Logo, company name

Description automatically generated

**DISSERTATION PROPOSAL**

**(COIS71052)**

**Development and Performance Analysis of Open-Source Tools for Building In-House SOC to Prevent Denial of Service (DoS) Attacks.**

**MSc in Computer Science**

**By**

**Muyideen Kazeem Oluwadare (21027842L)  
Computer Science (Cyber Security)**

**Supervised By: Awais Muhammad**

**Staffordshire University**

**May 2022**

Table of Contents

[1. Introduction 4](#_Toc128696162)

[2. Research Background 5](#_Toc128696163)

[3. Research Question 6](#_Toc128696164)

[4. Aim 7](#_Toc128696165)

[5. Objective 7](#_Toc128696166)

[6. Methodology 7](#_Toc128696167)

[7. Deliverables 7](#_Toc128696168)

[8. Academic Challenges 8](#_Toc128696169)

[9. Plan of work 8](#_Toc128696170)

[10. Resources 9](#_Toc128696171)

[References 10](#_Toc128696172)

**TABLE OF FIGURES**

[Figure 1: Plan of work (Gantt Chart) 8](#_Toc128695028)

### 1. Introduction

Today, the most pressing security concerns for companies and organizations are targeted and complex cyberattacks. So, security experts agree that sophisticated cyberattacks are gaining prominence as a significant threat to businesses worldwide (Sousa, 2019). However, cloud computing, bring-your-own-device (BYOD) policies, and teleworking technologies have eroded the traditional boundaries of the workplace, making it easier for cybercriminals to penetrate small businesses and corporate networks (Akinrolabu et al., 2018). Due to the growing need to prevent major cyber incidents, the subsequent trend towards centralizing security operations within businesses has risen SOCs' importance dramatically over the past five years(Vielberth et al., 2020). According to Soliman & Azer (2018), DoS attacks are launched against live services to make them not accessible to authorized users; however, these attacks pose a significant risk to the performance of the SOC by overwhelming the network with packets that are not needed. Also, the primary functions of SOCs are to ensure reliable security and act as the nerve center for an organization's security operations, monitoring and improving the safety of the whole business (Vielberth et al., 2020). Al-Dhaqm et al. (2020) explained that while security models are essential to businesses' survival, protecting their assets from both internal and external threats is the top priority of the management and business owners when the confidentiality, integrity, and availability (CIA triads) of their assets (personally identifiable information (PII), personal health information (PHI), business plans and organizational objectives) are at risk. Using several open-source technologies, such as Intrusion Detection and Prevention Systems (IDS/IPS), Security Information and Event Management (SIEM), Vulnerability Scanners, Endpoint Detection and Response (EDR) solutions, and Threat Intelligence Platforms, a SOC can help to identify and prevent these cyber-attacks on assets over a company's network (Institute of Electrical and Electronics Engineers et al., 2017). Small businesses and students can benefit from learning how to establish an in-house SOC utilizing a variety of open-source tools that can deliver the most outstanding performance and how these tools are used to identify and prevent various types of network threats (must, especially Denial of Service -DoS)(González-Granadillo et al., 2021). Conversely, no research has been conducted on how to select the best performance and reliable open-source tools to be used to build an in-house SOC to detect and prevent denial-of-service attacks; however, a notable number of examination has been conducted on topics such as cost-effective SOC construction, comparison of network IDS/IPS tools, and measuring the effectiveness of SOCs in detecting suspicious traffic. This research focus is to examine the viability of establishing an internal SOC using open-source technologies by selecting tools with optimal performance for the purpose of detecting and preventing network attacks (denial-of-service).

### 2. Research Background

Security operation centers (SOCs) are essential to modern businesses, helping them to fulfil their obligations by bolstering their cyber security strategy through various technologies and tools (commercial or open-source) designed to detect and prevent cyber-attacks (Dietz et al., 2020). However, SOC can be categorized into Insource SOC, Outsource SOC, and Hybrid SOC which use a security information and event management (SIEM), intrusion detection system, intrusion prevention system, and threat intelligence with each having its own distinct set of drawbacks and advantages (Onwubiko & Ouazzane, 2019). The effectiveness of a SOC is dependent on its forensic and analytical ability, internal processes, capabilities, and awareness of the enterprise network, which makes a case for further advancement in SIEM. Even though there are various ways to acquire a SOC, there is a wide range of obstacles to overcome during the configuration process and when choosing the best-performing tools to aid the SOC in detecting and preventing malicious network activities (Akinrolabu et al., 2018). There are a few essentials needed for a successful SOC to function and this includes the right people, processes, and technology that can effectively monitor, categorize, display, and react to cyber-attack (Janos & Dai, 2018). Janos & Dai (2018) further explained that a SOC necessitates the development of high-performance hardware and software technologies (IDS/IPS, Firewall, SIEM, etc) on the network which can carry out penetration testing, security audits, and port scanning for countermeasures in order to detect and prevent an attack such as Network attack while Rosso et al. (2022) stated that even though technology and automation play essential roles in security monitoring, human operators are still needed to investigate alerts, report, and address incidents. SOC operators (SOC analysts, incident responders, threat hunters, and SOC managers) need time and education to examine threat inputs from automated systems. Even though there are dozens of open-source tools available in the marketplace to meet different types of SOC (Insource, Outsource, or Hybrid SOC) needs, OSSIM, Wazuh, Grafana, Elastic Stack, Snort, Suricata, Ossec, PfSense, Nmap, Wireshark, Nessus, OpenVAS, OWASP ZAP, Cuckoo, Autopsy, OpenCTI, MISP, Sysmon are primarily appreciated and extensively used and these open-source tools can be used for reducing the cost of building the In-house SOC (Vaarandi & Mases, 2022). Vaarandi & Mases (2022) also mentioned that the Security Information and Event Management (SIEM) platform collects, analyses, and presents security alerts and other enterprise-wide data, making it an essential tool for any SOC and even though there has been much discussion about several elements of SOC, almost no papers have detailed the actual implementation of a SOC or guided how to build one. In agreement with Vielberth et al. (2020), numerous SOC features including incident management are completely created till now, and due to the flexibility with which different standards and best practices are applied to these features, they must be reviewed to ensure they are up to grade. Nevertheless, no comprehensive SOC standard or structure makes auditing a unified and complicated SOC difficult, nonetheless, it is essential (Islam et al., 2019). DoS attacks are launched to exhaust server resources and block legitimate users from connecting to resources. However, the packet arrival rate or processing time of each packet increases during a DoS attack where the victim's system is forced to do intensive computations, and to prevent unauthorized access, authentication, and authorization are often employed in organizations, for example, only authenticated clients are allowed to send or receive messages on specified topics (Syed et al., 2020). It is essential to stress, however, that the problem-solving abilities and in-depth knowledge of how to install, configure, and understand when to utilize these open-source tools detailed in the study to build a SOC render them inappropriate for ordinary people, students, small businesses, and end users. Due to improper maintenance, configuration, integration, and the inability to collect all necessary data for accurate intrusion detection, as well as a lack of section of best tools with better performance to address the primary purpose, many SOCs have used various open-source tools when building their SOC without considering their performance-based and the resources they consume for their specific operation (Alahmadi et al., 2022). While the relevance of SOC standardization and automation cannot be emphasized, several other factors must be considered when building a resilient and efficient SOC. People, processes, and technology contribute to a reliable and effective SOC. However, this research project will focus on the technology area, which will address the setback mentioned above by measuring the performance of these tools to detect and prevent the attack and how they can be integrated to create an effective SOC that will help small businesses to prevent and detect DoS, and also help students understand how to detect and prevent these attacks in a SOC environment.

### 3. Research Question

In order to collect appropriate and objective responses, a research problem with a substantial amount of information was developed. The primary question was, "To what degree is it possible to assess open-source technology's efficacy in establishing an In-house SOC network to counter Denial-of-Service (DoS) attacks?"

### 4. Aim

In order to build a dependable and effective in-house SOC that detects and prevents network attacks (DoS), this study aims to examine existing research on SOCs and the open-source tools used in SOCs, analyze the current challenges in their performance, and investigate and recommend the tools with the best performance.

### 5. Objective

* To conduct a literature review and investigate the current performance of open-source tools to mitigate DoS attacks in an Inhouse SOC.
* Research and highlight available open-source tools that can be used to build an internal SOC.
* To develop a python script to measure the performance (CPU, memory, and response time to detect and prevent DoS) of the open-source tools used to build a SOC.
* To implement an internal SOC using open-source tools.
* To test, implement and validate the DoS protection capabilities of the In-house SOC.

### 6. Methodology

As part of our research methodology, we'll review existing literature to identify SOC and open-source tools that prevent and mitigate DoS attacks. Using a Python script, we'll assess various open-source tools for detecting DoS attacks and integrate the most effective ones into an internal SOC. To evaluate the effectiveness of the internal SOC, we'll conduct penetration testing, and simulated DoS attacks, and explore ways to update and improve its performance. We'll document the entire project in a detailed report, including a preliminary analysis and a PowerPoint summary of the results. On the other hand, we'll be documenting the entire project in a thorough report, from preliminary analysis to a PowerPoint summary that outlines the results.

### 7. Deliverables

The following deliverables must be submitted upon completion of the research project:

* A project plan/Gantt chart detailing the duration of the entire research project.
* A complete project report with the screenshot showing the implementation of the In-house SOC
* An implementation of an in-house SOC system utilizing open-source software.
* A python script to measure the performance of the open-source tools used for implementing the In-house SOC
* PowerPoint slides explaining in detail the project's summary.

### 8. Academic Challenges

One of the main concerns among academics is whether an organization's own SOC can effectively prevent DoS attacks. It's important to ensure that the in-house SOC can be adapted easily to various enterprise sizes and explore new techniques to stop DoS attacks. However, the time constraint is a significant obstacle to extensive research. Additionally, there is a need to enhance existing Python expertise to evaluate the open-source tool's performance. Implementing the method in a widely-used programming language could be challenging. Lastly, ethical considerations should be taken into account to avoid any adverse impact of the defence mechanism.

### 9. Plan of work

The strategy relies on the midpoint evaluation and project work delivery schedule. Meeting the midway point deadline requires starting several tasks quickly to show progress and direction. The artifact and independent study are the main submission tasks. Critical analysis, a concise summary, and future research ideas will improve the study. In addition to project work and the artifact, presentations for the midpoint assessment and final oral will be presented. The following Gantt chart shows the estimated research project timeline by week and its milestones.

Timeline

Description automatically generated

Figure : Plan of work (Gantt Chart)

### 10. Resources

The following resources are required for the research project:

* Hardware Requirements
  + A personal computer with 16GB of RAM, Core i7 @ 2.5 GHz Quad-Core 64bit supported processor with a hard drive of 512GB storage space with a LAN port.
  + High-speed internet connection to download the required software framework, and to access research materials need for achieving the result of the research work.
* Software Requirements
  + A Linux OS Virtual Machine (Ubuntu, Kali preferred) residing as a guest on the host machine started above.
  + Windows OS Virtual Machine
  + Open-Source Tools such as Wireshark, Snort, Suricata, OSSIM, Wazuh, Ossec, NetworkMiner, Zeek, Nmap/Zenmap, Metasploit, LOIC, Yersinia, etc.
  + Python
  + Python IDE (PyCharm community version)
* Academic Digital Materials
  + Related research conference papers and journals, and textbooks access online through IEEE, ACM Digital Library, Google Scholar.

### References

Akinrolabu, O., Agrafiotis, I. & Erola, A. (2018). The challenge of detecting sophisticated attacks: Insights from SOC analysts. In: *ACM International Conference Proceeding Series*. 27 August 2018, Association for Computing Machinery.

Alahmadi, B.A., Axon, L. & Martinovic, I. (2022). *99% False Positives: A Qualitative Study of SOC Analysts’ Perspectives on Security Alarms*. [Online]. Boston: USENIX Association. Available from: <https://www.usenix.org/conference/usenixsecurity22/presentation/alahmadi>.

Al-Dhaqm, A., Razak, S.A., Siddique, K., Ikuesan, R.A. & Kebande, V.R. (2020). Towards the Development of an Integrated Incident Response Model for Database Forensic Investigation Field. *IEEE Access*. 8. p.pp. 145018–145032.

Dietz, M., Vielberth, M. & Pernul, G. (2020). Integrating digital twin security simulations in the security operations center. In: *ACM International Conference Proceeding Series*. 25 August 2020, Association for Computing Machinery.

González-Granadillo, G., González-Zarzosa, S. & Diaz, R. (2021). Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. *Sensors*. 21 (14).

Institute of Electrical and Electronics Engineers, Institute of Electrical and Electronics Engineers. Morocco Section, IEEE Communications Society & Institute of Electrical and Electronics Engineers. Region 8 (2017). *The 2017 International Symposium on Networks, Computers and Communications (ISNCC 2017) : May 16-18, 2017, Marrakech, Morocco*.

Islam, C., Babar, M.A. & Nepal, S. (2019). A multi-vocal review of security orchestration. *ACM Computing Surveys*. 52 (2).

Janos, F.D. & Dai, N.H.P. (2018). Security concerns towards security operations centers. In: *SACI 2018 - IEEE 12th International Symposium on Applied Computational Intelligence and Informatics, Proceedings*. 20 August 2018, Institute of Electrical and Electronics Engineers Inc., pp. 273–278.

Onwubiko, C. & Ouazzane, K. (2019). *Challenges towards Building an effective Cyber Security Operations Centre*.

Rosso, M., Campobasso, M., Gankhuyag, G. & Allodi, L. (2022). SAIBERSOC: A Methodology and Tool for Experimenting with Security Operation Centers. In: *Digital Threats: Research and Practice*. 1 June 2022, Association for Computing Machinery.

Soliman, M. & Azer, M.A. (2018). *Web Application API Blind Denial of Service Attacks; Web Application API Blind Denial of Service Attacks*.

Sousa, V. (2019). *A Review on Cyber Attacks and Its Preventive Measures*.

Syed, N.F., Baig, Z., Ibrahim, A. & Valli, C. (2020). Denial of service attack detection through machine learning for the IoT. *Journal of Information and Telecommunication*. 4 (4). p.pp. 482–503.

Vaarandi, R. & Mases, S. (2022). How to Build a SOC on a Budget. In: *Proceedings of the 2022 IEEE International Conference on Cyber Security and Resilience, CSR 2022*. 2022, Institute of Electrical and Electronics Engineers Inc., pp. 171–177.

Vielberth, M., Bohm, F., Fichtinger, I. & Pernul, G. (2020). Security Operations Center: A Systematic Study and Open Challenges. *IEEE Access*.