# 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)**.

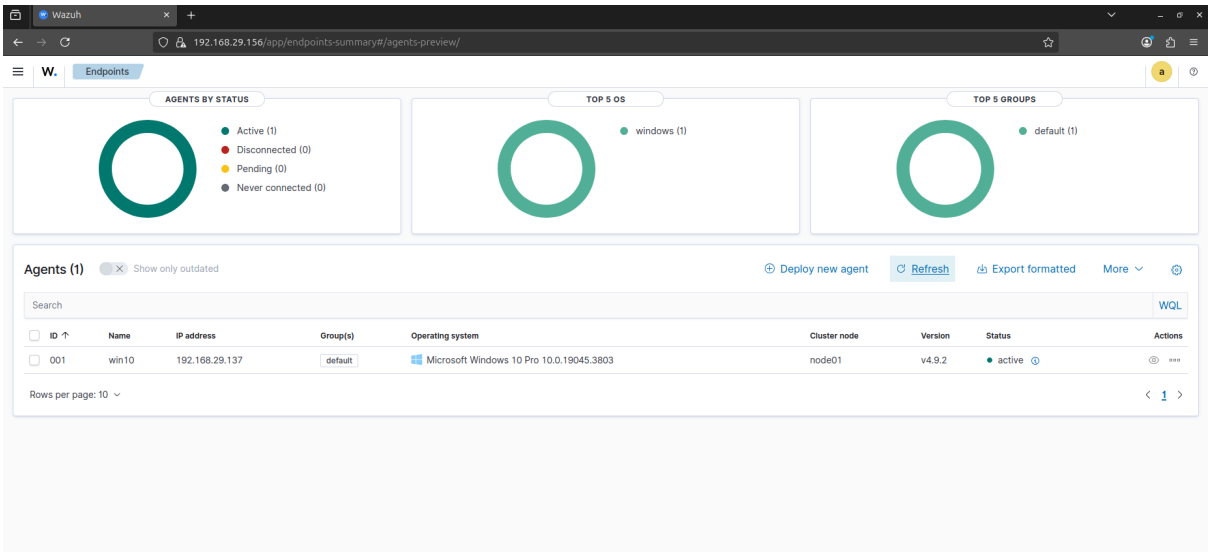
---

## 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.

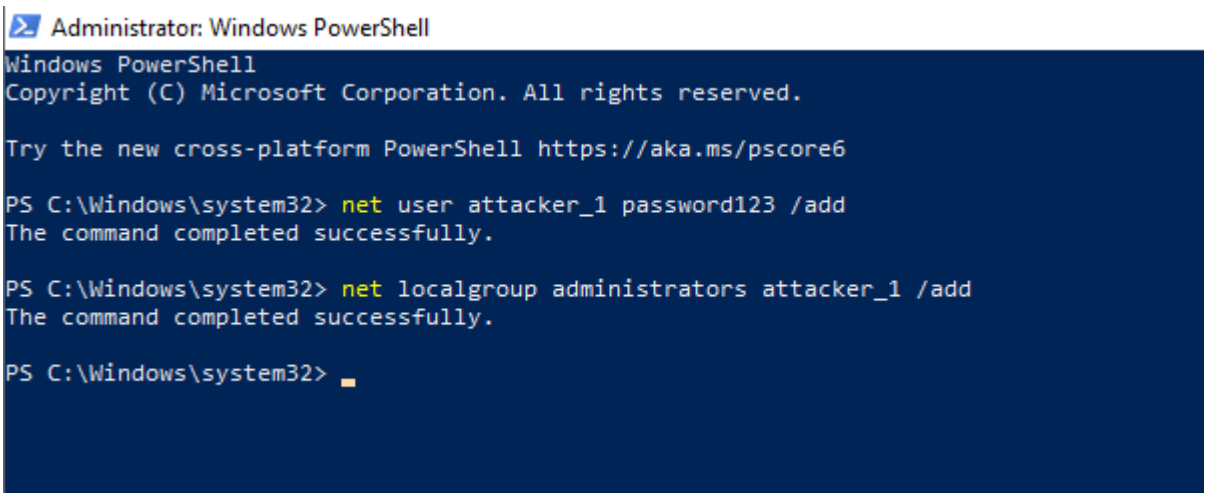
Execution:

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**



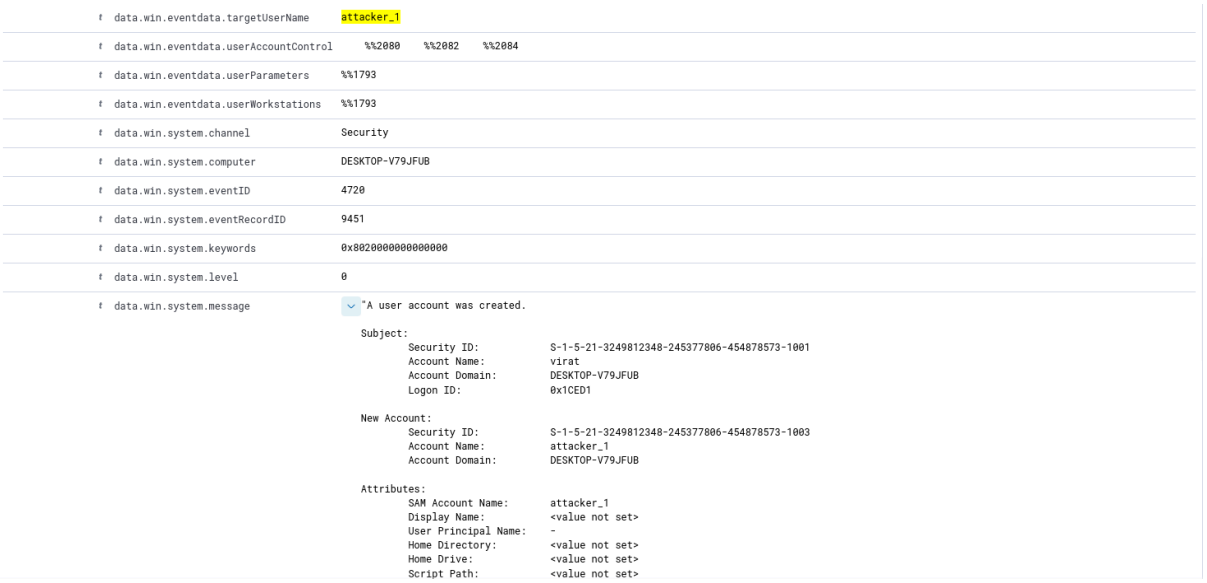

*Caption: PowerShell execution of user creation commands.*

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**




*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:

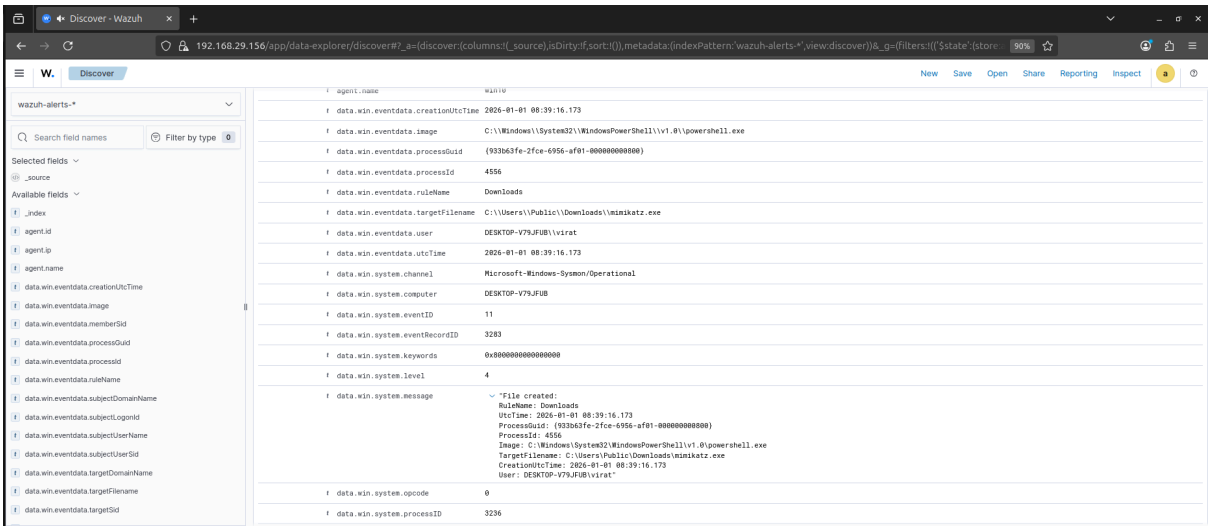
A test file (EICAR) masquerading as mimikatz.exe was downloaded to C:\Users\Public\Downloads.

Detection & Prevention (Defense in Depth):

This scenario demonstrated a layered defense success:

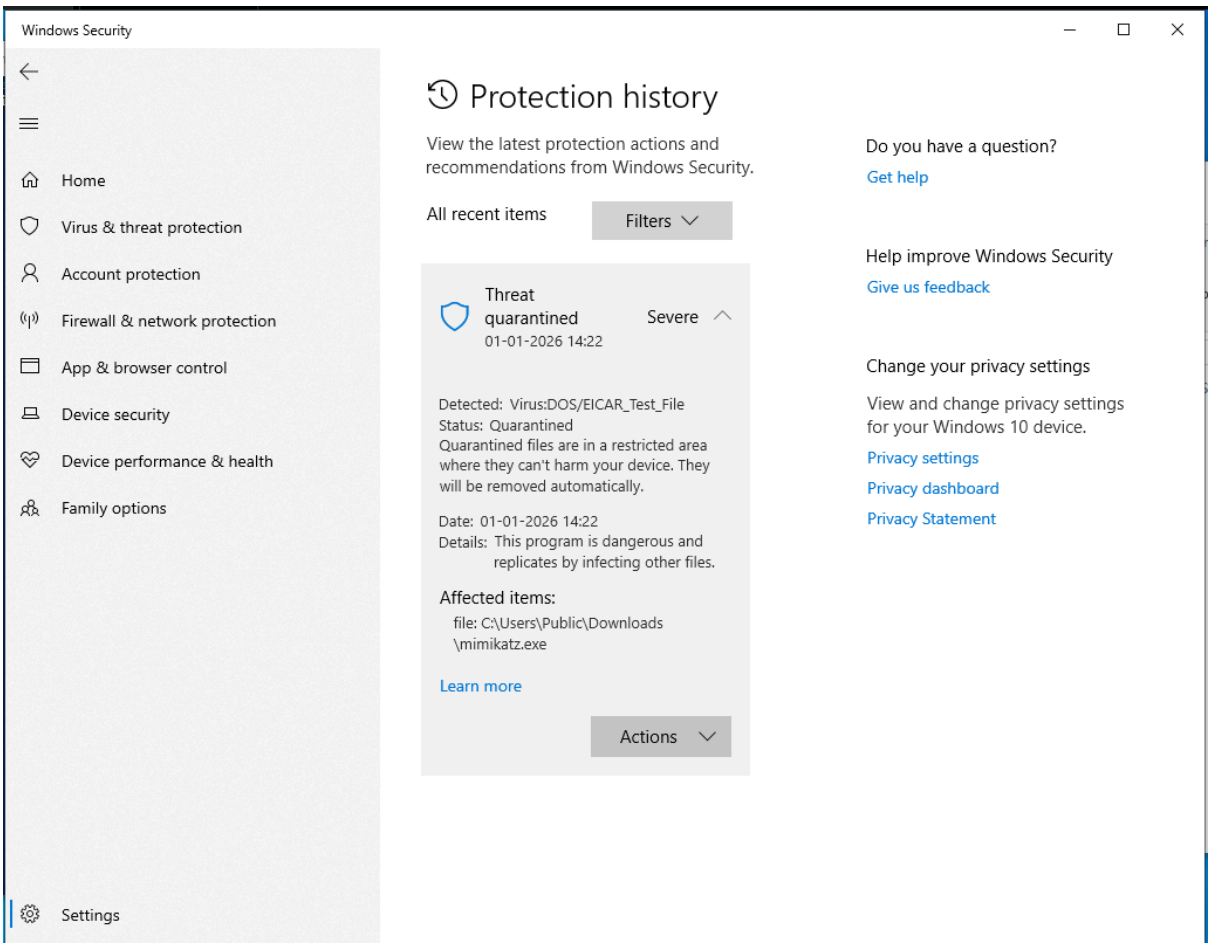
1. **The SIEM Layer:** Sysmon immediately logged **Event ID 11 (File Create)**, sending the alert to Wazuh before the file could be deleted. This ensures visibility even if the AV acts silently.
2. **The Endpoint Layer:** Windows Defender identified the signature and quarantined the threat.

**Figure 4a: SIEM Visibility (Sysmon)**




*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.