Project Status Report: SOC Phase 1

CYBERTRoN SIEM VISIBILITY

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

Table of Contents

🛡 1. Executive Summary

The primary goal of this project was to eliminate "Security Blind Spots" on a critical Windows asset. By deploying an open-source **Wazuh SIEM/XDR** solution, we have successfully moved from reactive recovery to proactive monitoring. The system is now actively collecting telemetry, monitoring file integrity, and scanning for vulnerabilities with **zero licensing costs**.

🏗 2. Lab Architecture & Infrastructure

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

Component	Hostname	Role	OS	Status
The Brain	Wazuh-Manager	SIEM/XDR Indexer & Dashboard	Ubuntu Linux	**Running**
The Eye	DESKTOP-0QPR8QG	Windows Victim 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:** Manually performed **Mutual Authentication** using a unique **Authentication Key** to establish an encrypted TLS channel (Port **1514**) between the victim and manager.

🔍 4. Security Capabilities Enabled

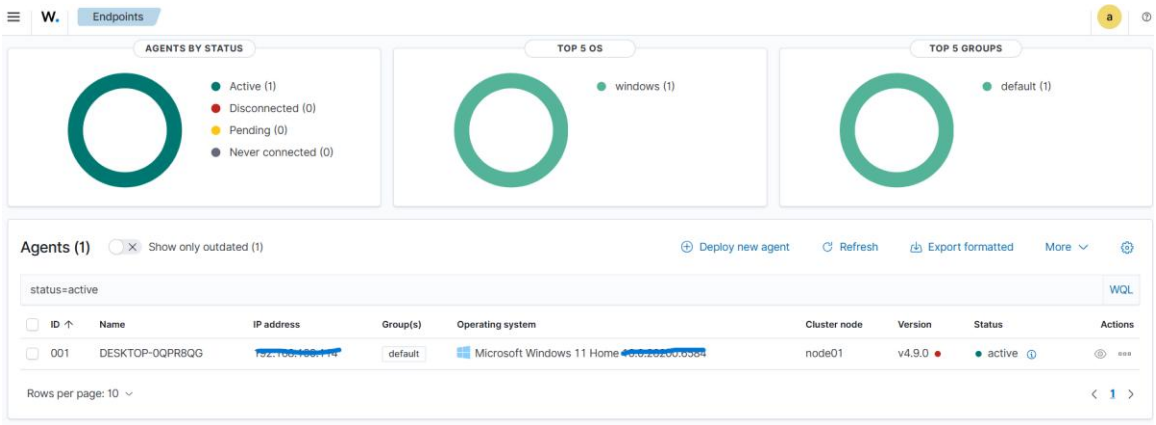
Capability	Function	Benefit
Log Management	Collects Windows Event Logs (ID 4624, 4625, etc.)	Provides an audit trail for all logins.
FIM	File Integrity Monitoring	Detects unauthorized changes to system files.
SCA	Security Configuration Assessment	Audits the system against CIS Benchmarks.
Vulnerability Detection	Continuous CVE Scanning	Identifies outdated software before exploitation.

🛡️ 5. Verification & Testing (The Proof)

- **Connection Test:** Verified via the agent_control -l command on the manager, showing **1 Active agent**.
- **Heartbeat Sync:** The dashboard confirms a successful data flow, with system inventory (RAM, CPU, Apps) successfully populated.

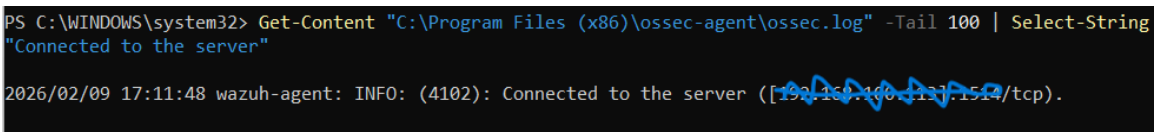
📸 6. Screenshots

1. The "1 Active" Dashboard



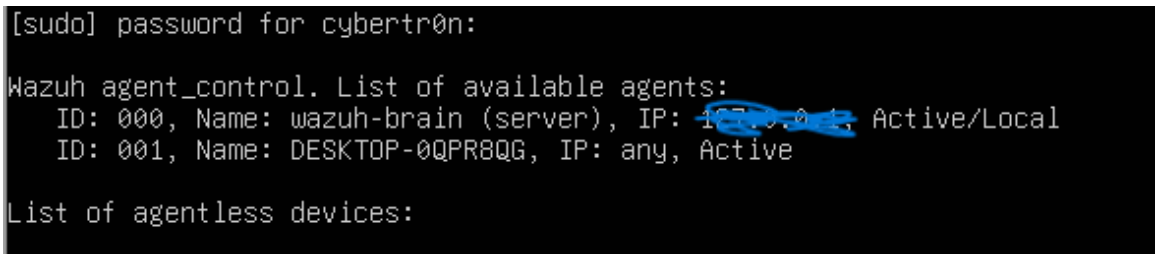
This is my primary proof of **Availability**. It shows that the manager is up and the agent is talking.

2. The "Handshake" Log (Victim VM)



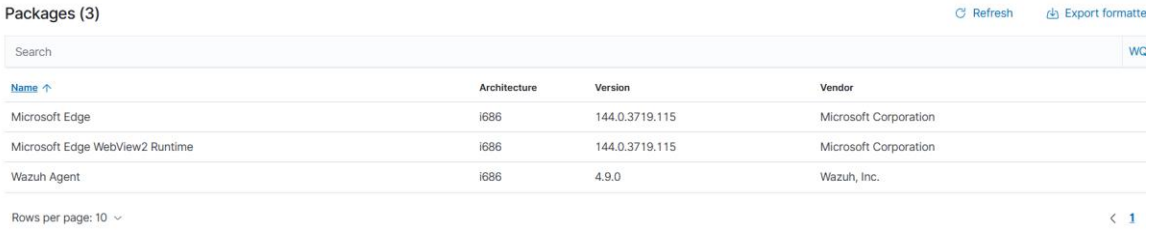
This proves not just that it *is* connected, but exactly *when* the secure tunnel was established.

3. The "Heartbeat" Log (Ubuntu side)



This proves the manager is receiving data in the CLI, which is important if the web GUI ever fails.

4. Initial Inventory Discovery



This proves the agent isn't just "connected," but is actually **forwarding data**.