Windows Security Monitoring and Threat Detection using Wazuh SIEM

Subject: **Windows Security Monitoring and Threat Detection using Wazuh SIEM**

Incident ID: IR-2025-1222-007

PREPARED BY:

Vignesh K.

SOC Analyst / Security Researcher

CERTIFICATIONS: Google Cybersecurity Professional

REPORT DATE: December 22, 2025

1. Overview

- **Project Focus:** Setup and demonstration of host-based security monitoring on a Windows 11 endpoint.
- **Platform Used:** Wazuh Security Information and Event Management (SIEM) platform (v4.14.1).
- **Primary Objective:** Validate Wazuh's effectiveness in collecting, analyzing, and alerting on Windows security events.
- **Outcome:** Established a baseline/foundational threat detection framework suitable for an entry-level Security Operations Center (SOC).

2. Technical Environment

The following table details the key components utilized in the project environment:

Component	Detail	Purpose
SIEM Platform	Wazuh v4.14.1	Core SIEM for security analytics and alerting
Manager OS	Ubuntu Linux	Host for the Wazuh Manager service
Endpoint	Windows 11	Target system with the Wazuh Agent installed
Visualization	Wazuh Dashboard (OpenSearch)	Front-end for data visualization and analysis

3. Log Architecture

The log ingestion architecture is centralized around the Wazuh Agent installed on the Windows 11 endpoint. This agent is configured to actively monitor and forward relevant security event logs (such as Windows Event Channel logs) over a secure channel to the Wazuh Manager, which is running on the Ubuntu Linux host.

The Manager receives these logs, normalizes them, and indexes them into the `wazuh-alerts-*` index pattern. Confirmation has been made that the Agent Status is "Active," and consistent log ingestion is confirmed, ensuring real-time telemetry from the endpoint is processed by the SIEM.

4. Detection Capabilities

Wazuh's default rule set provides robust detection coverage for common security events. Primary detection groups observed during the monitoring period include "Authentication Failures" (typically Rule Level 4 or higher) and generic "System Events" related to process execution and configuration changes.

In the last 24 hours of monitoring, the system generated the following alert statistics:

Severity	Count
Medium	1,248
Low	390

5. Detection & Analysis

Analysis and investigation were performed within the Wazuh Dashboard using the **Discover** view. The following filters were consistently applied to narrow down and investigate security events originating from the target Windows 11 endpoint:

- **Index:** `wazuh-alerts-*`
- **Agent Filter:** `agent.name: windows\_11\_wazuh`

Key observed fields used for triage and investigation included:

- `rule.id` (To identify the specific security rule triggered)
- `rule.groups` (To categorize the type of threat/event)
- `full\_log` (To inspect the raw log data for context)

6. MITRE ATT&CK Mapping

Wazuh SIEM facilitates Windows security monitoring and threat detection by offering native mapping of many of its detection rules to the MITRE ATT&CK framework. The system logs observed techniques that suggest potential malicious activity, including:

- **T1110 (Brute Force):** Identified through repeated Windows Event ID 4625 alerts.
- **T1078 (Valid Accounts):** Triggered when legitimate user accounts execute actions.
- **T1059 (Command Execution):** Detected upon the execution of specific suspicious command-line utilities.

7. Security Recommendations

Based on the project's findings and observed detection gaps, the following security recommendations are proposed:

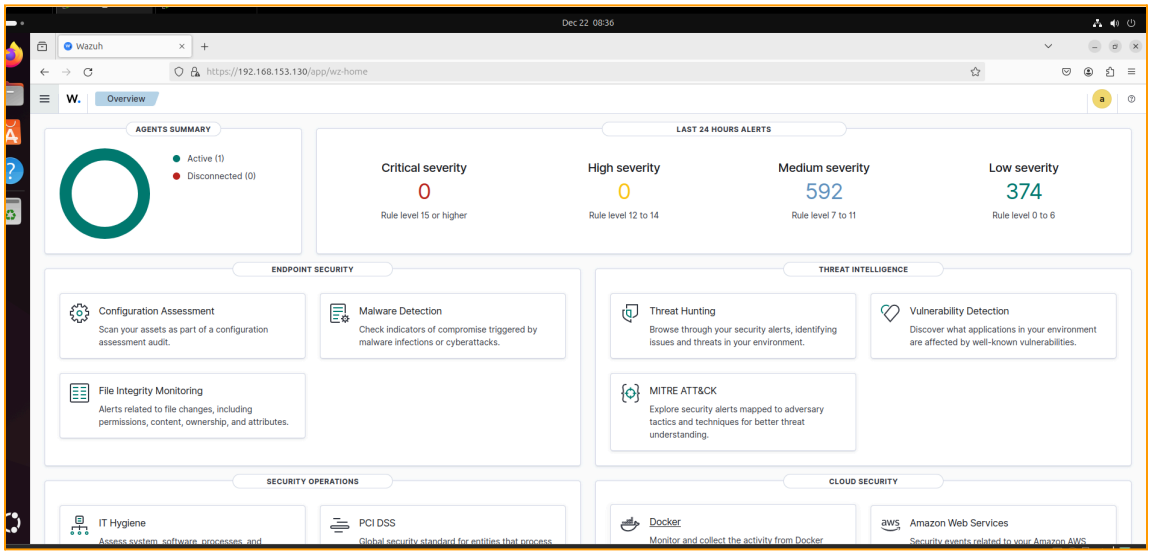
Priority	Recommendation	Description
HIGH	Enable Account Lockout Policy	Configure the Windows Group Policy to lock accounts after a low number of failed login attempts (e.g., 3-5) to mitigate T1110 (Brute Force).
MEDIUM	Enable Sysmon Integration	Integrate Sysmon logs into Wazuh. This will provide deeper telemetry on process creation, network connections, and file modifications for enhanced threat hunting.
MEDIUM	Implement MFA	Deploy Multi-Factor Authentication (MFA) across all critical user accounts to significantly reduce the risk associated with compromised credentials (T1078).

8. Conclusion

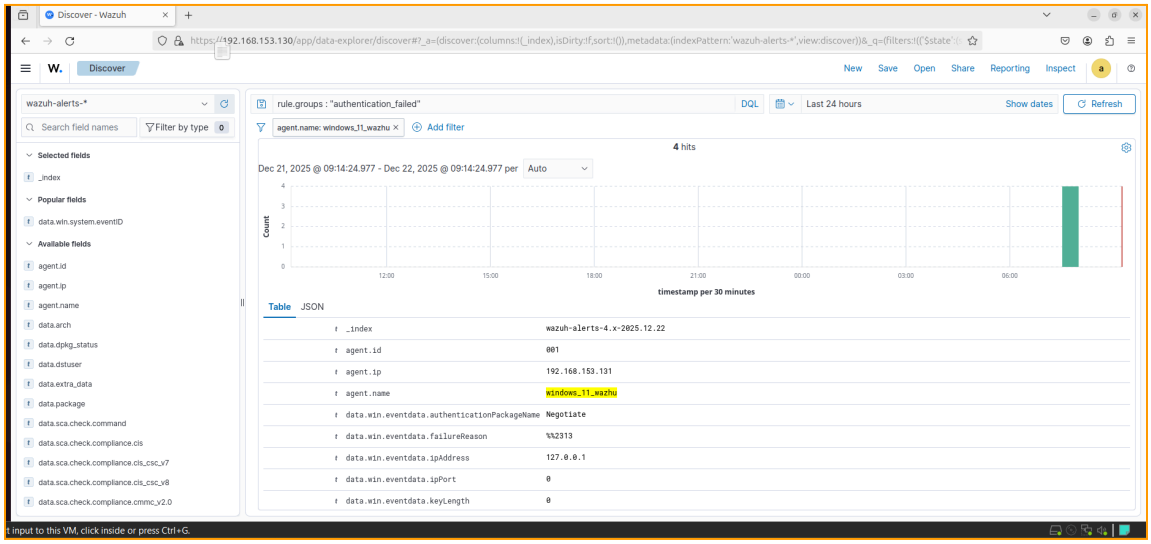
This project successfully validates the deployment and functionality of Wazuh v4.14.1 as a powerful, open-source SIEM solution for monitoring Windows 11 endpoints. The platform demonstrates effective log ingestion, rule-based alerting, and MITRE ATT&CK mapping, making it a viable and valuable tool for security monitoring in entry-level SOC environments.

9. Evidence

The following files contain the evidence supporting this project report:

- Wazuh Overview Dashboard: 🗋 File
- 

- Discover View showing applied filters: 🗋 File

- 

- Raw logs confirming multiple authentication failure events: 🗋 File
-