LONDON METROPOLITAN UNIVERSITY

Module Code & Module Title

CS6P05NI Final Year Project

Assessment Type

FYP Proposal Draft

Semester

2024 Autumn

PROJECT TITLE: SIEMLite

Student Name: Tank Prasad Pandeya

London Met ID: 22066453

College ID: np01nt4a220173

Internal Supervisor: Monil Adhikari

External Supervisor: Suraj Upadhyay

Assignment Due Date: 20th October 2024

Assignment Submission Date: 20th October 2024

I confirm that I understand my coursework needs to be submitted online via My Second Teacher under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

Table of Contents

Table of Tables

Table of Figure

1. Introduction

1.1. Introduction to the topic

In today's world, Cybersecurity has been a major concern in the field of Information Technology. From a small-scale enterprise to large companies, from private IT organizations to Government Organization, everybody needs to secure their data and digital assets from potential cyberattacks. To protect and mitigate digital assets from cyber threats, continuous security monitoring plays a very important role. In the field of cybersecurity, even there are some specific job roles related to security monitoring such as Security Analysts and SIEM engineers. For the purpose of monitoring, a specific tool known as SIEM (Security Information and Event Management) is widely used throughout the whole world. SIEM stands for Security Information and Event Management. It is a centralized software for monitoring an organization's IT assets for enabling security teams to manage potential threats proactively (Intelligent Technical Solutions, 2021). It provides insights into various security threats through a centralized collection and analysis of security data pulled from various systems.

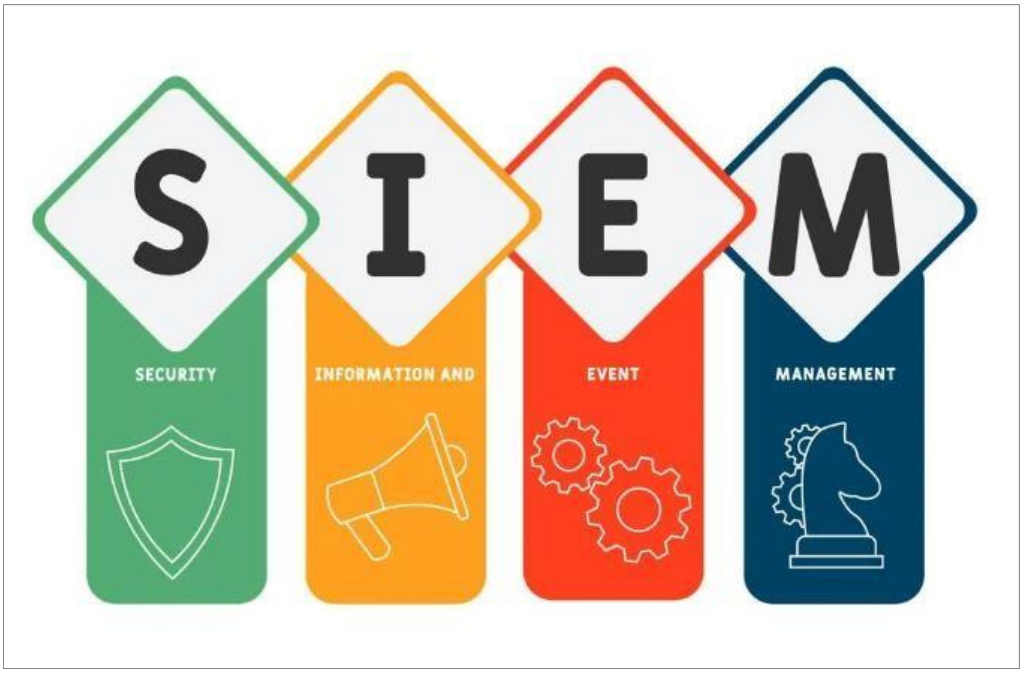

Figure 1 Security Information and Event Management (Forbes, 2023).

1.2. Problem Scenario

As cyber-attacks continue to rise, monitoring digital assets has become a critical aspect of IT security. Unfortunately, many IT companies have shown carelessness in their security monitoring efforts, leading to numerous data breaches that underscore the urgent need for effective solutions. Attackers are constantly seeking to exploit vulnerabilities in IT systems, applications, and hardware, making it essential for organizations to have robust oversight in place. The primary challenge is the inability to identify and respond to security incidents in real time, which can significantly increase the potential damage caused by these attacks (Dataversity, 2019).

While SIEM solutions are effective for protecting against and responding to cyber threats, a major concern is their cost. SIEM solutions are typically very expensive. The initial cost of purchasing and implementing a SIEM solution can be expensive for smaller organizations. Furthermore, their maintenance, updates and support can add to the overall cost (González-Granadillo, González-Zarzosa, & Diaz, 2021). According to Buchanan technology, the following is the average cost of in-house SIEM (Buchanan Technologies, 2022).

SIEM Software	$20,000 - $ 1 million
Implementation	$50,000
Training	$0-$10,000
Resources	$74,000-$500,000
Hardware	$25,000-$75,000
Infrastructure	$10,000

Table 1 Average cost of In-house SIEM (Buchanan Technologies, 2022)

While there are numerous SIEM solutions on the market, only a limited number are tailored specifically for malware detection and analysis. Most SIEM systems primarily focus on aggregating and monitoring suspicious logs, which is crucial for identifying potential threats. However, the challenge lies in finding a solution that goes beyond this general approach to specifically target malware patterns at the endpoint level.

An effective SIEM solution for malware detection should be able to not only collect and correlate logs but also analyse them for known malware signatures and behaviour patterns. Furthermore, it should offer robust alerting capabilities that prioritize incidents based on the severity of the detected malware. While some SIEM solutions may include vulnerability detection features, they often lack the specialized tools and methodologies required for comprehensive malware detection and analysis.

1.3. Solution

To tackle the issues outlined in the previous section, I propose an affordable SIEM solution that incorporates enhanced capabilities, providing advanced features specifically for malware detection and analysis, with a current focus on a particular type of malware.

The major features that this project includes are:

- Lightweight SIEM: A less resource consuming SIEM solution that contains some advanced SIEM features targeted for Small to Medium Scale Enterprises.
- Advanced Parsing and Normalization: Advanced parsing and normalization capability that is actively used for identification and in-depth analysis of malware.
- Enhanced Visualization: This feature provides effective and enhanced visualization for better analysis.
- Integrated threat Intelligence: Open-Source threat intelligence platform is integrated with SIEM solution for event correlation and better analysis.
- Enhanced Alerting: The alerting feature is enhanced with integration with popular communication channels like Slack and Gmail.

2. Aims and Objectives

2.1. Aim

The primary aim of this project is to build an affordable SIEM solution with enhanced capabilities such as enhanced visualizations, Intelligence enrichment, Detailed malware log analysis designed specifically to identify and analyse malwares on the basis of logs collected through endpoints.

2.2. Objectives

The objectives of this project are:

- Conduct in-depth research on SIEM solutions available in the market along with their features and capabilities.
- Develop a basic log analysis tool by integrating various open-source tools like beats, Elasticsearch, Wazuh, Graylog and Grafana, OpenSearch that are lightweight and consume less resources.
- Integrate this basic log analysis tool with Threat Intelligence platforms such as MISP or OpenCTI for continuous threat intelligence.
- Develop and add advanced alerting feature by integrating with communication platforms like MISP, OpenCTI.
- Provide enhanced visualization using the advanced features of Grafana.
- Provides detailed analysis on a specific type of malwares by collecting the related logs and by correlating them.

3. Expected Outcomes and Deliverables

3.1 Outcomes

By the end of this project, the SIEMLite system is anticipated to achieve the following outcomes:

- **Outcome 1:** SIEMLite is expected to deliver fundamental SIEM functions, including log collection, aggregation, and analysis.
- **Outcome 2:** SIEMLite should offer malware detection capability by gathering and correlating logs from endpoints that are suspicious and pertinent to specific malware threats.
- **Outcome 3:** SIEMLite should include basic threat intelligence feature for data enrichment and accurate analysis.

3.2 Deliverables

After achieving the above outcomes, this project is expected to produce the following deliverables:

- **Deliverable 1:** A SIEM solution prototype that has an advanced malware detection feature.
- **Deliverable 2:** A technical Documentation that provides the architecture, components, and working methodology of SIEMLite prototype.
- **Deliverable 3:** A user guide that offers instructions on how to install, configure, and effectively use the SIEMLite solution.
- **Deliverable 4:** A comprehensive testing report detailing the performance of the SIEMLite prototype.

4. Conclusion

In conclusion, while many SIEM solutions are available, there is a notable gap when it comes to those specifically designed for malware detection and analysis. Most existing solutions primarily focus on log aggregation and monitoring, leaving organizations without the targeted capabilities needed to effectively identify and respond to malware threats. To address this critical need, I propose developing an affordable SIEM solution with enhanced features tailored for advanced malware detection and analysis. By concentrating on specific malware types, this solution aims to fill the existing void in the market, providing organizations with the tools necessary to strengthen their security posture and mitigate risks associated with malware attacks. This focused approach not only enhances threat detection but also enables more efficient incident response, ultimately contributing to a more robust cybersecurity framework.

5. References

Buchanan Technologies. (2022, March 29). SIEM Pricing & SIEM Costs. Retrieved from Buchanan Technologies: https://www.buchanan.com/managed-siem-pricing/

Dataversity. (2019, October 1). What is SIEM and Why is it So important? Retrieved from Dataversity: https://www.dataversity.net/what-is-siem-and-why-is-it-so-important/

Intelligent Technical Solutions. (2021, October 4). Pros and Cons of Implementing SIEM. Retrieved from Intelligent Technical Solutions: https://www.itsasap.com/blog/pros-cons-siem