sciendo

Strategic Approaches to Cybersecurity: The Role of the Security Operations Center

Alisa Bilal Zorić
Veleučilište s pravom javnosti Baltazar Zaprešić, Croatia
Matija Kalamir
Span, Croatia

Abstract

The Security Operations Center (SOC) plays a crucial role in protecting organizations from a wide range of cyber threats, ensuring security, integrity, and business continuity. In today's digital environment, where cyberattacks pose a daily threat, the SOC serves as a centralized hub for monitoring, analyzing, and promptly responding to security incidents. By integrating the latest technologies, highly trained experts, and well-defined operational processes, the SOC identifies threats, significantly reduces risk, and prevents potential security incidents. As cyber threats become increasingly sophisticated and destructive, this paper aims to raise awareness of the dangers these attacks pose, analyze their potential impact on business operations, and explore strategies for mitigating risk. It provides an in-depth examination of various strategic approaches to cybersecurity defense, with a particular focus on the SOC's role and effectiveness in reducing security risks. Additionally, it analyses the key processes and technologies that form the backbone of an effective SOC, how SOC enhances incident response, and how best practices for risk reduction are applied in practice. The research is based on years of personal experience working in a SOC, as well as a comprehensive review of recent scientific studies, industry reports, and case studies that offer insight into the latest approaches and tools in cybersecurity.

Keywords: Security Operations Center (SOC); cybersecurity; threat detection; incident response; risk Management

Paper type: Research article

Received: Apr 4, 2025
Accepted: Aug 15, 2025

DOI: 10.2478/crdj-2025-0007

Introduction

In today's digital world, cybersecurity is no longer merely a technical issue but a strategic imperative that determines the stability and resilience of organizations of all sizes. Rather than being seen as an operational cost, security should be regarded as a long-term investment in business success and protection. As data becomes one of the most valuable assets, its compromise can lead not only to significant financial losses but also to irreparable damage to an organization's reputation and customer trust. According to the World Economic Forum (2024), cyber threats rank among the top five global risks, underscoring the need to integrate cybersecurity into core business strategies.

The rapid advancement of digital technologies and the acceleration of digital transformation have significantly improved business processes by increasing operational efficiency and data accessibility. However, these advancements have also introduced new vulnerabilities that malicious actors can exploit through increasingly sophisticated cyberattacks. As threats grow more complex and destructive, organizations can no longer rely solely on passive or reactive security measures. Instead, proactive security strategies are required to ensure timely threat detection, analysis, and response.

In this context, the Security Operations Center (SOC) has become a critical component of modern cybersecurity frameworks. Its role extends beyond identifying and neutralizing attacks – it also focuses on prevention and risk reduction through continuous monitoring, data analytics, and the implementation of advanced security technologies. Previous research has shown that the maturity of a Security Operations Center (SOC) significantly influences its ability to detect, contain, and mitigate advanced cyber threats. Schlette et al. (2021) introduced the CTI-SOC2M2 maturity model, which evaluates SOC capabilities by integrating cyber threat intelligence (CTI) into operational workflows. Taqafi et al (2023) developed a maturity capability framework that assesses SOC performance across people, processes, and technology, highlighting that higher maturity levels lead to shorter Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) due to better process integration and automation. Forsberg et al. (2023) proposed a set of technical performance metrics to measure the qualitative and quantitative effectiveness of SOC detection and prevention mechanisms, including detection efficacy, rule precision, and the success rate of automated defensive actions. These studies underline that SOC maturity, supported by structured frameworks and rigorous performance measurement, directly contributes to improving an organization's defensive capabilities against evolving cyber threats.

This paper explores in depth the key concepts of cybersecurity defense, with a particular focus on the importance and operational functions of the SOC. Additionally, it analyses the challenges that SOCs face in today's complex cyber environment and examines emerging trends shaping the future of security strategies and practices. The research is based on secondary data sources, including recent reports from industry leaders (Microsoft, IBM, SANS, NIST) and the authors' own experience managing SOC

operations. Regulatory frameworks such as NIS2, GDPR, and ISO/IEC 27001 are also included to ensure alignment with current compliance standards.

The structure of the paper is as follows: after the introduction, the second section outlines the main components of cybersecurity defense strategy with a focus on regulatory frameworks and threat typologies. The third section analyses the concept, functions, and models of SOCs. The fourth section presents key operational challenges and emerging trends. The fifth section offers a brief discussion and critical reflection, and the conclusion summarizes the key findings and suggests directions for future research.

Cybersecurity Defense Strategy

The growing threat of cyberattacks affects organizations regardless of industry or size. According to Microsoft's 2023 report (Microsoft Digital Report, 2024), 70 % of organizations that fell victim to ransomware attacks had fewer than 500 employees, demonstrating that no entity is exempt from risk. These findings underscore the necessity of a systematic approach to cybersecurity, not only at the organizational level but also at national and international levels.

Raising awareness of the importance of cybersecurity among all organizational stakeholders is critical. The key pillar of this initiative is developing a comprehensive cybersecurity strategy aligned with business objectives. This strategy must encompass all security processes, including risk assessment, prevention, detection, incident response, and system recovery.

Acknowledging the need for stronger regulatory measures, the European Union has introduced the NIS2 Directive (Directive 2022/2555 of the European Parliament and the Council on Network and Information Security, 2023), designed to enhance organizational resilience against cyberattacks across the EU. Organizations covered by this directive must adopt additional security measures that reinforce cybersecurity as a strategic business priority. Similarly, numerous international regulations (GDPR, DORA, PCI DSS) and industry standards (ISO/IEC 27001, ISO/IEC 27002, COBIT) seek to ensure compliance and strengthen system resilience globally. According to the 2023 Cybersecurity Research Report (Rackspace Technology, 2024), conducted in collaboration with Microsoft, cybersecurity is the most significant business concern. This further highlights the urgency of investing in security strategies. An essential component of an effective cybersecurity posture is collaboration and information sharing regarding threats, attack methodologies, malicious actors, and mitigation techniques. The exchange of security intelligence between the private and public sectors, academic institutions, and research organizations enhances the efficiency of threat response and reduces system vulnerabilities.

Cybercriminals operate with diverse motives and objectives (SANS Institute, 2025; Microsoft Threat Intelligence, 2024), with the most prevalent being:

- State-sponsored actors, primarily engaged in cyber espionage, financial disruption, or reputational sabotage of targeted entities.
- Financially motivated cybercriminals, operating independently of state affiliations, focused on economic gain.
- Malware developers and cyber mercenaries, specializing in creating and distributing malicious software and offering cyberattack services to third parties.

Ransomware and data exfiltration remain the most prevalent cyberattack methods. According to the SANS 2023 Attack and Threat Report, the incidence of these attack vectors surged by 73% from 2022 to 2023. Social engineering, particularly phishing, remains the primary initial access vector. The integration of artificial intelligence (AI) has significantly advanced phishing techniques, making them more sophisticated and more complex to detect. While early phishing attempts often exhibited grammatical inconsistencies that exposed their fraudulent nature, AI-generated phishing campaigns now appear highly polished and convincing. Cybercriminals exploit AI and emerging technologies to refine their attack strategies, underscoring the need for enhanced defensive measures that combine expertise, experience, and state-of-the-art security solutions.

Absolute cybersecurity is unachievable; organizations must recognize that no entity is immune to cyber threats and adopt a proactive approach to risk mitigation and defense.

One of the most widely recognized cybersecurity frameworks is the NIST Cybersecurity Framework (National Institute of Standards and Technology, 2024), designed for organizations of all sizes and sectors. It encompasses six core functions illustrated in *Figure 1*, which provides a visual summary of how these functions interconnect to support a comprehensive cybersecurity strategy:

1. Govern – Establishes cybersecurity risk management strategy, defines responsibilities, and aligns security policies and processes with business objectives.
2. Identify – Focuses on understanding organizational risks related to cybersecurity, including the identification of critical assets, data, personnel, services, and systems, as well as assessing potential threats and vulnerabilities.
3. Protect – Implements security controls and measures to safeguard organizational systems, data, and assets from cyber threats.
4. Detect – Enables timely identification of cyber threats and incidents through continuous monitoring of security events and anomalies that may indicate a security breach.
5. Respond – Defines actions for mitigating the impact of cyber incidents, ensuring an effective and swift response.

6. Recover – Facilitates system restoration and operational continuity following an incident, minimizing business disruptions.

Figure 1. NIST Cybersecurity Framework functions

Source: National Institute of Standards and Technology

Given the ongoing need for continuous engagement and evaluation, many organizations opt to outsource security functions to specialized service providers, allowing them to focus on core business operations without compromising cybersecurity. This often involves establishing a Security Operations Centre (SOC) – a centralized unit responsible for real-time threat detection, advanced attack mitigation, rapid incident response, risk assessment, and system recovery. By integrating all NIST framework functions, the SOC enhances an organization's ability to detect, respond to, and recover from cyber threats effectively.

Security Operations Center – The Foundation of Cyber Defense

Establishing a Security Operations Center (SOC) is crucial for strengthening resilience against cyber threats. Given the increasing frequency and sophistication of attacks, adequate protection without SOC services is becoming nearly impossible. There are various definitions of SOC, but one of the most precise comes from IBM (Scapicchio et al., 2025): *"A SOC is a center that enhances an organization's ability to detect threats, respond to incidents, and prevent them by integrating and coordinating all cybersecurity technologies and operations."* This definition highlights that SOC represents a synergy of people, processes, and technologies, working together to ensure continuous evaluation and improvement of security measures. SOC implementation can take different forms, with the most common models being:

- Internal SOC – established within the organization
- Hybrid SOC – a combination of internal and external security capabilities

- SOC outsourcing – whole delegation of SOC functions to external service providers

According to research by Hubbard and Orlando (2024), the recommended SOC model varies by organization size. Organizations with more than 10,000 endpoints typically implement an internal SOC. Those managing between 1,000 and 10,000 endpoints often adopt a hybrid SOC, and smaller organizations, with fewer than 1,000 endpoints, generally rely on SOC outsourcing.

Regardless of an organization's size, an increasing number are choosing to outsource SOC operations, primarily for financial and operational reasons. Establishing an internal SOC requires significant investment in skilled personnel, advanced technologies, and continuous training of security teams. Beyond economic considerations, challenges include ensuring 24/7/365 monitoring, maintaining infrastructure, adapting security protocols, and continuously analyzing emerging threats. Due to the complexity and costs associated with maintaining an in-house SOC, organizations are increasingly turning to external SOC service providers. These providers assume full responsibility for people, processes, and technologies, delivering state-of-the-art security solutions aligned with global standards.

The growing demand for professional security solutions is reflected in market trends. According to the Grand View Research Market Analysis Report (2024), the global SOC services market was valued at $5.80 billion in 2023, with an expected average annual growth rate of 9.3% through 2030. These figures confirm the critical role of SOC in modern cybersecurity strategies, as organizations seek to enhance their defenses in an increasingly complex threat landscape.

Security Operations Centers – Key Challenges

Security Operations Centers (SOCs) face a range of challenges that can significantly affect their effectiveness and ability to respond to increasingly sophisticated cyber threats. Among the most pressing issues is the global shortage of cybersecurity professionals, a critical problem with far-reaching implications. According to the World Economic Forum (2024), there is currently a global shortage of approximately four million cybersecurity experts. The problem is not only a lack of interested personnel but also the difficulty of finding qualified professionals with the necessary knowledge, experience, and willingness to learn continuously. As technologies, processes, and attacker tactics evolve rapidly, security professionals must remain a step ahead to combat emerging threats effectively.

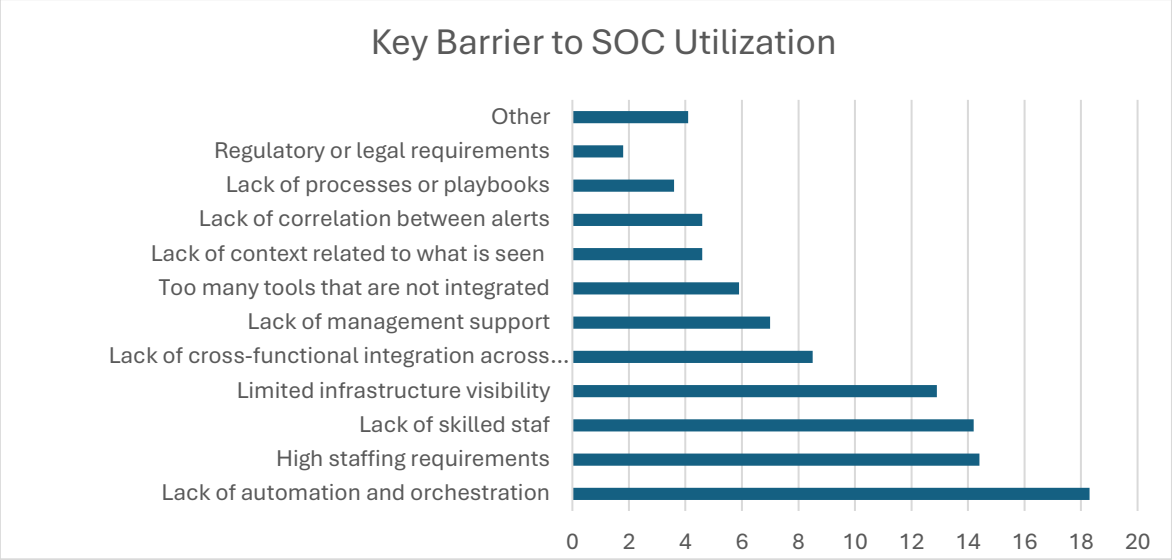
In their day-to-day work, SOC analysts often experience alert fatigue – a state of exhaustion caused by the overwhelming number of security alerts generated by various tools. This flood of alerts can reduce operational efficiency, lead to the oversight of critical incidents, and ultimately result in analyst burnout. To mitigate this issue, it is essential to advance security technologies to flag only high-impact alerts. A significant step in that direction is automating alert processing workflows.

Continual adaptation of security technologies presents a significant challenge for modern Security Operations Centers (SOCs). As attackers invest significant resources in developing advanced attack techniques, it is crucial that SOCs at least keep pace with these technological advancements—ideally, staying ahead of them.

Service providers managing SOCs also face challenges in collecting and analyzing data from heterogeneous environments, particularly in organizations that rely on legacy systems, hybrid IT architectures, or unregistered endpoints. Without complete visibility into all infrastructure components, SOCs cannot deliver comprehensive protection or a timely response to security threats.

These challenges were confirmed in the SANS 2024 SOC Survey (Crowley, 2025). The survey included 641 cybersecurity professionals, who identified key obstacles in SOC operations: a lack of automation and orchestration, high staffing demands, a shortage of skilled personnel, limited infrastructure visibility, and a lack of cross-functional integration across security, IR, and operations (Graph 1).

Graph 1 Key Barriers to SOC Utilization



Source: Author's work based on SANS 2024 SOC Survey

While the data itself is informative, its actual value lies in how these challenges manifest in real-world SOC environments. From the authors' experience managing SOC operations, the lack of automation and orchestration is not merely a technical shortfall – it is a systemic issue that affects the entire incident response lifecycle. Manual alert triage consumes valuable analyst time, increases the risk of human error, and contributes to alert fatigue. Implementing SOAR platforms and refining playbooks has proven to reduce this burden; however, success depends heavily on an organizational commitment to process maturity and cross-functional collaboration.

The shortage of skilled personnel is another critical challenge. It is not only a recruitment issue but also a retention and development problem. SOC analysts require

continuous training to keep pace with evolving threats, and without structured career paths and incentives, turnover rates remain high. The authors have observed that investing in internal knowledge-sharing programs and mentorship initiatives can significantly improve team stability and performance.

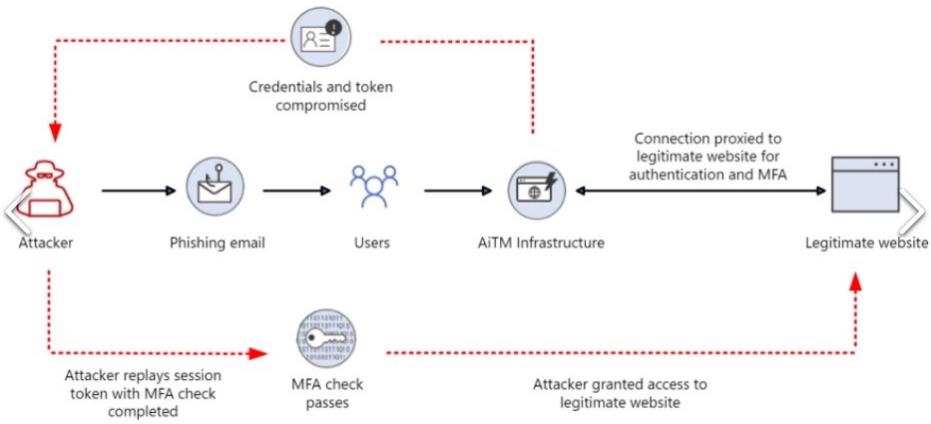
Limited infrastructure visibility often stems from legacy systems, hybrid architectures, and unregistered endpoints. In practice, this means that SOCs operate with blind spots, unable to correlate events across fragmented environments.

Security Operations Center – Practical Implementation

The primary functions of a Security Operations Center (SOC) are to detect security incidents and provide a rapid response. Organizations lacking continuous 24/7/365 security event monitoring significantly reduce their ability to detect threats early, thereby increasing the risk of severe system compromise. According to IBM's Cost of a Data Breach Report 2024, threat actors remain undetected within an organization for up to six months on average before executing an attack or achieving their ultimate objective. This highlights the critical importance of identifying anomalies and suspicious activity promptly to prevent major security breaches.

The following example illustrates the significance of continuous security monitoring and swift incident response. One of the most common attack vectors is the Adversary-in-the-Middle (AiTM) phishing attack—a sophisticated form of phishing in which a malicious actor intercepts communication between the victim and a legitimate website or service, thereby hijacking and compromising the victim's user account. In such attacks, the end user is typically unaware of malicious activity, as clicking a malicious link opens a legitimate-looking web page. The attacker exploits user inattention, intercepts the traffic, and steals the session token, thereby gaining unauthorized access not only to the intended service but also to all other services accessible via that token (Figure 2).

Figure 2: Adversary in the middle phishing attack



Source: Microsoft Threat Intelligence (2024)

It is important to note that such attacks are resistant to basic two-factor authentication. By compromising the user account, the attacker gains an initial base within the organization. For organizations without an established Security Operations Center (SOC), detecting this type of attack promptly would be highly challenging, if not impossible. The SOC's leading role in such cases is to identify anomalies and alerts that may indicate potential malicious activity. Relevant indicators in this scenario might include alerts such as Unfamiliar sign-in properties or a stolen session cookie being used, which point to suspicious logins or session hijacking attempts, particularly from foreign or unrecognized locations.

These types of attacks occur daily. Although security mechanisms and user education are important, they are often insufficient for comprehensive protection. The ultimate line of defense against sophisticated attacks lies in the SOC's ability to detect and contain threats early, thereby protecting not only individual user accounts but also the organization's entire IT infrastructure.

Discussion and conclusion

This paper explored the strategic positioning of the Security Operations Center (SOC) within an organization's broader cybersecurity framework and identified the factors that influence its effectiveness. The literature suggests that SOCs are no longer isolated technical units but are increasingly integrated into enterprise-wide risk management structures. This change requires organizations to move from reactive security models to proactive, intelligence-based defense. SOCs contribute to this shift by providing continuous situational awareness and serving as centers for threat analysis and coordinated response.

This paper emphasizes the importance of aligning SOC capabilities with business objectives, encompassing not only the deployment of advanced technologies (e.g., SIEM, SOAR, AI-based analytics) but also the development of interdepartmental collaboration, performance metrics, and security awareness across all organizational levels. SOC maturity depends not only on technological investment but also on the ability to embed cyber threat intelligence (CTI) into daily operations, address workforce skill gaps, and adapt processes to sector-specific regulatory demands. While maturity models and frameworks provide helpful guidance, practical implementation often faces constraints related to staffing, budgets, and integration complexity, especially in small and medium-sized enterprises.

However, certain limitations must be acknowledged. The analysis is conceptual and based on secondary sources, without direct empirical validation. Additionally, the generalizability of strategic SOC models may be constrained by sector-specific requirements, organizational maturity, and regulatory contexts. Operational metrics, such as Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR), are useful benchmarks, but they do not provide the complete picture of SOC effectiveness. They overlook factors such as detection accuracy and the effectiveness of automated responses. Adding qualitative indicators could help assess SOCs' actual defensive

capability more effectively. These aspects present valuable directions for future empirical research.

This paper highlights the importance of the Security Operations Center (SOC) as a key component of an organization's cybersecurity strategy. The analysis has shown that, in the context of increasingly sophisticated cyber threats, the establishment and operation of a SOC significantly contribute to the early detection of incidents, timely response, and continuous improvement of defense mechanisms. The main research question *is: How does SOC contribute to cybersecurity defense?* The topic was addressed through a structured overview of SOC components, their functions, and the benefits they provide. The findings confirm that organizations with a strategically implemented SOC are more effective in identifying and mitigating cyber risks. By presenting key elements, types of SOCs, and the challenges and trends associated with their development, this paper provides a foundation for a better understanding of SOCs' role in strengthening organizational resilience. However, the research is limited by the lack of primary empirical data.

Future research should focus on case studies and real-world performance metrics of SOC implementations across various industries, particularly in the context of integrating advanced technologies, such as artificial intelligence.

The paper concludes that building a SOC is not merely a technological upgrade, but a strategic imperative that requires adequate human resources and transparent processes with flexibility to adapt to evolving threats, regulatory requirements, and technological advancements.

References

1. Crowley, C. (2025). SANS Institute: *SANS 2024 SOC Survey: Facing Top Challenges in Security Operations* https://swimlane.com/wp-content/uploads/SANS-SOC-Survey_2024.pdf
2. Forsberg, J., & Frantti, T. (2023).. Technical performance metrics of a security operations center. *Computers & Security, 135*, 103529. https://doi.org/10.1016/j.cose.2023.103529
3. Grand View Research (2024). *Market Analysis Report 2023*: https://www.grandviewresearch.com/industry-analysis/managed-security-services-market
4. Hubbard, J. and Orlando, M. (2024). SANS: *Building and leading security operations centers:* https://www.sans.org/cyber-security-courses/building-leading-security-operations-centers/
5. IBM Reports. (2025). *Cost of a Data Breach Report 2024*, IBM reports: https://www.ibm.com/reports/data-breach
6. Microsoft Digital Report (2024). *Microsoft Digital Defense Report 2023 (MDDR)*: https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023
7. Microsoft Threat Intelligence (2024). *Research Threat intelligence Attacker techniques, tools, and infrastructure*: From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud, Microsoft Security Blog. https://www.microsoft.com/en-

us/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/

8. National Institute of Standards and Technology (2024). *The NIST Cybersecurity Framework (CSF) 2.0*: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
9. Rackspace Technology (2024). Rackspace Technology: *The 2023 Cybersecurity Research Report* https://www.rackspace.com/solve/2023-cybersecurity-research-report
10. Scapicchio, M., Downie A., Finio, M. (2025) *What is a SOC?* IBM: https://www.ibm.com/think/topics/security-operations-center
11. SANS Institute (2025) *SANS 2023 Attack and Threat Report* https://www.sans.org/white-papers/sans-2023-attack-threat-report/
12. Schlette, D., Vielberth, M., & Pernul, G. (2021). CTI-SOC2M2 - The quest for mature, intelligence-driven security operations and incident response capabilities. Computers & Security, 111, 102482. https://doi.org/10.1016/j.cose.2021.102482
13. Taqafi, I., Maleh, Y., & Ouazzane, K. (2023). A MATURITY CAPABILITY FRAMEWORK FOR SECURITY OPERATION CENTER. *EDPACS, 67*(3), 21-38. https://doi.org/10.1080/07366981.2023.2159047
14. World Economic Forum. (2024) *Global Cybersecurity Outlook 2024*: https://www.weforum.org/publications/global-cybersecurity-outlook-2024/

About the authors

Dr. sc. Alisa Bilal Zorić is a senior lecturer at the Polytechnic of Baltazar in Zaprešić, where she leads the undergraduate and graduate programs in Information Technologies and Applied Information Technologies. She holds a Ph.D. from the Faculty of Commercial and Business Sciences in Celje, Slovenia. Her research interests include mathematics, informatics, and IT, with a focus on their application in education and business. Dr. Zorić has published over 20 professional and scientific papers. She is an active member of the Croatian Mathematical Society and the Croatian Association for Artificial Intelligence. The author can be contacted at **abilal@bak.hr**.

Matija Kalamir is a graduate computer engineer with over 10 years of experience in the IT industry. He specializes in cybersecurity, with a strong focus on developing security solutions and managing Security Operations Centers (SOCs). Throughout his career, Matija has held leadership roles, including managing teams and projects to strengthen security infrastructure. With a deep understanding of both the technical and strategic aspects of IT, he is committed to ensuring secure, efficient systems in the ever-evolving digital landscape. The author can be contacted at **matija.kalamir@span.eu**.