**SPR530 Project Proposal**

**Project Title:**

In-Depth Analysis and Demonstration of Wazuh as an Open-Source SIEM Solution

**Student Name:**

Oluwadamilola Ogundipe

**Course:**

SPR530 – Advanced Security Integration

**Instructor:**

Professor Suranjit Paul

**Submission Date:**

4/17/2025

**1. Selected Security Solution:**

The concentration of this project is on Security Information and Event Management (SIEM); a critical security technology that deals with real-time log monitoring, threat detection, incident response, and compliance. I will perform an extensive analysis and practice demo of Wazuh, an open-source SIEM platform well-accepted in academia and corporate environments alike.

**2. Project Goal:**

The primary goal of this project is to gain in-depth technical knowledge about how SIEM solutions operate, especially with respect to detection rules, log correlation, alerting capability, and automated response mechanisms. The project will further explore applying Wazuh to detect and respond to brute-force SSH attacks.

**3. Detailed Analytical Strategy:**

A complete deconstruction will be done for the architecture of SIEM, which includes:

* Core: log collection; normalization; correlation; alerting; dashboarding
* Wazuh-specific architecture (agent-manager model, OpenSearch integration, configuration structure)
* Real-time detection by means of rule sets (for example, Rule ID 5760 for SSH brute-forcing)
* Active response capabilities (for example, firewalldrop)
* Behavior of the system in attack situations and mitigations.

This analysis would be amplified through live investigating, lab observation, and evaluations of the logs and alerts.

**4. Plan for Comparative Analysis:**

In order to get an understanding of the reputation of Wazuh in the global SIEM market, I will carry out a comparative analysis of the following solutions:

* Splunk Enterprise Security
* IBM QRadar
* Microsoft Sentinel
* Wazuh

This comparison will include:

* Deployment and infrastructure requirements
* Functionalities and customizations
* Cost and licensing
* Cloud versus on-premise modalities
* Suitability for educational and SMB use

It will further contribute to identifying those tools which are more appropriate for given operational scenarios.

**5. Choice of Tools for Task Breakdown:**

Demonstrated will be the solution known as Wazuh v4.5 The hands-on demo will include:

* Installation of Wazuh Server and Agent on Ubuntu VMs
* Simulating brute-force attack with Hydra
* Detecting the attack through Wazuh out-of-the-box rule set
* Triggering Active Response of Wazuh to block the attacker's IP address
* Verifying detection and response through logs and firewall output.

This live demonstration will thus offer technical proof of Wazuh's real-time detection and response capabilities.

**6. Final Verdict Plan:**

Concluding the project according to results from research and practical demonstration:

* A critical assessment of Wazuh's merits and demerits
* Examination of situations where Wazuh is fit or otherwise for certain use cases
* Recommendations for organizations that are considering the use of Wazuh
* Situations in which commercial SIEMs such as Sentinel or Splunk would be most appropriate

Moreover, in the final verdict, Wazuh will be evaluated as a good learning platform and may find its future usage in low-budget, high-visibility environments, such as academic labs, small and medium enterprises (SMBs), and SOC training.

**7. Conclusion:**

The proposal is a well-defined plan to compare and study SIEM technologies with special focus on Wazuh. From both theoretical studies as well as practical implementation, the project is committed to delivering an overall idea of the functionality of SIEM systems in actual threat scenarios. Wazhy was selected for its ease of use, simplicity, and full-featured active response features that make it the best tool for demonstration and examination. The output of this project should provide beneficial information regarding the use of open-source security tools on a day-to-day basis in today's cybersecurity practices.

**8. Refernces**

* Wazuh. (2024). Wazuh Documentation (v4.5). Accessed from: https//documentation.wazuh.com
* Microsoft. (2024). Microsoft Sentinel Documentation. Retrieved from https//learn.microsoft.com/en-us/azure/sentinel
* IBM. (2024). Overview about IBM QRadar SIEM. Retrieved from https//www.ibm.com/products/qradar-siem
* Splunk. (2024). Splunk Enterprise Security. Retrieved from https//www.splunk.com/en\_us/software/enterprise-security.html
* MITRE ATT&CK®. (2024). Adversarial Tactics and Techniques Framework. Retrieved from https//attack.mitre.org.
* Ubuntu. (2024). Ubuntu 20.04 LTS Documentation. Retrieved from https://ubuntu.com/server/docs
* THC Hydra. (2024). Hydra Network Login Cracker. Retrieved from https://github.com/vanhauser-thc/thc-hydra