



Abstract

This project was completed to design and implement a SIEM solution. The primary focuses were on the topology design, implementation of the SIEM and centralised log database and then the simulated cyber incidents that were used to evaluate the effectiveness of the SIEM itself. Based on the work completed, the SIEM was successfully implemented into the internal network, with Sysmon log information being parsed through to the SIEM for further analysis.

Introduction

With the ever-changing world of cybersecurity, organisations demand more advanced monitoring and responses for cyber incidents. SIEM solutions are an intrusion detection system (IDS), designed to collect log file information from network devices and analyse the information for suspicious activity [1]. Specifically this project aims to provide a custom Elasticsearch Kibana (ELK) SIEM solution for Carmarthenshire County Council (CCC), with an emphasis on centralising log files for Windows based workstations and servers. This SIEM will then be tested using simulated cyber incidents, to measure it’s effectiveness at detecting these threats as if they were happening live on the network. The overall goal is to demonstrate the feasibility of SIEM solutions, and how effective they are at detecting threats.

Aims and Objectives

- Aim:
- The aim of this project is to design, implement and evaluate a SIEM solution that can be used within CCC’s network. With the objective of having the solution tested against simulated cyber incidents, thereby assessing its effectiveness in enhancing organisational cybersecurity posture.
- Objectives:
1. Complete comprehensive literature review into SIEM solutions and methods/ standards for testing.
 2. Locate and document suitable methods for testing the SIEM solutions.
 3. Provide a comprehensive plan for implementing and testing the SIEM solution.
 4. Outline and document the experimental aspects of the project.
 5. Design the SIEM architecture, based on the system requirements of CCC.
 6. Design and Implement the desired simulated tests that will be used to evaluate the SIEM.
 7. Analyse the gathered data, and provide recommendations based on what was found.

References

[1] – Author: R. Botwright, Published: 2024, Name: "Defense In Depth - Network Security And Cyber Resilience", Publisher: Rob Botwright, [Accessed: 04th April 2025], Available: [Defense In Depth - Google Books](#)

[2] – Author: Cybersecurity & Infrastructure Security Agency, Published: 11th November 2024, Name: "Logging Made Easy", [Accessed: 3rd April 2025], Available: [Logging Made Easy | CISA](#)

[3] – Author: R. Johnson, Published: 10th January 2025, Publisher: HiTeX Press, Name: "Logstash Made Easy - A Beginner's Guide to Log Ingestion and Transformation", [Accessed: 5th April 2025], Available: [Logstash Made Easy - Google Books](#)

[4] – Author: Red Canary, Name: "Welcome to Atomic Red Team", [Accessed: 5th April 2025], Available: [Atomic Red Team](#)

Simulated Incident Testing & Results

To evaluate the effectiveness of the SIEM, a series of simulated cyber incidents were executed through using a combination of the Atomic Red Team framework and Kali Linux. The Atomic Red Team framework is a group of command line based, technical cyber tests, closely aligned with MITRE ATT&CK Tactics, Techniques and Procedures (TTP’s) [4]. Kali Linux, which is a Debian based operating system built for Penetration testing, was also used as it has a number of pre-built in tools which the researcher could use for attacking the test workstations and seeing how the SIEM would react. The chosen simulated incidents for this project were Credential Dumping (T1003) through Minikatz, Network reconnaissance through an NMAP ping sweep (T1046), and lateral movement through the use of PSEXec. The SIEM successfully detected and alerted all of these activities, with some having varying accuracy and response times, due to some logs not being generated correctly. The Minikatz credential dumping simulation resulted in high levels of detection, with minimal false positives being generated. However NMAP reconnaissance tests showed some delays, this was down to a combination of network bandwidth for the testing network and the complexity of correlating multiple events happening all at once. Overall the SIEM solution demonstrated a strong capacity in detecting the provided simulated incidents. However further refinements to the detection rules can be provided to improve efficiencies in a live environment, as the tools and techniques may not appear as straightforward as when run in a simulated test environment. However the results generated will provide a clear roadmap of what can be improved, providing further enhancements in detection logic and alerting mechanisms. Kibana also provide tools to be able to link it’s dashboard alerts to other external services, so post detection actions can also be tested. Figure 2 shows the average detection times for each of the tests. Overall, the graph shows that each test completed was able to definitively and quickly provide an alert on the SIEM dashboard. There were no times where a test wasn’t able to successfully alert to the cyber incident, however for NMAP and PSEXec, there were times where an alert wasn’t generated, and therefore data could not be added to the experiment table. Therefore these averages may not be fully accurate, however they are provided to show that at the core, the SIEM was successful in generating alerts for each test.

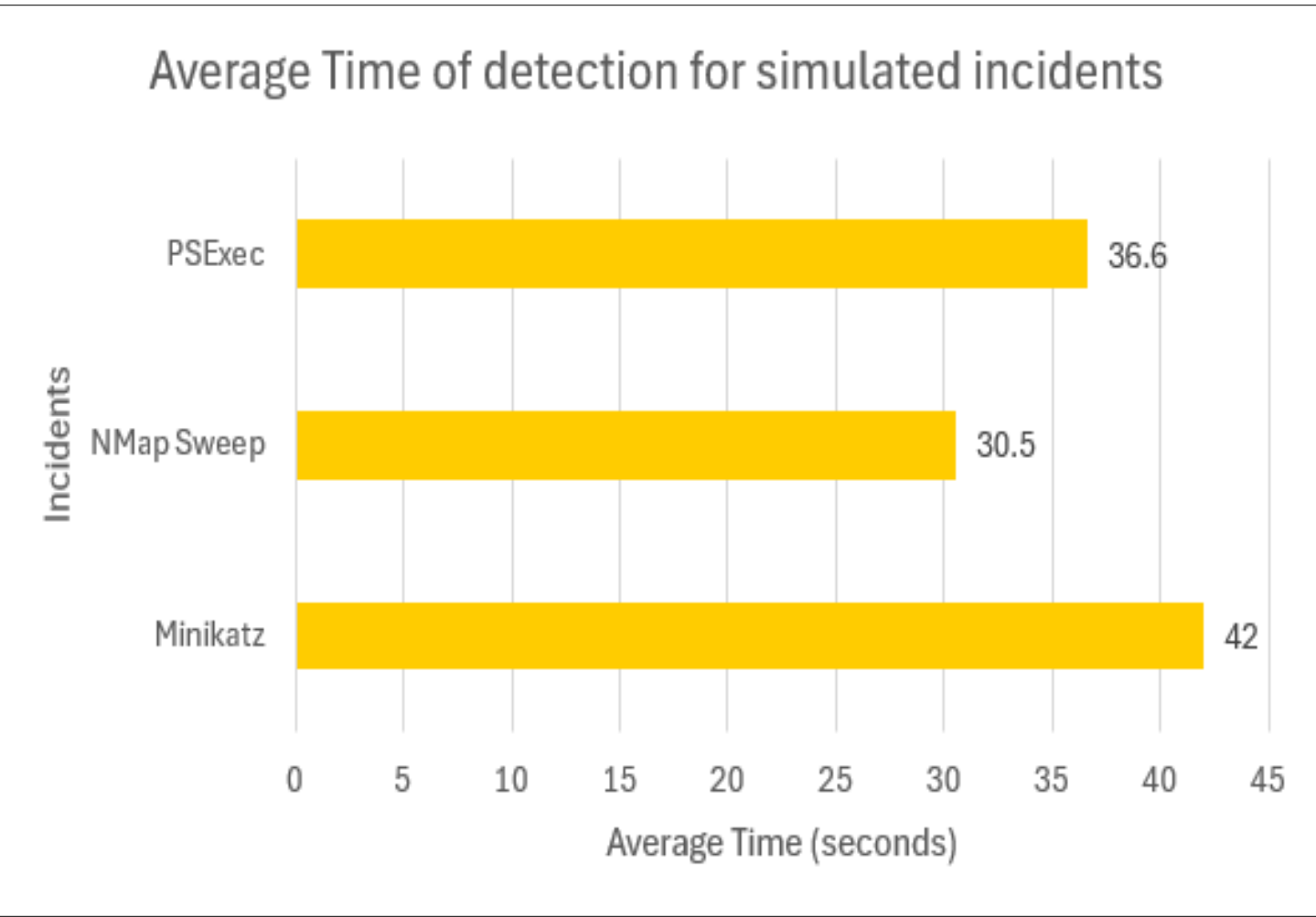


Figure 2—Graph of average detection times

SIEM Design & Implementation

As shown in Figure 1. The network topology for the SIEM consists of a Linux based server, which will host Logging Made Easy (LME). LME is a no cost Kibana based SIEM solution that provides both log management and threat detection services [2]. The remaining sections are the workstations, which are connected to the dashboard through an Elastic agent. The Kibana dashboard used for virtualising the log data, through the use of a data processing method called Logstash [3]. This architecture provides a centralised log management system, enabling real time analysis and detection of suspicious activities. The solution was implement through multiple phases, including server setup, Elastic agent configuration and detection rule creation.

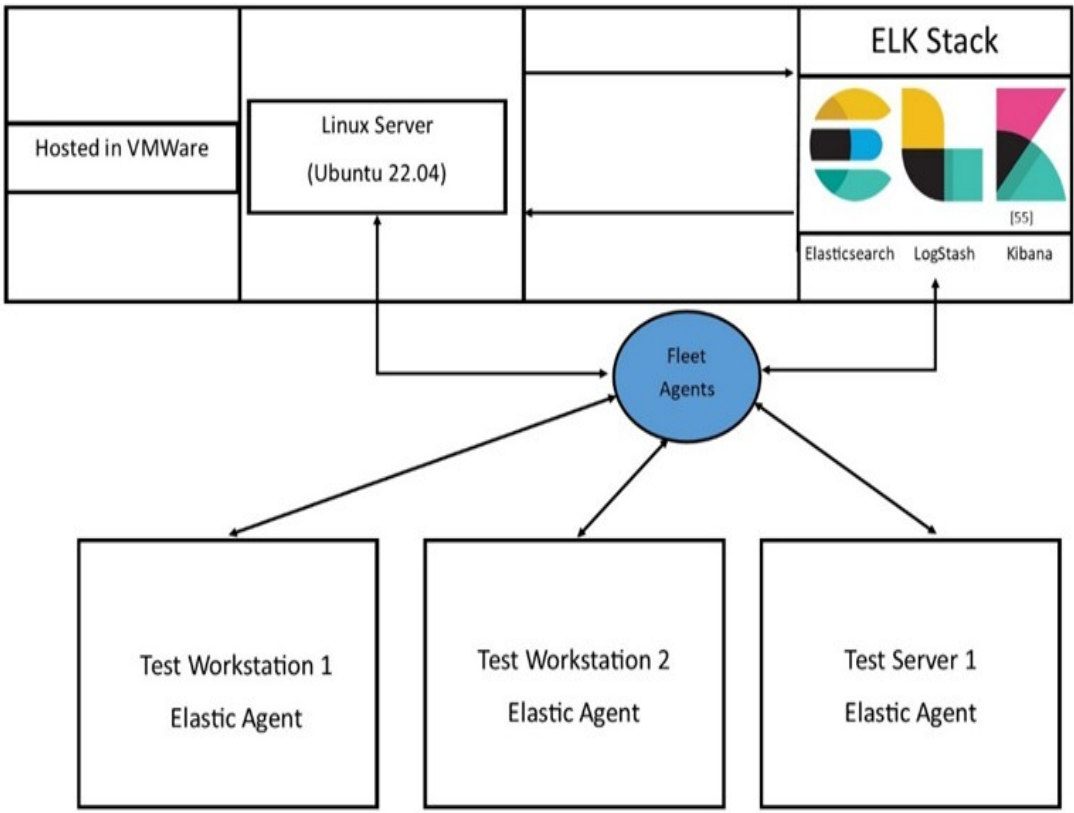


Figure 1—Network Topology of the ELK Stack

Conclusion

This project showcased the development and evaluation needed to implement and test a SIEM solution. Integrating real time log file analysis, the SIEM solution was able to successfully provide timely alerts to all of the simulated incidents, minus a few technical issues which were fully documented, and will lead to further improvements in future. This project highlights the importance of SIEM solutions in fortifying cybersecurity infrastructure and lays the groundwork for future research into optimising detection logic and automated responses to incidents.