Enhancing Cybersecurity Resilience through Improved Technical Measures in Incident Response Strategies

ASSOUJAA ISMAIL
Faculté des Sciences Dhar El Mahraz,
Université Sidi Mohamed Ben AbdellahThis link is disabled.,
Fez,
MOROCCO
https://orcid.org/0000-0001-8572-5593

Abstract: Weak credentials, insecure software, and low user awareness create significant vulnerabilities that cyber attackers exploit. Effective Incident Response (IR) is essential for mitigating cyberattacks, safeguarding critical infrastructure, and ensuring the continued functionality of software systems under attack. However, many organizations focus more on strengthening their digital defenses than on preparing robust incident response mechanisms. Common IR challenges include poor usability, high false positives, integration problems, limited resources, and a lack of collaboration and communication. Furthermore, insufficient training in soft skills like problem-solving and teamwork worsens the situation. IR frameworks emphasize the importance of structured response plans that guide organizations in managing and mitigating breaches, even when the attacker's identity remains unknown. To enhance IR effectiveness, this paper proposes adopting structured incident response playbooks. Additionally, organizations must improve cross-team collaboration and prioritize communication to mitigate evolving cyber threats. By focusing on incident preparation, real-time monitoring, and postincident learning, organizations can improve their resilience and readiness to respond to increasingly sophisticated attacks.

Keywords: Incident Response, Frameworks, Security

Received: April 12, 2024. Revised: October 13, 2024. Accepted: November 18, 2024. Published: December 24, 2024.

1. Introduction

Cybersecurity plays a critical role in safeguarding interconnected systems and critical infrastructure from unauthorized access and malicious activities. Organizations face a myriad of challenges, including weak credentials, insecure software, and low user awareness, which expose them to cyberattacks. While significant attention has been devoted to fortifying digital defenses, the need for robust IR capabilities has become increasingly critical to mitigate the impact of breaches when they occur. Cyber incidents such as ransomware attacks, unauthorized domain access, malware infections, and coordinated login attempts present serious threats to organizational security. However, many IR strategies focus predominantly on the technical aspects of incident management, often overlooking the practical capabilities needed to address such incidents comprehensively. A well-structured IR process is crucial for ensuring continued functionality and mitigating potential damages. The four key phases of incident response Preparation, Detection and Analysis, Containment, Eradication and Recovery, and Post-Incident Activity offer a systematic approach to managing security breaches. Challenges such as high false-positive rates, integration difficulties, resource constraints, and communication breakdowns, especially in areas requiring soft skills like teamwork and problem-solving, often impede the effectiveness of these processes. As cyber threats grow more sophisticated with the advent of advanced technologies, organizations must prioritize the development of comprehensive incident response strategies. Widely recognized frameworks, such as those from NIST and SANS, provide valuable guidelines for managing cyber incidents, from initial preparation to post-incident recovery. Additionally a tailored incident response playbook can enable organizations to respond effectively to specific threats, reducing risk and strengthening resilience against future attacks. Successful incident response demands technical expertise, collaboration, training, and strategic communication to maintain operational continuity and minimize damage. The paper is organized as follows: Section 2 explores assessing security levels and threat resilience. Section 3 outlines the incident response process, frameworks and challenges. Section 4 discusses the application of incident response in incident mitigation. Finally, Section 5 presents the Conclusion.

2. Assessing Security Levels and Threat Resilience

Organizations face diverse cyber threats, from malware to data breaches, requiring strong prevention, detection, and response capabilities. While many focus on strengthening defenses, they often neglect the importance of IR in minimizing damage. Evolving threats, weak credentials, and poor user awareness contribute to vulnerabilities, compounded by inadequate cybersecurity tools and a lack of skilled IR personnel. Effective IR, involving continuous threat assessment and proactive monitoring, is essential for resilience. Without well-integrated IR processes, communication issues and team silos can impede effective threat response.

2.1 Assessing Security Levels

Evaluating the security levels of an organization or system involves a comprehensive analysis of various factors that determine the protection and management of data throughout its lifecycle. The assessment focuses on how data is classified, collected, stored, used, and eventually destroyed, while

ensuring compliance with security policies and regulatory requirements. The key components of assessing security levels include:

- Type of Data: The first step in assessing security levels involves identifying the types of data handled by the organization. Data can be classified into various categories such as public, confidential, sensitive, or personal information. The classification determines the level of protection needed, with more stringent controls required for sensitive or personal data like personally identifiable information (PII), financial records, and healthcare information.
- Data Collection Methods: Security assessments also consider how data is collected, ensuring that the methods used to gather information are secure and comply with relevant regulations. Secure collection methods should prevent unauthorized access or tampering during the data acquisition process. For instance, secure forms, encrypted transmissions, and authentication mechanisms are vital in protecting data integrity and confidentiality during collection.
- Storage Methods: Data storage security is critical, as it involves protecting data at rest. Organizations should evaluate the security measures in place for data storage, such as encryption, access control, and backup strategies. Stored data, whether on-premises or in the cloud, must be protected from unauthorized access, loss, or corruption through multi-layered security techniques such as encryption algorithms, firewalls, and regular access control reviews.
- Data Usage: Once data is collected and stored, it must be used securely. Assessing security during usage focuses on ensuring that only authorized individuals or systems have access to the data and that it is used for its intended purpose. Role-based access control (RBAC) or the principle of least privilege should be enforced to restrict access to sensitive data. Monitoring and auditing data usage also ensure that any misuse or unauthorized access can be detected promptly.
- Data Destruction: A critical component of security assessment is how an organization handles the destruction of data. When data is no longer needed, it must be securely deleted to prevent unauthorized recovery. Secure data destruction methods include physical destruction of storage media, degaussing, or cryptographic erasure for digital data. Regular reviews of data retention policies and ensuring compliance with secure destruction protocols are necessary for maintaining high security levels.

2.2 Assessing Resilience

Resilience refers to an organization's ability to withstand, respond to, and recover from security incidents and attacks. Assessing resilience is essential for ensuring that systems and operations can continue functioning during and after an attack or failure. This assessment is typically performed through various testing and auditing methods aimed at identifying vulnerabilities and ensuring the effectiveness of security controls. Key methods for assessing resilience include:

- Penetration Testing: Penetration testing (pen-testing) simulates real-world attacks to assess the effectiveness of security measures and identify vulnerabilities that could be exploited by malicious actors. Internal penetration tests involve authorized personnel attempting to breach the system using the same techniques as external attackers. These tests provide valuable insight into how well systems can withstand an attack and allow organizations to proactively patch vulnerabilities before they are exploited.
- Internal Audits: Internal audits are crucial for evaluating whether security policies and procedures are being followed. They assess compliance with internal security standards, industry regulations, and best practices. Regular audits help ensure that security controls are operating as intended and identify areas where improvements are needed. Audits also help uncover gaps in security protocols, misconfigurations, or failures in implementing security measures, providing a foundation for remediation.
- Vulnerability Scans: Vulnerability scanning involves the automated analysis of systems and networks to detect known vulnerabilities that could be exploited by attackers. These scans are conducted regularly and focus on identifying outdated software, unpatched systems, misconfigurations, and weak points in security architecture. Regular scanning helps maintain a proactive defense by ensuring that all systems are up-to-date with the latest security patches and configurations.
- Incident Response Testing: Assessing resilience also involves testing the organizations ability to respond to security incidents. This includes conducting tabletop exercises, simulated attacks, and breach simulations to evaluate how well the incident response team and overall organization can detect, contain, and recover from a security breach. Incident response testing ensures that teams are prepared to respond effectively under pressure and that the organization has the tools and processes in place to minimize damage during an incident.
- Business Continuity and Disaster Recovery Tests: Resilience assessment must also cover business continuity and disaster recovery (BC/DR) plans. These tests evaluate an organizations ability to continue critical operations and recover from disruptions caused by attacks, natural disasters, or system failures. BC/DR testing involves simulating various disaster scenarios to ensure that recovery time objectives (RTO) and recovery point objectives (RPO) are met. Regular testing and updating of these plans are essential to ensure long-term resilience.

Both security level assessments and resilience evaluations are essential for building robust and secure systems. By systematically assessing how data is handled throughout its lifecycle and continuously testing the organization's ability to withstand attacks and recover from disruptions, organizations

can enhance both their security posture and resilience in the face of evolving threats.

3. Assessing Incident Severity and Response Capabilities

3.1 Assessing Incident Severity

Evaluating the severity of a security incident is critical for prioritizing response actions and resource allocation. One commonly used approach for assessing severity is the Common Vulnerability Scoring System (CVSS), which provides a standardized method to score the severity of security vulnerabilities on a scale of 0 to 10, with higher scores indicating greater severity. Incident severity can generally be categorized into three levels: low, medium, and high.

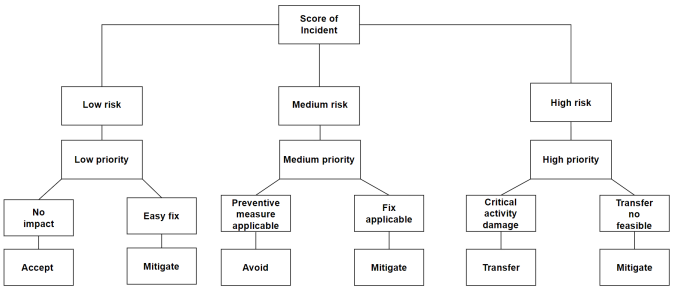
- Low Severity: Incidents classified as low severity typically involve minimal risk to the organization, with little to no impact on operations, data, or reputation. Low severity issues may include minor vulnerabilities such as outdated software or low-risk misconfigurations. In CVSS, these incidents often score between 0 and 3.9. Such incidents are unlikely to be exploited or have limited potential for harm if they are, making them lower priority for immediate response.
- Medium Severity: Medium severity incidents present a moderate level of risk, with potential to disrupt operations, cause reputational damage, or lead to limited data loss. These incidents might involve vulnerabilities that are more easily exploitable or require user interaction, such as phishing attempts or malware infections with limited impact. On the CVSS scale, medium severity issues typically score between 4.0 and 6.9. Organizations must pay attention to these incidents, as they can escalate if not addressed in a timely manner.
- High Severity: High severity incidents pose a significant risk to the organization, potentially leading to widespread disruption, data breaches, financial loss, or severe reputational damage. These incidents often involve critical vulnerabilities that are easily exploitable or have a high potential for harm, such as ransomware attacks or large-scale breaches of sensitive information. On the CVSS scale, high severity incidents score between 7.0 and 10. These incidents demand immediate action and the highest level of response to mitigate the risk.

3.2 Response Capabilities Based on Severity Levels

The response strategy for each incident should be tailored to the assessed severity level. Organizations can adopt different approaches, ranging from acceptance and mitigation to transfer, depending on the severity and the potential impact of the incident. The following outlines how response capabilities can be structured based on the severity of incidents:

- Response to Low Severity Incidents: For low-severity incidents, organizations have more flexibility in determining the appropriate response. Given the minimal risk posed by these incidents, organizations may choose to:
  Accept the Risk: If the incident has little to no impact and the cost of mitigation outweighs the risk, it may be reasonable to accept the risk without taking action. Mitigate the Risk: For easily addressable issues, such as applying a software patch or adjusting configurations, organizations can quickly mitigate the vulnerability with minimal effort. Since low-severity incidents are generally manageable and pose limited risk, the response can be less urgent, allowing the organization to focus resources on more critical threats.
- Response to Medium Severity Incidents Medium severity incidents require more active intervention, as they pose a higher risk than low-severity issues and can escalate if left unaddressed. The response to these incidents typically involves:
  Avoid the Risk: If possible, organizations may choose to avoid the risk by implementing preventive measures, such as blocking malicious IP addresses or restricting access to vulnerable systems. Mitigate the Risk: Mitigation efforts should be prioritized to reduce the potential impact of the incident. This may involve patching vulnerabilities, increasing monitoring, or strengthening access controls. Given their moderate risk, medium severity incidents require timely attention to prevent escalation into more serious issues, though the organization can often manage these incidents internally without significant disruption.
- Response to High Severity Incidents High-severity incidents demand the most comprehensive and immediate response, as they pose a serious threat to the organization's operations, data, and reputation. The response options for high-severity incidents include:
  Transfer the Risk: Organizations may choose to transfer the risk through cyber insurance, outsourcing incident response to third-party experts, or collaborating with law enforcement in cases of severe criminal activity. This approach is useful when the cost of handling the incident internally is too high. Mitigate the Risk: In cases where transferring the risk is not feasible, the organization must act swiftly to mitigate the incident. This may involve activating a full incident response team, isolating affected systems, and deploying countermeasures to contain and eradicate the threat. For high-severity incidents, immediate action is critical to minimize damage, and response efforts should be escalated to ensure that all necessary resources are mobilized to address the incident effectively.

Assessing incident severity and aligning response capabilities ensures that organizations can respond proportionally to threats, minimizing potential damage while optimizing resource allocation. By using frameworks like CVSS and tailoring responses to incident severity, organizations can enhance their incident response strategies and overall cybersecurity resilience.



4. Incident Response Process, Challenges & Enhancement Solutions

IR is a critical function for addressing and mitigating the impact of cyberattacks. As cyber threats evolve, organizations need robust strategies and frameworks that help them respond efficiently to these incidents. While organizations often focus on preventive measures such as improving digital defenses, the emphasis on effective incident response processes tends to lag behind, often due to a lack of practical capabilities and preparedness. This section outlines the incident response process, key frameworks, and the challenges organizations face in implementing effective incident response strategies.

4.1 Incident Response Process

The incident response process is essential for organizations to manage and mitigate the impact of cybersecurity incidents. It typically involves four key phases: preparation, detection and analysis, containment, eradication and recovery, and post-incident activity. Each phase is designed to ensure that organizations respond to threats systematically and efficiently.

1) Preparation: Preparation is the first phase of the incident response process, where organizations establish a strong foundation to handle potential incidents effectively. This involves developing and documenting policies, procedures, and playbooks tailored to specific types of security threats. The goal is to ensure readiness for any cybersecurity event by identifying roles and responsibilities, establishing an incident response team, and conducting regular training sessions for staff.
   Key preparation activities include setting up monitoring tools and systems for detecting security incidents, ensuring that incident responders have access to the necessary resources, and creating communication plans. These activities help build a solid framework that enables rapid, coordinated action when an incident occurs.
2) Detection and Analysis: In this phase, the focus is on detecting potential security incidents and accurately analyzing the situation. Detection is achieved through various mechanisms, including automated monitoring systems, security information and event management (SIEM) platforms, threat intelligence feeds, and reports from employees or external sources. Once suspicious activity is detected, a thorough analysis is conducted to assess the scope, urgency, and potential impact of the incident.
   Challenges in this phase often include dealing with false positives, the complexity of analyzing large volumes of data from different sources, and integration problems between security tools. The accuracy and speed of detection and analysis are critical in determining how quickly and effectively the organization can respond.
3) Containment, Eradication, and Recovery: Once an incident is confirmed, the containment phase is initiated to prevent further damage. Containment strategies may vary depending on the severity and type of attack. Short-term containment might involve isolating affected systems, while long-term containment focuses on preventing the attacker from regaining access.
   After containment, the eradication process begins, focusing on removing the threat from the environment. This could involve eliminating malicious software, closing vulnerabilities, or applying security patches. Finally, the recovery phase aims to restore normal business operations by bringing systems back online, restoring data from backups, and verifying that the environment is clean.
   This phase requires precise coordination and sufficient resources to minimize downtime and prevent recurrence of the attack. Inadequate recovery strategies can lead to further disruptions or lingering vulnerabilities.
4) Post-Incident Activity: After the incident has been resolved, it is critical to conduct a post-incident review. This phase focuses on learning from the incident to improve the organization's future response capabilities. The review includes documenting what happened, identifying the root cause, evaluating the effectiveness of the response, and highlighting areas for improvement.
   A key part of post-incident activity is conducting a "lessons-learned" session, where stakeholders discuss what worked well and where gaps in the response process occurred. Additionally, the incident response plan is refined based on these findings to enhance preparedness for future incidents. This phase also ensures that any regulatory reporting requirements are met, and the organization strengthens its security posture by addressing the vulnerabilities that led to the incident.

4.2 Challenges in Incident Response

Despite the availability of a structured frameworks, organizations face significant challenges in effectively implementing IR processes. These challenges are both technical and organizational, often undermining the ability to respond swiftly and efficiently to security incidents.

- Poor Usability of Tools: One of the primary challenges in incident response is the poor usability of security tools. Many incident response platforms are difficult to navigate or are not well-integrated with other systems.

This complexity hinders security team's ability to act quickly and effectively. Delays in response efforts often occur when tools require excessive time for configuration or when their interfaces are not intuitive, leading to inefficiencies in incident handling.

- High False Positives: Detection systems frequently generate numerous false positives, overwhelming security teams and diverting attention away from genuine threats. This problem is exacerbated by inadequate automation in security processes, which slows down the detection and analysis of real incidents. As a result, IR teams often spend valuable time sifting through non-critical alerts, delaying their response to actual security threats.
- Resource Limitations: Many organizations, particularly small and mid-sized businesses, face significant resource constraints. These organizations often lack the financial and personnel resources needed to maintain a fully functional incident response team. The absence of adequate resources leads to gaps in monitoring and response capabilities, increasing the organizations vulnerability to cyberattacks.
- Collaboration and Information Silos: Incident response teams frequently operate in isolation from other departments within the organization, such as IT and security operations. This siloed approach restricts collaboration and hinders efficient information sharing between teams. Without effective communication and coordination, incidents are often addressed too slowly or with incomplete information, resulting in suboptimal mitigation efforts.
- Lack of Soft Skills and Training: Incident response requires more than technical proficiency; effective problem-solving, communication, and teamwork are equally essential. However, many organizations fail to prioritize the development of these soft skills in their security teams. Additionally, the lack of regular training exercises, such as simulations or tabletop exercises, results in reduced readiness to handle real-world incidents. Teams that are not adequately trained may struggle to coordinate responses effectively during high-pressure situations.

Addressing Challenges in Incident Response To improve the effectiveness of incident response processes, organizations must implement solutions that address both technical and organizational challenges.

4.3 Enhancement Solutions in Incident Response

IR is essential for organizations to both react to cyberattacks and build resilience over time by learning from incidents and adapting defenses. Automation tools, like darknet sensors, threat intelligence sharing, and automated threat lists, enable early threat detection while maintaining privacy. Partnerships among Computer Security Incident Response Teams (CSIRTs) enhance collective resilience and visibility into potential threats. However, many organizations face challenges, such as high false positives, integration issues, resource limitations, and organizational barriers like poor communication and knowledge silos, which can limit IR effectiveness. To improve, organizations must foster interdepartmental collaboration, continuous training, and practical assessments of IR processes.

To Enhance Incident Response

- Integrating Incident Response with IT Operations:
  Effective incident management requires alignment between security and IT operations teams. Improved collaboration and regular communication reduce response time, enhance situational awareness, and enable coordinated responses.
- Developing Incident Response Playbooks:
  Customized playbooks for specific incidents (e.g., ransomware, malware) provide standardized procedures, ensuring teams act swiftly and consistently under pressure. Playbooks should be updated to reflect new threats and incorporate lessons learned from past incidents, outlining actions for each phase of the response process.
- Enhancing Training and Development:
  Continuous training, including simulations and tabletop exercises, is crucial for preparing incident response teams. Focusing on both technical and soft skills, such as communication and coordination, minimizes errors and improves response effectiveness during incidents.
- Proactive Threat Monitoring:
  Advanced monitoring, including darknet sensors and threat intelligence, helps organizations detect suspicious activity early. Automated tools balance privacy and threat data sharing, enabling swift responses. Continuous monitoring and threat-hunting provide real-time visibility, helping detect incidents before they escalate.

While incident response is essential for minimizing cyberattack impact, challenges such as poor tool usability, resource limitations, and inadequate collaboration must be addressed. Organizations should adopt integrated IR processes, leverage automated monitoring tools, and invest in training that develops both technical and interpersonal skills. By addressing these socio-technical barriers and continuously refining IR strategies, organizations can enhance cybersecurity resilience and improve their defenses against evolving threats.

5. Conclusion

The effectiveness of an organization's ability to detect, contain, and recover from cyberattacks is ultimately determined by the capabilities of its IR team. While IR teams are tasked with mitigating cyber threats and restoring system functionality, they often encounter a range of socio-technical barriers that undermine their performance. Additionally, the lack of practical skills such as problem-solving and teamwork contributes to operational inefficiencies. For incident response to be more effective, organizations must address these socio-technical barriers by developing comprehensive training programs that integrate technical skills with soft skills. Incorporating well-structured incident response playbooks. Such playbooks should include real-world use cases, emphasizing preparation, detection, analysis, containment, and recovery, tailored to the specific attack vectors that organizations may

encounter. Moreover, continuous learning and improvement must be emphasized to close the gaps in incident handling. This can be achieved by integrating feedback loops after each incident and ensuring that lessons learned from previous incidents are incorporated into future preparedness strategies. Overall, an adaptive, well-coordinated approach to incident response backed by training, robust frameworks, and collaboration will enhance an organization's resilience against evolving cyber threats and improve long-term cybersecurity management.

References

[1] Eduardo B. Fernndez, A Threat Model Approach to Threats and Vulnerabilities in On-line Social Networks. January 2010 DOI: 10.1007/978-3-642-16626-6_15 Source: DBLP
[2] Borja Sanz, Gonzalo Alvarez, Carlos Laorden, Pablo Garca Bringas. A Threat Model Approach to Attacks and Countermeasures in On-line Social Networks. October 2011.
[3] Mohammad Aijaz, Mohammed Nazir, Malik Nadeem Anwar Mohammad. Threat Modeling and Assessment Methods in the HealthcareIT System: A Critical Review and Systematic Evaluation. SN Computer Science (2023) 4:714. https://doi.org/10.1007/s42979-023-02221-1
[4] Suvda Myagmar Adam J. Lee William Yurcik. Threat Modeling as a Basis for Security Requirements.
[5] Mohammed Kharma, Adel Taweel. Threat Modeling in Cloud Computing - A Literature Review. February 2023. DOI: 10.1007/978-981-99-0272-9_19.
[6] Matteo Groe-Kampmann, Norbert Pohlmann, Markus Hertlein, Thorsten Holz. Threat Modeling for Mobile Health Systems. April 2018. DOI: 10.1109/WCNCW.2018.8369033.
[7] Habeeb Omotunde, Rosziati Ibrahim. A Review of Threat Modelling and Its Hybrid Approaches to Software Security Testing. December 2015.
[8] Eduardo B. Fernndez. Threat Modeling in Cyber-Physical Systems. August 2016. DOI: 10.1109/DASC-PICom-DataCom-CyberSciTec.2016.89
[9] ISMAIL ASSOUJAA, SIHAM EZZOUAK, HAKIMA MOUANIS. Compression Point in Field of Characteristic 3. Springer, I4CS 2022, CCIS 1747, pp. 104111, 2022 https://doi.org/10.1007/978-3-031-23201-5_7.
[10] ISMAIL ASSOUJAA, SIHAM EZZOUAK, HAKIMA MOUANIS. Tower Building Technique on Elliptic Curve with Embedding Degree 36. WSEAS TRANSACTIONS ON COMPUTERS. DOI: 10.37394/23205.2022.21.39.
[11] ISMAIL ASSOUJAA, SIHAM EZZOUAK, HAKIMA MOUANIS. Tower Building Technique on Elliptic Curve with Embedding Degree 72. WSEAS Transactions on Computer Research 10:126-138 DOI: 10.37394/232018.2022.10.17
[12] ISMAIL ASSOUJAA, SIHAM EZZOUAK, HAKIMA MOUANIS. TOWER BUILDING TECHNIQUEON ELLIPTIC CURVEWITH EMBEDDING DEGREE 18. Tatra mountains mathematical publications, DOI: 10.2478/tmmp-2023-0008Tatra Mt. Math. Publ. 83 (2023), 103118.
[13] ISMAIL ASSOUJAA, SIHAM EZZOUAK, HAKIMA MOUANIS. Pairing based cryptography New random point exchange key protocol. Conference: 2022 7th International Conference on Mathematics and Computers in Sciences and Industry (MCSI), DOI: 10.1109/MCSI55933.2022.00017.
[14] ISMAIL ASSOUJAA, SIHAM EZZOUAK. New Compression Point Reducing Memory Size in Field of Characteristic Different From 2 And 3.International Journal of Scientific Research and Innovative Studies. https://doi.org/10.5281/zenodo.11244720.
[15] ISMAIL ASSOUJAA, SIHAM EZZOUAK. Improving arithmetic calculations on elliptic curves with embedding degree 2i.3. Journal of Xidian University. https://doi.org/10.5281/Zenodo.11505701. ISSN No:1001-2400.
[16] ISMAIL ASSOUJAA, SIHAM EZZOUAK, Improving Arithmetic Calculations on Elliptic Curves with Embedding Degree 2i and 3j, International Journal of Recent Engineering Research and Development (IJRERD), ISSN: 2455-8761-Volume 09 Issue 03, PP. 131-142.
[17] ISMAIL ASSOUJAA, SIHAM EZZOUAK, Compression points in elliptic montgomery and edwards curves. ACM ISBN 979-8-4007-0929, https://doi.org/10.1145/3659677.3659834.
[18] Oluwafemi Oriola, Adesesan Barnabas Adeyemo, Maria Papadaki, Eduan Kotz. A collaborative approach for national cybersecurity incident management. Information and Computer Security. June 2021. DOI: 10.1108/ICS-02-2020-0027.
[19] Adeel Javaid. Incident Response Planning for Data Protection. SSRN Electronic Journal. January 2013. DOI: 10.2139/ssrn.2391677
[20] Faith Lekota, Marijke Coetzee. Cyber security Incident Response for the Sub-Saharan African Aviation Industry. August 2019.
[21] Keinaz Domingo. Implementing cyber security incident response playbook in a Philippine powergrid company. May 2022.
[22] Zamfiroiu Alin, Ramesh C Sharma. Cybersecurity Management for Incident Response. Romanian Cyber Security Journal. May 2022. DOI: 10.54851/v4i1y202208.
[23] Ashley O'Neil, Atif Ahmad, Sean B. Maynard. Cybersecurity Incident Response in Organisations: A Meta-level Framework for Scenario-based Training. Australasian Conference on Information Systems 2021, Sydney.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The author contributed in the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The author has no conflict of interest to declare that is relevant to the content of this article.