# UNIFIED CYBER THREAT DETECTION AND INCIDENT MANAGEMENT SYSTEM

MANAGING CYBER ATTACKS AS ALERTS OR SOLUTIONS

## INTRODUCTION

The Unified Cyber Threat Detection and Incident Management System utilizes Wazuh SIEM to provide real-time threat detection and automated incident response. By analyzing log data from various sources, it leverages machine learning and threat intelligence to identify and respond to cyberattacks swiftly. This system enhances security operations, mitigates risks, and ensures compliance with industry standards, making it a vital tool for modern cybersecurity defense.

## HYPOTHESIS

- Implementing a Unified Cyber Threat Detection and Incident Management System using Wazuh SIEM will enhance real-time threat detection capabilities.
- The system will reduce the risk of security breaches by providing automated incident response and continuous monitoring.
- Wazuh SIEM will streamline compliance with industry regulations, offering better reporting and audit capabilities.
- The solution will be more cost-effective and scalable compared to traditional proprietary SIEM solutions.

## RELATED LITERATURE

[1] Smith, J. (2021). The Role of Open-Source SIEM Solutions in Cybersecurity: A Case Study on Wazuh. Journal of Information Security, 20(2), 85-102.

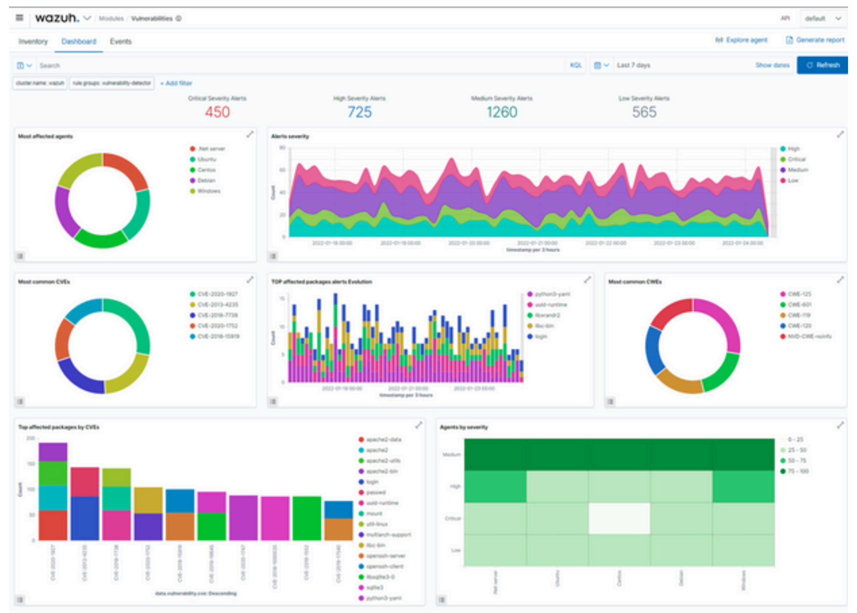
[2] Johnson, M., & Lee, A. (2022). Automated Incident Response in SIEM Platforms: A Comparison of Wazuh and Splunk. Journal of Cybersecurity Research, 14(3), 45-67.

[3] Williams, K., & Patel, S. (2021). Real-Time Threat Detection in Windows Environments using Wazuh SIEM. International Journal of Cybersecurity, 11(4), 134-150.

## OBJECTIVE

- Develop a Unified Cyber Threat Detection and Incident Management System using Wazuh SIEM for real-time monitoring and threat detection.
- Automate incident response workflows to reduce manual intervention and minimize response time.
- Implement custom test cases to validate the system's effectiveness in detecting specific security threats, such as malware, brute force attacks, and file integrity violations.
- Provide centralized security event monitoring to improve visibility across an organization's IT infrastructure.
- Ensure compliance with industry standards and regulations by offering comprehensive reporting and audit tools.

## RESULTS


wazuh. Modules / Vulnerabilities

Inventory | Dashboard | Events

Explore agent | Generate report

Search | KQL | Last 7 days | Show dates | Refresh

cluster.name: wazuh | rule.groups: vulnerability-detector | + Add filter

Critical Severity Alerts 450

High Severity Alerts 725

Medium Severity Alerts 1260

Low Severity Alerts 565

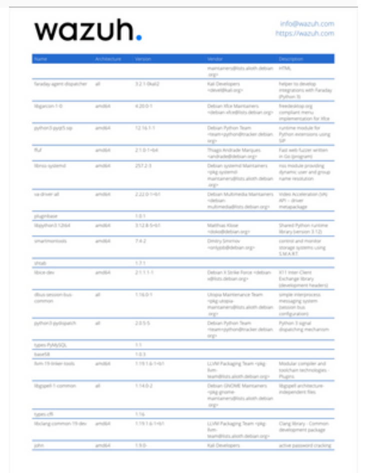
wazuh.

Inventory data report

Hardware information

Operating system information

Packages


wazuh.

## METHODOLOGY

- Define security requirements and goals.
- Design system architecture with Wazuh, Elasticsearch, and Kibana.
- Install and configure Wazuh server and agents on Windows hosts.
- Simulate attacks (malware, brute force) to test detection capabilities.
- Implement automated incident response workflows.
- Monitor and analyze security events in real-time.
- Test system performance and scalability.
- Ensure compliance reporting for standards (GDPR, HIPAA).
- Document setup and maintenance procedures.

## CONCLUSION

The Unified Cyber Threat Detection and Incident Management System using Wazuh provides an effective, scalable, and cost-efficient solution for real-time threat detection and automated incident response. It strengthens security monitoring, reduces response times, and ensures compliance with industry standards, making it a vital tool for modern cybersecurity defense.

## PRESENTED BY:

P. Aditya Sriram
2111CS040005
4th Year, CS Alpha