IEEE Open Journal of the
Computer Society

Received 8 January 2025; accepted 27 January 2025. Date of publication 30 January 2025;
date of current version 21 February 2025. The review of this article was arranged by Associate Editor Jingcai Guo.

Digital Object Identifier 10.1109/OJCS.2025.3536800

The Rise of Cognitive SOCs: A Systematic Literature Review on AI Approaches

FARID BINBESHR[1], MUHAMMAD IMAM[1,2], MUSTAFA GHALEB[1], MOSAB HAMDAN[4] (Senior Member, IEEE), MUSSADIQ ABDUL RAHIM[1], AND MOHAMMAD HAMMOUDEH[3] (Senior Member, IEEE)

[1]Interdisciplinary Research Center for Intelligent Secure Systems, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia
[2]Department of Computer Engineering, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia
[3]Department of Information and Computer Science, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia
[4]School of Computing, National College of Ireland, D02 VY45 Dublin, Ireland

CORRESPONDING AUTHOR: MUHAMMAD IMAM (e-mail: mimam@kfupm.edu.sa).

This work was supported by the Interdisciplinary Research Center for Intelligent Secure Systems at King Fahd University of Petroleum and Minerals under Grant INSS2510.

ABSTRACT The increasing sophistication of cyber threats has led to the evolution of Security Operations Centers (SOCs) towards more intelligent and adaptive systems. This review explores the integration of Artificial Intelligence (AI) in SOCs, focusing on their current state, challenges, opportunities, and advantages over traditional methods. We address three key questions: (1) What are the current AI approaches in SOCs? (2) What challenges and opportunities exist with these approaches? (3) What benefits do AI models offer in SOC environments compared to traditional methods? We analyzed 38 studies using a structured methodology involving database searches, quality checks, and data extraction. Our findings show that Machine Learning (ML) techniques dominate SOC research, with a trend towards multi-approach AI methods. We classified these into ML, Natural Language Processing, multi-approach, and others, forming a detailed taxonomy of AI applications in SOCs. Challenges include data quality, model interpretability, legacy system integration, and the need for constant adaptation. Opportunities involve task automation, enhanced threat detection, real-time analysis, and adaptive learning. AI-driven SOCs show better accuracy, reduced false positives, greater scalability, and predictive capabilities than traditional approaches. This review defines Cognitive SOCs, emphasizing their ability to mimic human-like processes. We offer practical insights for SOC designers and managers on implementing AI to improve security operations. Finally, we suggest future research directions in explainable AI, human-AI collaboration, and privacy-preserving AI for SOCs.

INDEX TERMS Artificial intelligence (AI), cognitive computing, cybersecurity, deep learning, explainable AI, human-AI collaboration, machine learning, natural language processing, network security, security automation, security information and event management (SIEM), security operations center (SOC), threat detection, threat intelligence, zero trust security.

I. INTRODUCTION

The rapid evolution of cyber threats demonstrated the need for more sophisticated and proactive Security Operations Centers (SOCs). Traditional SOCs often struggle to keep pace with the dynamic and complex nature of cyber threats [1], [2], leading to significant losses for governments and industries. In 2023 alone, US consumers and businesses lost over $12.5 billion to cybercrime [3], [4], with 45% of businesses experiencing a cloud-based data breach or failing an audit [5]. These alarming statistics led to increasing interest in leveraging Artificial Intelligence (AI) to enhance SOC capabilities. AI-powered security approaches gave rise to what is now termed Cognitive SOCs. Companies increasingly emphasize SOCs' preventative capabilities, which monitor and analyze networks, devices, and repositories, forming the core of an organization's security strategy. The primary objective of these enhanced SOCs is to continually improve the organization's security posture and protect its valuable assets.

Over the past two decades, SOC operations continuously evolved. A clear indicator of this evolution is the prevalence and significant advancement of Security Information and Event Management (SIEM) systems [6]. SIEM systems are equipped with real-time correlation engines that help promptly detect attacks on a company's infrastructure. This engine is responsible for comparing logs with correlation rules stored in the database to check for any matches [3]. When security analysts identify that the company might be targeted by hacker groups, quickly establishing and updating correlation rules to combat these threats becomes a top priority for the SOC. This proactive step is crucial as the first line of defense, ensuring that the SOC can swiftly respond and mitigate potential security breaches. Security analysts typically refer to Cyber Threat Intelligence (CTI) [7] to establish correlation rules. CTI may come from reports by well-known cybersecurity companies such as FireEye and CrowdStrike, or from free security platforms like Mitre ATT&CK or exchanges among security analysts on platforms such as Telegram or X (Twitter) [8].

Today, SIEM systems play a critical role in various analyst workflows, including identifying correlated threat patterns, security monitoring, and responding to incidents. A significant evolution in SIEM systems comes from the rapidly emerging threat intelligence market, which is expected to grow rapidly in the next few years, reaching $21.92 billion by 2028 [9]. This evolution enables security operations to shift from simple alert systems to advanced mechanisms capable of utilizing threat intelligence for predictive threat analysis.

Despite these advancements, modern SIEMs face many challenges. One significant challenge facing SIEMs is the labor-intensive repetitive tasks involved in analyzing CTI reports written in natural languages. CTI is often published in reports or blog posts, requiring security analysts to spend considerable time reading and analyzing them. This process increases the response time to attacks, and SIEMs struggled to scale for a large corpus of CTI reports. Although existing works apply Machine Learning (ML) techniques to automatically extract information from security-related documents, domain-specific AI models showed inadequacies in generalization [3].

The integration of AI into SOCs, leading to the development of Cognitive SOCs, promises to address classical SIEMs limitations by enabling real-time threat detection, predictive analytics, and automated response mechanisms. These technologies can process vast amounts of data at high speed, identifying patterns and anomalies that might indicate a security threat. AI-driven SOCs can detect known threats more efficiently and predict and identify new, previously unseen threats. This predictive capability is crucial for staying ahead of cyber adversaries who continually evolve their tactics to exploit new vulnerabilities [10]. As a result, cognitive SOCs leverage ML algorithms to analyze network traffic, user behavior, and system logs in real-time, providing security analysts with actionable insights and automated responses to mitigate threats. This reduces the time to detect and respond to incidents, minimizes the impact of breaches, and enhances the overall security posture of an organization. Furthermore, AI technologies can help automate routine tasks, freeing up security analysts to focus on more complex and strategic activities [10]. However, the application of these technologies in SOCs is still in its nascent stages, and there is a significant gap in the literature regarding their effectiveness, challenges, and potential improvements. This gap highlights the need for a comprehensive review to synthesize current knowledge and identify areas for future research.

A. MOTIVATION AND BACKGROUND

The motivation for this research stems from the observed limitations in traditional SOCs. Despite implementing advanced tools and methodologies, traditional SOCs are often reactive rather than proactive, leading to delayed responses and increased vulnerability. The sheer volume and complexity of data generated by modern IT environments make it challenging for human analysts to promptly detect and respond to threats. Integrating AI into SOCs promises to address these limitations by enabling real-time threat detection, predictive analytics, and automated response mechanisms [3], [10].

Traditional SOCs rely heavily on manual processes and rule-based systems, which can be slow and prone to errors. AI, on the other hand, can analyze vast amounts of data at high speed and identify patterns that may indicate a security threat. This capability is crucial given the increasing sophistication of cyber-attacks, which often involve subtle and complex tactics that can evade conventional detection methods. Moreover, the growing adoption of technologies such as the Internet of Things (IoT) and cloud computing expanded the attack surface, making it even more critical for SOCs to leverage advanced technologies to enhance their defenses [10].

B. SCOPE AND CONTRIBUTION

This Systematic Literature Review (SLR) aims to comprehensively evaluate the current state of AI approaches in SOCs. By synthesizing existing research, this review seeks to identify the key trends, challenges, benefits, and limitations associated with implementing AI solutions in SOC environments. The primary aim of this SLR is to determine the extent to which AI solutions improve SOC performance. The objectives are structured around several research questions:

1) What are the current state-of-the-art AI approaches in SOCs?
2) What are the key challenges and opportunities associated with implementing these approaches in the SOC environment?
3) What are the specific benefits and advantages of applying AI models in SOC environments compared to traditional SOC approaches?

The need for this review is justified by the growing complexity of cyber threats and the corresponding necessity for more intelligent and adaptive SOCs. This review has significant implications for both theory and practice. The findings can inform the development of more effective and efficient

SOCs, contribute to the academic discourse on cybersecurity, and provide practical insights for organizations looking to enhance their SOC capabilities through AI technologies. The contributions of this article are as follows:

- State-of-the-Art Analysis: Provide a comprehensive analysis of current AI approaches in SOCs, categorizing them into ML, Natural Language Processing (NLP), multi-approach, and other techniques.
- Cognitive SOC Definition: Synthesize insights from 38 studies to formulate a consolidated definition of SOCs with cognitive capabilities.
- Challenges and Opportunities: Identify key challenges in implementing AI in SOCs, such as data quality and model interpretability, alongside opportunities like automation and enhanced threat detection.
- Comparative Analysis: Highlight the specific benefits of AI-driven SOCs over traditional approaches, including improved accuracy, reduced false positives, and predictive capabilities.
- Future Research Directions: Suggesting areas for further investigation to advance cognitive SOC technologies and practices.

C. ARTICLE ORGANIZATION

This article is organized as follows: The Related Works section provides an overview of previous research in the field, highlighting key findings, and identifying gaps that this review aims to address. The Review Methodology section details the systematic approach used to conduct the literature review, including database identification, search query formulation, eligibility criteria, study selection, quality assessment, and data extraction. The findings from the reviewed studies, including study characteristics and quality assessment results, are presented in the Results section. The Discussion section explores the answers to the research questions, discusses the current state-of-the-art AI approaches in SOCs, identifies key challenges and opportunities, and highlights the specific benefits of AI models in SOC environments. Finally, the Conclusion section summarizes the main findings and suggests directions for future research.

II. RELATED WORKS

Recent studies explored various aspects of SOCs, focusing on their foundational elements, processes, technology, and the integration of AI. Here, we review several key works to highlight their contributions and limitations, providing a basis for understanding the context and gaps addressed in our research.

A. SOC CHALLENGES AND AUTOMATION

Shutock and Dietrich [15] conducted a comprehensive review of the challenges and solutions associated with SOCs. Their study highlighted the difficulties in integrating automation and advanced tools within SOCs, stressing the need to balance technological advancements with human expertise to maintain effective operations. This work identifies the ongoing challenges in achieving seamless automation and tool integration in SOCs.

Vielberth et al. [1] carried out a systematic study on SOCs, identifying open challenges such as the need for improved AI-driven solutions and enhanced collaboration between SOC components they emphasized the complexity of modern SOC operations and the necessity of leveraging advanced technologies and methodologies. Their research highlights critical gaps in current SOC operations, particularly regarding the effective use of AI.

B. AI AND ML INTEGRATION

The usability issues of ML-based tools in SOCs was assessed in [12]. This study showed that while ML tools offer substantial potential, their practical application is often limited by usability concerns, leading to increased workload and decreased efficiency for SOC analysts. This highlights the importance of designing user-friendly AI tools that can be seamlessly integrated into SOC workflows.

Moreover, the authors in [10] explored the application of AI in SOCs, focusing on detecting and responding to advanced cyber threats such as Advanced Persistent Threats (APTs) and zero-day attacks. This study research confirmed the transformative potential of AI in enhancing SOC capabilities and noted the ongoing challenges in implementation and scalability. This work is pivotal in understanding the current state-of-the-art and the practical challenges SOCs face in adopting AI technologies.

C. OPERATIONAL AWARENESS AND FRAMEWORKS

Ofte et al. [16] discussed the essential aspects of tactical cyber situational awareness within SOCs, emphasizing the importance of shared understanding and coordination. Their research stressed the need for effective situational awareness tools and processes to enhance SOC performance. This study highlights the critical role of situational awareness in SOC operations and the challenges in achieving it.

Similarly, Duna, et al. [13] provided a comparative study on implementing SOCs, noting the lack of adequate criteria or standard frameworks for building SOCs or hiring third-party SOC providers. Their study proposed a system for Next-Generation SOCs (NGSOC) for the Industrial Internet of Things (IIoT), emphasizing the integration of individuals, processes, and technology for improved cybersecurity threat prevention and identification.

D. INTEGRATION ARCHITECTURES

Shahjee and Ware [14] systematically analyzed the integration of Network Operation Centers (NOC) and SOCs, proposing an integrated architecture to counter cyber-security attacks, threats, and vandalism at a reduced operational cost. They highlighted the lack of comprehensive definitions and frameworks for such integration, which is vital for overcoming silos in SOC and NOC operations.

TABLE 1. Comparison of Survey Works on SOC Topics, Highlighting the Coverage of Various Aspects Such as SLR, Taxonomy, Cognitive Capabilities, AI Integration, Traditional vs Cognitive SOC, and Challenges and Opportunities Across Different Studies

Survey Paper	Year	SLR	Taxonomy	Cognitive Capabilities in SOCs	AI Integration	Traditional SOC Vs Cognitive SOC	Challenges and Opportunities
[11]	2019	X	X	X	X	X	X
[1]	2020	✓	✓	X	✓	X	X
[12]	2020	X	X	X	✓	X	X
[13]	2021	X	✓	X	X	X	X
[14]	2022	✓	X	X	✓	X	X
[15]	2022	X	✓	X	✓	X	X
[2]	2023	✓	X	X	X	X	X
[16]	2023	✓	X	✓	X	✓	X
[10]	2023	X	✓	X	✓	X	X
Our Work	**2024**	✓	✓	✓	✓	✓	✓

E. PERFORMANCE ANALYSIS

The issues faced by SOCs were investigated in [11] through a qualitative study, identifying both technical and non-technical challenges. Their study highlighted the disagreements between SOC managers and analysts, hindering SOC efficiency and effectiveness. They emphasized the need for better communication and understanding within SOC teams to improve overall performance.

Agyepong, et al. [2] proposed a systematic method for measuring the performance of SOC analysts, focusing on key performance indicators and metrics to evaluate SOC efficiency. Their work provides a framework for assessing and improving the performance of SOC operations.

Our research differs from these previous works by specifically focusing on integrating cognitive capabilities into SOCs, leveraging the latest advancements in AI to propose more intelligent and adaptive security solutions. By systematically reviewing the literature, we aim to provide a comprehensive and up-to-date overview of the current state and future directions of cognitive SOCs. Unlike previous studies that often focus on isolated aspects of SOC operations, our research provides a holistic analysis of cognitive SOCs, emphasizing the integration of AI to address cyber threats' complex and evolving nature. Furthermore, we critically analyze the existing literature to identify significant gaps and propose future research directions to help bridge these gaps, thereby contributing to both academic research and practical advancements in SOC technology and management. Additionally, a comparison of the survey works on SOC topics and their respective targets is provided in Table 1.

The table columns show the survey papers, year, SLR, taxonomy, Cognitive Capabilities in SOCs, AI integration, traditional SOC Vs cognitive SOC, and challenges and opportunities. The symbol ✓ indicates whether the subject is covered in the respective survey.

III. REVIEW METHODOLOGY

This section outlines the procedures adopted to carry out this SLR. Following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines [17] - the gold standard for systematic literature reviews - we detail the process of identifying suitable research databases, formulating the search query, establishing eligibility criteria, selecting relevant studies, conducting quality assessments, and devising a data extraction strategy. It details the process of identifying suitable research databases, formulating the search query, establishing eligibility criteria, selecting relevant studies, conducting quality assessments, and devising a data extraction strategy.

TABLE 2. Settings of the Search Query Across Different Databases, Detailing the Specific Refinement Criteria Used for Each Database to Ensure Comprehensive and Relevant Search Results

Databases	Refine By
IEEE Xplore	conferences and journals
ACM	Content type: Research Article
Scopus	Document type: conference paper and article; Language: English
WOS	Document type: article, proceeding paper, or early access
SienceDirect	Article type: research articles
Wiley	Article type: research articles
Taylor & Francis	-

A. DATABASES IDENTIFICATION

For this SLR, we investigated multiple research databases and selected IEEE Xplore (IEEE), the Association for Computing Machinery (ACM), Scopus, Web of Science (WoS), ScienceDirect, Wiley, and Taylor & Francis based on their ability to provide comprehensive and relevant search results aligned with our research objectives. Several other databases such as SpringerLink, Google Scholar, CiteSeerX, and Microsoft Academic were also explored but excluded after careful evaluation due to relevance and redundancy considerations.

In contrast, databases such as SpringerLink, Google Scholar, CiteSeerX, and Microsoft Academic were excluded from the review due to their tendency to produce irrelevant results or, in some cases, a complete lack of relevant articles. Table 2 outlines the settings of the search queries applied across the selected databases, detailing the specific refinement criteria used to ensure a thorough and focused collection of research materials.

B. SEARCH QUERY

We employed a focused search strategy to identify relevant studies relating to "Security Operation Centers" and the integration of advanced technologies such as "Machine Learning" and "Artificial Intelligence". Recognizing the varied terminologies used across the literature, we incorporated synonymous keywords to ensure a comprehensive search. The selected keywords for "Security Operation Centers" include "Cybersecurity Operation Centers" and related variations. For advanced technologies, keywords like "Deep Learning", AI, "Artificial Intelligence", cognitive, intelligent, and "next-gen" were used. The search string formulated for the databases is as follows:

"("Security Operation* Cent*" OR "Cybersecurity Operation* Cent*") AND ("Machine Learning" OR "Deep Learning" OR AI OR "Artificial Intelligence" OR cognitive OR intelligent OR next-gen* OR "Next Gen*")".

C. ELIGIBILITY CRITERIA

We applied the following eligibility criteria to ensure that the selected articles are relevant and of high quality:

IC1 Articles that utilize AI within SOC. These articles are essential to addressing the primary research question focused on AI applications in SOCs.

IC2 Original research articles that contribute new empirical findings. SLRs prioritize primary research to ensure a solid foundation of original and directly relevant data.

IC3 Articles written in the English language. It is challenging to access and accurately interpret articles in other languages, ensuring consistency and comprehensibility of the reviewed studies.

IC4 Articles that are fully accessible without restrictions. Full access to articles is necessary to comprehensively evaluate the research and address the research questions effectively.

D. STUDY SELECTION

The study selection process was conducted in several stages. Initially, the search string was applied across the chosen databases, and the resulting articles were imported into EndNote software for effective management. Following this, duplicate articles were identified and removed. The remaining articles were then screened based on their titles, abstracts, and keywords, with irrelevant ones being excluded. Finally, the remaining articles were read in full to extract the necessary data and ensure they met the eligibility criteria. These steps were carried out by three authors to maintain consistency with the predefined eligibility criteria.

E. QUALITY ASSESSMENT

To ensure a rigorous selection of literature for this review, we developed a comprehensive quality assessment framework. This framework serves as a critical tool in determining the appropriateness and value of the articles that passed our initial filtering process. Our assessment methodology employs a ten-point checklist, carefully designed to evaluate the potential contributions of each selected study to our review. Table 3 presents this checklist in detail.

The evaluation process involves a nuanced scoring system for each criterion:

- A score of 1 is assigned when an article fully satisfies a criterion.
- 0.5 points are awarded for partial fulfillment.
- 0 points are given when a criterion is not met at all.

This granular approach allows for a more precise assessment of each study's strengths and weaknesses across a broad range of quality indicators. The aggregate quality score for each article is calculated by summing the scores across all ten criteria, resulting in a possible range from 0 to 10. This cumulative score serves as a quantitative measure of the overall quality of each study, with higher scores indicating superior methodological rigor and relevance to our research objectives.

TABLE 3. Quality Assessment Checklist Used to Evaluate the Selected Articles, Covering Ten Criteria Across Design, Conduct, Analysis, and Conclusion Aspects of the Studies

Quality Parameter	Check Question
Design	Q01: Is the aim explicitly stated? Q02: Is the research method/design suitable and well-chosen? Q03: Is the study setting reproducible and adequately justified? Q04: Is the dataset accessible, relevant, and appropriate to the study? Q05: Are the measures used in the study fully defined and relevant?
Conduct	Q06: Are the data collection methods thoroughly described?
Analysis	Q07: Are the data analysis methods clearly and adequately explained? Q08: Are the results compared with findings from previous research?
Conclusion	Q09: Are the findings clearly stated and well-supported by the results? Q10: Are the study's limitations explicitly presented and discussed?

F. DATA EXTRACTION STRATEGY

To facilitate a systematic and comprehensive analysis of the selected literature, we developed a structured data extraction template using Microsoft Excel. This template was designed to capture essential information that directly addresses our research questions while simultaneously allowing for a thorough assessment of each article's quality. Our data extraction form encompasses numerous key elements, including:

1) Bibliographic information (ID, Title, Year, Author(s), Publication Type, Venue Name)
2) Research focus (Problem(s), Solution(s), Context/ Application)
3) Methodological details (AI Techniques, Research/Data collection method, Data Analysis Method)
4) Results and critical analysis (Findings, Limitations)
5) Dataset characteristics (Type, Size, Features, Labels)
6) Data handling techniques (Preprocessing, Cross-validation, Data Splitting, Data augmentation)
7) Model information (Pre-trained models used)
8) Tools and metrics employed
9) Comparative analysis (Methods Comparison)
10) Reviewer's insights (Comments/Notes, Category assignment)

This comprehensive data extraction strategy ensures a systematic and consistent approach to analyzing each selected article. By capturing a wide range of information, we can conduct a thorough analysis that informs our research questions and underpins the subsequent quality assessment.

IV. RESULTS

A. STUDY SELECTION RESULTS

The study selection process for this systematic literature review is illustrated in Fig. 1. Initially, 391 articles were retrieved from the databases and imported into EndNote for processing. Utilizing EndNote's duplicate removal feature, 142 duplicate articles were eliminated. Subsequently,

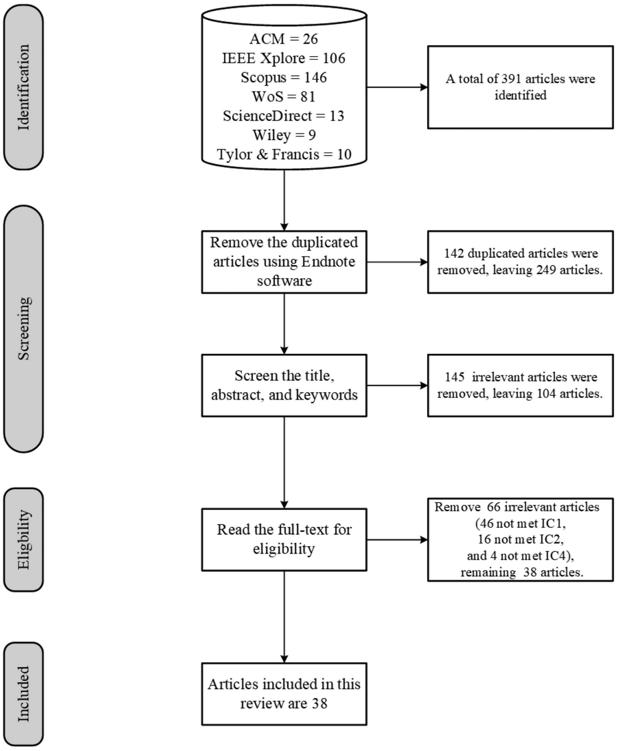
Identification
Screening
Eligibility
Included
ACM = 26
IEEE Xplore = 106
Scopus = 146
WoS = 81
ScienceDirect = 13
Wiley = 9
Tylor & Francis = 10
A total of 391 articles were identified
Remove the duplicated articles using Endnote software
142 duplicated articles were removed, leaving 249 articles.
Screen the title, abstract, and keywords
145 irrelevant articles were removed, leaving 104 articles.
Read the full-text for eligibility
Remove 66 irrelevant articles (46 not met IC1, 16 not met IC2, and 4 not met IC4), remaining 38 articles.
Articles included in this review are 38

FIGURE 1. Flow diagram of the systematic literature review process, showing the number of articles at each stage of screening and selection.

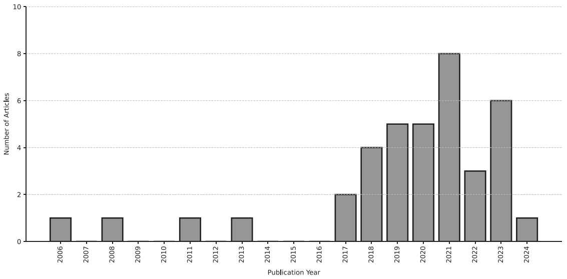

FIGURE 2. Distribution of selected articles by year of publication, showing an increase in research activity from 2017 to 2021.

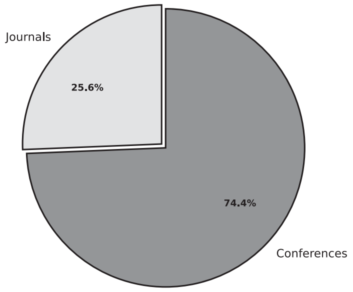

FIGURE 3. Pie chart showing the distribution of publications by type, with conferences accounting for 74.4% and journals for 25.6% of the selected articles.

an initial screening was conducted, where the remaining 249 articles were evaluated based on their titles, abstracts, and keywords. This led to the exclusion of 145 irrelevant articles. The full texts of the remaining 104 articles were then downloaded for further review. During this in-depth review, 65 articles were excluded for reasons such as irrelevance, being review articles rather than primary research, or being inaccessible. Consequently, the final selection comprised 38 studies.

B. STUDY CHARACTERISTICS

This section examines the key characteristics of the research articles identified through our systematic review process.

1) OVERVIEW OF AI TECHNIQUES

Our analysis encompassed a total of 38 studies (S01-S38) published between 2006 and 2024, as detailed in Table 4. The distribution of publication types reveals a balanced mix of journal articles and conference papers, with 14 journal publications and 24 conference proceedings. As shown in the table, the venues for these publications span a wide range of reputable sources in the fields of computer science, cybersecurity, and artificial intelligence. Notable journals include IEEE Transactions on Dependable and Secure Computing, Computers & Security, and IEEE Access, while prominent conference venues include various IEEE-sponsored events such as the International Conference on Big Data and the International Conference on Software Analysis, Evolution and Reengineering (SANER). Table 4 provides a comprehensive overview of each study, including the authors, publication years, publication types, and specific venues, offering readers a detailed reference for the literature included in this review.

2) TEMPORAL DISTRIBUTION AND PUBLICATION VENUES OF SOC AI STUDIES

The distribution of the selected articles based on the year of publication is shown in Fig. 2. Interestingly, there is a noticeable increase in research activity beginning around 2017, peaking in 2021. This trend reflects the growing recognition of AI and ML's potential to transform SOCs by automating tasks, enhancing threat detection, and managing the rising volume of security alerts. The surge in publications during these years underscores the urgency and importance placed on developing cognitive technologies to address the escalating complexity of cyber threats. The lower number of publications in earlier years indicates that the integration of AI into SOCs is a relatively recent focus within the research community. This trend highlights a shift toward more sophisticated and intelligent cybersecurity solutions.

The distribution of publications by type, as illustrated in Fig. 3 reveals that about two-thirds of the selected articles (28 articles) are from conferences, reflecting the fast-paced research in AI for SOCs. Journals, though fewer (10 articles), provide in-depth and peer-reviewed studies, highlighting the balance between rapid dissemination and thorough exploration.

As shown in Fig. 4, the distribution of research contexts indicates that a majority of studies are conducted within general cybersecurity environments, reflecting broad applicability

TABLE 4. Comprehensive List of 38 Publications Related to AI in SOC, Including Author Information, Publication Year, Type, and Venue, Spanning From 2006 to 2024

ID	Author (Year)	Type	Venue
S01	Vaarandi et al. (2024) [18]	Journal	Future Generation Computer Systems
S02	Sworna et al. (2023) [19]	Journal	ACM Trans. on Software Engineering and Methodology
S03	Sworna et al. (2023) [20]	Conference	IEEE Int. Conf. on Software Analysis, Evolution and Reengineering
S04	Presekal et al. (2023) [21]	Conference	IEEE Int. Conf. on Comm., Control, and Computing Tech. for Smart Grids
S05	Marmureanu et al. (2023) [22]	Conference	IEEE Int. Conf. on Comm., Control, and Computing Tech. for Smart Grids
S06	Jang et al. (2023) [23]	Journal	Sensors
S07	Hore et al. (2023) [24]	Journal	IEEE Trans. on Dependable and Secure Computing
S08	Kim et al. (2022) [25]	Journal	Computers & Security
S09	Islam et al. (2022) [26]	Journal	Journal of Network and Computer Applications
S10	Chiba et al. (2022) [27]	Journal	IEEE Access
S11	Wang et al. (2021) [28]	Conference	Int. Symposium on Grids & Clouds
S12	Perera et al. (2021) [29]	Conference	Int. Conf. for Convergence in Technology
S13	Ndichu et al. (2021) [30]	Conference	IEEE Int. Conf. on Big Data
S14	Ongun et al. (2021) [31]	Conference	IEEE Conf. on Communications and Network Security
S15	Najafi et al. (2021) [32]	Conference	Security and Privacy in Communication Networks
S16	Khan et al. (2021) [33]	Journal	Int. Journal of Cognitive Informatics and Natural Intelligence
S17	Choi et al. (2021) [34]	Conference	Asia Joint Conf. on Information Security
S18	Ban et al. (2021) [35]	Conference	Proc. of the 14th Cyber Security Experimentation and Test Workshop
S19	AfzaliSeresht et al. (2020) [36]	Conference	Not specified
S20	Shah et al. (2020) [37]	Journal	IEEE Trans. on Parallel and Distributed Systems
S21	Nishiyama et al. (2020) [38]	Conference	IEEE Symposium on Computers and Communications
S22	Karacay et al. (2020) [39]	Journal	The Computer Journal
S23	Yang et al. (2020) [40]	Conference	Information and Communications Security
S24	Shibahara et al. (2019) [41]	Conference	ACM Workshop on Artificial Intelligence and Security
S25	Huang et al. (2019) [42]	Conference	IEEE Int. Conf. on Big Data
S26	Gupta et al. (2019) [43]	Conference	IEEE Int. Conf. on Big Data
S27	Cazacu et al. (2019) [44]	Conference	eLearning and Software for Education Conf.
S28	Bienia et al. (2019) [45]	Conference	IEEE Int. Conf. on Enabling Technologies
S29	Demertzi et al. (2018) [46]	Journal	Big Data and Cognitive Computing
S30	Oprea et al. (2018) [47]	Conference	Annual Computer Security Applications Conf.
S31	Graf et al. (2018) [48]	Conference	Int. Conf. on Cyber Conflict
S32	Funaya et al. (2018) [49]	Conference	IEEE Conf. on Dependable and Secure Computing
S33	Feng et al. (2017) [50]	Conference	IEEE Int. Conf. on Intelligence and Security Informatics
S34	Erola et al. (2017) [51]	Conference	Int. Conf. on Cyber Situational Awareness, Data Analytics and Assessment
S35	Li et al. (2013) [52]	Journal	Int. Journal of Communication Systems
S36	Zhang et al. (2011) [53]	Conference	Int. Conf. on Intelligent Computation Technology and Automation
S37	Niu et al. (2008) [54]	Conference	Int. Conf. on Computational Intelligence and Security
S38	Niu et al. (2006) [55]	Conference	Int. Conf. on Computer-Aided Industrial Design and Conceptual Design

across various domains. SOCs account for a notable portion of the studies, underscoring the critical role these entities play in cybersecurity research. Additional contexts include corporate environments, educational institutions, Industrial Control Systems (ICS), large enterprises or Internet Service Providers (ISPs), and security vendors, suggesting a diversified approach to addressing cybersecurity challenges across different sectors.

3) AI APPROACHES IN SOC RESEARCH

a) Categories: The studies in our analysis employ a diverse range of AI techniques, which we categorized into four main groups with subcategories for clarity (see Fig. 5).

ML including traditional ML and Deep Learning (DL): Representing 71.1% of the studies (27 out of 38), this group is further divided into the following subcategories:

- Traditional ML: Encompassing 42.1% of the studies (16 out of 38), specifically in S01, S07, S09, S10, S13, S18, S20, S21, S22, S25, S27, S28, S29, S30, S32, and S34. These studies focus primarily on traditional ML methods for predictive modeling and classification tasks, reflecting the continued importance of ML in SOC environments.
- DL: Covering 29% of the studies (11 out of 38), specifically S02, S03, S04, S06, S08, S11, S24, S26, S31, S37, and S38. These studies employ advanced neural network

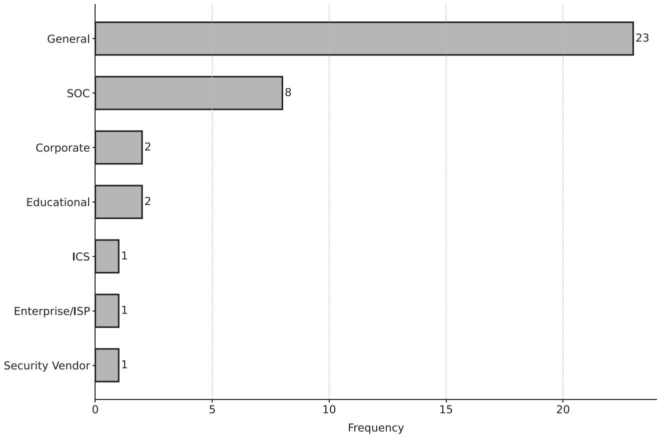

FIGURE 4. Bar chart illustrating the distribution of research contexts across the selected studies, with general cybersecurity environments being the most common.

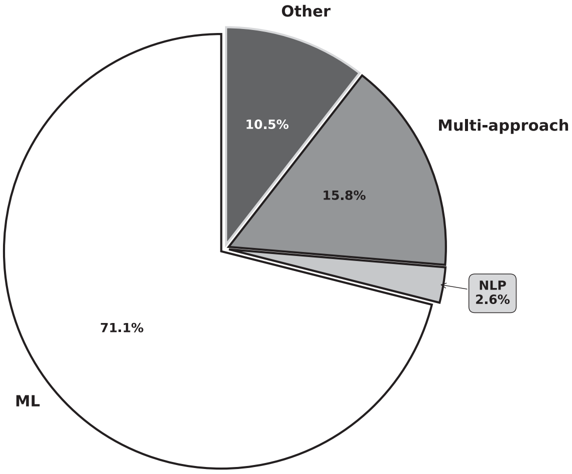

FIGURE 5. Distribution of AI categories in SOC research. ML (Traditional ML and DL) represents the most prevalent approach at 71.1%, followed by Multi-approach (15.8%), Other (10.5%), and NLP (2.6%). Traditional ML and DL account for 42.1% and 29% of total studies respectively.

techniques such as CNN, transfer learning, graph networks, and autoencoders, which are vital for processing complex data patterns in cybersecurity.

NLP: Utilized in 2.6% of the studies (1 out of 38), specifically S19. This method is mainly applied to text-based threat analysis and detection tasks, reflecting its unique but focused application in SOC research.

Multi-approach: Present in 15.8% of the studies (6 out of 38), that integrate different AI techniques like ML+DL, ML+NLP, and ML+DL+NLP. These studies, specifically S05, S12, S14, S17, S23, and S33, compare the effectiveness of different approaches, combining models from multiple AI categories to optimize performance in complex SOC tasks.

Other Approaches: Used in 10.5% of the studies (4 out of 38). These include research techniques that don't strictly fall into the other categories, offering innovative solutions to specific cybersecurity challenges.

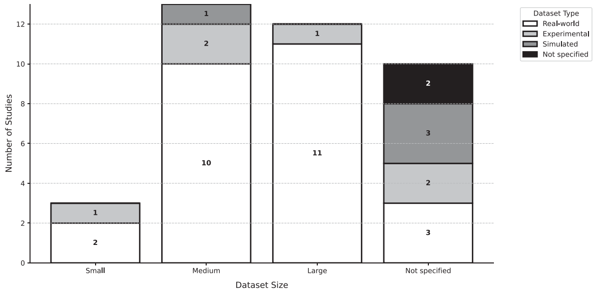

FIGURE 6. Stacked bar chart showing the distribution of dataset types (real-world, experimental, simulated, and not specified) across different dataset sizes in the selected studies.

This distribution highlights the predominance of ML techniques in SOC research. Mulit-approaches also play a significant role, indicating the value of integrating multiple AI techniques. NLP, while less frequently used on its own, is often incorporated into multi-approach techniques. The presence of other approaches demonstrates the diverse and innovative nature of AI applications in SOC research.

b) Datasets: The datasets used in SOC research exhibit significant diversity in type, size, and content, reflecting the complex nature of cybersecurity challenges (see Fig. 6). We categorize these datasets into three main types based on their origin and characteristics: real-world data, experimental data, and simulated or synthetic data.

Real-world data is the most prevalent, used in 26 studies (68.4%), including S01, S06, S08, S09, S10, S11, S17, S18, S21, S22, S23, S25, S26, S27, S28, S29, S30, S31, S32, S33, S34, S35, S36, S37, and S38. These datasets consist of actual security logs, network traffic, and events collected from production environments, providing authentic threat patterns and security incidents. They are particularly valuable for threat detection model training, anomaly detection, and real-world performance validation.

Experimental data, typically involving testbed setups and generated traffic, is employed in 6 studies (15.8%), such as S03, S05, S13, S14, S15, and S24. These datasets are generated in controlled laboratory environments or testbeds, offering a balance between realism and controlled conditions. They are particularly useful for testing specific attack detection capabilities, validating defense mechanisms, and benchmarking performance.

Simulated or synthetic data is utilized in 4 studies (10.5%), including S02, S04, S16, and S20. These datasets are artificially generated using simulation tools and mathematical models, helping address privacy concerns and data scarcity. They are particularly valuable in scenarios where real data is scarce, in privacy-sensitive applications, and for testing rare attack scenarios.

The dataset type for 2 studies (5.3%), specifically S07 and S12, was not specified.

Dataset sizes also vary widely. Large datasets exceeding 1 million samples are used in 12 studies (31.6%), including S01, S06, S08, S13, S14, S15, S17, S18, S24, S25, S30, and S33. Examples include S14 with 9.64 billion events and S17 with 56,478,922 events. Medium-sized datasets (10K-1 M samples) are used in 13 studies (34.2%), such as S04, S07, S09, S10, S16, S20, S21, S22, S23, S26, S29, S31, and S32. Examples include S06 with 1,276,275 events and S22 with around 40, 000 samples across different datasets. Small datasets ($< 10Ksamples$) are employed in 3 studies (7.9%), namely S02, S03, and S05, with examples like S02 using 815 API descriptions and S05 using 5,290 queries. The dataset size for 10 studies (26.3%) was not specified, including S11, S12, S19, S27, S28, S34, S35, S36, S37, and S38.

Several mainstream datasets serve essential roles in SOC security research, each capturing different aspects of cyber threats and security operations. The Enterprise Network Dataset from S17 stands out with over 56 million events spanning 1,459 IDS/IPS signatures collected over two years, while the ISCX-CIC Dataset family provides researchers with labeled network traffic data across three key collections: ISCX-Saturday (13, 775 records), CIC-Friday-Morning (13, 371 records), and CIC-Friday-Afternoon (13, 543 records). These are complemented by large-scale SOC alert collections, exemplified by S24's dataset of 5 million monthly alerts, and comprehensive threat intelligence repositories like S23's collection of 25, 092 CTI documents.

The evolution and diversity of these datasets reflect the changing landscape of security operations, from traditional intrusion detection to modern threat analysis. While established benchmarks like the DARPA Dataset continue to provide baseline metrics with its 2,658 labeled alerts, newer collections capture the complexity of contemporary threats and the scale of enterprise security operations. Together, these datasets enable researchers to evaluate detection capabilities, test analysis methods, and develop new approaches for processing security events and threat intelligence.

Other data types include threat intelligence data (e.g., S23, S30, S31), API descriptions (S02, S03), and incident response plans (S03). Some studies utilize unique data types such as user activity data, SIEM data, and video recordings (S27). The diversity in data types underscores the multifaceted nature of SOC operations and the varied approaches researchers are taking to address cybersecurity challenges.

Fig. 6 illustrates the distribution of dataset types across different dataset sizes. The figure clearly shows that real-world data dominates across all size categories, with a particularly strong presence in large datasets and those with unspecified sizes. This distribution reflects the field's emphasis on working with authentic security data, while also indicating areas where experimental and simulated data play important roles, especially in smaller-scale studies.

The prevalence of real-world datasets, particularly in larger sizes, suggests a trend towards more realistic and comprehensive analyses in SOC research. However, the significant number of studies with unspecified dataset size information (11 studies, 28.9%) highlights a need for more transparent reporting of dataset characteristics in future research. This lack of specificity in dataset size reporting presents a challenge in fully understanding the scale and scope of data used in some SOC studies.

c) Preprocessing techniques: Preprocessing plays a crucial role in SOC research due to the complex and often noisy nature of security data. Our analysis of the 38 studies reveals a variety of preprocessing techniques employed to prepare data for AI models. The most common preprocessing techniques observed are:

1) Normalization and Standardization: Used in 11 studies (28.9%), including S04, S07, S08, S09, S10, S17, S24, S25, S28, S29, and S31. This technique helps in scaling features to a common range, improving model performance.
2) Encoding: Particularly one-hot encoding, employed in 7 studies (18.4%), including S05, S13, S18, S25, S26, S28, and S32. This is crucial for converting categorical data into a format suitable for machine learning algorithms.
3) Data Cleaning: Applied in 9 studies (23.7%), including S02, S15, S16, S17, S18, S28, S34, S35, and S37. This involves removing noise, handling missing values, and eliminating irrelevant data.
4) Feature Engineering: Observed in 7 studies (18.4%), notably S06 (feature hashing), S24, S26, S29, S32, S33, and S37. This process involves creating new features or modifying existing ones to improve model performance.
5) Balancing Techniques: Applied in 5 studies (13.2%) to handle class imbalance, including S01, S08, S09, S13, and S25. Techniques such as SMOTE and random undersampling were used.
6) Text Preprocessing: Used in 5 studies (13.2%) dealing with textual data, including S02, S11, S23, S31, and S36. This involves techniques like tokenization, stopword removal, and lemmatization.
7) Dimensionality Reduction: Mentioned in 2 studies (5.3%), including S32 (matrix factorization) and potentially in studies using autoencoders.
8) Domain-specific preprocessing: Several studies employed techniques specific to cybersecurity data, such as log analysis (S21), payload vectorizing (S17), and alert correlation (S35).

It is worth noting that 10 studies (26.3%) did not specify their preprocessing techniques, which highlights a need for more transparent reporting in future research. Many studies employed multiple preprocessing techniques, reflecting the complex nature of SOC data and the need for comprehensive data preparation strategies.

Fig. 7 illustrates the distribution of preprocessing techniques across the studies, highlighting the prevalence of normalization, encoding, and data cleaning in SOC research.

Fig. 8 presents a comprehensive visualization of the data preprocessing pipeline employed in SOC environments. The pipeline begins with raw SOC data collection and progresses through several critical stages. The initial data cleaning phase addresses three key aspects: noise removal for handling missing values, filtering of irrelevant data, and domain-specific

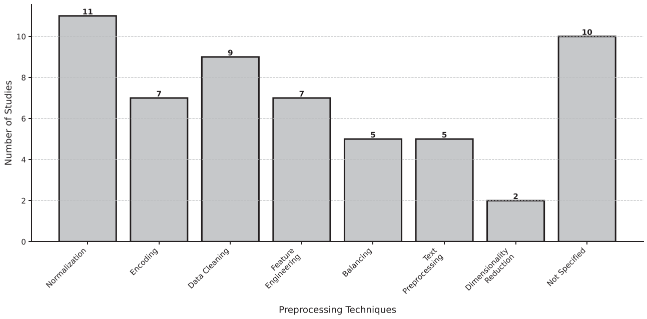

FIGURE 7. Bar chart illustrating the frequency of various preprocessing techniques used in SOC studies, with normalization and data cleaning being the most common.

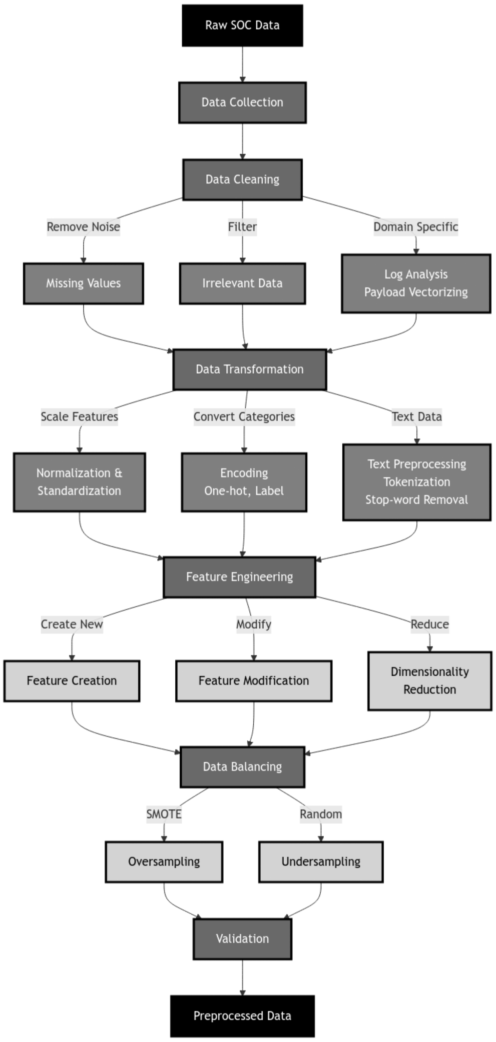

FIGURE 8. Data preprocessing pipeline in SOC environments, outlining the systematic transformation of raw security data through severeal key stages.

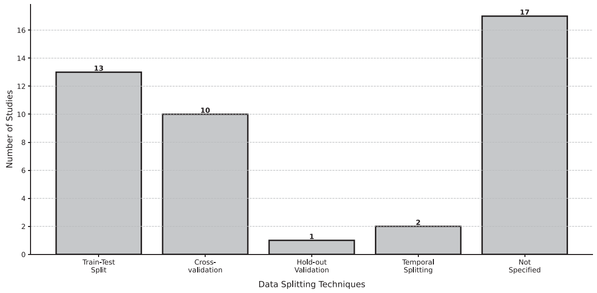

FIGURE 9. Bar chart showing the distribution of data splitting techniques used in the selected studies, highlighting the prevalence of train-test splits and cross-validation.

processing such as log analysis and payload vectorizing. Data transformation follows, incorporating scale feature normalization, category conversion through encoding, and text data preprocessing. The feature engineering stage introduces new features while modifying existing ones, with an option for dimensionality reduction. The final stages involve data balancing through SMOTE oversampling or random undersampling techniques, followed by validation to ensure data quality. This structured approach ensures that security data is properly prepared for AI model training while maintaining the integrity of security-relevant information.

d) Data splitting: Data splitting plays a crucial role in evaluating the performance and generalizability of AI models in SOC research. Our analysis of the 38 studies reveals diverse approaches to data splitting, with some studies employing multiple techniques (see Fig. 9). The most prevalent method is the train-test split, used in 13 studies (34.2%). This approach typically involves dividing the dataset into training and testing subsets, with common ratios including 80-20 (5 studies), 70-30 (3 studies), and 90-10 (2 studies). Train-test splitting is straightforward and provides a clear separation between training and evaluation data, but it may not fully capture the model's performance across different subsets of the data.

Cross-validation, employed in 10 studies (26.3%), is the second most common technique. Variations include k-fold cross-validation (7 studies) and stratified k-fold (1 study). Some studies specified the number of folds, with 5-fold and 10-fold being the most common. Cross-validation helps to mitigate the risk of overfitting and provides a more robust estimate of model performance, especially useful when dealing with limited datasets common in SOC research.

Hold-out validation was explicitly mentioned in one study, while temporal splitting, though not explicitly stated, is implied in studies dealing with time-series data (2 studies). Temporal splitting is particularly relevant for SOC research, as it mimics real-world scenarios where models are trained on historical data and tested on future events. This approach helps in assessing a model's ability to generalize to new, unseen patterns of cyber threats.

Notably, 17 studies (44.7%) did not provide clear information about their data splitting approach, highlighting a significant gap in methodological reporting. Some studies adopted unique or multi approaches, such as using "83.3% Top-10 Accuracy for downstream mapping" or combining cross-validation with a train-validation split. The diversity in data splitting techniques reflects the varied nature of SOC data

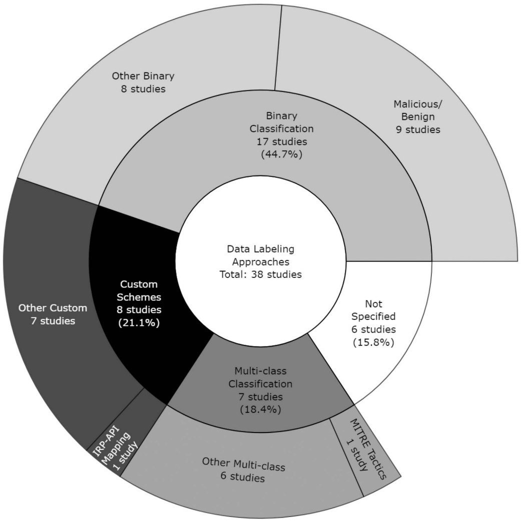

FIGURE 10. Sunburst diagram illustrating the distribution of data labeling approaches in SOC research, with binary classification being the most common method.

and research objectives, but the high number of unspecified approaches underscores the need for more standardized reporting practices in this field.

e) Data labeling: Data labeling approaches in SOC research exhibit a diverse range of methodologies, as illustrated in our sunburst diagram (Fig. 10). Our analysis encompasses 38 studies, revealing four primary categories of labeling strategies. Binary Classification emerges as the predominant approach, employed in 17 studies (44.7% of the total). Within this category, 9 studies utilize Malicious/Benign labeling, while 8 studies employ other binary classification schemes such as true/false, positive/negative, or risky/not risky. Multi-class Classification is the second most common approach, observed in 7 studies (18.4%). This category includes one study using MITRE tactic mapping and 6 studies employing various other multi-class labeling schemes, such as attack type classification (e.g., SQL injection, PHP admin attacks, dictionary attacks, XSS attacks) or threat level categorization (e.g., high threat, medium threat, low threat).

Custom Schemes represent a significant portion of the research, accounting for 8 studies (21.1%). This category encompasses specialized approaches tailored to specific SOC contexts, including one study utilizing IRP-API Mapping and 7 studies employing other custom labeling methods. Notably, 6 studies (15.8%) fall under the Not Specified category, indicating that these studies either used unique labeling approaches or did not explicitly detail their labeling methodology. This distribution underscores the complexity and variability in data labeling practices within SOC research. The prevalence of binary classification methods suggests a focus on straightforward, dichotomous categorizations in many SOC applications. However, the significant presence of multi-class and custom schemes highlights the need for more nuanced and context-specific labeling approaches in certain areas of SOC research. The existence of not specified labels points to an opportunity for more transparent and detailed reporting of labeling techniques in future studies, which could enhance reproducibility and comparability across research in this field.

TABLE 5. Detailed Quality Assessment Scores for the 38 Selected Articles, Evaluating Ten Criteria Across Design, Conduct, Analysis, and Conclusion Aspects, With Total Scores Ranging From 0.5 to 10

ID	Design					Conduct	Analysis		Conclusion		Total
	Q01 Aim	Q02 Research Methods	Q03 Settings	Q04 Dataset	Q05 Measures	Q06 Data Collection	Q07 Data Analysis	Q08 Comparison	Q09 Findings	Q10 Limitations	
S01	1	1	1	1	0.5	1	0.5	0	1	1	8
S02	1	1	1	1	1	1	1	0.5	1	0.5	9
S03	1	1	0.5	1	1	1	1	0.5	1	1	9
S04	1	1	0.5	1	1	1	0.5	0	1	0.5	7.5
S05	1	1	0.5	1	1	1	1	0	1	0.5	8
S06	1	1	0.5	1	1	1	1	0	1	0.5	8
S07	1	1	0.5	0.5	0.5	1	1	1	1	0	7.5
S08	1	1	1	1	1	1	1	0	1	0.5	8.5
S09	1	1	0.5	1	1	1	1	0	1	1	8.5
S10	1	1	0.5	1	0.5	1	1	0	1	1	8
S11	1	0.5	0.5	0.5	0	1	0	0	0	0	3.5
S12	0.5	0.5	0	0	0	0.5	0.5	0	0	0	2
S13	1	1	0.5	1	1	1	1	0	1	1	8.5
S14	1	1	1	1	1	1	1	1	1	0	9
S15	1	0.5	0.5	0.5	0.5	0.5	0.5	1	0.5	1	6.5
S16	1	0.5	0.5	0.5	0	0.5	0	0	0	0	3
S17	1	1	1	0.5	1	0.5	1	1	1	1	9
S18	1	1	0.5	1	1	1	1	0	1	1	8.5
S19	1	0.5	0	0.5	0	0	0.5	0	0	1	3.5
S20	1	1	0.5	1	1	0.5	1	0	1	0	7
S21	1	1	0.5	1	1	1	0.5	0.5	1	0.5	8
S22	1	1	0.5	1	1	1	1	0	1	0	7.5
S23	1	1	0.5	1	1	1	1	0	1	0	7.5
S24	1	1	0.5	1	1	1	1	1	1	1	9.5
S25	1	1	0.5	1	1	1	1	0	1	0	7.5
S26	1	1	1	1	1	1	1	1	0	0	8
S27	1	1	0	0	0	0.5	0.5	0	0.5	1	4.5
S28	1	1	0	0	1	0.5	0.5	0	0	1	5
S29	1	1	1	1	1	1	1	1	1	1	10
S30	1	0.5	0.5	0	1	1	1	1	1	0	7
S31	1	1	1	0	1	1	1	1	1	1	9
S32	1	1	0	0	1	0	0.5	1	1	1	6.5
S33	1	1	1	0	1	0	1	1	1	1	8
S34	1	0.5	0	0	1	0	0	0	1	1	4.5
S35	1	0.5	1	0	1	1	0.5	1	1	0	7
S36	0.5	0.5	0	0	0.5	0	0	0	0.5	0	2
S37	1	0.5	0	0	0.5	0	0	0	1	0	3
S38	1	0.5	0	0	0.5	0	0	0	1	0	3
Total	37.5	32.5	19.5	23	29.5	27.5	27	13.5	30.5	20	260.5

C. QUALITY ASSESSMENT RESULTS

The quality assessment of the selected articles, as presented in Table 5, evaluates each article across ten criteria, namely, aim, research methods, settings, dataset, measures, data collection, data analysis, comparison, findings, and limitations. The total score for each article provides a comprehensive insight into its overall quality.

Table 5 shows that the total scores of the articles range from 0.5 to 10, with an average score of approximately 6.7. The data reveals that a significant number of articles (33 out of 38) scored 5 or higher, demonstrating their substantial contribution to the review process and indicating their potential to provide valuable insights into the field of study. These articles generally performed well in areas such as research aim, methods, and data analysis, showcasing a high level of methodological rigor.

Conversely, a smaller subset of articles (6 out of 38) received low-quality scores of 4.5 or less. These articles exhibited deficiencies, particularly in critical aspects such as data collection, analysis, and limitations. These methodological weaknesses diminish the reliability and credibility of their findings, highlighting areas where research practices can be improved.

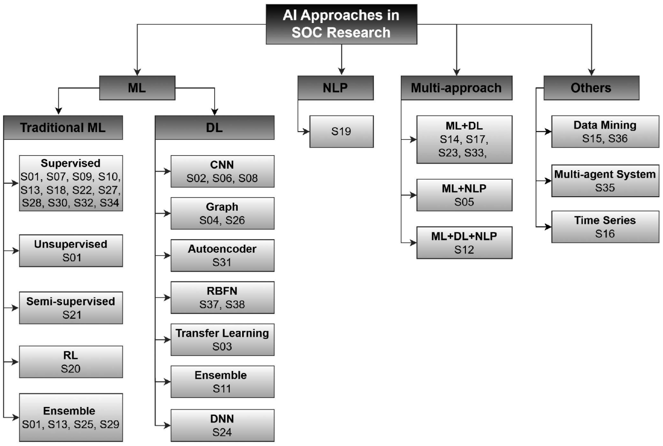

FIGURE 11. Taxonomy of state-of-the-art AI approaches in SOC research, illustrating the four main categories: ML(including traditional ML and DL), NLP, multi-approach, and other methods. The diagram showcases the subcategories within each main category, along with the corresponding studies that employ these techniques. This comprehensive classification reflects the diversity and complexity of AI techniques applied in SOC environments, while providing a clear mapping of research studies to specific AI approaches.

V. DISCUSSION

In this section, we explore the answers to the research questions presented in the introduction.

A. WHAT ARE THE CURRENT STATE-OF-THE-ART AI APPROACHES IN SOC?

In this section, we present two complementary perspectives on the current state-of-the-art AI approaches in SOCs. First, we provide a taxonomy based on the underlying AI technologies and methodologies. Then, we offer a contextual categorization that focuses on the functional applications of these AI techniques within SOC environments. This dual approach allows for a comprehensive understanding of both the technical landscape and the practical implementation of AI in modern SOCs.

1) TECHNOLOGICAL TAXONOMY OF AI APPROACHES IN SOC RESEARCH

As illustrated in Fig. 11, we categorize the current AI approaches in SOC into four main categories, namely, ML, NLP, multi-approach, and other methods.

This categorization provides a more precise classification of the AI techniques used in each study, acknowledging the complexity and diversity of approaches in SOC research. The details of these categories are shown below.

a) ML approaches in SOCs: The ML category includes both traditional ML techniques and DL methods. This combined category highlights the foundational role of ML-based approaches in SOC environments, enabling accurate threat detection, anomaly identification, and robust decision-making.

- Traditional ML: Traditional ML techniques focus on supervised, unsupervised, semi-supervised, reinforcement, and ensemble learning. These methods are used for classification, threat detection, and anomaly analysis.
  1) Supervised learning: Supervised ML is widely used in SOCs for threat detection and classification tasks. This approach relies on labeled data to train models that classify threats, detect anomalies, and prioritize incidents. Studies such as S01, S07, S09, S10, S13, S18, S22, S27, S28, S30, S32, and S34 apply supervised ML techniques to reduce false positives, detect and classify cyber threats, predict vulnerabilities, and prioritize malicious activities.
  2) Unsupervised learning: Unsupervised ML is employed to discover patterns or anomalies without the need for labeled data. This is particularly useful in SOCs for identifying novel or unknown threats. In addition to supervised learning, S01 uses unsupervised learning to detect anomalies and reduce analyst workload by identifying deviations from normal behavior.
  3) Semi-supervised learning: It combines both labeled and unlabeled data. This approach is particularly valuable when labeled data is scarce or expensive to obtain. In S21, semi-supervised learning is used for malware detection by analyzing logs, leveraging both labeled and unlabeled data.
  4) Reinforcement learning: It focuses on dynamic decision-making, where models learn by interacting with the environment to take actions that maximize a cumulative reward. This method is effective in managing and balancing alerts in SOCs. S20 applies Reinforcement Learning (RL) for alert management and load balancing, helping SOCs prioritize critical threats.
  5) Ensemble learning: It combines multiple models to improve prediction accuracy and robustness. It is useful in SOCs where reducing false positives and improving detection rates are critical. We mentioned that the authors of S01 utilized both supervised and unsupervised learning. They also examined Ensemble learning. Furthermore, studies such as S13, S25, and S29 utilize ensemble techniques for classifying true and false alerts, detecting intrusions, and classifying network traffic, enhancing the overall performance of the SOC.
- DL: DL techniques are becoming increasingly important in SOCs. They are effective in handling complex pattern recognition tasks, such as detecting sophisticated attacks or abnormal behaviors.
  1) CNNs: Convolutional Neural Networks (CNN) are widely used in SOCs for recognizing patterns and detecting anomalies in cybersecurity data. CNNs are effective at detecting attacks such as XSS, SQL injection, malware download, and Distributed Denial-of-Service (DDoS). S02, S06, and S08 apply CNNs for anomaly detection, threat detection, and SOC API integration.

2) Graph networks: Sources S04 and S26 apply graph-based DL models in order to prioritize events and analyze the source of potential attacks for faster incident response. Graph networks are used to model relationships between different entities in a network. This makes them valuable for analyzing network behavior and detecting anomalies.
3) Autoencoders: Autoencoders are unsupervised DL models that are used to detect anomalies by reconstructing data and identifying deviations from the norm. In S31, autoencoders are applied for incident classification and cyber situational awareness to help SOC teams understand ongoing threats and incidents more clearly.
4) RBFNs: Radial Basis Function Networks (RBFNs) are used in SOCs for function approximation and classification tasks. S37 and S38 apply RBFNs for intrusion detection and network security. RBFNs help in identify unauthorized access attempts and improve security defenses.
5) Transfer learning: It is leveraged in SOCs to reuse pre-trained models from one domain and adapt them to a different but related task. S03 employs transfer learning for API selection in Incident Response Planning (IRP), speeding up the process of selecting appropriate countermeasures by using pre-trained models.
6) Ensemble DL: These methods combine multiple DL models to improve detection accuracy and reduce false positives. In S11, ensemble DL techniques are used to improve threat identification and alert prioritization.
7) DNNs: Deep Neural Networks (DNN) are multilayered neural networks used in SOCs for complex data processing tasks. S24 uses DNNs to identify potential primary indicators of cyber threats.

b) NLP approaches in SOCs: NLP is used in SOCs to process and analyze large volumes of textual data, such as threat intelligence reports or logs. By extracting insights from text, NLP enables faster identification of threats and improves the analysis of threat intelligence. In S19, NLP is employed for threat prediction by analyzing textual data and extracting insights that help predict potential cyberattacks. Additionally, NLP is often combined with ML and DL in hybrid approaches to improve the processing and analysis of textual data within SOCs.

c) Multi-approach in SOC: Multi-approach in SOC refers to studies where multiple algorithms from different AI categories—such as ML, DL, and NLP—are used independently to perform specific tasks. The goal of these approaches is not to merge or create hybrid models but to compare the performance of each algorithm to determine the most effective one for the task at hand. By evaluating various AI techniques, SOCs can identify the best model for tasks like threat detection, classification, and analysis, enhancing overall cybersecurity operations.

1) ML+DL: These approaches are used in studies such as S14, S17, S23, and S33 to evaluate the effectiveness of ML and DL models and compare their performance to find the most suitable model for tasks like alert ranking, threat detection, and the classification of threat intelligence documents.
2) ML+NLP: These approaches refer to the use of ML and NLP in a study to tackle complex classification tasks. In S05, these methods are applied for multiclass-multilabel classification, particularly for MITRE tactics, with the models compared to enhance the accuracy of classifying security incidents.
3) ML+DL+NLP: These approaches involve applying ML, DL, and NLP techniques to address various tasks, such as threat prediction, classification, and analysis. In S12, ML, DL, and NLP algorithms are tested for threat prediction and classification in SOCs, with their performance compared to identify the best approach.

d) Other approaches in SOCs: This category encompasses specialized AI techniques and methodologies tailored for specific SOC operations that extend beyond traditional ML, DL, and NLP approaches. Within this category, data mining techniques (S15, S36) are employed to extract correlation rules among security events and discover high-level attack strategies, helping reduce alert volumes and uncover previously unknown threats. Multi-agent systems (S35) implement a hierarchical mobile-agent architecture that distributes security tasks across multiple agents, enhancing system robustness and computational efficiency through tasks like alert modification, normalization, and fusion. Time series analysis (S16) is utilized in cognitive threat-hunting tools to correlate security data across extended time periods, employing predictive models to identify anomalies and unusual network behaviors based on historical patterns. These diverse approaches contribute to SOC advancements in areas such as beaconing detection, threat hunting, and sophisticated event correlation analysis.

2) FUNCTIONAL CATEGORIZATION OF AI APPLICATIONS IN SOC ENVIRONMENTS

While the previous section categorized AI approaches based on the underlying technologies and methodologies, this section presents an alternative categorization based on the functional context and purpose of AI applications within SOC environments. This contextual perspective complements the technical categorization by highlighting how different AI techniques are applied to address specific operational challenges in SOCs, such as threat detection, and incident respons. By examining the applications from this functional viewpoint, we can better understand the practical impact and operational relevance of AI in enhancing SOC capabilities. This categorization also helps in identifying common themes and objectives across different technical approaches, providing insights into the current priorities and future directions of AI integration in SOC operations.

a) Threat detection, prediction, and analysis: This category focuses on the identification and characterization of potential security threats. It encompasses studies that develop models to recognize patterns of malicious activity, predict future attacks, and analyze the nature and impact of cyber threats. The emphasis is on the technical aspects of threat identification and understanding.

This category encompasses a wide range of studies (S04, S05, S06, S08, S09, S10, S11, S12, S14, S15, S16, S17, S19, S21, S23, S28, S29, S30, S34) focusing on identifying, predicting, and analyzing various cyber threats. It includes anomaly detection, threat prediction, malware detection, and classification of cyber threats using diverse AI techniques. These approaches are critical for identifying malicious activities or predicting potential threats before they can cause harm. Techniques such as Traditional ML, DL, and NLP are used to effectively detect and predict potential security incidents. For example, DL techniques like CNN and RNN were applied to detect abnormal behavior and identify complex cyber threats such as malware, DDoS, and SQL injections, while ML techniques like decision trees and SVMs are used to classify and predict threats. By detecting these anomalies in real-time or near real-time, these approaches significantly reduce the time to respond to potential security breaches.

b) Alert and event management: This category deals with the operational aspects of handling security alerts and events as they occur in real-time, serving as the first line of defense in SOC operations. It includes studies that address the initial triage, prioritization, filtering, and correlation of alerts as well as the management of security events to reduce analyst workload and improve response efficiency. The focus here is on optimizing the SOC's ability to process and respond to the high volume of security notifications generated by various detection systems.

This category includes studies (S01, S13, S18, S20, S24, S25, S26, S33, S35, S36) that deal with managing and prioritizing alerts and security events. These studies aim to reduce false positives, classify and prioritize alerts, and correlate events to improve SOC efficiency. Managing and prioritizing alerts is essential for reducing false positives and ensuring that SOC analysts can focus on the most critical threats. With the volume of alerts generated daily, AI techniques are employed to filter out false positives, rank alerts by severity, and prioritize critical incidents. Reinforcement learning and ensemble learning are often used to manage alerts and balance loads, while deep learning models assist in prioritizing incidents based on their potential impact. This automation reduces analyst workload, enabling teams to focus on high-priority tasks.

c) Incident response and vulnerability management: This category comprises studies (S02, S03, S07, S31, S32) that focus on improving incident response processes and managing vulnerabilities, addressing security issues after they have been confirmed through initial alert triage. This includes Application Programming Interface (API) selection for incident response planning, detecting and mitigating vulnerabilities, and enhancing cyber situational awareness. In incident response, AI is applied to optimize the handling of security breaches and automate key response tasks. Deep learning techniques, including CNNs and graph networks, are used to prioritize incidents and recommend response actions. Transfer learning models assist in selecting the appropriate APIs for incident response planning, speeding up the response process and improving the effectiveness of countermeasures. For vulnerability management, AI approaches, including supervised and ensemble ML models, are used to identify potential weaknesses and detect unauthorized access attempt

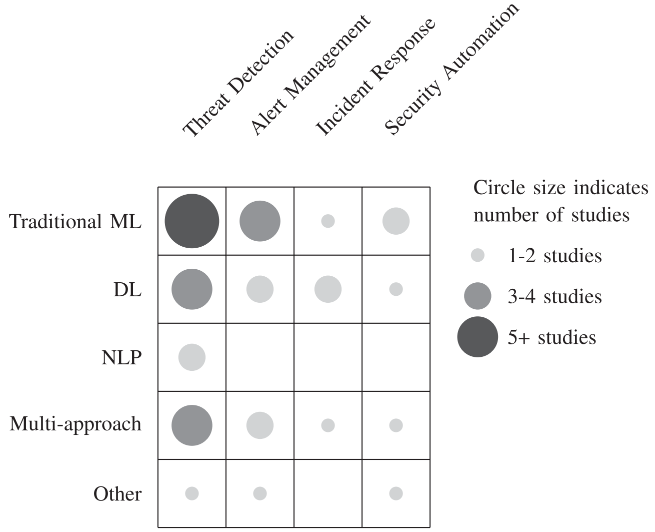

FIGURE 12. Cross-analysis matrix showing how ML approach (with Traditional ML and DL as subcategories) and other approaches (NLP, Multi-approach, Other) relate to functional applications in SOCs. Within ML, both Traditional ML and DL exhibit a strong presence in threat detection, while other approaches show varying degrees of adoption across functions.

d) Security automation and infrastructure: This final category includes studies (S22, S27, S37, S38) that concentrate on automating security processes and enhancing SOC infrastructure. This category covers areas such as privacy-preserving data classification, automation of training content generation, and improvements in intrusion detection systems and network security. Automation plays a pivotal role in SOCs, where AI is used to streamline routine security tasks. By automating these processes, AI reduces manual workload and allows security teams to focus on more critical tasks. Supervised learning techniques are employed to develop eLearning tools and automate vulnerability scanning, enhancing the overall efficiency of SOC operations.

3) CROSS-ANALYSIS OF AI TECHNOLOGIES AND FUNCTIONAL APPLICATIONS IN SOCS

Examining the intersection between the technological taxonomy and functional categorization of AI applications in SOCs reveals several insightful patterns and trends. To visualize this cross-analysis, we present a matrix in Fig. 12, which illustrates the distribution and concentration of AI approaches within each functional category of SOC operations.

As illustrated in Fig. 12, the threat detection category, which implies threat prediction and analysis, employs the most diverse range of AI technologies, including ML, DL, NLP, and multi-approach methods, reflecting the complexity of this task. This is evidenced by the larger, darker circles across multiple rows in the first column of the matrix. Alert and Event Management tasks show a preference for ML and ensemble methods, particularly effective for prioritization and filtering, as indicated by the medium-sized circles in the second column.

The matrix also reveals that Incident Response and Vulnerability Management lean towards DL techniques, especially for API selection and situational awareness, as shown by the concentration of circles in the DL row of the third column. Security Automation and Infrastructure primarily utilize ML methods, as illustrated by the consistent presence of circles in the ML row of the fourth column.

A clear evolution in AI techniques is visible across all functional categories, with earlier studies favoring traditional ML approaches and later ones incorporating more advanced DL and multi-approach methods. This trend is reflected in the distribution of circle sizes across the rows of the matrix.

Some studies demonstrate a holistic approach, applying multiple AI techniques across various SOC functions, while others focus on specific tasks using specialized techniques. NLP and multi-approach categories are predominantly used for threat detection and analysis, underscoring the importance of textual data in understanding and predicting threats.

Studies utilizing real-world data tend to employ more diverse AI techniques and span multiple functional categories, suggesting that real-world SOC challenges often require multi-faceted AI solutions. For large-scale, real-time processing tasks, ensemble and multi-approach are frequently used, indicating their superior scalability and performance in high-volume SOC environments. Emerging trends include the use of graph-based approaches for both threat detection and event prioritization, and the application of transfer learning in incident response.

This cross-analysis also highlights potential areas for future research. There appears to be a gap in the use of explainable AI techniques, which could be particularly valuable in alert management and incident response where human understanding is crucial. Additionally, few studies address the integration of AI techniques with existing SOC workflows and human analysts, presenting another opportunity for future exploration. Overall, this comprehensive view of AI applications in SOCs reveals the adaptive nature of AI techniques in addressing specific cybersecurity challenges and points to exciting directions for future advancements in this field.

This visualization not only summarizes the current state of AI applications in SOCs but also highlights potential gaps and opportunities for future research and development. Areas with smaller circles or empty cells in the matrix might represent under-investigated combinations of AI technologies and SOC functions, suggesting avenues for innovative approaches in enhancing SOC capabilities.

B. WHAT ARE THE KEY CHALLENGES AND OPPORTUNITIES ASSOCIATED WITH IMPLEMENTING THESE APPROACHES IN THE SOC ENVIRONMENT?

1) CHALLENGES

This subsection addresses the key challenges faced when implementing AI technologies in SOCs. These challenges include issues related to data quality, model interpretability, integration with existing systems, and the dynamic nature of cyber threats. We discuss how these obstacles impact the effectiveness of AI-driven SOCs and what strategies can be employed to overcome them.

- Data Quality and Availability: One of the most significant challenges in implementing AI in SOCs is the availability of high-quality data. AI models, particularly those based on ML and DL, require vast amounts of labeled data to train effectively. However, acquiring such data can be difficult due to privacy concerns, the variability of cyber-threats, and the need to label data accurately (S03, S18, S27). The heterogeneity of security data, which may come from various sources and formats, further complicates this issue.
- Model Interpretability: Many AI models, especially deep learning models, are often seen as “black boxes”. This lack of transparency can be problematic in SOC environments, where understanding how a model arrives at a decision is crucial for trust and accountability. SOC analysts need to justify actions based on AI recommendations, and without clear interpretability, this can be challenging (S13, S21, S35).
- Integration with Legacy Systems: Implementing AI within existing SOC infrastructures is not straightforward. SOCs often rely on legacy systems that may not be compatible with modern AI tools. Integrating AI solutions with these systems requires significant effort, including the development of APIs, middleware, or entirely new infrastructure components (S08, S16, S32). The cost and complexity of such integration can be a barrier for many organizations.
- Evolving Cyber Threats: The dynamic nature of cyber threats presents a constant challenge for AI models. These models need to be regularly updated and retrained to stay effective against new and emerging threats. This requires a continuous investment in resources and expertise to maintain the AI systems at peak performance (S06, S14, S23).

2) OPPORTUNITIES

In this subsection, we explore the opportunities presented by AI technologies to enhance the capabilities of SOCs. These opportunities include the automation of routine tasks, improved threat detection, real-time response capabilities, and adaptive learning. We examine how AI can be leveraged to make SOCs more efficient, scalable, and proactive in managing cybersecurity threats.

- Automation of Repetitive Tasks: AI offers significant opportunities to automate many of the routine tasks that burden SOC analysts, such as log analysis, threat hunting, and incident triaging. By automating these tasks, SOCs can free up analysts to focus on more strategic activities, such as threat hunting and incident response, leading to a more efficient and effective security operation (S04, S19, S29).
- Enhanced Threat Detection and Response: AI models are capable of identifying complex and subtle threats that traditional SOC tools might overlook. For example, ML models can detect patterns in data that signify a slow and stealthy attack, while DL models can recognize sophisticated attack signatures across vast datasets. This enhanced detection capability allows SOCs to respond to threats more quickly and accurately (S09, S22, S33).
- Real-Time Analysis and Response: AI-driven SOCs can analyze data and respond to threats in real-time, which is crucial for mitigating fast-moving cyber threats. Real-time analysis enables SOCs to detect and respond to threats as they happen, significantly reducing the window of exposure and potential damage (S10, S25, S30).
- Adaptive Learning and Improvement: AI models, particularly those based on reinforcement learning, can adapt and improve over time. This continuous learning process allows SOCs to stay ahead of evolving threats by refining their detection and response strategies based on real-world feedback (S11, S26, S34).

C. WHAT ARE THE SPECIFIC BENEFITS AND ADVANTAGES OF APPLYING AI MODELS IN SOC ENVIRONMENTS COMPARED TO TRADITIONAL SOC APPROACHES?

Some of the benefits and advantages of applying AI models in SOC environments compared to traditional SOC approaches are summarised as:

- Improved Accuracy and Speed: AI models, particularly those leveraging ML and DL capabilities, demonstrate superior processing capabilities for large-scale data analysis compared to traditional human-driven approaches. Study S14 achieved a remarkable 99.524% recall rate in identifying true security alerts, while S02's APIRO framework demonstrated 91.9% accuracy in recommending appropriate security tool APIs from natural language queries. These quantifiable improvements in accuracy directly translate to enhanced threat detection and incident response capabilities, significantly reducing the manual investigation burden on analysts.
- Reduction in False Positives: Traditional SOCs often struggle with high volumes of false positive alerts, which can lead to alert fatigue and potentially overlooked threats. AI-driven solutions have shown remarkable effectiveness in addressing this challenge through advanced pattern recognition and anomaly detection. Study S10's DomainPrio system achieved 89% balanced accuracy in identifying priority domains, while S14's approach required analyst review of only 0.433% of potential false alerts. This substantial reduction in false positives enables analysts to focus their expertise on investigating genuine security threats.
- Scalability and Flexibility: AI-driven SOCs demonstrate superior adaptability to increasing data volumes and security environment complexity compared to traditional approaches. Study S21 provides concrete evidence of this scalability through its successful implementation of reinforcement learning to manage workload distribution across nine distributed SOCs. This capability proves particularly valuable for large enterprises and global organizations that must process and analyze vast amounts of security data across multiple locations.
- Predictive Capabilities: AI models enable SOCs to shift from reactive to proactive security measures through advanced predictive analytics. Study S10 quantified this benefit by demonstrating the prevention of 341 unnecessary investigations over a 100-day period through accurate domain prioritization. Furthermore, study S14's system identified 24.3% more primary threat indicators that were previously undiscovered, while maintaining a low false positive rate of 5%. These results highlight AI's ability to forecast and prevent potential security threats before they materialize.
- Cost Efficiency: While precise cost savings data is limited in current research, several studies demonstrate efficiency gains that translate to cost benefits. Study S10 documented a 35% reduction in unnecessary domain investigations, indicating significant savings in analyst time and resources. Additionally, S14's 99.524% recall rate in critical alert detection substantially reduces manual auditing requirements. Study S30's implementation of ensemble methods for network traffic analysis showed improved accuracy and stability across datasets, suggesting reduced costs associated with incident response and error rectification. These efficiency improvements, combined with automated routine task handling, enable organizations to optimize their security operations while maintaining high effectiveness levels.

In summary, the integration of AI in SOCs marks a significant advancement in cybersecurity. These AI approaches enhance the capabilities of SOCs by improving accuracy, reducing response times, and offering predictive insights that were not possible with traditional methods. Despite the challenges of data quality, model interpretability, and integration with existing systems, the opportunities for automation, real-time response, and adaptive learning make AI a vital component of modern security operations. The specific benefits of AI models, including improved accuracy, reduced false positives, scalability, predictive capabilities, and cost efficiency, underscore their superiority over traditional SOC approaches, paving the way for more resilient and responsive security infrastructures.

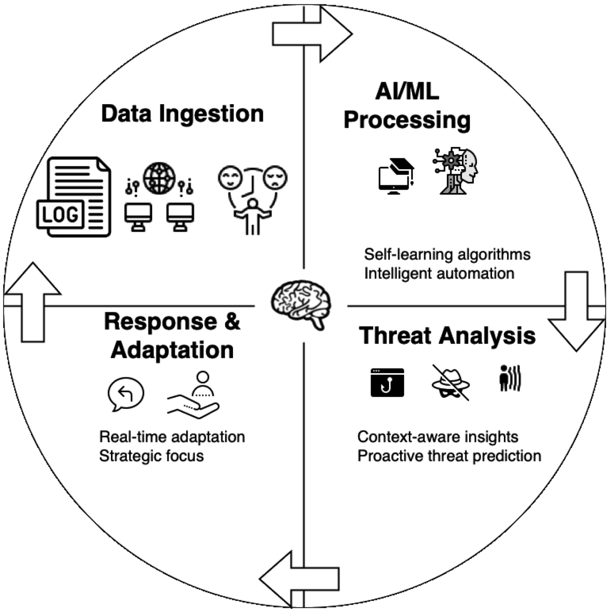

FIGURE 13. Circular diagram depicting the key components and processes of a Cognitive SOC, illustrating the continuous cycle of data ingestion, AI/ML processing, threat analysis, and response & adaptation.

D. INCORPORATING COGNITIVE CAPABILITIES IN SOCS: A COMPREHENSIVE DEFINITION

In recent years, the concept of a SOC evolved significantly with the advent of AI and ML technologies. Traditional SOCs, which primarily rely on human analysts and predefined rule sets, are now being enhanced with advanced cognitive capabilities. These capabilities enable more sophisticated, proactive, and efficient cybersecurity operations. This section provides a comprehensive definition of a SOC with cognitive capabilities by synthesizing insights from 38 research papers. We explore the core components, cognitive capabilities, integration and automation, human-machine collaboration, and holistic security management that define a cognitive SOC.

Fig. 13 illustrates the key components and processes of a cognitive SOC. The cyclic nature of the diagram emphasizes the continuous and interconnected operations of a cognitive SOC, focusing on four main areas: Data Ingestion, AI/ML Processing, Threat Analysis, and Response & Adaptation. This visual representation aligns with our comprehensive definition, which we explore in detail in the following subsections.

1) CORE COMPONENTS OF SOCS WITH COGNITIVE CAPABILITIES

The core components of a cognitive SOC lay the foundation for its advanced capabilities.

a) Data ingestion: The process begins with data ingestion, depicted in the upper-left quadrant of Fig. 13. This involves collecting and processing various types of data, such as logs, network traffic, and user behavior information. Effective data ingestion is crucial, as it feeds the subsequent AI/ML processing stages with the necessary inputs to analyze and detect potential threats.

b) AI/ML processing: The upper-right quadrant of Fig. 13 highlights AI/ML processing, which is central to a cognitive SOC. This component utilizes self-learning algorithms and intelligent automation to analyze the ingested data. AI and ML are extensively recognized across multiple studies as the backbone of cognitive SOCs, enabling automated threat detection, pattern recognition, and anomaly detection—critical functions for modern SOC operations (S01, S02, S03, S04, S05). Additionally, cognitive computing distinguishes cognitive SOCs from traditional ones, allowing these systems to adapt and respond more effectively to emerging threats (S06, S07, S08, S09, S10).

2) COGNITIVE CAPABILITIES IN SOCS

a) Threat analysis: The lower-right quadrant of Fig. 13 represents the threat analysis capabilities of a cognitive SOC. This includes context-aware insights and proactive threat prediction, which are vital for staying ahead of evolving cyber threats. Continuous learning and adaptation are critical functions of cognitive SOCs, as they enable these systems to keep pace with the rapidly changing threat landscape (S11, S12, S13, S14). The literature also highlights proactive threat detection as a key strength of cognitive SOCs, allowing them to anticipate and mitigate threats before they materialize (S15, S16, S17, S18, S19).

3) INTEGRATION AND AUTOMATION

The integration of AI/ML processing with threat analysis, as depicted in Fig. 13, facilitates advanced automation capabilities within cognitive SOCs. This integration allows the SOC to automate routine tasks and enhance operational efficiency. Automation is a significant benefit of cognitive SOCs, as it increases efficiency and reduces the potential for human error, a point well-documented in numerous studies (S20, S21, S22, S23, S24). Furthermore, real-time analysis is critical for modern SOCs, especially in scenarios that require swift action. The literature supports the role of cognitive SOCs in effectively delivering this capability (S25, S26, S27, S28, S29).

4) HUMAN-MACHINE COLLABORATION AND RESPONSE

The lower-left quadrant of Fig. 13 illustrates the response and adaptation capabilities of a cognitive SOC, which involve close human-machine collaboration. This collaboration enhances decision-making and allows security teams to focus on strategic tasks while AI handles routine operations. The synergy between AI-driven analysis and human expertise is consistently highlighted in the literature, where cognitive SOCs assist analysts in making quicker and more accurate decisions (S30, S31, S32, S33, S34).

5) HOLISTIC SECURITY MANAGEMENT

The circular flow in Fig. 13 represents the holistic and continuous nature of security management in a cognitive SOC. This holistic approach emphasizes the importance of context-aware insights and real-time adaptation in maintaining an effective security posture. The ability of cognitive SOCs to provide such context-aware insights is a key factor in their effectiveness, as documented in several studies (S35, S36, S37, S38).

6) CONSOLIDATED DEFINITION

A SOC with cognitive capabilities is an advanced cybersecurity infrastructure that utilizes AI, ML, and cognitive computing to enhance its ability to detect, analyze, and respond to cyber threats. These cognitive capabilities refer to the system's ability to mimic human-like processes such as learning, reasoning, and decision-making. This type of SOC leverages self-learning algorithms and intelligent automation to process vast amounts of data, predict potential threats, and adapt to evolving security challenges in real-time. Automating routine tasks and providing proactive, context-aware insights, allows security teams to focus on more strategic activities, resulting in a more efficient and effective defense against complex cyber threats.

This definition, supported by the visual representation in Fig. 13, emphasizes the integration of AI, ML, and cognitive computing to enhance threat detection, analysis, and response in a continuous, adaptive cycle. Cognitive SOCs represent a significant advancement over traditional SOC approaches, offering improved efficiency, proactive threat management, and enhanced decision-making capabilities in the face of evolving cybersecurity challenges.

E. REVIEW LIMITATION

1) POTENTIAL FOR MISSING STUDIES

Despite our comprehensive efforts, we can not guarantee that all relevant primary studies were captured in this review. This limitation arises due to the challenges inherent in search methodologies and the selective nature of the databases and sources utilized. To mitigate this, we conducted pilot searches on widely used databases and publishing platforms (e.g., WoS, Scopus, IEEE Xplore, etc.) to refine our search strings iteratively to enhance the capture of relevant studies.

2) STUDY SELECTION BIAS

The processes of study selection and data extraction are susceptible to biases, which could potentially influence the review's outcomes. To counteract this, we developed a detailed study protocol outlining the research questions, inclusion and exclusion criteria, and data extraction procedures. This protocol was reviewed and agreed upon by all authors and applied consistently throughout the review process. Three authors independently conducted the data extraction, with their results stored in shared folders for cross-checking by the rest of the team. Regular discussions were held to ensure accuracy and consistency in the selection and extraction processes. Despite these precautions, some level of bias due to subjective judgment or human error may persist.

VI. CONCLUSION AND FUTURE WORKS

This systematic literature review provides a comprehensive analysis of AI applications in SOCs, examining 38 studies. Our findings reveal the dominance of Traditional Machine Learning and Deep Learning techniques in SOC research, with a growing trend towards hybrid approaches. The integration of AI in SOCs has significantly improved threat detection accuracy, reduced false positives, and enhanced operational scalability. However, challenges persist in data quality, model interpretability, and integration with legacy systems. The emergence of cognitive SOCs, leveraging advanced AI to mimic human-like processes, represents a significant advancement over traditional approaches, offering improved efficiency, proactive threat management, and enhanced decision-making capabilities.

To realize the full potential of AI in SOCs, future research should focus on several key areas. These include developing explainable AI models to improve interpretability, investigating optimal human-AI collaboration strategies, and researching adaptive AI techniques for continuous learning against evolving threats. Additionally, exploring privacy-preserving AI methods for multi-organizational and cloud-based security environments, establishing standardized benchmarks for evaluating AI performance in SOCs, and advancing AI-driven proactive threat hunting and automated incident response capabilities are crucial. Addressing scalability challenges in large-scale, distributed SOC environments and conducting longitudinal studies on the long-term impact of AI integration on SOC performance and organizational cybersecurity posture will also be vital. By pursuing these research directions, the field can advance towards more robust, efficient, and effective AI-driven SOC operations. As the cybersecurity landscape continues to evolve, the integration of AI in SOCs will play a crucial role in defending against increasingly sophisticated cyber threats, necessitating ongoing research and development to fully realize its benefits and address existing challenges.

ACKNOWLEDGMENT

This work was done while Mosab Hamdan was working in ISS-KFUPM.

REFERENCES

[1] M. Vielberth, F. Böhm, I. Fichtinger, and G. Pernul, "Security operations center: A systematic study and open challenges," *IEEE Access*, vol. 8, pp. 227756–227779, 2020.

[2] E. Agyepong, Y. Cherdantseva, P. Reinecke, and P. Burnap, "A systematic method for measuring the performance of a cyber security operations centre analyst," *Comput. Secur.*, vol. 124, 2023, Art. no. 102959.

[3] P. Tseng, Z. Yeh, X. Dai, and P. Liu, "Using LLMs to automate threat intelligence analysis workflows in security operation centers," 2024, *arXiv:2407.13093*.

[4] Federal Bureau of Investigation (FBI), "Internet crime report (IC3) 2020," Internet Crime Complaint Center (IC3), Tech. Rep., 2020, Accessed: Jul. 29, 2024. [Online]. Available: https://www.ic3.gov/

[5] Verizon Business, "Data breach investigations report 2023," Verizon, Tech. Rep. 2023, Accessed: Jul. 29, 2024. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/

[6] M. Vielberth, "Security information and event management (SIEM)," in *Encyclopedia of Cryptography Security and Privacy*. Berlin, Germany: Springer, 2021, pp. 1–3.

[7] D. Schlette, M. Caselli, and G. Pernul, "A comparative study on cyber threat intelligence: The security incident response perspective," *IEEE Commun. Surveys Tut.*, vol. 23, no. 4, pp. 2525–2556, 4th Quarter 2021.

[8] MITRE Corporation, "MITRE ATT&CK framework.," 2025, Accessed: Jul. 29, 2024. [Online]. Available: https://attack.mitre.org/

[9] ReportLinker, "Threat intelligence global market report," Tech. Rep., 2025, Accessed: Jul. 29, 2024.

[10] M. A. Islam, "Application of artificial intelligence and machine learning in security operations center," Ph.D. dissertation, Middle Georgia State Univ., Macon, GA, USA, 2023.

[11] F. B. Kokulu et al., "Matched and mismatched SOCs: A qualitative study on security operations center issues," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2019, pp. 1955–1970.

[12] S. Oesch et al., "An assessment of the usability of machine learning-based tools for the security operations center," pp. 634–641, 2020.

[13] Y. Duna, M. Ab Razak, M. Zolkipli, T. Bee, and A. Firdaus, "Grasp on next generation security operation centre: Comparative study," *Int. J. Nonlinear Anal. Appl.*, vol. 12, no. 2, pp. 869–895, 2021.

[14] D. Shahjee and N. Ware, "Integrated network and security operation center: A systematic analysis," *IEEE Access*, vol. 10, pp. 27881–27895, 2022.

[15] J. R. Schmitt, M. Mink, and M. Meier, "Security operations centers: A holistic view on problems and solutions," in *Proc. 55th Hawaii Int. Conf. Syst. Sci.*, 2022, pp. 7555–7564.

[16] H. J. Ofte and S. Katsikas, "Understanding situation awareness in SOCs, a systematic literature review," *Comput. Secur.*, vol. 126, 2023, Art. no. 103069.

[17] M. J. Page et al., "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *BMJ*, vol. 372, 2021, Art. no. n71.

[18] R. Vaarandi, R. Vaarandi, and A. Guerra, "Stream clustering guided supervised learning for classifying NIDS alerts," *Future Gener. Comput. Syst.*, vol. 155, pp. 231–244, 2024.

[19] Z. T. Sworna, I. Chadni, and M. A. Babar, "APIRO: A framework for automated security tools API recommendation," *ACM Trans. Softw. Eng. Methodol.*, vol. 32, 2023, Art. no. 24.

[20] Z. T. Sworna, M. A. Babar, and A. Sreekumar, "IRP2API: Automated mapping of cyber security incident response plan to security tools' APIs," in *Proc. IEEE Int. Conf. Softw. Anal., Evol. Reengineering*, 2023, pp. 546–557.

[21] A. Presekal, A. Ştefanov, V. S. Rajkumar, and P. Palensky, "Cyber forensic analysis for operational technology using graph-based deep learning," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids*, 2023, pp. 1–7.

[22] M. Marmureanu and C. Opris, "MITRE tactics inference from Splunk queries," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids*, 2023, pp. 277–283.

[23] W. Jang, H. Kim, H. Seo, M. Kim, and M. Yoon, "SELID: Selective event labeling for intrusion detection datasets," *Sensors*, vol. 23, no. 13, 2023, Art. no. 6105.

[24] S. Hore, F. Moomtaheen, F. Moomtaheen, and X. Ou, "Towards optimal triage and mitigation of context-sensitive cyber vulnerabilities," *IEEE Trans. Dependable Secure Comput.*, vol. 20, no. 2, pp. 1270–1285, Mar./Apr. 2023.

[25] J.-y. Kim and H.-Y. Kwon, "Threat classification model for security information event management focusing on model efficiency," *Comput. Secur.*, vol. 120, 2022, Art. no. 102789.

[26] C. Islam, M. A. Babar, R. Croft, and H. Janicke, "SmartValidator: A framework for automatic identification and classification of cyber threat data," *J. Netw. Comput. Appl.*, vol. 202, 2022, Art. no. 103370.

[27] D. Chiba et al., "Domainprio: Prioritizing domain name investigations to improve SOC efficiency," *IEEE Access*, vol. 10, pp. 34352–34368, 2022.

[28] J. Wang et al., "A comprehensive security operation center based on Big Data analytics and threat intelligence," in *Proc. Int. Symp. Grids Clouds*, 2021, pp. 22–26.

[29] A. Perera, S. Rathnayaka, N. D. Perera, W. W. Madushanka, and A. N. Senarathne, "The next gen security operation center," in *Proc. Int. Conf. Convergence Technol.*, 2021, pp. 1–9.

[30] S. Ndichu, T. Ban, T. Takahashi, and D. Inoue, "A machine learning approach to detection of critical alerts from imbalanced multi-appliance threat alert logs," in *Proc. IEEE Int. Conf. Big Data*, 2021, pp. 2119–2127.

[31] T. Ongun et al., "PORTFILER: Port-level network profiling for self-propagating malware detection," in *Proc. IEEE Conf. Commun. Netw. Secur.*, 2021, pp. 182–190.

[32] P. Najafi, F. Cheng, and C. Meinel, "SIEMA: Bringing advanced analytics to legacy security information and event management," in *Proc. Secur. Privacy Commun. Netw.*, 2021, pp. 25–43.

[33] M. S. Khan et al., "Cyber threat hunting: A cognitive endpoint behavior analytic system," *Int. J. Cogn. Inform. Natural Intell.*, vol. 15, no. 4, 2021, Art. no. 23.

[34] I. Choi, J. Lee, T. Kwon, K. Kim, Y. Choi, and J. Song, "An easy-to-use framework to build and operate AI-based intrusion detection for in-situ monitoring," in *Proc. Asia Joint Conf. Inf. Secur.*, 2021, pp. 1–8.

[35] T. Ban, N. Samuel, T. Takahashi, and D. Inoue, "Combat security alert fatigue with AI-assisted techniques," in *Proc. 14th Cyber Secur. Experimentation Test Workshop Virtual*, 2021, pp. 9–16.

[36] N. AfzaliSeresht, Y. Miao, Q. Liu, A. Teshome, and W. Ye, "Investigating cyber alerts with graph-based analytics and narrative visualization," in *Proc. IEEE 24th Int. Conf. Inf. Visualisation*, 2020, pp. 521–529.

[37] A. Shah, R. Ganesan, S. Jajodia, P. Samarati, and H. Cam, "Adaptive alert management for balancing optimal performance among distributed CSOCs using reinforcement learning," *IEEE Trans. Parallel Distrib. Syst.*, vol. 31, no. 1, pp. 16–33, Jan. 2020.

[38] T. Nishiyama, A. Kumagai, K. Kamiya, and K. Takahashi, "SILU: Strategy involving large-scale unlabeled logs for improving malware detector," in *Proc. IEEE Symp. Comput. Commun.*, 2020, pp. 1–7.

[39] L. Karaçay, E. Savas, and H. Alptekin, "Intrusion detection over encrypted network data," *Comput. J.*, vol. 63, no. 4, pp. 604–619, Apr. 2020.

[40] W. Yang and K.-Y. Lam, "Automated cyber threat intelligence reports classification for early warning of cyber attacks in next generation SOC," in *Proc. 21st Int. Conf. Inf. Commun. Secur.*, 2020, pp. 145–164.

[41] T. Shibahara, H. Kodera, D. Chiba, M. Akiyama, K. Hato, and O. Söderström, "Cross-vendor knowledge transfer for managed security services with triplet network," in *Proc. 12th ACM Workshop Artif. Intell. Secur.*, 2019, pp. 59–69.

[42] A. F. Huang, Y. Chi-Wei, H.-C. Tai, Y. Chuan, J. J. Huang, and Y.-H. Liao, "Suspicious network event recognition using modified stacking ensemble machine learning," in *Proc. IEEE Int. Conf. Big Data*, 2019, pp. 5873–5880.

[43] N. Gupta, I. Traore, and P. M. F. De Quinan, "Automated event prioritization for security operation center using deep learning," in *Proc. IEEE Int. Conf. Big Data*, 2019, pp. 5864–5872.

[44] M. Cazacu, C. Bodea, M. I. Dascălu, and C. Cucu, "Using the activity theory to identify the challenges of designing elearning tools based on machine learning for security operations centers," in *Proc. eLearn. Softw. Educ. Conf.*, 2019, pp. 452–461.

[45] P. Bienias, G. Kołaczek, and A. Warzyński, "Architecture of anomaly detection module for the security operations center," in *Proc. IEEE 28th Int. Conf. Enabling Technol.: Infrastructure Collaborative Enterprises*, 2019, pp. 126–131.

[46] K. Demertzis, P. Kikiras, N. Tziritas, S. L. Sanchez, and L. Iliadis, "The next generation cognitive security operations center: Network flow forensics using cybersecurity intelligence," *Big Data Cogn. Comput.*, vol. 2, no. 4, 2018, Art. no. 35.

[47] A. Oprea, Z. Li, R. Norris, and K. Bowers, "MADE: Security analytics for enterprise threat detection," in *Proc. 34th Annu. Comput. Secur. Appl. Conf.*, 2018, pp. 124–136.

[48] R. Graf and R. King, "Neural network and blockchain based technique for cyber threat intelligence and situational awareness," in *Proc. IEEE 10th Int. Conf. Cyber Conflict*, 2018, pp. 409–426.

[49] K. Funaya, S. Bajaj, K. Sharad, and A. Srivastava, "Optimizing the sequence of vulnerability scanning injections," in *Proc. IEEE Conf. Dependable Secure Comput.*, 2018, pp. 1–2.

[50] C. Feng, S. Wu, and N. Liu, "A user-centric machine learning framework for cyber security operations center," in *Proc. IEEE Int. Conf. Intell. Secur. Inform.*, 2017, pp. 173–175.

[51] A. Erola, I. Agrafiotis, J. Happa, M. Goldsmith, S. Creese, and P. A. Legg, "Richerpicture: Semi-automated cyber defence using context-aware data analytics," in *Proc. Int. Conf. Cyber Situational Awareness, Data Anal. Assessment*, 2017, pp. 1–8.

[52] J.-S. Li, C.-J. Hsieh, and H.-Y. Lin, "A hierarchical mobile-agent-based security operation center," *Int. J. Commun. Syst.*, vol. 26, no. 12, pp. 1503–1519, 2013.

[53] D. Zhang and D. Zhang, "The analysis of event correlation in security operations center," in *Proc. IEEE 4th Int. Conf. Intell. Comput. Technol. Autom.*, 2011, pp. 1214–1216.

[54] Y. Niu and Y. C. Peng, "Application of radial function neural network in network security," in *Proc. Int. Conf. Comput. Intell. Secur.*, 2008, pp. 458–463.

[55] N. Yi, Z. Qi-Lun, and P. Hong, "Network security management based on data fusion technology," in *Proc. IEEE 7th Int. Conf. Comput.-Aided Ind. Des. Conceptual Des.*, 2006, pp. 889–892.

FARID BINBESHR received the bachelor's degree in computer science from Hadhramout University, Al Mukalla, Yemen, in 2009, the master's degree in computer networks from the King Fahd University of Petroleum and Minerals (KFUPM), Dhahran, Saudi Arabia, in 2014, and the Ph.D. degree in computer security from the University of Malaya, Kuala Lumpur, Malaysia, in 2023. He is currently a Postdoctoral Research Fellow with the Intelligent Secure Systems Center, KFUPM. His research focuses on enhancing computer networks and security, with a particular interest in applying artificial intelligence techniques to develop innovative solutions. Certified in ethical hacking and security analysis, he possesses extensive hands-on experience in cybersecurity, encompassing secure system architecture, network defense, penetration testing, and risk assessment. He has also taught various cybersecurity and network-related courses, bridging the gap between theoretical knowledge and practical implementation in the field.

MUHAMMAD IMAM received the B.Sc. and M.Sc. degrees in computer engineering from the King Fahd University of Petroleum & Minerals, Dhahran, Saudi Arabia, and the Ph.D. degree in electrical and computer engineering from Carleton University, Ottawa, ON, Canada, in 2013. Since then, he has been an Assistant Professor with the Computer Engineering Department, King Fahd University of Petroleum & Minerals. He was appointed as the Director of the Business Incubator program at the Entrepreneurship Institute for three years (2017–2020). His research interests include system logic design, cybersecurity, blockchain, deep learning and computer networks.

MUSTAFA GHALEB received the M.Sc. and Ph.D. degrees in computer science from the King Fahd University of Petroleum and Minerals (KFUPM), Dhahran, Saudi Arabia. He is currently a Postdoctoral Research Fellow with the Interdisciplinary Research Center for Intelligent Secure Systems (IRC-ISS), KFUPM. His research interests include cybersecurity, Internet of Things (IoT), distributed computing, NLP, trust modeling, and deep learning applications in various domains.

MOSAB HAMDAN (Senior Member, IEEE) received the B.Sc. degree in computer and electronic systems engineering from the University of Science and Technology (UST), Omdurman, Sudan, in 2010, the M.Sc. degree in computer architecture and networking from the University of Khartoum, Khartoum, Sudan, in 2014, and the Ph.D. degree in electrical engineering (computer networks) from Universiti Teknologi Malaysia (UTM), Johor Bahru, Malaysia, in 2021. From 2010 to 2015, he was a Teaching Assistant and Lecturer with the Department of Computer and Electronic Systems Engineering, UST. He was a Research Fellow with several esteemed institutions, including UTM, Universiti Malaysia Sabah, Kota Kinabalu, Malaysia, University of São Paulo, São Paulo, Brazil, King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia, and South East Technological University. He is currently an Assistant Professor with the School of Computing, National College of Ireland, Dublin, Ireland. His main research interests include computer networks, network security, software-defined networking, the Internet of Things, smart cities, intelligent transportation systems, and future networks.

MUSSADIQ ABDUL RAHIM received the B.S. (Hons.) degree from CIIT, in 2013, the M.S. degree in computer science from PIEAS, in 2015, and the Ph.D. degree in computer science and technology from BIT, in 2020. He brings prior teaching experience to his current research focus with the King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia. He explores human–machine interaction through applied AI and deep learning for realworld challenges, such as human behavior, power resilience, and a variety of emerging research problems.

MOHAMMAD HAMMOUDEH (Senior Member, IEEE) is currently Saudi Aramco's Cybersecurity Chair Professor with the King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia. His research interests include the applications of zero trust security to internet-connected critical national infrastructures, blockchains, and other complex highly decentralised systems.