INCIDENT RESPONSE REPORT

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

Incident ID: IR-2025-1224-009

PREPARED BY:

Vignesh K.

SOC Analyst / Security Researcher

CERTIFICATIONS: Google Cybersecurity Professional

REPORT DATE: December 24, 2025

Incident ID	IR-2025-1224-009
Date	December 24, 2025
Severity	Medium
Status	Closed (Lab Simulation)

1. Project Overview and Goal

- This project demonstrates how **Wazuh File Integrity Monitoring (FIM)** can be used to detect **unauthorized file and Windows Registry modifications** on a Windows 11 endpoint.

2. Technical Environment and Tools

Component	**Description**
Target System	**Windows 11 (Endpoint) VM**
SIEM / Manager	**Wazuh Manager (Ubuntu VM)**
Agent Version	**Wazuh Agent v4.14.1**
Detection Module	**Syscheck (File Integrity Monitoring)**

Dashboard	**Wazuh Web Interface**

3. Attack Simulation:

To simulate a **Defense Evasion scenario (MITRE ATT&CK T1562)**, the following specific actions were performed on the endpoint:

Simulated Adversary Actions

- **Registry Tampering:** Modified registry keys related to critical services:
  - `WinDefend` (Windows Defender)
  - `W32Time` (Windows Time Service)
- **Configuration Manipulation:** Triggered checksum changes to monitored registry paths.
- **Integrity Violation:** Forced hash mismatches to generate Syscheck alerts.

> **Note:** These actions resemble real-world attempts to weaken endpoint defenses prior to executing malware or ransomware.

4. Detection Mechanism

How Wazuh Detected the Activity

1. **Baseline Creation:** Wazuh stored cryptographic hashes of monitored registry keys.
2. **Continuous Monitoring:** The **Syscheck** module periodically rescanned monitored paths.
3. **Change Detection:** Any modification resulted in a hash mismatch.
4. **Alert Generation:** Wazuh generated alerts containing:
   - Old vs. New checksum values.

    - Affected Registry path.
    - Rule ID and severity level.
5. **Visualization:** All alerts were visualized in the Wazuh FIM Dashboard, enabling clear identification of *what* changed, *when* it changed, and *which* agent was affected.

5. FIM Configuration (`ossec.conf`)

The File Integrity Monitoring logic is defined within the `<syscheck>` configuration block on the Windows agent.

Key Configuration Concepts

- **`<syscheck>`:** Enables integrity monitoring.
- **Registry Paths:** Paths under `HKEY_LOCAL_MACHINE` were explicitly monitored.
- **Critical Services:** Security-related services were prioritized (not ignored).
- **Real-time Alerting:** Configured for sensitive keys to ensure immediate notification.

> **Why Registry Monitoring Matters** Registry modifications are a high-confidence indicator of defense evasion, persistence mechanisms, or security control tampering. Monitoring these paths gives SOC teams an early warning of compromise attempts.

6. Result Interpretation

Each alert contained detailed forensic data, providing a clear audit trail.

Alert Details

- **Registry Path:** The specific key modified.
- **Action Type:** `Modified`
- **Checksums:** Comparison of Old vs. New hash values.
- **Context:** Rule ID and Severity Level.

Analyst Interpretation Unauthorized changes to `WinDefend` or `W32Time` strongly indicate **pre-attack preparation** by an adversary. Such activity is commonly observed before ransomware execution or lateral movement.

7. Security Recommendations

To harden the environment based on these findings:

HIGH Priority

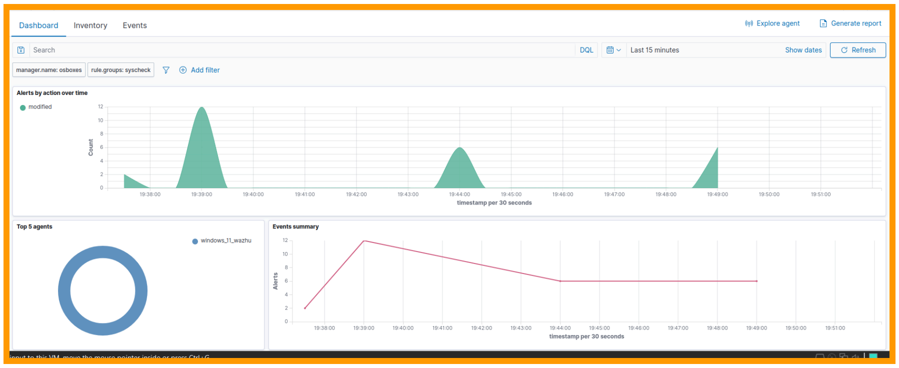
- **Enable Wazuh Active Response:** Automatically revert critical registry changes or isolate the endpoint upon high-risk modification.
- **Custom Rules:** Create custom high-severity rules to escalate Defender or security service tampering to **Level 12+**.

MEDIUM Priority

- **Enforce Least Privilege:** Restrict registry editing capabilities via Group Policy Objects (GPO).
- **Tune Syscheck Frequency:** Scan critical paths every **300 seconds** to balance system performance with detection speed.

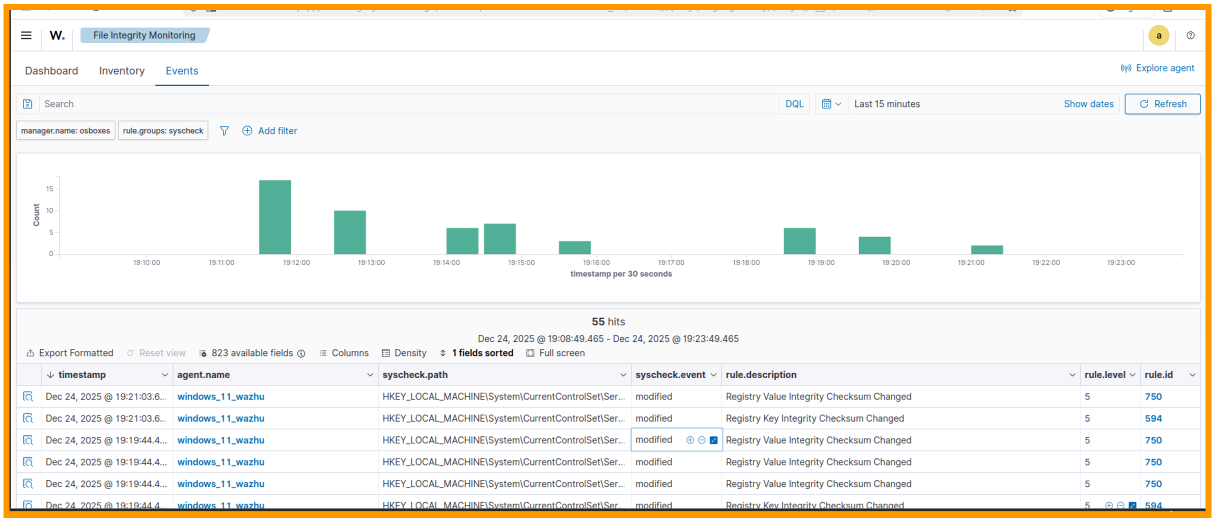
8. Evidence

8.1 Wazuh Dashboard



- Agent status: **Active**
- Event trend visualization available.
- Mapped to MITRE ATT&CK framework.

8.2 FIM Events



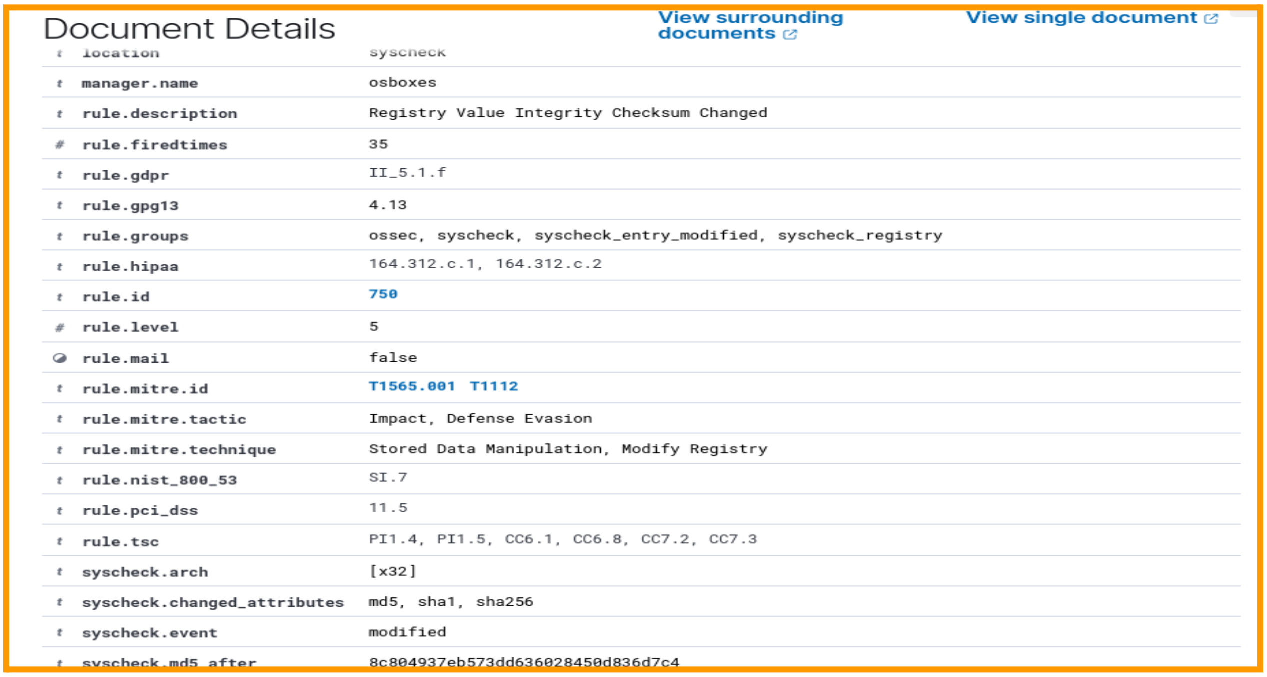
55 hits

Dec 24, 2025 @ 19:08:49.465 - Dec 24, 2025 @ 19:23:49.465

timestamp	agent.name	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
Dec 24, 2025 @ 19:21:03.6...	windows_11_wazhu	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Value Integrity Checksum Changed	5	750
Dec 24, 2025 @ 19:21:03.6...	windows_11_wazhu	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Key Integrity Checksum Changed	5	594
Dec 24, 2025 @ 19:19:44.4...	windows_11_wazhu	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Value Integrity Checksum Changed	5	750
Dec 24, 2025 @ 19:19:44.4...	windows_11_wazhu	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Value Integrity Checksum Changed	5	750
Dec 24, 2025 @ 19:19:44.4...	windows_11_wazhu	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Value Integrity Checksum Changed	5	750
Dec 24, 2025 @ 19:19:44.4...	windows_11_wazhu	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Key Integrity Checksum Changed	5	594

- **Event Type:** Registry checksum mismatch alerts.
- **Rule IDs:** `594`, `750`.
- **Action:** Modified.

8.3 Event Logs



Document Details

t	location	syscheck
t	manager.name	osboxes
t	rule.description	Registry Value Integrity Checksum Changed
#	rule.firedtimes	35
t	rule.gdpr	II_5.1.f
t	rule.gpg13	4.13
t	rule.groups	ossec, syscheck, syscheck_entry_modified, syscheck_registry
t	rule.hipaa	164.312.c.1, 164.312.c.2
t	rule.id	750
#	rule.level	5
◒	rule.mail	false
t	rule.mitre.id	T1565.001 T1112
t	rule.mitre.tactic	Impact, Defense Evasion
t	rule.mitre.technique	Stored Data Manipulation, Modify Registry
t	rule.nist_800_53	SI.7
t	rule.pci_dss	11.5
t	rule.tsc	PI1.4, PI1.5, CC6.1, CC6.8, CC7.2, CC7.3
t	syscheck.arch	[x32]
t	syscheck.changed_attributes	md5, sha1, sha256
t	syscheck.event	modified
t	syscheck.md5_after	8c804937eb573dd636028450d836d7c4

- Full hash comparison (Before / After).
- Clear attribution to module: `Syscheck`.
- Timestamped forensic records for timeline reconstruction.

9. Conclusion

This project successfully demonstrates how **Wazuh File Integrity Monitoring** can detect defense evasion techniques through registry and configuration changes. Registry monitoring is a foundational SOC control that provides:

1. Early compromise detection.
2. High-confidence alerts.
3. Actionable forensic evidence.

Implementing **Active Response** and custom alerting will significantly improve endpoint resilience against advanced threats.