ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҒЫЛЫМ
ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РЕСПУБЛИКИ КАЗАХСТАН
MINISTRY OF SCIENCE AND HIGHER EDUCATION
OF THE REPUBLIC OF KAZAKHSTAN

ҚАЗАҚСТАН ӨНДІРІС КӨЛІГІ

ПРОМЫШЛЕННЫЙ ТРАНСПОРТ КАЗАХСТАНА

INDUSTRIAL TRANSPORT OF KAZAKHSTAN

ISSN 1814-5787 (print)
ISSN 3006-0273 (online)

ХАЛЫҚАРАЛЫҚ
КӨЛІКТІК-
ГУМАНИТАРЛЫҚ
УНИВЕРСИТЕТІ

МЕЖДУНАРОДНЫЙ
ТРАНСПОРТНО-
ГУМАНИТАРНЫЙ
УНИВЕРСИТЕТ

2025 №3(87)

июль - сентябрь

«Қазақстан өндіріс көлігі» журналы
ISSN: 1814-5787 (print)
ISSN: 3006-0273 (online)
Меншік иесі: Халықаралық көлік-гуманитарлық университеті (Алматы қ.).
Қазақстан Республикасы Ақпарат және қоғамдық даму министрлігінде тіркелген. Тіркеу туралы куәлік № KZ27VPY00074524, 28.07.2023 ж. берілген.
Тақырып бағыты: Есептеу техникасы, ақпараттық жүйелер, электр энергетикасы және көлікті автоматтандыру.
Мерзімділігі: жылына 4 рет.
Тираж: 500 дана.
Редакция мекенжайы: Қазақстан, Алматы қ., Жетісу-1 ықшам ауданы, 32а үй.
Кон. Тел.: 8 (727) 376-74-78.
E-mail: info@mtgu.edu.kz
Журнал сайты: https://prom.mtgu.edu.kz

Журнал «Промышленный транспорт Казахстана»
ISSN: 1814-5787 (print)
ISSN: 3006-0273 (online)
Собственник: Международный транспортно-гуманитарный университет (г. Алматы).
Свидетельство о постановке на учет периодического печатного издания в Министерство информации и общественного развития Республики Казахстан № KZ27VPY00074524, выданное от 28.07.2023 г.
Тематическая направленность: вычислительная техника, информационные системы, электроэнергетика и автоматизация транспорта.
Периодичность: 4 раза в год.
Тираж: 500 экземпляров.
Адрес редакции: г. Алматы, мкрн. Жетысу-1, д. 32а. Кон. Тел.: 8(727) 376-74-78
E-mail: info@mtgu.edu.kz
Сайт журнала: http://prom.mtgu.edu.kz

Industrial Transport of Kazakhstan
ISSN: 1814-5787 (print)
ISSN: 3006-0273 (online)
Owner: International university of transportation and humanities (Almaty).
The certificate of registration of a periodical printed publication in the Ministry of Information and Social Development of the Republic of Kazakhstan, Information Committee KZ27VPY00074524, issued July 28, 2023.
Thematic focus: computer engineering, information systems, electrical power engineering, and transport automation.
Periodicity: 4 times a year.
Circulation: 500 copies.
Editorial address: Kazakhstan, Almaty, microdistrict Zhetysu-1, building 32a. Tel.: 8 (727) 376-74-78
E-mail: info@mtgu.edu.kz
Journal website: http://prom.mtgu.edu.kz

МАЗМҰНЫ

ЭЛЕКТР ЭНЕРГЕТИКАСЫ ЖӘНЕ КӨЛІКТІ АВТОМАТТАНДЫРУ

ЕСЕПТЕУ ТЕХНИКАСЫ ЖӘНЕ АҚПАРАТТЫҚ ЖҮЙЕЛЕР

СОДЕРЖАНИЕ

ЭЛЕКТРОЭНЕРГЕТИКА И АВТОМАТИЗАЦИЯ ТРАНСПОРТА

ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И ИНФОРМАЦИОННЫЕ СИСТЕМЫ

CONTENTS

ELECTRICAL POWER ENGINEERING AND TRANSPORT AUTOMATION

COMPUTER ENGINEERING AND INFORMATION SYSTEMS

ЕСЕПТЕУ ТЕХНИКАСЫ ЖӘНЕ АҚПАРАТТЫҚ ЖҮЙЕЛЕР / ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И ИНФОРМАЦИОННЫЕ СИСТЕМЫ / COMPUTER ENGINEERING AND INFORMATION SYSTEMS

Industrial Transport of Kazakhstan
ISSN 1814-5787 (print)
ISSN 3006-0273 (online)
Vol. 22. Is. 3. Number 87 (2025). Pp. 58–72
Journal homepage: https:// prom.mtgu.edu.kz
https://doi.org/ 10.58420.ptk.2025.87.03.005
UDC 004.056.53

SECURING SOCS: UNDERSTANDING VULNERABILITIES, THEIR IMPACT AND MITIGATION STRATEGIS

A.A. Altynbekov[1]*, G. Alin[2], S. Amanzholova[3], M. Saleh[4]
[1]International University of Information Technologies, Almaty, Kazakhstan;
[2]Astana IT University, Astana, Kazakhstan.
E-mail: 41378@iitu.edu.kz

Ali Altynbekov — master's degree student, faculty of computer technology and cybersecurity, International University of Information Technologies
E-mail: 41378@iitu.edu.kz. https:/orcid.org/0009-0001-5360-0128;
Galymzada Alin — Candidate of technical sciences, assistant professor at the CyberSecurity Department, International University of Information Technologies
E-mail: g.alin@iitu.edu.kz. https:/orcid.org/0000-0003-1028-5452;
Saule Amanzholova — Candidate of technical sciences, Associate professor, Cybersecurity, Astana IT University
E-mail: s.amanzholova@astanait.edu.kz. https:/orcid.org/0000-0002-6779-9393;
Mohammed Saleh — PhD, Associate Professor, Cybersecurity, International Information Technology University
E-mail: m.saleh@iitu.edu.kz. https:/orcid.org/0000-0003-4673-5056

Abstract. Security Operations Centers (SOCs) play a vital role in defending organizations against increasingly sophisticated cyber threats; however, they themselves remain vulnerable to weaknesses that can undermine their overall effectiveness. This review paper provides a comprehensive analysis of key vulnerabilities within SOC environments, evaluates their impact on threat detection and incident response capabilities, and explores effective mitigation strategies aimed at enhancing SOC resilience. By systematically examining existing academic literature, industry reports, and real-world case studies, the paper investigates both technical and organizational vulnerabilities that affect SOC performance. Common challenges identified include under-resourced teams, tool misconfigurations, inefficient incident response workflows, staffing shortages, and reliance on outdated technologies. The consequences of these vulnerabilities are discussed in relation to delayed threat detection, heightened risk of security breaches, and an overall decline in organizational cybersecurity posture. The review synthesizes best practices and recommended mitigation strategies, such as improving SOC staffing levels, enhancing tool interoperability, and implementing automation to streamline incident response. Furthermore, it highlights the potential of emerging technologies—particularly artificial intelligence (AI) and

machine learning (ML)—to strengthen SOC operations and improve adaptability to the evolving cyber threat landscape. Emphasis is also placed on the importance of robust communication protocols, continuous analyst training, and the integration of holistic security practices across all organizational layers. In conclusion, understanding and addressing vulnerabilities within SOCs is critical for sustaining effective cybersecurity defense. The study underscores the importance of harmonizing human expertise with technological innovation, demonstrating that such synergy significantly reinforces both preventive and responsive capabilities against emerging threats. Future research should further explore the application of AI and ML in SOCs to enhance agility and resilience in an ever-changing threat environment.

Keywords: soc, vulnerabilities, threat detection, automation, artificial intelligence (AI), machine learning (ML), resilience

For citation: A. Altynbekov, G. Alin, S. Amanzholova, M. Saleh. Securing socs: understanding vulnerabilities, their impact, and mitigation strategies//Industrial Transport of Kazakhstan. 2025. Vol. 22. No.87. Pp. 58–72. (In Russ.). https://doi.org/ 10.58420.ptk.2025.87.03.005

Conflict of interest: The authors declare that there is no conflict of interest.

SOC ҚАУІПСІЗДІГІ: ОСАЛДЫҚТАРДЫ, ОЛАРДЫҢ ӘСЕРІН ЖӘНЕ САЛДАРЫН АЗАЙТУ СТРАТЕГИЯЛАРЫН ТҮСІНУ

А.А. Алтынбеков[1], Г. Алин[2], С. Аманжолова[3], М. Салех[4]

[1]Халықаралық ақпараттық технологиялар университеті, Алматы, Қазақстан;
[2]Астана IT Университеті, Астана, Қазақстан.
E-mail: 41378@iitu.edu.kz

Али Алтынбеков — магистрант, Компьютерлік технологиялар және киберқауіпсіздік факультеті, Ақпараттық технологиялар халықаралық университеті
E-mail: 41378@iitu.edu.kz. https:/orcid.org/0009-0001-5360-0128;
Галымзада Алин — техника ғылымдарының кандидаты, киберқауіпсіздік кафедрасының ассистент профессоры, Халықаралық ақпараттық технологиялар университеті
E-mail: g.alin@iitu.edu.kz. https:/orcid.org/0000-0003-1028-5452;
Сауле Аманжолова — техника ғылымдарының кандидаты, Киберқауіпсіздік кафедрасының қауымдастырылған профессоры, Астана IT университеті
E-mail: s.amanzholova@astanait.edu.kz. https:/orcid.org/0000-0002-6779-9393;
Мохаммед Салех — PhD, Киберқауіпсіздік кафедрасының қауымдастырылған профессоры, Ақпараттық технологиялар халықаралық университеті
E-mail: m.saleh@iitu.edu.kz. https:/orcid.org/0000-0003-4673-5056.

Аннотация. Қауіпсіздік операциялары орталықтары (Security Operations Centers, SOCs) ұйымдарды барған сайын күрделі киберқауіптерден қорғауда шешуші рөл атқарады. Алайда олардың өздері де тиімділігіне нұқсан келтіретін осалдықтарға бейім болуы мүмкін. Бұл шолу мақаласында SOC орталарындағы негізгі осалдықтар жан-жақты талданады, олардың қауіптерді анықтау мен оларға жауап беру қабілетіне әсері бағаланады және SOC тұрақтылығын арттыруға бағытталған тиімді стратегиялар қарастырылады. Қолданыстағы ғылыми әдебиеттер, салалық есептер және нақты жағдайлар (кейстер) негізінде зерттеу SOC қызметіне әсер ететін техникалық және ұйымдастырушылық осалдықтарды жүйелі түрде талдайды. Анықталған негізгі мәселелерге ресурстардың жетіспеушілігі, құралдардың дұрыс конфигурацияланбауы, инциденттерге жауап беру процестерінің тиімсіздігі, кадр тапшылығы және ескірген технологияларды қолдану жатады. Бұл осалдықтардың салдары қауіптерді анықтаудың кешігуі, қауіпсіздік бұзылыстарының қаупінің артуы және ұйымның жалпы киберқауіпсіздік деңгейінің төмендеуі түрінде

көрінеді. Мақалада SOC кадрлық әлеуетін арттыру, құралдардың өзара интеграциясын күшейту және инциденттерге жауап беру үдерістерін автоматтандыру сияқты ұсынылған жұмсарту стратегиялары талданады. Сонымен қатар, жасанды интеллект (AI) пен машиналық оқыту (ML) технологияларының SOC жұмысын жетілдіру және дамып келе жатқан киберқауіптер ландшафтына бейімделу әлеуеті қарастырылады. Зерттеу сенімді коммуникация хаттамаларын құрудың, талдаушыларды үздіксіз оқытудың және ұйым деңгейлерінде қауіпсіздіктің тұтас тәсілдерін енгізудің маңыздылығына баса назар аударады. Қорытындылай келе, SOC жүйелеріндегі осалдықтарды түсіну және оларды жою ұйымның киберқауіпсіздік қорғанысын тиімді сақтау үшін аса маңызды. Мақалада адам капиталы мен технологиялық шешімдердің өзара үйлесімін қамтамасыз етудің маңыздылығы атап өтіледі. Мұндай синергия жаңа қауіптердің алдын алу мен оларға жедел жауап беру қабілетін едәуір күшейтеді. Болашақ зерттеулер SOC жүйелерінде жасанды интеллект пен машиналық оқыту технологияларын қолдану бағыттарын тереңірек зерттеуге бағытталуы тиіс.

Түйін сөздер: soc, осалдықтар, қауіптерді анықтау, автоматтандыру, жасанды интеллект, машиналық оқыту, төзімділік

Дәйексөздер үшін: А. Алтынбеков, Г. Алин, С. Аманжолова, М. Салех. SOC қауіпсіздігі: осалдықтарды, олардың әсерін және салдарын азайту стратегияларын түсіну//Industrial Transport of Kazakhstan. 2025. Том. 22. № 87. 58–72 бет. (Орыс тіл.). https://doi.org/ 10.58420.ptk.2025.87.03.005

Мүдделер қақтығысы: Авторлар осы мақалада мүдделер қақтығысы жоқ деп мәлімдейді.

ЗАЩИТА SOCS: ПОНИМАНИЕ УЯЗВИМОСТЕЙ, ИХ ВОЗДЕЙСТВИЯ И СТРАТЕГИЙ СМЯГЧЕНИЯ ПОСЛЕДСТВИЙ

А.А. Алтынбеков[1], Г. Алин[2], С. Аманжолова[3], М. Салех[4]

[1]Международный университет информационных технологий, Алматы, Казахстан;
Астана IT Университет, Астана, Казахстан.
E-mail: 41378@iitu.edu.kz

Али Алтынбеков — магистратрант, факультет компьютерных технологий и кибербезопасности, Международный университет информационных технологий
E-mail: 41378@iitu.edu.kz. https:/orcid.org/0009-0001-5360-0128;
Галымзада Алин — кандидат технических наук, ассистент профессор кафедры кибербезопасности, Международный университет информационных технологий
E-mail: g.alin@iitu.edu.kz. https:/orcid.org/0000-0003-1028-5452;
Сауле Аманжолова — кандидат технических наук, ассоциированный профессор кафедры кибербезопасности Астана IT-университет
E-mail: s.amanzholova@astanait.edu.kz. https:/orcid.org/0000-0002-6779-9393;
Мохаммед Салех — PhD, ассоциированный профессор кафедры кибербезопасности, Международный университет информационных технологий
E-mail: m.saleh@iitu.edu.kz. https:/orcid.org/0000-0003-4673-5056

Аннотация. Операционные центры обеспечения устойчивости (SOCs) имеют решающее значение для защиты организаций от все более изощренных киберугроз; однако они сами подвержены уязвимостям, которые могут поставить под угрозу их эффективность. В этом обзорном документе представлен всесторонний анализ ключевых уязвимостей в среде SOC, оценивается их влияние на возможности обнаружения и реагирования, а также

рассматриваются эффективные стратегии смягчения последствий для повышения устойчивости SOC. На основе систематического анализа существующей литературы, отраслевых отчетов и тематических исследований в документе рассматриваются как технические, так и организационные уязвимости, влияющие на производительность SOC. Выявленные общие проблемы включают нехватку ресурсов у команд, неправильную настройку инструментов, неэффективные процессы реагирования на инциденты, нехватку персонала и устаревшие технологии. Влияние этих уязвимостей обсуждается с точки зрения задержки обнаружения угроз, повышенного риска нарушений безопасности и общего ухудшения состояния кибербезопасности организации. В обзоре также обобщены рекомендуемые стратегии смягчения последствий, такие как повышение уровня укомплектованности SOC персоналом, усиление интеграции инструментов и внедрение технологий автоматизации для реагирования на инциденты. Кроме того, в обзоре рассматривается потенциал передовых технологий, таких как искусственный интеллект и машинное обучение, для улучшения функционирования SOC и адаптации к меняющемуся ландшафту киберугроз. Особое внимание уделяется созданию надежных коммуникационных протоколов, непрерывному обучению аналитиков и интеграции целостных методов обеспечения безопасности на различных уровнях организации. В заключение, понимание и устранение уязвимостей в SOCs имеет решающее значение для поддержания эффективной защиты от кибербезопасности. В документе подчеркивается необходимость скоординированных усилий по интеграции человеческого опыта с технологическими решениями, подчеркивая, как такая синергия способствует предотвращению и реагированию на возникающие угрозы. Будущие направления исследований включают дальнейшее изучение приложений искусственного интеллекта и машинного обучения в социальных сетях, чтобы лучше реагировать на постоянно меняющийся ландшафт угроз.

Ключевые слова: soc, уязвимости, обнаружение угроз, автоматизация, искусственный интеллект, машинное обучение, устойчивость

Для цитирования: А. Алтынбеков, Г. Алин, С. Аманжолова, М. Салех. защита socs: понимание уязвимостей, их воздействия и стратегий смягчения последствий//Industrial Transport of Kazakhstan. 2025. Т. 22. No. 87. Стр. 58–72. (На русс.). https://doi.org/10.58420.ptk.2025.87.03.005

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Introduction.

In the digital age, organizations face increasingly sophisticated cyber threats, ranging from zero-day exploits and ransomware attacks to state-sponsored intrusions targeting IT infrastructures (Riggs, 2023: 1–26; Aslan, 2017: 222–225: 222–225; Demertzis, 2018: 1–17). The rapid evolution of these threats has highlighted the crucial role of Security Operations Centers (SOCs)—centralized units responsible for continuous monitoring, threat detection, and incident response (Agyepong, 2020: 88–105; Muniz, 2015). SOCs integrate skilled analysts, advanced tools, and structured workflows to establish resilient cybersecurity defenses (Onwubiko, 2019b: 11–39; Vielberth, 2020: 227756–227779).

Despite their strategic importance, SOCs face persistent technical and organizational vulnerabilities that compromise their effectiveness. Technical issues, such as tool misconfigurations, poor system interoperability, and outdated infrastructure, hinder timely threat detection and response (Banati, 2022: 143–147; Kiselev, 2022: 39–51). Organizational factors—including staff shortages, high turnover, skill gaps, and weak communication—further reduce SOC performance (Reeves, 2023: 1–11; Kokulu, 2019: 1955 - 1970). These vulnerabilities create exploitable gaps for attackers, potentially leading to financial losses, reputational damage, and regulatory penalties (Anton, 2003: 50; Resilience, 2024:1–22). Although SOCs are critical to cybersecurity, comprehensive research addressing internal vulnerabilities and mitigation strategies

remains limited (Vielberth, 2020: 227756–227779; Taqafi, 2023: 21–38). This knowledge gap justifies the focus of the present study.

The relevance of this research lies in its potential to enhance SOC design, strategic management, and operational resilience. By systematically examining both technical and organizational vulnerabilities, the study contributes to the development of evidence-based strategies that integrate human expertise, advanced tools, and emerging technologies such as artificial intelligence (AI) and machine learning (ML) (Aslan, 2017: 222–225; Demertzis, 2018: 1–17). The study's findings are expected to provide practical guidance for organizations seeking to strengthen cybersecurity infrastructure and improve incident response capabilities.

Object of study: Security Operations Centers (SOCs) and their role in organizational cybersecurity.

Subject of study: Internal vulnerabilities affecting SOC effectiveness, including technical and organizational aspects, and strategies for their mitigation.

Focus: How SOC vulnerabilities influence threat detection and response, and the potential role of advanced technologies in mitigating these weaknesses.

Aim: To investigate the internal vulnerabilities of SOCs and propose strategies to enhance their resilience and operational effectiveness.

Objectives:

- Identify and categorize technical and organizational vulnerabilities within SOCs.
- Analyze the impact of these vulnerabilities on threat detection and incident response.
- Examine mitigation strategies, including AI and ML applications, to enhance SOC performance.
- Provide recommendations for improving SOC resilience through integrated technological and human-centered approaches.

The study employs a systematic literature review of peer-reviewed publications, industry reports, and case studies to gather comprehensive insights into SOC vulnerabilities. Databases such as Google Scholar, IEEE Xplore, and Scopus were used to identify relevant sources. Inclusion criteria focused on English-language publications addressing SOC vulnerabilities, mitigation strategies, and the application of AI and ML. A two-stage screening process (titles/abstracts followed by full-text review) ensured rigorous selection. Qualitative synthesis allowed identification of recurring patterns, gaps, and best practices.

Effective mitigation of SOC vulnerabilities requires an integrated approach that combines technological solutions (e.g., AI/ML, automation) with human-centered strategies (e.g., continuous training, optimized staffing, and structured communication) to enhance detection capabilities and overall resilience.

This study provides a structured framework for understanding SOC vulnerabilities, their operational impacts, and applicable mitigation strategies. By bridging the gap between technical and organizational perspectives, it informs the development of adaptive, resilient, and future-ready SOC architectures capable of countering evolving cyber threats.

Materials and methods.

This study adopted a structured approach to collect and analyze literature on vulnerabilities within Security Operations Centers (SOCs) and their mitigation strategies. The review encompassed scholarly research, industry reports, and case studies to ensure a comprehensive perspective.

Sources were identified using platforms such as Google Scholar, IEEE Xplore, and Scopus, which provided access to peer-reviewed publications and technical literature on SOCs. AI tools were also employed to identify and summarize recent studies, ensuring coverage of the latest cybersecurity developments.

Inclusion criteria targeted English-language publications, focusing on peer-reviewed articles, industry reports, and studies involving SOC vulnerabilities and mitigation—particularly those referencing artificial intelligence (AI) and machine learning (ML). Irrelevant or low-quality

publications were excluded. Search terms included “SOC vulnerabilities,” “cybersecurity impact,” and “mitigation strategies,” combined using Boolean operators.

After eliminating duplicates, a two-stage screening process was applied: first by titles and abstracts, then through full-text review. Selected studies were categorized into themes such as technical flaws (e.g., outdated tools), organizational challenges (e.g., staff shortages), performance impacts, and mitigation methods like automation and AI. All steps are shown in Figure 1.

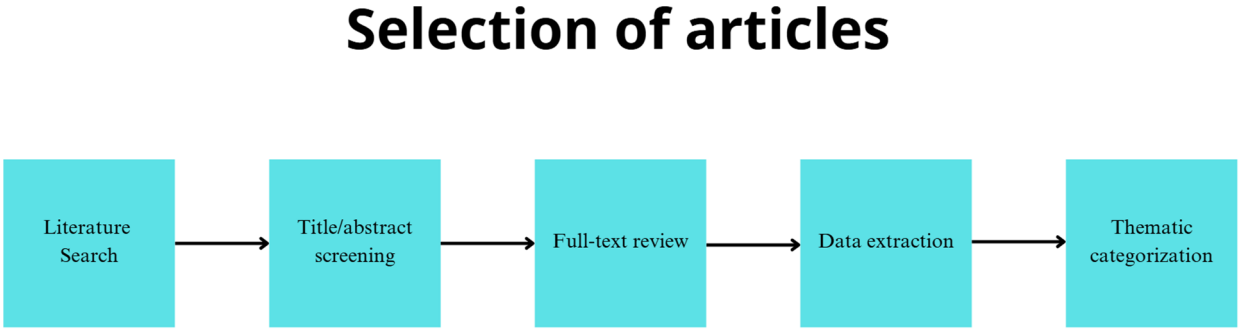

Fig. 1. Selection of articles

Data extraction focused on identifying how vulnerabilities affect key SOC functions such as threat detection and response. The review highlighted strategies—particularly AI/ML applications—used to enhance SOC efficiency and adaptability. A qualitative synthesis identified recurring patterns and knowledge gaps, offering deeper insight into how these vulnerabilities collectively impact SOC effectiveness.

Acknowledged limitations include potential bias due to language restrictions and the exclusion of unpublished organizational insights. Moreover, the rapid evolution of cybersecurity may affect the timeliness of some findings.

Ethical research practices were maintained throughout the study, including proper citation of all sources and adherence to academic integrity standards. This methodology ensures a rigorous and transparent analysis of SOC vulnerabilities and corresponding mitigation approaches.

Results and Discussions.

Security Operations Centers (SOCs) are central to an organization’s cybersecurity framework, providing real-time threat detection and response. Despite their critical importance, SOCs face technological, procedural, and human-related challenges that can compromise their performance. Addressing these issues requires a holistic approach that integrates process optimization, technological advancement, and human expertise.

Numerous studies have explored SOC design and improvement strategies. Agyepong et al. (2020) and Muniz et al. (2015) offer foundational insights into SOC implementation and operation, emphasizing their essential role in safeguarding organizational assets. Anton et al. (2003) propose a structured vulnerability assessment framework, while Aslan and Samet (2017) advocate for proactive defense mechanisms through increased vulnerability awareness. Hore et al. (2023) stress the importance of effective triage and prioritization of cyber threats, and Degrass (2022) introduces innovative vulnerability remediation techniques.

To enhance SOC performance, Banati et al. (2022) explore the use of attack graphs as tools to visualize threats and improve response efficiency. Demertzis et al. (2018) propose a cognitive SOC model that leverages cybersecurity intelligence and forensic analysis to accelerate decision-making. Practical implementation challenges are discussed by Kiselev et al. (2022), who share real-world SOC deployment experiences, while Kokulu et al. (2019) analyze organizational mismatches that reduce SOC efficiency. Janos and Dai (2018) identify common SOC security gaps requiring strategic mitigation.

Human factors also play a crucial role. Reeves and Ashenden (2023) examine SOC decision-making processes and recommend the use of cyber deception technologies to improve detection capabilities. Taqafi et al. (2023) introduce a maturity capability model for systematic

SOC evaluation. Vielberth et al. (2020) synthesize existing research and highlight ongoing operational and academic challenges in the SOC field.

Furthermore, Riggs et al. (2023) analyze the role of SOCs in protecting critical infrastructure, linking vulnerabilities to potential systemic disruptions. Resilience (2024) discusses strategies for adapting SOCs to evolving cyber threats and ensuring robust resilience. Onwubiko (2019b) emphasizes the need for strong situational awareness and continuous monitoring, while Onwubiko and Ouazzane (2019) address structural and technological integration challenges in SOC development.

Collectively, the reviewed studies reflect the dynamic evolution of SOCs and the continuous efforts to counter emerging cybersecurity threats. They underscore the importance of proactive vulnerability management, advanced detection techniques, and the integration of human expertise to improve SOC effectiveness. As threats become increasingly complex, these insights form a critical foundation for building resilient and adaptive security operations.

Table 1. Summary of Key Contributions and Relevance of Reviewed SOC Literature

Source/Author(s)	Key Contribution	Relevance to SOC Challenges
Agyepong et al.	Overview of SOC concepts and implementation strategies	Critical role in organizational security frameworks
Anton et al.	Vulnerability Assessment and Mitigation Methodology	Systematic approach to identify and mitigate risks
Aslan and Samet	Proactive defense mechanisms for mitigating vulnerabilities	Strengthens cybersecurity postures
Banati et al.	Use of attack graphs to enhance SOC operations	Improves threat detection and response efficiency
Degrass	Innovative techniques for operational vulnerability remediation	Contributes to proactive security measures
Demertzis et al.	Next-generation cognitive SOC using network flow forensics	Enhances decision-making and response times
Hore et al.	Optimal triage and mitigation of context-sensitive vulnerabilities	Efficient threat prioritization and resource allocation
Janos and Dai	Insights into security concerns related to SOCs	Highlights vulnerabilities and improvement areas
Kiselev, Korotkikh, and Shott	Practical experiences in establishing SOCs	Best practices and common pitfalls in SOC implementation
Kokulu et al.	Qualitative study on SOC challenges and solutions	Addresses mismatches and challenges in SOC operations
Muniz, McIntyre, and AlFardan	Practical aspects of building, operating, and maintaining SOCs	Insights for robust security infrastructures
Onwubiko	Importance of situational awareness and threat intelligence	Supports effective monitoring and cyber defense
Ouazzane and Onwubiko	Challenges in building effective SOCs	Focus on structure, resources, and advanced technologies
Reeves and Ashenden	Decision-making processes in SOCs with cyber deception technology	Enhances threat detection and response strategies
Resilience	Strategies for enhancing SOC resilience	Adaptation strategies for evolving threats
Riggs et al.	Mitigation strategies for vulnerabilities in critical infrastructure	Focus on safeguarding critical services
Taqafi, Maleh, and Ouazzane	Maturity capability framework for assessing SOC effectiveness	Systematically assesses and improves SOC effectiveness
Vielberth et al.	Systematic study identifying open challenges in SOCs	Emphasizes need for continuous SOC development

The systematic review of the literature provided a comprehensive understanding of the vulnerabilities affecting Security Operations Centers (SOCs), their overall impact on organizational cybersecurity, and the strategies available for their mitigation. The findings are categorized into three main groups, as illustrated in Figure 2:

- Technical vulnerabilities,

- Organizational vulnerabilities, and
- Mitigation strategies, including the potential application of advanced technologies such as artificial intelligence (AI) and machine learning (ML).

This classification framework facilitates a clearer analysis of how different types of vulnerabilities interact and influence SOC performance, while also highlighting innovative approaches that can enhance operational resilience and efficiency.

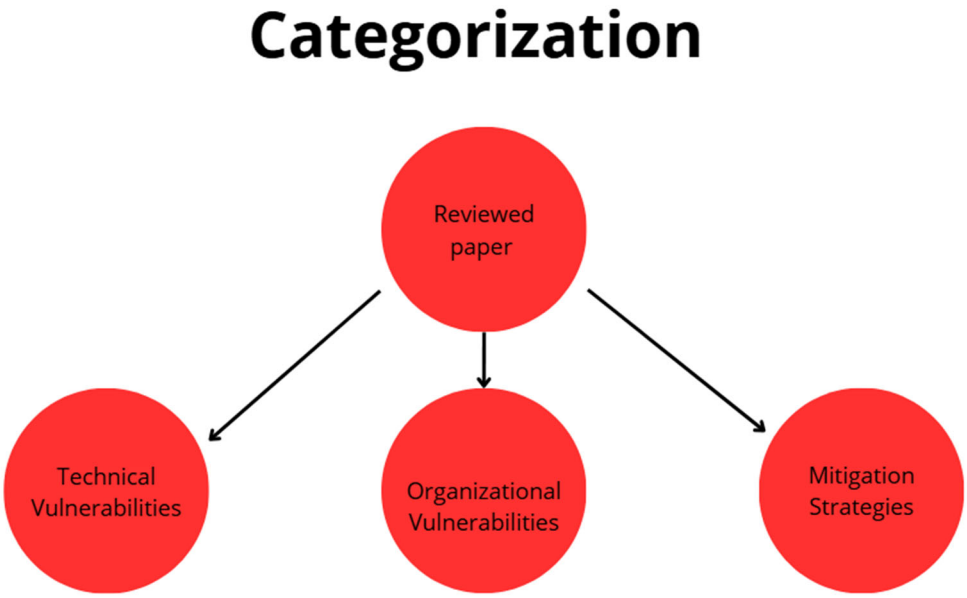

Fig. 2. Categorization of revied papers

Technical Vulnerabilities in SOCs

One of the most prevalent technical vulnerabilities identified is the misconfiguration of security tools within SOCs. Misconfigurations can create blind spots in security monitoring, allowing threats to go undetected (Banati, 2022: 143–147; Kiselev, 2022: 39–51). Banati et al. highlight that the improper setup of intrusion detection systems and firewalls can result in false negatives, where malicious activities are not flagged, thereby compromising the organization's overall security posture (Banati, 2022: 143–147).

The integration of disparate security tools also presents a significant challenge. Many SOCs rely on multiple security solutions that fail to communicate seamlessly with each other, resulting in data silos and inefficient incident response processes (Demertzis, 2018: 1–17). Demertzis et al. emphasize that this lack of interoperability limits the SOC's ability to correlate events across different platforms, reducing the overall effectiveness of threat detection and analysis (Demertzis, 2018: 1–17).

Dependence on outdated technologies and legacy systems represents another critical vulnerability. Legacy infrastructure often lacks the features necessary to address modern cyber threats and may not receive timely security updates, rendering it more susceptible to exploits (Kiselev, 2022: 39–51). Kiselev et al. note that such outdated systems can hinder the adoption of innovative security solutions, limiting the SOC's capability to counter advanced persistent threats (Kiselev, 2022: 39–51).

Organizational Vulnerabilities in SOCs

Under-resourced teams are among the most common organizational vulnerabilities within SOCs. Insufficient staffing leads to analyst fatigue, decreased morale, and an increased likelihood of oversight in monitoring activities (Kokulu, 2019: 1955 - 1970; Onwubiko, 2019a: 1–10). Kokulu et al. found that staffing shortages directly contribute to delayed incident responses and reduced overall efficiency in security operations (Kokulu, 2019: 1955 - 1970).

The cybersecurity industry also experiences high turnover rates due to factors such as burnout, intense job market competition, and limited career development opportunities. High turnover disrupts team cohesion and leads to the loss of institutional knowledge, thereby weakening SOC effectiveness (Janos, 2018: 273–278; Reeves, 2023: 1–11). Reeves and Ashenden emphasize that retaining skilled personnel is crucial for maintaining a resilient and high-performing SOC (Reeves, 2023: 1–11).

A lack of continuous training and professional development leaves SOC analysts unprepared to manage emerging threats. Without up-to-date knowledge of new attack vectors and evolving security technologies, analysts may fail to detect or appropriately respond to incidents (Agyepong et al., 2020).

Effective communication is also essential for coordinated incident response. The absence of clear communication protocols within the SOC and between departments can lead to confusion and delayed actions during critical incidents (Kokulu, 2019: 1955 - 1970; Onwubiko, 2019a: 1–10). Kokulu et al. emphasize that organizational silos hinder information sharing, which is vital for timely and effective response efforts (Kokulu, 2019: 1955 - 1970).

Impact of SOC Vulnerabilities on Detection and Response Capabilities

The identified vulnerabilities significantly affect SOCs' ability to detect and respond to cyber threats efficiently. Both technical and organizational weaknesses contribute to slower identification and remediation of security incidents. Delayed threat detection provides attackers with more time to infiltrate systems, exfiltrate data, and cause extensive damage (Anton et al., 2003; Resilience, 2024:1–22).

Figure 3 illustrates the average detection times across industries based on findings by Anton et al. and Resilience (Anton et al., 2003; Resilience, 2024:1–22). For instance, the healthcare industry reports the longest average detection time—approximately 211 days. Such prolonged delays highlight the critical need for enhanced SOC processes and technologies to ensure timely identification of security breaches.

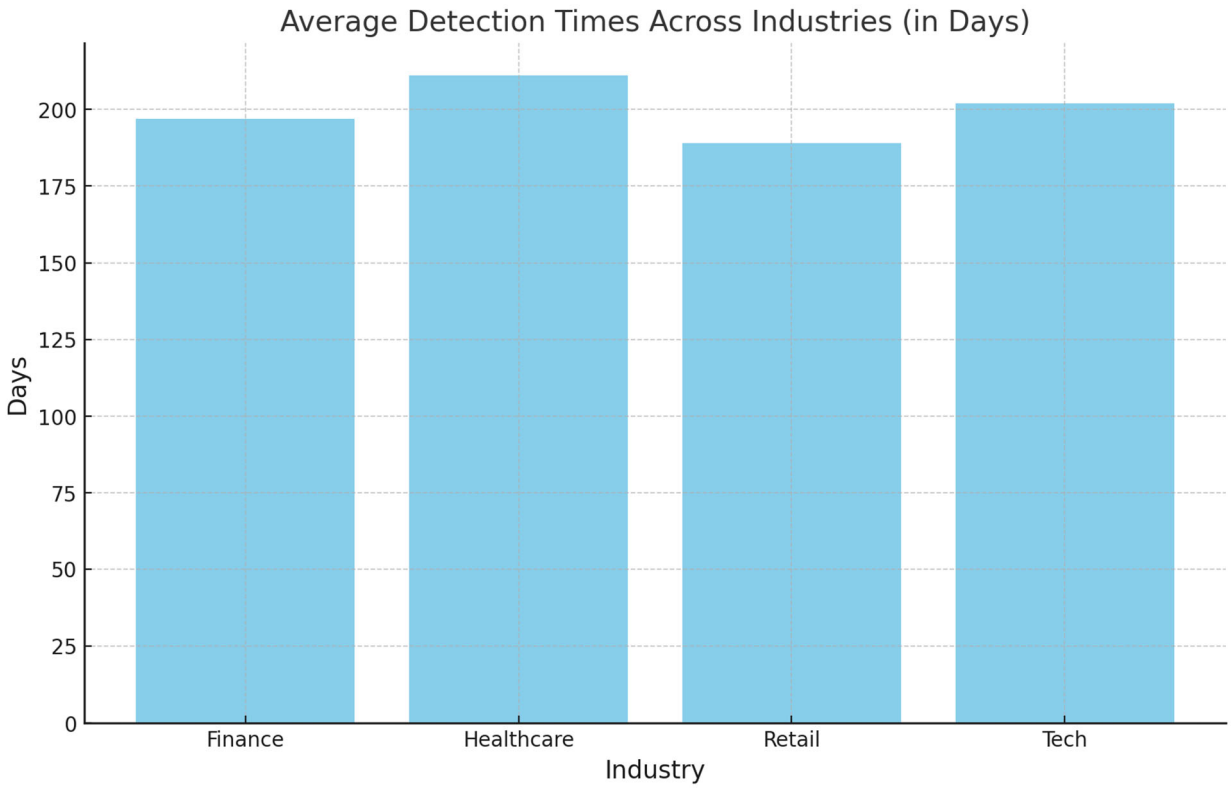

Fig. 3. Average Detection Times Across Industries

Anton et al. (2003) indicate that timely detection is critical for minimizing the overall impact of security breaches. Vulnerabilities within SOCs heighten the likelihood of successful cyberattacks, as inefficient processes and inadequate defenses create exploitable opportunities for adversaries. Such weaknesses can result in severe financial losses, reputational harm, and erosion of stakeholder trust (Riggs, 2023: 1–26). Riggs et al. further emphasize that compromised SOCs can trigger cascading effects across critical infrastructure protection systems, amplifying the broader consequences of cyber incidents (Riggs, 2023: 1–26).

The financial cost of delayed detection is substantial. Resilience (2024) reports that organizations suffering major data breaches face average expenses of approximately $4.45 million per incident. These costs encompass legal fees, regulatory fines, loss of revenue, and expenditures on containment and remediation. The magnitude of these losses reinforces the urgent need for investment in advanced detection technologies, improved automation, and continuous staff training.

Figure 4 presents the cost breakdown of data breaches as reported by Resilience (2024). Lost revenue constitutes the largest share (33.7%), followed by legal and regulatory expenses (27.0%). These statistics underscore the financial and operational urgency of addressing SOC vulnerabilities to prevent long-term economic and reputational damage.

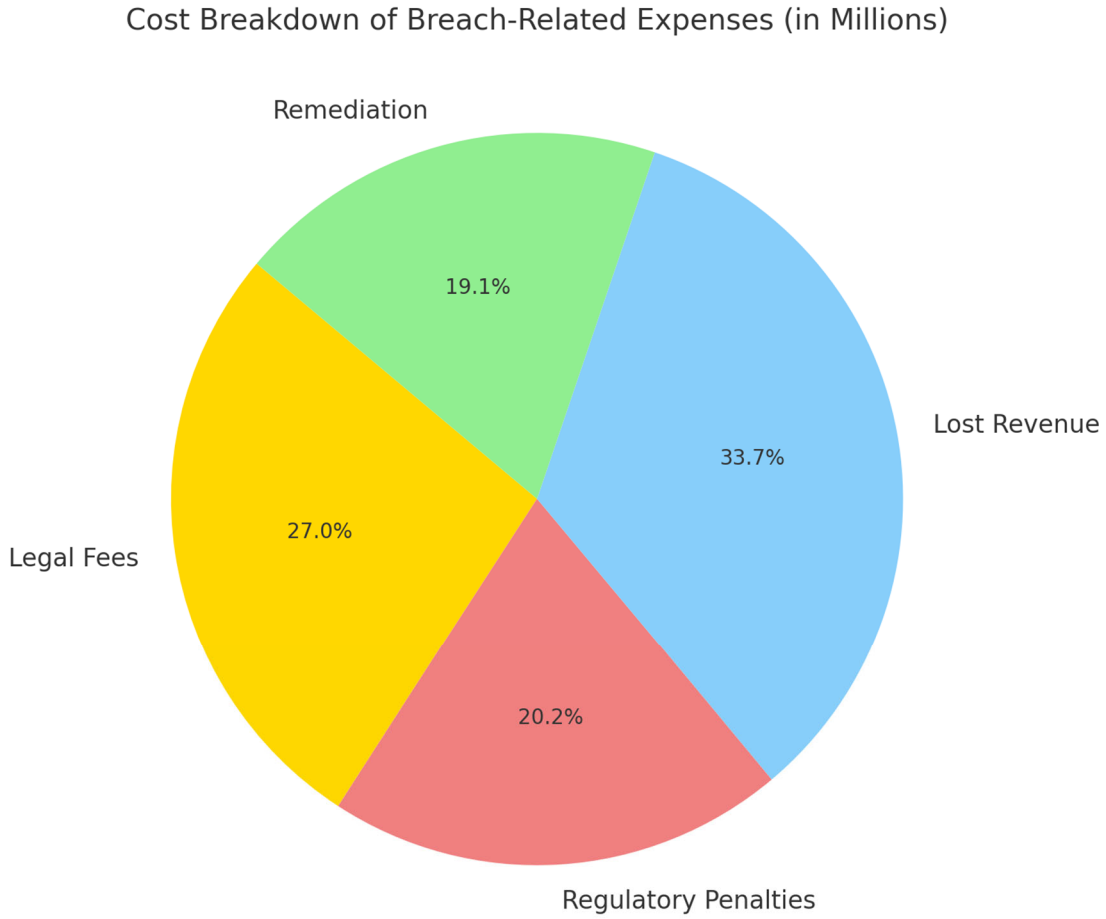

Fig. 4. Cost Breakdown of Breach-Related Expenses (in Millions)

PPersistent vulnerabilities erode the overall cybersecurity posture of an organization. A weakened SOC is unable to adequately protect assets, ensure regulatory compliance, or maintain stakeholder trust (Onwubiko, 2019b: 11–39; Vielberth, 2020: 227756–227779). Vielberth et al. note that organizations with vulnerable SOCs exhibit lower resilience to cyber threats and face greater challenges in recovering from security incidents (Vielberth, 2020: 227756–227779).

Mitigation Strategies for Enhancing SOC Resilience

The literature identifies several strategies to address the aforementioned vulnerabilities and improve SOC performance.

Addressing staffing shortages requires not only hiring additional personnel but also optimizing workforce allocation. Implementing flexible staffing models and engaging remote analysts can expand coverage and reduce employee burnout (Onwubiko, 2019a: 1–10; Taqafi, 2023: 21–38). Taqafi (2023) propose a maturity capability framework to systematically assess and enhance staffing effectiveness within SOC environments.

Investing in security platforms that support interoperability and centralized management can mitigate technical vulnerabilities related to tool misconfigurations and integration issues (Demertzis, 2018: 1–17).

Automation plays a critical role in reducing the manual workload of analysts, allowing them to focus on complex threat investigations. Implementing automated incident response workflows and leveraging security orchestration tools can streamline operations, minimize response times, and reduce the likelihood of human error (Banati, 2022: 143–147; Degrass, 2022: 1–14). Degrass highlights the effectiveness of automation in enabling proactive vulnerability remediation (Degrass, 2022: 1–14).

The application of artificial intelligence (AI) and machine learning (ML) offers significant potential for strengthening SOC capabilities. These technologies can analyze large volumes of data to detect patterns indicative of cyber threats, predict potential vulnerabilities, and recommend mitigation measures (Aslan, 2017: 222–225; Demertzis, 2018: 1–17). Aslan and Samet (2017) emphasize that AI-driven solutions can augment human expertise by enhancing real-time threat detection and incident response mechanisms.

Investing in continuous training programs ensures that SOC personnel remain up to date with emerging threats and technologies. Certifications, workshops, and simulation exercises help analysts strengthen their technical skills and confidence in incident management (Agyepong, 2020: 88–105). Onwubiko (2019b) underscores the importance of education in developing situational awareness and effective monitoring capabilities.

Developing standardized communication procedures fosters better coordination within the SOC and across organizational departments. Regular meetings, incident debriefings, and collaborative communication platforms can enhance information sharing and improve response efficiency (Kokul., 2019; Reeves, 2023: 1–11). Reeves and Ashenden (2023) advocate for integrating communication frameworks directly into SOC workflows to strengthen decision-making and operational consistency.

Potential of Advanced Technologies in SOC Operations

The integration of advanced technologies such as AI and ML is emerging as a cornerstone strategy for enhancing SOC resilience and adaptability.

Figure 5 illustrates the adoption rates of AI and ML technologies as reported by Aslan and Samet (2017), Demertzis et al. (2018), and Hore et al. (2023). The timeline demonstrates the progression from basic vulnerability awareness in 2017 to the implementation of sophisticated predictive analytics in 2023. This evolution highlights the growing reliance on intelligent technologies to enhance SOC operations, automate analysis, and improve the speed and accuracy of cyber defense mechanisms.

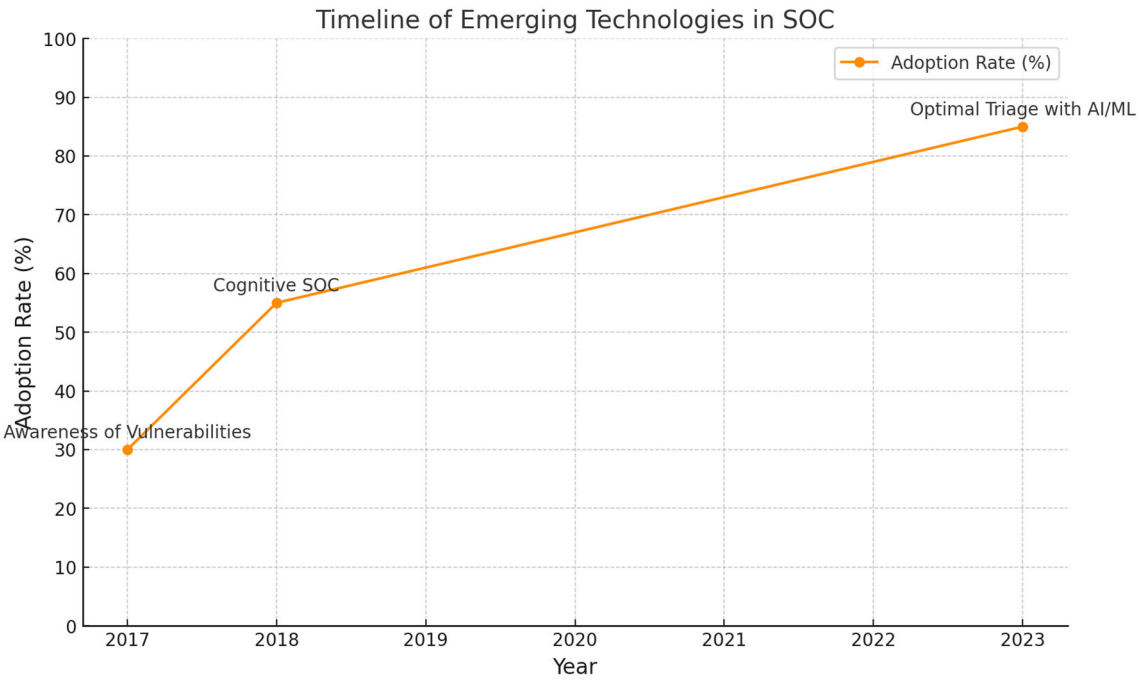

Fig. 5. Timeline of Emerging Technologies in SOC

AI and ML can process vast datasets to identify patterns and anomalies indicative of potential security threats. Predictive analytics enable SOCs to anticipate attacks and proactively reinforce their defenses (Demertzis, 2018: 1–17; Hore, 2023). Hore et al. demonstrate how ML algorithms can optimize vulnerability triage and mitigation efforts, improving prioritization accuracy and reducing remediation time (Hore, 2023).

Machine learning models can automate routine operational tasks such as alert prioritization and initial incident response. This automation accelerates response times and enables human analysts to focus on complex threat investigations (Degrass, 2022: 1–14; Vielberth, 2020: 227756–227779). Vielberth et al. discuss the emergence of cognitive SOCs that leverage AI for intelligent decision-making and adaptive security management (Vielberth, 2020: 227756–227779).

AI technologies augment human capabilities by providing actionable insights and recommendations, effectively bridging gaps caused by staffing shortages or skill limitations (Aslan, 2017: 222–225; Demertzis, 2018: 1–17). Aslan and Samet highlight that AI is not a replacement for human analysts but a force multiplier that enhances their ability to manage threats more effectively (Aslan, 2017: 222–225).

The results of this review underscore the multifaceted nature of SOC vulnerabilities—spanning both technical and organizational dimensions. These weaknesses significantly impair detection and response efficiency, underscoring the need for comprehensive mitigation strategies. Integrating improvements in staffing, technology interoperability, automation, and analyst training is essential for strengthening SOC resilience. The adoption of AI and ML represents a promising avenue for advancing SOC capabilities, offering powerful tools to manage the growing scale and complexity of cyber threats.

Technical and organizational vulnerabilities collectively hinder SOC effectiveness. Misconfigured tools, fragmented systems, and limited automation reduce situational awareness and extend incident response times. Without structured workflows and real-time threat intelligence integration, SOC teams struggle to maintain operational efficiency and consistency.

The reviewed literature indicates that adopting cognitive SOC architectures and AI-based triage systems can substantially improve detection speed and analytical accuracy. However,

human-centric challenges—such as staff burnout, limited training opportunities, and weak communication channels—must also be addressed to ensure effective and sustainable operations.

Organizational readiness and strategic alignment play a critical role in enhancing SOC resilience. Implementing maturity capability models and continuous improvement frameworks enables organizations to identify performance gaps and optimize resource allocation.

Cross-sector experiences from critical infrastructure, financial institutions, and large enterprises emphasize the importance of building adaptable and scalable SOC architectures. Long-term investment in both technical automation and human capacity development is key to transforming SOCs from reactive monitoring hubs into proactive defense centers capable of anticipating and neutralizing emerging threats.

Conclusion.

This study systematically examined the internal vulnerabilities of Security Operations Centers (SOCs), their impact on organizational cybersecurity, and potential mitigation strategies. The research aimed to identify both technical and organizational weaknesses within SOCs, assess how these vulnerabilities affect threat detection and response, and explore advanced solutions, including artificial intelligence (AI) and machine learning (ML), for enhancing SOC performance.

Implementation of Research Goals and Methods

The objectives of the study were successfully addressed through a structured literature review methodology. Peer-reviewed publications, industry reports, and case studies were analyzed to capture a comprehensive view of SOC vulnerabilities and mitigation approaches. Databases such as Google Scholar, IEEE Xplore, and Scopus were used to collect relevant studies. Inclusion and exclusion criteria ensured the quality and relevance of selected sources, while a two-stage screening process—first by titles and abstracts, then through full-text review—allowed systematic classification of information. Thematic categorization focused on technical vulnerabilities (e.g., tool misconfigurations, legacy systems), organizational vulnerabilities (e.g., staffing shortages, skill gaps, weak communication), and mitigation strategies (e.g., automation, AI/ML integration, training programs). Qualitative synthesis was employed to identify recurring patterns, knowledge gaps, and emerging best practices.

The analysis revealed that technical vulnerabilities remain a significant challenge for SOCs. Misconfigurations of security tools, lack of interoperability among platforms, and reliance on outdated infrastructure directly impair threat detection and incident response. These technical gaps create blind spots that adversaries can exploit, delaying incident identification and prolonging exposure to cyberattacks.

Organizational vulnerabilities were found to be equally critical. Staffing shortages, high personnel turnover, and insufficient professional training reduce operational efficiency and threaten timely response to incidents. Ineffective communication within SOCs and across organizational departments further exacerbates these challenges. Collectively, these vulnerabilities compromise the SOC's ability to maintain continuous situational awareness and respond proactively to emerging threats.

The study also highlighted the importance of advanced technologies in mitigating SOC vulnerabilities. AI and ML applications provide significant opportunities for improving detection accuracy, prioritizing alerts, and automating repetitive tasks, thus allowing human analysts to focus on complex threat investigations. Predictive analytics and cognitive SOC architectures enhance the ability to anticipate attacks and optimize resource allocation. Additionally, automation and orchestration tools reduce the likelihood of human error, improve response times, and contribute to proactive vulnerability remediation.

Based on the findings, it can be concluded that SOC effectiveness depends on a balanced integration of technological solutions and human expertise. Technical improvements alone are insufficient if organizational factors—such as workforce management, training, and communication protocols—are neglected. Likewise, even highly skilled personnel cannot compensate for misconfigured tools or fragmented infrastructure. The research confirms the initial

hypothesis: enhancing SOC resilience requires a holistic approach that combines automation, AI/ML, structured workflows, and human capacity development.

Furthermore, the study demonstrates that SOC vulnerabilities have significant operational and financial consequences. Delayed detection and ineffective response not only threaten the security of critical information assets but can also result in substantial financial losses, reputational damage, and compliance penalties. Addressing these vulnerabilities is therefore a strategic necessity for organizations operating in the digital environment.

The findings offer several directions for future research and practical application. Organizations can implement maturity models to assess SOC effectiveness, optimize staffing models, and design continuous professional development programs. AI-driven tools and cognitive SOC architectures provide a promising avenue for enhancing analytical capabilities and adaptive decision-making. The study also suggests that cross-sector collaboration and knowledge sharing could strengthen SOC practices and promote standardized operational procedures.

From a practical standpoint, these insights can guide the design and improvement of SOCs across industries, particularly in sectors handling critical infrastructure, finance, healthcare, and large-scale enterprises. By integrating technical advancements with human-centered management, organizations can transition SOCs from reactive monitoring units into proactive defense centers capable of anticipating and neutralizing emerging cyber threats.

In conclusion, this research contributes to the scientific understanding of SOC vulnerabilities by providing a structured analysis of their causes, impacts, and mitigation strategies. The study confirms that an integrated approach—combining technological, organizational, and human factors—is essential for enhancing SOC performance. Future studies should explore the practical integration of AI and ML in real-world SOC environments, focusing on trust in automation, analyst adaptability, and organizational transformation. These developments will ensure that SOCs remain resilient, efficient, and capable of safeguarding organizational assets against evolving cyber threats.

REFERENCES

Agyepong, 2020 — Agyepong E., Cherdantseva Y., Reinecke P., Burnap P. Cyber Security Operations Centre Concepts and Implementation. // Modern Theories and Practices for Cyber Ethics and Security Compliance. — 2020. — Pp. 88–105. [Eng.]

Anton, 2003 — Anton P.S., Anderson R.H., Mesic R., Scheiern M. Finding and fixing vulnerabilities in information systems: The Vulnerability Assessment & Mitigation Methodology. Report. — National Defense Research Institute, RAND Corporation, Santa Monica, CA. — 2003. — 117 p. [Eng.]

Aslan, 2017 — Aslan Ö., Samet R. Mitigating Cyber Security Attacks by Being Aware of Vulnerabilities and Bugs. // Proceedings of the 2017 International Conference on Cyberworlds (CW). — 2017. — Pp. 222–225. [Eng.]

Banati, 2022 — Banati, A., Rigo, E., Fleiner, R., Kail, E. Use Cases of Attack Graph for SOC Optimization Purpose. // 26th IEEE International Conference on Intelligent Engineering Systems (INES). — 2022. — Pp. 143–147. [Eng.]

Demertzis, 2018 — Demertzis, K., Kikiras, P., Tziritas, N., Sanchez, S.L., Iliadis, L. The Next Generation Cognitive Security Operations Center: Network Flow Forensics Using Cybersecurity Intelligence. // Big Data and Cognitive Computing. — 2(4). — 2018. — Pp. 1–17. [Eng.]

Degrass, 2022 — Degrass E. Techniques for Identifying and Remediating Operational Vulnerabilities. — US Patent Application 17/430, — 968. — 2022. — Pp. 1–14. [Eng.]

Hore, 2023 — Hore, S., Moomtaheen, F., Shah, A., Ou, X. Towards Optimal Triage and Mitigation of Context- Sensitive Cyber Vulnerabilities. // IEEE Transactions on Dependable and Secure Computing. — 2023. — 20(2). — Pp. 1270–1285. [Eng.]

Janos, 2018 — Janos, F.D., Dai, N.H.P. Security Concerns Towards Security Operations Centers. // IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI). — 2018. — Pp. 273–278. [Eng.]

Kiselev, 2022 — Kiselev, A.A., Korotkikh, I.V., Shott, V.V. The Practice of Making a Security Operations Center. // Digital Technology Security. — 2022. — 4. — Pp. 39–51. [Eng.]

Kokulu, 2019 — Kokulu, F.B., Shoshitaishvili, Y., Soneji, A., Zhao, Z., Ahn, G.J., Bao, T., Doupé, A. Matched and Mismatched SOCs: A Qualitative Study on Security Operations Center Issues. // Proceedings of the ACM Conference on Computer and Communications Security. — 2019. — Pp. 1955 - 1970. [Eng.]

Onwubiko, 2019a — Onwubiko, C. Cyber Security Operations Centre: Security Monitoring for Protecting Business and Supporting Cyber Defense Strategy. // CCS '19: 2019 ACM SIGSAC Conference on Computer and Communications Security, UK. — 2019. — Pp. 1–10. [Eng.]

Onwubiko, 2019b — Onwubiko C., Ouazzane K. Challenges Towards Building an Effective Cyber Security Operations Centre. // International Journal on Cyber Situational Awareness. — 2019.— 4(1). — Pp. 11–39. [Eng.]

Reeves, 2023 — Reeves, A., Ashenden, D. Understanding Decision Making in Security Operations Centres: Building the Case for Cyber Deception Technology. // Frontiers in Psychology. — 2023. — 14. — Pp. 1–11. [Eng.]

Resilience, 2024 — Resilience E. Optimizing Security Operations Centers for Enhanced Cyber Resilience. // Navigating IT Governance for Resilient Organizations. — 2024. — Pp. 1–22. [Eng.]

Riggs, 2023 — Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M.A., Amir, A., Vuda, K.V., Sarwat, A.I. Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure. // Sensors. — 2023. — 23(8). — Pp. 1–26. [Eng.]

Taqafi, 2023 — Taqafi, I., Maleh, Y., Ouazzane, K. A Maturity Capability Framework for Security Operation Center. // EDPACS. — 2023. — 67(3). — Pp. 21–38. [Eng.]

Vielberth, 2020 — Vielberth, M., Bohm, F., Fichtinger, I., Pernul, G. Security Operations Center: A Systematic Study and Open Challenges. // IEEE Access. — 2020. — 8.— Pp. 227756–227779. [Eng.]

ҚАЗАҚСТАН ӨНДІРІС КӨЛІГІ

ПРОМЫШЛЕННЫЙ ТРАНСПОРТ КАЗАХСТАНА

INDUSTRIAL TRANSPORT OF KAZAKHSTAN

Правила оформления статьи для публикации в журнале на сайте:
http://prom.mtgu.edu.kz

ISSN: 1814-5787 (print)
ISSN: 3006-0273 (online)

Собственник:
Международный транспортно-гуманитарный университет
(Казахстан, г.Алматы).

ОТВЕТСТВЕННЫЙ РЕДАКТОР
Мылтыкбаева Айгуль Тауарбековна

КОМПЬЮТЕРНАЯ ВЕРСТКА
Букина Светлана Владимировна

Подписано в печать 15.09.2025.Формат 60x84 1/8 .Бумага офсет №1.Гарнитура «Таймс» .Печать RISO.

Объем 13,4 усл.п.л. Тираж 500 экз.

Отпечатано и сверстано в ИП «Salem» с.Бескайнар, ул.Мичурин, 52/1, тел.: +77072619261

Издание «Международный транспортно-гуманитарный университет»
Адрес редакции: г. Алматы, мкрн. Жетысу-1, д. 32а.