WAZUH SIEM

Security Detection Report

Homelab Security Monitoring Project

Date: March 2026

Platform: Wazuh SIEM (Microsoft Azure)

NIST SP 800-53 Rev. 5 | MITRE ATT&CK | Loi 05-20

1. Introduction & Scope

This report documents the detection capabilities validated during live testing of a cloud-native Wazuh SIEM homelab environment. All tests were conducted on March 14, 2026 against a controlled infrastructure consisting of a Wazuh Manager hosted on Microsoft Azure and two monitored endpoints: a Windows 10 host and a WSL (Ubuntu) instance.

The objective of this testing was to validate three core security capabilities:

- Real-time detection of credential-based attacks and privilege escalation attempts
- File Integrity Monitoring (FIM) for unauthorized changes to critical system paths
- Custom rule authoring for organization-specific threat scenarios

Environment	Microsoft Azure — Ubuntu 22.04 LTS VM
Wazuh Manager	L1-Wazuh-1 (Private IP: 10.0.0.4)
Monitored Agents	WSL-1 (Ubuntu WSL), L1-Wazuh-1 (Windows Host)
Test Date	March 14, 2026
Frameworks	NIST SP 800-53, Loi 05-20, MITRE ATT&CK, PCI-DSS, GDPR

SECTION 1 — ATTACK SIMULATION & DETECTION

2. Attack Simulation & Detection

2.1 Overview

A credential-based brute-force attack was simulated against the WSL endpoint using repeated failed sudo authentication attempts. This technique mirrors real-world privilege escalation patterns used by threat actors during post-compromise activity.

2.2 Attack Methodology

Tools & Commands Used

```
# Simulate repeated failed sudo attempts
for i in {1..10}; do sudo -k && echo "wrongpassword" | sudo -S ls 2>/dev/null; done

# Verify log entries were written
sudo tail -20 /var/log/auth.log
```

The loop triggered 10 successive authentication failures, each logged to /var/log/auth.log with full PAM audit detail including source user, destination user, TTY, and working directory.

2.3 Wazuh Detection Results

Wazuh detected the attack pattern and fired the following alerts within seconds of the simulation:

Rule ID	Description	Severity	MITRE Tactic
5401	Failed attempt to run sudo	Medium (5)	Privilege Escalation
5503	PAM: User login failed	Medium (5)	Credential Access
5402	Successful sudo to ROOT	Medium (3)	Defense Evasion

2.4 Key Findings

- Rule 5401 fired 10 consecutive times, with rule.firedtimes incrementing on each attempt. This demonstrates Wazuh's ability to correlate repeated events from the same source in a short amount of time.

`rule.firedtimes:` `10`

- Rule 5503 automatically mapped to MITRE T1110.001 (Password Guessing) under the Credential Access tactic.

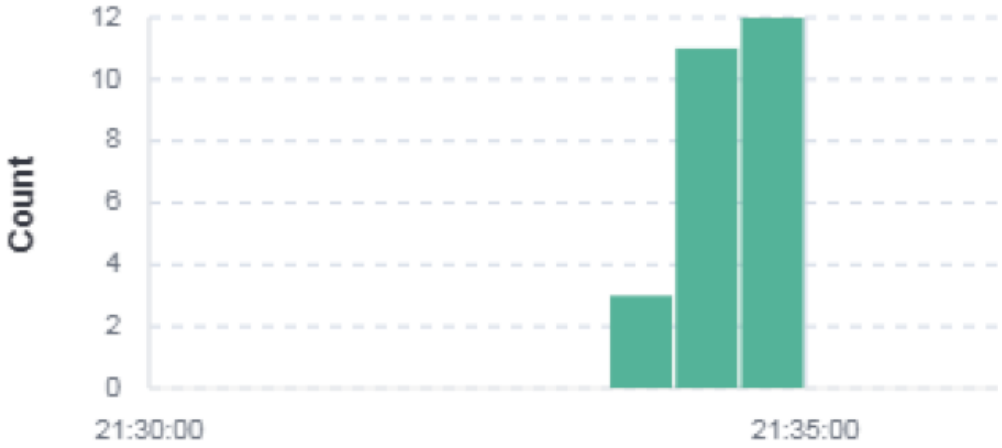
`rule.mitre.technique:` `Password Guessing` `rule.mitre.id:` `T1110.001`

- All alerts were automatically enriched with NIST SP 800-53 (AU.14, AC.7), PCI-DSS, HIPAA, and GDPR compliance tags with zero manual configuration.

`rule.pci_dss:` `10.2.4, 10.2.5` `rule.hipaa:` `164.312.b`

`rule.nist_800_53:` `AU.14, AC.7` `rule.gdpr:` `IV_35.7.d, IV_32.2`

- The histogram spike at 21:34–21:35 UTC provides a clear visual forensic timeline of the attack pattern.



2.5 Compliance Mapping

The brute-force simulation produced alert data that maps directly to multiple compliance frameworks, this section will explore each framework in detail:

- **NIST SP 800-53 CA-7 (Continuous Monitoring):** CA-7 requires organizations to establish a continuous monitoring strategy that includes ongoing assessment of security controls and real-time alerting on anomalous activity. This test validates CA-7 because Wazuh detected the authentication attack pattern within seconds of onset, without any manual intervention. The automatic escalation of **rule.firedtimes** from 1 to 10 across consecutive events demonstrates that the system logs and correlates events into a determined attack pattern, which is the core intent of continuous monitoring.

- **NIST SP 800-53 AC-7 (Unsuccessful Login Attempts):** AC-7 specifically mandates that systems enforce a limit on consecutive invalid access attempts and automatically alert on violations. **Rule 5401 ("Failed attempt to run sudo")** firing 10 consecutive times with escalating rule.firedtimes directly satisfies the detection requirement of AC-7. Notably, the alert metadata captured the exact user, destination (root) and command attempted (/usr/bin/ls),

- **NIST SP 800-53 AU-14 (Session Audit):** AU-14 requires that systems provide the capability to capture and audit all content of user sessions. The PAM-level logging captured in this test, including session open, session close, and each individual authentication failure, demonstrates compliance with AU-14. Wazuh's decoder extracted structured fields (data.srcuser, data.dstuser, data.tty, data.command) from raw PAM logs, making the audit trail more readable and queryable.

- **MITRE ATT&CK Dual-Tactic Coverage:** Wazuh automatically mapped the simulation to two distinct MITRE tactics simultaneously: **Privilege Escalation (T1548.003, Sudo Caching)** and **Credential Access (T1110.001, Password Guessing).** This dual mapping is significant as it reflects the reality that a single attack sequence can satisfy multiple attacker goals. A defender reviewing these alerts would immediately understand both ***what*** the attacker attempted and ***why***.

- **PCI-DSS 10.2.4 & 10.2.5:** PCI-DSS Requirement 10.2 mandates logging of all invalid access attempts **(10.2.4)** alongside the use of and changes to identification and authentication mechanisms **(10.2.5)**. Both were auto-tagged on the captured alerts, confirming that this SIEM deployment would **satisfy PCI-DSS** audit evidence requirements.

SECTION 2 — FILE INTEGRITY MONITORING

3. File Integrity Monitoring (FIM)

3.1 Overview

File Integrity Monitoring was tested by introducing a new file into the /etc directory, a critical system path monitored by Wazuh's syscheck engine. This simulates the behavior of an attacker dropping a backdoor or a malicious file in a sensitive location.

3.2 FIM Configuration

The following directories are actively monitored by the Wazuh syscheck engine on the WSL agent:

```
<directories>/etc,/usr/bin,/usr/sbin</directories>
<directories>/bin,/sbin,/boot</directories>
```

The scan frequency was temporarily reduced from 43,200 seconds (12 hours) to 60 seconds for testing purposes, then restored to the original value after evidence was captured. A time of 43,200 seconds is set as the default configuration in order to ease the load on system resources.

3.3 Test Methodology

```
# Temporarily reduce scan frequency for live testing
sudo sed -i 's/<frequency>43200/<frequency>60/' /var/ossec/etc/ossec.conf
sudo systemctl restart wazuh-agent

# Drop a suspicious file in monitored directory
sudo touch /etc/totally-not-a-backdoor.conf

# Restore original frequency after evidence captured
sudo sed -i 's/<frequency>60/<frequency>43200/' /var/ossec/etc/ossec.conf
sudo systemctl restart wazuh-agent

# Cleanup
sudo rm /etc/totally-not-a-backdoor.conf
```

3.4 Wazuh Detection Results

Wazuh detected the file creation within 60 seconds and generated a detailed alert containing full forensic metadata:

syscheck.path	/etc/totally-not-a-backdoor.conf
syscheck.event	added
syscheck.sha256_after	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
syscheck.md5_after	d41d8cd98f00b204e9800998ecf8427e
syscheck.sha1_after	da39a3ee5e6b4b0d3255bfef95601890afd80709
syscheck.perm_after	rw-r--r--
syscheck.uname_after	root
rule.level	5
Compliance Tags	PCI-DSS 11.5, HIPAA 164.312.c.1, 164.312.c.2, TSC PI1.4, PI1.5

3.5 Key Findings

- Wazuh captured SHA256, SHA1, and MD5 hashes of the file immediately upon creation; Enabling cryptographic verification of the file through the possible usage of cross-platform cryptographic hash and malware metadata index services (VirusTotal).
- File permissions, owner, inode, and GID were all recorded automatically thus providing a complete forensic snapshot.
- PCI-DSS 11.5, HIPAA 164.312.c.1/c.2, and TSC compliance controls were auto-mapped to the alert with no manual configuration.
- This capability directly satisfies the FIM requirement under **Loi 05-20** and **NIST SP 800-53 SI-7 (Software, Firmware, and Information Integrity)**.

SECTION 3 — CUSTOM RULE DEVELOPMENT

4. Custom Detection Rule Development

4.1 Overview

A custom Wazuh rule was authored to detect new user account creation on the monitored Azure VM. This scenario maps to **MITRE ATT&CK Technique T1136 (Create Account)** and is a common attacker persistence mechanism used to maintain access after initial compromise.

4.2 Rule Authoring

The rule was created in ***/var/ossec/etc/rules/local_rules.xml*** on the **Wazuh Manager:**

```
<group name="local,syslog,">
  <rule id="100001" level="15">
    <if_sid>5902</if_sid>
    <description>New user account created on $(hostname)</description>
    <mitre>
      <id>T1136</id>
    </mitre>
    <group>authentication,pci_dss_8.1,gpg13_4.13,gdpr_IV_35.7.d,</group>
  </rule>
</group>
```

Key design decisions:

- **Rule ID 100001:** custom rules must be in the 100000+ range to avoid conflicts with built-in Wazuh rules.
- **Level 15 (Critical):** new user creation outside of change management windows is a high-level indicator of compromise.
- **if_sid 5902:** chains off Wazuh's *built-in* user creation event, ensuring the custom rule inherits full log context.
- **MITRE T1136 tag:** enables automatic tactic/technique mapping in the Wazuh Dashboard.

4.3 Test Methodology

```
# Reloading Wazuh Manager to apply new rule
sudo systemctl restart wazuh-manager

# Trigger the rule by creating a test user
sudo useradd hackerman

# Verify and cleanup (post test)
sudo userdel -r hackerman
```

4.4 Detection Results

The custom rule fired immediately upon user creation with the following alert data:

rule.id	100001 (Custom Rule)
rule.level	15 (CRITICAL)
rule.description	New user account created on **L1-Wazuh-1**
data.dstuser	hackerman
data.uid / data.gid	1001 / 1001
data.home	/home/hackerman
data.shell	/bin/sh
rule.mitre.id	T1136
rule.mitre.tactic	Persistence
rule.mail	**true** (email alert triggered)
Compliance Tags	PCI-DSS 8.1, GPG13 4.13, GDPR IV_35.7.d

4.5 Key Findings

- The custom rule fired at Critical (level 15) severity. This is the highest severity tier in Wazuh. In a real SOC environment, this would **not** be overlooked.
- Wazuh captured the full account details including UID, GID, home directory, and shell. This provides complete forensic context for incident response and analysis teams.
- **rule.mail: true** confirms that in a real world deployment with SMTP configured, a critical alert email would be dispatched automatically to responsible figures.
- This demonstrates the ability to extend Wazuh **beyond** default rules to cover organization-specific threat scenarios and custom compliance requirements

SECTION 4 — COMPLIANCE MAPPING SUMMARY

5. Compliance Mapping Summary

5.1 Cross-Framework Control Coverage

The following table summarizes how each test scenario maps across **NIST SP 800-53, MITRE ATT&CK**, and other compliance frameworks. All mappings were automatically generated by Wazuh with no manual tagging required.

Scenario	NIST SP 800-53	MITRE ATT&CK	Compliance Tags
Brute-Force / Auth Failure	**CA-7, AC-7, AU-14**	**T1110.001 — Password Guessing**	**PCI-DSS 10.2.4 HIPAA 164.312.b GDPR IV_35.7.d**
Privilege Escalation	**AC-6, AU-9, SI-2**	**T1548.003 — Sudo Caching**	**PCI-DSS 10.2.5 TSC CC6.8 CC7.2**
File Integrity Monitoring	**SI-7, AU-9, CM-3**	**T1565 — Data Manipulation**	**PCI-DSS 11.5 HIPAA 164.312.c.1**
New User Creation (Custom)	**AC-2, IA-2, AU-12**	**T1136 — Create Account**	**PCI-DSS 8.1 GDPR IV_35.7.d GPG13 4.13**

5.2 Loi 05-20 Alignment

Morocco's Loi 05-20 on Cybersecurity (Introduced July 25, 2020) establishes a legal framework for protecting information systems of public entities and critical infrastructures. The law organizes its security requirements around three core axes: risk detection and management, security incident notification, and protective measures for information systems. The following capabilities validated in this lab directly address those axes:

- **Risk Detection & Monitoring:** Continuous real-time detection of credential attacks and privilege escalation attempts, satisfying the law's requirement for active monitoring of information system threats.
- **Incident Notification:** Wazuh's automatic severity escalation and alerting capabilities align with the law's incident reporting obligations.
- **Information System Integrity: FIM (File Integrity Monitoring)** with cryptographic hash verification directly addresses the law's requirement to preserve the integrity and availability of sensitive information systems *(per Articles 5 and 14 on IS classification and impact analysis)*

6. Recommendations

The following recommendations are drawn directly from observations made during this testing:

High	**Configure SMTP for Production Alerting** During custom rule testing, **rule.mail: true** fired on the Critical level 15 alert, Confirming the alerting pipeline is active but unconnected. Configuring **SMTP** in **/var/ossec/etc/ossec.conf** would operationalize this immediately, ensuring critical events like new user creation trigger email notifications to an on-call address without requiring dashboard access.
High	**Increase FIM Scan Frequency on Critical Paths** The default syscheck frequency of **43,200 seconds (12 hours)** means a file dropped in a directory containing sensitive files could go undetected for up to half a day in normal operation. Reducing the frequency to **300–600 seconds** for **high-sensitivity paths (/etc, /bin, /sbin)** would significantly reduce detection latency without meaningful performance impact.
High	**Expand FIM to Include User Home Directories** Current FIM coverage targets system binaries and **/etc**. Extending monitoring to **/home** and **/root** would catch attacker-placed persistence artifacts.
Medium	**Integrate a Threat Intelligence Feed** The brute-force simulation successfully detected the attack pattern but had no visibility into whether the source IP was a known threat actor. Integrating Wazuh with a commercial **threat intelligence** feed such as **AlienVault OTX** or **VirusTotal** would enrich alerts with reputation data.
Medium	**Implement Active Response Rules** Wazuh supports automated active response actions triggered by alert thresholds. For example, **automatically blocking** a source IP via **iptables** after **5** consecutive failed authentication attempts. Given that detection is now validated, the logical next layer is **automated containment**.
Low	**Enable Wazuh Vulnerability Detection Module** Wazuh includes a **built-in vulnerability detection module that** cross-references installed packages against the **NVD (National Vulnerability Database).** Enabling this on both endpoints would add a passive **CVE identification** layer to the existing detection capabilities.

7. Conclusion

The live testing of the Wazuh SIEM homelab environment successfully validated its core detection capabilities across critical security domains. The environment proved highly effective in detecting and correlating sophisticated attack patterns, maintaining system integrity, and supporting custom threat intelligence.

Key takeaways from the testing include:

- **Real-Time Threat Detection:** The platform demonstrated immediate and accurate detection of brute-force and privilege escalation attempts **(simulated via sudo failures)**, showcasing its ability to rapidly detect and escalate events into determined attack patterns.

- **Forensic and Integrity Assurance: File Integrity Monitoring (FIM)** successfully identified unauthorized changes to critical system directories, automatically generating detailed forensic metadata for threat analysis and response.

- **Extensibility and Customization:** The successful deployment of a custom rule to detect new user account creation validates the platform's flexibility, allowing security teams to tailor monitoring to organization-specific needs.

- **Automated Compliance Mapping:** Arguably the most important security feature, all of the security alerts were automatically tagged and mapped against five major security and regulatory frameworks **(NIST SP 800-53, MITRE ATT&CK, PCI-DSS, HIPAA, and GDPR)** with zero manual configuration. This capability significantly streamlines audit preparation and ensures continuous regulatory compliance, particularly satisfying requirements under **Loi 05-20** for Moroccan based enterprises.