



Community-Powered Vulnerability Management

Students: Theodore Atis, Daniel Granados, Marlon Iglesias Diaz

Mentor: Masoud Sadjadi

Instructor/Faculty Masoud Sadjadi, Florida International University

PROBLEM

Organizations today confront an escalating array of cyber threats, including sophisticated malware, targeted attacks, and expanding attack surfaces from cloud services and remote work. Traditional security measures often fall short, exposing organizations to the risk of data breaches, financial losses, and reputational damage. This project addresses the critical need for a comprehensive and proactive vulnerability management strategy, leveraging an agentless SIEM like Greenbone and an agent-based SIEM called Wazuh, to identify, prioritize, and remediate vulnerabilities and provide a robust defense against evolving cyber threats.

COLLABORATIVE VULNERABILITY MANAGEMENT

1. Asset Identification

Greenbone (Agentless): Conducts network-wide scans to identify assets, including servers, network devices, and applications, providing a comprehensive overview of the organizational infrastructure.

Wazuh (Agent-based): Monitors individual endpoints, identifying critical assets such as workstations and servers and continuously assessing their security posture.

2. Vulnerability Assessment

Greenbone (Agentless): Identifies vulnerabilities in software, misconfigurations, and potential entry points across the network through periodic scans.

Wazuh (Agent-based): Correlates vulnerability data from Greenbone with real-time endpoint activities, assessing the actual risk level and potential exposure.

3. Threat Detection

Greenbone (Agentless): Provides insight into potential threats through vulnerability identification, helping preemptively address weaknesses that could be exploited.

Wazuh (Agent-based): Monitors endpoint logs, file integrity, and system activities, detecting signs of malicious behavior, unauthorized access attempts, or deviations from normal patterns.

4. Prioritization and Risk Scorings

Greenbone (Agentless): Prioritizes vulnerabilities based on severity, enabling the organization to focus on addressing the most critical issues first.

Wazuh (Agent-based): Contributes to risk scoring by providing real-time data on potential threats, assisting in prioritizing responses based on the active exploitation or severity of incidents.

5. Incident Responses

Greenbone (Agentless): Alerts the security team to vulnerabilities, initiating the incident response process to remediate identified issues.

Wazuh (Agent-based): Triggers automated responses or alerts in real-time when it detects malicious activities, aiding in swift incident response to minimize potential damage.

6. Continuous Monitoring

Greenbone (Agentless): Conducts periodic scans to ensure continuous monitoring of the organization's attack surface for emerging vulnerabilities.

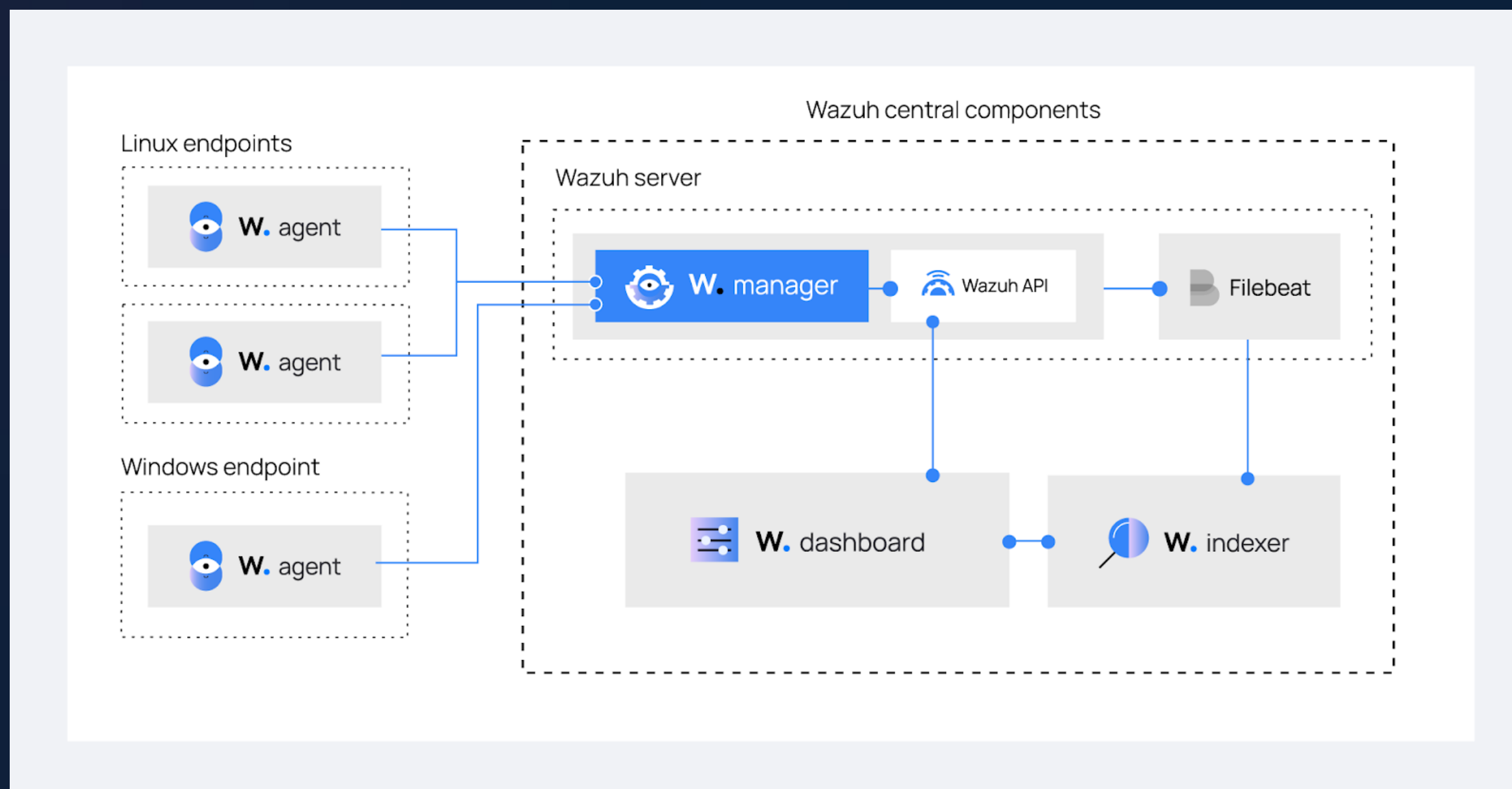
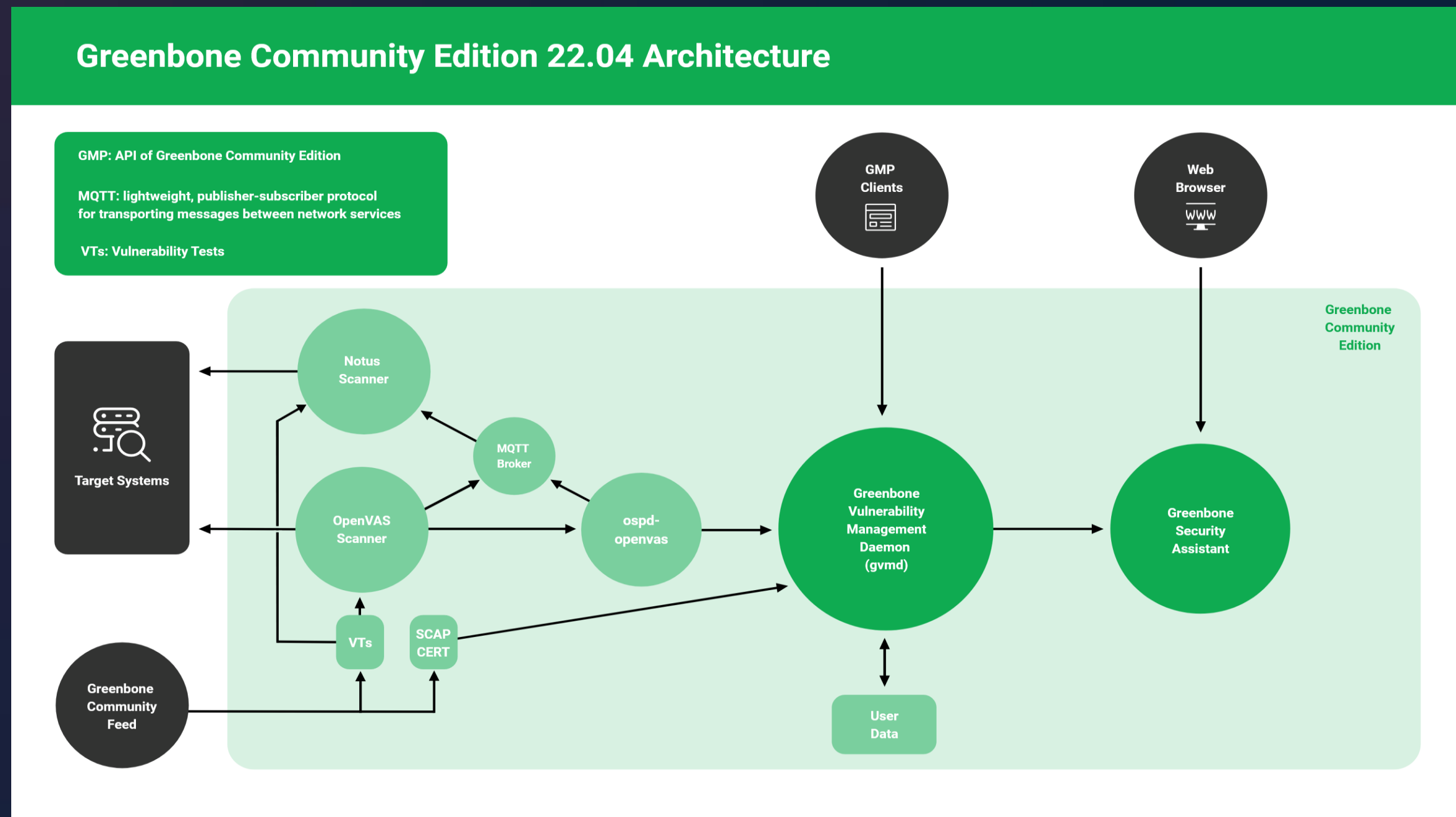
Wazuh (Agent-based): Provides continuous real-time monitoring of endpoints, adapting to changes in the threat landscape and ensuring ongoing security.

7. Reporting and Compliance

Greenbone (Agentless): Generates comprehensive reports on identified vulnerabilities, aiding in compliance assessments and regulatory requirements.

Wazuh (Agent-based): Assists in compliance by monitoring and reporting on security events, ensuring adherence to security policies and regulations.

HOW IT WORKS



CURRENT SYSTEM

Agentless SIEM GVM

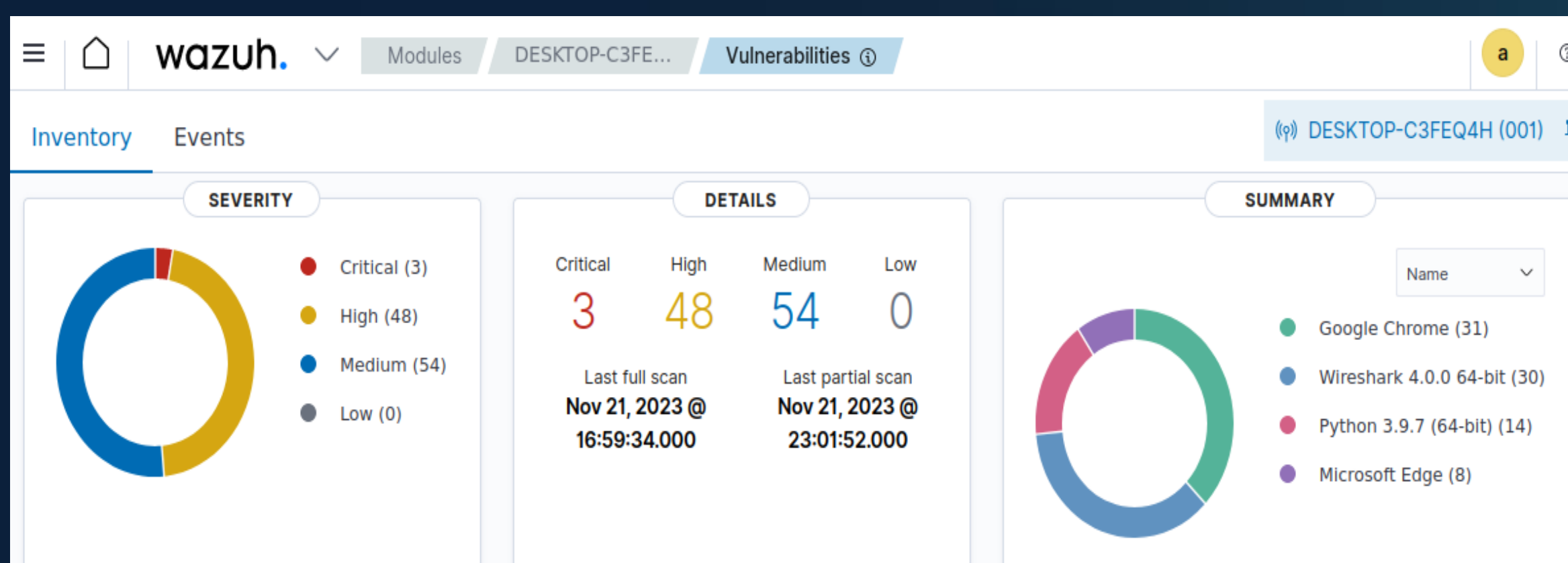
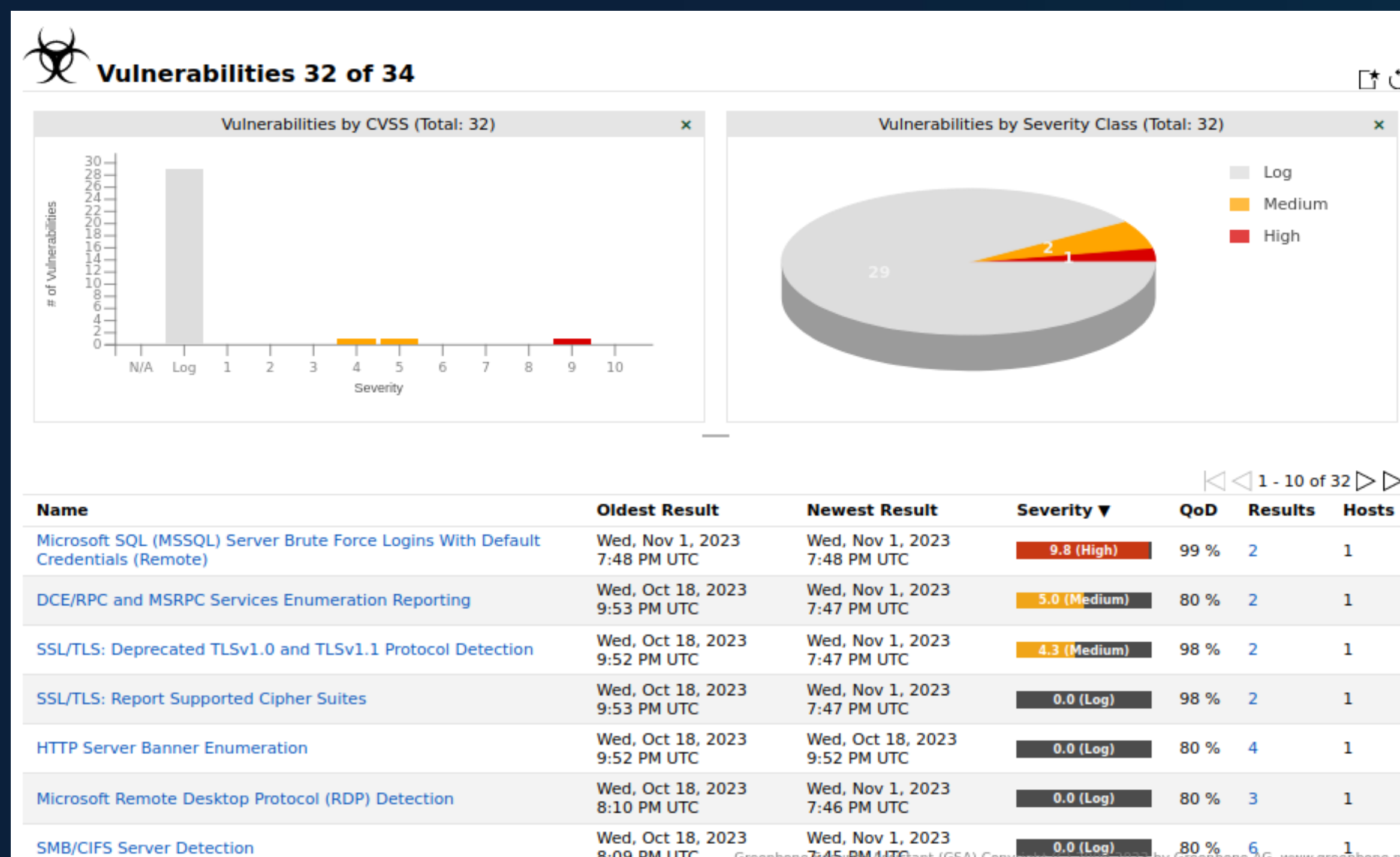
(Greenbone Vulnerability Manager)

Greenbone operates without installing agents on individual devices. It utilizes network-based scans to identify vulnerabilities across the organization's infrastructure. It detects vulnerabilities such as unpatched software, misconfigurations, and potential entry points for cyber threats. The agentless approach ensures minimal impact on individual devices.

Agent-based SIEM Wazuh

Wazuh, being agent-based, involves the installation of agents on individual endpoints. These agents continuously monitor local logs, file integrity, and system activities for signs of malicious behavior. Wazuh agents installed on employee workstations and critical servers actively monitor for any suspicious activities or deviations from normal behavior.

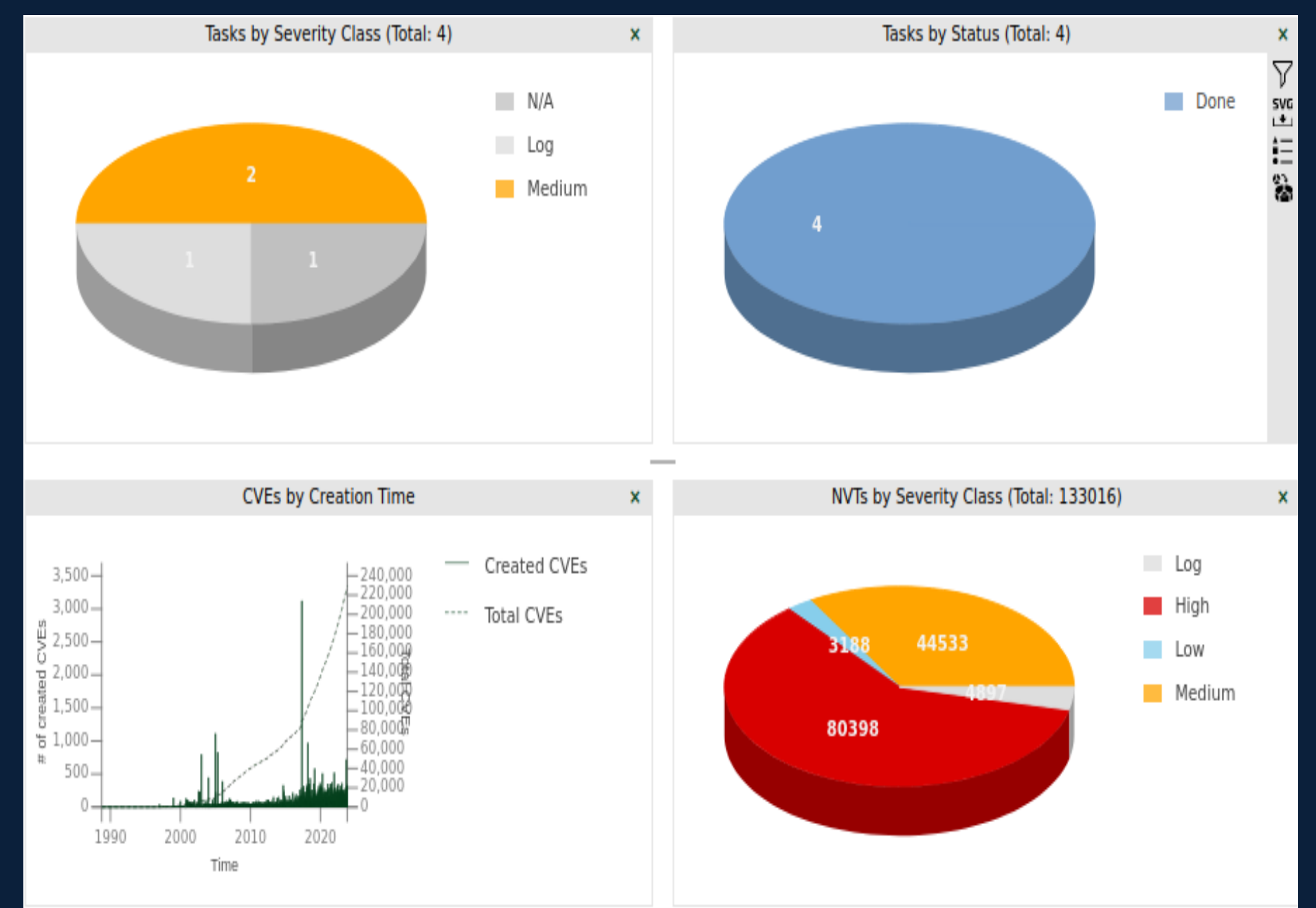
RESULTS



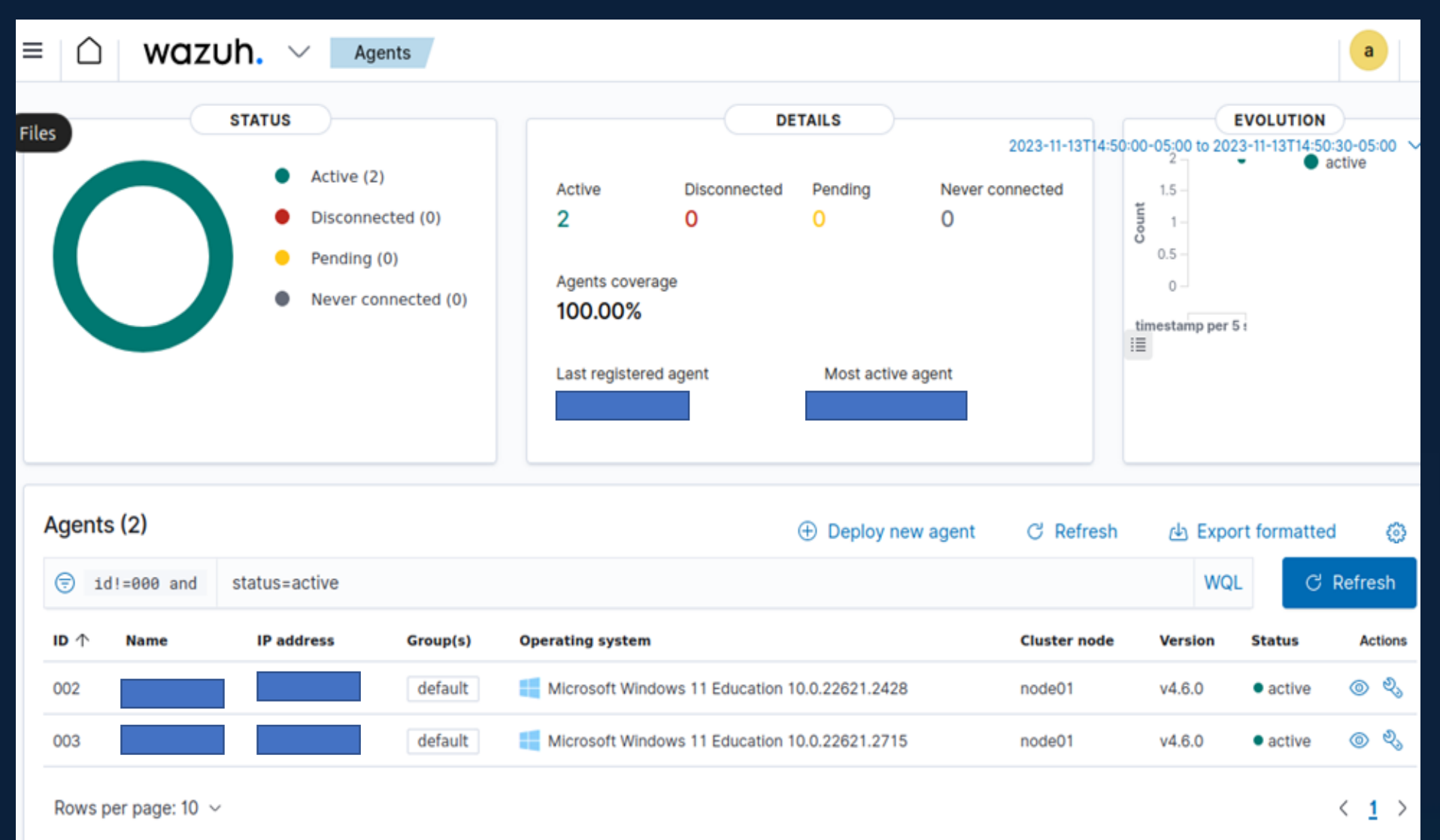
Acknowledgement

The material presented in this poster is based upon the work supported by Masoud Sadjadi. I thank Masoud Sadjadi for his assistance and mentorship that I received throughout the senior design project.

GVM Assessment



Wazuh Assessment/Analytics



SUMMARY

In this comprehensive risk assessment, the organization leverages the strengths of Greenbone, an agentless SIEM, and Wazuh, an agent-based SIEM, to fortify its cybersecurity defenses. Greenbone conducts network-wide scans, identifying vulnerabilities and potential threats, while Wazuh monitors individual endpoints in real-time, correlating vulnerability data and detecting signs of malicious behavior. This integrated approach allows for a proactive and unified risk assessment, prioritizing vulnerabilities, facilitating swift incident response, and ensuring continuous monitoring to safeguard the organization against evolving cyber threats.

REFERENCES

- Greenbone Vulnerability Management Manuals: <https://www.greenbone.net/en/documents>
- Wazuh Documentation: <https://documentation.wazuh.com/current/proof-of-concept-guide/index.html>
- <https://nvd.nist.gov/vuln/detail/cve-2023-5730>