INCIDENT REPORT – USE CASE 1

File Integrity Monitoring (Ubuntu Agent)

Incident ID: SOC-FIM-001
Incident Title: Unauthorized Modification of Critical System File
Date & Time: Jan 18, 2026 @ 15:33:00
Detection Source: Wazuh SIEM – File Integrity Monitoring (Syscheck)

Affected Asset
Host: Ubuntu Agent
Asset Type: Linux Endpoint
Severity: Medium

Incident Summary
Wazuh SIEM detected a modification to a critical system file on the Ubuntu endpoint using its File Integrity Monitoring capability. Unauthorized changes to system files may indicate insider activity, privilege misuse, or persistence techniques if performed maliciously.

Detection Details
Monitored File: /etc/passwd
Event Type: File Modified
Wazuh Rule ID: 550
Rule Level: 7
Detection Module: Syscheck (FIM)
Agent Operating System: Ubuntu Linux

Investigation and Analysis
The alert timestamp and affected file were reviewed to validate the event. System logs and recent user activity were analyzed around the time of detection. The file modification was confirmed to have been manually performed for testing purposes. No additional indicators of compromise were identified during the investigation.

Classification
True Positive – Authorized Activity (Test Case Validation)

Root Cause
Authorized manual modification of a monitored system file performed to validate the effectiveness of the File Integrity Monitoring control.

Impact Assessment
No service disruption was observed. There was no evidence of malicious persistence, privilege escalation, or system compromise. The security control functioned as expected by detecting the file modification.

Response Actions
The alert was reviewed and validated by the SOC analyst. The modified file contents were verified. No remediation actions were required due to the activity being part of a controlled test scenario.

Lessons Learned
File Integrity Monitoring effectively detects unauthorized or unexpected changes to critical system files. Such alerts are valuable for early identification of persistence attempts and configuration tampering activities.

MITRE ATT&CK Mapping
Technique ID: T1565.001
Technique Name: Stored Data Manipulation

Incident Status

Closed – Informational (Test Case Validation)