INFORMATION SECURITY

Gap Analysis Report

Wazuh SIEM Homelab Environment

Date: March 2026
Scope: Wazuh SIEM Homelab (Azure VM + WSL Endpoints)
NIST SP 800-53 Rev. 5 | ISO/IEC 27001:2022 | Loi 05-20

1. Executive Summary

This gap analysis evaluates the security posture of a cloud-native Wazuh SIEM homelab environment against three frameworks: NIST SP 800-53 Revision 5, ISO/IEC 27001:2022, and Morocco's Loi 05-20 on Cybersecurity. The assessment is grounded in live testing results documented in the accompanying Technical Detection Report.

The environment demonstrates strong detection and monitoring capabilities. This is validated through live attack simulations, File Integrity Monitoring, and custom rule deployment. However, several governance, process, and configuration gaps exist that would need to be addressed before the environment could be considered fully compliant with any of the three frameworks.

Framework	Satisfied	Partial	Gap	Overall
NIST SP 800-53 Rev. 5	**6**	**4**	**3**	**Partial**
ISO/IEC 27001:2022	**5**	**4**	**3**	**Partial**
Loi 05-20 (Morocco)	**3**	**2**	**2**	**Partial**

2. Scope & Methodology

2.1 Scope

This assessment covers the Wazuh SIEM homelab environment documented in the Technical Detection Report. The scope includes the Wazuh Manager on Azure, two monitored endpoints (Windows 10 and WSL Ubuntu), Azure NSG network controls, and detection rule and FIM configuration. Physical security, third-party supplier management, and HR controls are out of scope for this homelab environment.

2.2 Assessment Status Definitions

✓ **SATISFIED**	The control is fully implemented and validated by live evidence from the Technical Detection Report.
~ PARTIAL	The control is partially implemented. Technical capability exists but policy, process, or configuration gaps remain.
✗ GAP	The control is not implemented. No technical capability or documented process exists to satisfy the requirement.

Assessment Date	March 2026
Evidence Source	Wazuh SIEM Technical Detection Report (March 14, 2026)
NIST Version	SP 800-53 Revision 5
ISO Version	ISO/IEC 27001:2022 (Annex A controls referenced as A.X.XX)
Loi 05-20	Loi n° 05-20 relative à la cybersécurité, promulguée le 25 juillet 2020

PART 1 — NIST SP 800-53 REV. 5 GAP ANALYSIS

3. NIST SP 800-53 Rev. 5

3.1 Control Assessment

Controls were selected based on direct relevance to a SIEM monitoring environment. All control IDs and names are drawn from NIST SP 800-53 Revision 5 (published September 2020, updated January 2022). Controls outside the scope of a detection-focused deployment are excluded.

Control ID	Control Name	Status	Observation / Evidence	Risk
CA-7	Continuous Monitoring	✓ SATISFIED	Real-time alerting validated by live attack simulation. rule.firedtimes escalation from 1 to 10 proves sustained pattern detection and correlation, not just single-event logging.	Low
AC-7	Unsuccessful Logon Attempts	✓ SATISFIED	Rules 5401 and 5503 fired on each failed sudo attempt with full metadata: user, destination (root), command (/usr/bin/ls), TTY. Directly satisfies AC-7 audit trail requirements.	Low
AU-2	Event Logging	✓ SATISFIED	PAM, sudo, and syscheck events captured and forwarded to Wazuh Manager. Coverage includes authentication, privilege use, session open/close, and file integrity events.	Low
AU-12	Audit Record Generation	✓ SATISFIED	Wazuh agents generate structured audit records with timestamps, agent ID, rule ID, and auto-populated compliance tags on both endpoints.	Low
SI-7	Software, Firmware, and Information Integrity	✓ SATISFIED	FIM validated via live test: SHA256, MD5, SHA1 hashes captured on file creation in /etc within 60 seconds. Cryptographic verification of file state is operational.	Low
AC-2	Account Management	~ PARTIAL	Custom rule 100001 detects new user creation (T1136, Critical level 15). No formal account lifecycle policy exists and no detection of dormant or unauthorised accounts beyond creation events.	Medium
AU-9	Protection of Audit Information	~ PARTIAL	Logs forwarded to Wazuh Manager but no immutability or tamper-evident storage configured. A root-level attacker could modify /var/log/auth.log before Wazuh ingestion.	Medium
IR-4	Incident Handling	~ PARTIAL	Detection and alerting are operational. No formal Incident Response Plan or runbook exists.	Medium

Control ID	Control Name	Status	Observation / Evidence	Risk
SC-7	Boundary Protection	~ PARTIAL	Azure NSG enforces least privilege: TCP 1514/1515, whitelisted SSH, HTTPS 443, implicit deny. No IDS/IPS layer exists beyond Wazuh alert-based detection.	Medium
RA-5	Vulnerability Monitoring and Scanning	✗ GAP	Wazuh vulnerability detection module not enabled. No CVE scanning or patch management process documented or operational on any endpoint.	High
PL-2	System Security Plans	✗ GAP	No formal System Security Plan documents the environment's security architecture, control baselines, or risk acceptance decisions.	Medium
CP-9	System Backup	✗ GAP	No backup or recovery strategy documented for the Wazuh Manager VM. Azure outage or VM compromise results in total loss of configuration and historical alerts.	High

3.2 Key Observations

- The environment's strongest area is audit and monitoring. CA-7, AC-7, AU-2, AU-12, and SI-7 are all fully satisfied with live evidence
- The most significant gaps are operational and governance-focused: no vulnerability scanning (RA-5), no formal System Security Plan (PL-2), and no backup strategy (CP-9)
- Audit log protection (AU-9) is the highest-risk partial control: logs on the endpoint are vulnerable to tampering before Wazuh ingests them
- Incident Response (IR-4) is partially satisfied by detection capability but requires a written process and connected alerting to meet full compliance

PART 2 — ISO/IEC 27001:2022 GAP ANALYSIS

4. ISO/IEC 27001:2022

4.1 Control Assessment

Controls are referenced using the ISO/IEC 27001:2022 Annex A numbering scheme (93 controls across four themes: Organisational 5.x, People 6.x, Physical 7.x, Technological 8.x). One entry references Clause 6.1 of the main body (risk treatment), which is distinct from Annex A and is clearly labelled as such.

Control ID	Control Name	Status	Observation / Evidence	Risk
A.8.15	Logging	✓ SATISFIED	Wazuh captures structured logs across all endpoints with timestamps, agent ID, rule ID, user context, and compliance tags. Evidence documented in Technical Report Section 2.	Low
A.8.16	Monitoring Activities	✓ SATISFIED	Real-time monitoring operational. Histogram spike demonstrates event correlation and timeline reconstruction during the simulated attack.	Low
A.8.7	Protection Against Malware	✓ SATISFIED	FIM detects unauthorised file placement in /etc. Custom rule 100001 detects new account creation (T1136, MITRE ATT&CK).	Low
A.8.8	Management of Technical Vulnerabilities	~ PARTIAL	Wazuh SCA performs CIS Benchmark auditing on both endpoints. Vulnerability detection module is a remaining gap but SCA layer partially satisfies A.8.8.	Low
A.5.26	Response to IS Incidents	~ PARTIAL	Alerting pipeline operational with MITRE tactic tagging enabling structured triage. Active response capability exists in Wazuh but is not yet configured.	Low
A.8.17	Clock Synchronisation	~ PARTIAL	Timestamps in Wazuh alerts are consistent within sessions (UTC observed). No NTP synchronisation policy is documented across all endpoints.	Low
A.5.28	Collection of Evidence	~ PARTIAL	Wazuh generates detailed forensic metadata (hashes, permissions, user context). No formal evidence preservation or chain-of-custody process documented for legal proceedings.	Medium

Control ID	Control Name	Status	Observation / Evidence	Risk
Clause 6.1	Risk Treatment (Main Body)	~ PARTIAL	Technical controls address known risks. No formal risk assessment or risk treatment plan has been produced prior to this document. Note: Clause 6.1 is a main body requirement, not an Annex A control.	Medium
A.5.29	Information Security During Disruption	~ PARTIAL	No business continuity or disaster recovery plan exists for the monitoring environment. An Azure region outage would disable all detection capability with no failover.	Medium
A.5.5	Contact with Authorities	✗ GAP	No process exists for notifying DGSSI or other competent authorities in the event of a significant security incident. Cross-framework gap with Loi 05-20 Art. 8.	Medium
A.5.36	Compliance with IS Policies, Rules and Standards	✗ GAP	No Information Security Policy document exists. Without a baseline policy, compliance cannot be formally assessed or demonstrated to third parties or auditors.	High
A.8.32	Change Management	✗ GAP	Configuration changes to Wazuh rules and agent settings are made without a formal change management process. No change log or approval workflow documented.	Medium

4.2 Key Observations

- **ISO 27001:2022** places greater emphasis on documented processes and organisational controls, this is where the environment's gaps are most concentrated
- The absence of an IS Policy (A.5.36) is the highest-priority gap as it is a foundational document of the ISMS (Information Security Management System)
- **A.5.5** (Contact with Authorities) is a gap with direct cross-framework relevance to Loi 05-20, making it a dual-framework high priority item.
- **Clause 6.1** (Risk Treatment) is partially addressed by this gap analysis document itself which constitutes a formal risk identification and treatment input

PART 3 — LOI 05-20 GAP ANALYSIS

5. Loi 05-20 (Morocco Cybersecurity Law)

5.1 Framework Overview

Loi n° 05-20 relative à la cybersécurité was promulgated on July 25, 2020. It establishes Morocco's national cybersecurity framework with obligations for public entities and critical infrastructure operators. Controls below are mapped to specific articles of the law as published.

5.2 Article Reference Summary

Art. 4	Each entity must develop and implement an IS security policy; identify risks; take technical and organisational measures; and undergo regular IS audits.
Art. 5	Each entity must classify its informational assets and IS by sensitivity (confidentiality, integrity, availability) and apply proportionate protection measures.
Art. 6	Each entity must designate a Responsable de la Sécurité des Systèmes d'Information (RSSI) who is the interlocutor with the national authority.
Art. 7	Each entity must put in place appropriate monitoring and detection means for events likely to affect the security of its IS.
Art. 8	Each entity must declare any incident affecting security or functioning of its IS to the national authority (DGSSI) as soon as it becomes aware of it.
Art. 9	Each entity must prepare a business continuity or recovery plan, tested regularly, covering IS failures and disasters.

5.3 Control Assessment

Control ID	Control Name	Status	Observation / Evidence	Risk
Art. 4 + 5	IS Policy, Risk Management & Asset Classification	✓ **SATISFIED**	Azure NSG rules enforce least privilege. AES-256 encrypted agent tunnels secure log transport. FIM enforces proportionate protection on classified system paths (/etc, /bin, /sbin). Technical measures are operational and validated.	**Low**
Art. 7	Detection Monitoring Means	✓ **SATISFIED**	Wazuh provides real-time detection across all endpoints with MITRE ATT&CK tactic tagging. Validated against credential attacks, FIM events, and custom persistence scenarios. Fully satisfies Art. 7's monitoring requirement.	**Low**

Control ID	Control Name	Status	Observation / Evidence	Risk
Art. 5	IS Asset Classification	✓ SATISFIED	Monitored directories are implicitly classified by sensitivity (/etc, /bin for high-sensitivity; endpoints categorised by role). FIM scope reflects proportionate protection per Art. 5.	Low
Art. 8 + 4	Incident Notification to DGSSI & IS Auditing	~ PARTIAL	Wazuh generates structured incident evidence (alerts, hashes, MITRE tags) that could form the basis of an Art. 8 declaration. However, no notification procedure or contact exists for DGSSI. Art. 4 auditing is partially met by this gap analysis but no recurring audit schedule is defined.	Medium
Art. 9	Business Continuity / Recovery Plan	~ PARTIAL	No business continuity or recovery plan exists for the monitoring environment. An Azure outage would disable detection capability entirely. Partially addressed by recommending VM backup configuration.	Medium
Art. 4 + 6	IS Policy Document & RSSI Designation	✗ GAP	No Information Security Policy document exists as required by Art. 4. No RSSI (or equivalent responsible person) has been formally designated as required by Art. 6. These are foundational governance requirements.	High
Art. 8	DGSSI Incident Notification Procedure	✗ GAP	No documented process for reporting significant incidents to the national authority (DGSSI) as required by Art. 8. For any Moroccan entity in scope, this would constitute a direct regulatory non-compliance in the event of an incident.	High

5.4 Key Observations

- Art. 7 (detection monitoring) is the strongest alignment point. The Wazuh environment directly and fully satisfies Morocco's legal requirement for IS monitoring means.
- Art. 8 (DGSSI notification) remains the most operationally critical gap.
- Art. 4 and Art. 6 together form the governance foundation of the law: The absence of both an IS policy and a designated RSSI means the environment's technical controls cannot be formally governed or attributed.

PART 4 — CONSOLIDATED RISK REGISTER

6. Consolidated Risk Register

The following risk register consolidates the highest-priority gaps across all three frameworks. Residual risk is assessed on likelihood and impact given the current state of the environment.

ID	Risk Description	Likelihood	Impact	Risk Rating	Recommended Control	Framework Ref.
R-01	No IS Policy document exists. Compliance cannot be formally demonstrated to any auditor or third party	High	High	High	Draft and publish a foundational IS Policy covering access, classification, incidents, and acceptable use	*ISO A.5.36, Loi Art. 4 & 6*
R-02	No backup for Wazuh Manager VM. Total configuration and alert loss on failure or outage	Medium	High	High	Implement Azure VM snapshots with tested recovery procedure	*NIST CP-9, Loi Art. 9*
R-03	Wazuh vulnerability detection module not enabled. unpatched CVEs may not get detected	Medium	High	High	Enable vulnerability detection module; establish patch review cadence	*NIST RA-5, ISO A.8.8*
R-04	No DGSSI notification procedure. Regulatory obligation unmet.	Low	High	High	Document and test an incident notification procedure targeting DGSSI	*Loi Art. 8, ISO A.5.5*
R-05	Audit logs stored on endpoint before ingestion. vulnerable to tampering	Medium	Medium	Medium	Forward logs to WORM/immutable storage or enable Wazuh log signing	*NIST AU-9, ISO A.8.15*
R-06	No formal Incident Response Plan. detection exists but the response process does not.	Medium	Medium	Medium	Draft a minimal IRP with defined roles, escalation steps, and SMTP configured	*NIST IR-4, ISO A.5.26*
R-07	No change management for Wazuh rule/config modifications	Low	Medium	Medium	Implement a change log and peer review process for all rule modifications	*ISO A.8.32*
R-08	FIM scan frequency of 12 hours creates detection window for file-based persistence	Medium	Medium	Medium	Reduce syscheck frequency to 300–600 seconds on high-sensitivity paths	*NIST SI-7, ISO A.8.15*

PART 5 — REMEDIATION ROADMAP

7. Remediation Roadmap

Actions are prioritised by risk level and sequenced so that foundational governance items are completed before technical enhancements. All High-priority items require no new infrastructure as they are documentation or configuration tasks achievable within days.

Priority	Action	Framework(s)	Effort	Timeframe
High	Draft an IS Policy (access control, classification, incident handling, acceptable use)	*ISO A.5.36, Loi Art. 4 & 6*	Low doc only	Week 1
High	Configure Azure VM backup / snapshot with tested recovery procedure	*NIST CP-9, Loi Art. 9*	Low Azure native	Week 1
High	Enable Wazuh vulnerability detection module on both endpoints	*NIST RA-5, ISO A.8.8*	Low config	Week 1
High	Document a DGSSI incident notification procedure	*Loi Art. 8, ISO A.5.5*	Low doc only	Week 1–2
Medium	Configure SMTP on Wazuh Manager to activate rule.mail alerting	*NIST IR-4, ISO A.5.26*	Low config	Week 2
Medium	Draft a minimal Incident Response Plan with roles and escalation steps	*NIST IR-4, ISO A.5.26*	Medium process	Week 2–3
Medium	Reduce FIM scan frequency to 300–600 seconds on /etc, /bin, /sbin	*NIST SI-7, ISO A.8.15*	Low config	Week 2
Medium	Forward logs to immutable storage or enable Wazuh log integrity checking	*NIST AU-9, ISO A.8.15*	Medium technical	Week 3–4
Medium	Implement a change log for Wazuh rule and configuration modifications	*ISO A.8.32*	Low process	Week 3
Low	Author additional custom rules	*NIST CA-7, SI-7*	Medium technical	Month 2
Low	Integrate AlienVault OTX or VirusTotal threat intelligence feed	*NIST CA-7, ISO A.8.16*	Medium technical	Month 2
Low	Expand FIM scope to include /home and /root directories	*NIST SI-7, ISO A.8.15*	Low config	Month 2

8. Conclusion

This gap analysis confirms that the homelab environment has a strong technical foundation, particularly in continuous monitoring, audit logging, file integrity, and detection rule coverage.

However, a consistent pattern emerges across NIST SP 800-53, ISO 27001:2022, and Loi 05-20: the environment's governance and process layer is largely absent. There is no Information Security Policy, no Incident Response Plan, no formal risk treatment documentation, and no backup or recovery strategy. These are foundational requirements that can't be satisfied by technical controls alone.

Critically, the highest-priority remediation actions are also the lowest-effort: drafting an IS Policy, configuring VM backups, enabling vulnerability scanning, and documenting a DGSSI notification procedure are all achievable within a week with no new infrastructure.

This document, together with the Technical Detection Report, constitutes a complete and verifiable security assessment of the homelab environment, providing recommendations and steps for remediation and strengthening of the overall security posture.