Windows File & Registry Integrity Monitoring using Wazuh (FIM)

Subject: **Windows File & Registry Integrity Monitoring using Wazuh (FIM)**

Incident ID: IR-2025-1223-008

PREPARED BY:

Vignesh K.

SOC Analyst / Security Researcher

CERTIFICATIONS: Google Cybersecurity Professional

REPORT DATE: December 23, 2025

1. Project Overview and Goal

Overview: This project demonstrates the detection of unauthorized file and registry changes on a Windows 11 endpoint using Wazuh File Integrity Monitoring (FIM).

The goal is to detect defense evasion techniques where adversaries modify system configurations to blind security tools.

2. Technical Environment and Tools

The technical components and tools used for this assessment are detailed below.

Component	Description	Detail
Target System	The victim endpoint.	Windows 11
SIEM / Manager	The central monitoring server.	Wazuh Manager (Ubuntu VM)
Primary Tools	FIM Module	Wazuh Agent (v4.14.1) & Syscheck

3. Attack Simulation

To simulate an adversary attempting Defense Evasion (MITRE ATT&CK T1562), the following actions were performed:

- **Registry Modification:** Modified keys related to **Windows Defender** (simulating an attempt to disable AV).
- **Service Tampering:** Altered registry keys for the **Windows Time Service** to manipulate system time.
- **Integrity Violation:** Triggered immediate checksum mismatch alerts on the Wazuh manager.

4. Detection

Wazuh was used to detect unauthorized changes by correlating file state comparisons against a known baseline.

- **Syscheck Logic:** The Wazuh FIM module (Syscheck) scans the endpoint at defined intervals. It stores the cryptographic checksums (MD5/SHA256) of monitored files and registry keys.
- **Comparison & Alerting:** When a file or registry key is modified, the agent recalculates the hash. If the new hash differs from the stored baseline, Wazuh generates an alert (e.g., Rule ID 550).
- **Visualization:** These alerts are visualized in the Wazuh Dashboard, allowing the analyst to see exactly *what* changed (old value vs. new value) and *who* made the change.
- **Refinement:** To reduce noise, specific directories (like temp folders) are ignored, while critical paths (like System32 and CurrentControlSet) are set to report changes in real-time.

5. FIM Configuration (ossec.conf)

The core configuration used for detection is located in the `ossec.conf` file on the agent:

Detailed Explanation of Configuration Components

Configuration Component	Description
`<syscheck>`	This tag initiates the File Integrity Monitoring module. It instructs the Wazuh agent to run the integrity checking process.
`<registry ignore="no">`	This is the critical filter. It specifies which registry hives or keys to monitor.
`ignore="no"`	Ensures that changes to this key are **not** ignored and will trigger an alert.
Path Definition	The text inside the tags (e.g., `HKEY_LOCAL_MACHINE...`) defines the exact path to monitor. By monitoring Windows Defender keys, we ensure that any attempt to turn off real-time protection is logged immediately.

Result Interpretation

The output of this configuration is an alert containing the `syscheck.diff` field. This field shows the "Before" and "After" state of the registry key. A security analyst immediately looks for unauthorized changes in these keys, as this strongly suggests an attacker is trying to "blind" the system before launching a larger attack (like ransomware).

6. Security Recommendations (Next Steps)

Based on the detection results, the following remediation measures and security enhancements are recommended:

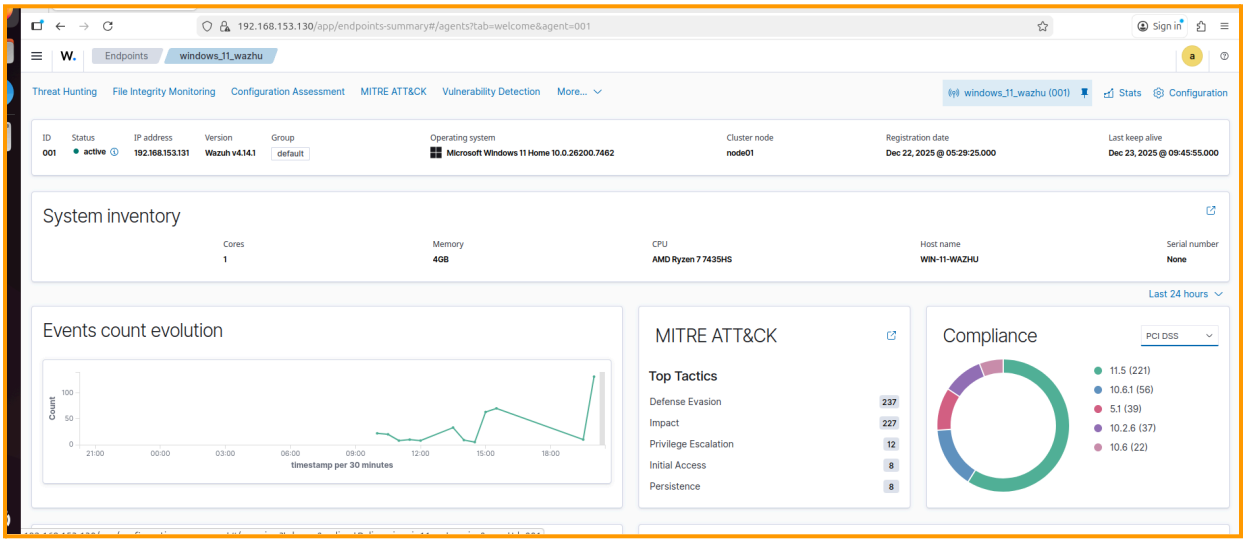
- **HIGH: Enable Active Response:** Configure Wazuh Active Response to automatically revert critical registry changes or isolate the endpoint if specific high-severity keys (like Windows Defender) are tampered with.
- **HIGH: Monitor and Alert:** Create a custom rule to trigger a "Level 12" alert specifically when keys related to security services are modified/deleted, ensuring immediate SOC visibility.
- **MEDIUM: Least Privilege:** Restrict registry editing permissions via Group Policy (GPO) so that only Domain Admins can modify keys in `HKEY_LOCAL_MACHINE\SYSTEM`.
- **MEDIUM: Frequency Tuning:** Adjust the frequency setting in Syscheck to balance between performance and detection speed (e.g., scan critical paths every 300 seconds).

7. Conclusion

This project successfully validated the capability of using Wazuh to detect sophisticated Defense Evasion techniques. The monitoring of the Windows Registry is a foundational detection control. Immediate action on the security recommendations, particularly Active Response, is essential to harden the system against persistence and evasion threats.

8. Evidence

8.1 Wazuh_Dashboard



8.2 FIM-Events

FIM: Recent events

Time ↓	Path	Action	Rule description	Rule Lev...	Rule Id
Dec 23, 2025 @ 09:45:42.926	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WinDefend	modified	Registry Value Integrity Checksum Changed	5	750
Dec 23, 2025 @ 09:45:42.926	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WinDefend	modified	Registry Key Integrity Checksum Changed	5	594
Dec 23, 2025 @ 09:45:42.915	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WinDefend\Security	modified	Registry Key Integrity Checksum Changed	5	594
Dec 23, 2025 @ 09:45:42.119	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WdFilter\Security	modified	Registry Key Integrity Checksum Changed	5	594
Dec 23, 2025 @ 09:45:41.285	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\SecureTimeLimits	modified	Registry Value Integrity Checksum Changed	5	750

8.3 Event-Logs