

Independent Project - Proposal - Cameron Brown (2004688)

by Cameron Brown

Submission date: 18-Oct-2023 10:17PM (UTC+0100)

Submission ID: 213678307

File name: 23166_Cameron_Brown_Independent_Project_-_Proposal_-_Cameron_Brown__2004688__508662_244306879.docx (162.55K)

Word count: 2347

Character count: 12450

Evaluating the Efficacy of SIEM Systems in Detecting and Mitigating Cyber Attacks

Research Proposal

Cameron Brown

Preferred Supervisor: Nitheesh Kaliyamurthy (or
Kapilan Radhakrishnan)

Word count: 2001

Contents

Contents 2

1. Introduction 3

2. Background to the Proposed Research 3

3. Aims & Objectives 4

4. Methodology 4

 4.1 Research Methodology 4

 4.1.1 Philosophy 4

 4.1.2 Approach 4

 4.1.3 Literature Review 5

 4.1.4 Risks & Limitations 5

 4.1.5 Ethical Issues 6

 4.1.6 Validity, Reliability & Generalisability 6

 4.1.7 Data Evaluation Methods 6

 4.2 Development Methodology 6

5 Resources and Planning 6

 5.1 Hardware Resources 6

 5.2 Software Resources 6

 5.5 Project Plan 7

6. Reference List 8

1. Introduction

Data is a core part of modern society. Whether you're sending a text message to a family member, engaging in an online company video meeting, or sending an email to your boss, you'll be sending data across the network. This data gets protected by various means, but these protections aren't always perfect as new and obscure attacks can creep up and catch an organisation by surprise. This can leave data vulnerable if they aren't already prepared to deal with it. This is what makes SIEM (Security information and event management) software incredibly useful, SIEMs collect and allow users to analyse logs from an organisations system and allows them to detect and prevent malicious activity, giving them an edge towards fighting attacks that they likely would not have had prior [1]. Threat detection and incident response efficiency in an organisation improves drastically with the use of an SIEM software due to the sheer number of convenient tools that they provide to the users.

I'm proposing my project on this topic due to having an interest in defending against cyber-attacks. With ongoing modules (Advanced Cyber Security), plenty of online learning possibilities (TryHackMe, HackTheBox), planning to obtain industry recognised certifications from providers such as Cisco and CompTIA, and a lot of motivation towards starting a career relevant to cyber security, I had decided that this would be a great opportunity to get a foot in the door towards furthering my chances of securing a career in that field and allow me to get some hands on experience with relevant tools along the way.

2. Background to the Proposed Research

Log data holds records of all the events that happen in a system. Events are usually automatically logged which gives the users detailed information on what happened on that system during that time, including what happened and when it happened. Managing and analysing these logs is vital for an organisation to remain safe and secure. "Event log data is initially collected at device level and may be transferred at an aggregate level to a remote destination, e.g., in the 'cloud'." [2] Because these logs can be gathered and transferred to a remote destination, it's possible to manage and analyse logs from many different systems. Due to this, there are jobs based off using software known as SIEM (Security information and event management) to aid in analysing these logs. SIEMs have very useful features such as:

- Search and Analysis: SIEM software allows its users to search through the logs of a system and to analyse them to find any potential harm that could either be obvious or hidden within. [3]
- Alerting: Alerts can be set up in an SIEM to notify users about certain events. This allows an organisation to respond to an incident at a pace that they may not have been able to otherwise. [3] These alerts also allow the organisation to easily escalate the issue to higher ups if certain analysts aren't quite capable of dealing with the issue themselves.
- Data Retention: SIEMs allow data to be retained for certain amounts of time. This allows certain logs to be analysed for a forensic investigation into an old incident or breach. This also allows an organisation to compare old security policies to new policies to find out how much the security practices have improved over time. [3]

3. Aims & Objectives

This project aims to access the effectiveness of SIEM tools in detecting and preventing attacks on systems. The capabilities of these SIEM tools will be evaluated based on how they respond and mitigate threats and security incidents. Insights and recommendations for improving the implementation and configurations of these SIEM tools will be given to improve the efficacy of the tools in protecting information.

To complete this project, many objectives will need to be met, these objectives include:

- Selection of SIEM tools: Many of the SIEM tools used in the industry are quite costly, but many of these also have free licenses which will be very useful for putting the SIEM tools to use in the project without worrying about a trial period running out before the project has concluded.
- Setting up virtual machines: To mitigate any risk of threats on any real network, virtual machines will be set up and all aspects of the threat deployment and the detection and mitigation of the threats will all be done on a virtual machine.
- Attack simulation: To analyse the efficacy of these SIEM tools, attacks will be simulated on these virtual machines with the SIEM tools installed and set up.
- Evaluation of detection and mitigation capabilities: Once the machines have been attacked by these threats, an evaluation of how well the tools detected and mitigated the threats will be done.
- Recommendations based on information gathered: With the attack simulation and the evaluation done, recommendations based on the information gathered will be given to help improve the efficacy of these SIEM tools to secure data in a more efficient way.

4. Methodology

4.1 Research Methodology

Due to the nature of the project being an experiment based on simulating attacks on machines and evaluating the efficacy of the SIEM tools, the research methodology will be quantitative due to the statistics that will be provided during the project.

4.1.1 Philosophy

This project will use a positivistic philosophy due to the results gathered being objective. The experiments will provide statistics rather than opinions, personal bias will not exist in the results while a phenomenological philosophy would mostly be used for data that is subjective with low reliability.

4.1.2 Approach

An inductive approach will be used for this project. This is because the goal is to evaluate data collected during the experiment and then develop insights and recommendations based on the findings over the course of the project. While the findings will be objective, the insights and recommendations provided afterwards will be subjective. A downside to inductive is that the interpretation of the data will need to be skilled and accurate, therefore adequate research on the topic will be done to assist in the accuracy of the interpretation of the data gathered.

Cameron Brown
2004688

4.1.3 Literature Review

With technology becoming more important and widespread as the years go by, the need to secure these technologies also becomes more important. Due to this, there is no shortage of academic research on the topic of the use of SIEMs in cyber security. One report that stands out is titled “Risk Assessment Driven Use of Advanced SIEM Technology for Cyber Protection of Critical e-Health Processes” by Luigi Coppolino, et al. This report provides valuable insight into the use of SIEM tools to improve the security of a “Smart Hospital (i.e., one where IT is massively used), with challenging security requirements.” [4]

One of the reports main focuses is on the risk assessment driven approach. In which this method is used to identify the vulnerabilities and threats to the e-Health of the systems apart of the hospital. The report mentions that an SIEM has been “specifically tailored to the needs of hospitals and health care institutions—with advanced data processing and event correlation capabilities.” [4] Having a customised SIEM tool allows for a much more efficient way to protect against threats and attacks that is likely to be more personalised towards a hospital where people’s lives can be dependent on these technologies staying on and active, and where very confidential information on patients are stored.

Granadillo, Zarzosa and Díaz were the authors of a report titled “Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures”. An interesting section of this report is titled “Limitations of Current SIEMs” where the authors discuss in detail about the main limitations of SIEM tools, and what the authors themselves think could be done to help alleviate these limitations. One of the sections that stand out is about the reliance on humans, the authors go on to write about how “in many cases, threat responses still require humans to carry out the analysis and make decisions with respect to understanding the threats, defining the appropriate countermeasures, and deploying them.” [5, p.9] Considering how a majority of the current SIEM tools have great automation tools in place, such as alerts, correction rules, workflows and the currently emerging usefulness of AI and machine learning. AI and machine learning has been an incredibly useful asset in automation, especially since some of these AI and machine learning use decades of information to help investigate and respond to threats. [6]

Byrant and Saiedian wrote a report titled “A novel kill-chain framework for remote security log analysis with SIEM software”. In which the authors give an in-depth insight on a framework that, as mentioned in the conclusion, was able to detect “25 out of 26 test cases (96% detection rate) compared to seven out of 26 test cases (26.9% detection rate) with the default SIEM framework.” [7] Which shows that customising an SIEM to fit the needs can drastically improve the efficacy of threat detection.

4.1.4 Risks & Limitations

A risk with this project is if the attacks are exposed to a network, which could cause harm to the devices on that network. To prevent this from happening, everything included in the experiment will be done on virtual machines to keep it separated from real networks and real devices. The limitations of the projects would be the costs of the full licenses of SIEM software, to handle this limitation, the free licenses will be used instead which still provide everything needed to complete the project.

Cameron Brown
2004688

4.1.5 Ethical Issues

With all risks being managed and avoided, there would be no ethical issues. But if a mistake occurs and the attacks are simulated on a real network rather than a VM, then the data security of the devices on that network will be breached.

4.1.6 Validity, Reliability & Generalisability

4.1.6.1 Validity

Simulating attacks on a network being protected by SIEM tools would be a very good way to validate the efficacy of these tools in a real-life scenario.

4.1.6.2 Reliability

Other researchers would likely do a similar experiment and gain similar results if they investigated the problem that the project aims to solve.

4.1.6.3 Generalisability

The results of this project apply to any organisation that uses SIEM tools to help with cyber security threats. These organizations use the same or very similar tools to keep their data secure and the project evaluates the efficacy of these tools.

4.1.7 Data Evaluation Methods

4.1.7.1 Data Collection

Quantitative data will be collected via the results of the experiment that will be conducted. The project will eventually be concluded, and results will be gathered no matter the outcome of the experiment. The minimum amount of data needed will be the results of how well the SIEM tools do against the attacks that will be simulated on the machines.

4.1.7.2 Data Evaluation

The data will be evaluated using inferential statistics, data will be collected, and the evaluated data will help solve the problem that the research question aims to solve. The data will likely be presented using summary statistics and data visualization in the form of graphs and charts.

4.2 Development Methodology

The development methodology that will be used will be “kanban”. As this is a project that will be conducted by a singular person, kanban works better than other methodologies due to being fit for solo projects.

5 Resources and Planning

The resources that will be needed will be a computer with sufficient hardware to run virtual machines and SIEM software.

5.1 Hardware Resources

The hardware needed will be a computer. This computer will need to be able to run virtual machines and SIEM software with ease to make the project proceed smoothly.

5.2 Software Resources

This project will require the use of much software. This includes VirtualBox, at the current time, version 7.0.12 is the newest version for this software so that will be used.

Operating systems for VirtualBox will be needed to conduct the experiment so an ISO file for Windows 10 gathered from Microsoft themselves will be needed.

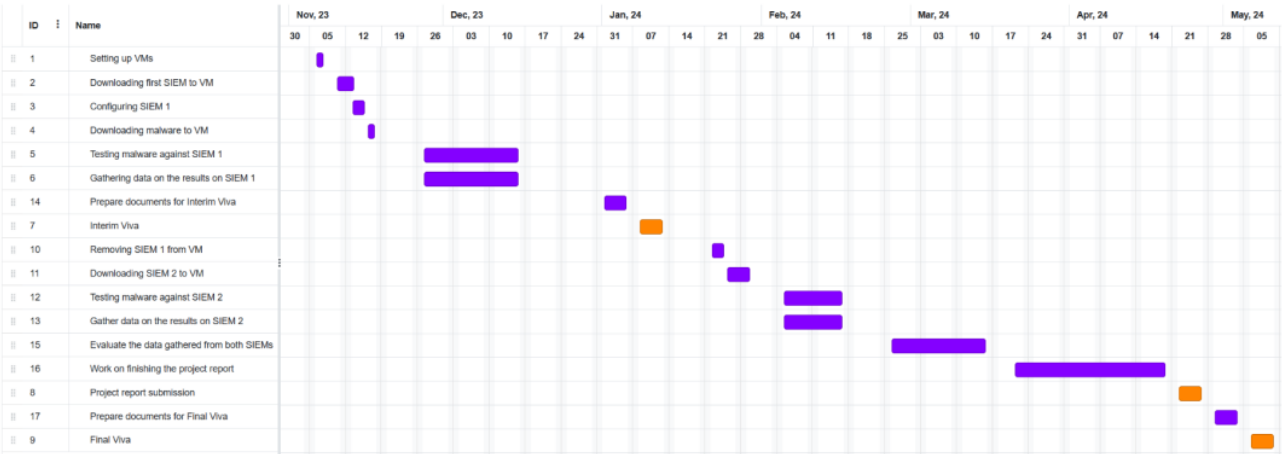
Cameron Brown
2004688

SIEM tools will be needed, Splunk and Graylog will be chosen due to having free licenses that have plenty of features to complete the experiment. These will be gathered from their official websites.

Malware will also be needed to simulate an attack on the systems. This will be gathered from a known and respected malware repository on Github.

5.5 Project Plan

Proposed Gantt chart:



Cameron Brown
2004688

6. Reference List

- [1] C. Kidd "What's SIEM? Security Information & Event Management Explained" 2023. [Online] Available: https://www.splunk.com/en_us/blog/learn/siem-security-information-event-management.html
- [2] R. Turkington, M.D. Mulvenna, R.R Bond, S. O'neill, C. Armour. "The Application of User Event Log Data for Mental Health and Wellbeing Analysis." (2018).
- [3] J. M. López Velásquez, S. M. Martínez Monterrubio, L. E. Sánchez Crespo, and D. Garcia Rosado, "Systematic review of SIEM technology: SIEM-SC birth," International journal of information security, vol. 22, no. 3, pp. 691–711, 2023, doi: 10.1007/s10207-022-00657-9.
- [4] L. Coppolino, L. Sgaglione, S. D'Antonio, M. Magliulo, L. Romano, R. Pacelli. "Risk Assessment Driven Use of Advanced SIEM Technology for Cyber Protection of Critical e-Health Processes." (2021). Available: <https://link.springer.com/article/10.1007/s42979-021-00858-4>
- [5] G. Granadillo, S. Zarzosa, R. Díaz. "Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors". (2021). doi: 10.3390/s21144759
- [6] Eduardo Kassner "The first born-in-the-cloud SIEM with built-in AI" [Online] Available: <https://blogs.partner.microsoft.com/partner/the-first-born-in-the-cloud-siem-with-built-in-ai/>
- [7] B.D Bryant, H. Saiedian. "A novel kill-chain framework for remote security log analysis with SIEM software". (2017). doi: 10.1016/j.cose.2017.03.003

Independent Project - Proposal - Cameron Brown (2004688)

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

75/100

PROJECT PROPOSAL – ACCA6020 INDEPENDENT PROJECT

Student [2004688](#) (Cameron Brown)
Mark 75

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	15
- To enhance the introduction, consider providing a brief example or case study that illustrates the need for SIEM software in a real-world scenario. This would engage the reader and make the introduction more compelling.		

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 - Consider adding a subsection that discusses recent developments or emerging trends in SIEM technology to keep the background information up-to-date.	20	14
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 be analysed - - While the objectives are clear, it would be beneficial to add specific metrics or criteria for evaluating SIEM tool effectiveness. This would make the evaluation more precise	30	24

and provide a clearer basis for recommendations. - It would be helpful to specify how data will be collected during the attack simulation and how the results will be quantitatively analyzed. This would provide more detail on the research process.		
Resources / Planning (200 words)		
List of any deliverables; Clear diagram showing both timing and resource use; Completed ethics form; Limited and relevant appendices - The section on data collection and evaluation methods could benefit from more details, including the specific data points to be collected and how they will be analyzed statistically.	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 - While it's clear and coherent, there's	15	12

room for improvement in the narrative's flow.		
TOTAL	100	65

PAGE 1
PAGE 2
PAGE 3
PAGE 4
PAGE 5
PAGE 6
PAGE 7
PAGE 8