SOC Incident Report

Project 2 — Windows Endpoint Detection & Response

Date: Lab Simulation
Analyst: Tawanda Ngazimbi
Monitoring Platform: Wazuh
Endpoint: Windows 11
SOC Environment: Isolated Virtual SOC Lab

---

1. Executive Summary

During routine monitoring of Windows endpoint telemetry, the SOC detected two distinct security events:

1. A sequence of **failed authentication attempts**, indicative of a potential brute-force attack.

2. A **Windows service creation event**, commonly associated with persistence techniques.

Both events were investigated, triaged, and documented following standard SOC incident-handling procedures. The activity was confirmed to be **intentional lab simulation**, conducted to validate detection and response capabilities.

---

2. Environment Overview

- **SIEM:** Wazuh Manager (Ubuntu)
- **Endpoint Agent:** Wazuh Agent on Windows 11
- **Network:** Internal isolated SOC-LAB network
- **Log Sources:** Windows Security Event Logs

---

3. Incident A — Authentication Brute Force Attempt

Detection

- **Rule Group:** `authentication_failed`
- **Event ID:** 4625
- **Alert Severity:** Medium
- **Description:** Failed logon attempt – unknown user or bad password

Multiple authentication failures were detected within a short timeframe on the Windows endpoint.

Analysis & Triage

- Confirmed repeated failed logon attempts against the same endpoint.
- No successful authentication followed the failures.
- No evidence of account lockout, privilege escalation, or lateral movement.
- Activity originated locally and was not externally sourced.

MITRE ATT&CK Mapping

- **T1110 — Brute Force**
- **T1110.001 — Password Guessing**

Outcome

- **Classification:** Benign (Lab Simulation)

- **Impact:** None
- **Response:** No containment required
- **Result:** Authentication failure detection validated successfully

---

4. Incident B — Windows Service Creation (Persistence)

Detection

- **Rule Group:** `windows_security`
- **Event ID:** 4697
- **Alert Severity:** High
- **Description:** A service was installed on the system

Service creation is a common persistence mechanism used by attackers to maintain access.

Analysis & Triage

- Identified the creation of a non-standard service (`TestService`).
- Reviewed binary path and execution context.
- No indicators of malicious payload execution or further persistence activity.
- Service was removed immediately after creation as part of controlled testing.

MITRE ATT&CK Mapping

- **T1543.003 — Create or Modify System Process: Windows Service**

Outcome

- **Classification:** Benign (Lab Simulation)
- **Impact:** None
- **Response:** Service removal confirmed
- **Result:** Persistence detection and alerting validated successfully

---

5. Analyst Assessment

These incidents demonstrate effective:

- Log ingestion and normalization
- Alert generation and prioritisation
- Threat classification using MITRE ATT&CK
- Incident triage and decision-making
- Clear documentation and reporting

No further remediation actions were required.

---

6. Lessons Learned & Improvements

- Failed logon thresholds can be tuned to reduce noise while maintaining visibility.
- Service creation alerts should remain high-priority due to persistence risk.
- Incident documentation ensures repeatability and audit readiness.

---

7. Final Conclusion

The SOC successfully detected, analysed, and resolved both authentication and persistence-related security events. This project confirms that the monitoring environment, detection rules, and analyst workflows are operating as intended and provides a solid foundation for future threat-hunting and response simulations.