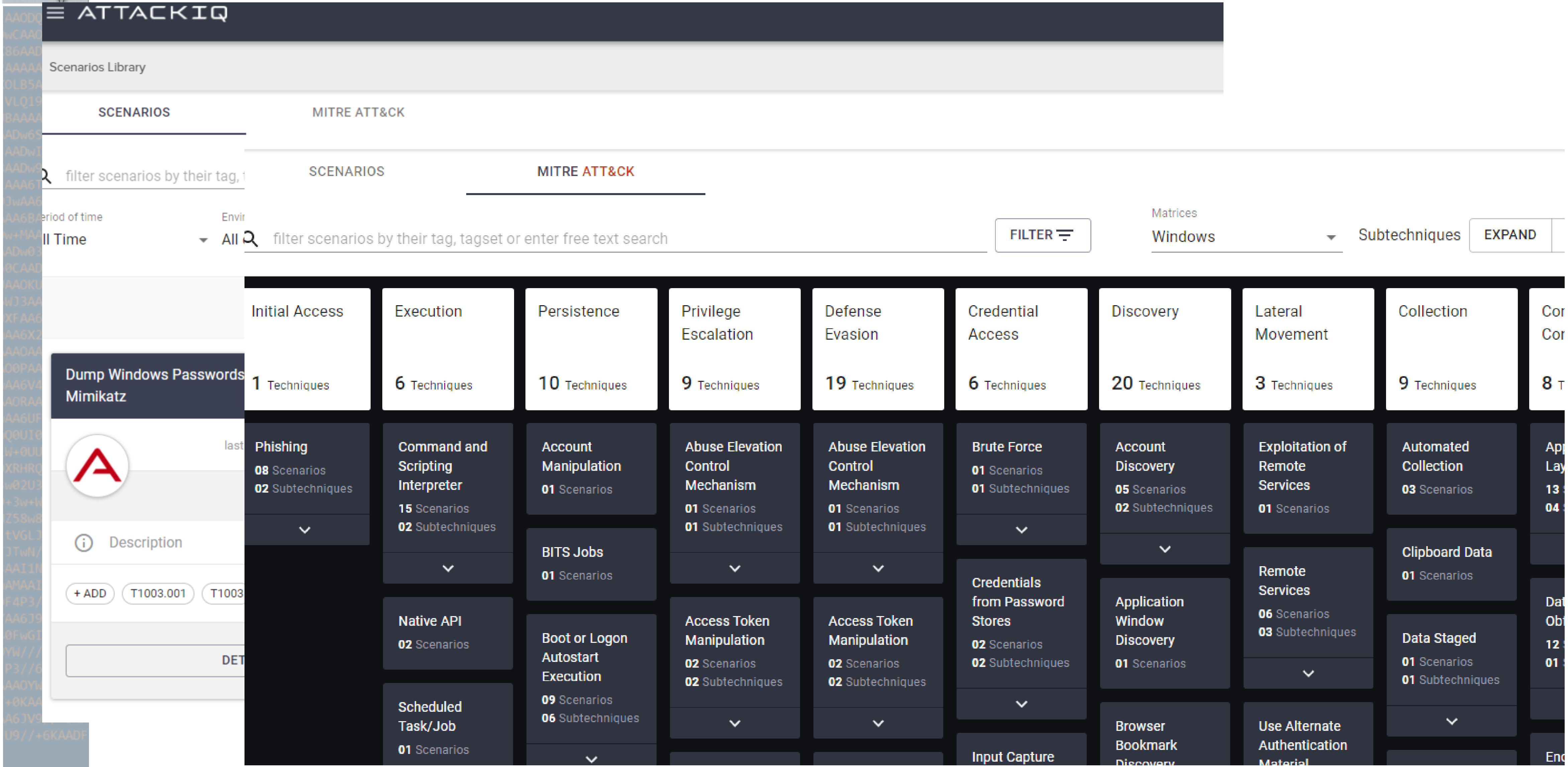
OFFENSIVEDEFENSE

AttackIQ delivers continuous validation of your enterprise security program so you can find the gaps, strengthen your security posture and exercise your incident response capabilities.

ATTACKIQ

Overview – Commercial Product €€€

ATTACKIQ - Scenarios



Scenarios Library

SCENARIOS | MITRE ATT&CK

filter scenarios by their tag, t

eriod of time: ll Time

Envir: All

Dump Windows Passwords Mimikatz

last

Description

+ ADD | T1003.001 | T1003

DET

SCENARIOS | MITRE ATT&CK

filter scenarios by their tag, tagset or enter free text search

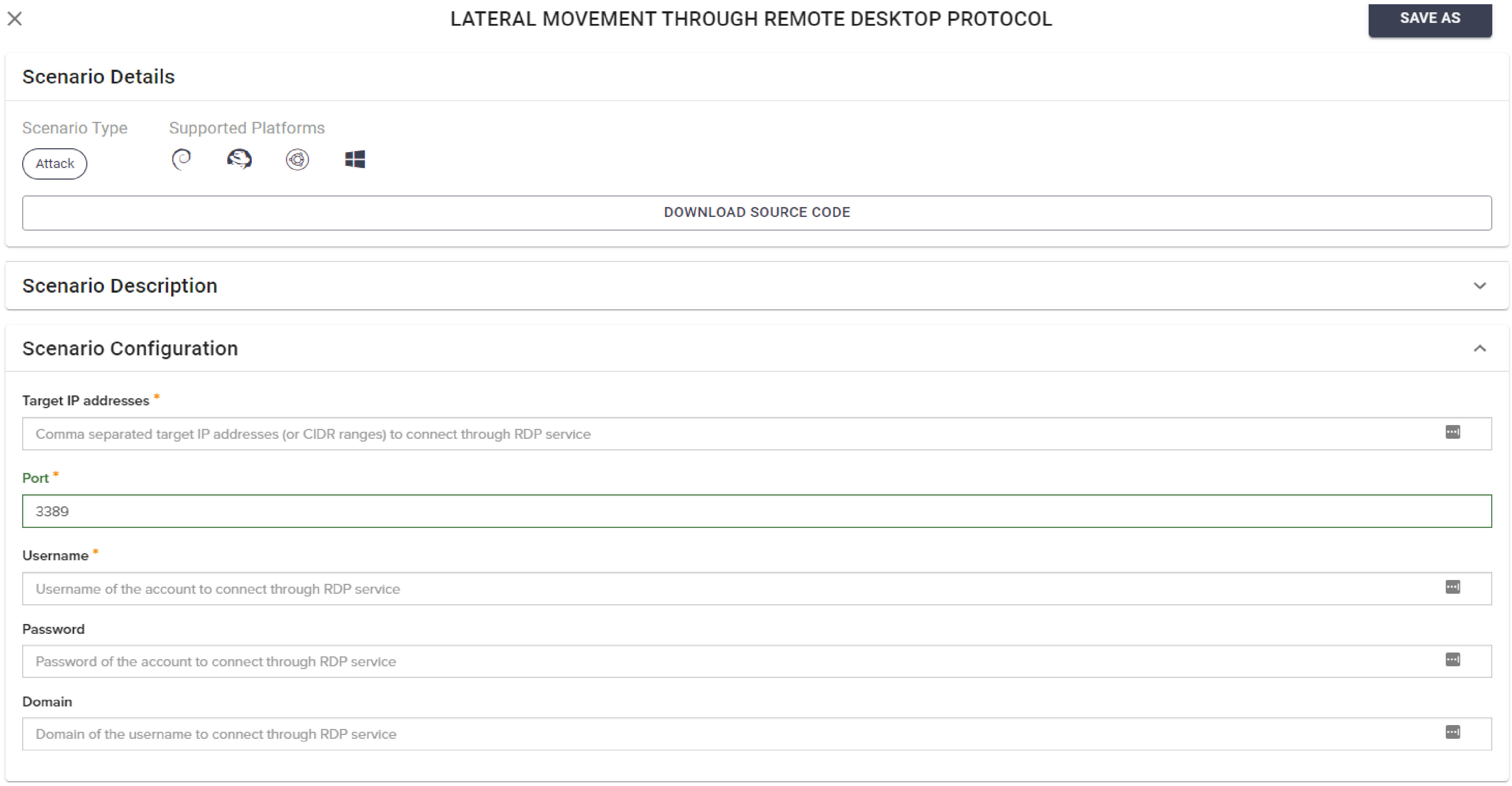
FILTER

Matrices: Windows

Subtechniques | EXPAND

Initial Access 1 Techniques	Execution 6 Techniques	Persistence 10 Techniques	Privilege Escalation 9 Techniques	Defense Evasion 19 Techniques	Credential Access 6 Techniques	Discovery 20 Techniques	Lateral Movement 3 Techniques	Collection 9 Techniques	Cor Cor 8 T
Phishing 08 Scenarios 02 Subtechniques	Command and Scripting Interpreter 15 Scenarios 02 Subtechniques	Account Manipulation 01 Scenarios	Abuse Elevation Control Mechanism 01 Scenarios 01 Subtechniques	Abuse Elevation Control Mechanism 01 Scenarios 01 Subtechniques	Brute Force 01 Scenarios 01 Subtechniques	Account Discovery 05 Scenarios 02 Subtechniques	Exploitation of Remote Services 01 Scenarios	Automated Collection 03 Scenarios	App Lay 13 04
	Native API 02 Scenarios	BITS Jobs 01 Scenarios	Access Token Manipulation 02 Scenarios 02 Subtechniques	Access Token Manipulation 02 Scenarios 02 Subtechniques	Credentials from Password Stores 02 Scenarios 02 Subtechniques	Application Window Discovery 01 Scenarios	Remote Services 06 Scenarios 03 Subtechniques	Clipboard Data 01 Scenarios	Dat Obf 12 01
	Scheduled Task/Job 01 Scenarios	Boot or Logon Autostart Execution 09 Scenarios 06 Subtechniques			Input Capture	Browser Bookmark Discovery	Use Alternate Authentication Material	Data Staged 01 Scenarios 01 Subtechniques	Enc

ATTACKIQ – Scenarios Detail



LATERAL MOVEMENT THROUGH REMOTE DESKTOP PROTOCOL

SAVE AS

Scenario Details

Scenario Type: Attack

Supported Platforms

DOWNLOAD SOURCE CODE

Scenario Description

Scenario Configuration

Target IP addresses *

Comma separated target IP addresses (or CIDR ranges) to connect through RDP service

Port *

3389

Username *

Username of the account to connect through RDP service

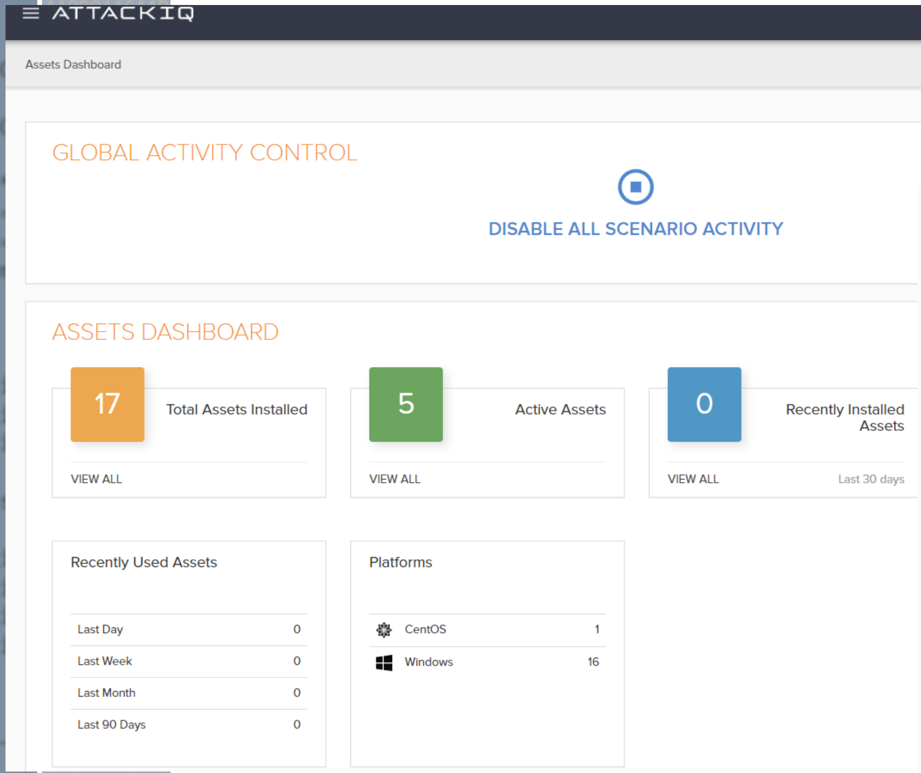
Password

Password of the account to connect through RDP service

Domain

Domain of the username to connect through RDP service

ATTACKIQ - Agents



Assets Dashboard

GLOBAL ACTIVITY CONTROL

DISABLE ALL SCENARIO ACTIVITY

ASSETS DASHBOARD

17 Total Assets Installed
VIEW ALL

5 Active Assets
VIEW ALL

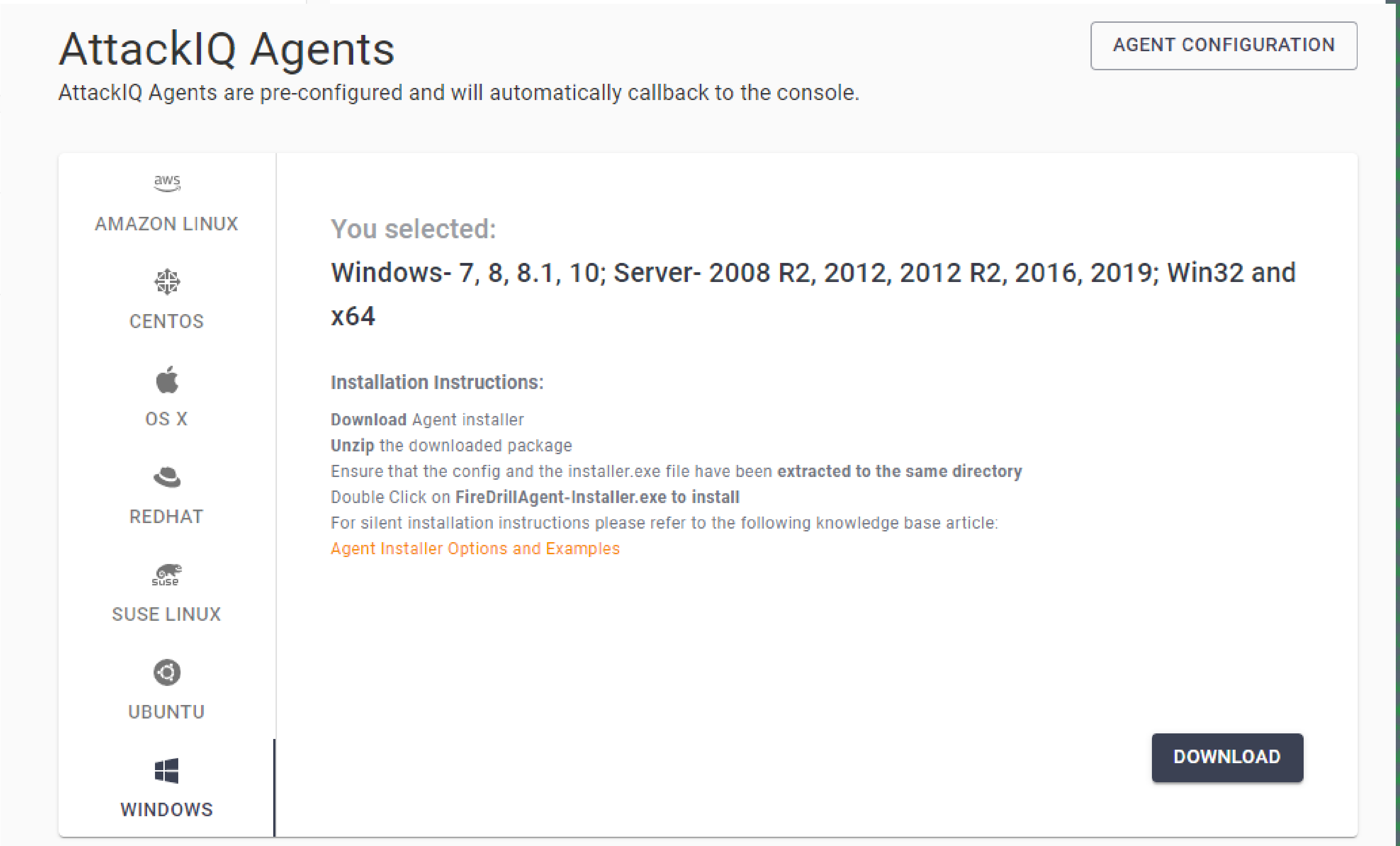
0 Recently Installed Assets
VIEW ALL Last 30 days

Recently Used Assets

Last Day	0
Last Week	0
Last Month	0
Last 90 Days	0

Platforms

CentOS	1
Windows	16



AttackIQ Agents

AttackIQ Agents are pre-configured and will automatically callback to the console.

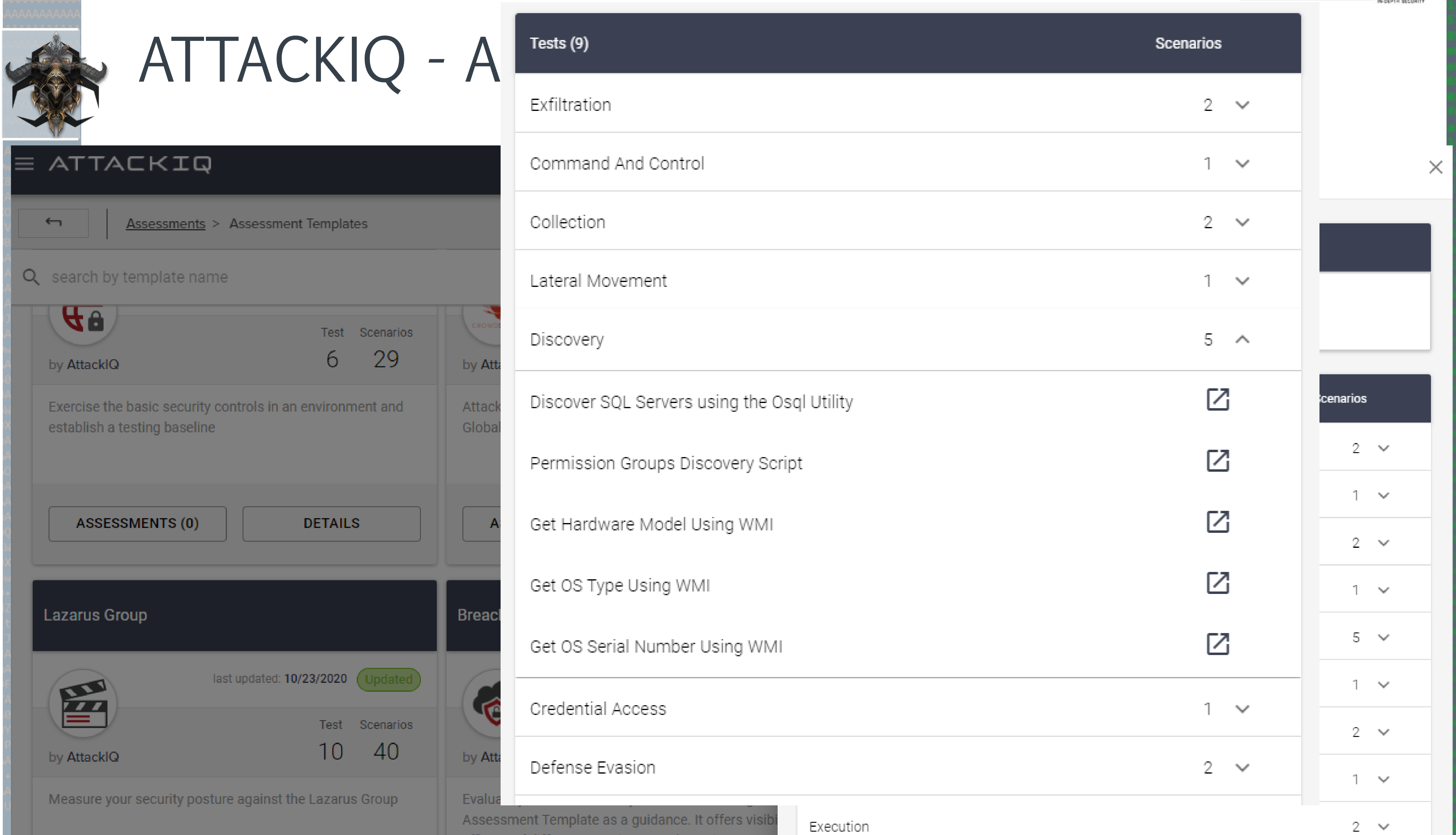
You selected:

Windows- 7, 8, 8.1, 10; Server- 2008 R2, 2012, 2012 R2, 2016, 2019; Win32 and x64

Installation Instructions:

Download Agent installer
Unzip the downloaded package
Ensure that the config and the installer.exe file have been **extracted to the same directory**
Double Click on **FireDrillAgent-Installer.exe to install**
For silent installation instructions please refer to the following knowledge base article:
Agent Installer Options and Examples

ATTACKIQ - A



Assessments > Assessment Templates

search by template name

by AttackIQ

Test	Scenarios
6	29

Exercise the basic security controls in an environment and establish a testing baseline

Lazarus Group

last updated: 10/23/2020 Updated

by AttackIQ

Test	Scenarios
10	40

Measure your security posture against the Lazarus Group

Breac

by Att

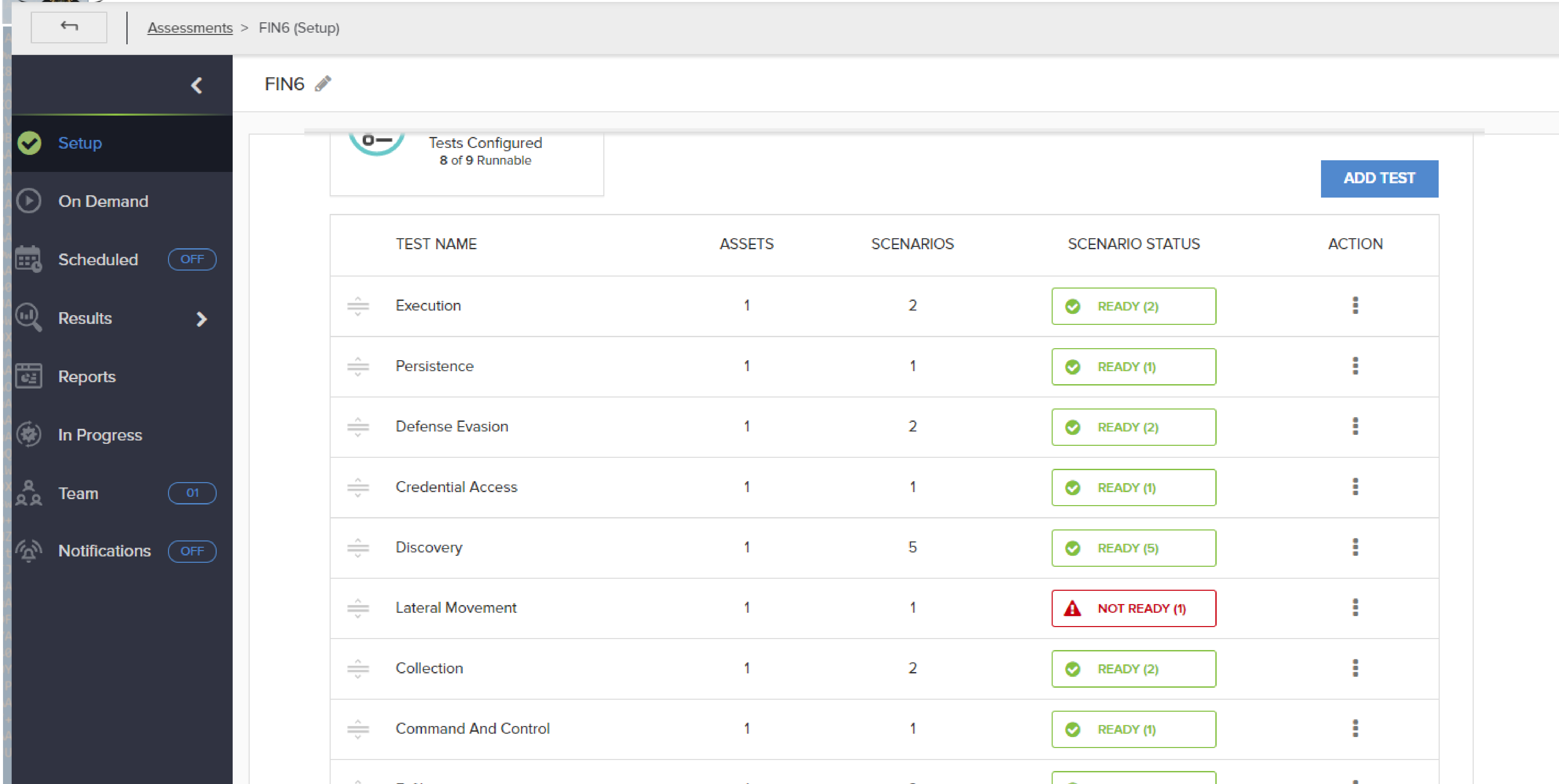
Attack
Global

Evalua
Assessment Template as a guidance. It offers visibi

Tests (9)	Scenarios
Exfiltration	2
Command And Control	1
Collection	2
Lateral Movement	1
Discovery	5
Discover SQL Servers using the Osql Utility	
Permission Groups Discovery Script	
Get Hardware Model Using WMI	
Get OS Type Using WMI	
Get OS Serial Number Using WMI	
Credential Access	1
Defense Evasion	2

	cenarios
	2
	1
	2
	1
	5
	1
	2
	1
Execution	2

ATTACKIQ – Assessments Plan

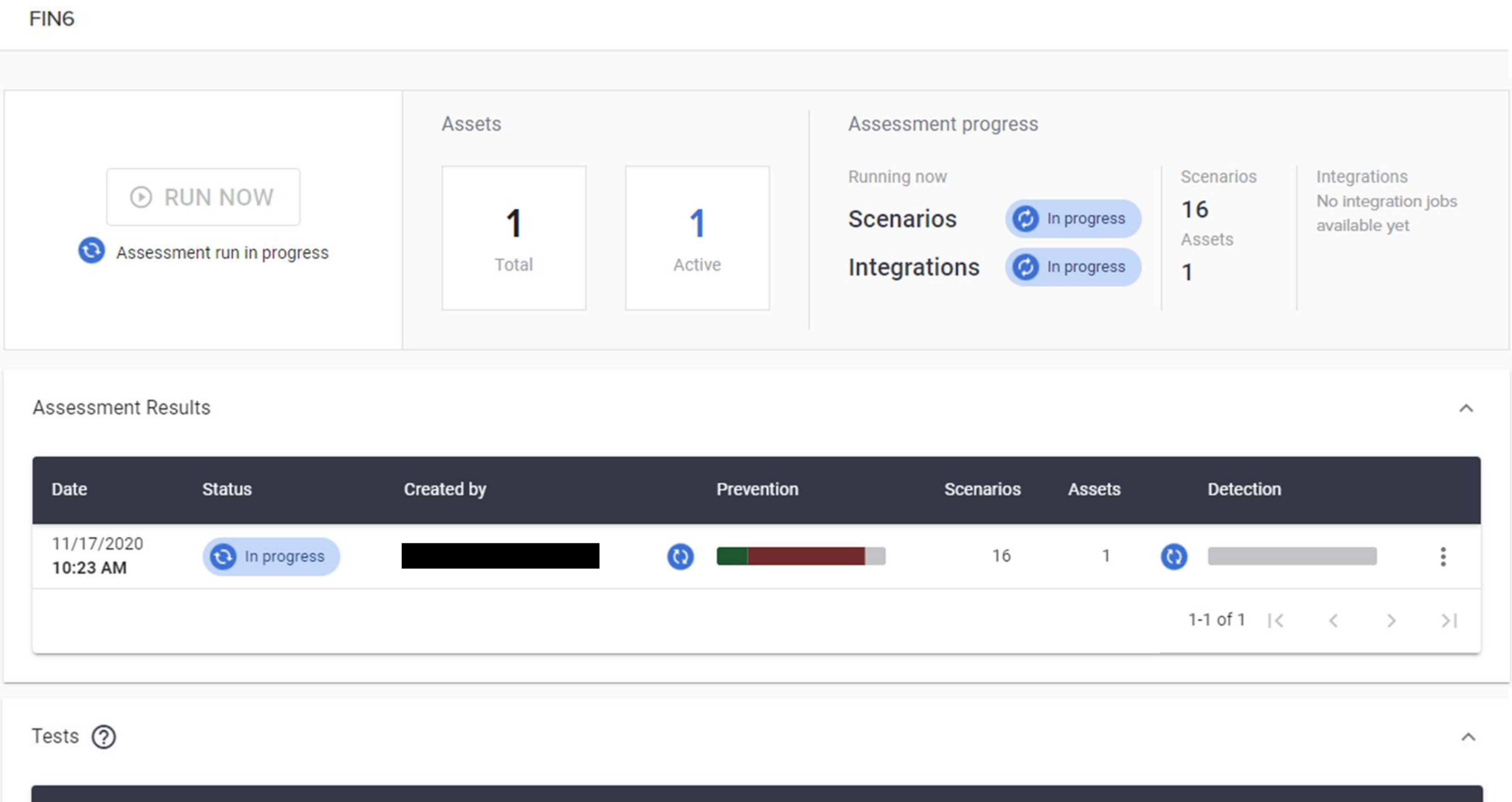


FIN6

Tests Configured
8 of 9 Runnable

TEST NAME	ASSETS	SCENARIOS	SCENARIO STATUS	ACTION
Execution	1	2	READY (2)	⋮
Persistence	1	1	READY (1)	⋮
Defense Evasion	1	2	READY (2)	⋮
Credential Access	1	1	READY (1)	⋮
Discovery	1	5	READY (5)	⋮
Lateral Movement	1	1	NOT READY (1)	⋮
Collection	1	2	READY (2)	⋮
Command And Control	1	1	READY (1)	⋮

ATTACKIQ – Assessment Run



FIN6

RUN NOW

Assessment run in progress

Assets

1 Total	1 Active

Assessment progress

Running now

Scenarios: In progress

Integrations: In progress

Scenarios
16

Assets
1

Integrations
No integration jobs available yet

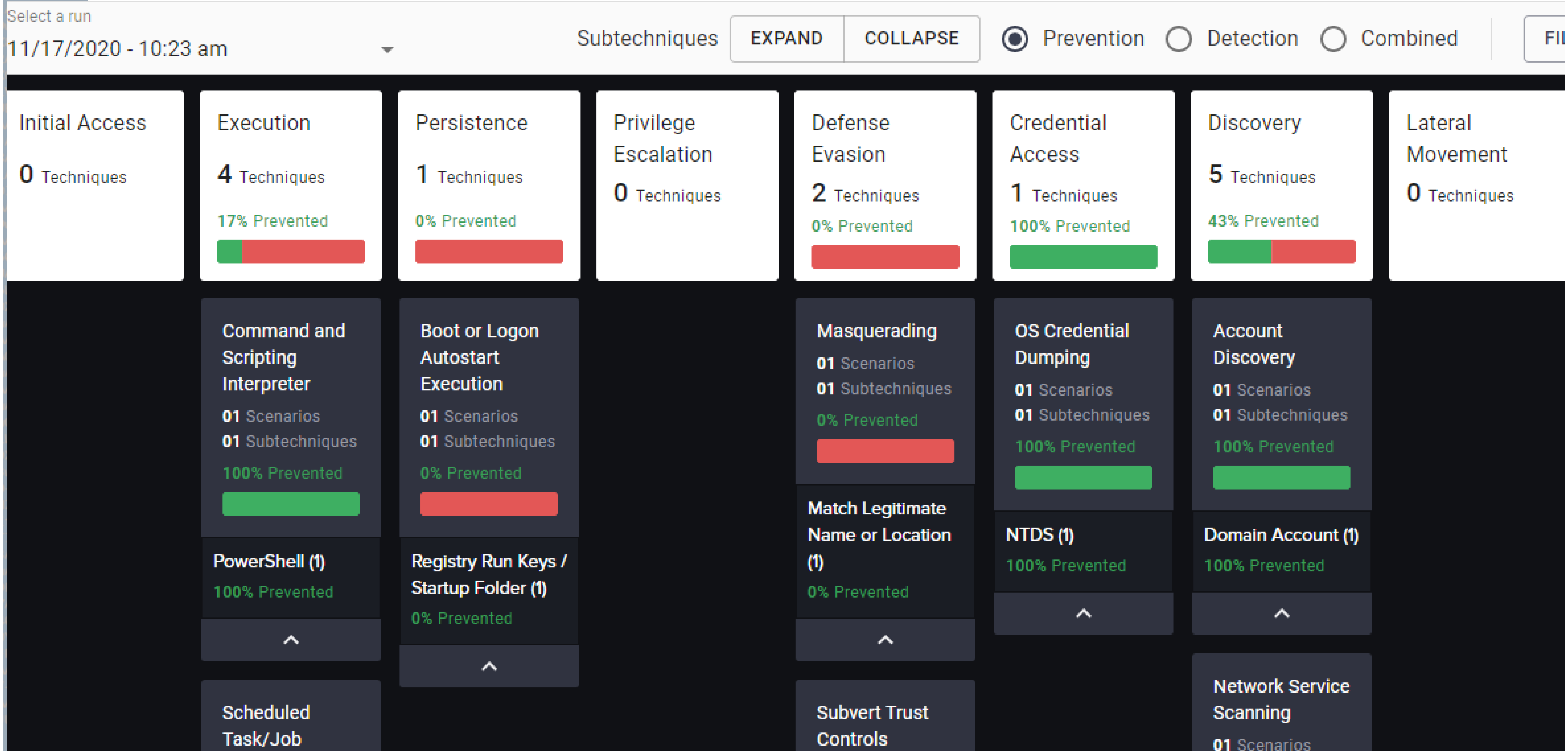
Assessment Results

Date	Status	Created by	Prevention	Scenarios	Assets	Detection
11/17/2020 **10:23 AM**	In progress	[redacted]		16	1	

1-1 of 1

Tests

ATTACKIQ - Report



Select a run
11/17/2020 - 10:23 am

Subtechniques EXPAND COLLAPSE ● Prevention ○ Detection ○ Combined FII

Initial Access
0 Techniques

Execution
4 Techniques
17% Prevented

- Command and Scripting Interpreter
  01 Scenarios
  01 Subtechniques
  100% Prevented
  - PowerShell (1)
    100% Prevented
- Scheduled Task/Job

Persistence
1 Techniques
0% Prevented

- Boot or Logon Autostart Execution
  01 Scenarios
  01 Subtechniques
  0% Prevented
  - Registry Run Keys / Startup Folder (1)
    0% Prevented

Privilege Escalation
0 Techniques

Defense Evasion
2 Techniques
0% Prevented

- Masquerading
  01 Scenarios
  01 Subtechniques
  0% Prevented
  - Match Legitimate Name or Location (1)
    0% Prevented
- Subvert Trust Controls

Credential Access
1 Techniques
100% Prevented

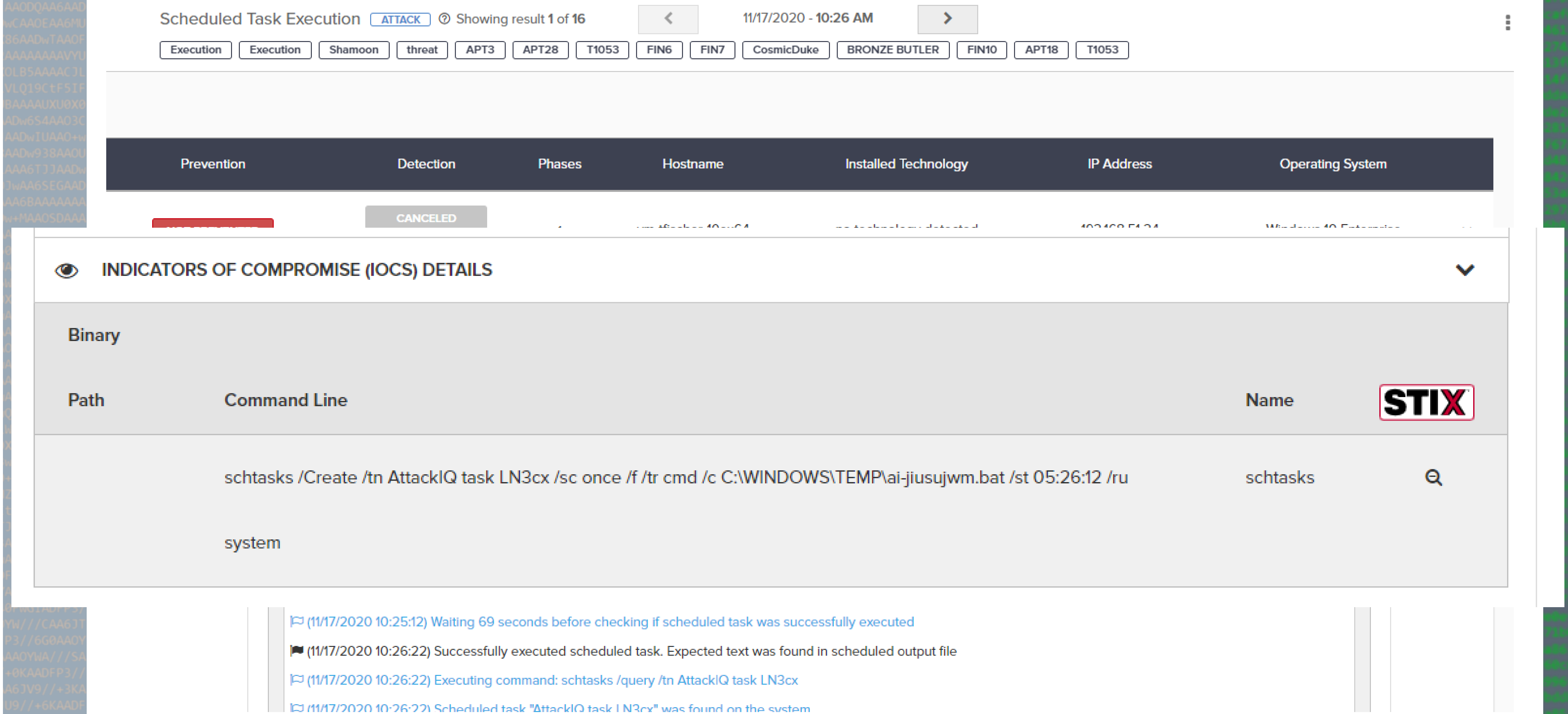
- OS Credential Dumping
  01 Scenarios
  01 Subtechniques
  100% Prevented
  - NTDS (1)
    100% Prevented

Discovery
5 Techniques
43% Prevented

- Account Discovery
  01 Scenarios
  01 Subtechniques
  100% Prevented
  - Domain Account (1)
    100% Prevented
- Network Service Scanning
  01 Scenarios

Lateral Movement
0 Techniques

ATTACKIQ – Report Detail Action



Scheduled Task Execution ATTACK Showing result 1 of 16 11/17/2020 - 10:26 AM

Execution | Execution | Shamoon | threat | APT3 | APT28 | T1053 | FIN6 | FIN7 | CosmicDuke | BRONZE BUTLER | FIN10 | APT18 | T1053

Prevention	Detection	Phases	Hostname	Installed Technology	IP Address	Operating System
	CANCELED					

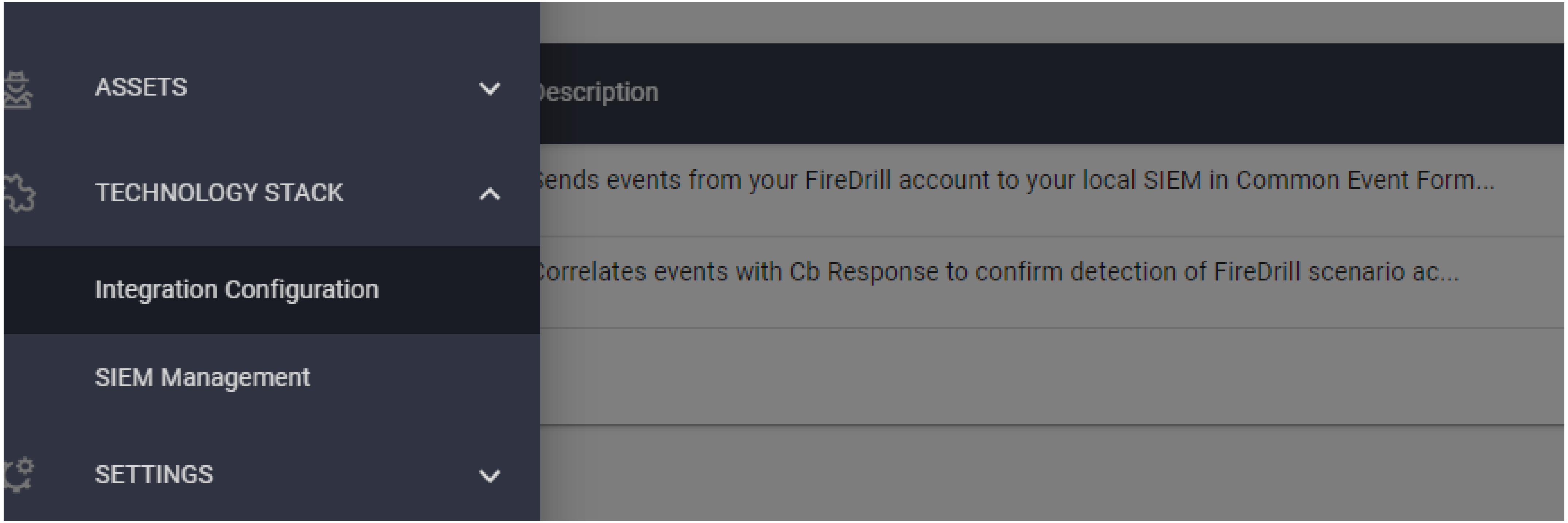
INDICATORS OF COMPROMISE (IOCS) DETAILS

Binary

Path	Command Line	Name	STIX
	schtasks /Create /tn AttackIQ task LN3cx /sc once /f /tr cmd /c C:\WINDOWS\TEMP\ai-jiusujwm.bat /st 05:26:12 /ru system	schtasks	

```
(11/17/2020 10:25:12) Waiting 69 seconds before checking if scheduled task was successfully executed
(11/17/2020 10:26:22) Successfully executed scheduled task. Expected text was found in scheduled output file
(11/17/2020 10:26:22) Executing command: schtasks /query /tn AttackIQ task LN3cx
(11/17/2020 10:26:22) Scheduled task "AttackIQ task LN3cx" was found on the system
```

ATTACKIQ - Integrations

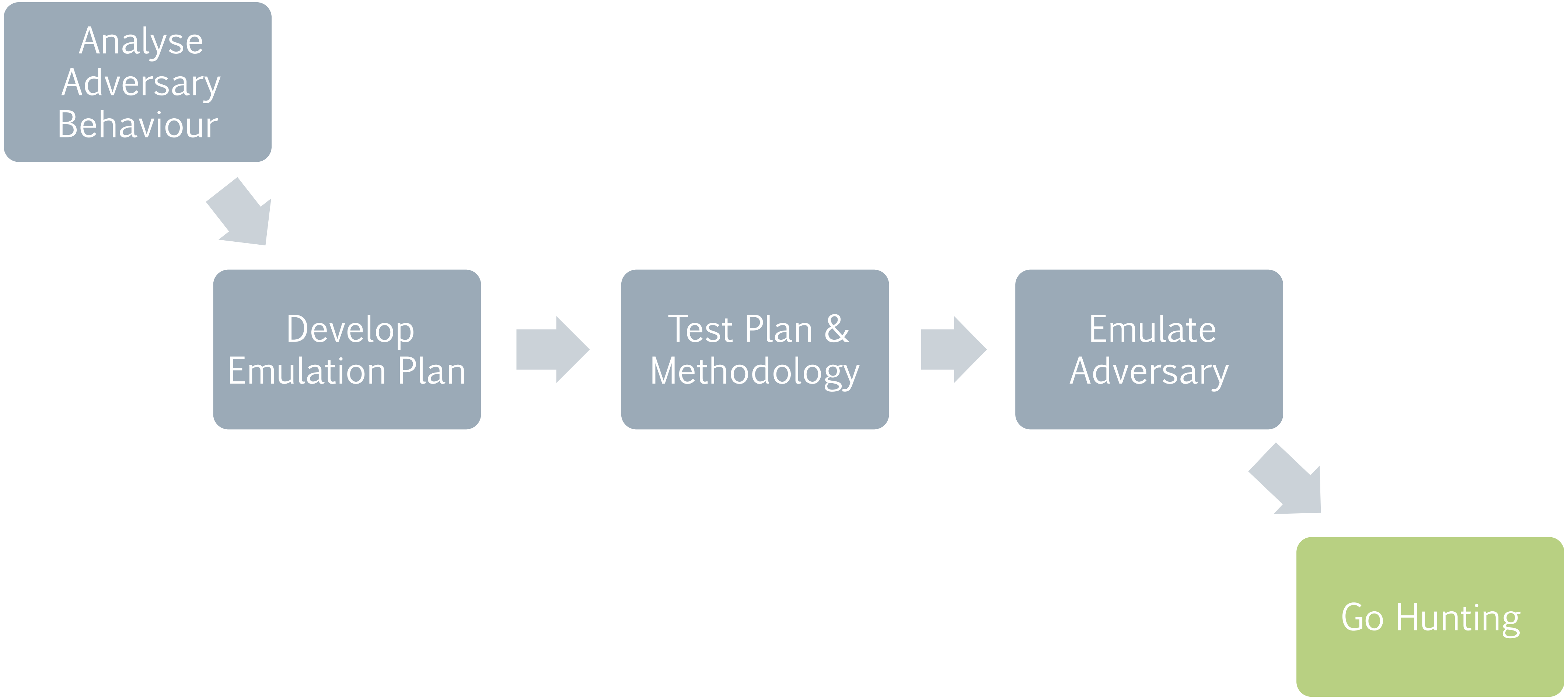


Description
ends events from your FireDrill account to your local SIEM in Common Event Form...
orrelates events with Cb Response to confirm detection of FireDrill scenario ac...

```
C_ERROR)

zeptr=C_ER
rn;


C_PREFIX)

C_PREFIX;
 prefix;


C_DATAW0)

C_MODRM)

*iptr++;
= b & 0xC0
= b & 0x07
mod!=0xC0)

 (f&C_67)

if ((mod==
if (mod==0
if (mod==0

se

if (mod==0
if (mod==0
if (rm==0x
if ((rm==0


_MODRM

C_MEM67)
C_DATA66)

C_MEM1)  i
C_MEM2)  i
C_MEM4)  i

C_DATA1) i
C_DATA2) i
C_DATA4) i
```

AAAAAA
AAAAAA
AAAAAA
AAAAAA
AAAAAA
AAAAAA
AAAAAA
AAAAAA
2AAOQA
YTAAA6
J0AAOL
5UZAAD
wOX4AA
AAAAAC
AAA61A
1D7DSL
JTCJRL
9MF9AA
BEAJRt
wAA6UE
AA6UAA
EAAA6Y
JAAO+D
wVYAAC
A6QAAD
AAA6UP
AAAAAA
YwAA6T
AADwD2
/XAAA6
w23IAA
D0AA6X
L2IAAC
w1AAON
AAAOLQ
wWAAOX
AO+JAA
AIF/It
BUID1A
0XE0XC
KLHRAA
J82JXD
YtFA++
wAAAQB
ItNIwV
L5tKtT
NKAADV
DYX///
ADFP3/
/6GQAA
9//+wK
NQ///A
A6JX9/
40FHGM
ADFWP3

So Go Hunt



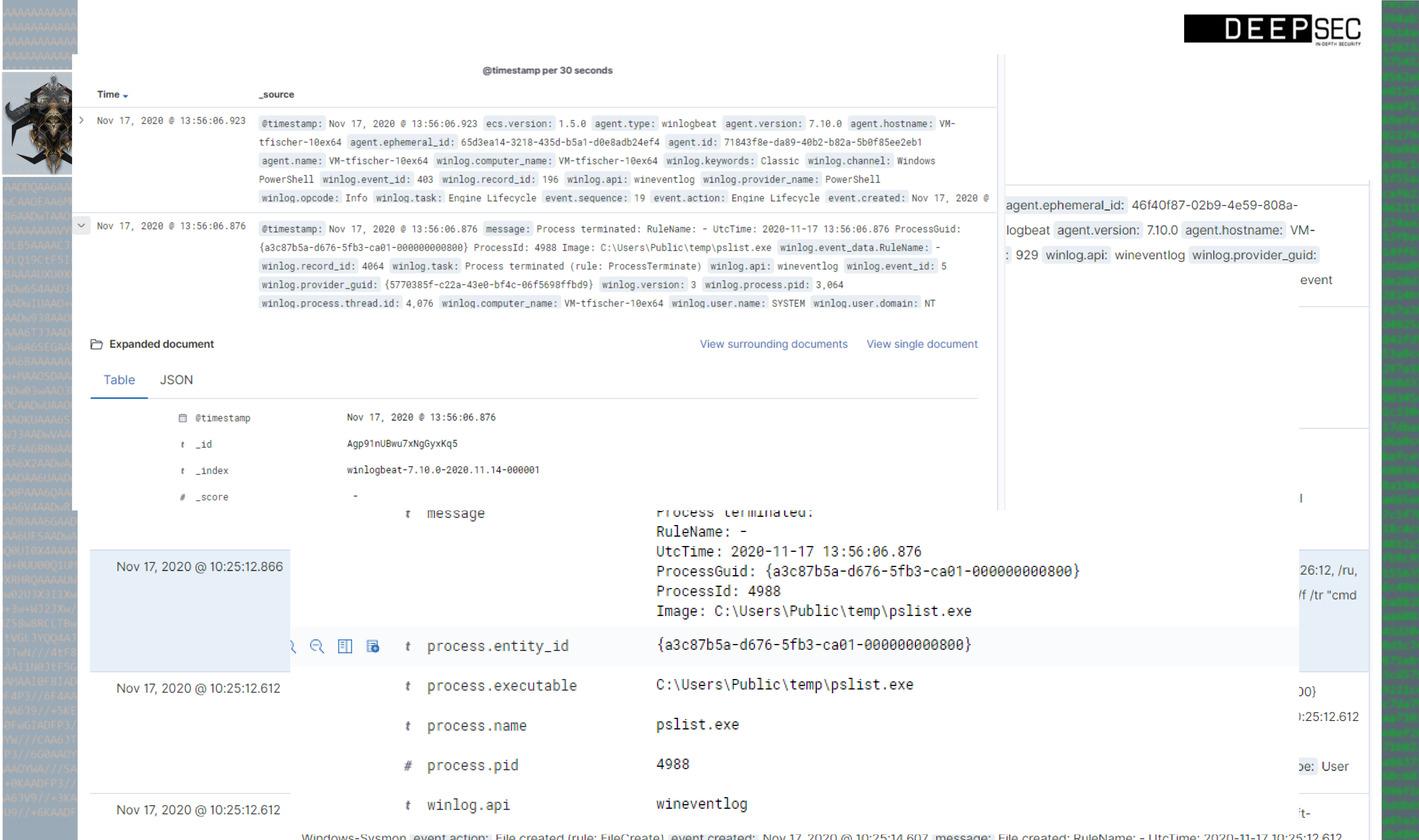
Analyse Adversary Behaviour

Develop Emulation Plan

Test Plan & Methodology

Emulate Adversary

Go Hunting



DEEPSEC IN-DEPTH SECURITY

@timestamp per 30 seconds

Time	_source
Nov 17, 2020 @ 13:56:06.923	@timestamp: Nov 17, 2020 @ 13:56:06.923 ecs.version: 1.5.0 agent.type: winlogbeat agent.version: 7.10.0 agent.hostname: VM-tfischer-10ex64 agent.ephemeral_id: 65d3ea14-3218-435d-b5a1-d0e8adb24ef4 agent.id: 71843f8e-da89-40b2-b82a-5b0f85ee2eb1 agent.name: VM-tfischer-10ex64 winlog.computer_name: VM-tfischer-10ex64 winlog.keywords: Classic winlog.channel: Windows PowerShell winlog.event_id: 403 winlog.record_id: 196 winlog.api: wineventlog winlog.provider_name: PowerShell winlog.opcode: Info winlog.task: Engine Lifecycle event.sequence: 19 event.action: Engine Lifecycle event.created: Nov 17, 2020 @
Nov 17, 2020 @ 13:56:06.876	@timestamp: Nov 17, 2020 @ 13:56:06.876 message: Process terminated: RuleName: - UtcTime: 2020-11-17 13:56:06.876 ProcessGuid: {a3c87b5a-d676-5fb3-ca01-000000000800} ProcessId: 4988 Image: C:\Users\Public\temp\pslist.exe winlog.event_data.RuleName: - winlog.record_id: 4064 winlog.task: Process terminated (rule: ProcessTerminate) winlog.api: wineventlog winlog.event_id: 5 winlog.provider_guid: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} winlog.version: 3 winlog.process.pid: 3,064 winlog.process.thread.id: 4,076 winlog.computer_name: VM-tfischer-10ex64 winlog.user.name: SYSTEM winlog.user.domain: NT

Expanded document

View surrounding documents View single document

Table JSON

@timestamp	Nov 17, 2020 @ 13:56:06.876
_id	Agp91nUBwu7xNgGyxKq5
_index	winlogbeat-7.10.0-2020.11.14-000001
_score	-
message	Process terminated: RuleName: - UtcTime: 2020-11-17 13:56:06.876 ProcessGuid: {a3c87b5a-d676-5fb3-ca01-000000000800} ProcessId: 4988 Image: C:\Users\Public\temp\pslist.exe
process.entity_id	{a3c87b5a-d676-5fb3-ca01-000000000800}
process.executable	C:\Users\Public\temp\pslist.exe
process.name	pslist.exe
process.pid	4988
winlog.api	wineventlog

agent.ephemeral_id: 46f40f87-02b9-4e59-808a-
logbeat agent.version: 7.10.0 agent.hostname: VM-
: 929 winlog.api: wineventlog winlog.provider_guid:
event

Nov 17, 2020 @ 10:25:12.866 26:12, /ru, /f /tr "cmd

Nov 17, 2020 @ 10:25:12.612 00} :25:12.612 pe: User

Nov 17, 2020 @ 10:25:12.612 ft-

Windows-Sysmon event.action: File created (rule: FileCreate) event.created: Nov 17, 2020 @ 10:25:14.607 message: File created: RuleName: - UtcTime: 2020-11-17 10:25:12.612

Closing thoughts

› Use adversary emulation to test your threat hunting program
  - Validate you have enough data points
  - Can you see the emulated adversaries' techniques
  - Develop plans during purple team exercise

› Match your emulation plans to threat intelligence
  - Target your activities to what matters
  - Use ATT&CK TTPs to simulate known actors
  - Improvise; TTPs can change over time

› Build a threat-based defense

> “identify pertinent information, prioritize it, draw conclusions from it, and communicate it...”
>
> *Amy E. Herman*

@Fvt

- tvfischer+sec@gmail.com
- tvfischer@pm.me
- keybase.io/fvt