

ProjectProposalFinal

by James Turner

Submission date: 19-Oct-2025 05:05PM (UTC+0100)

Submission ID: 265685844

File name: 49143_James_Turner_ProjectProposalFinal_695044_1994990007.docx (98.09K)

Word count: 1673

Character count: 9523



Independent Project Proposal

ACCA6020

James Turner (2304088)

ACCA6020 – Independent Project

Research Proposal

Introduction including aims and objectives

Project Title: Implementation and Evaluation on an Open-Source Security Information and Event Management (SIEM) for Small Scale Networks

In our modern age of computing, cyber threats are becoming increasingly common for both larger and smaller organisations. For larger companies, investing in commercial Security Information and Event Management (SIEM) solutions is quite common, as they can help to consolidate network activity while providing real-time malware detection abilities. However, smaller companies and publicly funded institutions such as schools do not often have the budget for commercial licences for these solutions, leaving them exposed to otherwise preventable attacks. The project being proposed aims to address this problem by investigating an open-source SIEM, more precisely Wazuh, can provide a practical and compelling solution for monitoring small scale networks.

The main aim of this project is to design, deploy and evaluate Wazuh, the open-source SIEM, in a virtual environment to research and assess its ability to detect and deal with common security events such as unsuccessful login attempts, network port scanning and potentially suspicious activity. In order to achieve this aim, the following SMART (Specific, Measurable, Achievable, Relevant, Time) objectives are being proposed:

- 1.) Deploy and configure a SIEM system on a dedicated virtual server, with at least one client attached to the server and SIEM. This will be deemed a success via successful logs and display in the Wazuh dashboard.
- 2.) Simulate common security events, such as brute force login attacks using Hydra and reconnaissance attacks using Nmap. These tools will be implemented using another virtual machine in a safe and contained environment to ensure outside networks are not affected. This will be deemed a success via a collection of the recorded events by the SIEM.
- 3.) Evaluate the SIEMs accuracy and response-time. This includes recording the total amount of security alerts generated by the SIEM versus the total number of events generated by the simulation tools, as well as rate of false positives. This will be deemed a success by documenting the percentage of events detected by the SIEM including the average time-to-alert.
- 4.) Assess SIEM usability and effectiveness. This includes an examination of the initial set-up process of the SIEM, its ease of use, as well as interpretation of alerts shown on the dashboard. This will be deemed a success by providing an assessment and reflection on the SIEM.

In order for this project to be considered a success, the SIEM must be able to reliably detect a multitude of common attack types via simulated tools, providing understandable visualisations into the networks activity, all while being approachable and user-friendly. This will be proved using a configured virtual Network for the SIEM to be implemented, multiple screenshots of dashboard and log contents, including a 10,000-word report which will summarise the methodology, results, evaluation, and reflections on the project as a whole.

Project Background and Literature Review

An effective cyber-security solution relies on fast detection of potentially malicious activity across both host devices and the network itself. SIEM systems aim to provide a centralised location for collecting, comparing, and analysing information logs from multiple sources [1]. SIEM tools are a combination of two separate components, a Security Information Management (SIM) which deals with log storage and reporting, while Security Event Management (SEM) deals with real-time data correlation and alerts. These two components work together to provide a cohesive protection layer for cyber defence. [2]

Historically, SIEMs were adopted by larger organisations who already had dedicated security teams and large-scale infrastructure in place, due to their licensing costs and other requirements. However, the amount of small and medium-sized enterprises (SMEs) requiring similar detection tools and alert capabilities has vastly increased, but they simply cannot afford the current market tools. As a result, there have been several open-source tools created that have already been evaluated, including Wazuh, OSSIM and Elastic Security. [1] [3] [4]. These tools aim to provide a comparable experience to paid SIEMs while having a reduced cost and often reduced complexity.

Manzoor et al [1] conducted a thorough study on various different open source SIEMs for SMEs. These included Wazuh, OSSIM, SIEMONSTER and Elastic Security. Their results showed that Wazuh achieved the highest overall rating between the four different SIEMs. These results included ratings for security event management, usability, and customisability. Bezas and Filippidou [2] also evaluated several different SIEMs, and found that often “commercial SIEM solutions tend to be complex and expensive, the open source tools meet the needs of many organisations” This shows that especially for smaller businesses, the open source tools tend to be better suited for smaller environments due to their cost and approachability.

Conversely, Hackländer-Jansen et al [5] showed that SIEM rulesets can be exploited and bypassed, with almost 40% of common open-source SIEM rules being able to be fully or partially evaded, leading to undetected intrusions and is a major security risk if not identified and addressed. In order

to address this, deep learning techniques could be introduced via log-based anomaly detection, which Le and Zhang [6] had explored. While the initial results from their analysis seemed promising, the performance of the models was not as good as expected and as such will take some time before deep learning algorithms can help to reduce false-positives for log-based detection.

This project aims to build upon these studies by deploying a Wazuh SIEM within a controlled virtual environment and to simulate real-world attacks on the system using the MITRE ATT&CK and Cyber Kill Chain frameworks to establish detection performance and accuracy.

Project Design

This project will utilise a Waterfall development methodology, providing a structured framework tailored for smaller projects with clearly defined objectives and deliverable content. Waterfall has several well-defined phases, including: Requirements, Design, Implementation, Testing and Evaluation. This development methodology is appropriate for this project due to the clear objectives set, having limited outside stakeholder feedback and project time constraints. The overall goal for the project is to design, deploy and analyse an open-source SIEM (Wazuh) in a controlled virtual environment to determine its effectiveness and usability for small network environments.

Development Phases

Requirements | The first phase of this development aims to determine system requirements, number of client systems required, sources for logging information.

Design | A virtual network will be designed using VirtualBox virtual machines to simulate a small network environment similar to those found in SMEs or schools. It will include one Wazuh server, two client machines including one windows and one Linux based machines. All machines will be host-only to isolate the network from the internet and ensure ethical compliance.

Implementation | Wazuh will be installed and configured on the server machine, which will integrate with Elastic Stack for log management and data visualisation. On the client machines, Sysmon will be used to generate event logs for Wazuh to evaluate, with Nmap and Hydra used to simulate reconnaissance and brute force attacks on the network. All of the tools mentioned are industry-standard and open-source, meaning they are available for everyone to use and deploy as they see fit.

Testing | This phase includes deploying the simulated attacks against the network, with event data being collected and shown via Wazuh's dashboard. These attacks will follow the MITRE ATT&CK framework for uniformity in techniques and procedures based on real-world observations.

Analysis | The collected data via logs will be analysed to identify false-positive ratio, detection accuracy and time-delay for attacks to be recognised.

Methodology justification

The waterfall methodology was chosen as it closely aligns with the project's clear, defined objectives. Agile was originally considered for this project, however, as it relies on constant stakeholder feedback and flexible requirements, it was deemed unsuitable for this project. Each stage of waterfall requires the previous stage to have been completed, which naturally will be a great fit as only one person will

be working on the project and will not have the ability to develop different parts of the project simultaneously.

Overall, waterfall provides a suitable approach for the project being proposed, ensuring technical exploration and clear assessment, ensuring that the project is both thorough and feasible for an undergraduate project.

Resources/Planning

At the projects conclusion, there will be several key deliverables to determine the success of the project. The primary deliverable will be a fully configured virtual environment with an open-source SIEM (Wazuh) being deployed and maintained, connected to various client machines. Additional deliverables includes technical reports documenting the set-up and installation of Wazuh and client machines, included dataset documenting events and alerts generated by the SIEM, as well as a final report detailing the methodologies implemented, overall findings and evaluation for SMEs. The following Gantt chart displays the provisional project schedule



Resources

The project will be developed on both university and personal workstations. Each workstation will require a minimum of 16GB RAM, and preferably a Quad-core processor to host the various virtual machines necessary. The software running on these machines can include: Wazuh, Elastic Stack, Sysmon, Nmap, and Hydra. All are open-source and freely available, allowing both students/SMEs/schools to easily replicate the project without licence concerns.

Bibliography

- [1] A. W. A. F. J. A. M. Jawad Manzoor, "Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs," *PloS one*, vol. 19, no. 3, 2024.
- [2] F. F. Konstantinos Bezas, "Comparative Analysis of Open Source Security Information & Event Management Systems (SIEMs)," *Indonesian Journal of Computer Science*, vol. 12, no. 2, pp. 443-468, 2023.
- [3] J. M. M. A. A. Z. U. A. T. A. M. Aamna Tariq, "Open source SIEM solutions for an enterprise," *Information and Computer Security*, vol. 31, no. 1, pp. 88-107, 2022.
- [4] R. L. d. C. C. L. S. C. R. Ana Paula Vazão, "Implementing and evaluating a GDPR-compliant open-source SIEM solution," *Journal of Information Security and Applications*, vol. 75, 2023.
- [5] R. U. M. H. S. S. M. H. Louis Hackländer, "You Cannot Escape Me: Detecting Evasions of SIEM Rules in Enterprise Networks," USENIX Association, Philadelphia, 2024.
- [6] H. Z. Van-Hoang Le, "Log-based Anomaly Detection with Deep Learning;," ICSE, Pittsburgh, 2022.

FINAL GRADE

GENERAL COMMENTS

64/100

PROJECT PROPOSAL – ACCA6020 INDEPENDENT PROJECT

Student James Turner
Mark 67

Intro / A&O (400 words)		
Project title; Identification of a specific problem to be investigated; Well-defined aims and SMART objectives; Explaining why this project is worth doing; Discussion of what the project needs to do in order to be a success; Description any deliverables that will be produced at the end of the project	20	14
The project title and objectives are clear and measurable. Success criteria are well-defined but limiting, Your ethics form stats a Windows and Linux clients but I would like to see a mix of 3 - 5 clients being deployed not the minimum of one stated in the proposal. Could		

better justify the importance beyond cost and explicitly link objectives to the overall aim.		
Background to the Project / Literature Review (400 words)		
Description of how the work to be done by in the project relates to the work identified in the literature review; Discussion of any ethical issues raised by the project Identifying what has already been done within the field; Topic familiarity; Brief literature review using appropriate sources – 6-8 journal papers and book chapters rather than just websites; Selection of relevant models & concepts Good overview of SIEM concepts and relevant topic. Mentions limitations and emerging solutions. Ethical considerations would be expected with this type of project and a stronger link between literature gaps and proposed work when it comes to the final report.	20	13
Project Design (500 words)		
Clear statement of which development methods are to be used and why they are appropriate; Clear statement of which tools are to be used and why they are appropriate; Clear description of how data collected will	30	19

be analysed Methodology and tools are appropriate and well-rationalised. Testing aligns with MITRE ATT&CK. More depth of the project could have been given on analysis and any contingency plans in case the VM fails.		
Resources / Planning (200 words)		
List of any deliverables; Clear diagram showing both timing and resource use; Completed ethics form; Limited and relevant appendices Lists deliverables and hardware/software requirements clearly. Gantt chart mentioned. Resource allocation and timing could be more detailed and how this would align with the waterfall methodology.	15	10

Document Presentation		
Correct spelling, grammar and punctuation; Flow of narrative/fluency; Coherence; Word processed ; Correct use of referencing with bibliography; Strict word limit Appropriate technical language, but grammatical refinements and formatting needed to adhere to what is expected. Such as paragraph spacing and heading being at the end of a page	15	8
TOTAL	100	64

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8
