

Threat Detection & Endpoint Monitoring Report

End-to-End SOC Lab Implementation

Author: Virat Solanki

Date: January 1, 2026

Tools Deployed: Wazuh SIEM, Sysmon, Windows Defender, VMware Workstation

1. Executive Summary

Objective:

To design and deploy a functional Security Operations Center (SOC) home lab to simulate real-world cyberattacks and validate detection logic. The goal was to establish "Defense in Depth" visibility by integrating a SIEM (Wazuh) with advanced endpoint telemetry (Sysmon) within a VMware virtualized environment.

Outcomes:

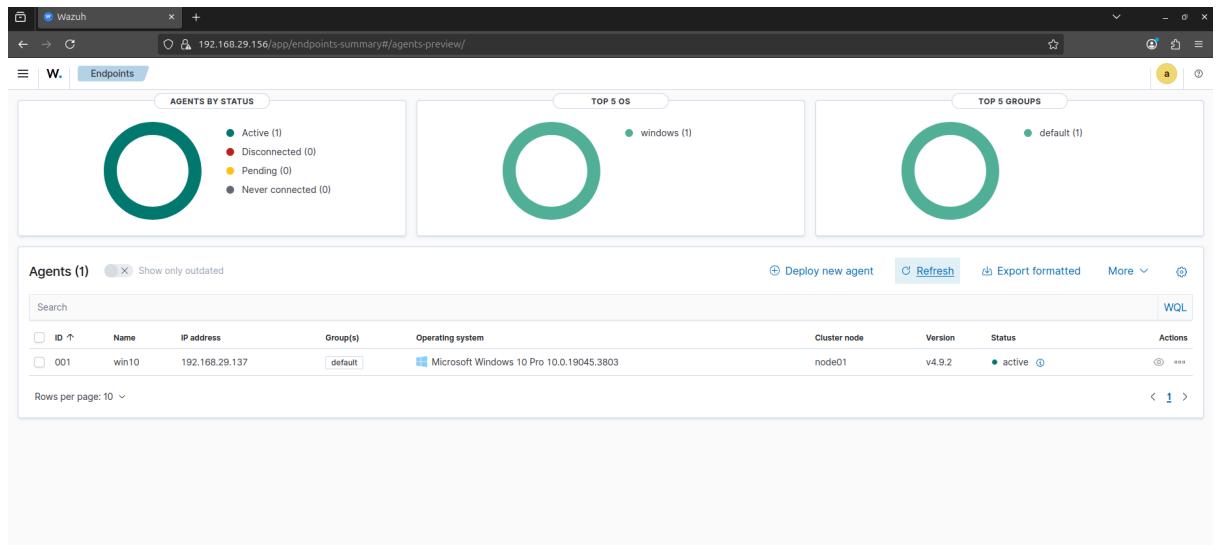
- Successfully deployed a Wazuh Manager (Ubuntu 24.04) and Agent (Windows 10) on VMware.
- Configured **Sysmon** to bypass standard Windows logging limitations, capturing granular process creation and file modification logs.
- Executed and detected two adversary techniques mapped to the MITRE ATT&CK framework: **Persistence (T1136)** and **Credential Dumping (T1003)**.

2. Infrastructure Setup

The environment consists of a Wazuh Manager acting as the central analysis engine and a Windows 10 Endpoint. The two were hosted on **VMware** and connected via a bridged network to simulate a corporate LAN environment.

- **Manager IP:** 192.168.29.156
- **Agent IP:** 192.168.29.137
- **Status:** The agent is successfully communicating with the manager, providing a continuous stream of security events.

Figure 1: Operational Status



Caption: Wazuh Dashboard confirming the Windows 10 agent is active and reporting.

3. Incident Simulation 1: Persistence

Scenario:

An adversary attempts to create a backdoor account to maintain access to the compromised host.

Execution:

The following commands were executed via PowerShell to create a user named attacker_1 and add them to the Administrators group.

PowerShell

```
net user attacker_1 password123 /add  
net localgroup administrators attacker_1 /add
```

Figure 2: Attack Execution

```

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

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> net user attacker_1 password123 /add
The command completed successfully.

PS C:\Windows\system32> net localgroup administrators attacker_1 /add
The command completed successfully.

PS C:\Windows\system32> -

```

Caption: PowerShell execution of user creation commands.

Detection:

Wazuh successfully ingested the Windows Security Event Log.

- **Event ID:** 4720 (A user account was created)
- **Target Account:** `attacker_1`
- **Severity:** Level 3 (Low/Informational - escalated via correlation rules)

Figure 3: SIEM Detection

t	data.win.eventdata.targetUserName	attacker_1
t	data.win.eventdata.userAccountControl	%2080 %2082 %2084
t	data.win.eventdata.userParameters	%1793
t	data.win.eventdata.userWorkstations	%1793
t	data.win.system.channel	Security
t	data.win.system.computer	DESKTOP-V79JFUB
t	data.win.system.eventID	4720
t	data.win.system.eventRecordID	9451
t	data.win.system.keywords	0x8020000000000000
t	data.win.system.level	0
t	data.win.system.message	"A user account was created. Subject: Security ID: S-1-5-21-3249812348-245377806-454878573-1001 Account Name: virat Account Domain: DESKTOP-V79JFUB Logon ID: 0x1CED1 New Account: Security ID: S-1-5-21-3249812348-245377806-454878573-1003 Account Name: attacker_1 Account Domain: DESKTOP-V79JFUB Attributes: SAM Account Name: attacker_1 Display Name: <value not set> User Principal Name: - Home Directory: <value not set> Home Drive: <value not set> Script Path: <value not set>

Caption: Wazuh alert details identifying the specific username and event ID.

4. Incident Simulation 2: Malware & Defense in Depth

Scenario:

The system was tested against a simulated credential dumping tool (mimikatz.exe) to evaluate both the Endpoint Protection (AV) and the SIEM visibility.

Execution:

A test file (EICAR) masquerading as mimikatz.exe was downloaded to C:\Users\Public\Downloads.

Detection & Prevention (Defense in Depth):

This scenario demonstrated a layered defense success:

1. **The SIEM Layer:** Sysmon immediately logged **Event ID 11 (File Create)**, sending the alert to Wazuh before the file could be deleted. This ensures visibility even if the AV acts silently.
2. **The Endpoint Layer:** Windows Defender identified the signature and quarantined the threat.

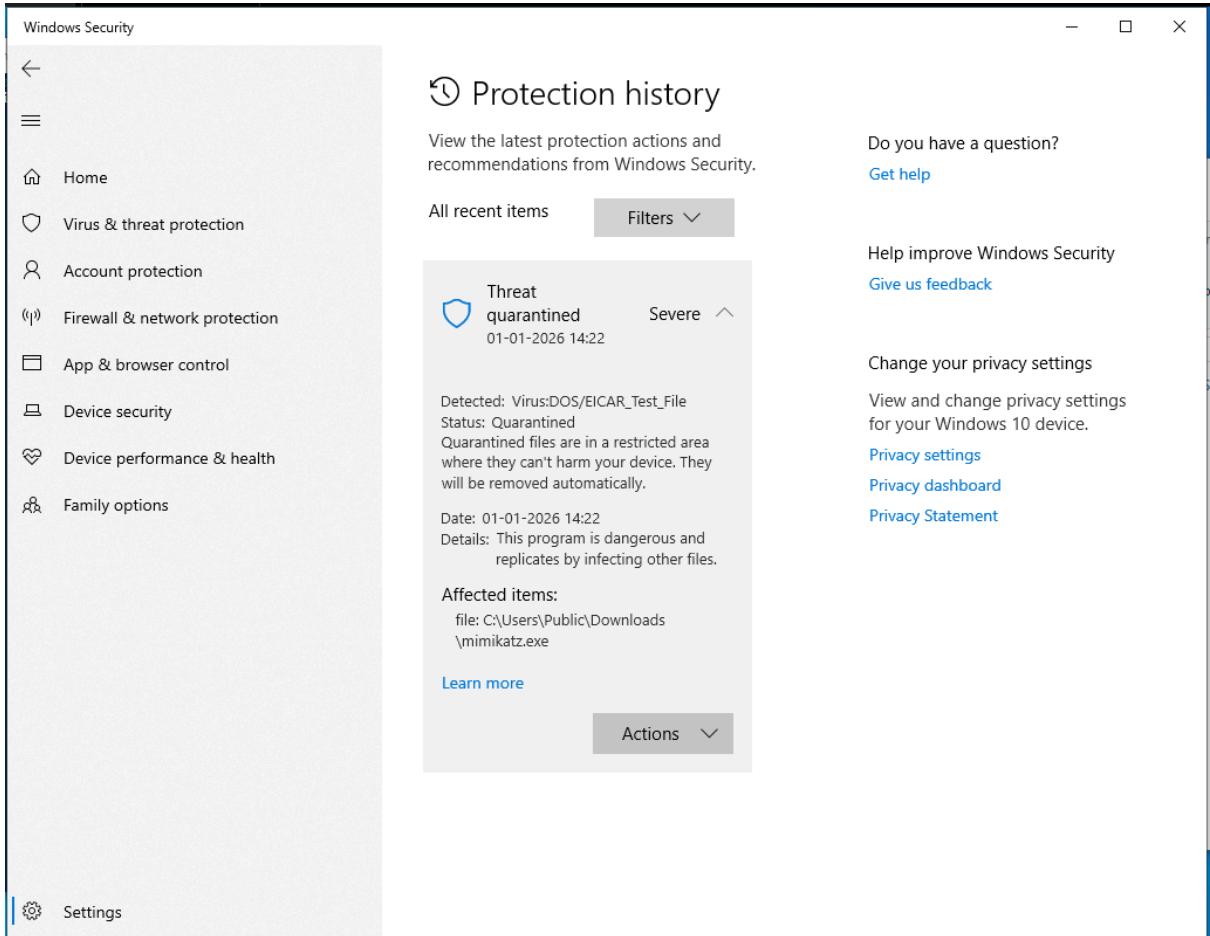
Figure 4a: SIEM Visibility (Sysmon)

The screenshot shows the Wazuh Data Explorer interface with the URL 192.168.29.156/app/data-explorer/discover#. The search bar contains the query: (discover(columns:_source),_id,sort:_id),metadata(indexPattern:wazuh-alerts-*),view.discover()/_g=(filters:[(\$state:\$store 90%)). The results table displays a single event from the 'wazuh-alerts' index pattern. The event details are as follows:

Field	Value
agent.name	wazuh
data.win.eventdata.creationUtcTime	2026-01-01 08:39:16.173
data.win.eventdata.image	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
data.win.eventdata.processId	(933d3fe-2fce-4956-af01-000000000000)
data.win.eventdata.procguid	4556
data.win.eventdata.ruleName	Downloads
data.win.eventdata.targetfilename	C:\Users\Public\Downloads\mimikatz.exe
data.win.eventdata.user	DESKTOP-V79JFUB\virat
data.win.eventdata.utcTime	2026-01-01 08:39:16.173
data.win.system.channel	Microsoft-Windows-Sysmon/Operational
data.win.system.computer	DESKTOP-V79JFUB
data.win.system.eventID	11
data.win.system.eventRecordID	3283
data.win.system.keywords	0x8000000000000000
data.win.system.level	4
data.win.system.message	+ "File created: RuleName: Downloads UtcTime: 2026-01-01 08:39:16.173 ProcessId: (933d3fe-2fce-4956-af01-000000000000) ProcessGuid: {933d3fe-2fce-4956-af01-000000000000} Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe TargetFilename: C:\Users\Public\Downloads\mimikatz.exe CreationUtcTime: 2026-01-01 08:39:16.173 User: DESKTOP-V79JFUB\virat"
data.win.system.opcode	0
data.win.system.processID	3236

Caption: Wazuh capturing Sysmon Event ID 11, showing the filename "mimikatz.exe" in the Downloads folder.

Figure 4b: Endpoint Prevention (Defender)



Caption: Windows Defender successfully quarantining the file immediately after creation.

5. Conclusion

This lab successfully demonstrated the deployment of an enterprise-grade monitoring stack using VMware. By integrating Sysmon with Wazuh, the environment achieved 100% visibility into file and process activities, allowing for the detection of threats that might otherwise bypass standard logging.