World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Incident response: A structured model from detection to containment and recovery

Courage Ojo [1,*], Emmanuel Ayodeji Osoko [2], Joy Nnenna Okolo [3] and Mamudat Jaji [4]

[1] *Department of Computing; East Tennessee State University; United States.*
[2] *Department of Electrical Engineering and Computer Science; Ohio University; Ohio; United States.*
[3] *Department of Computer Science; South Dakota State University; Brookings; United States.*
[4] *Department of Nursing; George Washington University; Washington DC; United States.*

World Journal of Advanced Research and Reviews; 2024, 24(01), 1401–1407

Publication history: Received on 04 September 2024; revised on 13 October 2024; accepted on 15 October 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.24.1.3148

Abstract

As cyber-attacks evolve in sophistication; organizations are under constant threat. This necessitates a cohesive approach to prioritize incident response (IR) capabilities and mitigate potential damages. This research paper explores integrating Information Security Management (ISM) and Incident Response (IR) functions; underlining the need for a unified strategy that leverages organizational learning theory. The study comprehensively analyzes the Incident Response Lifecycle; outlining the critical phases of preparation; detection and analysis; containment; eradication; recovery; and post-incident activities. It also investigates the crucial role and structure of Incident Response Teams (IRTs); advocating for tailored team formations that adapt to the dynamic nature of cyber incidents. By fostering collaboration between ISM and IR functions and focusing on technical and socio-technical factors; organizations can enhance their resilience against cyber threats and improve their overall security posture.

Keywords: Incident response; Detection and response; Security; Frameworks

1. Introduction

Organizations today face a constant barrage of digital threats from various malicious actors. The potential damage from these threats can be far-reaching, affecting the organization's data, reputation, and operational continuity. As a result, large organizations typically allocate resources to a dedicated **information security management** (ISM) function tasked with safeguarding their digital assets. The ISM team is responsible for conducting thorough risk assessments, crafting comprehensive strategies, and offering clear policies and training to guide employees and management. This function also implements technological measures such as firewalls, antivirus software, and encryption tools to prevent unauthorized access to sensitive information [1].

Despite these precautions, organizations must accept that no defense is perfect. Security breaches can and do happen often. Many organizations introduced a dedicated **incident response** (IR) function to address such inevitable incidents. The IR team is designed to mitigate the damage caused by cyber-attacks, enabling the organization to recover quickly and restore digital services. However, an expected shortfall is that many organizations need to integrate their ISM and IR functions fully. When these functions operate in silos, organizations miss opportunities to enhance their overall security posture.

This paper proposes a conceptual framework that utilizes organizational learning theory to explain how the ISM and IR functions can be more effectively integrated. Organizations can create a continuous learning loop that enhances their security capabilities by fostering strong collaboration between these teams. This integration helps respond to security incidents more efficiently and positions organizations to proactively address emerging threats and attacks. A well-

* Corresponding author: Courage Ojo; https://orcid.org/0009-0007-5092-6994

coordinated ISM and IR relationship generates numerous benefits, including improved awareness of potential security risks, better compilation and analysis of threat intelligence, elimination of vulnerabilities in existing defenses, critical evaluation of security protocols, and a strengthened ability to respond to future incidents [2].

Cybersecurity incident response teams (CSIRTs) play a crucial role in protecting the digital assets of both individuals and organizations across the globe. However, CSIRTs are relatively new compared to other organizational teams, and there is still much to learn about maximizing their effectiveness. While significant research has been conducted on traditional team dynamics, CSIRTs have yet to benefit from this body of knowledge fully. To improve the performance and development of CSIRTs, researchers suggest that attention should be given to specific areas such as team adaptation, communication strategies, problem-solving abilities, building trust among team members, and cultivating shared knowledge. These elements are essential for enhancing the effectiveness of CSIRTs and ensuring they function optimally as a cohesive unit [3].

In the cybersecurity incident response exercise guidance paper, Wlosinski provided a framework for implementing incident response based on an organization's strategic objectives and sizes. The paper identified attack vectors and their identification mechanisms, incident response scenarios, and the data needed to execute such responses [4].

O'Neil, Ahmad, and Maynard created a scenario-based approach for training CSIRT teams to overcome technical barriers to incident response [5]. The paper identified the socio-technical issues facing organizations' incident response procedures and classified them according to information technology systems' people, processes, and technology framework. After that, a framework for training incident responders incorporating practical approaches was created and tested.

2. Material and methods

This section explores the methodologies for implementing a structured incident response lifecycle equipped with incident response capabilities. Our approach incorporates the key phases identified by the National Institute of Standards and Technology (NIST): Preparation, Detection and analysis, Containment, Eradication and recovery, and Post-Incident Activity. Each phase is analyzed to determine the necessary actions, tools, and resources organizations must implement to manage cybersecurity incidents effectively. Our proposed methodology emphasizes proactive measures during the preparation phase to ensure readiness for potential threats, advanced detection techniques to identify incidents promptly, strategies for effective containment and eradication of threats, and the importance of conducting thorough post-incident reviews to enhance future incident response efforts.

The following subsections provide insights into each phase, highlighting the activities and considerations necessary to establish an effective incident response capability.

2.1. Incident response lifecycle

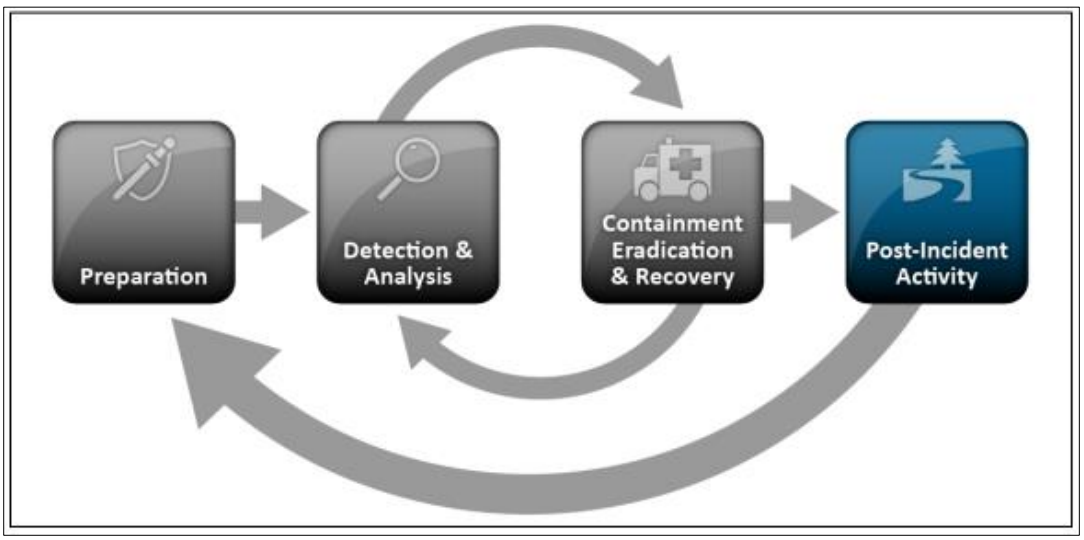

Figure 1 Incident Response Life Cycle [6]

The Incident Response Lifecycle refers to an organization's structured response process for cybersecurity incidents. This lifecycle is essential for minimizing a cyber-attack's impact and restoring normal operations as quickly as possible in organizations. By following a systematic approach, organizations can address immediate threats and enhance their ability to prevent future incidents and cyber-attacks. The National Institute of Standards and Technology (NIST) breaks the cyber incident response lifecycle into four main stages: Preparation, Detection & analysis, Containment, eradication, & recovery, and Post-incident activity [6]. Figure 1 below shows the lifecycle of an incident response:

- **Preparation**: In the preparation phase, the possible incidents are evaluated and assessed to determine the potential impact and the steps that can be taken to reduce damage. With proper preparation, an organization could avoid severe financial losses, compliance issues, and long-term damage to its reputation. In this first stage, the incident response team focuses on preventing incidents. They work to protect the organization by executing asset inventory and ranking, risk assessments, security monitoring, vulnerability assessments, monitoring, planning, and training, among other tasks [7]. This phase results in a clear incident response plan to identify, prioritize, and address security incidents.
- **Detection & analysis:** Here, teams identify, investigate, and assess suspicious activity or incidents within an organization's network or systems. This process ensures that potential security breaches are quickly addressed to minimize impact. It is important to note that a cyber attack or threat has occurred, and the response procedures have begun here. The goal of detection is to identify security incidents or malicious activities, such as unauthorized access, malware, data exfiltration, etc., using methods such as Log Monitoring, Anomaly Detection, and Alerting Systems [8]. These methods make it easier to spot cyber attacks before they escalate.
- **Containment, eradication & recovery:** Containment comes after identifying an event and concluding that action is required to limit its impact. This involves gathering information on the event's characteristics, determining the population of affected assets, and then quarantining those systems until the situation is resolved and business is back to normal [9]. Containment isolates the affected systems and prevents the incident from propagating further. Quickly implementing containment actions allows organizations to minimize incident-caused damage and limit the potential for further harm. Thompson highlights that eradication removes all the remnants of a cyberattack [10]. The eradication phase focuses on eliminating malicious artifacts. This step is vital in restoring accounts, systems, and technologies to a known, safe, and secure state, removing any traces of the threat. It is also essential to note that, for some incidents, eradication is either unnecessary or performed during recovery. Finally, during the recovery phase, administrators work to restore systems to regular operation, ensuring they are functioning correctly and addressing any vulnerabilities to prevent future incidents. Recovery efforts may include restoring systems from clean backups, rebuilding compromised systems, replacing infected files with clean versions, applying patches, updating passwords, and enhancing network security measures like firewall rules and router access control lists.
- **Post-incident activity**: The goal of this phase, also known as a postmortem, is to understand precisely what occurred, why it happened, and how to prevent it from happening again. This review goes beyond technical aspects; it may also involve changes to policies or infrastructure. The purpose of this phase is not to assign blame (though this can sometimes occur) but rather to reduce the likelihood or impact of future incidents. Additionally, heightened system logging and network monitoring are often implemented during this stage. It's common for attackers to target the same system again or use similar methods to compromise other resources within the organization. Another goal is to **scope the damage;** a comprehensive review helps assess the entire response process, minimizing the impact and ensuring more effective recovery. Finally, post-incident activities are to **make improvements**. These reviews aim to strengthen cybersecurity defenses, close gaps, and ultimately mature the organization's security posture to handle future incidents better [11].

We formulate a model for forming an incident response team based on the IR lifecycle. We collected data from 10 Security Operation Centers across different industries. Operators and managers of these SOCs were asked the following questions:

- What industry does your SOC and incident response team serve?
- What is the conceptual framework on which your incident response team is built? (Roles, team size)
- What are the specific threats facing your industry?
- How often does your team conduct tabletop and training exercises?
- What metrics are used by the IR team to measure success?
- What challenges are faced when interfacing between technical and non-technical teams during IR activities?
- Is your IR tooling sufficient to execute the incident response?

3. Results and discussion

This study's findings on incident response teams (IRTs) and their roles in managing cybersecurity incidents are discussed here. Details include the composition of IRTs, their formation and structure, and the implications of these findings for enhancing organizational resilience against cyber threats.

3.1. Incident response teams (IRT)

An IRT is a dedicated group of professionals from various business groups within an organization responsible for identifying, handling, containing, eradicating, and recovering from IT incidents. These personnel are ready to respond to incidents as soon as they occur. The incident response team is also in charge of organizing post-event analysis and developing strategies to prevent the recurrence of the occurrence.

There are various types of Incident Response Teams (IRTs), Security Operations Centers (SOC), Computer Security Incident Response Teams (CSIRT), and Computer Emergency Response Teams (CERT). Each team has its specific focus and role in managing and responding to security incidents. For instance, **SOCs** primarily focus on monitoring and analyzing activity on networks and endpoints, aiming to detect and respond to threats in real time. **CSIRTs**, on the other hand, are more specialized in coordinating responses to security incidents across an organization, investigating the root cause, and ensuring long-term remediation. Lastly, **CERTs** often operate at a higher level, responding to large-scale or critical security incidents that affect multiple organizations or regions and may even provide guidance or frameworks for other teams to follow.

While each team's structure and responsibilities may differ, they all play crucial roles in protecting assets, minimizing damage, and restoring services immediately after an incident. Hence, these teams must be appropriately formed.

3.2. Formation and structure of an IRT

The model questions presented in section 2 were completed by 80 operators and managers across 10 SOCs. The findings from the questionnaire were as follows:

3.3. Industry-Specific Threats

The first question aimed to understand the industries each SOC serves and the specific threats they face. Across all sectors, the main threats identified were consistent, though some sector-specific variations were observed:

- **Finance and healthcare:** The most significant threats include ransomware, insider threats, and data exfiltration. These industries are heavily regulated, prioritizing compliance and data protection.
- **Retail:** Point-of-sale (POS) malware and phishing attacks targeting payment information were identified as critical threats, and ransomware was also a major concern.
- **Manufacturing:** The threat landscape includes operational technology (OT) attacks, industrial espionage, and supply chain vulnerabilities.
- **Technology:** Distributed Denial of Service (DDoS) attacks, Advanced Persistent Threats (APTs), and software supply chain attacks were prominent in this sector.

Despite industry differences, all SOCs reported a rise in ransomware and phishing attacks, underscoring the need for solid incident response across various sectors.

3.4. Team structure and composition

The size and structure of IR teams varied widely, depending on organizational size, industry, and resources. Most SOCs reported the following typical roles within their IR teams:

- **Incident handlers** – Responsible for coordinating and executing incident response procedures.
- **Forensic analysts** – Tasked with investigating the root cause and impact of incidents.
- **Threat hunters** – Actively searching for threats within the organization's environment.
- **Security engineers** – Focused on implementing technological defenses to prevent future incidents.

Most SOCs had teams ranging from 5 to 15 members, with larger teams in industries like finance and healthcare, where regulations demand more extensive security capabilities. SOCs in smaller industries like retail and manufacturing had

leaner IR teams, often relying on automated tools to compensate for fewer personnel. However, most SOCs emphasized the importance of clear role definitions and cross-functional collaboration between IR teams, particularly when handling significant cyber incidents.

3.5. Training frequency

There was a notable difference in how often training and tabletop exercises were conducted:

- **Finance, healthcare, and technology SOCs**: These teams conducted quarterly training exercises, ensuring that their response teams were well-prepared for emerging threats. These organizations strongly emphasized scenario-based exercises, including technical and non-technical participants.
- **Retail and manufacturing SOCs**: These sectors performed annual or biannual training exercises, often tied to specific compliance requirements rather than a proactive strategy. Smaller SOCs also cited limited resources as a barrier to more frequent training.

Across all SOCs, scenario-based exercises improved the team's ability to respond to real-world incidents, particularly in sectors with complex regulatory environments.

3.6. Metrics for success

To evaluate the effectiveness of their incident response, SOCs used the following metrics:

- **Mean time to detect (MTTD)**: The time it takes for a SOC to identify an incident.
- **Mean time to respond (MTTR)**: The time is taken to contain, eradicate, and recover from an incident.
- **Number of incidents escalated**: SOCs measured the incidents that escalated to critical levels requiring executive-level intervention.
- **Post-incident reviews**: The completion and findings of post-incident reports were vital to improving future response efforts.

The finance and healthcare sectors reported the highest level of focus on reducing MTTD and MTTR due to the high financial and reputational risks posed by cyber incidents. The data from SOCs servicing the retail and manufacturing sectors tended more towards minimizing downtime and financial loss.

3.7. Collaboration between technical and non-technical teams

A common theme across all SOCs was the challenge of ensuring smooth communication between technical and non-technical teams. These challenges included:

- **Non-technical understanding of cybersecurity risks**: Non-technical staff, such as legal and communications teams, often needed more technical knowledge to fully comprehend the severity of incidents, leading to delays in decision-making.
- **Overlapping responsibilities**: In some cases, it was unclear which teams (e.g., legal vs. technical teams) were responsible for critical decisions, particularly when incidents involved regulatory violations.
- **Crisis communication**: Effective communication with external stakeholders (customers, media, regulators) often lagged due to the technical teams' focus on containment and eradication rather than communication.

Many SOCs mentioned that implementing cross-training programs for non-technical staff to understand the incident response and cybersecurity terminology could help bridge this gap.

3.8. Incident response tooling

The adequacy of IR tools varied, with larger organizations expressing confidence in their tooling while smaller organizations indicated a resource gap.

- **Finance and technology SOCs**: These SOCs reported that their IR tools (e.g., SIEMs, SOAR platforms, forensic analysis tools) were sufficient to handle most incidents. They had automated tools for monitoring, detection, and response.

- **Retail and manufacturing SOCs**: These sectors frequently mentioned that their IR tooling was insufficient, relying heavily on manual processes or outsourced services for significant incidents. This inadequate tooling sometimes delayed their response, especially when dealing with large-scale incidents like ransomware.

All SOCs stressed the importance of having updated, efficient tooling to keep up with the evolving threat landscape, with many noting plans to upgrade their systems.

The answers to our model questions show that while the design and operation of incident response teams vary across industries, common operations can be leveraged to provide a standardized approach to standing up incident response teams. Based on these results, we propose the following IR team structure:

- **Team Leader/Incident Commander**: This individual coordinates the response and makes decisions.
- **Core Response Team**: This team includes specialized roles like:
    - **Incident Responder/Analyst**: Gathers data, conducts the initial analysis, and provides situational awareness.
    - **Forensic Specialist**: Handles deep technical investigations, including digital forensics and evidence collection.
    - **Monitoring & Reporting**: Provides real-time updates and assessments throughout the incident to keep the team informed and adjust the strategy as needed.

- **Communication Lead**: Manages internal and external communications with other departments and stakeholders (e.g., media, legal).

Figure 2 below shows the structure of the incident response team and the flow of communications between the composite team members and stakeholders.

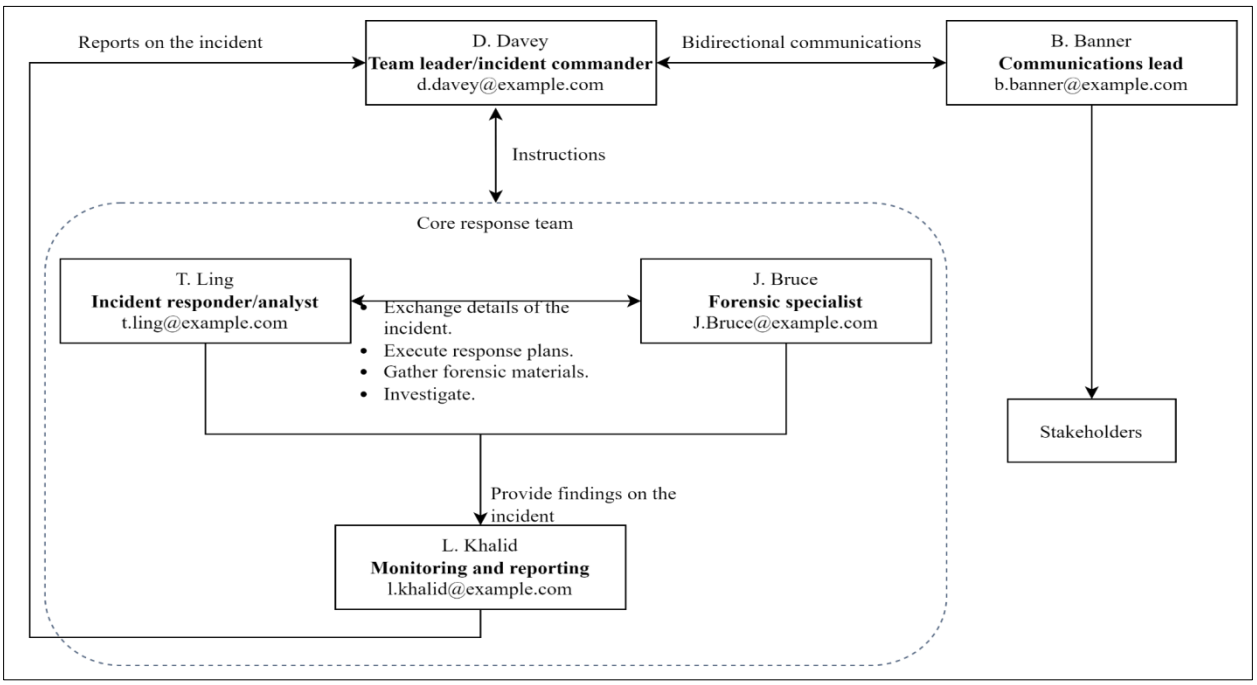

Figure 2 Model of an IR team and operational flow

4. Conclusion

Our model reflects the basic personnel composition for setting up an incident response team. It allows for flexibility in team composition while maintaining their basic essence, conforming to the dynamic nature of incident response work and ensuring that security incidents are appropriately contained and resolved. Our findings align with and expand upon existing ethnographic studies and industry standards, showing that incident team formation has undergone significant changes over time. Specifically, these teams' ad hoc structure represents a change from the more rigid team structures traditionally seen in comparable contexts.

Integrating information security management and incident response functions is vital for organizations striving to navigate the complex landscape of cybersecurity threats. This paper highlights the importance of a structured incident response lifecycle and the role of tailored incident response teams in effectively managing incidents. By adopting a proactive approach to preparation, employing advanced detection techniques, and fostering collaborative team dynamics, organizations can significantly enhance their ability to respond to cyber incidents. Furthermore, post-incident activities provide valuable insights that can continuously improve security practices. As cyber threats continue to evolve, organizations must prioritize the development of sophisticated tools and strategies that support agile and effective incident response, ensuring that they are well-equipped to safeguard their digital assets and maintain operational continuity.

Compliance with ethical standards

Disclosure of conflict of interest

There are no conflicts of interest.

References

[1] Schneier B. The Future of Incident Response. IEEE Security & Privacy. 2014; 12(5): 96-96. Available from: https://doi.org/10.1109/MSP.2014.102.

[2] Ahmad A, Desouza KC, Maynard SB, Naseer H, Baskerville RL. How integration of cyber security management and incident response enables organizational learning. Journal of the Association for Information Science and Technology. 2020; 71(8): 939-953. Available from: https://doi.org/10.1002/asi.24311.

[3] Steinke J, Bolunmez B, Fletcher L, Wang V, Tomassetti A, Repchick K. Improving Cybersecurity Incident Response Team Effectiveness Using Teams-Based Research. IEEE Security & Privacy. 2015; 13(4): 20-29. Available from: https://doi.org/10.1109/MSP.2015.71.

[4] Wlosinski LG. Cybersecurity Incident Response Exercise Guidance [Internet]. ISACA Journal. 2020; 4. Accessed 03 September 2024. Available from https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance.

[5] O'Neill A, Ahmad A, Maynard SB. Cybersecurity Incident Response in Organisations: A Meta-level Framework for Scenario-based Training. Proceedings of the Human Factors and Ergonomics Society Annual Meeting. 2021; Available from: https://doi.org/10.48550/arXiv.2108.04996

[6] Cichonski P, Millar T, Grance T, Scarfone K. Computer security incident handling guide (Special Publication 800-61, Revision 2). National Institute of Standards & Technology. 2012.

[7] Karlzen H, Sommestad T. Automatic incident response solutions: a review of proposed solutions' input and output. Proceedings of the 18th International Conference on Availability, Reliability and Security (ARES '23). Association for Computing Machinery, New York, NY, USA. 2023; 37: 1-9. Available from: https://doi.org/10.1145/3600160.3605066

[8] Jayabalan L, Ganapathi P. A Comprehensive Study on Classification of Passive Intrusion and Extrusion Detection System. Academy & Industry Research and Collaboration Center (AIRCC). 2013; 281-292. Available from: https://doi.org/10.5121/csit.2013.3529.

[9] Thompson EC. Containment. In: Apress eBooks [Internet]. 2018; 99–116. Available from: https://doi.org/10.1007/978-1-4842-3870-7_8

[10] Thompson EC. Eradication, recovery, and post-incident review. In: Apress eBooks [Internet]. 2018; 117–23. Available from: https://doi.org/10.1007/978-1-4842-3870-7_9

[11] Fritchen K. A K-12 guide to post-incident analysis | ManagedMethods [Internet]. ManagedMethods Cybersecurity, Safety & Compliance for K-12. 2024. Available from: https://managedmethods.com/blog/post-incident-analysis/

[12] Brown JM, Greenspan S, Biddle R. Incident response teams in IT operations centers: the T-TOCs model of team functionality. Cognition Technology & Work [Internet]. 2016; 18(4): 695–716. Available from: https://doi.org/10.1007/s10111-016-0374-2

[13] Bassey C, Chinda ET, Idowu S. Building a scalable Security Operations Center: a focus on open-source tools. Journal of Engineering Research and Reports [Internet]. 2024; 26(7): 196-209. Available from: https://doi.org/10.9734/jerr/2024/v26i71203