European Research Studies Journal
Volume XXVIII, Issue 1, 2025

pp. 575-588

Effectiveness of Information Security Incident Management Systems: Identifying Practices, Challenges and Development Perspectives

Submitted 12/01/25, 1st revision 11/02/25, 2nd revision 28/02/25, accepted 10/03/25

Sławomir Żurawski[1], Aneta Chrząszcz[2], Zbigniew Ciekanowski[3], Yury Pauliuchuk[4], Sylwester Pietrzyk[5], Barbara Wyrzykowska[6]

Abstract:

Purpose: *The primary objective of this article was to investigate the effectiveness of information security incident management systems and assess their impact on the level of organizational protection. The analysis includes identifying key practices, challenges, and development perspectives in this area. Additionally, the article provides practical recommendations to support organizations in improving their response mechanisms to threats and enhancing resilience against security incidents.*
Methodology/Approach: *The study focuses on analysing different approaches to incident management, comparing traditional methods with modern ones based on automation and artificial intelligence, and evaluating their impact on key effectiveness metrics such as Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), and False Positive Rate. As part of the project, a review of scientific literature, analysis of industry reports, and case studies of organizations implementing various incident management systems were conducted.*
Findings: *The analysis indicates that organizations implementing modern incident management technologies can significantly reduce response times and decrease false alarms, leading to improved operational efficiency for security teams. The use of automation and AI enables more precise threat detection and minimizes human errors. However, organizations face challenges such as high implementation costs, a shortage of skilled professionals, and difficulties integrating new technologies.*

[1]*State Academy of Applied Sciences in Chełm, Poland, ORCID: 0000-0001-9527-3391, e-mail: slawomir.zurawski@onet.pl;*
[2]*Akademia Bialska im. Jana Pawła II w Białej Podlaskiej, Poland, ORCID: 0000-0001-9749-274X, e-mail: aneta.chrzaszcz@op.pl;*
[3]*Wydział Nauk Społecznych, Uniwersytet w Siedlcach Poland, ORCID 0000-0002-2077-5124, e-mail: y.pauliuchuk@wp.pl;*
[4]*Wydział Nauk Społecznych, Uniwersytet w Siedlcach Poland, ORCID: 0000-0002-2077-5124, e-mail: y.pauliuchuk@wp.pl;*
[5]*Warsaw Management University, Poland, ORCID: 0000-0001-7697-0853, e-mail: spietrzyk16@gmail.com;*
[6]*Institute of Management, Warsaw University of Life Sciences, Poland, ORCID: 0000-0002-7025-0799, e-mail: barbara_wyrzykowska@sggw.edu.pl;*

Practical implications: *The study's findings are highly relevant for organizations aiming to improve the effectiveness of incident management. Key recommendations include, investing in automation and AI to reduce response times and enhance the precision of threat detection, training employees and developing cybersecurity competencies to effectively manage modern systems, integrating incident management with the overall cybersecurity strategy to adopt a more holistic approach to protecting organizational assets, fostering cross-sector collaboration and sharing threat information, which will enhance global protection against cyberattacks.*
Originality/value: *In summary, the future of incident management depends on an organization's ability to adapt new technologies, improve operational processes, and continuously enhance the competencies of IT security teams.*

Keywords: *Incident management, information security, effectiveness, cybersecurity.*

JEL codes: *M12, L86, D83.*

Paper type: *Research article.*

1. Introduction

Modern organizations operate in a dynamic and complex digital environment that brings numerous information security threats. Security incidents, such as hacking attacks, data breaches, or malicious software, can result in significant financial losses, loss of customer trust, and violations of legal compliance. Consequently, effective Information Security Incident Management (ISIM) has become a critical component of organizational protection strategies (Grima *et al.*, 2023).

Information Security Incident Management Systems (ISIMS) enable rapid detection, analysis, and mitigation of threats, minimizing their impact on organizational operations. Implementing modern solutions such as Security Information and Event Management (SIEM) or Security Orchestration, Automation, and Response (SOAR) allows for process automation and enhances the efficiency of incident response. However, the effectiveness of these systems depends on several factors, including the quality of collected data, integration with other security tools, and the competencies of the team responsible for their operation.

The purpose of this article is to analyse the effectiveness of information security incident management systems as a key component of organizational protection. In the first section, theoretical foundations of incident management will be presented, including applicable standards and the stages of threat response.

The second section will focus on analysing the efficiency of various solutions, discussing key performance indicators and the impact of automation on response time. The final section will provide recommendations for improving incident management systems and discuss future development directions in this field.

2. Materials and Methods

The primary goal of the article was to determine the effectiveness of information security incident management systems and their impact on the level of organizational protection.

The analysis included identifying key practices, challenges, and development perspectives in this area. Additionally, the study aimed to develop practical recommendations to support organizations in improving their mechanisms for responding to threats and increasing resilience to security incidents.

To conduct a comprehensive analysis of the effectiveness of information security incident management systems, the following data collection methods were used:

- Review of scientific literature – analysis of academic articles, industry publications, and reports related to incident management.
- Analysis of industry reports – review of data from reputable sources specializing in cybersecurity.
- Case studies – analysis of organizations implementing various incident management systems to evaluate their effectiveness under real-world conditions.
- Performance metrics analysis – comparison of key indicators such as Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), and False Positive Rate.

After gathering and analysing the research materials, the following steps were taken in the development of the results:

1. Classification of Incident Management Approaches – A comparison of traditional methods with modern solutions utilizing automation and artificial intelligence.
2. Assessment of the Impact of Modern Technologies – An analysis of how implementing AI-based systems affects response times and operational efficiency of security teams.
3. Identification of Challenges – Highlighting key barriers to adopting modern technologies, such as high implementation costs or lack of qualified personnel.
4. Formulating Recommendations – Developing practical guidelines for organizations on investing in technology, training, and integrating incident management with a global cybersecurity strategy.

In summary, this study provides a comprehensive analysis of the effectiveness of incident management systems and identifies key directions for their development, emphasizing the importance of innovative technologies and the competencies of IT security teams.

3. Theoretical Foundations of Information Security Incident Management

Information security incident management is a key element of an organization's strategy to protect itself against cyber threats. In the era of advancing digitalization and an increasing number of cyberattacks, organizations must implement effective systems that enable the rapid detection, analysis, and mitigation of incidents that could threaten the integrity, confidentiality, and availability of their resources. An information security incident is defined as any event that may lead to a breach of an organization's security, whether caused by hacking attacks, human error, or technical failures. The most common incidents include malware attacks, phishing, unauthorized system access, data leaks, and disruptions to IT services such as DDoS attacks (Rosenberg, Schneider, Scherb and Asprion, 2023).

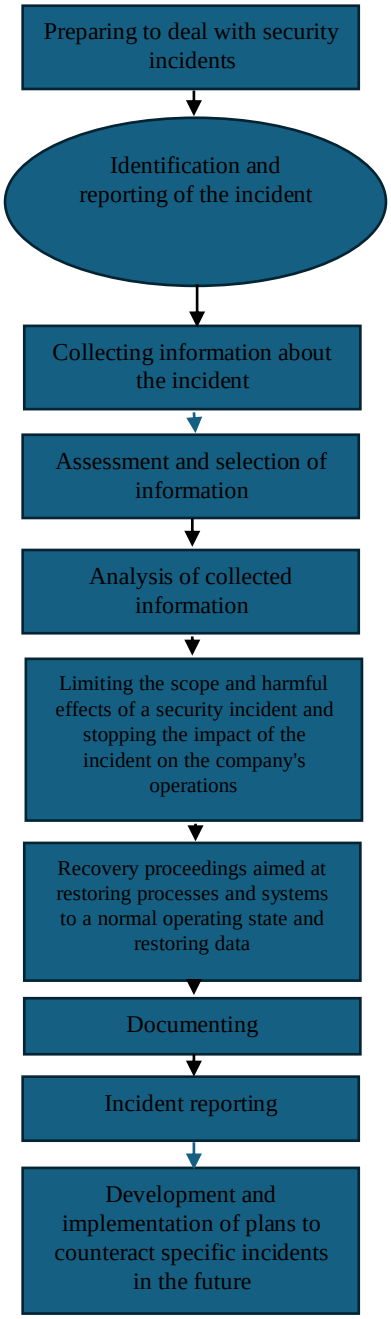
To effectively manage incidents, organizations implement security incident management systems that encompass both operational procedures and advanced technologies. Modern systems, such as Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR), and Endpoint Detection and Response (EDR), enable network monitoring, analysis of suspicious events, and automation of threat responses (Tyagi *et al.*, 2023).

Security Information and Event Management systems (SIEM) were developed to help administrators design security policies and manage events from various sources (González-Granadillo *et al.*, 2021, p. 3). SIEM allows for the aggregation and analysis of logs from different sources to identify potential incidents, while SOAR further automates response processes, significantly reducing the time to neutralize threats (Bartwal *et al.*, 2022; Velinov *et al.*, 2023).

In turn, EDR systems monitor endpoint activity, identifying suspicious behaviour and minimizing infection risk. Implementing these solutions enables organizations not only to effectively detect and respond to incidents but also to analyse historical data and improve cybersecurity strategies based on accumulated experience (Arfeen, 2021, p. 4). Figure 1 illustrates the security incident management process.

The effectiveness of incident management also requires compliance with international standards and regulations that define best practices in this area. The ISO/IEC 27035 standard provides comprehensive guidelines on incident response methodology and risk analysis, while NIST SP 800-61, developed by the U.S. National Institute of Standards and Technology, specifies frameworks for detecting and mitigating threats (Soto and Olier, 2023). In the context of legal regulations, the European GDPR (General Data Protection Regulation) plays a key role by imposing obligations on organizations to adequately secure personal data and report breaches within a specified timeframe. Adhering to these standards not only helps organizations avoid legal consequences but also builds trust among customers and stakeholders, which is crucial for their long-term operations (Ciekanowski *et al.*, 2023, p. 795).

Figure 1. *Security incident management process.*



Source: *Niebezpiecznik.pl. (2024). Zarządzanie incydentami bezpieczeństwa informacji w przedsiębiorstwie. Pozyskano 16 lutego 2025, z https://niebezpiecznik.pl/artykul/zarzadzanie-incydentami-bezpieczenstwa.*

Faced with increasingly advanced threats, organizations must continuously improve their incident management systems to effectively minimize the risk of attacks and their negative consequences. Implementing modern technologies, automating processes, and adhering to international standards and regulations are key elements of an effective security strategy. These measures enable organizations to maintain resilience against cyber threats and ensure business continuity (Rychły-Lipińska and Kamiński, 2024).

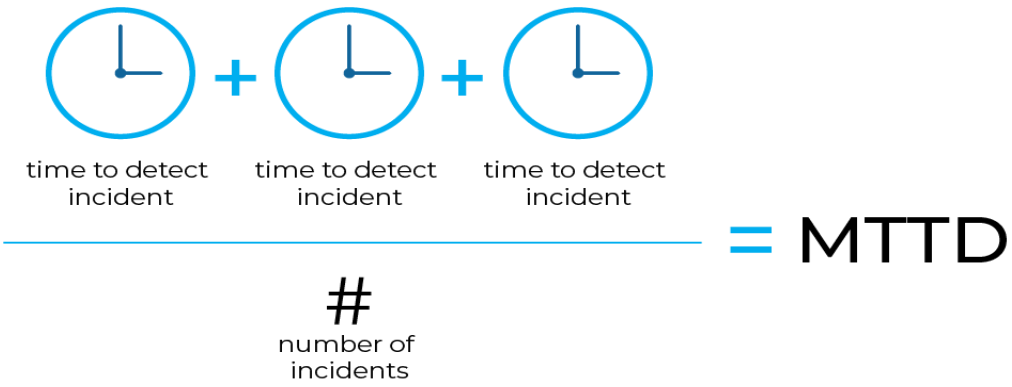
4. Analysis of the Effectiveness of Incident Management Systems in Organizations

The analysis of the effectiveness of information security incident management systems in organizations is a key aspect of evaluating their ability to respond quickly and efficiently to threats. The effectiveness of these systems can be measured using various indicators that determine how effectively an organization detects, analyses, and neutralizes incidents. The most important indicators include (Antczak, Dębicka and Nowakowska-Grunt, 2023):

- Mean Time to Detect (MTTD),
- Mean Time to Respond (MTTR),
- (False Positive Rate).

MTTD defines the average time required to detect an incident, which is crucial in preventing the escalation of threats. The shorter the MTTD, the greater the chance of quickly neutralizing an attack before it causes significant damage. Figure 2 illustrates a schema for calculating MTTD.

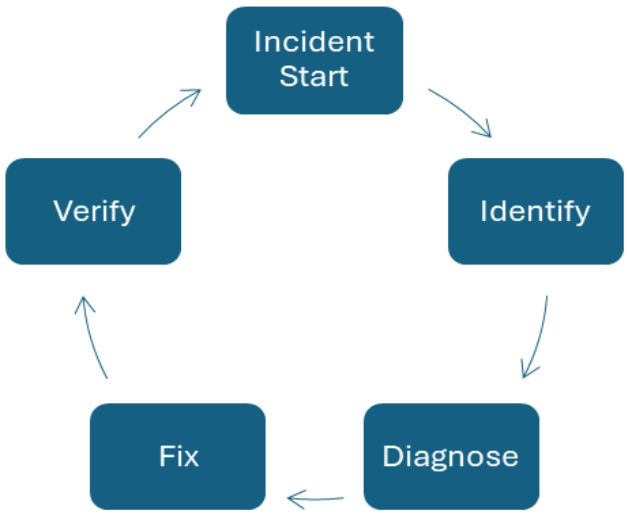
Figure 2. *Schema for calculating MTTD.*



Source: *Plutora. (n.d.). MTTD (Mean Time to Detect): Defined and Explained. Plutora. Retrieved February 19, 2025, from https://www.plutora.com/blog/mttd-mean-time-to-detect-defined-explained*

On the other hand, MTTR (Mean Time To Resolve) is the average time needed to fully resolve an incident, from detection to the restoration of normal system operation. Figure 3 shows time signatures that help identify opportunities for improvement in incident response.

Figure 3. *Timestamps that help identify improvement opportunities in incident response*



Source: *BMC Software. (n.d.). Using Mean Time to Identify (MTTI) as a Service Desk Metric. BMC Software Blogs. Retrieved February 19, 2025, from https://www.bmc.com/blogs/mtti-service-desk-metric.*

Organizations aim to achieve the shortest possible Mean Time to Repair (MTTR) to minimize the impact of incidents. However, this metric is influenced by several factors, such as the availability of skilled personnel and the level of process automation.

The False Positive Rate (FPR) measures the percentage of reported incidents that turn out to be false alarms. A high number of false positives can unnecessarily burden security teams and divert attention from real threats. Therefore, effective incident management systems should minimize this rate by utilizing advanced methods for event analysis and filtering (Yang *et al.*, 2015, p. 5).

One of the most important trends in incident management is the automation and use of artificial intelligence to analyse threats and make quick decisions (Walasek, 2016). Traditional systems mainly relied on manual processing of alerts by security analysts, which often led to delays and human errors. The introduction of SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation and Response) technologies allows for a significant reduction in response time through the automatic classification of incidents and initiation of appropriate actions based on predefined procedures.

Artificial intelligence, by analysing network behaviour patterns, can also identify anomalies that may indicate potential threats, even if they have not yet been recognized in traditional signature databases. Automation not only reduces MTTD and MTTR values but also limits the number of false alarms, which translates into more efficient use of organizational resources.

To better illustrate the effectiveness of different approaches to incident management, it's worth examining a case study comparing traditional manual incident processing systems with modern automated solutions. In one of the analysed organizations, before the implementation of SIEM and SOAR, the Mean Time to Detect (MTTD) averaged 12 hours, and the Mean Time to Repair (MTTR) exceeded 24 hours, as analysts had to manually analyse each alert and make appropriate decisions.

After implementing modern technologies, the incident detection time was reduced to 2 hours, and full problem resolution occurred on average within 6 hours. Automation also reduced the false alarm rate from 40% to 15%, significantly improving the efficiency of the cybersecurity team. The data source is anonymous, used only to present a real case. This case shows that organizations investing in modern technologies and automation can significantly improve their ability to respond to incidents and minimize their impact.

Despite the obvious benefits of implementing modern incident management systems, many organizations face significant barriers that hinder the effective implementation of these solutions (Ciekanowski *et al.*, 2024). One of the greatest challenges is the lack of qualified cybersecurity specialists who could effectively manage advanced tools and adapt them to the organization's specifics. Another barrier is the high cost of implementing and maintaining modern systems, especially for small and medium-sized enterprises, which often do not have the necessary budgets for IT security investments.

Additionally, organizations may encounter difficulties integrating new technologies with existing IT systems and meeting regulatory requirements, which can vary by industry and jurisdiction. Internal resistance and lack of awareness about the importance of incident management also pose significant challenges, as effective implementation requires engagement not only from IT teams but also from management and employees at various levels of the organization.

In summary, the effectiveness of incident management systems for information security can be evaluated based on key indicators such as Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), and the false alarm rate. Automation and artificial intelligence play increasingly significant roles in improving the efficiency of these systems, enabling faster detection and neutralization of threats. Case studies show that organizations investing in modern solutions can significantly reduce response times and enhance cybersecurity effectiveness, allowing for earlier responses to threats (Ojdana-Kościuszko, 2024, p. 143).

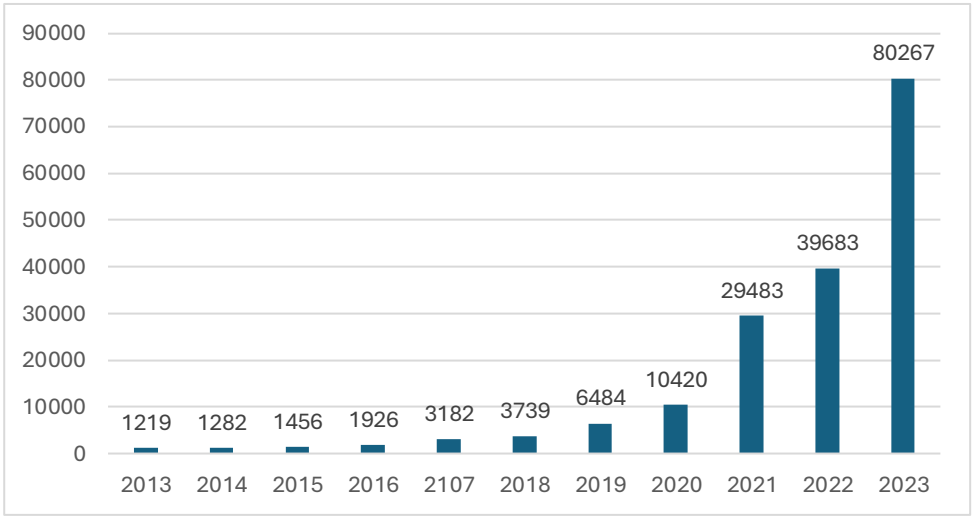
However, implementing advanced systems encounters various barriers, such as a lack of specialists, high implementation costs, and difficulties with technology integration. Therefore, a key challenge for organizations remains finding a balance between investing in modern technologies and effectively managing human and financial resources to maximize the effectiveness of information protection efforts.

5. Recommendations and the Future of Incident Management

Effective management of information security incidents requires not only the implementation of modern technological tools but also an appropriate operational strategy that allows organizations to minimize risk and effectively respond to threats. Best practices in incident management include early detection of threats, rapid response, effective escalation procedures, and continuous improvement of processes based on conducted analyses.

A key element of an effective approach is also the use of well-defined security policies and training employees, who often represent the weakest link in an organization's cybersecurity structure. Regular tests, such as simulation exercises and penetration tests, enable the assessment of an organization's readiness for real threats and the identification of areas needing improvement. For better illustration of the issue, Figure 1 presents a summary of the number of incidents handled by CERT Polska from 2013 to 2023.

Figure 1. *A summary of the number of incidents handled by CERT Polska from 2013 to 2023.*

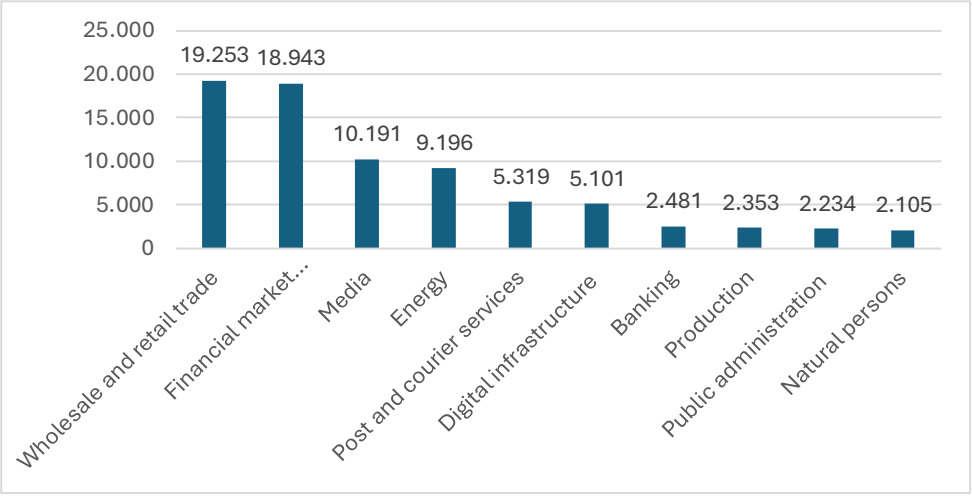


Source: *CERT Polska. (2024). Raport roczny za 2023 r. CERT Polska. Retrieved February 19, 2025, from https://www.cert.pl/raporty/raport-roczny-2023*.

Incident management cannot function in isolation from an organization's overall cybersecurity strategy. Its effectiveness depends on integration with other protective systems, such as risk management, IT infrastructure protection, threat monitoring, and identity and access management. A key aspect is collaboration between various organizational departments to ensure swift decision-making and efficient communication during incidents.

Organizations should also strive to implement a Zero Trust approach, which assumes that every request for access to IT resources must be thoroughly verified, regardless of its source (Yunfei, Quanyan, 2023). Figure 2 illustrates the incidents handled by CERT Polska in 2023, categorized by economic sectors.

***Figure 2**. Incidents handled by CERT Polska in 2023, broken down by economic sectors.*

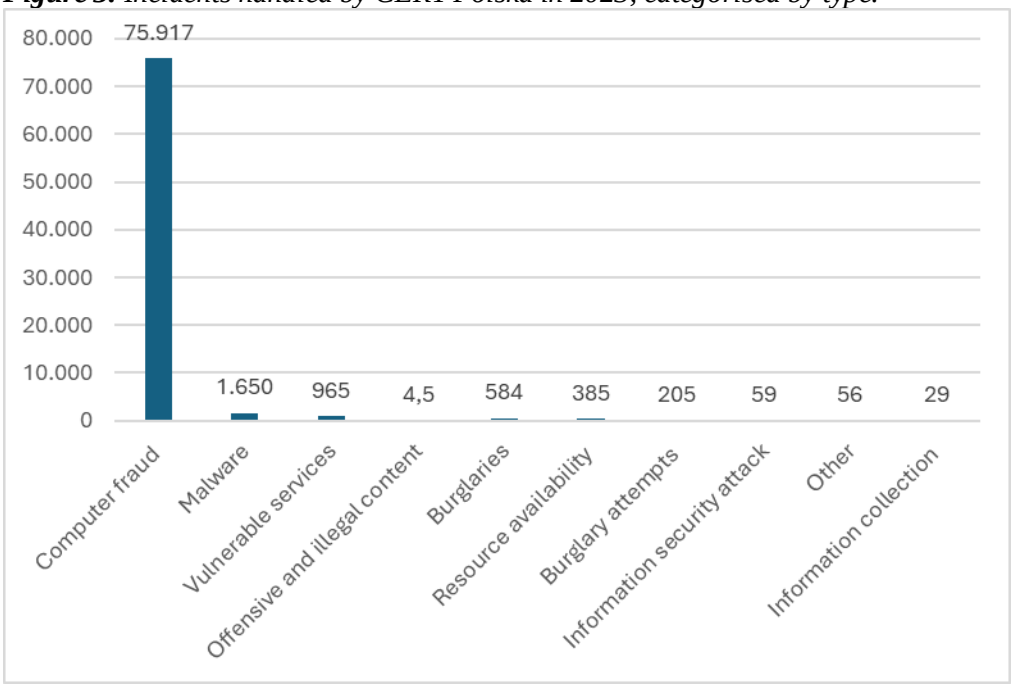


***Source:** CERT Polska. (2024). Raport roczny za 2023 r. CERT Polska. Retrieved February 19, 2025, from https://www.cert.pl/raporty/raport-roczny-2023.*

The greatest threats are concentrated in the commercial and financial sectors, which handle vast amounts of data and transactions. At the same time, significant risks also affect the media, energy, and digital infrastructure sectors, highlighting the growing dependence of the modern economy on information technologies. Figure 3 presents incidents handled by CERT Polska in 2023, categorized by type.

The chart clearly indicates that computer scams are the biggest problem in the field of cybersecurity, significantly surpassing other threats. Other categories, such as malware and vulnerable services, are also important, but their scale is incomparably smaller. In the context of future incident management, the development of technology, including artificial intelligence and machine learning, will play a crucial role.

Figure 3. *Incidents handled by CERT Polska in 2023, categorised by type.*



Source: *CERT Polska, Annual Report for 2023.*

AI can significantly enhance the effectiveness of systems by analysing vast amounts of data in real-time, identifying anomalies, and predictively detecting threats before an incident occurs. The automation of incident response processes, including automatic classification and prioritization of events, allows for a significant reduction in the time it takes to detect and eliminate threats.

Additionally, the development of blockchain technology can increase data security by enabling immutability and full transparency in auditing incidents. In the future, solutions like Extended Detection and Response (XDR) will also play a larger role, combining data from various systems and enabling a holistic approach to incident analysis (Shaji, 2023).

The effectiveness of incident management systems depends on their integration with the overall cybersecurity strategy, the implementation of best practices, and the use of modern technologies, including AI and automation. In the future, key research directions should focus on improving methods for predictive threat detection, enhancing the effectiveness of behavioural analysis systems, and minimizing false positives.

The dynamic development of technology and the growing number of cyber threats require organizations to continuously adapt their incident management approach to

effectively protect their assets from new and increasingly sophisticated attacks. (Ciekanowski *et al.*, 2023, p. 795).

6. Conclusion

Information security incident management is a key element of any organization's cybersecurity strategy. The effectiveness of these systems depends on several factors, including the speed of threat detection and response, integration with other security solutions, and the level of automation and use of artificial intelligence.

Analysis shows that organizations implementing modern technologies such as SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation, and Response), or XDR (Extended Detection and Response) significantly reduce response times to incidents and minimize the impact of cyberattacks. However, even the best technologies cannot replace a well-organized process. This process should include clearly defined procedures, trained personnel, and effective mechanisms for escalation and post-incident analysis.

The conclusions from the conducted research and analysis indicate that organizations must treat incident management as an integral part of their cybersecurity strategy rather than as a separate process. Key elements include continuous threat monitoring, adapting to the evolving landscape of cyberattacks, and investing in employee skill development. Implementing best practices such as the Zero Trust approach, regular penetration testing, and simulation exercises enhances organizational resilience to incidents and enables faster responses in the event of an actual attack.

Despite technological advancements and increasing automation, incident management continues to face numerous challenges. Organizations often encounter barriers such as a lack of skilled specialists, difficulties in integrating modern systems with existing infrastructure, and the high costs of implementing advanced solutions.

Therefore, key areas for further action should include investments in developing cybersecurity personnel, creating more accessible and scalable incident management systems, and improving artificial intelligence algorithms to more effectively filter false alarms and predict threats.

The need for further research and action in the effectiveness of incident management systems is undeniable. Developing methods for predictive incident detection, integrating artificial intelligence (AI) with security systems, and creating better risk assessment mechanisms are key directions for the future of cybersecurity.

Organizations must also actively share experiences and threat data to counteract attacks more effectively and build a more resilient digital ecosystem. Only through a

holistic approach—combining technology, processes, and people—can the impact of incidents be minimized and security ensured in an ever-evolving digital environment.

References:

Antczak, J., Dębicka, E., Nowakowska-Grunt, J. 2023. Wybrane aspekty zarządzania bezpieczeństwem informacji w organizacjach. Wydawnictwo Naukowe.

Arfeen, A., Ahmed, S., Khan, M. A., Jafri, S.F.A. 2021. Endpoint Detection & Response: A Malware Identification Solution, Międzynarodowa konferencja na temat wojny i bezpieczeństwa cybernetycznego (ICCWS), Islamabad, Pakistan, pp. 1-8.

Bartwal, U., Mukhopadhyay, S., Negi, R., Shukla, S. 2022. Security Orchestration, Automation, and Response Engine for Deployment of Behavioural Honeypots. IEEE Conference on Dependable and Secure Computing (DSC), Edynburg, Wielka Brytania, pp. 1-8

Ciekanowski, M, Żurawski, S., Ciekanowski, Z., Pauliuchuk, Y., Czech, A. 2024. Chief Information Security Officer: A Vital Component of Organizational Information Security Management. European Research Studies Journal, Volume XXVII, Issue 2, pp. 35-46.

Ciekanowski, Z., Gruchelski, M., Nowicka, J., Żurawski, S., Pauliuchuk, Y. 2023. Cyberspace as a Source of New Threats to the Security of the European Union. European Research Studies Journal, Volume XXVI, Issue 3, pp. 782-797.

Ciekanowski, Z., Nowicka, J., Czternastek, M., Żurawski, S., Mikosik, P. 2024. How Cybersecurity Shapes Effective Organizational Management. European Research Studies Journal, Volume XXVII, Issue 2, pp. 454-464.

González-Granadillo, G., González-Zarzosa, S., Diaz, R. 2021. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors, 21, 4759, pp. 1-28.

Grima, S., Thalassinos, E., Cristea, M., Kadłubek, M., Maditinos, D., Peiseniece, L. (Eds.). 2023. Digital transformation, strategic resilience, cyber security and risk management. Emerald Publishing Limited.

Liu, Y., Zhang, J., Sarabi, A., Liu, M., Karir, M., Bailey, M. 2015. Predicting Cyber Security Incidents Using Feature-Based Characterization of Network-Level Malicious Activities. In: Proceedings of the 2015 ACM International Workshop on International Workshop on Security and Privacy Analytics (IWSPA '15). Association for Computing Machinery, New York, NY, USA, pp. 3-9.

MTTD (Mean Time to Detect): Defined and Explained. https://www.plutora.com/blog/mttd-mean-time-to-detect-defined-explained.

Ojdana-Kościuszko, M. 2024. Ewolucja i wyzwania polskiego systemu cyberbezpieczeństwa. De Securitate Et Defensione. O Bezpieczeństwie I Obronności, 10(1), pp. 128-146.

Raport roczny z działalności CERT Polska za 2023 r., CERT Polska.

Rosenberg, M., Schneider, B., Scherb, C., Asprion, P.M. 2023. An adaptable approach for successful SIEM adoption in companies. arXiv preprint. Retrieved from: https://arxiv.org/abs/2308.01065.

Rychły-Lipińska, A., Kamiński, W. 2024. Bezpieczeństwo informacji w erze pracy zdalnej a rola modelu ISO 27001:2017. Wydawnictwo Ekonomiczne.

Shaji George, A., Sagayarajan, S., Baskar, T., Hovan George, A.S. 2023. Extending Detection and Response: How MXDR Evolves Cybersecurity. Partners Universal International Innovation Journal, 1(4), pp. 268-285.

Soto V., Olier, E. 2023. Guide for the Design of Cybersecurity Incident Drills through the Adaptation of Standards and Methodologies such as ISO/IEC 27035, NIST SP 800-61 and NIST SP 800-84 at Banco Popular.

Tyagi, P., Grima, S., Sood, K., Balamurugan, B., Özen, E., Thalassinos, E. (Eds.). 2023. Smart analytics, artificial intelligence and sustainable performance management in a global digitalised economy. Emerald Publishing Limited.

Velinov, E., Kadłubek, M., Thalassinos, E., Grima, S., Maditinos, D. 2023. Digital Transformation and Data Governance: Top Management Teams Perspectives. In: Digital Transformation, Strategic Resilience, Cyber Security and Risk Management (pp. 147-158). Emerald Publishing Limited.

Using Mean Time to Identify (MTTI) as a Service Desk Metric – BMC Software | Blogs.

Walasek, R. 2016. Systemy bezpieczeństwa informacji w przedsiębiorstwach logistycznych – wyniki badania. Wydawnictwo Logistyczne.

Zarządzanie incydentami bezpieczeństwa informacji w przedsiębiorstwie - Niebezpiecznik.pl.