

# SOC Homelab Project

## Objective

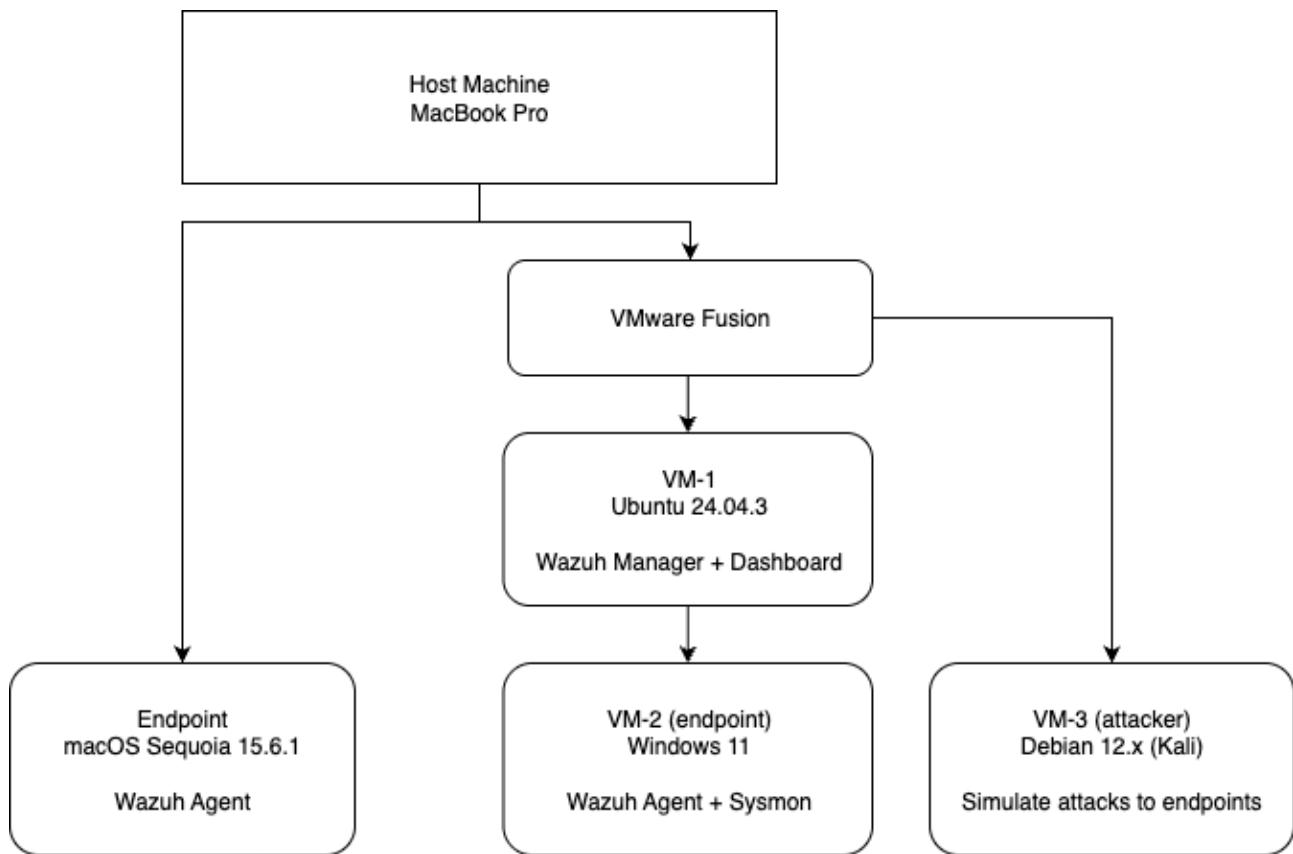
Build a SOC environment to practice endpoint monitoring, log analysis, and incident detection.

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

#### 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 endpoint. The user has run the command `sudo grep ^status /Library/Ossec/var/run/wazuh-agentd.state` and received the output: "status='connected'". The terminal window has a title bar 'raychiu -- zsh -- 100x29'.

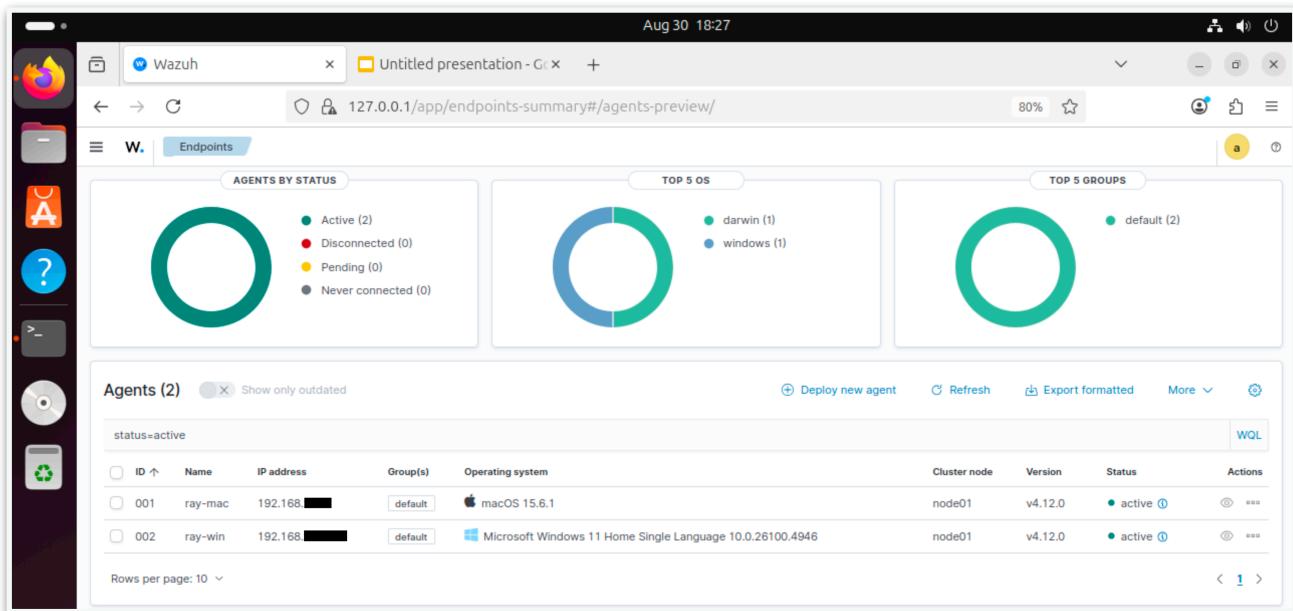
## Instance 2 - Ubuntu VM

- Installed Wazuh Manager + Dashboard

### Troubleshoot

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

Screenshot - Connected agents on Wazuh Dashboard on Ubuntu



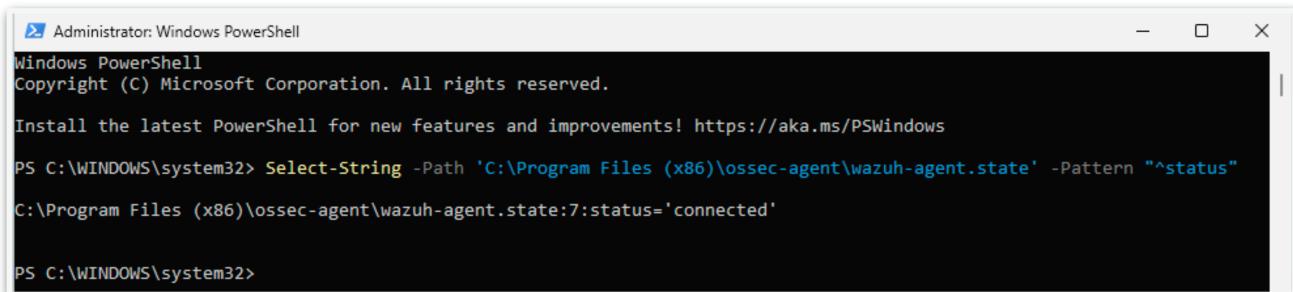
## Instance 3 - Windows VM

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

### Troubleshoot

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

### Screenshot - Wazuh agent status on Windows Endpoint



```

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

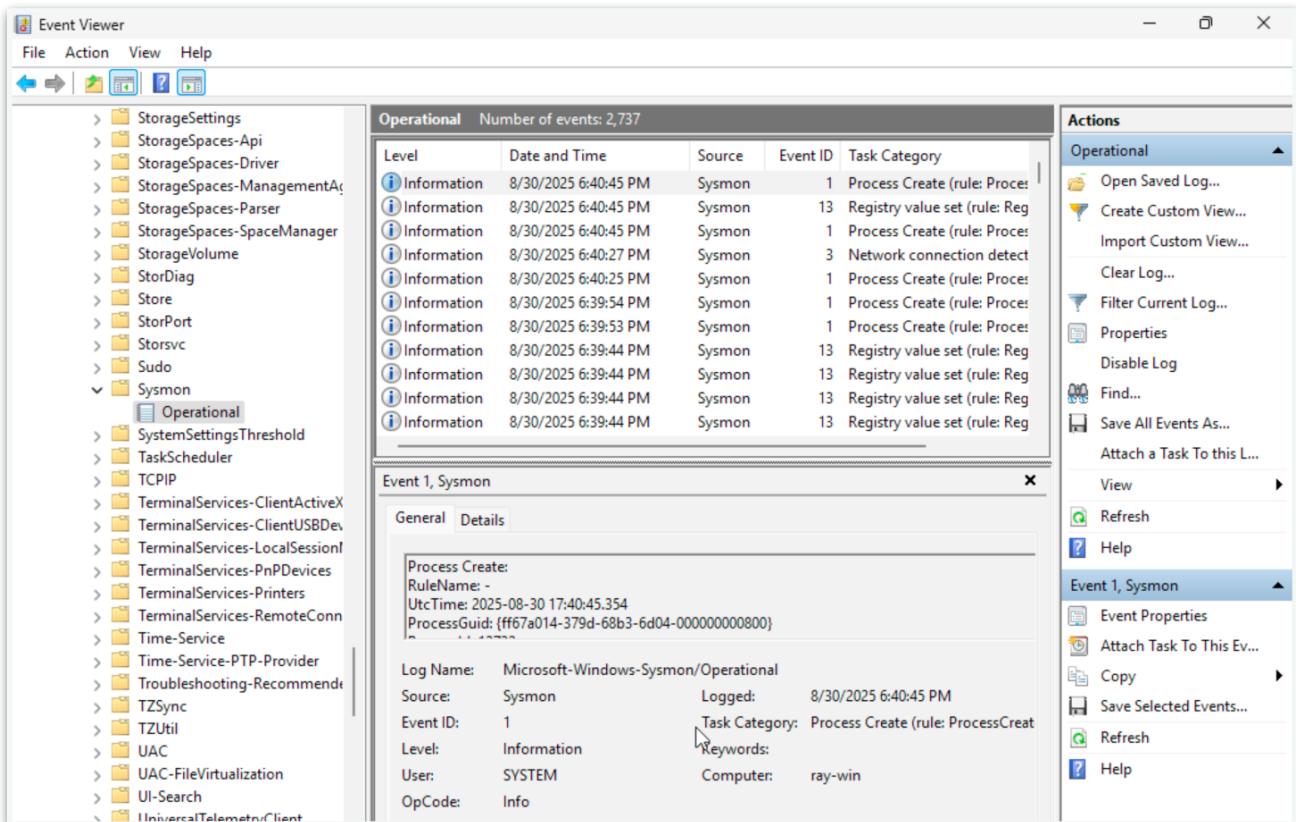
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

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

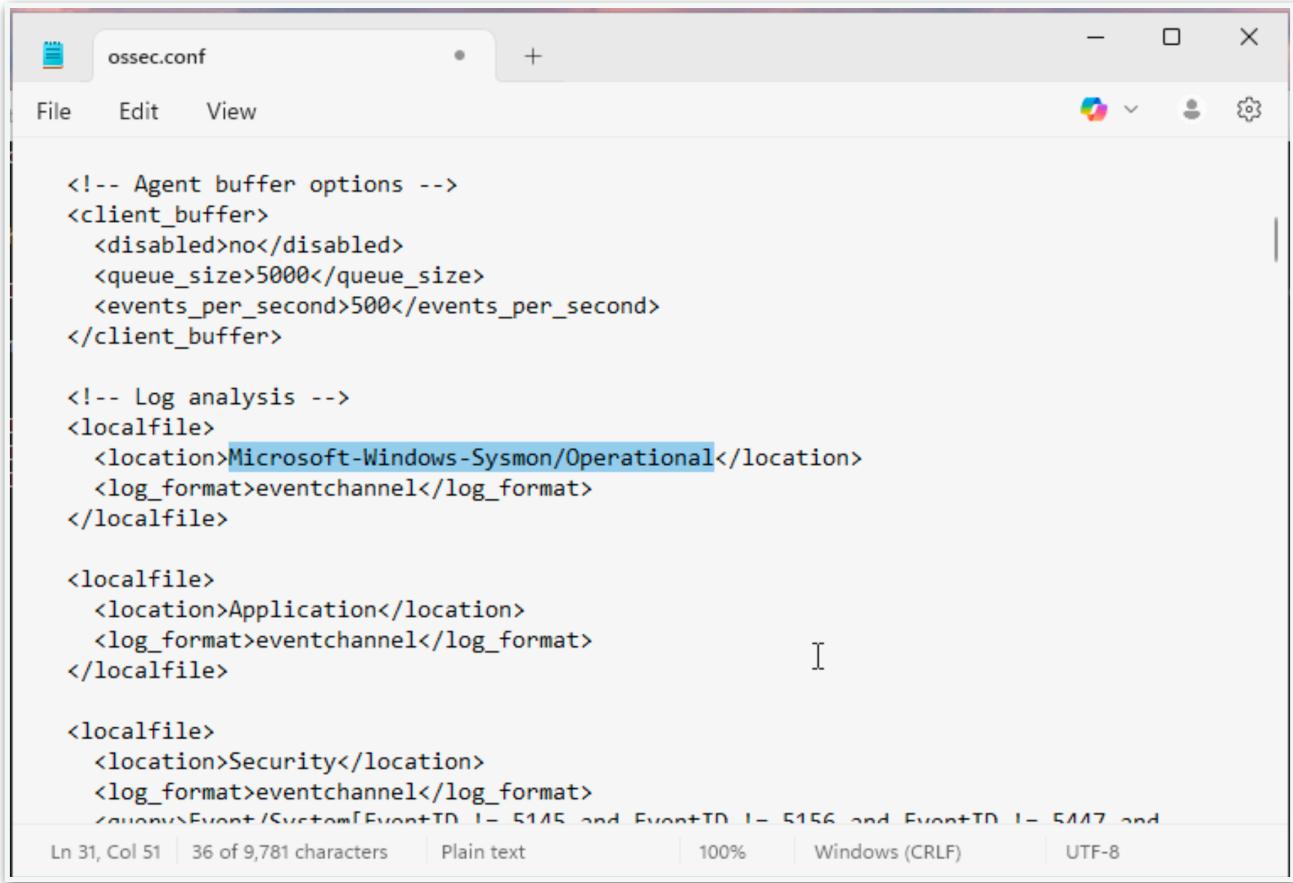


The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of event logs categorized by source, including Storage, StorageSpaces, StorDiag, Store, StorPort, Storsvc, Sudo, and Sysmon. The Sysmon category is expanded, showing sub-categories like Operational, SystemSettingsThreshold, TaskScheduler, and TCP/IP. The main pane displays the 'Operational' log with 2,737 events. A specific event is selected, showing details in the bottom pane. The event details include:

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)

The right pane contains an 'Actions' menu with various options such as Open Saved Log..., Create Custom View..., Import Custom View..., Clear Log..., Filter Current Log..., Properties, Disable Log, Find..., Save All Events As..., Attach a Task To this Log..., View, Refresh, and Help.

## Screenshot - Config to forward Sysmon logs to Wazuh dashboard



```

<!-- Agent buffer options -->
<client_buffer>
  <disabled>no</disabled>
  <queue_size>5000</queue_size>
  <events_per_second>500</events_per_second>
</client_buffer>

<!-- Log analysis -->
<localfile>
  <location>Microsoft-Windows-Sysmon/Operational</location>
  <log_format>eventchannel</log_format>
</localfile>

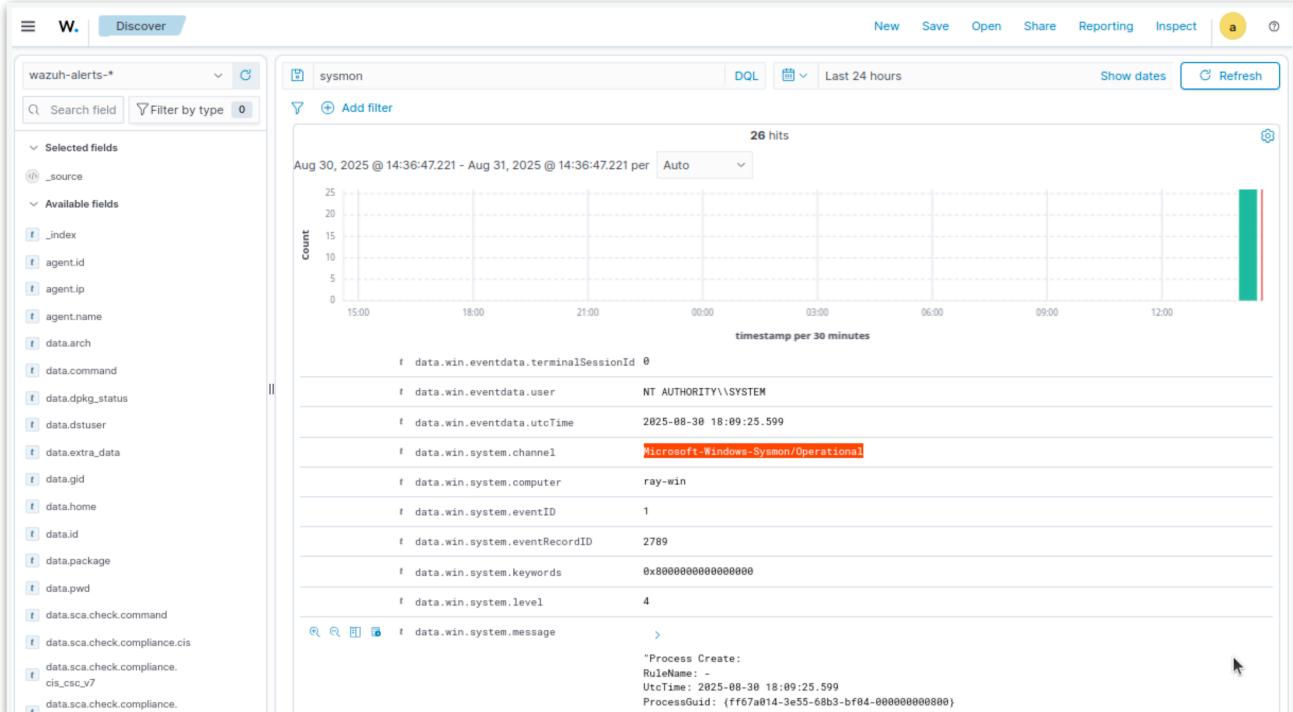
<localfile>
  <location>Application</location>
  <log_format>eventchannel</log_format>
</localfile>

<localfile>
  <location>Security</location>
  <log_format>eventchannel</log_format>
</localfile>

```

Ln 31, Col 51 | 36 of 9,781 characters | Plain text | 100% | Windows (CRLF) | UTF-8

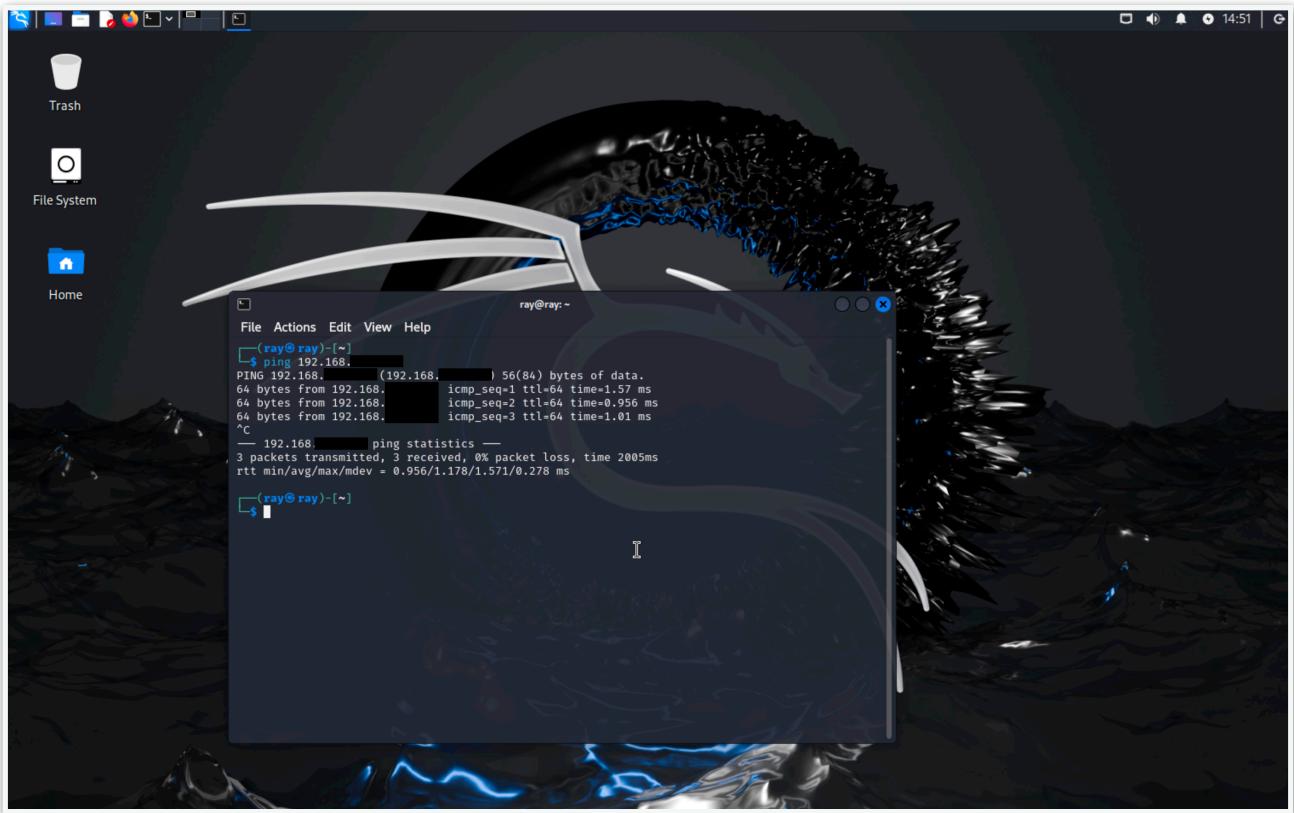
## Screenshot - Verify Sysmon logs collection in Wazuh dashboard



## 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"> <li>Enter wrong password in Windows Lock Screen</li> </ul>
Result	<ul style="list-style-type: none"> <li>Event detected by agent and shown on Wazuh dashboard</li> <li>Filtered logs by “data.win.system.eventID: 4625”</li> </ul>
Screenshot	

## Test 2

Date	2025-09-06
Target	Windows Endpoint
Method	<ul style="list-style-type: none"> <li>Simulate brute-force attack on Windows Endpoint</li> <li>Created “victim” user on Windows with weak password</li> <li>Use Hydra on Kali Linux to attempt brute-force</li> </ul>
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).

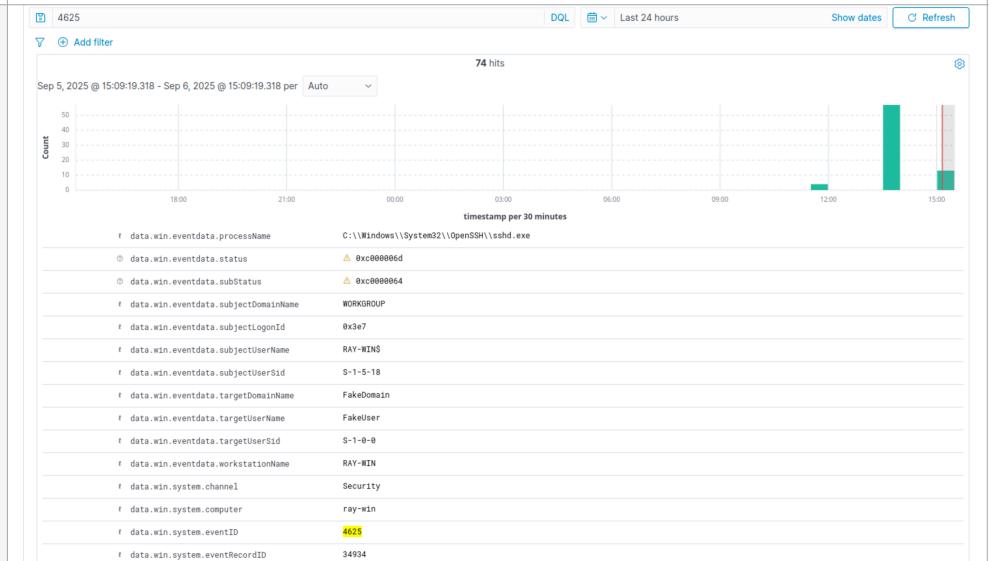
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-06 13:50:12
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries 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

### 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 &lt;integration&gt; &lt;name&gt;virustotal&lt;/name&gt; &lt;api_key&gt;*****&lt;/api_key&gt; &lt;group&gt;syscheck&lt;/group&gt; &lt;alert_format&gt;json&lt;/alert_format&gt; &lt;/integration&gt;  # Config Wazuh agent to monitor "Downloads" &lt;syscheck&gt; &lt;directories check_all="yes" realtime="yes"&gt;C:\Users*\Downloads&lt;/ directories&gt; &lt;/syscheck&gt;  # Test download and flagged by Wazuh - success</pre>																								
Screenshot File hash check on VirusTotal	<p>The screenshot shows the VirusTotal interface with the following details:</p> <ul style="list-style-type: none"> <li><b>File Hash:</b> 2546dcff5ad854d4ddc64fbf056871cd5a00f2471cb7a5bfd4ac23b6e9eedad</li> <li><b>Community Score:</b> 488</li> <li><b>Threat Categories:</b> virus, eicar/test</li> <li><b>Family Labels:</b> eicar, test, file</li> <li><b>Security Vendors' Analysis:</b> <table border="1"> <thead> <tr> <th>Vendor</th> <th>Threat Label</th> <th>Notes</th> </tr> </thead> <tbody> <tr><td>AhnLab-V3</td><td>Virus/EICAR_Test_File</td><td>Alibaba</td></tr> <tr><td>AliCloud</td><td>Engtest:Multi/Eicar</td><td>ALYac</td></tr> <tr><td>Anti-AVL</td><td>TestFile/Win32.EICAR</td><td>Arcabit</td></tr> <tr><td>Avast</td><td>EICAR Test-NOT Virus!!!</td><td>Avast-Mobile</td></tr> <tr><td>AVG</td><td>EICAR Test-NOT Virus!!!</td><td>Avira (no cloud)</td></tr> <tr><td>Baidu</td><td>Win32.Test.Eicar.a</td><td>BitDefender</td></tr> <tr><td>ClamAV</td><td>Win.Test.EICAR_HDB-1</td><td>CMC</td></tr> </tbody> </table> </li> </ul>	Vendor	Threat Label	Notes	AhnLab-V3	Virus/EICAR_Test_File	Alibaba	AliCloud	Engtest:Multi/Eicar	ALYac	Anti-AVL	TestFile/Win32.EICAR	Arcabit	Avast	EICAR Test-NOT Virus!!!	Avast-Mobile	AVG	EICAR Test-NOT Virus!!!	Avira (no cloud)	Baidu	Win32.Test.Eicar.a	BitDefender	ClamAV	Win.Test.EICAR_HDB-1	CMC
Vendor	Threat Label	Notes																							
AhnLab-V3	Virus/EICAR_Test_File	Alibaba																							
AliCloud	Engtest:Multi/Eicar	ALYac																							
Anti-AVL	TestFile/Win32.EICAR	Arcabit																							
Avast	EICAR Test-NOT Virus!!!	Avast-Mobile																							
AVG	EICAR Test-NOT Virus!!!	Avira (no cloud)																							
Baidu	Win32.Test.Eicar.a	BitDefender																							
ClamAV	Win.Test.EICAR_HDB-1	CMC																							

Screenshot VirusTotal API integration in config file	<pre> &lt;!-- VirusTotal integration --&gt; &lt;integration&gt;   &lt;name&gt;virustotal&lt;/name&gt;   &lt;api_key&gt;1b[REDACTED]e5&lt;/api_key&gt;   &lt;group&gt;syscheck&lt;/group&gt;   &lt;alert_format&gt;json&lt;/alert_format&gt; &lt;/integration&gt;  &lt;!-- System inventory --&gt; &lt;wodle name="syscollector"&gt;   &lt;disabled&gt;no&lt;/disabled&gt;   &lt;interval&gt;1h&lt;/interval&gt; </pre>																																
Screenshot VirusTotal sys check config	<pre> &lt;!-- Directories to check (perform all possible verifications) --&gt; &lt;directories check_all="yes" realtime="yes"&gt;C:\Users\*\Downloads&lt;/directories&gt; &lt;directories&gt;/etc,/usr/bin,/usr/sbin&lt;/directories&gt; &lt;directories&gt;/bin,/sbin,/boot&lt;/directories&gt; </pre>																																
Screenshot Malicious file download alert on dashboard from VirusTotal API integration	<p>Sep 5, 2025 @ 18:05:11.882 - Sep 6, 2025 @ 18:05:11.882 per Auto</p> <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>&gt; <a href="https://www.virustotal.com/gui/file/2546dcffc5ad854d4ddc64fbf056871cd5a0f2471cb7a5bfd4ac23b6e9eedad/detection/f-2546dcffc5ad854d4ddc64fbf056871cd5a0f2471cb7a5bfd4ac23b6e9eedad-1757164397">https://www.virustotal.com/gui/file/2546dcffc5ad854d4ddc64fbf056871cd5a0f2471cb7a5bfd4ac23b6e9eedad/detection/f-2546dcffc5ad854d4ddc64fbf056871cd5a0f2471cb7a5bfd4ac23b6e9eedad-1757164397</a></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	> <a href="https://www.virustotal.com/gui/file/2546dcffc5ad854d4ddc64fbf056871cd5a0f2471cb7a5bfd4ac23b6e9eedad/detection/f-2546dcffc5ad854d4ddc64fbf056871cd5a0f2471cb7a5bfd4ac23b6e9eedad-1757164397">https://www.virustotal.com/gui/file/2546dcffc5ad854d4ddc64fbf056871cd5a0f2471cb7a5bfd4ac23b6e9eedad/detection/f-2546dcffc5ad854d4ddc64fbf056871cd5a0f2471cb7a5bfd4ac23b6e9eedad-1757164397</a>	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	> <a href="https://www.virustotal.com/gui/file/2546dcffc5ad854d4ddc64fbf056871cd5a0f2471cb7a5bfd4ac23b6e9eedad/detection/f-2546dcffc5ad854d4ddc64fbf056871cd5a0f2471cb7a5bfd4ac23b6e9eedad-1757164397">https://www.virustotal.com/gui/file/2546dcffc5ad854d4ddc64fbf056871cd5a0f2471cb7a5bfd4ac23b6e9eedad/detection/f-2546dcffc5ad854d4ddc64fbf056871cd5a0f2471cb7a5bfd4ac23b6e9eedad-1757164397</a>																																
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																																

### 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	<b>CVE-2022-40898</b> 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	<b>CVE-2022-40899</b> 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	<b>CVE-2024-6345</b> 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><b>CVE-2024-44142</b>  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%