Tank_prasad_Pandeya.docx

Islington College,Nepal

Document Details

Submission ID

trn:oid:::3618:72980068

Submission Date

Dec 3, 2024, 11:08 PM GMT+5:45

Download Date

Dec 3, 2024, 11:09 PM GMT+5:45

File Name

Tank_prasad_Pandeya.docx

File Size

18.8 KB

22 Pages

2,669 Words

16,311 Characters

21% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Match Groups

29 Not Cited or Quoted 13%
Matches with neither in-text citation nor quotation marks

13 Missing Quotations 8%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

14%	Internet sources
1%	Publications
20%	Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Match Groups

- **29** Not Cited or Quoted 13%
  Matches with neither in-text citation nor quotation marks
- **13** Missing Quotations 8%
  Matches that are still very similar to source material
- **0** Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- **0** Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

14%	Internet sources
1%	Publications
20%	Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Internet	pdfs.semanticscholar.org	7%
2	Internet	docplayer.net	2%
3	Submitted works	University of Melbourne on 2024-03-27	2%
4	Submitted works	Kingston University on 2024-01-10	1%
5	Internet	www.grandviewresearch.com	1%
6	Submitted works	University of College Cork on 2023-07-22	1%
7	Internet	blog.imei.com.au	1%
8	Internet	www.ncbi.nlm.nih.gov	1%
9	Submitted works	University of South Africa on 2024-11-03	1%
10	Submitted works	Kepler College on 2024-02-25	1%

11	Submitted works	University of Melbourne on 2023-03-30	1%
12	Submitted works	Ivy Tech Community College Central Office on 2023-10-06	0%
13	Internet	www.asprom.com	0%
14	Submitted works	Saint Francis College on 2024-06-05	0%
15	Publication	Ton Duc Thang University	0%
16	Submitted works	Universiti Malaysia Pahang on 2012-05-21	0%
17	Submitted works	Asia Pacific University College of Technology and Innovation (UCTI) on 2024-05-12	0%
18	Submitted works	Bournemouth University on 2023-08-25	0%
19	Submitted works	University of East London on 2023-05-12	0%
20	Submitted works	University of Portsmouth on 2024-12-02	0%
21	Submitted works		0%
22	Submitted works	Stillman College on 2024-03-26	0%
23	Submitted works	The University of the South Pacific on 2024-10-11	0%

Acknowledgment

15 I would like to express my heartfelt gratitude to my supervisors, Mr. Monil Adhikari and Mr. Suraj Upadhyaya, for giving me the opportunity to work on my final year project on SIEM solutions, a topic I have been eager to explore for a long time. Their invaluable guidance was essential throughout the development of this project. Mr. Suraj Upadhyaya's external supervision and industry expertise enriched my work with valuable market insights, while Mr. Monil Adhikari's academic guidance and support with documentation were crucial.

20 Additionally, I would like to extend my sincere thanks to the Islington College team, 10 including the faculty and module instructors, for their unwavering support, encouragement, and guidance during my final year project. Their continuous support 10 has significantly contributed to my professional growth, and I am deeply grateful for the opportunity to be part of the Islington College academic community.

Abstract

Cyber defense plays a crucial role in cybersecurity, offering protection against various cyber threats. To ensure continuous monitoring of digital assets, SIEM (Security Incident and Event Management) solutions are widely implemented. This project presents a cost-effective and resource-efficient SIEM solution designed to monitor and analyze an organization’s digital assets, safeguarding them from external cyberattacks and threats. Additionally, the solution features malware detection, identifying potential threats based on signature analysis during monitoring.

The project follows the Scrum methodology to ensure efficient planning, development, and execution, with continuous improvements throughout the development cycle. It is structured in phases, including research, development, implementation, and finalization. By utilizing this tool, Small and Medium-sized Enterprises (SMEs) can effectively protect their digital assets from cyberattacks.

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. Additionally, a specific tool known as SIEM (Security Information and Event Management) is widely used throughout the whole world for security monitoring. A SIEM (Security Information and Event Management) system combines two key functions: Security Information Management (SIM), which involves the collection and analysis of log data and events, and Security Event Management (SEM), which focuses on real-time monitoring and alerting (Leung, 2021).

The term was Introduced by research and consulting company Gartner in 2005 (Miloslavsakya, 2018). Over the last decade, many companies have created commercial SIEM solutions.The global SIEM market size was valued at USD 3.95 billion in 2022 and is expected to grow at a compound annual growth rate of 14.5% from 2023 to 2030 (Grand View Research, 2022). Gartner has classified SIEM solution as leaders (organizations that execute well against their current competitors), visionaries (organization that understand where the market is going and have a vision for changing market rules), niche players (organizations that focus successfully on small segment) and challengers (organizations that execute well today but do not demonstrate an understanding of market direction) (González-Granadillo , et al., 2021).

Figure 1: Magic Quadrant for Analytics and Business Intelligence Platforms (Davies, et al., 2024).

1.2. Problem Scenario

As cyber-attacks continue to rise, monitoring digital assets has become a critical aspect of IT security. 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.

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 , et al., 2021). The images below display the budget for Security Information and Event Management for both Medium and Small-Scale Enterprises, as outlined by Trustwave Holdings, Inc.

Figure 2: SIEM Budgeting for Scall Enterprise according to Trustwave Holdings, Inc (Trustwave Holdings, Inc, 2015).

Figure 3: SIEM Budgeting for Medium Enterprise according to Trustwave Enterprise, Inc (Trustwave Holdings, Inc, 2015).

An effective SIEM solution for malware detection should be able to not only collect and correlate logs but also analyze them for known malware signatures and behavior patterns. Furthermore, it should offer robust reporting 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 which are cost effective and are ideal for small and medium scale industries. Some SIEM solutions, like Splunk and QRadar, offer this feature, but they may not be affordable for every small or medium-sized business.

1.3. Project as a Solution

To tackle the market issues outlined in the previous section, an affordable SIEM solution is proposed that incorporates the following features:

Lightweight SIEM: A less resource-consuming SIEM solution that contains some advanced SIEM features targeted at Small to Medium Scale Enterprises.

Parsing and Normalization: Parsing and normalization capability that is actively used for in-depth analysis of logs.

Integrated threat Intelligence: Open-Source threat intelligence platform is integrated with SIEM solution for event correlation and better analysis.

Reporting: The reporting feature is enhanced with integration with popular communication channels like Slack and Gmail.

Aim and Objectives

19 2.1. Aim

The aim of this project is to build a SIEM solution with detailed malware log analysis designed specifically to identify malware based on logs collected through endpoints.

18 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 that are lightweight and consume less resources.

Integrate this basic log analysis tool with Threat Intelligence platforms for continuous threat intelligence.

Develop and add advanced reporting features by integrating with communication platforms.

Provide enhanced visualization using the advanced features of different open-source visualization software.

Provides malware detection capability for a specific type of malware by monitoring the activities it performs on the endpoint and generating alert rules based on those behaviors.

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 a specific malware.

Outcome 3: SIEMLite should include threat intelligence 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 a malware detection feature.

Deliverable 2: A technical Documentation that provides the architecture, components, and working methodology of SIEMLite solution.

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.

Project risks, Threats & Contingency Plans

4.1. Project Risk and Threats

This project can possess the following threats and risks:

Compatibility Issues and Integration Complexity: SIEMLite is created by combining various open-source solutions, which can result in integration challenges and compatibility issues with other systems.

Need for Skilled Personnel: Operating and maintaining SIEMLite requires skilled professionals and a shortage of qualified personnel in cybersecurity can delay the product’s market implementation.

Performance and Latency: SIEMLite can be resource intensive, leading to potential performance issues if the hardware requirements are not met. Additionally, high latency in detection could delay the response to the security incidents.

Challenges with Threat Intel and Integration Issues: While integrating Threat Intel feed can enhance the SIEM’s ability to detect emerging threats, there may be issues with false positives and difficulties in the integration process.

Technical Failure: There is risk of technical issues such as system crash, data loss or server downtime.

4.2. Contingency Plans

Compatibility and Integration Issues: To address technology complexities, compatible backup open-source solutions are utilized, which facilitate integration with other systems.

Need for Expertise: Providing a comprehensive user guide that details how SIEMLite operates, helps users to get up to speed without requiring advanced technical expertise.

Performance and Latency: Implementing a multi-node cluster to distribute resource usage across nodes and conducting regular performance tests to identify and resolve any performance bottlenecks.

Challenges with threat intelligence and integration issues: Carefully selecting and utilizing high-quality, relevant threat intelligence platform to avoid integration issues and minimize false positives.

Technical Failure: Technical failure can be mitigated using regular backups and regular optimizations.

Methodology

Software Development Life Cycle (SDLC) is a framework for planning, analyzing, designing, developing, testing and deploying software. The SDLC methodologies are diverse, each offering a unique approach tailored to specific project needs, complexities and goals. The SDLC process outlines the stages involved in developing software from conception to deployment.

5.1. Considered Methodologies

5.1.1. Prototype Model

In this methodology, a throwaway prototype is built to understand the requirements of the clients. It involves iterative refinement of the prototype based on the user input until the desired functionality and design is achieved (Nydick & Liberatore, 2008). It is useful when the requirements are unclear or subject to change.

Figure 4: Phases of Prototype Model (theKnowledgeAcademy, 2024).

More about prototype model in Appendix 1 (Prototype Model)

5.1.1.1. Reason behind not choosing Prototyping model

The following are the reasons why prototyping models are not appropriate for this project:

Evolving Requirements and Unclear Scope: In complex systems like SIEM, evolving requirements and an unclear scope make it difficult to capture all necessary security needs and define the full system requirements during the initial prototype phase.

Insufficient Continuous Feedback: Prototypes are simplified versions of the final product, limiting the ability to gather continuous user feedback, which is essential for addressing security needs and user requirements in a SIEM solution.

5.2. Used Methodology.

5.2.1. Scrum

It is a simple but popular agile framework that offers guidelines for managing and overseeing the software along with product development procedure (Omonije, 2024). In scrum, each development cycle is divided into a series of iterations where each iteration is called a sprint. The maximum duration of each sprint is 30 days (Sharma, et al., 2012). Scrums' initial point is Product Backlog. It is a list of activities which will be developed during the project (Carvalho & Mello, 2011). During each sprint, one sprint meeting is held every day to take the feedback on how much work has been done. After each sprint review is taken to determine whether all requirements have already been implemented or not to decide the requirements that should be implemented at the next sprint.

Figure 5: Structure of Agile Scrum Methodology (Scrum.org, 2023).

More about Scrum in Appendix 2 (Scrum Methodology)

5.2.2.1. Reasons behind Choosing Scrum

Continuous Feedback: Scrum enables continuous feedback in developing SIEM features, making it easier to adapt to changes and enhance functionality based on user input.

Flexibility to Change Requirements: Scrum supports evolving SIEM requirements by allowing flexible adjustments to priorities during sprint planning, ensuring changes are integrated without disrupting the project.

Transparency and Continuous Improvement: Regular sprint reviews and daily scrums help identify issues early and drive continuous improvement based on team feedback and challenges.

Risk Management: Scrum's iterative approach allows for managing risks in smaller increments, reducing impact and enabling faster mitigation compared to traditional models like Prototyping.

Resources Requirement

This project requires various hardware and software which are listed below:

6.1. Hardware Requirements

The hardware that is required for this project is listed below:

Computer: Personal Computer

CPU: Intel/AMD (I510th Gen or Ryzen 5)

GPU: NVIDIA GTX 1650

SSD: NVME 512 GB

RAM: 16GB

Stable Internet Connection

6.2. Software Requirements

Deployment: Docker/ Virtual Machine

Version Control: GitHub

Designing: Canva, draw.io

Documentation: MS Word

IDE: VS Code

Work Breakdown Structure (WBS)

Figure 6: Work Breakdown Structure for SIEMLite.

Milestones

Figure 7: Milestone Chart for SIEMLite.

Project Grant Chart

Figure 8: Project Gantt Chart for SIEMLite.

10. 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, an affordable SIEM solution with enhanced features tailored for advanced malware detection and analysis is proposed. 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.

12. Appendix

12.1. Appendix 1 (Prototype Model)

12.1.1. Advantages of Prototype Model

The advantages of Prototype Model are:

User Centric Development: It strongly emphasizes user involvement and feedback. By creating prototypes, this methodology ensures that the final product closely aligns with the user needs, preferences and expectations (Govardhan & Munassar, 2010).

Improved Communication: Prototyping enhances communication and collaboration between developers and end-users. This model visualizes the software functionality early, which makes better understanding for stakeholders.

Faster Development: This model focuses on rapid creation of prototypes of the software user interface and functionality. These prototypes are developed quickly to address the requirements of users.

Clearer Requirements: Due to continuous user feedback, misunderstandings regarding system functionality and design can be identified and resolved early in the development phase.

12.1.2. Disadvantages of Prototype Model

Even if there are various advantages of Prototyping model, it also has some advantages that organization should consider when deciding whether to use this model for software development project. Some disadvantages of this model are:

1 Limited Scalability: For large and complex system, the iterative model can become challenging to manage effectively. Extending prototyping to massive prototype can lead to increased complexity and resource demands (Liberatore & Nydick, 2008).

Incomplete Functionalities: Prototypes are typically created rapidly to collect user feedback, which may lead to certain functionalities being left out, causing some requirements to be overlooked (Bassil, 2012).

3 High Costs: Developing multiple prototypes and conducting iterative cycles of development and user feedback can be resource-intensive, resulting in higher development costs. This can make prototyping models less effective for projects with limited budgets.

3 Schedule Overrun: The iterative process of the Prototyping model can cause delays if the development and feedback phases go beyond the originally planned timeline, potentially impacting the project's schedule.

12.2. Appendix 2 (Scrum Methodology)

12.2.1. Advantages of Scrum

17 The advantages of Scrum are:

Improved Flexibility and Adaptability: Scrum allows teams to adapt quick changes in the requirements, priorities or market conditions through its iterative sprints and frequent feedback loops.

Enhanced Collaboration: Scrum emphasizes teamwork, open communication and regular interactions between team members which lead to better collaboration and problem solving.

Increased Transparency: Daily scrums, sprint reviews ensure that stakeholders and team members are kept informed about progress, challenges and goals.

Improved Quality: Continuous testing and review during each step help identify issues early, leading to higher product quality.

12.2.2. Disadvantages of Scrum

The disadvantages of Scrum are:

12 Not Ideal for all projects: Scrum may not be suitable for projects with fixed
1 requirements or strict deadlines, such as projects with well defined scopes or those that require a high level of documentation and predictability.

14 Inconsistent Results from Team Maturity: The success of scrum depends on the experience and maturity of the team. Teams that are less skilled in Scrum practice may produce inconsistent results and may struggle with the iterative nature of the framework.

Requires Strong Product Owner Involvement: It heavily depends on the role of Product Owner to prioritize and make decisions. If the owner is unclear about the requirements, it can significantly impact on the team’s productivity and focus