Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 04 Issue: 5 | May-2026
ISSN (O) 3107-6696

Web-Based SOC Ticketing System for Improving Incident Management in Security Operations Centre

Asif Iqbal Hajamydeen[1], Muhamad Kamarul Lukman Kamarudin[2], Muhammad Irsyad Abdullah[3], Md Gapar Md Johar[4]

[1,2] *Artificial Intelligence and Cyber Security Centre, Management and Science University, Malaysia*
[3,4] *Software Engineering and Digital Innovation Centre, Management and Science University, Malaysia*

Abstract - Security Operations Centres (SOCs) are responsible for managing and responding to cybersecurity incidents in increasingly complex threat environments. However, many SOCs still rely on manual or fragmented methods to track incidents, which can result in inefficiencies and delayed response times. To address this issue, this paper presents the design and implementation of a web-based SOC ticketing system aimed at improving incident management processes. The proposed system provides centralized incident tracking, ticket prioritization, status monitoring, and role-based access through a web interface. The system was developed using a system-based research approach and evaluated through functional and scenario-based testing. The results indicate that the proposed system improves incident organization, enhances visibility of incident status, and supports more efficient SOC workflows. This study demonstrates the practicality of lightweight web-based ticketing solutions in strengthening SOC incident management.

Key Words: Security Operations Centre (SOC), Incident Management, Ticketing System, Web-Based System, Cybersecurity, Incident Response, Workflow Automation

1. INTRODUCTION

Security Operations centres (SOCs) serves a critical role in monitoring, detecting, and responding to cybersecurity incidents in present establishments. As cyber threats increase in scale and complexity, SOC teams are needed to process an increasing number of security alerts while maintaining timely and effective incident response. The ability to manage security incidents efficiently has therefore become a critical factor in maintaining an organization's overall cybersecurity posture [1][5].

Despite the importance of SOC operations, many organizations continue to face challenges in managing security incidents effectively. Incident tracking is often performed using manual or semi-structured methods such as spreadsheets, emails, or generic task management tools. These approaches can lead to fragmented incident records, inconsistent documentation, limited visibility of incident status, and delays in response actions [2]. Such limitations reduce the effectiveness of SOC workflows and complicate post-incident analysis. The increasing volume of security alerts further amplifies these challenges. SOC analysts must prioritize incidents based on severity, assign tasks to appropriate personnel, and coordinate response activities under time constraints. Without a centralized incident management platform, SOC teams may experience alert fatigue, inefficient collaboration, and reduced situational awareness, ultimately impacting incident response efficiency [1][8].

Ticketing systems have been widely adopted in IT service management to support structured handling of incidents and service requests. These systems provide centralized tracking, workflow automation, task assignment, and status monitoring throughout the incident lifecycle [3][4]. In the context of SOC operations, a ticketing system can serve as a central repository for security incidents, enabling improved coordination, accountability, and visibility across response teams. However, many existing ticketing solutions are designed for general IT support and may not fully address the specific operational requirements of SOC environments [6].

To address these challenges, this paper presents the design and implementation of a web-based SOC ticketing system aimed at improving incident management in Security Operations centres. The proposed system delivers an organised roadmap for incident reporting, prioritization, assignment, and resolution through a consolidated web interface. By uniting incident information and regulating response processes, the system requests to enhance operational effectiveness and support active SOC incident handling.

The primary contribution of this study is the development of a practical and lightweight SOC ticketing solution based on real-world operational needs. The system is evaluated using functional testing and scenario-based analysis to assess its effectiveness in supporting SOC incident management tasks. This work demonstrates how a web-based ticketing system can improve incident organization and coordination without introducing excessive complexity.

2. Literature Review

This section reviews existing literature related to Security Operations Centre (SOC) operations, cybersecurity incident management, and the application of ticketing systems to support structured incident handling. The review focuses on identifying challenges faced by SOC teams in managing incidents and examines how ticketing systems and web-based

platforms can improve operational efficiency, visibility, and collaboration.

A. Security Operations Centre and Incident Management

Security Operations Centres (SOCs) are used to monitor, detect, analyse and respond to cybersecurity incidents, regardless of the environment. With the increase of cyber-attacks and their complexity, SOC teams are inundated with security alerts and need to respond to them quickly and accurately. The SANS Institute reports that many SOCs have alert overload, insufficient staffing and sub-optimal incident workflows that impact their response effectiveness and analyst performance [1]. Incident management is an important component of SOC operations, and defines how incidents are documented, prioritized, assigned and resolved. Robinson notes that many organizations do not have a unified incident response process, which leads to a disjointed approach to incident response and varying results of the response [2]. Without formal incident tracking, it can be challenging for SOC teams to coordinate incident response activities, monitor the progress of incidents, and perform post incident analysis.

Some studies have pointed out the advantages of centralized incident management – including a single source for incident information and response activities – for improving the effectiveness of the SOC. SOC response strategies are effective when there are clear workflows, prioritisation and documentation in decision-making and accountability [8]. Without a centralised system, SOC analysts may rely on informal communication channels which can result in a loss of situational awareness, or miscommunication, during a critical incident. Moreover, new challenges to the SOC operations have arisen with the growing trend of remote and distance working. Distributed SOC teams need tools that provide collaboration and instant access to incident information, regardless of location. Local systems or manual processes based traditional incident management solutions cannot cover these developing operational needs [1].

B. Ticketing Systems in Incident Management

Incident and service management ticketing systems are very popular in IT Service Management for incident and service management, and other operational processes have been performed systematically. They are used as a central system to capture issues, ownership, progress and action taken to resolve them. “Today’s ticketing systems can streamline operations by automating repetitive tasks, optimising workflows and providing real-time information on the status of the incidents [3],” says Atomicwork. Freshworks states that ticketing systems play a crucial role in managing the entire ticketing lifecycle, from creation to resolution [4]. Ticketing systems allow to capture all incident information in one place and avoid relying on multiple communication channels like email and messaging apps. This centralized approach will improve collaboration, accountability and traceability, especially in time-critical environments like SOCs.

While many of the benefits of traditional IT ticketing systems are true, they won't always fit into SOC operations. These systems are useful for general incident tracking but may not contain incident handling-specific features such as, but not limited to, severity-based prioritisation, quick escalation, and/or analyst workload management [2][6]. This may lead to SOC teams tailoring generic ticketing systems in ways that may not be directly applicable to security workflows, resulting in less effectiveness.

Recent literature indicates that the best ticketing solutions for a SOC should be flexible, easy to use and should fit into the incident response processes. A ticketing system with workflow customisation, access control based on user roles and detailed information on incidents will better fulfil the specific requirements of SOCs [3]. These capabilities enable SOC teams to respond to complex incidents more effectively, and ensure consistency in incident response practices.

C. Web-Based Systems for SOC Operations

As they are easily accessible, easily scalable, and easily integrated, web-based systems are gaining in popularity. Web-based platforms in SOCs enable easy access to incident data and facilitate collaboration among analysts from various locations. Kamal et al. showed that Web-based security tools can be used to increase operational visibility and better decision making by using centralized dashboards and real-time access to security data [7]. Another benefit of web-based incident management is the ability to support ongoing SOC operations because information on incidents is available to analysts from various devices and without the need for local infrastructure. This is particularly beneficial for companies that have 24-hour SOCs and/or a distributed security team [1]. Also, a web-based platform allows for easy operation and maintenance of the system, reducing the burden of traditional on-premises hardware and software.

In addition, the literature on SOC tooling highlights the importance of systems that are lightweight and modular, with a focus on the essential operational needs. Organisations may benefit from using web-based platforms that provide essential incident management capabilities and can be flexible as needs change over time, rather than more complex and resource intensive platforms [6]. Both types of systems can be integrated into the current SOC tools and processes without a major modification.

D. Challenges and Gaps in Existing Solutions

Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 04 Issue: 5 | May-2026
ISSN (O) 3107-6696

The literature search results show that SOCs are still struggling with the increasing number and complexity of cyber security issues. Ticketing systems provide a streamlined workflow and also centralise incident tracking. Web-based systems improve ease of access and also collaboration. Despite this, many solutions available today do not fully meet the needs of SOCs and have problems with poor incident prioritisation, workflow integration and usability.

The findings suggest that a web-based SOC ticketing solution is desirable but it needs to be able to provide the structure for incident management and address the issues of today's SOC environments. This research is an extension of previous research because this research created and implemented a practical solution for SOC incident management needs in a real-world environment that is a ticketing solution.

E. Summary of Literature Findings

The literature reviewed indicates that the challenge SOCs are facing concerning the volume and complexity of cybersecurity incidents is a persistent challenge. Ticketing systems offer workflows and centralised incident tracking. Web-based systems increase accessibility and collaboration. Many solutions are not fully compliant with the needs of SOCs, which results in a lack of optimisation in incident prioritisation, workflow alignment and usability. The results indicate the necessity of a dedicated web-based SOC ticketing system that allows for structured incident handling and complements the challenges faced in existing SOCs. The current project is a continuation of the ongoing research, which involves designing and implementing a practical SOC ticketing solution meeting the requirements of the real incident management.

3. System Methodology

In this research a system-based development methodology is applied to design and implement a web-based SOC ticketing system to improve the SOC incident management process. The methodology focuses on understanding the requirements for SOC operations, drawing out a structured system architecture, implementing a core ticketing system and assessing the system through functional testing and scenario testing. This is aligned with operational cybersecurity support systems development guidelines with pragmatic approach [1][3].

A. Requirement Analysis

The requirement analysis phase focused on gaining insights into what are the main challenges faced by the SOC teams in processing cybersecurity incidents. A number of important requirements were identified from the literature as well as from the experience gained. These are the centralized incident tracking, structured ticket workflow and severity-based prioritization and role-based access control requirements for different SOC roles such as analysts, managers etc. [1][2].

This role relationship with the functions of the system is illustrated in Fig. 1. The use case diagram has some user cases shown representing the interaction between different users and the system, such as creating tickets, escalation, resolution submission, verification and reporting. SOC analysts are responsible for creating and monitoring tickets and managers are responsible for monitoring ticket assignment and approval. The engineers and the programmers resolve issues and submit evidence, while the executives are responsible for checking on the reports and trends of the system. This is a clear resolution for the responsibilities of each of the roles involved in the incident management process in this structured model of interaction. The idea of the proposed system is to alleviate some of the frequent issues faced in SOC operations, such as miscommunication, lack of accountability, and inefficiency.

The literature highlights that the poor performance in incident management is related to the lack of integration of tools used, and inconsistent documentation [2]. The proposed system was thus designed to integrate the information about the incident into a single platform which gives real-time view of the status of the incident. Moreover, the current ticketing solutions should be able to be automated and standardized to minimize manual processes and enhance responsiveness [3][4].

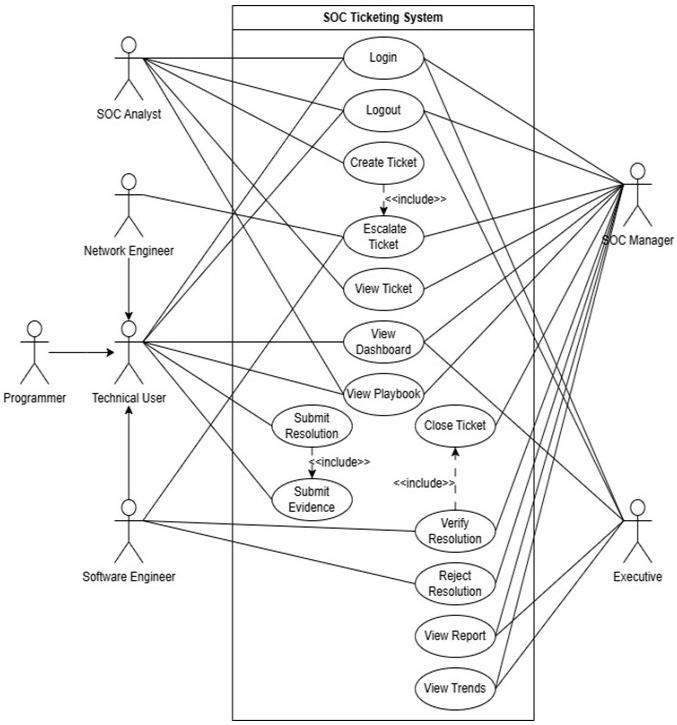

Fig. 1. Use case diagram of the SOC Ticketing System

B. System Design Approach

The system design phase included organizing the requirements into a system design. The proposed SOC ticketing system is a web-based system to ensure it is accessible, scalable, and easily deployable. Systems that allow web-based access to a centralized repository of incident data

Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 04 Issue: 5 | May-2026
ISSN (O) 3107-6696

and allow collaboration among analysts can support distributed SOC operations [7]. The overall architecture of the system is shown in Fig. 2. The diagram shows a relationship between the user roles, the ticketing core, and various other modules like playbook management, evidence management, and reporting. The ticketing core is the backbone and are used for various aspects like creating tickets, setting ticket severity and tracking ticket status etc. The life cycle of incidents in this system is clearly defined with ticket creation, ticket prioritisation, assignment, status change, incident resolution submission, verification and incident closure. The lifecycle ensures that incidents will be handled in a consistent and systematic way in the entire incident response process.

The architecture includes supporting elements such as playbooks and evidence management. Playbooks are a uniform approach to addressing specific incidents. Evidence modules for upload and preservation of evidence in the course of investigation. Reporting and analytics feature also enhance the system's functionality and provide valuable insights on trends and performance metrics on incidents.

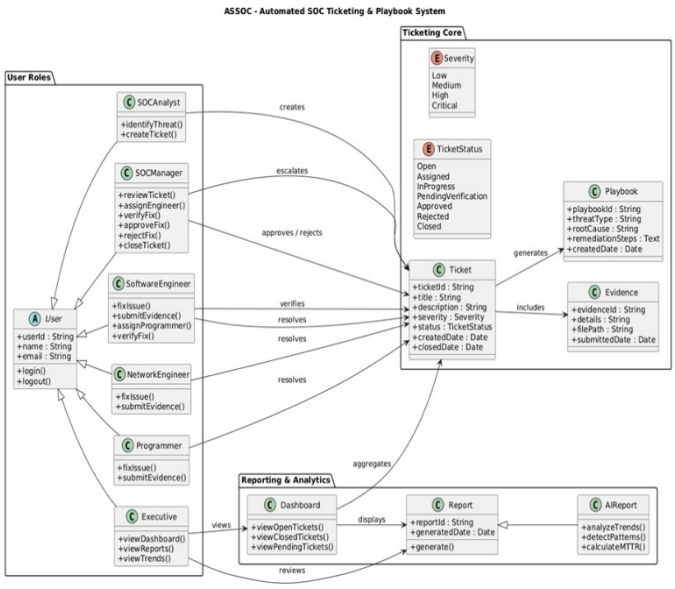

Fig. 2. Overall architecture of the SOC Ticketing System

RBAC is employed to make sure that only the users that have the proper access rights can make use of the functionalities applicable to his/her position. This increases the security of the system but does not impact on the efficiency. The system design follows good practice in incident management and is structured, modular and scalable to manage cyber security incidents.

C. System Implementation Environment

The proposed SOC ticketing system has been built using a web-based technology stack for easy and secure deployment. The system backend is coded in Python and based on Django web framework, which is fast and secure. The incident records, user information and system logs were kept on the relational database management system. It was deployed to a Linux based server environment to provide stability and compatibility with the commonly used SOC infrastructure. The application was deployed with web server and application server environment which can handle multiple concurrent users and handle requests reliably. The deployment follows best practices for hosting web-based security management systems and allows for ongoing SOC operations [3][7].

D. System Development

The system development stage included the deployment of the architecture and functions created. SOC Ticketing System Main functions of the SOC ticketing system includes: Incident reporting, Incident categorization, Priority assignment to the incidents, Assignment of incidents to the SOC analysts, Tracking the incidents and Documenting the incident resolution. These are typical functionalities in most modern ticketing systems for the structured handling of incidents [4].

During the development process, simplicity and usability were key points so that SOC analysts can interact with the system efficiently in the event of a crisis. Previous research has shown that system complexity can negatively impact the analyst's performance and the system's adoption [1][3]. The system was therefore designed with an interface that minimises cognitive load and facilitates routine incident management.

E. System Testing and Evaluation Method

The proposed system was evaluated with functional testing and scenario-based analysis. Functional testing was conducted to ensure that all features of the systems work as expected, such as creating tickets, assigning them, prioritising, and updating their status. This way, the system will fulfil the requirements and help with the necessary SOC workflows.

Common SOC incident handling scenarios were simulated using scenario-based testing, including high severity incident reporting, assignment of an incident to an analyst and incident resolution. In system studies related to SOC, scenario-based evaluation is a common method for evaluating the usability and effectiveness of a system's workflows in practice [6][7]. These evaluations were then analysed to measure the system's effectiveness in enhancing the organization, visibility and coordination of incidents in SOC operations.

4. Results and Discussion

The proposed web-based SOC ticketing system was evaluated using functional testing and scenario-based analysis to assess its effectiveness in improving incident management within a Security Operations Centre (SOC). The evaluation focuses on system functionality, workflow efficiency, usability, and overall operational improvement.

A. Functional Testing Results

All the important functions of the system were verified for functionality to ensure correct operation. The

Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 04 Issue: 5 | May-2026
ISSN (O) 3107-6696

following are the main functions examined: The system's dashboard (Fig. 3 and Fig. 4), ticket creation and severity classification (Fig. 5), tracking of ticket status (Fig. 5), ticket assignment (Fig. 6), submission of ticket resolutions (Fig. 7 and Fig. 8), and ticket closing.

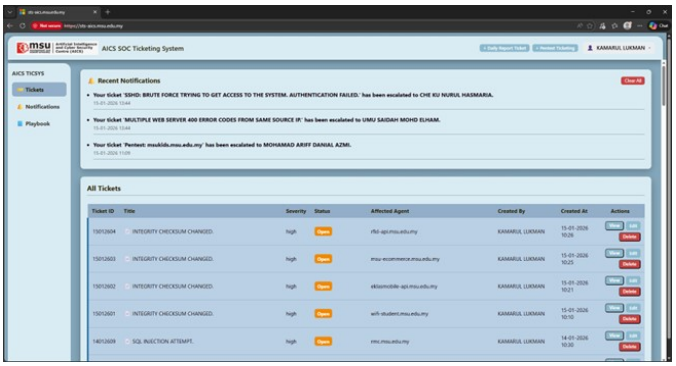

Fig. 3. SOC Analyst, SOC Manager, Engineers and Programmers' Dashboard

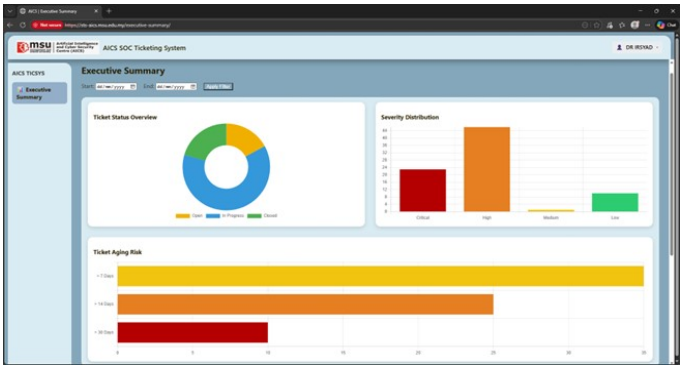

Fig. 4. Executives' Dashboard

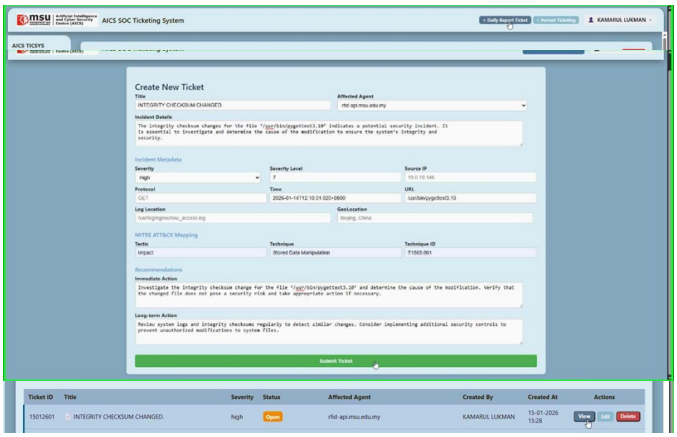

Fig. 5. Ticket Creation

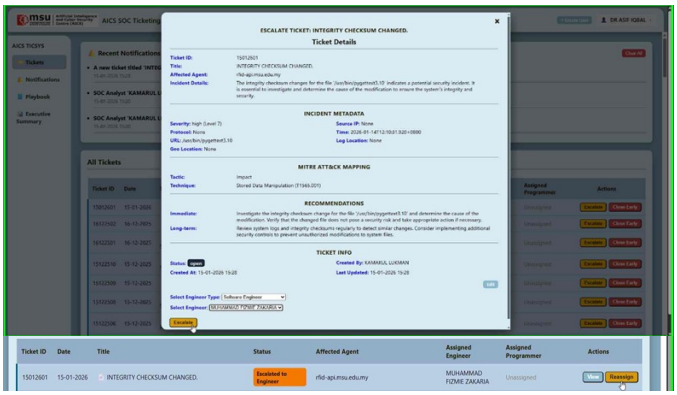

Fig. 6. Ticket Assignment

Fig. 7. Resolution Submission

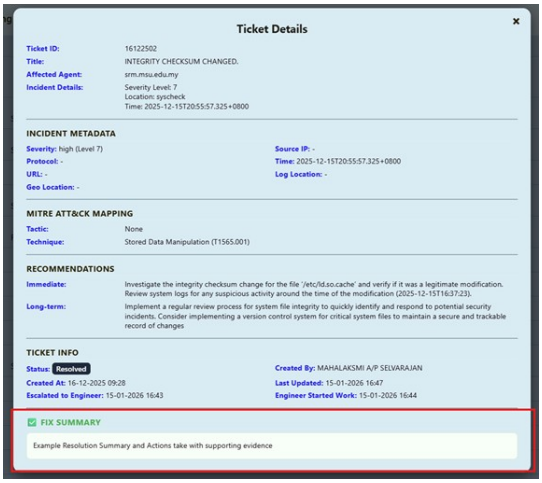

Fig. 8. Submitted Resolution

The results indicate that all the main features worked as expected with no major system failures. SOC analysts could develop and classify tickets according to severity levels including low, medium, high and critical. Managers could assign the tickets to the appropriate engineers and engineers could update the ticket status and provide the resolution. The system also facilitated evidence submission and verification processes, allowing for comprehensive documentation of all incident handling activities. Overall, the functional testing validates the system to achieve structured incident management requirements.

B. Scenario-Based Evaluation

To test the usefulness of the incident handling in practice, some incident handling scenarios were simulated

Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 04 Issue: 5 | May-2026
ISSN (O) 3107-6696

according to the typical incident handling in SOC. Such situations involve high severity incidents, regular alerts and escalated cases that require multiple level verification.

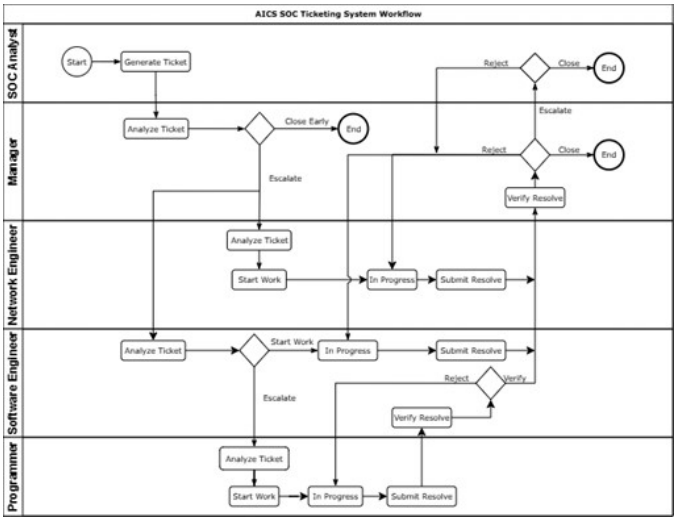

Fig. 9. Activity diagram of the SOC Ticketing System

In another high severity incident, a ticket was opened and escalated to the SOC manager's attention in a timely fashion. A relevant engineer was assigned to the task and investigated and submitted a resolution. This resolution was verified and approved/rejected prior to final closure.

The process illustrated in Fig. 9 outlines the process of incidents passing through various stages, such as creation, analysis, escalation, resolution, and verification. The system allowed for seamless communication among SOC analysts, managers, and engineers, minimising delays and enhancing task clarity. The system offers a more streamlined and clear process, unlike manual techniques like email or spreadsheets, where all parties can monitor the progress of incidents in real-time.

C. System Usability and Performance

During testing the system was observed to be user-friendly and efficient. The web-based interface provides distributed SOC operations by enabling users to access the system from various locations without the need for extra configuration. For usability it is simple and easy to understand interface making it easy to create tickets, update tickets, and view dashboards without a lot of training. This is particularly important in SOC environments where the analysts must respond quickly and, in a time, constrained scenario.

It's best used on the department network with fast and reliable response times to get the best performance out of the system. But, on the University network or public networks, a significant decrease in performance was noticed such as delays in page loading and ticket updates. Such a difference in performance is probably due to network latency, bandwidth constraints and server access. These delays exist and the system goes on working but in some applications where time is critical, the delays may affect the user experience.

D. Operational Improvements

The SOC ticketing system brought about a number of enhancements in the incident management processes. First of all, the system offers a centralized incident tracking, that means no need for spreadsheets or emails. This is useful in ensuring that all the data associated with an incident are kept in a single platform. Secondly, it raises the awareness of incident status. The progress of each ticket, along with who is working on it and what actions are done are easily visible to the user. Thirdly, the structured workflow improves the coordination of various roles in the SOC. There are less confusion and accountability, assignments and verification are clear. Finally, the system can be utilized to record incidents more effectively which may be beneficial for reporting, auditing and future analysis. The above improvements illustrate the effectiveness of the proposed system in improving the SOC operations.

E. Limitations of the System

Furthermore, the evaluation of the system was carried out under controlled conditions and limited number of users. Therefore, the performance of the system in large scale SOC operation and high number of alerts has not been fully tested. The system holds promise for a lightweight and practical solution for enhancing SOC workflows, despite these limitations. It lays the foundation for future development, integration, automation, and scalability.

5. CONCLUSIONS

This paper proposed and implemented a web-based SOC ticketing system design, which improves the incident management process for SOCs. The study addressed some of the following challenges: teams lack suitable coordination, lack of visibility and the SOC operations were fragmented with regard to incident tracking. The proposed system will include a centralized platform that will have structured workflows, severity-based ticket prioritization, role-based access control, and a real-time tracking system for ticket status. The functional test result and scenario-based analysis result indicate that the system is effective in enhancing the organization of incidents, increasing visibility and providing better coordination between the SOC analysts, managers and engineers. The system works well in a controlled environment, but there are a few issues that were mentioned, including the fact that it relies on the network for performance and that it doesn't have all the bells and whistles, including automation and intelligent prioritisation. These restrictions identify things that could be improved in the future. In conclusion, the proposed SOC ticketing system is a feasible and simple solution to improve incident management procedures. Future research could include using SIEM capabilities, integrating AI-driven recommendations and enhancing system scalability for larger SOCs.

REFERENCES

[1] SANS Institute, “SOC Survey and Best Practices,” 2020.
[2] Robinson, T., “IT Incident Management: Future Trends,” *GRC Viewpoint*, 2022.

[3] Atomicwork, "IT Ticketing System: Key Capabilities, Benefits and Top Solutions," 2024.
[4] Freshworks, "What is an IT Ticketing System?" https://www.freshworks.com/ticketing-system/it/
[5] IBM Security, *Cost of a Data Breach Report*, 2022.
[6] Hajamydeen, A. I., Hasni, M. D., & Abdullah, M. I. (2024). Integrating Wazuh for Efficient Real-Time Threat Monitoring and Vulnerability Assessment in a SOC Environment. In *Utilizing Renewable Energy, Technology, and Education for Industry 5.0* (pp. 292-320). IGI Global Scientific Publishing.
[7] Kamal, A., Hajamydeen, A. I., & Jaharadak, A. A., "Log Necropsy: Web-Based Log Analysis Tool," IEEE ICSPC, 2022.
[8] Abdullah, M. I., Abas, A. I., & Hajamydeen, A. I., "Effective SOC Response Strategies Using MITRE ATT&CK," *Journal of Emerging Technologies and Industrial Applications*, 2024.