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

ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

2025 (24) 4

қазан- желтоқсан

ISSN 2708–2032 (print)
ISSN 2708–2040 (online)

Халықаралық ақпараттық және коммуникациялық технологиялар журналы
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Меншік иесі: АҚ «Халықаралық ақпараттық технологиялар университеті» (Алматы қ.).
Қазақстан Республикасы Ақпарат және қоғамдық даму министрлігіне мерзімді баспасөз басылымын есепке қою туралы куәлік № KZ82VPY00020475, 20.02.2020 ж. берілген
Тақырып бағыты: ақпараттық технологиялар, ақпараттық қауіпсіздік және коммуникациялық технологиялар, әлеуметтік-экономикалық жүйелерді дамытудағы цифрлық технология.
Мерзімділігі: жылына 4 рет.
Тираж: 100 дана.
Редакция мекенжайы: 050040 Алматы қ., Манас қ., 34/1, каб. 709, тел: +7 (727) 244-51-09.
E-mail: ijict@iitu.edu.kz
Журнал сайты: https://journal.iitu.edu.kz

Международный журнал информационных и коммуникационных технологий
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Собственник: АО «Международный университет информационных технологий» (г. Алматы).
Свидетельство о постановке на учет периодического печатного издания в Министерство информации и общественного развития Республики Казахстан **№ KZ82VPY00020475,** выданное от **20.02.2020 г.**
Тематическая направленность: информационные технологии, информационная безопасность и коммуникационные технологии, цифровые технологии в развитии социо-экономических систем**.**
Периодичность: 4 раза в год.
Тираж: 100 экземпляров.
Адрес редакции: 050040 г. Алматы, ул. Манаса 34/1, каб. 709, тел: +7 (727) 244-51-09.
E-mail: ijict@iitu.edu.kz Сайт журнала: https://journal.iitu.edu.kz

«International Journal of Information and Communication Technologies»
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Owner: International Information Technology University JSC (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 No. KZ82VPY00020475, issued on 20.02.2020.
Thematic focus: information technology, digital technologies in the development of socio-economic systems, information security and communication technologies
Periodicity: 4 times a year.
Circulation: 100 copies.
Editorial address: 050040. Manas st. 34/1, Almaty. +7 (727) 244-51-09. E-mail: ijict@iitu.edu.kz
Journal website: https://journal.iitu.edu.kz

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Vol. 6. Is. 4. Number 24 (2025). Pp. 01–19
Journal homepage: https://journal.iitu.edu.kz
https://doi.org/10.54309/IJICT.2025.24.4.001

SECURING SOCS: UNDERSTANDING VULNERABILITIES, THEIR IMPACT, AND MITIGATION STRATEGIES

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

Altynbekov Ali — master's student, Faculty of Computer Technology and Cybersecurity, International Information Technology University, Almaty,

Kazakhstan

E-mail: 41378@iitu.edu.kz. https://orcid.org/0009-0001-5360-0128;
Alin Galymzada — Candidate of Technical Sciences, assistant professor, Cybersecurity Department, International Information Technology University, Almaty, Kazakhstan
E-mail: g.alin@iitu.edu.kz. https://orcid.org/0000-0003-1028-5452;
Amanzholova Saule — Candidate of Technical Sciences, associate professor, Cybersecurity Department, Astana IT University
E-mail: s.amanzholova@astanait.edu.kz. https://orcid.org/0000-0002-6779-9393;
Saleh Mohammed — PhD, associate professor, Cybersecurity Department, International Information Technology University, Almaty, Kazakhstan
E-mail: m.saleh@iitu.edu.kz. https://orcid.org/0000-0003-4673-5056.

Abstract. Security Operations Centers (SOCs) are critical for defending orga-nizations against increasingly sophisticated cyber threats; however, they themselves are susceptible to vulnerabilities that can compromise their effectiveness. This review paper provides a comprehensive analysis of key vulnerabilities within SOC environ-ments, assesses their impact on detection and response capabilities, and explores ef-fective mitigation strategies to enhance SOC resilience. By systematically reviewing existing literature, industry reports, and case studies, the paper examines both tech-nical and organizational vulnerabilities affecting SOC performance. Common issues identified include under-resourced teams, tool misconfigurations, inefficient incident response processes, staffing shortages, and outdated technologies. The impact of these vulnerabilities is discussed in terms of delayed threat detection, increased risk of security breaches, and overall degradation of organizational cybersecurity posture. The review also synthesizes recommended mitigation strategies such as improving SOC staffing

levels, enhancing tool integration, and adopting automation technologies for incident response. Additionally, it explores the potential of advanced technologies like artificial intelligence and machine learning to enhance SOC operations and adapt to the evolving cyber threat landscape. Emphasis is placed on fostering robust com-munication protocols, promoting continuous analyst training, and integrating holistic security practices across various organizational layers. In conclusion, understanding and addressing vulnerabilities within SOCs is crucial for maintaining effective cy-bersecurity defenses. The paper underscores the need for coordinated efforts to inte-grate human expertise with technological solutions, highlighting how such synergy fortifies both prevention and response to emerging threats. Future research directions include further exploration of AI and machine learning applications in SOCs to better respond to an ever-evolving threat landscape.

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

For citation: A. Altynbekov, G. Alin, S. Amanzholova, M. Saleh. Securing socs: understanding vulnerabilities, their impact, and mitigation strategies//International journal of information and communication technologies. 2025. Vol. 6. No. 24. Pp. 01–19 (In Eng.). https://doi.org/10.54309/IJICT.2025.24.4.001

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

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

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

Алтынбеков Али — магистрант, Компьютерлік технологиялар және киберқауіпсіздік факультеті, Ақпараттық технологиялар халықаралық университеті
E-mail: 41378@iitu.edu.kz. https://orcid.org/0009-0001-5360-0128;
Алин Галымзада — 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;
Аманжолова Сауле — техника ғылымдарының кандидаты, Киберқауіпсіздік кафедрасының қауымдастырылған профессоры, Астана IT университеті
E-mail: s.amanzholova@astanait.edu.kz. https://orcid.org/0000-0002-6779-9393;
Салех Мохаммед — 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 (SOCs) ұйымдар-ды барған сайын күрделі киберқауіптерден қорғау үшін өте маңызды; дегенмен, олардың өздері олардың тиімділігіне нұқсан келтіруі мүмкін осалдықтарға бей-ім. Бұл шолу мақаласы SOC орталарындағы негізгі осалдықтардың жан-жақты талдауын қамтамасыз етеді, олардың анықтау және әрекет ету мүмкіндіктері-не әсерін бағалайды және SOC тұрақтылығын арттыру үшін тиімді жұмсар-ту стратегияларын зерттейді. Қолданыстағы әдебиеттерді, салалық есептерді және кейстерді жүйелі түрде қарастыра отырып, мақалада SOC өнімділігіне әсер ететін техникалық және ұйымдастырушылық осалдықтар қарастырылады. Анықталған жалпы мәселелерге ресурстардың жетіспеушілігі, құралдардың дұрыс конфигурацияланбауы, инциденттерге әрекет етудің тиімсіз процестері, қызметкерлердің жетіспеушілігі және ескірген технологиялар жатады. Бұл осал-дықтардың әсері қауіптерді анықтаудың кешігуі, қауіпсіздіктің бұзылу қаупінің жоғарылауы және ұйымның киберқауіпсіздік жағдайының жалпы нашарлауы тұрғысынан талқыланады. Шолу СОНЫМЕН қатар SOC қызметкерлерінің са-нын жақсарту, құралдардың интеграциясын жақсарту және инциденттерге жау-ап беру үшін автоматтандыру технологияларын енгізу сияқты ұсынылған жұм-сарту стратегияларын синтездейді. Сонымен қатар, ол SOC жұмысын жақсарту және дамып келе жатқан киберқауіптер ландшафтына бейімделу үшін жасан-ды интеллект және машиналық оқыту сияқты озық технологиялардың әлеуетін зерттейді. Сенімді байланыс хаттамаларын әзірлеуге, талдаушыларды үздіксіз оқытуға жәрдемдесуге және әртүрлі ұйымдық деңгейлерде қауіпсіздіктің тұтас әдістерін біріктіруге баса назар аударылады. Қорытындылай келе, Soc жүйесін-дегі осалдықтарды түсіну және жою киберқауіпсіздікті қорғаудың тиімді құрал-дарын сақтау үшін өте маңызды. Құжатта адам тәжірибесін технологиялық шешімдермен біріктіру бойынша үйлестірілген күш-жігердің қажеттілігі атап өтіліп, мұндай синергия пайда болатын қауіптердің алдын алуды да, оларға жа-уап беруді де қалай күшейтетіні көрсетілген. Болашақ зерттеу бағыттары үнемі өзгеріп отыратын қауіп-қатер ландшафтына жақсырақ жауап беру үшін Soc-да жасанды интеллект пен машиналық оқыту қолданбаларын одан әрі зерт-теуді қамтиды.

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 // Халықаралық ақпараттық және коммуникациялық технологиялар журналы. 2025. Т. 6. № 24. Б. 01–19 (ағыл. тілінде). https://doi.org/10.54309/IJICT.2025.24.4.001

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

А.А. Алтынбеков[1], Г. Алин[2], С. Аманжолова[1], М. Салех[1]
[1]Международный университет информационных технологий, Алматы, Казахстан;
[2]Астана ИТ университет, Астана, Казахстан.
E-mail: 41378@iitu.edu.kz

Алтынбеков Али — магистратрант, факультет компьютерных технологий и кибербезопасности, Международный университет информационных технологий, Алматы, Казахстан
E-mail: 41378@iitu.edu.kz. https://orcid.org/0009-0001-5360-0128;
Алин Галымзада — кандидат технических наук, ассистент профессор, кафедра кибербезопасности, Международный университет информационных технологий, Алматы, Казахстан
E-mail: g.alin@iitu.edu.kz. https://orcid.org/0000-0003-1028-5452;
Аманжолова Сауле — кандидат технических наук, ассоциированный профессор, кафедра кибербезопасности, Астана ИТ университет, Астана, Казахстан
E-mail: s.amanzholova@astanait.edu.kz. https://orcid.org/0000-0002-6779-9393;
Салех Мохаммед — PhD, ассоциированный профессор, кафедра 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 поста-вить под угрозу их эффективность. В этом обзорном документе представлен все-сторонний анализ ключевых уязвимостей в среде SOC, оценивается их влияние на возможности обнаружения и реагирования, а также рассматриваются эффек-тивные 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, не-правильную настройку инструментов, неэффективные процессы реагирования на инциденты, нехватку персонала и устаревшие технологии. Влияние этих уязвимостей обсуждается с точки зрения задержки обнаружения угроз, повы-шенного риска нарушений безопасности и общего ухудшения состояния

кибербезопасности организации. В обзоре также обобщены рекомендуемые страте-гии 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 технологиче-скими решениями, подчеркивая, как такая синергия способствует предотвраще-нию и реагированию на возникающие угрозы. Будущие направления исследова-ний 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 // Международный журнал информационных и коммуникационных технологий. 2025. Т. 6. No. 24. Стр. 01–19. (На анг.). https://doi.org/10.54309/IJICT.2025.24.4.001

Introduction

In today's digital landscape, where technological innovation is a key driv-er of organizational success, the proliferation of cyber threats presents significant challenges to maintaining secure information systems (Riggs et al., 2023; Aslan & Samet, 2017). Cyber adversaries are increasingly sophisticated, employing advanced techniques such as zero-day exploits, ransomware, and state-sponsored attacks to ex-ploit vulnerabilities within organizational infrastructures (Grobler et al., 2018; De-mertzis et al., 2018). To defend against these evolving threats, organizations deploy Security Operations Centers (SOCs), which serve as centralized units for continuous monitoring, detection, analysis, and response to cybersecurity incidents (Agyepong et al., 2020; Muniz et al., 2015). SOCs combine skilled personnel, cutting-edge technologies, and structured processes to provide comprehensive cybersecurity defense mechanisms (Onwubiko, 2015; Vielberth et al., 2020).

Despite their critical role, SOCs face inherent vulnerabilities that can diminish their operational effectiveness (Kokulu et al., 2019; Janos & Dai, 2018).

Technical challenges such as tool misconfigurations, lack of interoperability between security solutions, and reliance on legacy systems can impede the SOC's ability to detect and respond to threats promptly (Banati et al., 2022; Kiselev et al., 2022). For instance, Banati et al. discuss how the use of attack graphs can optimize SOC operations by ad-dressing technical inefficiencies (Banati et al., 2022). Organizational issues, including insufficient staffing levels, high turnover rates, inadequate training, and lack of clear communication channels, further exacerbate these technical shortcomings (Reeves & Ashenden, 2023; Onwubiko & Ouazzane, 2019). Kokulu et al. highlight that mis-matched SOCs, where the organizational structure does not align with operational needs, are particularly prone to such vulnerabilities (Kokulu et al., 2019).

The consequences of these vulnerabilities are substantial. Delays in threat detection and response due to internal SOC weaknesses can result in significant financial losses, operational disruptions, regulatory penalties, and erosion of stakeholder trust (Anton et al., n.d.; Resilience, 2024). As cyber threats become more advanced and persistent, the inability of SOCs to adapt and address internal vulnerabilities pos-es a critical risk to organizational security (Vielberth et al., 2020; Onwubiko, 2017). Despite the recognition of these challenges, there is a scarcity of comprehensive stud-ies that systematically analyze SOC vulnerabilities and their impact on cybersecurity operations (Vielberth et al., 2020; Taqafi et al., 2023). Addressing this research gap is imperative for developing effective strategies to enhance SOC resilience and efficacy (Aslan & Samet, 2017; Hore et al., 2023).

This review paper, titled "Securing SOCs: Understanding Vulnerabilities, Their Impact, and Mitigation Strategies," aims to bridge this gap by providing a thor-ough examination of the vulnerabilities affecting SOCs and proposing actionable solutions. The primary objectives are to identify and categorize the key technical and organizational vulnerabilities within SOC environments, assess the impact of these vulnerabilities on SOC performance, and explore effective mitigation strategies that can enhance SOC capabilities and resilience (Vielberth et al., 2020; Taqafi et al., 2023). By synthesizing current research and best practices, this paper seeks to con-tribute to the advancement of SOC effectiveness in the face of evolving cyber threats.

To achieve these objectives, the paper seeks to answer several research questions: What are the most prevalent technical and organizational vulnerabilities affect-ing SOCs today? How do these vulnerabilities impact the operational effectiveness of SOCs in detecting and responding to cyber threats? What strategies can be imple-mented to mitigate these vulnerabilities and improve SOC performance? How can emerging technologies such as artificial intelligence (AI) and machine learning (ML) be leveraged to address SOC vulnerabilities?

To address the research objectives systematically, the paper is organized into

three main sections. Section 2 will cover the methodology of literature collection of papers, detailing the criteria for selecting relevant studies and the approaches used to gather and analyze data. Section 3 should include the results of the paper's analysis, presenting an in-depth discussion of the identified technical and organizational vulnerabilities affecting SOCs, their impact on detection and response capabilities, and the mitigation strategies proposed in the literature. The last section will be the conclusion, summarizing the key findings of the study, discussing implications for cybersecurity professionals, and suggesting future research directions, particularly in exploring the role of AI and ML in enhancing SOC operations.

Methodology

This section outlines the systematic approach to collecting and analyzing lit-erature on vulnerabilities within Security Operations Centers (SOCs) and their mit-igation strategies. The methodology was designed to provide a comprehensive and unbiased review of research, industry reports, and case studies.

The literature search strategy employed multiple reputable platforms. Google Scholar served as a broad resource for scholarly works across disciplines. IEEE Xplore provided access to technical literature in computer science and engineering, critical for sourcing papers on SOCs. Scopus covered peer-reviewed journals, conference proceedings, and books, ensuring diverse and high-quality sources. Advanced AI tools were also utilized to aggregate and summarize recent publications, capturing the latest developments in cybersecurity.

To ensure the relevance and quality of selected literature, inclusion criteria focused on publications from 2010 onward, emphasizing peer-reviewed articles, industry reports, and case studies on SOC vulnerabilities and mitigation strategies, including the use of AI and machine learning. Exclusion criteria eliminated non-English articles and publications lacking substantial contributions or relevance to SOCs. Keywords and phrases were grouped into categories—SOC vulnerabilities, impact analysis, and mitigation strategies—with Boolean operators enhancing search efficiency.

The initial search yielded numerous publications, with duplicates removed using reference management tools. A two-stage screening process followed: first, articles were assessed by titles and abstracts for relevance; then, selected articles underwent fulltext review to confirm suitability. Extracted data were organized into thematic categories such as technical vulnerabilities (e.g., outdated technologies, tool misconfigurations), organizational challenges (e.g., staffing shortages), impacts on SOC performance, and mitigation strategies like automation and AI applications. As shown in figure 1.

Data extraction involved identifying critical information such as specific tech-nical and organizational challenges and their direct effects on SOC performance met-rics like threat detection and incident response times. This process also highlighted the various technological and operational strategies employed by organizations to mitigate these vulnerabilities. For example, advancements in machine learning algo-rithms were often cited as a means of improving SOC efficiency through realtime threat detection and proactive incident response measures.

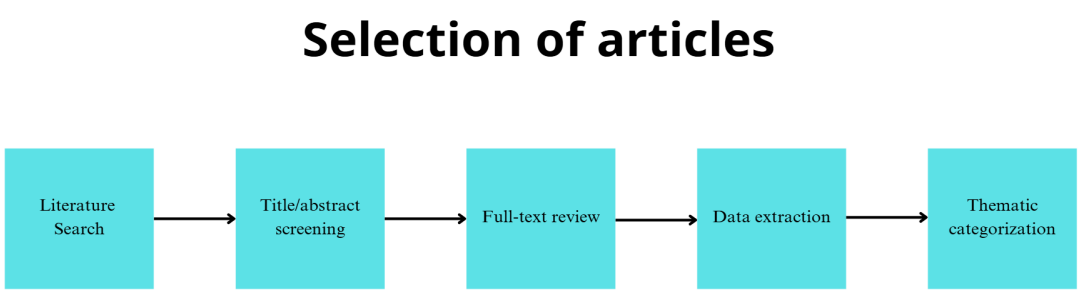

Fig. 1. Selection of articles

These findings were com-pared across studies to evaluate their effectiveness and applicability in different orga-nizational contexts.

A qualitative synthesis identified patterns, gaps, and insights across studies, focusing on the interplay between vulnerabilities and their cumulative effects on SOC effectiveness. This approach provided a holistic understanding of challenges and pro-posed solutions to enhance resilience.

Certain limitations were acknowledged. The reliance on published literature may exclude unpublished or organizational insights, introducing potential publication bias. Restricting the search to English-language studies could omit valuable interna-tional research. Additionally, the rapid evolution of cybersecurity means findings may require ongoing updates.

Ethical considerations guided the research process. Proper citation ensured acknowledgment of original authors, maintaining academic integrity. The study ad-hered to ethical guidelines, emphasizing transparency and respect for intellectual property.

This methodology offers a thorough analysis of SOC vulnerabilities and miti-gation strategies, contributing valuable insights to help organizations strengthen their defenses in an evolving cybersecurity landscape.

Results

Literature Review. Securing Security Operations Centers (SOCs) involves understanding their vulnerabilities, the impact of these vulnerabilities, and implementing effective mitigation strategies. SOCs are integral to an organization's cybersecurity strategy, providing real-time threat detection and response capabilities. However, they face challenges such as technological constraints, procedural complexities, and human factors, which can hinder their effectiveness. Addressing these challenges requires a comprehensive approach that includes optimizing processes, leveraging technology, and enhancing human expertise.

Various studies have extensively explored the development, optimization, and challenges associated with Security Operations Centers (SOCs) to enhance cybersecurity resilience. Agyepong et al. provide a comprehensive overview of SOC concepts and implementation strategies, emphasizing their critical role in organizational security frameworks (Agyepong et al., 2020). Similarly, Muniz, McIntyre, and AlFardan delve into the practical aspects of building, operating, and maintaining SOCs, offering valuable insights for practitioners aiming to establish robust security infrastructures (Muniz et al., 2015).

Addressing vulnerabilities is a focal point in cybersecurity research. Anton et al. introduce the Vulnerability Assessment and Mitigation Methodology, highlighting systematic approaches to identify and mitigate security risks effectively (Anton et al., n.d.). Aslan and Samet focus on mitigating cyber attacks by raising awareness of vulnerabilities and bugs, suggesting proactive defense mechanisms to strengthen security postures (Aslan & Samet, 2017). Degrass presents innovative techniques for identifying and remediating operational vulnerabilities, contributing to proactive security measures within organizations (E Degrass - US Patent App. 17/430 & 2022, 2022). Hore et al. propose methods for optimal triage and mitigation of context-sensitive cyber vulnerabilities, aiming to prioritize threats and allocate resources efficiently (Hore et al., 2023).

For SOC optimization, Banati et al. examine the use of attack graphs to enhance SOC operations, demonstrating how visualization tools can aid in threat detection and response (Banati et al., 2022). Demertzis et al. discuss the next-generation cognitive SOC, utilizing network flow forensics and cybersecurity intelligence to improve response times and decision-making processes (Demertzis et al., 2018). Li and Hsieh explore the implementation of distributed hierarchical SOCs using mobile agent groups, offering solutions for scalable and flexible security management (Li & Hsieh, 2010). Yuan and Zou highlight the role of correlation analysis in SOCs, showing how data integration can improve security operations and incident detection rates (Yuan & Zou, 2011).

Operational challenges within SOCs are further explored by Kiselev, Korotkikh, and Shott, who share practical experiences in establishing a SOC, discussing best practices and common pitfalls (Kiselev et al., 2022). Kokulu et al. conduct a qualitative study on SOC issues, identifying mismatches and challenges that can hinder security efforts and proposing solutions to address them (Kokulu et al., 2019). Janos and Dai investigate security concerns related to SOCs, providing insights into potential vulnerabilities and areas needing improvement (Janos & Dai, 2018).

Understanding human factors in SOCs, Reeves and Ashenden investigate decision-making processes within these centers, advocating for the use of cyber deception technology to enhance threat detection and response strategies (Reeves & Ashenden, 2023). Taqafi, Maleh, and Ouazzane propose a maturity capability framework for SOCs, aiming to assess and improve their effectiveness systematically (Taqafi et al., 2023). Vielberth et al. conduct a systematic study on SOCs, identifying open challenges and areas for future research, emphasizing the need for continuous development in SOC practices (Vielberth et al., 2020).

In the context of critical infrastructure protection, Riggs et al. (Riggs et al., 2023) discuss the impact of vulnerabilities and present mitigation strategies to ensure cyber-secure environments, highlighting the importance of SOCs in safeguarding essential services. Grobler, Jacobs, and van Niekerk emphasize the role of cybersecurity centers in threat detection and mitigation, providing insights into their implementation and operational effectiveness (Grobler et al., 2018). Resilience focuses on opti-

mizing SOCs for enhanced cyber resilience, discussing strategies for improvement and adaptation in the face of evolving threats (Resilience, 2024).

Onwubiko underscores the importance of security monitoring, situational awareness, and threat intelligence within SOCs to support cyber defense strategies (Onwubiko, 2015; Onwubiko, 2017). Together with Ouazzane, Onwubiko identifies challenges in building effective SOCs, highlighting organizational structure, resource allocation, and the integration of advanced technologies as key factors (Onwubiko & Ouazzane, 2019).

Schönfeld discusses the role of SOCs in the medical technology field, highlighting their importance in securing sensitive data and complying with regulatory requirements (Schönfeld, 2023). This sector-specific insight demonstrates the broad applicability of SOC principles across different industries.

Collectively, this body of work underscores the evolving nature of SOCs and the continuous efforts by researchers and practitioners to address cybersecurity threats effectively. The studies highlight the importance of proactive vulnerability management, advanced threat detection techniques, and the integration of human factors in enhancing the effectiveness of SOCs. As cybersecurity threats become more sophisticated, the insights from these studies provide a foundation for developing resilient and adaptive security operations capable of protecting critical assets and information. All the articles studied above can be seen in a simplified form on table 1.

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
Muniz, McIntyre, and AlFardan	Practical aspects of building, operating, and maintaining SOCs	Insights for robust security infrastructures
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
Degrass	Innovative techniques for operational vulnerability remediation	Contributes to proactive security measures
Hore et al.	Optimal triage and mitigation of context-sensitive vulnerabilities	Efficient threat prioritization and resource allocation
Banati et al.	Use of attack graphs to enhance SOC operations	Improves threat detection and response efficiency
Demertzis et al.	Next-generation cognitive SOC using network flow forensics	Enhances decision-making and response times
Li and Hsieh	Distributed hierarchical SOCs using mobile agent groups	Solutions for scalable and flexible SOC management

Yuan and Zou	Role of correlation analysis in improving SOC performance	Improves incident detection rates through data integration
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
Janos and Dai	Insights into security concerns related to SOCs	Highlights vulnerabilities and improvement areas
Reeves and Ashenden	Decision-making processes in SOCs with cyber deception technology	Enhances threat detection and response strategies
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
Riggs et al.	Mitigation strategies for vulnerabilities in critical infrastructure	Focus on safeguarding critical services
Grobler, Jacobs, and van Niekerk	Role of cybersecurity centers in threat detection and mitigation	Insights into implementation and operational effectiveness
Resilience	Strategies for enhancing SOC resilience	Adaptation strategies for evolving threats
Onwubiko (2015), (2017)	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
Schönfeld	Role of SOCs in medical technology security and compliance	Broad applicability across industries

The systematic review of the literature revealed a comprehensive understanding of the vulnerabilities affecting Security Operations Centers (SOCs), their impact on organizational cybersecurity, and the strategies available for mitigation. The findings are organized into three main categories as shown on Figure 2: technical vulnerabilities, organizational vulnerabilities, and mitigation strategies, including the potential role of advanced technologies such as artificial intelligence (AI) and machine learning (ML).

Technical Vulnerabilities in SOCs

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

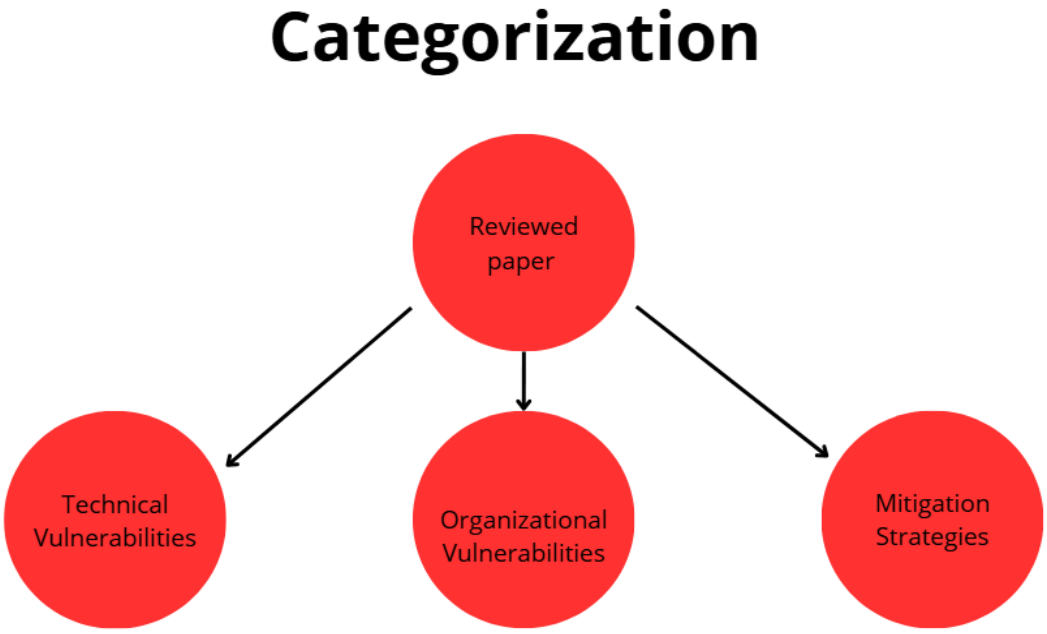

Fig. 2. Categorization of revied papers

The integration of disparate security tools poses a significant challenge. Many SOCs rely on multiple security solutions that do not seamlessly communicate with each other, leading to information silos and inefficient incident response processes (Demertzis et al., 2018; Yuan & Zou, 2011). Demertzis et al. emphasize that the lack of interoperability hinders the SOC's ability to correlate events across different platforms, reducing the effectiveness of threat detection and analysis (Demertzis et al., 2018).

Dependence on outdated technologies and legacy systems is another critical vulnerability. Legacy systems often lack the necessary features to combat modern cyber threats and may not receive regular security updates, making them susceptible to exploits (Kiselev et al., 2022; Li & Hsieh, 2010). Kiselev et al. note that legacy infrastructure can impede the adoption of new security solutions, limiting the SOC's capability to respond to advanced persistent threats (Kiselev et al., 2022).

Organizational Vulnerabilities in SOCs

Under-resourced teams are a common organizational vulnerability within SOCs. Insufficient staffing leads to overworked analysts, increased fatigue, and a higher likelihood of oversight in monitoring activities (Kokulu et al., 2019), (Onwubiko & Ouazzane, 2019). Kokulu et al. found that staffing shortages result in delayed incident responses and reduced overall efficiency in security operations (Kokulu et al., 2019).

The cybersecurity field faces high turnover rates due to factors such as burnout, competitive job markets, and inadequate career development opportunities. High turnover disrupts team cohesion and results in the loss of institutional knowledge,

weakening the SOC's effectiveness (Janos & Dai, 2018; Reeves & Ashenden, 2023). Reeves and Ashenden suggest that retaining skilled personnel is crucial for maintaining robust security operations (Reeves & Ashenden, 2023).

A lack of continuous training and professional development leaves SOC personnel ill-equipped to handle emerging threats. Without up-to-date knowledge of the latest attack vectors and security technologies, analysts may fail to identify or respond appropriately to incidents (Agyepong et al., 2020; Onwubiko, 2017). Onwubiko stresses the importance of ongoing education to enhance situational awareness and threat intelligence capabilities (Onwubiko, 2017).

Effective communication is 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 et al., 2019; Onwubiko & Ouazzane, 2019). Kokulu et al. highlight that organizational silos hinder information sharing, which is vital for a timely and effective security response (Kokulu et al., 2019).

Impact of SOC Vulnerabilities on Detection and Response Capabilities

The identified vulnerabilities have a profound impact on the SOC's ability to detect and respond to cyber threats effectively.

Technical and organizational shortcomings contribute to slower identification of security incidents. Delayed threat detection allows attackers more time to infiltrate systems, exfiltrate data, and cause damage (Anton et al., n.d.; Resilience, 2024).

Figure 3 illustrates the average detection times across industries based on findings by Anton et al. and Resilience (Anton et al., n.d.; Resilience, 2024). For example, the healthcare industry reports the longest detection time, averaging 211 days. Such delays highlight critical vulnerabilities in identifying security breaches promptly.

Anton et al. indicate that timely detection is critical in minimizing the impact of security breaches (Anton et al., n.d.).

Vulnerabilities within SOCs heighten the risk of successful cyber attacks. Inefficient processes and inadequate defenses provide opportunities for adversaries to exploit weaknesses, leading to potential financial losses and reputational damage (Grobler et al., 2018; Riggs et al., 2023). Riggs et al. emphasize that compromised SOCs can have cascading effects on critical infrastructure protection (Riggs et al., 2023).

The cost of delayed detection can be significant. For instance, E. Resilience (Resilience, 2024) reports that organizations experiencing major data breaches incur average costs of $4.45 million per incident. These expenses include legal fees, regulatory penalties, lost revenue, and the cost of remediation efforts. The financial toll reinforces the necessity of investing in advanced detection technologies and staff training.

Figure 4 presents the cost breakdown of data breaches as reported by Resilience (Resilience, 2024).

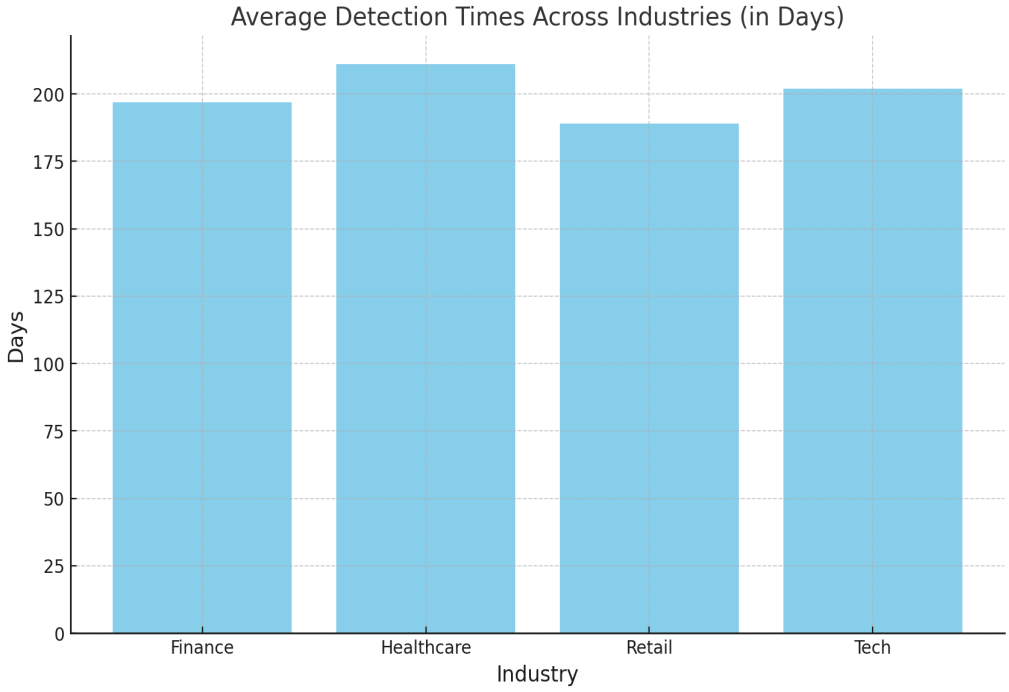

Fig. 3. Average Detection Times Across Industries

Lost revenue constitutes the largest portion (33.7 %), followed by legal fees (27.0 %). These statistics underscore the financial urgency of addressing SOC vulnerabilities.

Persistent vulnerabilities erode the overall cybersecurity posture of an organization. A weakened SOC cannot adequately protect assets, comply with regulatory requirements, or maintain stakeholder trust (Onwubiko, 2015; Vielberth et al., 2020). Vielberth et al. note that organizations with vulnerable SOCs are less resilient to cyber threats and may struggle to recover from incidents (Vielberth et al., 2020).

Mitigation Strategies for Enhancing SOC Resilience

The literature suggests several strategies to address the identified vulnerabilities and improve SOC performance.

Addressing staffing shortages involves not only hiring additional personnel but also optimizing workforce allocation. Implementing flexible staffing models and utilizing remote analysts can expand coverage and reduce burnout (Onwubiko & Ouazzane, 2019; Taqafi et al., 2023). Taqafi et al. propose a maturity capability framework to assess and enhance staffing effectiveness within SOCs (Taqafi et al., 2023).

Investing in security platforms that offer interoperability and centralized management can mitigate technical vulnerabilities related to tool misconfigurations and integration issues (Demertzis et al., 2018; Yuan & Zou, 2011). Yuan and Zou demonstrate how correlation analysis and integrated systems improve incident detection rates and response times (Yuan & Zou, 2011).

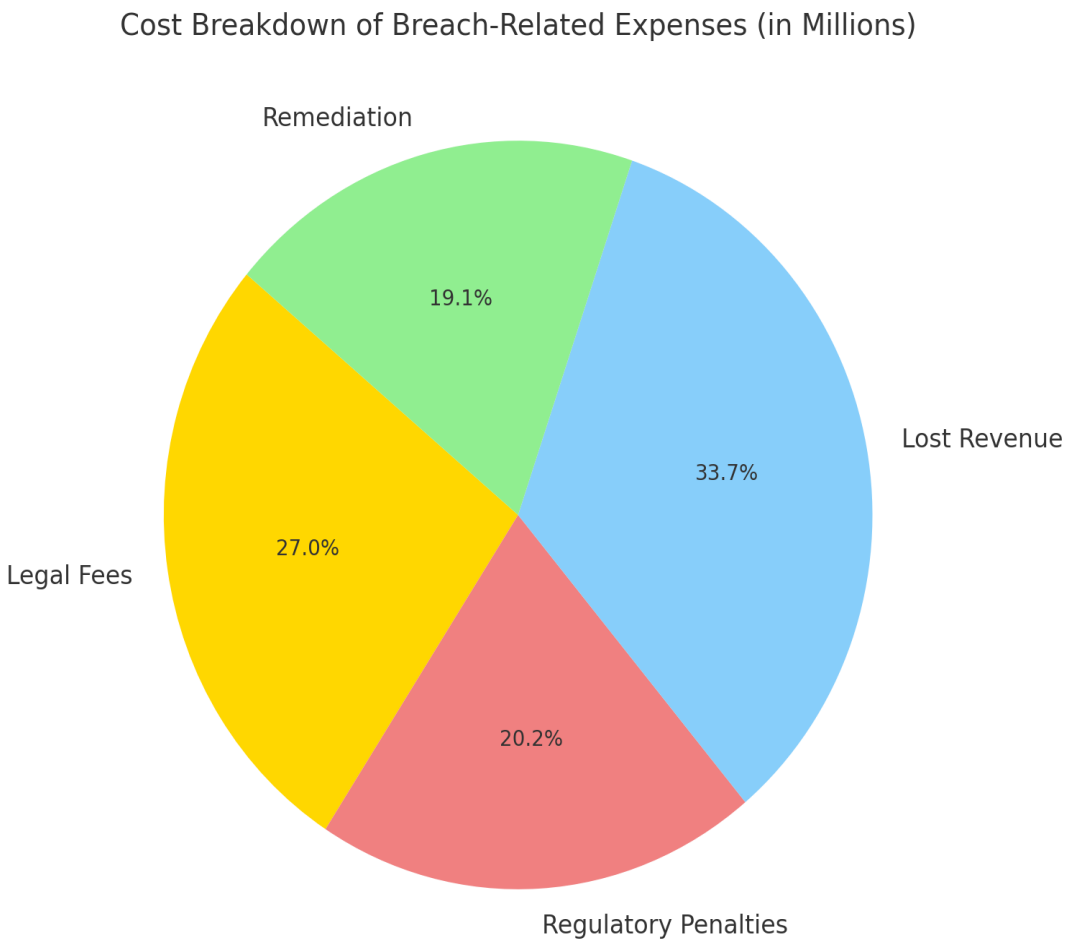

Fig. 4. Cost Breakdown of Breach-Related Expenses (in Millions)

Automation reduces the manual workload on analysts, allowing them to focus on complex threat analysis. Implementing automated incident response workflows and utilizing security orchestration tools can streamline operations and reduce the potential for human error (Banati et al., 2022; E Degrass - US Patent App. 17/430 & 2022, 2022). Degrass highlights the effectiveness of automation in proactive vulnerability remediation (E Degrass - US Patent App. 17/430 & 2022, 2022).

The application of AI and ML offers significant potential in enhancing SOC capabilities. These technologies can analyze vast amounts of data to identify patterns indicative of cyber threats, predict potential vulnerabilities, and recommend mitigation actions (Aslan & Samet, 2017; Demertzis et al., 2018). Aslan and Samet discuss how AI-driven solutions can augment human analysts, providing advanced threat detection and response mechanisms (Aslan & Samet, 2017).

Investing in continuous training programs ensures that SOC personnel remain knowledgeable about the latest threats and technologies. Certifications, workshops,

and simulation exercises can improve analysts' skills and confidence in handling incidents (Agyepong et al., 2020; Onwubiko, 2017). Onwubiko emphasizes the role of education in developing situational awareness and effective security monitoring (Onwubiko, 2015).

Developing standardized communication procedures facilitates better coordination within the SOC and across the organization. Regular meetings, incident debriefings, and collaborative platforms can enhance information sharing and response efficiency (Kokulu et al., 2019; Reeves & Ashenden, 2023). Reeves and Ashenden advocate for integrating communication strategies into SOC workflows to improve decision-making processes (Reeves & Ashenden, 2023).

Potential of Advanced Technologies in SOC Operations

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

Figure 5 highlights the adoption rates of advanced technologies like AI and ML, as reported by Aslan and Samet, Demertzis et al., and Hore et al. (Demertzis et al., 2018; Aslan & Samet, 2017; Hore et al., 2023). The timeline demonstrates the progression from basic vulnerability awareness in 2017 to sophisticated predictive analytics in 2023, illustrating the growing reliance on these technologies to enhance SOC operations.

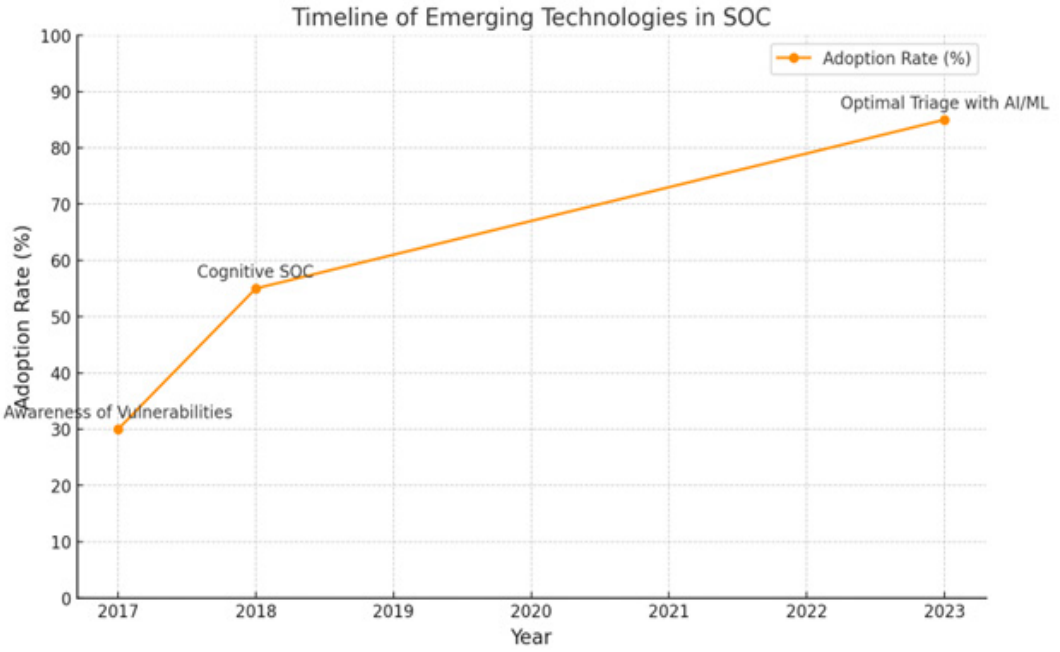

Fig. 5. Timeline of Emerging Technologies in SOC

AI and ML can process large datasets to identify trends and anomalies that may signify security threats. Predictive analytics enable SOCs to anticipate attacks and proactively strengthen defenses (Demertzis et al., 2018; Hore et al., 2023). Hore

et al. demonstrate the use of ML algorithms in optimizing vulnerability triage and mitigation efforts (Hore et al., 2023).

Machine learning models can automate routine tasks, such as alert prioritization and initial incident response actions. This automation accelerates response times and allows human analysts to concentrate on complex investigations (E Degrass - US Patent App. 17/430 & 2022, 2022; Vielberth et al., 2020). Vielberth et al. discuss the role of cognitive SOCs that leverage AI for intelligent decision-making (Vielberth et al., 2020).

AI technologies can augment human capabilities by providing insights and recommendations, effectively bridging gaps caused by staffing shortages or skill deficiencies (Aslan & Samet, 2017; Demertzis et al., 2018). Aslan and Samet highlight that AI does not replace human analysts but enhances their ability to manage threats more effectively (Aslan & Samet, 2017).

The results of this review underscore the multifaceted nature of vulnerabilities within SOCs, encompassing both technical and organizational dimensions. These vulnerabilities significantly impair the SOC's ability to detect and respond to cyber threats, necessitating a comprehensive approach to mitigation. Strategies that combine improvements in staffing, technology integration, automation, and training are essential for enhancing SOC resilience. The incorporation of AI and ML technologies presents a promising avenue for advancing SOC capabilities, offering tools to manage the increasing volume and complexity of cyber threats.

Discussion

The findings highlight the multifaceted vulnerabilities Security Operations Centers (SOCs) face, spanning both technical and organizational domains. Technical issues like tool misconfigurations, fragmented security solutions, and legacy infrastructures limit comprehensive threat detection and response capabilities, creating detection blind spots and complicating incident correlation (Demertzis et al., 2018), (Banati et al., 2022; Kiselev et al., 2022; Yuan & Zou, 2011). Meanwhile, organizational challenges—such as insufficient staffing, high turnover, inadequate training, and poor communication—further reduce SOC effectiveness by straining human resources, eroding institutional knowledge, and inhibiting timely information sharing (Agyepong et al., 2020; Kokulu et al., 2019; Janos & Dai, 2018; Reeves & Ashenden, 2023; Onwubiko & Ouazzane, 2019; Onwubiko, 2017).

Addressing these vulnerabilities demands a holistic approach. Optimizing staffing levels, enhancing continuous training, and establishing clear communication protocols can strengthen SOC teams and restore operational continuity (Onwubiko, 2015), (Kokulu et al., 2019; Reeves & Ashenden, 2023; Onwubiko & Ouazzane, 2019). Technological improvements, such as integrating interoperable security platforms and adopting automation, can streamline workflows, alleviate analyst workloads, and improve incident detection and response times (Demertzis et al., 2018; Banati et al., 2022; E Degrass - US Patent App. 17/430 & 2022, 2022; Yuan & Zou, 2011). Moreover, advanced technologies like AI and ML can bolster human-machine

collaboration by rapidly analyzing massive data streams, identifying subtle threat patterns, and providing intelligent, data-driven insights without replacing the invaluable judgment and expertise of human analysts (Aslan & Samet, 2017; Demertzis et al., 2018).

While technical advancements are essential, they are not a substitute for a skilled and adaptable workforce. Cultivating a culture of continuous learning, innovation, and collaboration remains paramount. Although this review may not capture every industry insight and is subject to the evolving threat landscape, it reinforces that future research should focus on implementing AI and ML in real-world SOC settings and examining the interplay between technological enhancements and human factors. Ultimately, improving SOC resilience hinges on integrating technical refinements with strategic workforce development to safeguard organizations against increasingly sophisticated cyber threats.

Conclusion

This review has highlighted the interconnected technical and organizational vulnerabilities affecting SOCs and their substantial impact on cybersecurity. Issues such as tool misconfigurations, outdated systems, staffing shortages, high turnover rates, inadequate training, and poor communication channels collectively reduce the SOC's ability to detect and respond promptly to sophisticated threats. These findings underscore the need for a comprehensive approach that integrates both technology and human capital.

Strengthening SOC resilience involves investing in advanced technologies like AI and ML, which can process large datasets, identify threat patterns, and automate routine tasks. Simultaneously, organizations must address staffing challenges through better resource allocation, continuous training, and fostering collaborative work environments. Ensuring that analysts remain informed, supported, and engaged is vital for maintaining robust security operations.

As cyber threats evolve, future research should investigate how AI and ML can be practically integrated into SOCs, considering factors such as trust in automation, analyst learning curves, and potential shifts in job roles. Striking a balance between innovative technology, skilled personnel, and a supportive organizational culture can ensure that SOCs remain adaptive, proactive, and effective in safeguarding organizational assets and infrastructure.

REFERENCES

Agyepong, E., Cherdantseva, Y., Reinecke, P. & Burnap, P. (2020). *Cyber Security Operations Centre Concepts and Implementation*. https://doi.org/10.4018/978-1-7998-3149-5.ch006

Anton, Philip S., Anderson, Robert H., Mesic, Richard, Scheiern, & Michael. (n.d.). *The Vulnerability Assessment & Mitigation Methodology*. RAND NATIONAL DEFENSE RESEARCH INST SANTA MONICA CA. Retrieved November 26. — 2024, from https://apps.dtic.mil/sti/citations/ADA440505

Aslan, Ö., & Samet, R. (2017). Mitigating cyber security attacks by being aware of vulnerabilities and bugs. *Proceedings - 2017 International Conference on Cyberworlds, CW 2017 - in Cooperation with: Eurographics Association International Federation for Information Processing ACM SIGGRAPH*, *2017 — January*. https://doi.org/10.1109/CW.2017.22

Banati, A., Rigo, E., Fleiner, R., & Kail, E. (2022). Use cases of attack graph for SOC optimization purpose.

ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Правила оформления статьи для публикации в журнале на сайте:
https://journal.iitu.edu.kz
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Собственник: АО «Международный университет информационных технологий» (Казахстан, Алматы)

Подписано в печать 15.12.2025.
Формат 60x881/8. Бумага офсетная. Печать - ризограф. 9,0 п.л. Тираж 100
050040 г. Алматы, ул. Манаса 34/1, каб. 709, тел: +7 (727) 244-51-09).

Издание Международного университета информационных технологий
Издательский центр КБТУ, Алматы, ул. Толе би, 59