Samson Schmidt 2026

Security Monitoring Lab Using Wazuh SIEM

Overview

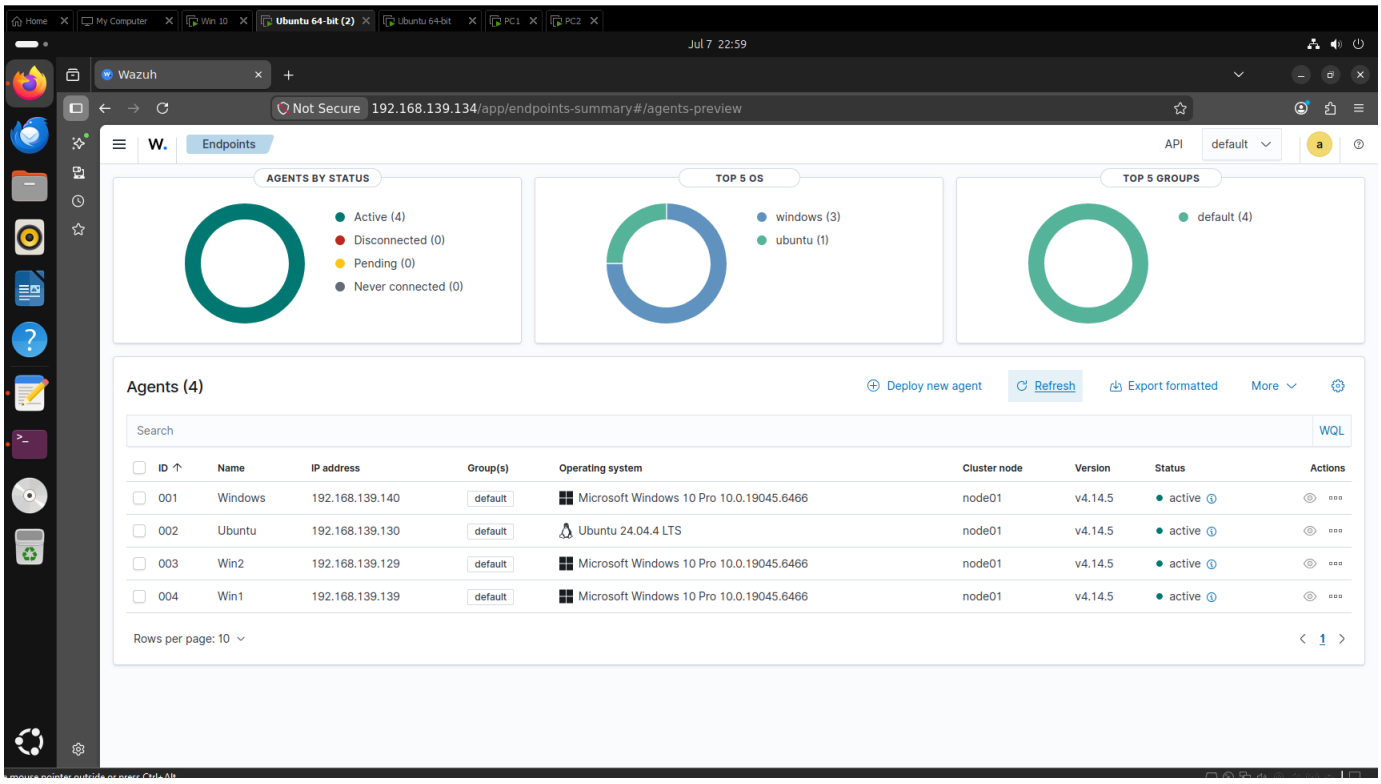
Built a virtualized security monitoring environment using VMware and Wazuh to simulate enterprise-level endpoint security operations. Configured multiple Windows and Linux systems for centralized monitoring, vulnerability detection, and file integrity monitoring (FIM).

Step 1: SIEM Deployment & Endpoint Enrollment

Deployed the Wazuh platform in a VMware lab and connected four endpoints for centralized security monitoring.

Configured the environment with:

- Three Windows endpoints and one Ubuntu Linux endpoint
- Wazuh agents installed and reporting as active
- Centralized endpoint visibility through the Wazuh dashboard
- A controlled lab network for testing security events and alerts

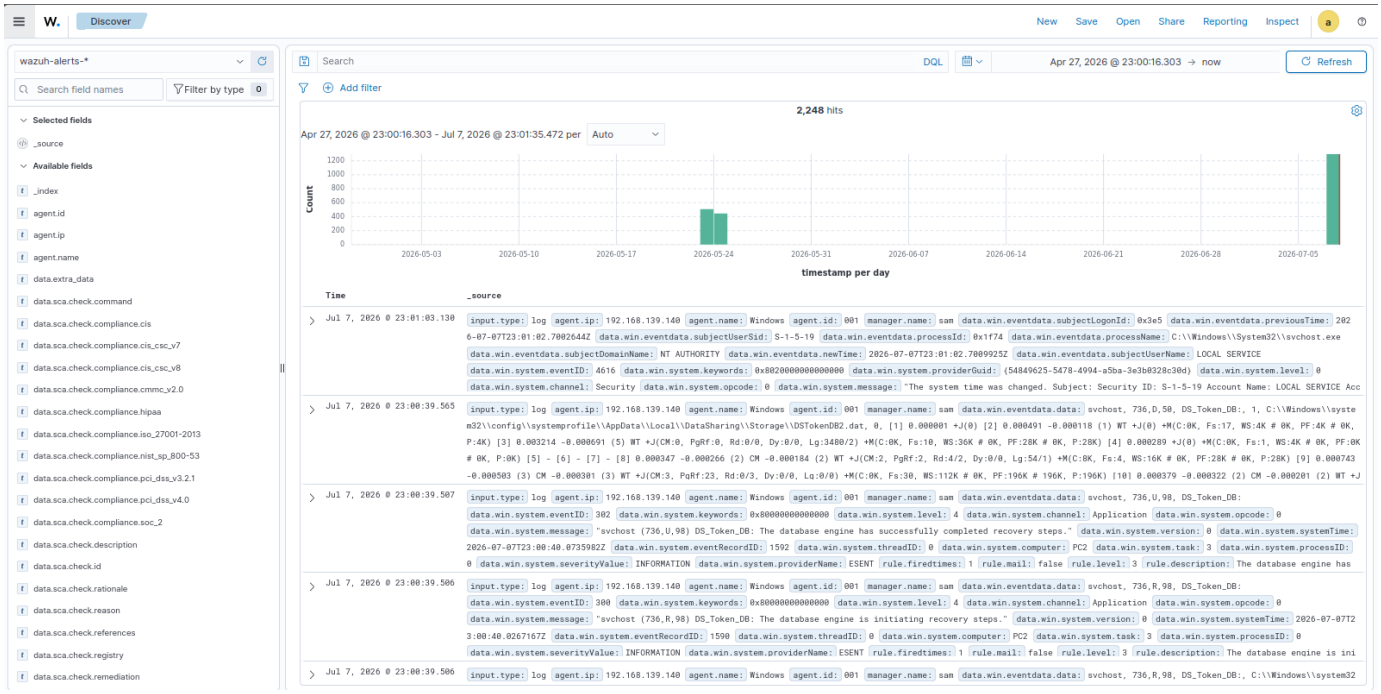


Step 2: Centralized Log Collection & Event Analysis

Collected security telemetry from monitored endpoints and reviewed events in Wazuh Discover to practice SIEM investigation workflows.

Analyzed event data including:

- Windows security and application logs
- Agent names, IP addresses, and event timestamps
- Event IDs, severity levels, and rule descriptions
- Raw event fields used to investigate endpoint activity

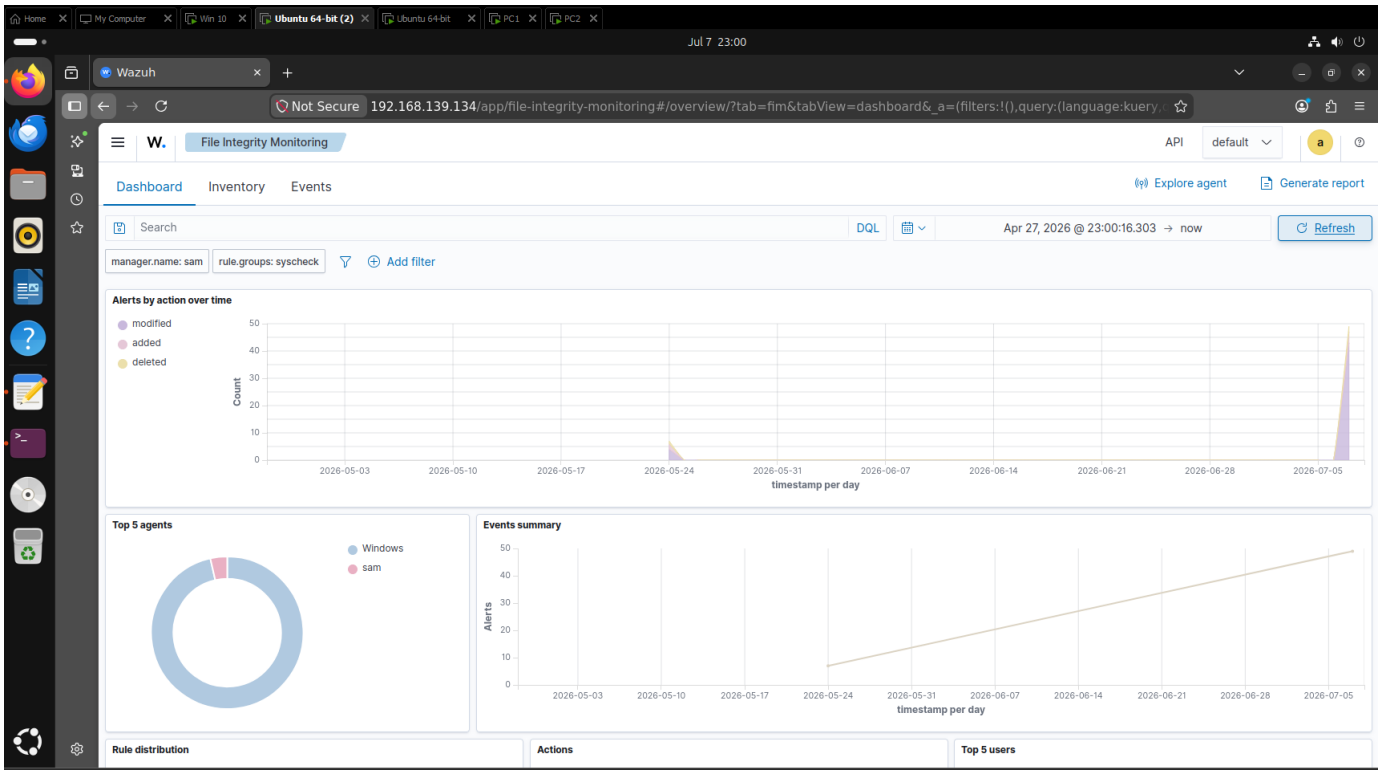


Step 3: File Integrity Monitoring (FIM)

Configured and reviewed file integrity monitoring alerts to identify changes made to files and registry locations on monitored systems.

Monitored for:

- Files and registry entries that were added, modified, or deleted
- FIM alert activity over time
- Affected agents and user accounts
- Rule distribution and change-related event patterns

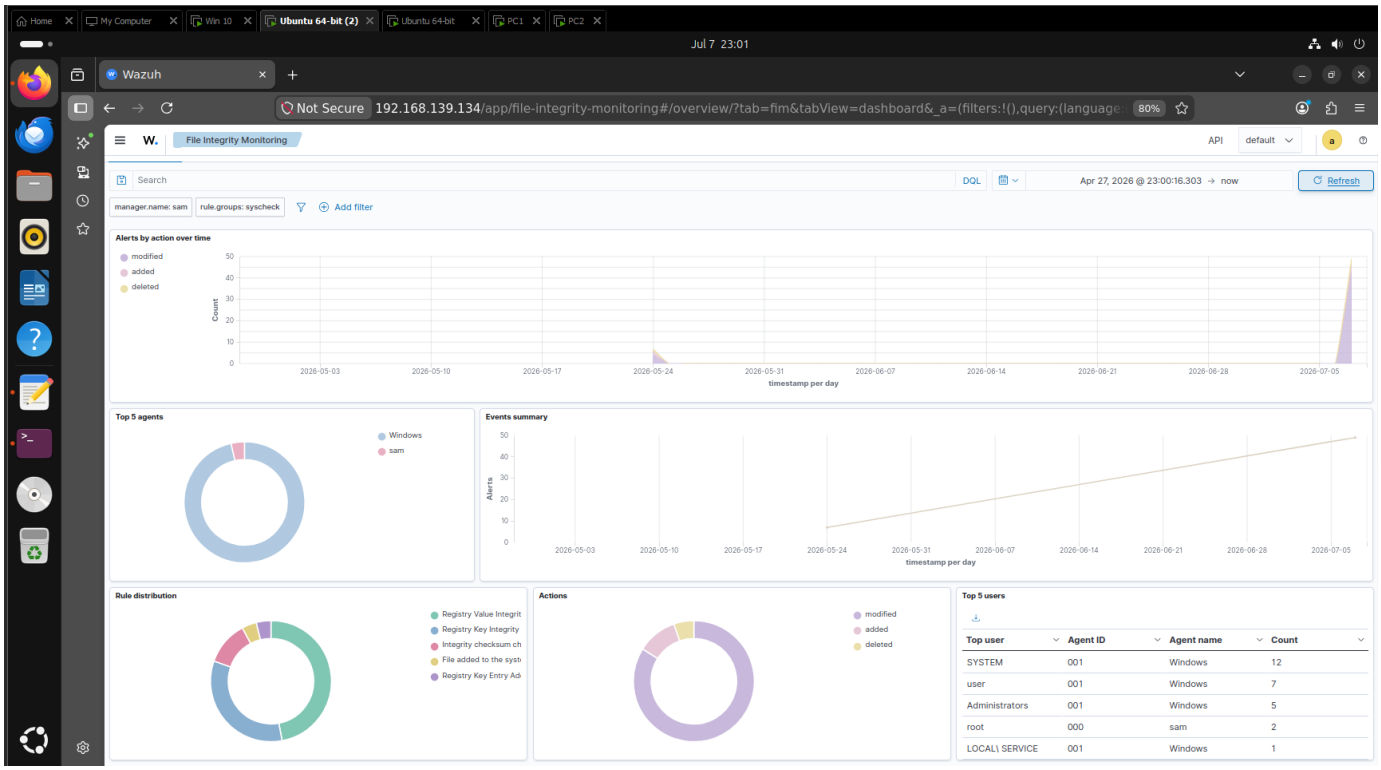


Step 4: FIM Alert Review & Investigation

Used the expanded FIM dashboard to review alert trends, affected users, rule distribution, and the actions associated with detected changes.

The investigation focused on:

- Comparing modified, added, and deleted activity
- Identifying the endpoints generating the most FIM alerts
- Reviewing user and service accounts tied to changes
- Using dashboard summaries to prioritize deeper event review

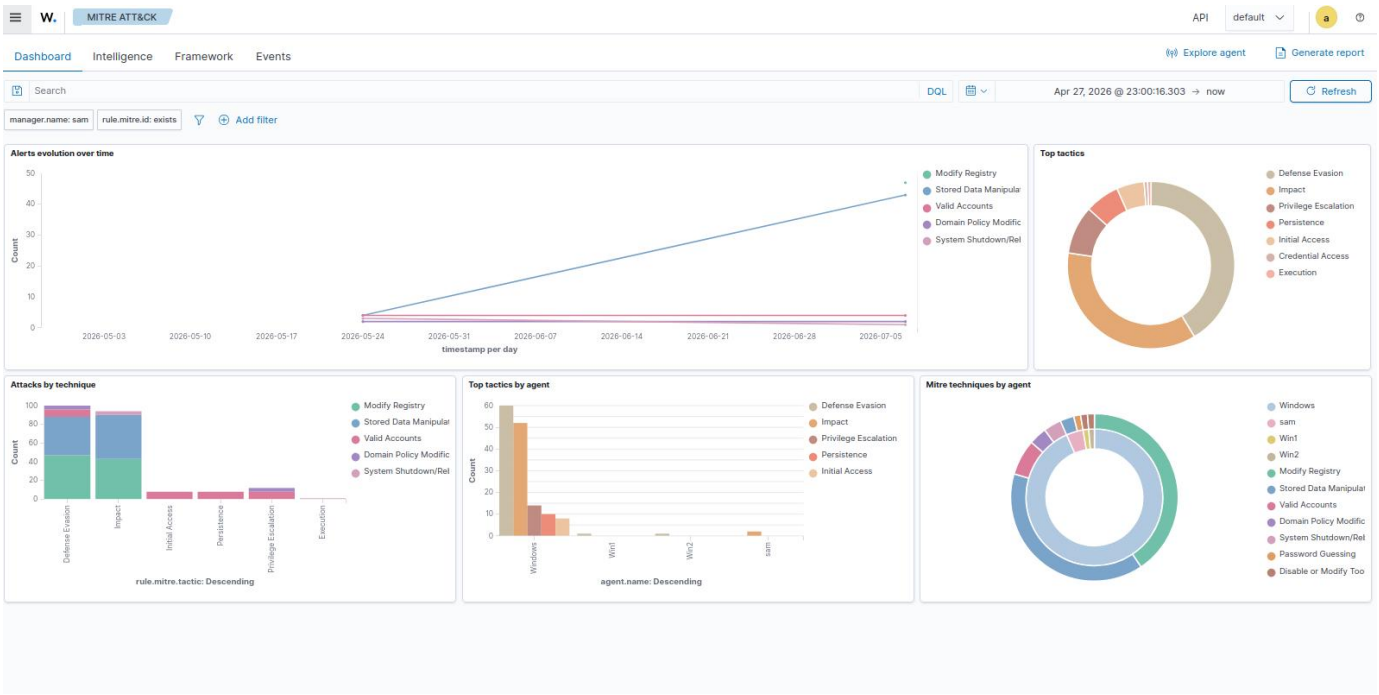


Step 5: MITRE ATT&CK Mapping

Reviewed Wazuh alerts mapped to the MITRE ATT&CK framework to connect endpoint activity with recognized adversary tactics and techniques.

Observed mappings included:

- Defense Evasion and Impact
- Privilege Escalation and Persistence
- Initial Access, Credential Access, and Execution
- Techniques such as Modify Registry, Valid Accounts, and Stored Data Manipulation

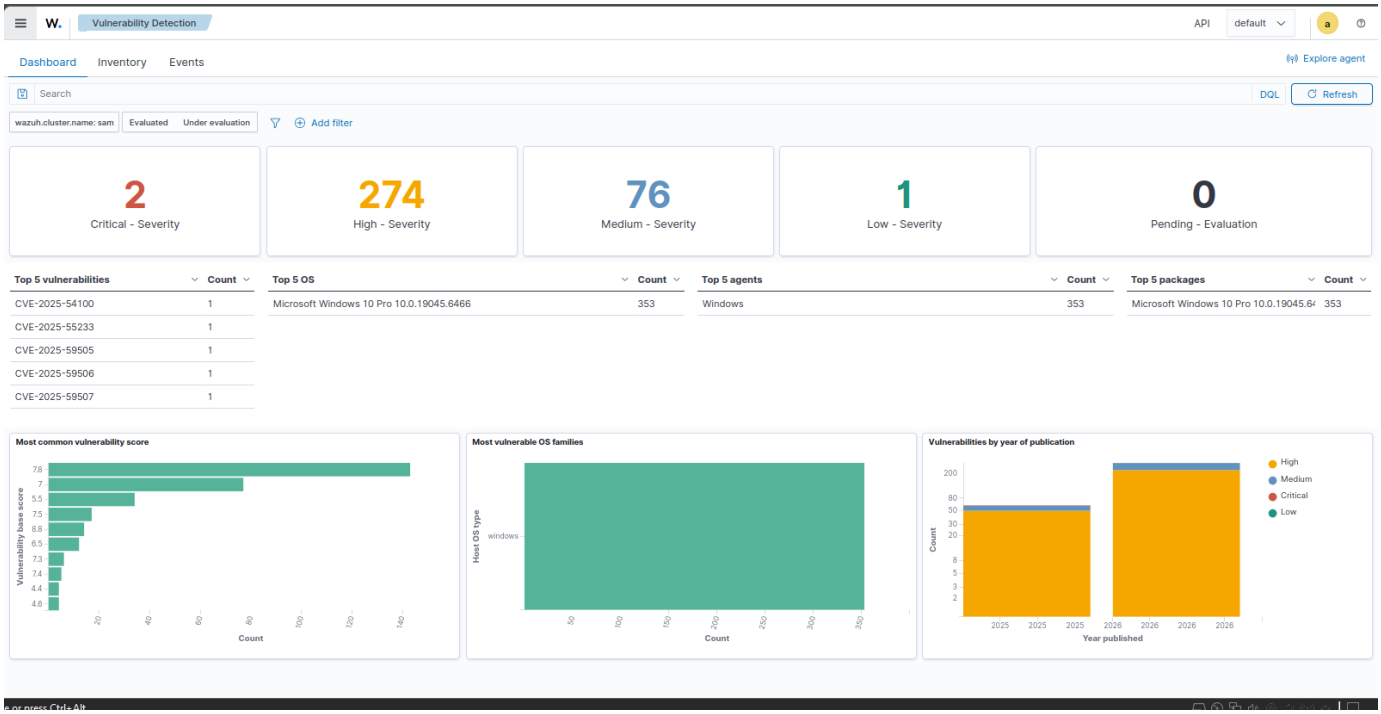


Step 6: Vulnerability Detection & Assessment

Used Wazuh vulnerability detection to identify and categorize endpoint exposure based on severity and affected software packages.

Reviewed:

- Critical, high, medium, and low-severity findings
- CVE identifiers and affected operating systems
- Vulnerability scores and publication years
- Endpoints and packages requiring remediation or further validation



Project Outcome

Successfully built and operated a multi-endpoint Wazuh SIEM lab that provided centralized visibility across Windows and Linux systems. The project delivered hands-on experience with SIEM deployment, endpoint onboarding, security event investigation, file integrity monitoring, MITRE ATT&CK mapping, and vulnerability assessment.

Key skills demonstrated:

- SIEM deployment and configuration
- Windows and Linux endpoint monitoring
- Centralized log collection and security event analysis
- File integrity monitoring setup and alert investigation
- MITRE ATT&CK-based alert interpretation
- Vulnerability detection and risk prioritization