Project Status Report: SOC Phase 1

CYBERTRoN SIEM VISIBILITY

Orinea Mulaudzi | Status: operational | 2026/02/09

Table of Contents

🛡 1. Executive Summary

The primary objective of this phase was to mitigate visibility gaps on a critical Windows workstation. By deploying an open-source Wazuh SIEM/XDR solution, the security posture has transitioned from reactive recovery to proactive, real-time monitoring. **This deployment introduces real-time visibility into 100% of system authentication events, significantly reducing the potential Time-to-Detect (TTD) for unauthorized access.** Furthermore, it establishes a baseline for regulatory compliance by auditing the environment against **CIS Benchmarks**.

🏗 2. Lab Architecture & Infrastructure

The lab utilizes a **Manager-Agent** architecture, ensuring centralized command and decentralized data collection.

Component	Hostname	Role	OS	Status
SIEM Manager	Wazuh-Manager	SIEM/XDR Indexer & Dashboard	Ubuntu Linux	**Running**
Monitored Asset	DESKTOP-0QPR8QG	Windows Endpoint	Windows 10/11	**Active**

🛠 3. Implementation Details

The deployment was executed across three critical stages:

1. **Manager Provisioning:** Deployed the Wazuh single-node stack on Ubuntu. This included the **Analysis Engine** and the **RESTful API** for dashboard interaction.
2. **Agent Deployment:** Installed the Wazuh agent on " DESKTOP-0QPR8QG" via PowerShell.
3. **Secure Enrollment:** Enforced **Mutual TLS (mTLS) authentication** using a unique key to establish an encrypted channel via Port 1514. This ensures encrypted command-and-control traffic and prevents rogue agent enrollment.

🔍 4. Security Capabilities Enabled

Capability	Function	Benefit
Log Management	Collects Windows Event Logs (ID 4624, 4625, etc.)	Provides an audit trail for all logins.
FIM	File Integrity Monitoring	Detects unauthorized changes to system files.
SCA	Security Configuration Assessment	Audits the system against CIS Benchmarks.
Vulnerability Detection	Continuous CVE Scanning	Identifies outdated software before exploitation.

5. Verification & Testing

- **Connectivity:** Verified via agent_control -l, confirming one active agent managed by the server.
- **Data Ingestion:** The dashboard confirms successful population of system inventory, including RAM, CPU, and installed applications.
- **Telemetry Confirmation:** Verified that the agent is actively forwarding package data, including Microsoft Edge and Wazuh Agent telemetry.

6. Screenshots

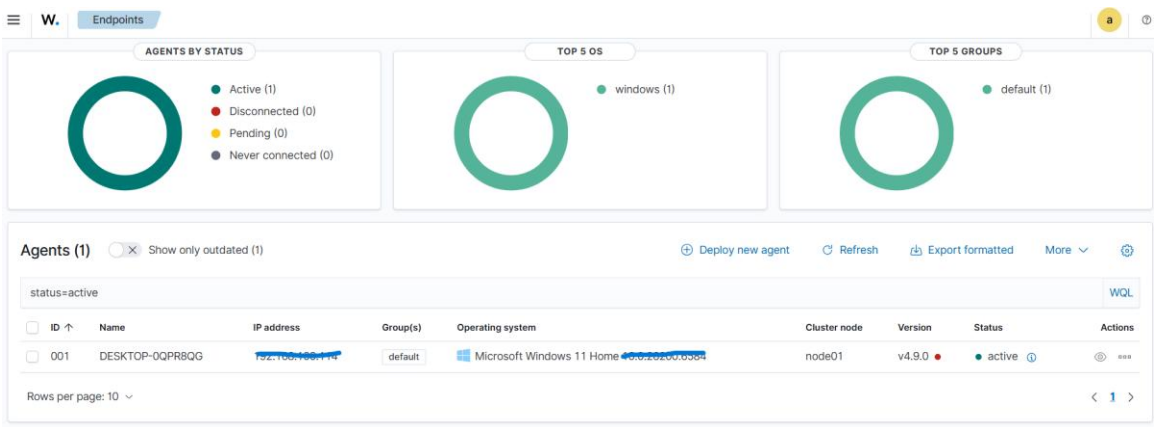

Figure 1: Service Availability Dashboard: Confirms the manager is operational and the agent is actively communicating.

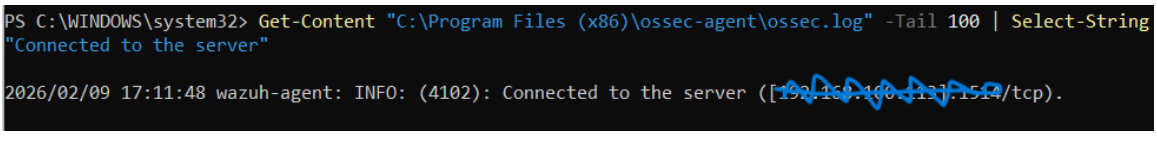

Figure 2: Secure Handshake Log: Powerhide output from the target asset shows a successful "Connected to the server" status established on 2026/02/09 at 17:11:48

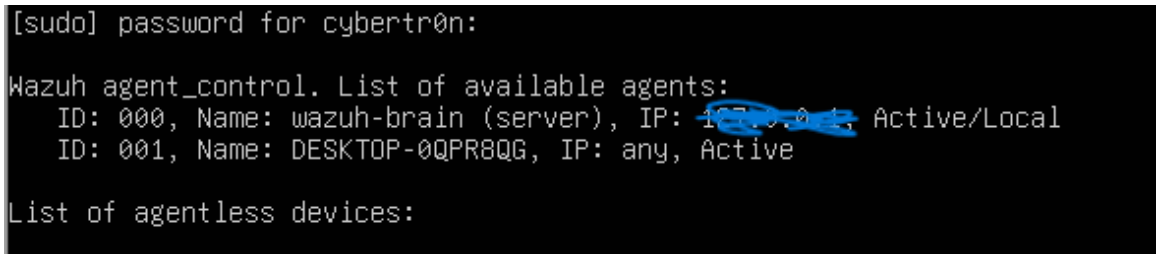

Figure 3: CLI Management: Manager-side CLI output confirms Agent 001 is "Active" and providing data, serving as a failover verification for the web GUI.

📸 7. Next Steps

Strategic Goal for Phase 2: Behavioral Detection & Baseline Verification The objective of Phase 2 is to validate the SIEM's ability to detect **unauthorized administrative changes**. Rather than relying on custom-coded rules, the focus is on leveraging **Wazuh's out-of-the-box (OOTB) intelligence** to identify "Persistence" techniques (MITRE T1136), such as the creation of unauthorized local accounts. This ensures that the SOC remains functional and alert-capable even without complex manual configurations.