# Exploring the Role of Artificial Intelligence in Enhancing Security Operations: A Systematic Review

DESPOINA GIARIMPAMPA, SnT, University of Luxembourg, Luxembourg, Luxembourg
ROLAND MEIER, Cyber-Defense Campus, armasuisse, Bern, Switzerland
TEGAWENDÉ F. BISSYANDÉ, SnT, University of Luxembourg, Luxembourg, Luxembourg
VINCENT LENDERS, Cyber-Defense Campus, armasuisse, Bern, Switzerland
JACQUES KLEIN, SnT, University of Luxembourg, Luxembourg, Luxembourg

Artificial intelligence (AI) is reshaping Security Operations Centers (SOCs). This systematic literature review analyses AI's transformative impact across the NIST Cybersecurity Framework. The analysis of 189 papers related to AI use-cases for SOCs shows widespread application of AI for detection, with 65% of studies focusing on it. Yet, it also reveals deficiencies in recovery, the underutilisation of explainable AI models—with 88% of studies relying on non-explainable approaches— the sporadic release of tools as open-source and an over-reliance on proprietary datasets. Common motivations for papers include efficiency, error reduction, and cost savings, with challenges in data reliance, and integration complexity.

CCS Concepts: • **Security and privacy** → **Network security**; • **Networks** → *Network monitoring*; • **General and reference** → **Surveys and overviews**; • **Computing methodologies** → **Artificial intelligence**; • **Applied computing** → Operations research; Network forensics;

Additional Key Words and Phrases: Machine learning algorithms, cybersecurity, SOC automation, AI in cyber defense, security operations center (SOC)

**ACM Reference Format:**
Despoina Giarimpampa, Roland Meier, Tegawendé F. Bissyandé, Vincent Lenders, and Jacques Klein. 2025. Exploring the Role of Artificial Intelligence in Enhancing Security Operations: A Systematic Review. *ACM Comput. Surv.* 58, 3, Article 67 (September 2025), 38 pages. https://doi.org/10.1145/3747587

## 1 Introduction

The exponential growth of complexity and frequency of cyber threats has thrust cybersecurity to the forefront of organisational priorities. A recent study by JupiterOne [93] highlights a staggering 133% increase in the total number of cyber assets involved in business processes in 2023 alone. This surge underscores the expanding attack surface that **Security Operations Centres** (**SOCs**) must monitor and protect. The strain on SOC teams is evident, with 78% of staff working beyond regular hours to manage the mounting workload [45]. In this context, the game-changing integration of

Authors' Contact Information: Despoina Giarimpampa (corressponding author), SnT, University of Luxembourg, Luxembourg, Luxembourg; e-mail: giar.des@gmail.com; Roland Meier, Cyber-Defense Campus, armasuisse, Bern, Switzerland; e-mail: roland.meier@armasuisse.ch; Tegawendé F. Bissyandé, SnT, University of Luxembourg, Luxembourg, Luxembourg; e-mail: tegawende.bissyande@uni.lu; Vincent Lenders, Cyber-Defense Campus, armasuisse, Bern, Switzerland; e-mail: Vincent.Lenders@armasuisse.ch; Jacques Klein, SnT, University of Luxembourg, Luxembourg, Luxembourg; e-mail: jacques.klein@uni.lu.


ACM 0360-0300/2025/09-ART67
https://doi.org/10.1145/3747587

**Artificial Intelligence** (**AI**) into SOC practices has garnered substantial attention, promising to revolutionise the effectiveness and efficiency of cybersecurity operations, offering a significant improvement over traditional rule-based tools.

As the demand for AI-driven solutions in SOC surges, there remains a critical gap in the current literature. Existing reviews have explored aspects of AI taxonomy [96], integration [40], and have offered valuable insights into specific challenges such as real-time threat detection [181], intrusion detection [147, 225], automation [48], and situation awareness [152, 203] in SOC environments. However, they fail to provide a holistic view that encompasses all interconnected aspects of these challenges. These studies highlight limitations such as the lack of comprehensive frameworks [7], formalised explainability [147], available datasets [225], and the difficulty of effectively integrating AI across all SOC functions [188]. Furthermore, research often focuses on isolated use cases [9, 15, 17, 171] without considering the broader context of SOC operations and the operational complexities involved.

The need for a new **systematic literature review** (**SLR**) arises from these significant gaps in the existing body of work. This review does not only map the current state-of-the-art applications of AI in SOCs but it also critically assesses the limitations, challenges, and research gaps identified in previous studies. By examining prevailing trends, adoption patterns, and underexplored areas, this review provides a comprehensive overview that serves as a foundation for future research and development in the field. The goal is to deliver a more extensive and integrative assessment of AI-driven SOC solutions, one that addresses the complexities of modern cybersecurity demands while paving the way for more effective, scalable, and explainable AI applications in SOC operations.

### 1.1 Scope and Definition of Security Operations Centres (SOCs)

SOCs are critical components within organisational security frameworks, designated to proactively monitor, detect, respond to, and mitigate cybersecurity threats. The concept of a SOC encompasses a range of operational models, each designed to address the specific security needs of an organisation.

*1.1.1 Definition of a SOC.* Although there is no universal definition, several authoritative sources provide similar perspectives on what constitutes a SOC. According to the International Council of E-Commerce Consultants (EC Council) a SOC is described as "a team of cybersecurity personnel dedicated to monitoring and analysing an organisation's security while responding to potential or current breaches" [30]. CompTIA defines a SOC as "a team of experts that proactively monitor an organisation's ability to operate securely" [5]. Splunk characterises a SOC as a "centralised location where security professionals build and maintain the security architecture that monitors, detects, analyses and responds to cybersecurity incidents and threats, typically around the clock" [1]. These definitions collectively highlight the dual role of the SOC in both proactive surveillance and reactive incident management, underscoring the versatile nature of SOCs in adapting to diverse cybersecurity landscapes.

*1.1.2 Operational Scope of SOCs.* The operational scope of a SOC is delineated by its core functions, which are illustrated in Figure 1. This flowchart breaks down the SOC's activities into several key areas:

(1) **Identification and Monitoring:** Continuous monitoring of network and system activities to identify potential security events. This includes asset management and vulnerability assessments to establish a robust cybersecurity posture.
(2) **Threat Detection:** Utilisation of advanced analytical tools and methodologies to detect anomalies that could indicate cybersecurity incidents. This function leverages data integration from multiple sources, including threat intelligence feeds, to enhance detection capabilities.

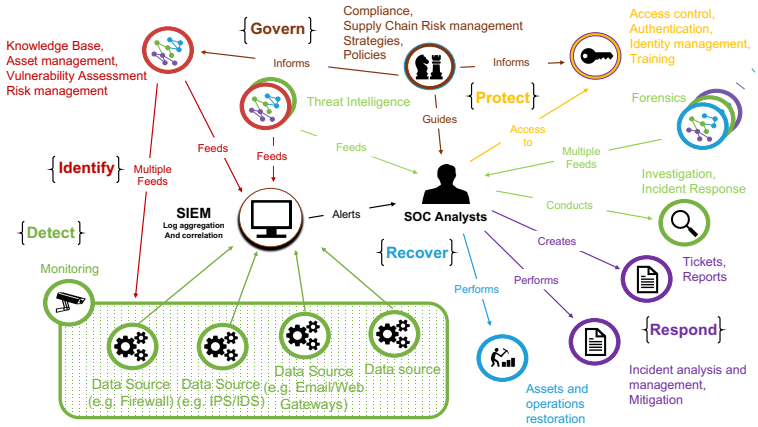



Fig. 1. Flowchart of SOC functionalities and processes.

(3) **Incident Response:** Once a threat is detected, the SOC personnel are responsible for coordinating and executing response strategies to mitigate risks. This includes incident analysis, containment efforts, and, crucially, communication with relevant stakeholders to effectively manage the incident lifecycle.
(4) **Recovery and Post-Incident Analysis:** Activities focused on restoring systems to operational status and analysing the incident to prevent future occurrences. Recovery also involves learning lessons and adapting strategies based on new insights gained from the breach.

The functions and responsibilities that define the role of a SOC within an organisation, as described above, are based on the NIST **Cybersecurity Framework** (**CSF**) 2.0 [4].

### 1.2 NIST Cybersecurity Framework Overview

The NIST CSF 2.0 provides structured guidance to help organisations manage and mitigate cybersecurity risks effectively. Central to the framework are five core functions that collectively outline the primary roles and activities within a cybersecurity programme.

(1) **Identify:** Develops an organisational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. This function underpins the foundation for all other functions in the framework.
(2) **Protect:** Outlines appropriate safeguards to ensure the delivery of critical infrastructure services. Protective measures help to limit or contain the impact of potential cybersecurity events.
(3) **Detect:** Defines the activities to identify the occurrence of a cybersecurity event. Timely detection helps organisations to effectively identify cybersecurity events.
(4) **Respond:** Includes actions to take regarding a detected cybersecurity event. Response activities help to contain the impact of a potential cybersecurity incident.
(5) **Recover:** Identifies activities to maintain resilience and restore any capabilities or services impaired due to a cybersecurity event, ensuring timely recovery to normal operations.

These core functions form a comprehensive framework that equips SOCs with the necessary tools to systematically address the full spectrum of cybersecurity challenges, from prevention to recovery.

### 1.3 Adopted Definition of Artificial Intelligence (AI)

Establishing a precise definition of AI is fundamental to our analysis of its implementation in **Security Operations Centers (SOCs)**. While the field has numerous interpretations and definitions [176], our study adopts a focused, operational perspective: AI is defined as a technology that enables machines to imitate various complex human skills, such as problem solving, learning from feedback, and making decisions with some degree of autonomy. AI involves systems that display intelligent behaviour by analysing their environment and taking actions to achieve specific goals. This definition encompasses a range of applications currently recognised as AI, while also allowing future technological developments and understanding. AI is not just about the use of algorithms or digital technology; it specifically involves systems that can operate with a level of independence to mimic human cognitive functions [191]. Crucially, this conceptualisation emphasises AI's capacity for autonomous operation—a characteristic that fundamentally differentiates it from traditional rule-based systems.

### 1.4 Research Questions

This SLR answers the following research questions regarding AI utilisation in SOCs:

- **RQ1: What are the current state-of-the-art applications of AI tools for SOC usage, and what are the prevailing trends and overall adoption patterns?** We explore the broad and detailed integration of AI in SOCs, identifying trends and adoption patterns.
- **RQ2: What is the motivation behind the development of AI tools in SOCs?** This question examines the motivations driving AI adoption in SOCs, aiming to align technology with organisational goals.
- **RQ3: To what extent are open-source tools proposed?** We investigate the use and influence of open-source tools in SOCs to understand their accessibility and impact.
- **RQ4: Which are the most frequently used AI algorithms?** Our analysis focuses on the prevalent AI algorithms used.
- **RQ5: Which are the most frequently used datasets and what are their specific characteristics in availability, and relevance to real-world scenarios?** We examine key datasets used in SOC applications, assessing their relevance and applicability to real-world needs.
- **RQ6: To what extent is the concept of explainability used in the AI tools?** This question explores the integration of explainability in AI models, highlighting its importance for transparency in cybersecurity.
- **RQ7: What are the limitations and challenges of the current applications?** We evaluate the limitations and challenges of AI in SOCs, identifying areas for future research and innovation.

The overarching aims of this review are to illuminate the AI landscape within SOCs, exploring its applications, trends, tools, algorithms, datasets, explainability, limitations, and challenges to guide future research and strategic decision-making.

### 1.5 Target Audience

The findings of this review and meta-analysis provide essential insights for cyber security practitioners, researchers, policymakers, and other stakeholders considering AI adoption within SOC operations. This work is pertinent to a diverse range of readers, ranging from SOC professionals to academic scholars, offering valuable knowledge to improve cyber defence strategies.

For cyber security practitioners, the review highlights state-of-the-art AI proposals and their operational benefits in SOCs, emphasising strategic AI solutions. Researchers will find a thorough

synthesis of the literature that sparks further exploration, while policymakers can make informed decisions about AI integration based on comprehensive trend analyses. Technology developers gain understanding of current challenges and opportunities in AI-driven solutions, and educators can use these insights to enhance learning in AI and cyber security disciplines.

Detailed insights tailored to specific reader groups, including how each section relates to particular research questions, are provided in our repository.[1] This ensures that each audience can find relevant and practical information to guide their decisions, matched to the defined RQs.

### 1.6 Contributions

In this SLR, we have conducted a comprehensive analysis to understand the role of AI within SOCs. Our review provides the following key contributions:

- Systematic Review of the Literature: We engaged in a systematic process of identifying relevant studies, extracting data, and synthesising findings. This process involved defining search criteria, selecting studies based on predefined eligibility criteria, and performing qualitative and quantitative analyses. Our efforts culminated in a comprehensive synthesis that maps a path for substantial future contributions to the cybersecurity field.
- Analysis of AI Applications: We provide a detailed examination of the AI tools proposed for SOC usage, addressing their effectiveness, explainability, and integration across SOC functions. This analysis, derived from the review of 189 scientific papers, provides a detailed overview of current state-of-the-art applications, the prevailing trends, and adoption patterns within SOC environments.
- Framework for Future Research: By categorising the existing literature according to the NIST CSF, this review not only organises previous studies systematically, but also provides a structured approach to understanding how AI tools can be better developed and implemented across different SOC functions. This framework serves as a basis for future innovations and strategic implementations in the field.
- Identification of Research Gaps and Motivation: Our study identifies significant gaps in the existing research and discusses the motivations driving the development of AI tools for SOC applications. By highlighting the limitations in current methodologies and frameworks, especially in terms of explainability and real-time applicability, we suggest avenues for future research focused on developing more transparent and adaptable AI solutions.

The rest of the article is organised as follows. Section 2 outlines the methodology employed, detailing the procedures and techniques used to gather and analyse data. Section 3 presents the results, highlighting key findings and trends identified from the data analysis. Section 4 provides a discussion of the implications of these results, exploring their significance and limitations in the context of existing literature, and suggests directions for future research. Section 5 discusses the related work in detail, contextualising our contributions within the broader research landscape. Finally, Section 6 concludes the article. Given the multifaceted nature of the topic, some discussions are addressed directly after presenting the results for a more direct connection between findings and their implications as they emerge, while limitations are included within discussions rather than exclusively in the conclusion section of the article, allowing findings to be interpreted more immediately within their context.

## 2 Methods

In this section, we describe the methodology used to conduct this review of the literature.

[1] https://github.com/desgiar/AI4SOC-SLR

Table 1. Search Keywords

| Line | Keywords |
|---|---|
| 1 | Security Operation? Cent* |
| 2 | SOC?; CSOC?; NOC? |
| 3 | AI; Artificial Intelligence; Machine Learning; Deep Learning; Neural Network? |

Given the frequent appearance of related but distinct concepts in the reviewed studies, we clarify our use of terminology at the outset. AI is used as an umbrella term encompassing a range of techniques aimed at simulating intelligent behavior. Within this scope, **Machine Learning** (**ML**) is a subset of AI and it refers to data-driven approaches that enable systems to learn and improve from experience. **Deep Learning** (**DL**), in turn, is a specialised subset of ML, characterised by the use of multi-layered artificial neural networks to model complex patterns in data. These distinctions are maintained throughout the review; while "AI" is used as the overarching term, we specify "ML" and "DL" where appropriate to reflect the scope and nature of each contribution.

### 2.1 PRISMA Statement

This SLR follows the guidelines outlined in the PRISMA 2020 statement [157]. The PRISMA framework provides a structured approach to systematically identify, select, and evaluate relevant studies for our research questions. By adhering to this recognised guideline, we minimise bias and increase the reliability of our findings.

### 2.2 Eligibility Criteria

To ensure the rigour, relevance and currency of this SLR, a set of predefined criteria has been defined, shown in Figure 2(a).

The flowchart outlines the selection criteria and the process for including research papers in a review of the literature focused on AI-enabled automation. The reason why we consider only papers published after January 2017 is to align with significant increases in AI development and deployment [128].

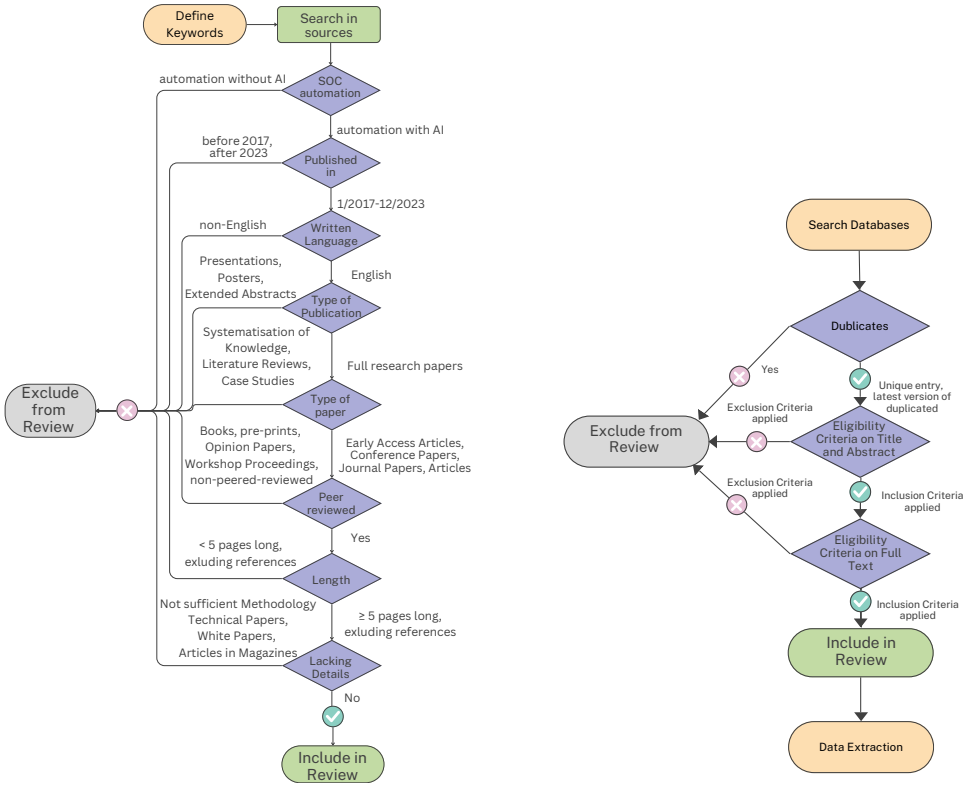
### 2.3 Information Sources

Our SLR required a thorough search to collect relevant scholarly works. We devised a strategic approach to extensively explore the following major databases: ACM Digital Library,[2] IEEE Xplore,[3] SpringerLink,[4] ScienceDirect,[5] Scopus,[6] Web of Science,[7] and Wiley Online Library[8] to ensure a broad and authoritative data selection.

### 2.4 Search Strategy

To delve into the existing literature, we crafted a set of search keywords, as outlined in Table 1. These keywords were selected to cover a broad spectrum of relevant topics within our research scope. Each line in the table represents a distinct category.

[2] https://dl.acm.org/
[3] https://ieeexplore.ieee.org/
[4] https://link.springer.com/
[5] https://www.sciencedirect.com/
[6] https://www.scopus.com/
[7] https://webofscience.com/
[8] https://onlinelibrary.wiley.com/




(a) Eligibility criteria (b) Search strategy

Fig. 2. Criteria and strategies for literature inclusion in the review.

The search string links terms from each category to ensure relevant and comprehensive results. Specifically, the search strategy was constructed as follows:

$$s \equiv l1 \text{ AND } l2 \text{ AND } l3$$

where each line $l$ represents a disjunction of its respective keywords. For example, $l2$ could be represented as

$$l2 \equiv \{\text{SOC OR SOCs OR CSOC OR CSOCs OR NOC OR NOCs}\}$$

We also needed a methodical and exhaustive establishment of the eligibility criteria to ensure the selection of relevant. Therefore, we devised and processed the search strategy presented in Figure 2(b). Wherever possible, we also excluded any results that were classified as “Review”, “Survey,” or “Case Study” in their titles.

Our keywords and search expressions, tailored to each database, are detailed in our repository,[9] ensuring a comprehensive and targeted approach to capture the relevant literature.

[9] https://github.com/desgiar/AI4SOC-SLR

### 2.5 Selection and Collection Processes

During the screening stage, a reviewer (one of the authors) evaluated all records, while a second reviewer (another author) performed a validation test on random samples. To ensure objectivity and cautious scrutiny, both reviewers worked independently and were blinded to each other's decisions. In instances where disagreements arose between the two, they were resolved through a consensus-based discussion.

### 2.6 Data Items

In our review, we specifically sought data on the effectiveness and efficiency of AI tools implemented within SOCs. We defined our outcomes of interest to cover a broad spectrum of AI applications in SOC environments, reflecting various techniques and their purposes in enhancing SOC operations. However, we excluded studies that solely discussed theoretical frameworks without empirical validation, speculative essays on potential AI applications in SOCs, and articles that focused on broader cyber security measures without a clear emphasis on the implementation of AI tools in SOC contexts.

Our selection process involved a systematic evaluation of each study's relevance to our defined outcomes, ensuring that the data collected were directly applicable to the assessment of AI tools in SOCs. In instances where studies provided incomplete information or lacked clarity on certain aspects, we categorised the data as "info not available" or "n/a" (not available). This categorisation was based on the context provided by each study, allowing us to systematically assess the availability and relevance of the data.

Given the extensive volume of relevant literature, it was necessary to also refine our scope to effectively manage the review. We analysed all studies on the implementation of AI tools in SOCs, applying the same analytical criteria throughout. Although we treated most studies uniformly, for certain specific research questions, we focused on in-depth publications from the top 10% venues. These questions are discussed in more detail in Section 2.9 where we elaborate on the insights they provide into SOC operations.

### 2.7 Study Risk of Bias Assessment

To ensure the validity and reliability of our findings, we carefully considered the risk of bias in the studies incorporated into our review. In the context of AI tools for SOC environments, biases can distort the actual effectiveness or performance of the tool, leading to incorrect conclusions. Therefore, in an attempt to provide an exhaustive and impartial review, we employed the following methods to reduce study risk bias:

— Use of multiple data sources: to avoid the risk of database-specific bias, we consulted multiple academic and industry databases
— Comprehensive Search Strings: the search terms were deliberately broad to capture as many relevant articles as possible. A combination of terms related to "AI", "Artificial Intelligence", "Machine Learning", "Deep Learning", "Neural Networks" and others ensured that the literature search was inclusive
— Eligibility Criteria: we set clearly defined criteria at the outset to ensure consistent article selection. Both inclusion and exclusion criteria were based on objective parameters, ensuring that the selection process remained free from individual biases.

While we did not apply a formal scoring or quality appraisal tool—given the lack of standardised frameworks tailored to computer science research—we took several steps to ensure the credibility of the studies included. This included focusing on peer-reviewed publications, enforcing strict eligibility criteria (e.g., minimum paper length, empirical validation), and excluding conceptual or

informal studies. These steps served to mitigate the risk of including low-quality or non-reproducible research, even in the absence of a numerical quality rating scheme.

### 2.8 Effect Measures

In our systematic review, we came across various outcomes reported by the studies. Below, we list the instances we sought—even if that information is not always available in the reviewed paper.

(1) **Prevailing trends** (RQ1) refer to what is currently popular and/or gaining traction every year since 2017
(2) **Overall adoption pattern** (RQ1) refer to the general trajectory of what is adopted and integrated since 2017
(3) **Open-source** (RQ3) is determined by the:
   — presence of link to a software repository
   — (and/or) source code in the paper
   — (and/or) explicit mention of licence by the authors
(4) **Explainability** (RQ6) can be assessed by the:
   — explicit mention of **explainable AI** (**XAI**) methods by the authors (Explainability Level:High)
   — presence of surrogate models: complex models might be interpreted using simpler, more explainable "surrogate" models (Explainability Level:Moderate)
   — model type: simpler models like linear regression, decision trees, and logistic regression tend to be more interpretable than complex models like deep neural networks (Explainability Level:Moderate)
   — feature analysis: examining the contributions of individual features to model outputs through sensitivity analysis and feature importance metrics (Explainability Level:Moderate)
   — presence of visualisations such as heat-maps, partial dependence plots, and feature importance charts (Explainability Level:Moderate)
   — narrative explanation: plain-language summaries or rule lists can be generated to explain model decisions (Explainability Level:Moderate)

   A paper can be considered as having a high degree of explainability if it includes at least three of the criteria marked with a moderate explainability level.

### 2.9 Synthesis Methods

We employ both qualitative and quantitative synthesis methods, each tailored to specific research questions to maximise the clarity of our findings.

— Quantitative Synthesis: For research questions RQ3, RQ4, RQ5, and RQ6, which examine the prevalence, effectiveness, efficiency, and explainability of AI tools within SOC environments, we utilised a comprehensive quantitative analysis approach. This approach encompasses all publications included in our review, involves statistical methods to aggregate data from all studies, to ensure a robust statistical examination, and to capture broader trends across the entire corpus of literature. It also allows for robust metaanalytical techniques to be applied where applicable. We displayed the results of individual studies and their synthesis using structured tables and graphical representations.
— Qualitative Synthesis: Conversely, for RQ2 and RQ7, which focus on the motivations behind the development of the AI tool and the challenges faced, a qualitative analysis is more appropriate. This component of our synthesis is restricted to the primary studies selected that have been published in the top 10% of the venues. We conducted a narrative analysis to extract motivations and challenges, which were then thematically analysed. This selective approach

allows us to dig deeper into the most influential research, providing nuanced insights into the developments and trends within the field.

By distinguishing between these two methods of synthesis, we ensure that each set of research questions is addressed using the most appropriate and methodologically sound approach.

Due to the wide variation in study types, evaluation metrics, datasets, and research goals across the included papers, a formal meta-analysis was not feasible. Instead, we adopted a descriptive and thematic synthesis approach, which is more suitable for reviews in computer science domains where standardised quantitative outcomes are uncommon.

### 2.10 Reporting Bias Assessment

In this rapidly evolving scientific field, there is a potential risk of reporting bias, where only successful tool implementations or favourable outcomes are published. To assess the risk of bias due to missing results, which may arise from selective outcome reporting and to reduce the risk of post hoc changes based on observed results, we relied on the following methods.

— Broad Search Strategy: Our SLR encompassed not just mainstream highly-cited publications but also lesser-known papers to capture a wide range of AI tools designed for SOCs
— Critical Analysis: Rather than focusing solely on the reported successes of AI tools, papers were critically examined for any limitations, challenges, or areas of improvement (RQ7). This approach ensures that not just the positive but also the negative or inconclusive aspects of AI tool design are considered
— Consistent Outcome Measures: to avoid measurement or detection bias, standardised metrics (see Section 2.8) were consistently used across studies to evaluate AI tool performance in SOC environments
— Documenting Decisions: Every decision to include or exclude a paper was documented with clear reasons. This transparency ensures that the review process can be audited and understood by external parties, adding an extra layer of credibility

### 2.11 Certainty Assessment

To provide a precise and meaningful synthesis of the existing literature on AI tools for SOC environments, it is crucial not only to identify and summarise the relevant articles, but also to assess the certainty or confidence in the body of evidence presented.

— Directness of Evidence: we preferred direct evidence linking the AI tool to the desired outcome in SOC environments (e.g., reduced false positives, improved threat detection rates) over indirect outcomes.
— Quality of Reporting: papers that provide detailed methodologies, and were transparent about their limitations were considered to offer higher certainty

## 3 Results

In this section, we present the findings of our study. The results are organised according to the research questions described in Section 1.4.

### 3.1 Study Selection

As we mentioned in Section 2.1, we followed the PRISMA flow process [157] for the complete collection and selection of the literature, as illustrated in Figure 3.

Initially, 863 records were identified across multiple databases. Prior to screening, 30 records were removed due to duplication and 26 for other reasons, including items flagged by publishers with expressions of concern (indicating potential issues with the reliability of the content), records

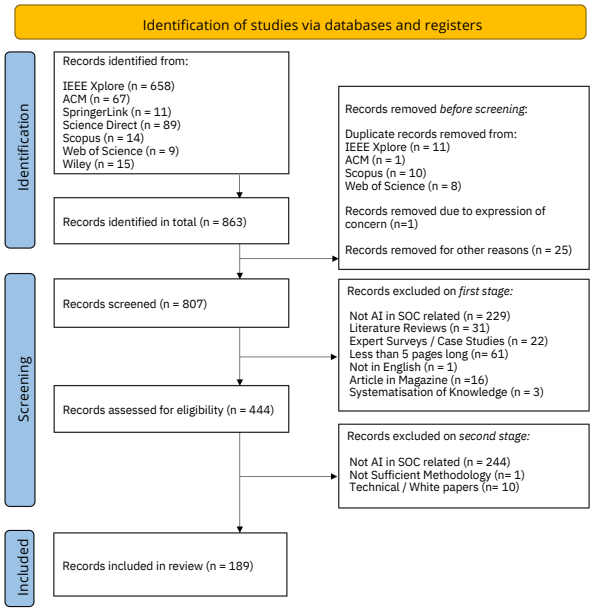



Fig. 3. Flow diagram for this SLR.

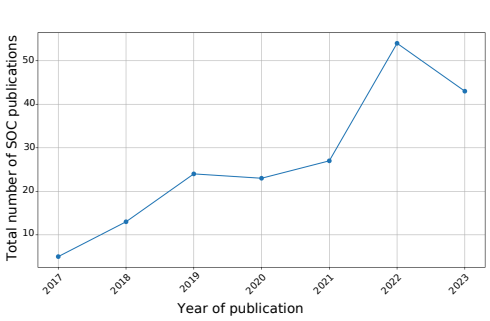
consisting only of table of contents or abstracts, and front matters. Upon screening, 807 records were evaluated, with further exclusions based on relevance and criteria discussed in 2.2, such as article type, length, language, and methodology. We also excluded categories such as **Proofs of Concept (PoCs)** [111], and papers focused on overview and analysis [58] or the evaluation [41, 59, 125] of ML algorithms. These exclusions were necessary as PoC papers typically explore feasibility rather than practical implementation, and lack comprehensive data on efficacy within SOC environments. Similarly, papers solely evaluating ML algorithms often lacked integration with SOC workflows or considerations of operational constraints and cybersecurity applications. By excluding these categories, the review ensures that the studies included are directly relevant to the practical challenges and applications of AI in SOC environments, offering insightful advancements in the field.

Following a detailed eligibility assessment of 444 records (as shown in 2.4), 189 were ultimately included in the review.

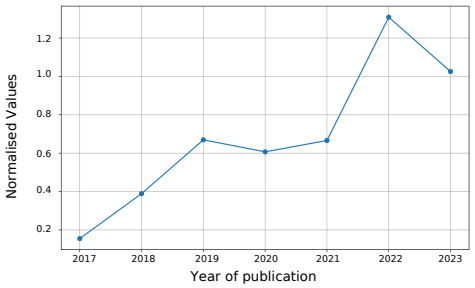
### 3.2 Current State-of-the-Art, Prevailing Publication Trends, and Adoption Patterns

In the current state-of-the-art, we delve into the prevailing trends and adoption patterns of AI tools within SOCs. Our structured analysis provides insights into the venues publishing the relevant research, a chronological review of advancements over time, and a detailed categorisation of these technologies according to the NIST CSF core functions. In addition, we classify the findings based on overarching themes that emerge across the studies.

*3.2.1 Time Frame.* The examination of publication trends within our selected SLR corpus is illustrated in Figure 4(a). To ensure the reliability of our findings, we normalised the data based on the total number of publications indexed in the Scopus database, as shown in Figure 4(b). The studies span from 2017 to 2023 and as evident from the figures, there has been a notable increase, in both the total number of SOC-related publications and their proportion relative to the global




(a) Trends in AI-related publications for SOC




(b) Ratio of SOC publications to total Scopus publications

Fig. 4. Trends and ratios of SOC-related AI publications.

research output. This trend underscores an expanding academic interest in SOC technologies and strategies, indicative of their rising prominence within cybersecurity research circles.

Starting from a modest number of five publications in 2017, the count rose steadily, peaking at 54 publications by 2022. This crescendo aligns with intensified research and development activities in AI applications for SOCs, as cybersecurity evolving dynamics become more complex. Interestingly, the relative decline in 2023, calls for a deeper analysis to understand underlying factors such as changes in research funding, academic focus, global economic conditions, or even the time taken for indexing papers in data sources that might influence research output that might influence research output. While the decrease is not drastic, it still represents a noticeable reduction.

This growth trajectory and the ensuing dip provide critical insights into the temporal dynamics of research interest and resource allocation in cybersecurity. They not only reflect the academic community's response to emerging threats, but also highlight potential areas where future research could either consolidate established knowledge or venture into unexplored territories within the realm of cybersecurity and AI applications in SOC environments.

*3.2.2 Venues.* We now analyse the distribution between conferences and journals. Conferences constitute 64.60% of the publications, while journals account for 35.40% of our sources. This distribution is significant as it reflects the dynamic and rapidly evolving nature of the field, where researchers often choose conferences to present their initial results because of faster publication times. Journals, on the other hand, are chosen for more comprehensive studies and have undergone a more rigorous peer review process.

For the full list of primary studies, published in the top 10% of venues included in our review, see Table 2. We did the selection based on the recognised academic metrics mentioned in 2.9. We used Scopus[10] metrics to evaluate journals and CORE rankings[11] for conferences. We opt for this approach, as the CORE rankings for journals were discontinued from March 2022 [3], necessitating a reliable alternative that continues to reflect current standards. This dual approach ensures that our selection encompasses publications that are not only influential but also adhere to high standards of academic impact. By prioritising these metrics, we aim at highlighting studies that provide the most significant contributions to the field, ensuring that our analysis is grounded in quality and excellence. There are 64 studies included in Table 2.

[10] https://www.scopus.com/sources/
[11] http://portal.core.edu.au/conf-ranks/

Table 2. The Full List of the Primary (Top 10%) Publications Selected

| Venue | Ranking/ Percentile | Publications |
|---|---|---|
| *Conference* | | |
| ACSAC | A | [36, 108, 154, 175, 230] |
| CCS | A* | [66] |
| IEEE S&P | A* | [205, 228] |
| RAID | A | [51, 110] |
| SANER | A | [195] |
| *Journal* | | |
| IEEE Access | 92 | [98, 101, 102, 105, 113, 114, 174, 193, 194, 224], [20, 37, 61, 70, 71, 82, 126, 137, 202] |
| Journal of Computer and Security | 99 | [28, 68, 73, 83, 106, 121, 173, 201] |
| IEEE Transactions on Dependable and Secure Computing | 92 | [33, 57, 139, 204, 226] |
| Journal of Information Security and Applications | 94 | [54, 86, 99, 215] |
| Journal of Future Generation Computer Systems | 98 | [24, 79, 179] |
| IEEE Internet of Things Journal | 97 | [55, 91, 158] |
| ACM Transactions on Intelligent Systems and Technology | 95 | [187] |
| IEEE Transactions on Visualisation and Computer Graphics | 91 | [75] |
| IEEE Communications Surveys & Tutorials | 99 | [13] |
| IEEE Transactions on Industrial Informatics | 99 | [39] |
| Journal of Cybersecurity | 97 | [14] |
| Journal of Expert Systems with Applications | 96 | [12] |
| Jounal of Chaos, Solitons & Fractals | 99 | [161] |
| Journal of Decision Support Systems | 98 | [97] |
| Journal of Information Systems | 96 | [18] |
| Journal of Network and Computer Applications | 98 | [89, 92] |

*3.2.3 Framework.* Following the chronological and venue distribution analysis of the studies, we transition our exploration to a framework-oriented approach. The NIST CSF, as outlined in 1.2 for a SOC environment, serves as our foundational structure to categorise the studies. By mapping the studies to these functions, we provide a comprehensive view of how AI tools are being integrated into the SOC workflow. Table 3 catalogues a concise overview of the 189 studies included in our review based on their classification to CSF.

As depicted in Figure 5, the distribution of studies between NIST functions reveals the current focus areas in the implementation of AI tools within SOC environments. The majority of the studies (129 entries) mainly focus on the "detect" function, highlighting the prevalent emphasis on threat detection capabilities within SOCs. This is followed by "identify" and "protect", each with 40 and 21 entries, respectively, which underscores the importance of asset management, risk assessment, and safeguarding measures in initial security setups. "Respond", with 22 entries, shows a growing engagement in post-incident handling. The "recover" function indicates an area for further research and development in recovery processes in SOCs. Finally, studies that span multiple NIST functions often include elements of the "respond" phase, indicating that, although these tools are not primarily designed for response activities, there is a noticeable shift towards incorporating response capabilities or analysis.

**RQ1:** A chronological analysis shows a rising trend in AI tool publications for SOCs, predominantly at conferences, while most top-tier papers appearing in journals. This trend is complemented by a NIST-oriented approach where the "detect" function dominates, pointing to a focused yet critical need for advancements in "respond" and "recover" functions within SOC environments.

Table 3. List of the Studies Based on the NIST CSF 2.0 Core Functions

| Function | Publications | Total | Main class |
|---|---|---|---|
| Identify | [8, 16, 19, 23, 31, 32, 39, 42, 44, 49, 60, 61, 63, 75, 77, 81, 83, 92, 98, 99, 126, 127, 140, 141, 155, 173, 178, 180, 192, 194, 205, 212, 214, 218, 220, 226, 229, 230]*, [129]*, [165]* | 40 | 19.57% |
| Protect | [13, 22, 25, 27, 52, 60, 95, 129, 136, 156, 158, 159, 182, 199, 227]*, [54]*, [177]*, [212]*, [55]*, [121]*, [200]* | 21 | 7.40% |
| Detect | [6, 12, 14, 18, 20, 21, 24, 26, 28, 29, 33–38, 44, 46, 47, 50, 51, 53–56, 62, 64–71, 73, 74, 78, 79, 82, 84, 85, 91, 94, 97, 100–110, 112–124, 130, 133, 134, 137–139, 142–146, 148–150, 153, 161–166, 169, 170, 172, 174, 175, 177, 179, 183–185, 187, 193, 197, 198, 200–202, 204, 206–208, 210, 211, 213, 215–217, 219, 221–224, 228, 230, 231]*, [227]*, [13]*, [212]*, [180]*, [129]* | 129 | 65.08% |
| Respond | [10, 11, 43, 57, 76, 80, 86, 88, 89, 121, 131, 132, 160, 186, 195, 196]*, [36]*, [110]*, [51]*, [200]*, [129]*, [163]*, [180]*, [65]* | 24 | 7.93% |
| Recover | - | 0 | 0% |

Entries with an asterisk (*) indicate a secondary classification of a study already primarily classified elsewhere. "Main class" denotes the percentage of studies primarily classified under each function.

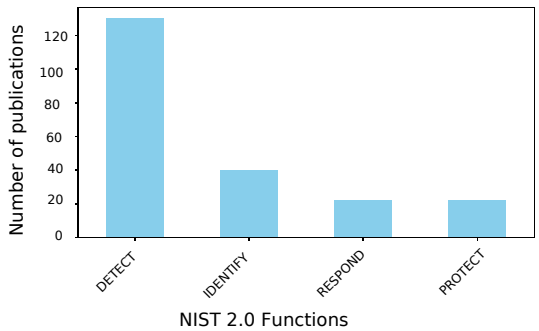



Fig. 5. Distribution of AI-enabled SOC publications by NIST 2.0 functions.

### 3.3 Motivations

In addressing the motivation behind the development of AI tools for SOC, we conducted a qualitative synthesis focusing on the studies published in the top 10% of venues. These papers were subjected to a detailed narrative examination and the motivations for developing AI tools were extracted and thematically analysed. The analysis revealed several core motivations which were grouped into distinct categories as shown in Table 4. Our goal was to provide a deeper understanding of the forces driving AI integration into SOC environments, based on the most influential and high-impact research within the field.

**RQ2** The development of AI tools for SOCs is motivated by a variety of factors. Key drivers include the need for greater efficiency, enhanced detection capabilities, error reduction, scalability, and cost savings.

Table 4. Key Motivational Themes Identified

| Motivation | NIST | Explanation | Examples | Publications |
|---|---|---|---|---|
| Improvement in Threat Detection and Response | Detect, Respond | Enhancing the accuracy, speed, and reliability of identifying and mitigating threats. Includes automation and efficiency improvements for SOC workflows. | Real-time threat detection, automated incident response, streamlining SOC processes, reducing false positives, improving detection algorithms, and faster response times. | [12, 86, 89, 105, 114, 161, 173, 179, 187, 215] |
| Application of Advanced AI Techniques | Detect, Respond | Leveraging cutting-edge AI methodologies to solve complex cybersecurity challenges. | Reinforcement learning, adversarial machine learning, and explainable AI techniques. | [54, 99, 114, 187, 194] |
| Real-Time and Scalable Solutions | Detect, Respond | Developing solutions that handle large-scale and high-speed cybersecurity requirements. | Scalable anomaly detection, live-streaming data analysis. | [12, 173, 224] |
| Explainability in AI Models | Detect, Respond | Making AI model decisions understandable through explainable predictions and clear reasoning. | Feature attribution in detection models, clear explanations for classification results. | [194] |
| Adaptability to Evolving Threats | Identify, Protect | Developing systems that can adapt to dynamic and sophisticated cyber threats. | AI models for emerging malware, proactive defenses against zero-day attacks. | [89, 105, 114, 173, 194] |
| Trust and Transparency | Identify, Protect | Ensuring that AI systems are trustworthy, fair, and transparent, with reliable operations. | Ethical audits, bias detection in classifiers, and transparent training methodologies. | [194] |
| Integration of Cyber Threat Intelligence (CTI) | Protect, Detect | Using CTI to improve threat detection, response, and proactive defenses. | OSINT evaluation, regression models for CTI prediction, timeliness of alerts. | [18, 194, 201] |
| Enhanced Situation Awareness and Intelligence Sharing | Identify | Providing real-time insights into cybersecurity threats and improving information sharing between stakeholders. | Leveraging social media for threat awareness, sharing threat intelligence across organisations. | [18, 201] |
| Enhanced Vulnerability and Security Assessment | Identify | Improving methods for identifying and assessing vulnerabilities in systems and networks. | Enhanced SIEM systems, better situational awareness, and proactive risk assessments. | [92, 99, 106] |
| Focus on Specialised Threat Areas | Protect | Addressing niche areas of cybersecurity like IoT botnets, DGA-based malware, and specific malware families. | IoT-specific IDS, botnet traffic detection, and advanced malware classification. | [79, 194] |
| Network Security Enhancements | Protect | Strengthening the monitoring and protection of network environments. | Traffic analysis, anomaly detection, and identifying malicious activities in networks. | [24, 86, 102] |
| Strengthening Email and Phishing Defences | Protect | Improving the detection and prevention of email-based threats, including phishing. | AI models for phishing detection, enhanced spam email classification. | [68] |
| Focus on Industrial and IoT Security | Protect | Addressing the unique security needs of industrial systems and IoT environments. | Securing IoT, dual-layer IDS for IoT, and smart industry cybersecurity. | [14, 79] |
| Optimisation of Machine Learning Models | Detect | Improving the design and performance of machine learning models used in cybersecurity. | Active learning, handling imbalanced datasets, and refining anomaly detection models. | [79, 99, 106, 114] |
| Advancements in Intrusion Detection Systems (IDS) | Detect | Enhancing the robustness, accuracy, and applicability of IDS for modern networks. | GAN-based IDS, IDS for IoT and SDN environments. | [14, 54, 102, 161, 224] |
| Improvement in Malware Detection and Classification | Detect | Enhancing the accuracy and efficiency of detecting and categorising malware. | Using graph-based representations, reducing false alarms, and classifying malware families. | [28, 70, 73, 108] |
| Enhancements in SOC Tools and Operations | Respond | Improving the tools, technologies, and workflows used in SOCs to handle modern cybersecurity challenges. | API integration for incident mapping, advanced tool support for analysts. | [89, 154, 175] |
| Reduction of Cognitive Load on Analysts | Respond | Minimising the mental strain on security analysts by simplifying complex processes and reducing noise. | Prioritising alerts, reducing alert fatigue, and providing actionable insights. | [114, 173, 187, 215] |
| Reduction of Manual Efforts in Security Operations | Respond | Automating labor-intensive tasks in SOC workflows to save time and resources. | Automating log analysis, mapping incident response plans to APIs. | [89, 97, 114, 194, 215] |

Table 5. The List of All Publications with Some Information According to the Available Tools Proposed

| Open Source | Indicator | Publications |
|---|---|---|
| Yes | Link to Github Repository | [21, 27, 66, 73, 78, 102, 110, 124, 139, 205, 207, 230] |
| Yes | Link to Gitlab Repository | [50] |
| Yes | Public release of datasets and code mentioned | [178] |
| Yes | Release of code and datasets to IEEE Code Ocean and IEEE DataPort platforms | [228] |
| Maybe | Open-sourcing the prototype code after integrated into security products | [218] |

### 3.4 Open-Source Tools

We categorised each paper based on whether the introduced tool is published as **open source software** (**OSS**). Among the reviewed articles, only 16 (8.50%), provided explicit information about proposing and/or implementing open source tools, indicating a direct engagement or recommendation of such tools. In contrast, the vast majority (173 (91.50%) did not provide specific details about open source tools, pointing to a significant gap in explicit OSS advocacy or usage details within the literature.

Further analysis of the papers suggesting potential OSS usage shows that 1 paper (6.25%% of this specific subset) might suggest an open-source tool, albeit without definitive confirmation. Meanwhile, 15 papers (93.75% of this subset) definitively identified the use of open source tools, emphasising a clear but limited recognition of open-source solutions in academic discussions.

Further analysis reveals that of the papers with explicit information, 15 (93.75% of this specific subset) have definitively identified the use of OSS tools, such as by providing links to GitHub or GitLab repositories, or announcing the public release of datasets and code, while, 1 paper (6.25% of this subset) indicates a potential future release of open-source tools ("Maybe OSS"), suggesting a tentative but not confirmed engagement with OSS practices.

These insights reflect the varying degrees of open source tool proposal within the scholarly community, illustrating direct and indirect references to their use and importance. For a detailed breakdown of these categories, see Table 5.

**RQ3:** Among the reviewed papers, only 8.50% provide some information on whether the proposed tools are open-sourced, with most including definitive evidence such as repository links or public releases. The vast majority (91.50%) do not provide information, highlighting a significant gap in the literature.

### 3.5 Algorithms

The range of AI algorithms utilised in the literature is diverse and expansive. As detailed in Table 6, AI algorithms span multiple families and types, from traditional ML methods to advanced generative AI.

Figure 6 illustrates the top 10 algorithms by frequency of usage, highlighting a strong preference for ML classifiers such as Random Forests and Support Vector Machines.

**RQ4:**The literature features a diverse range of AI algorithms, with a notable preference for Random Forests and Support Vector Machines.

Table 6. The Full List of the AI Algorithms Used in the Proposed Tools for SOC

| AI Families | Types | Category | Total |
|---|---|---|---|
| *Machine Learning* | | | |
| | Supervised Learning | Classifiers | 143 |
| | | Ensemble Methods | 9 |
| | Unsupervised Learning | Clustering | 6 |
| | | Anomaly Detection | 18 |
| | Neural Networks | | 27 |
| *Deep Learning* | | | |
| | Convolutional Networks | | 24 |
| | Recurrent Networks | | 32 |
| | Autoencoders | | 9 |
| *Natural Language Processing* | | | |
| | Techniques | | 16 |
| | Advanced NLP | | 6 |
| *Reinforcement Learning* | | | 7 |
| *Generative AI* | | | 6 |
| *Custom Algorithms* | | | 3 |
| *Federated Learning* | | | 2 |

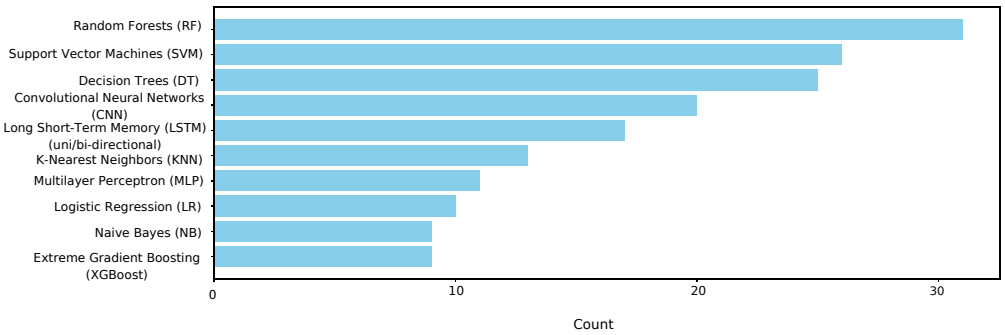


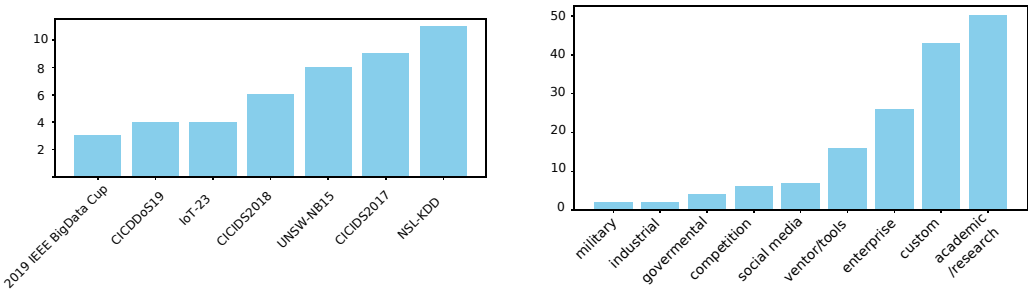

Fig. 6. Top 10 algorithms used in literature.

### 3.6 Datasets

In this section, we examine the datasets employed. Figure 7(a) presents the most frequently used datasets. The list reveals that NSL-KDD [151], CICIDS2017 [189], UNSW-NB15 [135], and CSE-CIC-IDS-2018 [2] are the most referenced datasets, along with notable mentions of IoT-23 [72], CICDDoS19 [190], and 2019 IEEE BigData Cup [87]. These datasets are indispensable for testing intrusion detection systems and evaluating cyber attacks, providing structured data for training and testing ML models in cyber security scenarios.

In addition, Figure 7(b) presents all the datasets reviewed and classified into various categories. Academic/research datasets which represent the largest category, generated and maintained by academic institutions for security model evaluations. Custom datasets, and enterprise datasets follow, highlighting data tailored for specific research or collected from organisational systems, respectively.

Dataset availability remains a critical factor, as shown in Figure 8, where only 28 datasets are confirmed available, and a significant portion (159) lack clear availability information. It also details




(a) Most frequent datasets (b) Categories of datasets

Fig. 7. Frequency and types of cybersecurity datasets used in literature.

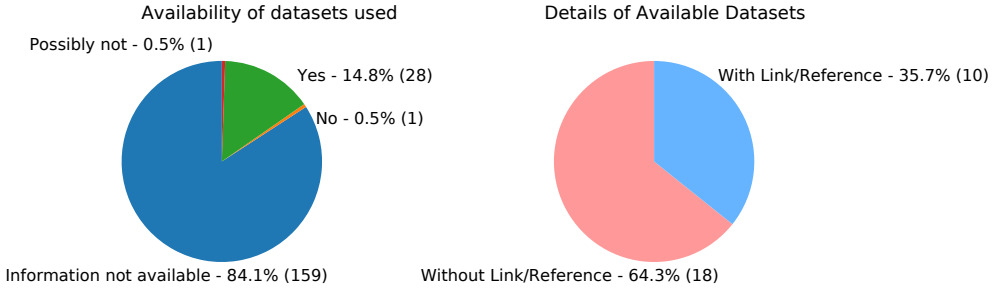



Fig. 8. Availability of datasets used in the literarture.

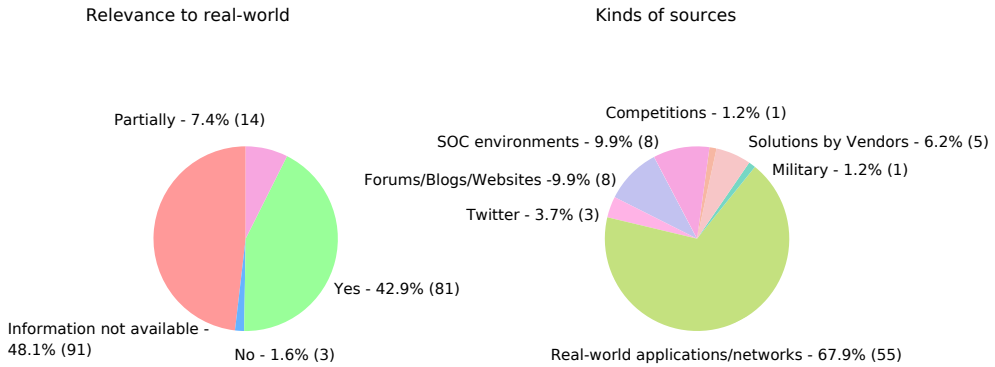



Fig. 9. Relevance of datasets to real-world.

that among the available datasets, 18 are provided without and 10 with proper references or links, mainly to GitHub repositories.

55 datasets are directly sourced from real-world applications or networks, emphasising the relevance of practical data in cybersecurity research. Other sources include social media, vendor solutions, and SOC environments, further depicted in Figure 9.

This data informs us about the trends and challenges in dataset usage for AI in SOC research, highlighting the need for better documentation and accessibility to foster research reproducibility and advancement.

Table 7. The List of All the Publications with Some Information as Per the Proposed Tool Explainability

| Publication | Use of XAI | Use of Simpler/Interpretable models | Use of Surrogate models | Narrative Explanation | Feature analysis | Visualisations | Explainability Level |
|---|---|---|---|---|---|---|---|
| [217] | ✓ | | | | | | High |
| [211] | | ✓ | ✓ | | | ✓ | High |
| [154] | | ✓ | | | | | Moderate |
| [50] | ✓ | ✓ | | | ✓ | | High |
| [108] | ✓ | | | | | | High |
| [194] | ✓ | | | | | | High |
| [156] | | ✓ | | ✓ | | ✓ | High |
| [197] | | ✓ | | | | ✓ | Moderate |
| [139] | | ✓ | | ✓ | | ✓ | High |
| [105] | ✓ | | | | | | High |
| [148] | | | | | ✓ | | Moderate |
| [67] | ✓ | | | | | | High |
| [37] | | ✓ | | | | | Moderate |
| [6] | | ✓ | | ✓ | | ✓ | High |
| [205] | | ✓ | | | | | Moderate |
| [53] | | ✓ | | ✓ | ✓ | | High |
| [204] | ✓ | ✓ | | ✓ | ✓ | | High |
| [121] | ✓ | | | | | | High |
| [110] | | | ✓ | | ✓ | ✓ | High |
| [51] | ✓ | | | | ✓ | ✓ | High |
| [123] | ✓ | | | | ✓ | ✓ | High |
| [145] | ✓ | ✓ | | | | ✓ | High |

**RQ5:** The most frequently used datasets in AI for SOC research include NSL-KDD, CICIDS2017 and UNSW-NB15. Availability information is often lacking, with only 14.80% of datasets confirmed as accessible. These datasets are primarily sourced from real-world applications or networks, indicating their high relevance to practical cybersecurity scenarios. Also, there is an over-reliance on proprietary datasets.

### 3.7 Explainability

We also assess the extent of explainability incorporated into AI models across various studies. From the articles examined, only 22 publications reveal engagement with explainability. Out of this subset, 77.27% explicitly embraced explainability methodologies, see (Table 7). A notable proportion, 22.73%, has a moderate level of explainability, indicating that these studies incorporate some level of explainability in their methodologies, even without the application of nuanced XAI techniques.

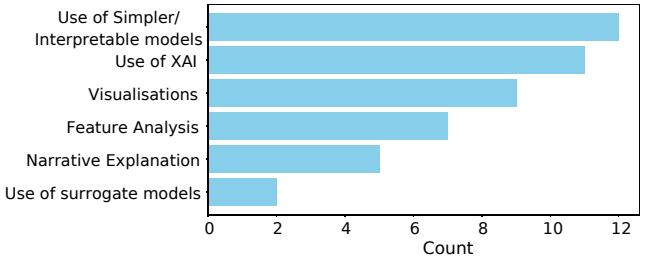



Fig. 10. Indicators of an explainable model.

The breakdown of explainability techniques shows a preference for simpler and more explainable models, with visualisations use of XAI also prominently used (Figure 10). Specifically, the use of simpler/interpretable models was the most commonly reported approach, reflecting a trend toward reducing model complexity for enhanced explainability.

However, our review also highlights a significant gap in methodology reporting, with only 11.64% of the studies explicitly providing information on the extension of the techniques employed to achieve explainability. This suggests a transparency gap that could hinder the replication and broader adoption of explainable AI techniques.

A detailed tabulation of the explainability attributes in the selected publications further underscores the diverse approaches to integrating explainability into AI systems. While several studies leveraged multiple techniques for explainability, others relied on specific methods tailored to their research context, with partial explainability reflecting either an emerging integration of these techniques or a focused application relevant to specific model functionalities.

**RQ6:** Among the analysed papers, 5.82% introduce models with inherent transparency, making them easily explainable, while an additional 5.82% employ techniques to moderately enhance the explainability of their models. However, a significant majority, 88.36% of the papers do not include any information on theexplainability of their models.

### 3.8 Literature Limitations and Challenges

As part of our qualitative synthesis of studies published in top-tier venues, we identified several critical limitations and challenges that impact the applicability and scalability of current SOC AI tools. These findings not only highlight pivotal research gaps but also emphasise the pressing need for innovative solutions tailored to meet the dynamic requirements of cybersecurity.

Table 8 lists the significant limitations revealed in the reviewed literature, illustrating the constraints that current research must navigate. These limitations necessitate innovative approaches to transcend these barriers. Conversely, Table 9 delineates the principal challenges noted in the studies, each underscoring essential areas for development and collaboration in the cybersecurity field.

**RQ7:** The exploration of limitations and challenges in SOC AI tools reveals critical gaps such as data reliance, scalability issues, and integration complexity, driving the need for innovative and adaptable cybersecurity solutions.

Table 8. Limitations in Literature

| Limitations | Explanation | Publications |
|---|---|---|
| Reliance on Available Data | Dependence on existing data sources which may not always be representative or comprehensive, affecting the model's accuracy and applicability in real scenarios. | [89, 98, 230] |
| Scalability and Performance Issues | Difficulties in scaling cybersecurity solutions to handle large volumes of data efficiently without degradation in performance. This includes the need for systems to operate effectively under varying network loads and transaction volumes. | [12, 24, 28, 66, 68, 82, 215] |
| Complexity of Integration and Adaptation | Related to integration of cybersecurity systems into existing infrastructures and their adaptation to new or changing technologies and threat landscapes. | [161, 173, 187, 201] |
| Resource and Computational Requirements | Points to the high resource and computational demands of running advanced cybersecurity models, especially in real-time scenarios. | [12, 20, 66, 68, 86, 98, 99] |
| Lack of Generalisability | Many AI tools are tested under controlled conditions and fail to perform as expected across different settings or data types, due to the training on datasets that do not fully capture the diversity of real-world scenarios. | [12, 13, 24, 28, 33, 68, 71, 97, 110, 137, 161, 187, 201, 202, 205, 215] |
| Interpretability and Explainability | The black-box nature of many AI models makes it difficult for SOC operators to understand and trust the outputs, as they cannot explain the decisions made by complex models. | [12, 13, 28, 33, 39, 39, 51, 71, 86, 97, 99, 113, 121, 202, 204, 226] |
| Data Privacy and Legal Concerns | Handling sensitive data, complying with privacy laws, and ethical concerns, which can limit the data available for training and affect the deployment of cybersecurity solutions. | [173, 230] |

Table 9. Challenges in Literature

| Challenges | Explanation | Publications |
|---|---|---|
| Handling Complex and Evolving Threats | Difficulty in adapting detection models to rapidly evolving cyber threats. It involves the need for models that can dynamically update and respond to new threat behaviours without extensive retraining. | [12, 28, 37, 51, 54, 66, 71, 82, 86, 89, 97–99, 110, 137, 195, 202, 226] |
| Data Quality and Availability | Involving the limitations in the availability of high-quality, diverse datasets necessary for training robust detection models. This impacts the model's ability to generalise and function effectively in varied real-world scenarios. | [12, 20, 24, 33, 66, 71, 73, 98, 113, 137, 161, 201, 204, 226] |
| Real-Time Detection and Analysis | Refers to the requirement for cybersecurity tools to perform threat detection and response in real-time, managing the high-speed data flow characteristic of modern networks while maintaining accuracy. | [18, 24, 37, 39, 82, 86, 121, 137, 139, 161, 173, 201, 205, 215] |
| Adaptation to Diverse Environments | Deploying cybersecurity systems that are effective across different network architectures, operational technologies, and varying scales of enterprise environments. | [14, 24, 37, 39, 66, 89, 137, 161, 195, 201, 202] |
| Model Training and Learning Issues | Encompasses difficulties such as limited training data, the complexity of training models on multifaceted cyber threats, and the need for models to quickly adapt to new threats. | [39, 66, 71, 79, 97, 99, 121, 137, 202, 204, 226] |
| Accuracy and Efficiency in Detection | Balancing the speed of detection and the accuracy, particularly in environments where the volume and complexity of data can significantly vary. | [37, 39, 97, 99, 106, 110, 161, 201] |
| Human-Machine Interaction | Concerns the need for effective interfaces between cybersecurity personnel and automated systems, ensuring that users can understand, interact with, and appropriately trust the machine-generated insights for decision-making. | [39, 66, 68, 79, 83, 137, 173, 205] |

## 4 Discussion

### 4.1 Analysis and Future Directions

Our SLR aims to bridge the gaps by offering a holistic overview of the AI tools proposed for SOCs, highlighting both the algorithmic advancements and the strides made toward developing explainable AI systems. In doing so, our goal is to foster a deeper understanding of the tools

available and their implications for security practice, thus guiding future research directions in this critical area of cybersecurity.

The predominance of conference papers in our review reflects a strategic shift within the cybersecurity community towards more agile and immediate dissemination of research findings. Given the rapidly evolving landscape of cyber threats and technological advancements, this approach can be seen as a pragmatic adaptation that ensures that the latest solutions and insights reach practitioners and researchers rapidly, in a field that demands quick responses to emerging threats and novel technologies. Conferences facilitate the quick exchange of ideas and foster collaborations more effectively than the slower, more deliberate process typical of journal publications.

However, the under-representation in top-tier venues reflects a larger challenge within the cybersecurity research community. The scarcity of publications in top-tier venues may suggest a maturity issue, where groundbreaking, novel ideas that top-tier venues demand are less frequent. Also, academic venues often prioritise theoretical advances and universal methodologies over applied, compared with specific-case studies, which are more typical in SOC research. The practical nature of SOC studies, focusing on immediate applicability rather than broad theoretical contributions, might not align well with the publication criteria of high impact venues. Future research should bridge this gap, encouraging studies that balance theoretical rigor with practical relevance to enhance both the depth and applicability of research in high-impact journals.

Despite the growing relevance of AI in cybersecurity, and beyond publishing challenges, the overall academic exploration of its role in SOCs remains limited. Several structural and practical barriers may account for this. First, SOC operations are highly application-driven, and research in this area often focuses on operational outcomes rather than theoretical advances, which can make it less aligned with traditional academic publishing norms. Second, access to real-world SOC environments and data is heavily restricted due to confidentiality, legal, and ethical concerns, hindering empirical validation and reproducibility. Third, meaningful AI integration in SOCs requires deep interdisciplinary collaboration—combining expertise in cybersecurity, AI, human factors, and business processes—something that remains challenging within the typically siloed structure of academic research. Addressing these issues may require stronger partnerships between academia and industry, incentivised data-sharing frameworks, and funding mechanisms that prioritise applied, reproducible, and cross-disciplinary work.

Another significant observation is the concentration of research on the "Detect" function within the NIST framework, while "Respond" and "Recover" functions are notably underexplored. This distribution could reflect a focus on immediate and detectable benefits of AI in SOC operations, such as threat detection, over the more complex and less direct applications in response and recovery phases. The implications of this are profound, suggesting a potential vulnerability in SOCs that are not fully leveraging AI in all aspects of cybersecurity operations. Future research should address these gaps by exploring AI's role in the "Respond" and "Recover" phases; crucial for a holistic security strategy. The limited attention to the 'Recover' function, in particular, may stem from its inherently process-driven and often post-incident nature, combined with the lack of benchmark datasets and available real-time or real-world data to train and evaluate AI models. Moreover, recovery activities such as system restoration, impact assessment, and policy updates tend to rely more heavily on organisational policies and manual procedures, making them less amenable to current AI capabilities. These factors could help explain the research imbalance and highlight the need for novel approaches that adapt AI techniques to support recovery workflows. Additionally, the predominance of certain AI tools in the "Detect" function suggests a potential over-reliance that might overshadow necessary advancements in other critical areas of SOC operations.

We have also identified a diverse array of motivational factors driving the development of AI tools for SOCs. Key among these motivations is the imperative to enhance threat detection and

response capabilities. AI tools are being developed to increase the accuracy, speed, and efficiency of detecting and responding to cyber threats. Innovations in AI are helping to automate and streamline SOC workflows, significantly reducing response times and false positives. In addition, the emphasis on reducing the cognitive burden on analysts through automation alleviates human factors, which are often the bottleneck in timely threat detection and response. These motivational drivers highlight the broader implications of AI integration in SOCs, suggesting a paradigm shift toward more resilient, responsive, and intelligent cybersecurity infrastructures that can anticipate and counteract emerging threats more effectively.

As we extend our contributions beyond identification, we offer an overview of detailed discussions on algorithms, datasets, and the availability of open-source tools and tools with explainable features.

The analysis around the adoption and proposal of open-source tools reveals a significant gap in the current literature. Promoting open-source projects can foster innovation and collaboration, crucial for advancing technology and developing community-driven solutions. On the other hand, the limited focus on open-source tools may reflect a hesitance due to security concerns or a lack of robust community support for developing and maintaining such tools, which is crucial for their sustained utility in high-stakes environments like SOCs. Enhancing the robustness and security of open-source AI tools could address concerns about their adoption in sensitive environments. To support open-source development, future efforts could focus on creating dedicated funding schemes, fostering academic-industry partnerships that prioritise open licensing, and establishing incentive structures (e.g., recognition or citation systems) that reward the contribution and long-term maintenance of open-source SOC tools. These measures would help reduce institutional barriers and make open-source solutions more viable and trusted within operational security contexts.

The frequent use of specific AI algorithms, such as random forests and support vector machines, suggests a potential under-exploitation of newer or less conventional algorithms that might offer improved performance or better address specific types of cyber threats.

Another point of discussion is the difficulty in getting comprehensive, publicly available datasets for SOC applications. Recurrent use of specific datasets such as NSL-KDD and CICIDS2017 is undoubtedly beneficial in the development and benchmarking of AI tools. Yet, the challenge remains in the form of diversity and realism of the dataset, which are necessary to truly validate the efficacy of AI tools under varied and realistic conditions. Relying on proprietary datasets limits access and reduces the generalisability of findings. Diversifying the datasets used for training and testing those tools can significantly improve their applicability and performance across different scenarios. We also call for a concerted effort to develop and share more open datasets that reflect the real-world complexity.

While there is a growing acknowledgment of the importance of explainability in AI tools for SOCs, the actual integration of explainable AI methodologies is not widespread. This gap underscores a crucial area for future research, particularly in developing tools that are not only effective but also transparent and understandable by human operators in SOC environments. Nonetheless, increasing the integration of explainable AI practices will not only make AI tools more user-friendly, but will also enhance their trustworthiness and acceptance among SOC personnel.

Finally, the identified limitations and challenges underscore the need for innovation and collaboration across domains such as computer science, data science, AI, legal and ethical frameworks, human-computer interaction, and business management. This multidisciplinary approach is essential for developing robust, efficient, and user-friendly cybersecurity solutions that are adaptable to the evolving threat landscape.

In conclusion, the future of AI tool integration into SOC operations should focus on several key areas. While its influence continues to grow, factors such as integration complexity, data availability

and incomplete spectrum of response and recovery solutions impact its effectiveness. This study provides a structured evaluation of AI's role in SOCs, offering insights into its current applications, methodology and limitations, and laying the foundation for a clearer understanding of its power on cybersecurity operations.

### 4.2 Limitations of Our Study

Despite the detailed methodology applied in this SLR, several limitations must be acknowledged. The search strategy used in this study was designed to be comprehensive, using a structured set of keywords in multiple academic databases. However, the focus on keywords like "SOC" may have inadvertently excluded relevant studies that do not explicitly use this terminology. In academic contexts, SOC-related tools and AI applications might be discussed under different terms, with academia potentially using different nomenclature compared with business or industry settings where these terms are more common. This limitation could result in an incomplete capture of the full spectrum of AI tools applicable to SOC environments.

Additionally, this article is an SLR and does not include empirical validation of the AI tools discussed. The findings and conclusions are based on the reported results of the reviewed studies, and as such, the practical effectiveness and efficiency of these AI tools in real-world SOC environments remain largely theoretical. Future research should aim at empiricallying test these tools in operational settings to validate their performance and applicability.

Moreover, the quality of the studies included in the review varies significantly, which could affect the reliability of the synthesised findings. Some studies may have methodological weaknesses, such as small sample sizes, limited datasets, or insufficient validation of AI models. While the review attempted to assess and account for these factors, variability in study quality remains a potential source of bias in general conclusions.

Another limitation stems from the decision to restrict the qualitative synthesis for RQ2 and RQ7 to studies published in the top 10% of venues. While this approach helped ensure a focus on high-quality, peer-reviewed research and made the analysis manageable, it may have introduced bias. As a result, innovative contributions from smaller venues might have been overlooked. Future reviews could expand the scope to include a broader range of publications to capture a more diverse set of perspectives and early-stage innovations.

Lastly, the review covers studies published up to December 2023, which may limit its ability to capture the very latest developments in AI technologies for SOC environments. Given the rapid pace of innovation in AI and cybersecurity, new tools, methodologies, and applications may have emerged since the cut-off date, which is not reflected in this review. This temporal limitation means that the findings might not fully represent the latest state of the art in AI for SOCs.

These limitations suggest that while the review provides a comprehensive overview of AI tools in SOC environments, there is a need for ongoing research and empirical validation to address these gaps and ensure that the findings remain relevant as the field continues to evolve.

## 5 Related Work

Several literature reviews have been conducted to provide insight into the state-of-the-art, focusing on various aspects such as AI integration, challenges, and methodologies. These studies are summarised in Table 10, highlighting their purpose, scope, and contributions.

Studies by Vielberth et al. [209] and Kaur et al. [96] explored broad applications and challenges of AI in SOCs. In contrast, Agyepong et al. [7] and Yang et al. [225] focused specifically on aspects such as analyst performance and intrusion detection systems, respectively. The works of Ünal et al. [203] discussed enhancements to SIEM tools, and Shahjee et al. [188] examined the integration of NOCs with SOCs. Lastly, Islam et al. [90] addressed security orchestration, and Ainslie et al. [9]

Table 10. Comparison with Existing Surveys

| Survey | Purpose | Type | Data sources | #Papers | Period | AI focus | Explainability focus | Contributions |
|---|---|---|---|---|---|---|---|---|
| [209] | state-of-the-art in SOCs, common baseline for SOC research, challenges and gaps in the literature | SLR | IEEE Xplore, ACM Digital Library, SpingerLink, EBSCO Host, Willey ONline Library, Web of Science, Dimensions | 158 | Jan 1990 to June 2020 | Medium | Medium | SOC definitions and SOC building blocks, challenges and gaps in AI integration |
| [96] | state-of-the-art research in AI applications for cybersecurity, identify specific use cases, trends | SLR | Scopus | 236 | Nov 2021 to Feb 2022 | High | Medium | taxonomy, research gaps, future research directions |
| [7] | challenges faced by SOC analysts, their performance metrics | SLR | Scopus, IEEE Xplore, ACM, ScienceDirect, Google Scholar, Google | 15 | 2008-2018 | Medium | Low | future research directions, key themes in literature |
| [225] | review on intrusion detection systems, focusing on various methodologies, datasets, and the current state of research across different network environments | SLR | Scopus, Google Scholar, WoS | 119 | – | Medium | Medium | first SLR for network security ID, 52 cybersecurity datasets categorised by their attributes, research gaps, future research directions |
| [203] | state-of-the-art in enhancement of SIEM tools to evaluate the current state of CSA, predict upcoming challenges in maintaining awareness | SLR | – | – | – | Medium | Medium | holistic view of Cyber Situation Awareness, categorisation of solutions related to SIEM tools |
| [188] | state-of-the-art architecture for integrated NOCs and SOCs, challenges and requirements for effective integration | SLR | – | 75 | – | Medium | Low | systematic architecture for integrated NOC and SOC, roadmap for future research |
| [90] | current state of security orchestration, focusing on the integration of AI in SOCs, gaps in effectiveness of security tools | MLR | Journal of Computer Security, ACM SIGSAC Conference on Computer and Communications Security, USENIX Security Symposium, Proceedings of RSA conferences, IEEE Xplore, ACM, Scopus, Annual Computer Security Applications Conference, IEEE Security and Privacy, Google search engine, Websites | 95 | Jan 2007 to Jul 2017 | High | Medium | gaps in literature regarding AI integration in SOCs, challenges of real-time threat detection and automation, future research |
| [9] | state-of-the-art CTI, CTI integration with AI in SOCs | SLR | Google Scholar | 169 | 2011 onwards | Medium | Medium | research gaps, research agenda to enhance CTI effectiveness |
| Our study | state-of-the-art in AI for SOCs, searching the extent of explainability models | SLR | ACM, IEEE Xplore, SpringerLink, ScienceDirect, Scopus, Web of Science, and Wiley Online Library | 157 | 2017 onwards | High | High | Limitations and Future Directions, Motivations, Holistic overview of AI proposed tools for SOCs (algorithms, datasets, open-source licence), Identification of explainable tools |

considered **cyber threat intelligence** (**CTI**). Whilst these studies identified significant gaps in AI integration and CTI effectiveness, they provided a medium focus on AI and its explainability.

Our SLR builds upon these prior studies, which, while insightful, have often offered limited discussion on the role of AI's explainability. This oversight highlights a significant gap as SOCs handle increasingly complex security threats where explainability is not just an added feature, but a necessity.

We reviewed papers similar in scope to the extensive surveys by Kaur et al. [96] and Ainslie et al. [9], yet our focus on explainability alongside AI integration provides a unique contribution that is critical in the current AI-driven security environment.

Additionally, our survey places significant emphasis on the specific algorithms and datasets used in these applications, a focus that is vital because the choice of algorithm and the quality of the datasets directly influence the effectiveness and reliability of AI solutions.

Furthermore, our analysis goes beyond mere identification and categorisation. We explore the motivations behind the proposal of AI methods for SOCs as well as the limitations and challenges of those methods, aiming to enhance both theoretical and practical understandings in the field.

Finally, recent reviews by Radanliev [167, 168] explore broad cybersecurity topics, but do not cover AI use in SOCs or apply a NIST CSF lens. Our study fills this gap with a focused review of AI tools in SOC operations.

## 6 Conclusion

With this SLR, our contribution is twofold: Firstly, we provide a comprehensive overview of the current state of AI tools in SOCs, identifying key technological and methodological limitations. Secondly, we propose a research agenda that emphasises the development of new AI methodologies that can be seamlessly integrated into existing SOC infrastructures, enhancing both their effectiveness and their trustworthiness.

Furthermore, our research does not simply catalogue existing tools and methodologies; it provides a critical evaluation of these technologies, highlighting their motivations, practical applications, challenges in real-world SOC environments, and the extent to which these models are explainable. In doing so, we address the crucial need for operational transparency in high-stakes environments where decisions must be not only effective, but also interpretable by human operators. We also include the need for better dataset availability, improved algorithmic diversity, and the integration of AI-driven response and recovery mechanisms.

Ultimately, our findings reveal that while AI is transforming SOC operations, its application remains uneven across different security functions. AI-driven solutions are widely proposed for detection, yet there are clear gaps in their implementation for response and recovery. Moreover, challenges related to integration, scalability, data availability, and model explainability continue to hinder their full potential. By mapping the landscape of AI tools for SOCs, this study aims to pave the way for future research that can enhance the functionality, transparency, and reliability of AI applications in SOC environments, ensuring that they meet the evolving challenges of cybersecurity with efficacy and ethical responsibility.

## Acknowledgments

We acknowledge the use of ChatGPT (3.5-turbo, 4o and 4) in polishing the paper.

## References

[1] 2021. The Power of Splunk. (Aug. 2021). Retrieved from https://www.splunk.com/en_us/blog/learn/soc-security-operation-center.html

[2] 2024. A Realistic Cyber Defense Dataset (CSE-CIC-IDS2018)—Registry of Open Data on AWS. (Dec. 2024). Retrieved from https://registry.opendata.aws/cse-cic-ids2018 [Online; accessed 28. dec. 2024].

[3] 2024. core.edu.au - CORE Rankings Portal. (Nov. 2024). Retrieved from https://www.core.edu.au/conference-portal [Online; accessed 13. nov.. 2024].
[4] 2024. Cybersecurity Framework | NIST. (Dec. 2024). Retrieved from https://www.nist.gov/cyberframework [Online; accessed 31. dec. 2024].
[5] 2025. What Is a Security Operations Center | Cybersecurity | CompTIA. (Jan. 2025). Retrieved from https://www.comptia.org/content/articles/what-is-a-security-operations-center#:~:text=Simply%20put%2C%20a%20security%20operations,where%20SOC%20analysts%20work%20together.
[6] Jesse Ables, Thomas Kirby, William Anderson, Sudip Mittal, Shahram Rahimi, Ioana Banicescu, and Maria Seale. 2022. Creating an explainable intrusion detection system using self organizing maps. In *2022 IEEE Symposium Series on Computational Intelligence (SSCI)*. IEEE, 404–412.
[7] Enoch Agyepong, Yulia Cherdantseva, Philipp Reinecke, and Pete Burnap. 2020. Challenges and performance metrics for security operations center analysts: A systematic review. *Journal of Cyber Security Technology* 4, 3 (2020), 125–152.
[8] Ashish Ahire and Mustafa Abdallah. 2023. Reinforcement learning for enhancing human security resource allocation in protecting assets with heterogeneous losses. *Proceedings of the 2023 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems*, 9–15. DOI: https://doi.org/10.1145/3579988.3585057
[9] Scott Ainslie, Dean Thompson, Sean Maynard, and Atif Ahmad. 2023. Cyber-threat intelligence for security decision-making: A review and research agenda for practice. *Computers & Security* 132 (2023), 103352.
[10] Georgios Aivatoglou, Mike Anastasiadis, Georgios Spanos, Antonis Voulgaridis, Konstantinos Votis, Dimitrios Tzovaras, and Lefteris Angelis. 2022. A RAkEL-based methodology to estimate software vulnerability characteristics & score-an application to EU project ECHO. *Multimedia Tools and Applications* 81, 7 (2022), 9459–9479.
[11] Bushra A AlAhmadi and Ivan Martinovic. 2018. MalClassifier: Malware family classification using network flow sequence behaviour. In *2018 APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, 1–13.
[12] Moutaz Alazab, Ruba Abu Khurma, Albara Awajan, and David Camacho. 2022. A new intrusion detection system based on moth–flame optimizer algorithm. *Expert Systems with Applications* 210 (2022), 118439.
[13] Cristina Alcaraz and Javier Lopez. 2022. Digital twin: A comprehensive survey of security threats. *IEEE Communications Surveys & Tutorials* 24, 3 (2022), 1475–1503.
[14] Rubayyi Alghamdi and Martine Bellaiche. 2023. An ensemble deep learning based IDS for IoT using lambda architecture. *Cybersecurity* 6, 1 (2023), 5.
[15] Yusuf S AlMahmeed and Alauddin Y Al-Omay. 2022. Zero-day attack solutions using threat hunting intelligence: Extensive survey. In *2022 International Conference on Data Analytics for Business and Industry (ICDABI)*. IEEE, 309–314.
[16] Mohammed Almukaynizi, Ericsson Marin, Eric Nunes, Paulo Shakarian, Gerardo I Simari, Dipsy Kapoor, and Timothy Siedlecki. 2018. Darkmention: A deployed system to predict enterprise-targeted external cyberattacks. In *2018 IEEE International Conference on Intelligence and Security Informatics (ISI)*. IEEE, 31–36.
[17] Mohammed A Althamir, Jawhara Z Boodai, and MM Hafizur Rahman. 2023. A mini literature review on challenges and opportunity in threat intelligence. In *2023 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*. IEEE, 558–563.
[18] Fernando Alves, Aurélien Bettini, Pedro M. Ferreira, and Alysson Bessani. 2021. Processing tweets for cybersecurity threat awareness. *Information Systems* 95 (2021), 101586.
[19] Fernando Alves, Pedro Miguel Ferreira, and Alysson Bessani. 2019. Design of a classification model for a twitter-based streaming threat monitor. In *2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*. IEEE, 9–14.
[20] Tudor Andreica, Christian-Daniel Curiac, Camil Jichici, and Bogdan Groza. 2022. Android head units vs. In-vehicle ECUs: Performance assessment for deploying in-vehicle intrusion detection systems for the CAN bus. *IEEE Access* 10 (2022), 95161–95178.
[21] Mahmoud Atari and Amjed Al-Mousa. 2022. A machine-learning based approach for detecting phishing urls. In *2022 International Conference on Intelligent Data Science Technologies and Applications (IDSTA)*. IEEE, 82–88.
[22] Shahriar Badsha, Iman Vakilinia, and Shamik Sengupta. 2019. Privacy preserving cyber threat information sharing and learning for cyber defense. In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, 0708–0714.
[23] Tao Ban, Ndichu Samuel, Takeshi Takahashi, and Daisuke Inoue. 2021. Combat security alert fatigue with AI-assisted techniques. *Cyber Security Experimentation and Test Workshop*, 9–16. DOI: https://doi.org/10.1145/3474718.3474723
[24] Muthu M Baskaran, Thomas Henretty, James Ezick, Richard Lethin, and David Bruns-Smith. 2019. Enhancing network visibility and security through tensor analysis. *Future Generation Computer Systems* 96 (2019), 207–215.
[25] Piotr Bienias, Grzegorz Kołaczek, and Arkadiusz Warzyński. 2019. Architecture of anomaly detection module for the security operations center. In *2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*. IEEE, 126–131.

[26] Abdelwahab Boualouache and Thomas Engel. 2022. Federated learning-based inter-slice attack detection for 5G-V2X sliced networks. In *2022 IEEE 96th Vehicular Technology Conference (VTC2022-Fall)*. IEEE, 1–6.
[27] Joel Brogan, Nell Barber, David Cornett, and David Bolme. 2023. VDiSC: An open source framework for distributed smart city vision and biometric surveillance networks. In *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision*. 148–154.
[28] Pete Burnap, Richard French, Frederick Turner, and Kevin Jones. 2018. Malware classification using self organising feature maps and machine activity data. *Computers & Security* 73 (2018), 399–410.
[29] Alessio Buscemi, Manasvi Ponaka, Mahdi Fotouhi, Florian Jomrich, Christian Koebel, and Thomas Engel. 2023. An intrusion detection system against rogue master attacks on gptp. In *2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring)*. IEEE, 1–7.
[30] E. C.-Council. 2024. What security operations center SOC is | fundamentals of SOC cyber security | EC-council. *Cybersecurity Exchange* (March 2024). Retrieved from https://www.eccouncil.org/cybersecurity-exchange/security-operation-center/what-is-soc-security-operations-center/#:~:text=A%20Security%20Operations%20Center%20(SOC,security%20systems%20in%20real%20time.
[31] Albert Calvo, Santiago Escuder, Josep Escrig, Marta Arias, Nil Ortiz, and Jordi Guijarro. 2023. A data-driven approach for risk exposure analysis in enterprise security. In *2023 IEEE 10th International Conference on Data Science and Advanced Analytics (DSAA)*. IEEE, 1–9.
[32] Hasan Cam. 2019. Model-guided infection prediction and active defense using context-specific cybersecurity observations. In *MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM)*. IEEE, 1–6.
[33] Yidong Chai, Yonghang Zhou, Weifeng Li, and Yuanchun Jiang. 2021. An explainable multi-modal hierarchical attention model for developing phishing threat intelligence. *IEEE Transactions on Dependable and Secure Computing* 19, 2 (2021), 790–803.
[34] Haipeng Chen, Andrew Duncklee, Sushil Jajodia, Rui Liu, Sean Mcnamara, and V. S. Subrahmanian. 2022. PCAM: A data-driven probabilistic cyber-alert management framework. *ACM Trans. Internet Technol.* 22, 3 (2022), 1–24. https://doi.org/10.1145/3511101
[35] Yang Chen, Saba Al-Rubaye, Antonios Tsourdos, Lawrence Baker, and Colin Gillingham. 2023. Differentially-private federated intrusion detection via knowledge distillation in third-party IoT systems of smart airports. In *ICC 2023-IEEE International Conference on Communications*. IEEE, 603–608.
[36] Andrew Chi, Blake Anderson, and Michael K Reiter. 2023. Prioritizing remediation of enterprise hosts by malware execution risk. In *Proceedings of the 39th Annual Computer Security Applications Conference*. 550–564.
[37] Daiki Chiba, Mitsuaki Akiyama, Yuto Otsuki, Hiroki Hada, Takeshi Yagi, Tobias Fiebig, and Michel Van Eeten. 2022. Domainprio: Prioritizing domain name investigations to improve SOC efficiency. *IEEE Access* 10 (2022), 34352–34368.
[38] Ikje Choi, Jun Lee, Taewoong Kwon, Kyuil Kim, Yoonsu Choi, and Jungsuk Song. 2021. An easy-to-use framework to build and operate ai-based intrusion detection for in-situ monitoring. In *2021 16th Asia Joint Conference on Information Security (AsiaJCIS)*. IEEE, 1–8.
[39] Marcello Cinque, Christian Esposito, and Antonio Pecchia. 2019. Security log analysis in critical industrial systems exploiting game theoretic feature selection and evidence combination. *IEEE Transactions on Industrial Informatics* 16, 6 (2019), 3871–3880.
[40] Christopher Collins, Denis Dennehy, Kieran Conboy, and Patrick Mikalef. 2021. Artificial intelligence in information systems research: A systematic literature review and research agenda. *International Journal of Information Management* 60 (2021), 102383.
[41] Prerit Datta, Natalie Lodinger, Akbar Siami Namin, and Keith S Jones. 2020. Predicting consequences of cyber-attacks. In *2020 IEEE International Conference on Big Data (Big Data)*. IEEE, 2073–2078.
[42] Noemí DeCastro-García, Ángel L Muñoz Castañeda, and Mario Fernández-Rodríguez. 2020. Machine learning for automatic assignment of the severity of cybersecurity events. *Computational and Mathematical Methods* 2, 1 (2020), e1072.
[43] Nathan Deguara, Junaid Arshad, Anum Paracha, and Muhammad Ajmal Azad. 2022. Threat miner-a text analysis engine for threat identification using dark web data. In *2022 IEEE International Conference on Big Data (Big Data)*. IEEE, 3043–3052.
[44] Konstantinos Demertzis, Nikos Tziritas, Panayiotis Kikiras, Salvador Llopis Sanchez, and Lazaros Iliadis. 2019. The next generation cognitive security operations center: Adaptive analytic lambda architecture for efficient defense against adversarial attacks. *Big Data and Cognitive Computing* 3, 1 (2019), 6.
[45] Devo. 2023. New SOC performance report: Security analysts are overworked and under resourced | devo blog. *Devo* (July 2023). Retrieved from https://www.devo.com/blog/new-soc-performance-report-security-analysts-are-overworked-and-under-resourced
[46] Nuno Dionísio, Fernando Alves, Pedro M. Ferreira, and Alysson Bessani. 2019. Cyberthreat detection from twitter using deep neural networks. In *2019 International Joint Conference on Neural Networks (IJCNN)*. IEEE, 1–8.

[47] Nuno Dionísio, Fernando Alves, Pedro M. Ferreira, and Alysson Bessani. 2020. Towards end-to-end cyberthreat detection from Twitter using multi-task learning. In *2020 International Joint Conference on Neural Networks (IJCNN)*. IEEE, 1–8.

[48] Michael Donevski and Tanveer Zia. 2018. A survey of anomaly and automation from a cybersecurity perspective. In *2018 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 1–6.

[49] Cong Dong, YuFan Chen, YunJian Zhang, Bo Jiang, DongXu Han, and BaoXu Liu. 2019. An approach for scale suspicious network events detection. In *2019 IEEE International Conference on Big Data (Big Data)*. IEEE, 5854–5863.

[50] Arthur Drichel, Nils Faerber, and Ulrike Meyer. 2021. First step towards explainable dga multiclass classification. In *Proceedings of the 16th International Conference on Availability, Reliability and Security*. 1–13.

[51] Arthur Drichel and Ulrike Meyer. 2023. False sense of security: Leveraging XAI to analyze the reasoning and true performance of context-less DGA classifiers. In *Proceedings of the 26th International Symposium on Research in Attacks, Intrusions and Defenses*. 330–345.

[52] Benjamin Drozdenko and Makia Powell. 2022. Utilizing deep learning techniques to detect zero day exploits in network traffic flows. In *2022 IEEE 13th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. IEEE, 0163–0172.

[53] Jiayi Duan, Ziheng Zeng, Alina Oprea, and Shobha Vasudevan. 2018. Automated generation and selection of interpretable features for enterprise security. In *2018 IEEE International Conference on Big Data (Big Data)*. IEEE, 1258–1265.

[54] Phan The Duy, Nghi Hoang Khoa, Hien Do Hoang, Van-Hau Pham, et al. 2023. Investigating on the robustness of flow-based intrusion detection system against adversarial samples using generative adversarial networks. *Journal of Information Security and Applications* 74 (2023), 103472.

[55] Phan The Duy, Nguyen Huu Quyen, Nghi Hoang Khoa, Tuan-Dung Tran, and Van-Hau Pham. 2023. FedChain-hunter: A reliable and privacy-preserving aggregation for federated threat hunting framework in SDN-based IIoT. *Internet of Things* 24 (2023), 100966.

[56] Ogerta Elezaj, Sule Yildirim Yayilgan, Mohamed Abomhara, Prosper Yeng, and Javed Ahmed. 2019. Data-driven intrusion detection system for small and medium enterprises. In *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*. IEEE, 1–7.

[57] Aviad Elitzur, Rami Puzis, and Polina Zilberman. 2019. Attack hypothesis generation. In *2019 European Intelligence and Security Informatics Conference (EISIC)*. IEEE, 40–47.

[58] Hafiz M. Farooq and Naif M. Otaibi. 2018. Optimal machine learning algorithms for cyber threat detection. In *2018 UKSim-AMSS 20th International Conference on Computer Modelling and Simulation (UKSim)*. 32–37. DOI: https://doi.org/10.1109/UKSim.2018.00018

[59] Hafiz M Farooq and Naif M Otaibi. 2018. Optimal machine learning algorithms for cyber threat detection. In *2018 UKSim-AMSS 20th International Conference on Computer Modelling and Simulation (UKSim)*. IEEE, 32–37.

[60] Katheryn A. Farris, Ankit Shah, George Cybenko, Rajesh Ganesan, and Sushil Jajodia. 2018. VULCON: A system for vulnerability prioritization, mitigation, and management. *ACM Trans. Priv. Secur.* 21, 4 (2018), 1–28. https://doi.org/10.1145/3196884

[61] Juan Ramón Feijoo-Martínez, Alicia Guerrero-Curieses, Francisco Gimeno-Blanes, Mario Castro-Fernández, and José Luis Rojo-Álvarez. 2023. Cybersecurity alert prioritization in a critical high power grid with latent spaces. *IEEE Access* 11 (2023), 23754–23770.

[62] Tiago Fernandes, Luis Dias, and Miguel Correia. 2020. C2bid: Cluster change-based intrusion detection. In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, 310–319.

[63] Mohamed Amine Ferrag, Merouane Debbah, and Muna Al-Hawawreh. 2023. Generative ai for cyber threat-hunting in 6g-enabled iot networks. In *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*. IEEE, 16–25.

[64] James B Fraley and James Cannady. 2017. The promise of machine learning in cybersecurity. In *SoutheastCon 2017*. IEEE, 1–6.

[65] Hamdi Friji, Ioannis Mavromatis, Adrian Sanchez-Mompo, Pietro Carnelli, Alexis Olivereau, and Aftab Khan. 2023. Multi-stage attack detection and prediction using graph neural networks: An IoT feasibility study. In *2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, 620–627.

[66] Chuanpu Fu, Qi Li, Ke Xu, and Jianping Wu. 2023. Point cloud analysis for ML-based malicious traffic detection: Reducing majorities of false positive alarms. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*. 1005–1019.

[67] Koji Fujita, Toshiki Shibahara, Daiki Chiba, Mitsuaki Akiyama, and Masato Uchida. 2022. Objection!: Identifying misclassified malicious activities with XAI. In *ICC 2022-IEEE International Conference on Communications*. IEEE, 2065–2070.

[68] Luigi Gallo, Alessandro Maiello, Alessio Botta, and Giorgio Ventre. 2021. 2 Years in the anti-phishing group of a large company. *Computers & Security* 105 (2021), 102259.
[69] Yun Gao, Hirokazu Hasegawa, Yukiko Yamaguchi, and Hajime Shimada. 2021. Malware detection using gradient boosting decision trees with customized log loss function. In *2021 International Conference on Information Networking (ICOIN)*. IEEE, 273–278.
[70] Yun Gao, Hirokazu Hasegawa, Yukiko Yamaguchi, and Hajime Shimada. 2022. Malware detection by control-flow graph level representation learning with graph isomorphism network. *IEEE Access* 10 (2022), 111830–111841.
[71] Yun Gao, Hirokazu Hasegawa, Yukiko Yamaguchi, and Hajime Shimada. 2022. Malware detection using LightGBM with a custom logistic loss function. *IEEE Access* 10 (2022), 47792–47804.
[72] Sebastian Garcia, Agustin Parmisano, and Maria Jose Erquiaga. 2020. IoT-23: A labeled dataset with malicious and benign IoT network traffic. (Jan. 2020). DOI: https://doi.org/10.5281/zenodo.4743746
[73] Pedro García-Teodoro, José Antonio Gómez-Hernández, and Alberto Abellán-Galera. 2022. Multi-labeling of complex, multi-behavioral malware samples. *Computers & Security* 121 (2022), 102845.
[74] Pierre-Francois Gimenez, Jonathan Roux, Eric Alata, Guillaume Auriol, Mohamed Kaaniche, and Vincent Nicomette. 2021. RIDS: Radio intrusion detection and diagnosis system for wireless communications in smart environment. *ACM Trans. Cyber-Phys. Syst.* 5, 3 (2021), 1–1. https://doi.org/10.1145/3441458
[75] John R. Goodall, Eric D. Ragan, Chad A. Steed, Joel W. Reed, G. David Richardson, Kelly MT Huffer, Robert A. Bridges, and Jason A. Laska. 2018. Situ: Identifying and explaining suspicious behavior in networks. *IEEE Transactions on Visualization and Computer Graphics* 25, 1 (2018), 204–214.
[76] Robert Gove. 2021. Automatic narrative summarization for visualizing cyber security logs and incident reports. *IEEE Transactions on Visualization and Computer Graphics* 28, 1 (2021), 1182–1190.
[77] Roman Graf and Ross King. 2018. Neural network and blockchain based technique for cyber threat intelligence and situational awareness. In *2018 10th International Conference on Cyber Conflict (CyCon)*. IEEE, 409–426.
[78] Michael Guarino, Pablo Rivas, and Casimer DeCusatis. 2020. Towards adversarially robust DDoS-attack classification. In *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. IEEE, 0285–0291.
[79] Alejandro Guerra-Manzanares and Hayretdin Bahsi. 2023. On the application of active learning for efficient and effective IoT botnet detection. *Future Generation Computer Systems* 141 (2023), 40–53.
[80] Lucas CB Guimarães, Gabriel Antonio F. Rebello, Felipe S. Fernandes, Gustavo F. Camilo, Lucas Airam C. de Souza, Danyel C. dos Santos, Luiz Gustavo CM de Oliveira, and Otto Carlos MB Duarte. 2020. TeMIA-NT: ThrEat monitoring and intelligent data analytics of network traffic. In *2020 4th Conference on Cloud and Internet of Things (CIoT)*. IEEE, 9–16.
[81] Nitika Gupta, Issa Traore, and Paulo Magella Faria de Quinan. 2019. Automated event prioritization for security operation center using deep learning. In *2019 IEEE International Conference on Big Data (Big Data)*. IEEE, 5864–5872.
[82] Chansu Han, Jun-ichi Takeuchi, Takeshi Takahashi, and Daisuke Inoue. 2022. Dark-TRACER: Early detection framework for malware activity based on anomalous spatiotemporal patterns. *IEEE Access* 10 (2022), 13038–13058.
[83] Ryan Heartfield and George Loukas. 2018. Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. *Computers & Security* 76 (2018), 101–127.
[84] Angus FM Huang, Yang Chi-Wei, Hsiao-Chi Tai, Yang Chuan, Jay JC Huang, and Yu-Han Liao. 2019. Suspicious network event recognition using modified stacking ensemble machine learning. In *2019 IEEE International Conference on Big Data (Big Data)*. IEEE, 5873–5880.
[85] Lanxiao Huang, Tyler Cody, Christopher Redino, Abdul Rahman, Akshay Kakkar, Deepak Kushwaha, Cheng Wang, Ryan Clark, Daniel Radke, Peter Beling, et al. 2022. Exposing surveillance detection routes via reinforcement learning, attack graphs, and cyber terrain. In *2022 21st IEEE International Conference on Machine Learning and Applications (ICMLA)*. IEEE, 1350–1357.
[86] Kieran Hughes, Kieran McLaughlin, and Sakir Sezer. 2022. A model-free approach to intrusion response systems. *Journal of Information Security and Applications* 66 (2022), 103150.
[87] IEEE. IEEE Big Data 2019 Big Data Cup. Retrieved from https://rapid.cis.unimelb.edu.au/BigDataChallenge/Tasks.html. (n.d.). [Accessed 28-12-2024].
[88] Masahiro Ishii, Kento Mori, Ryoichi Kuwana, and Satoshi Matsuura. 2022. Multi-label classification of cybersecurity text with distant supervision. *Proceedings of the 17th International Conference on Availability, Reliability and Security*. DOI: https://doi.org/10.1145/3538969.3543795
[89] Chadni Islam, M. Ali Babar, Roland Croft, and Helge Janicke. 2022. SmartValidator: A framework for automatic identification and classification of cyber threat data. *Journal of Network and Computer Applications* 202 (2022), 103370.
[90] Chadni Islam, Muhammad Ali Babar, and Surya Nepal. 2019. A multi-vocal review of security orchestration. *ACM Computing Surveys (CSUR)* 52, 2 (2019), 1–45.

[91] Danish Javeed, Tianhan Gao, Muhammad Shahid Saeed, and Muhammad Taimoor Khan. 2023. FOG-empowered augmented-intelligence-based proactive defensive mechanism for IoT-enabled smart industries. *IEEE Internet of Things Journal* 10, 21 (2023), 18599–18608.
[92] Yuning Jiang and Yacine Atif. 2021. A selective ensemble model for cognitive cybersecurity analysis. *Journal of Network and Computer Applications* 193 (2021), 103210.
[93] JupiterOne. 2023. State of Cyber assets report. (2023). Retrieved from https://info.jupiterone.com/hubfs/SCAR%202023/jupiterone_2023-state-of-cyber-assets-report_scar.pdf
[94] Jiaqi Kang, Huiran Yang, Yan Zhang, Yueyue Dai, Mengqi Zhan, and Weiping Wang. 2022. Actdetector: A sequence-based framework for network attack activity detection. In *2022 IEEE Symposium on Computers and Communications (ISCC)*. IEEE, 1–7.
[95] Leyli Karaçay, Erkay Savaş, and Halit Alptekin. 2020. Intrusion detection over encrypted network data. *Comput. J.* 63, 1 (2020), 604–619.
[96] Ramanpreet Kaur, Dušan Gabrijelčič, and Tomaž Klobučar. 2023. Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion* 97 (2023), 101804.
[97] Varol O Kayhan, Manish Agrawal, and Shivendu Shivendu. 2023. Cyber threat detection: Unsupervised hunting of anomalous commands (UHAC). *Decision Support Systems* 168 (2023), 113928.
[98] Ofir Erets Kdosha, Gilad Rosenthal, Kobi Cohen, Alon Freund, Avishay Bartik, and Aviv Ron. 2020. REMaDD: Resource-efficient malicious domains detector in large-scale networks. *IEEE Access* 8 (2020), 66327–66337.
[99] Hakan Kekül, Burhan Ergen, and Halil Arslan. 2021. A multiclass hybrid approach to estimating software vulnerability vectors and severity score. *Journal of Information Security and Applications* 63 (2021), 103028.
[100] Clifford Kemp, Chad Calvert, and Taghi M Khoshgoftaar. 2021. Detecting slow application-layer DoS attacks with PCA. In *2021 IEEE 22nd International Conference on Information Reuse and Integration for Data Science (IRI)*. IEEE, 176–183.
[101] Egon Kidmose, Matija Stevanovic, Søren Brandbyge, and Jens M Pedersen. 2020. Featureless discovery of correlated and false intrusion alerts. *IEEE Access* 8 (2020), 108748–108765.
[102] Aechan Kim, Mohyun Park, and Dong Hoon Lee. 2020. AI-IDS: Application of deep learning to real-time web intrusion detection. *IEEE Access* 8 (2020), 70245–70261.
[103] Danny Kim, Daniel Mirsky, Amir Majlesi-Kupaei, and Rajeev Barua. 2018. A hybrid static tool to increase the usability and scalability of dynamic detection of malware. In *2018 13th International Conference on Malicious and Unwanted Software (MALWARE)*. IEEE, 115–123.
[104] Heejung Kim and Hwankuk Kim. 2022. Comparative experiment on TTP classification with class imbalance using oversampling from CTI dataset. *Security and Communication Networks* 2022, 1 (2022), 5021125.
[105] Hongbi Kim, Yongsoo Lee, Eungyu Lee, and Taejin Lee. 2021. Cost-effective valuable data detection based on the reliability of artificial intelligence. *IEEE Access* 9 (2021), 108959–108974.
[106] Jae-yeol Kim and Hyuk-Yoon Kwon. 2022. Threat classification model for security information event management focusing on model efficiency. *Computers & Security* 120 (2022), 102789.
[107] Satoru Koda, Yusuke Kambara, Takanori Oikawa, Kazuyoshi Furukawa, Yuki Unno, and Masahiko Murakami. 2020. Anomalous IP address detection on traffic logs using novel word embedding. In *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE, 1504–1509.
[108] Yuma Kurogome, Yuto Otsuki, Yuhei Kawakoya, Makoto Iwamura, Syogo Hayashi, Tatsuya Mori, and Koushik Sen. 2019. EIGER: Automated IOC generation for accurate and interpretable endpoint malware detection. In *35th Annual Computer Security Applications Conference*. 687–701.
[109] Masaki Kuwano, Momoka Okuma, Satoshi Okada, and Takuho Mitsunaga. 2022. ATT&CK behavior forecasting based on collaborative filtering and graph databases. In *2022 IEEE International Conference on Computing (ICOCO)*. IEEE, 191–197.
[110] Maxime Lanvin, Pierre-François Gimenez, Yufei Han, Frédéric Majorczyk, Ludovic Mé, and Eric Totel. 2023. Towards understanding alerts raised by unsupervised network intrusion detection systems. In *26th International Symposium on Research in Attacks, Intrusions and Defenses*. 135–150.
[111] Outi–Marja Latvala, Ivo Emanuilov, Tatu Niskanen, Pia Raitio, Jarno Salonen, Diogo Santos, and Katerina Yordanova. 2022. Proof-of-concept for a granular incident management information sharing scheme. In *2022 IEEE World AI IoT Congress (AIIoT)*. 515–520. DOI: https://doi.org/10.1109/AIIoT54504.2022.9817254
[112] Tim Laue, Carsten Kleiner, Kai-Oliver Detken, and Timo Klecker. 2021. A SIEM architecture for multidimensional anomaly detection. In *11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*. IEEE, 136–142.
[113] David Lazar, Kobi Cohen, Alon Freund, Avishay Bartik, and Aviv Ron. 2021. IMDoC: Identification of malicious domain campaigns via DNS and communicating files. *IEEE Access* 9 (2021), 45242–45258.

[114] Jonghoon Lee, Jonghyun Kim, Ikkyun Kim, and Kijun Han. 2019. Cyber threat detection based on artificial neural networks using event profiles. *IEEE Access* 7 (2019), 165607–165626.

[115] Jehyun Lee, Farren Tang, Phyo May Thet, Desmond Yeoh, Mitch Rybczynski, and Dinil Mon Divakaran. 2022. Sierra: Ranking anomalous activities in enterprise networks. In *2022 IEEE 7th European Symposium on Security and Privacy (EuroS&P)*. IEEE, 44–59.

[116] Moemedi Lefoane, Ibrahim Ghafir, Sohag Kabir, and Irfan-Ullah Awan. 2023. Latent dirichlet allocation for the detection of multi-stage attacks. In *2023 24th International Arab Conference on Information Technology (ACIT)*. IEEE, 1–7.

[117] Anying Li and Derek Lin. 2018. Generating interpretable network asset clusters for security analytics. In *2018 IEEE International Conference on Big Data (Big Data)*. IEEE, 2972–2979.

[118] Hao Li, Zhenxiang Chen, Riccardo Spolaor, Qiben Yan, Chuan Zhao, and Bo Yang. 2019. Dart: Detecting unseen malware variants using adaptation regularization transfer learning. In *ICC 2019-2019 IEEE International Conference on Communications (ICC)*. IEEE, 1–6.

[119] Jiacheng Li, Tong Li, Runzi Zhang, Di Wu, Hao Yue, and Zhen Yang. 2023. APM: An attack path-based method for APT attack detection on few-shot learning. In *2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, 10–19.

[120] Xiu-Ru Liang, Huei-Tang Li, Chiung-Ying Huang, Wei-An Chen, Yi-Feng Chen, Zhi-Jia Gao, Meng-Wei Sun, and Hao-Cheng Chia. 2023. Outlier-based anomaly detection in firewall logs. In *2023 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI)*. IEEE, 1–10.

[121] Ivandro O Lopes, Deqing Zou, Ihsan H Abdulqadder, Saeed Akbar, Zhen Li, Francis Ruambo, and Wagner Pereira. 2023. Network intrusion detection based on the temporal convolutional model. *Computers & Security* 135 (2023), 103465.

[122] André Manuel Macedo and João Paulo Magalhães. 2023. Detection of network intrusions using anomaly detection. In *2023 20th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA)*. IEEE, 1–6.

[123] Stefan Machmeier, Maximilian Hoecker, and Vincent Heuveline. 2023. Explainable artificial intelligence for improving a session-based malware traffic classification with deep learning. In *2023 IEEE Symposium Series on Computational Intelligence (SSCI)*. IEEE, 850–855.

[124] Francesco Marchiori, Mauro Conti, and Nino Vincenzo Verde. 2023. Stixnet: A novel and modular solution for extracting all stix objects in cti reports. In *Proceedings of the 18th International Conference on Availability, Reliability and Security*. 1–11.

[125] Dan-Georgian Marculet, Razvan Benchea, and Dragos Teodor Gavrilut. 2019. Methods for training neural networks with zero false positives for malware detection. In *2019 21st International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC)*. 230–236. DOI: https://doi.org/10.1109/SYNASC49474.2019.00039

[126] Renato Marinho and Raimir Holanda. 2023. Automated emerging cyber threat identification and profiling based on natural language processing. *IEEE Access* 11 (2023), 58915–58936.

[127] Cláudio Martins and Ibéria Medeiros. 2022. Generating quality threat intelligence leveraging OSINT and a cyber threat unified taxonomy. *ACM Trans. Priv. Secur.* 25, 3 (2022), 1–39. https://doi.org/10.1145/3530977

[128] Nestor Maslej, Loredana Fattorini, Erik Brynjolfsson, John Etchemendy, Katrina Ligett, Terah Lyons, James Manyika, Helen Ngo, Juan Carlos Niebles, Vanessa Parli, et al. 2023. Artificial intelligence index report 2023. arXiv:2310.03715. Retrieved from https://arxiv.org/abs/2310.03715

[129] Luís Mata, Sinan Wannous, David Duarte, Eva Maia, Pedro Vieira, and Isabel Praça. 2023. On the implementation of a secure and energetically efficient NOC for mobile networks. In *2023 International Conference on Smart Applications, Communications and Networking (SmartNets)*. IEEE, 1–8.

[130] Rui Mei, Han-Bing Yan, Zhi-Hui Han, and Jian-Chun Jiang. 2021. CTScopy: Hunting cyber threats within enterprise via provenance graph-based analysis. In *2021 IEEE 21st International Conference on Software Quality, Reliability and Security (QRS)*. IEEE, 28–39.

[131] Otgonpurev Mendsaikhan, Hirokazu Hasegawa, Yukiko Yamaguchi, and Hajime Shimada. 2019. Identification of cybersecurity specific content using the Doc2Vec language model. In *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, Vol. 1. IEEE, 396–401.

[132] John Mern, Kyle Hatch, Ryan Silva, Cameron Hickert, Tamim Sookoor, and Mykel J. Kochenderfer. 2022. Autonomous attack mitigation for industrial control systems. In *2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*. IEEE, 28–36.

[133] Mamoru Mimura and Hidema Tanaka. 2017. Long-term performance of a generic intrusion detection method using Doc2vec. In *2017 Fifth International Symposium on Computing and Networking (CANDAR)*. IEEE, 456–462.

[134] Andrew Morin and Tyler Moore. 2022. Towards cost-balanced intrusion detection in OT environments. In *2022 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 1–6.

[135] Nour Moustafa and Jill Slay. 2015. UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In *2015 Military Communications and Information Systems Conference (MilCIS)*. 1–6. DOI: https://doi.org/10.1109/MilCIS.2015.7348942

[136] Yohan Muliono, Mohamad Yusof Darus, Chrisando Ryan Pardomuan, Muhammad Azizi Mohd Ariffin, and Aditya Kurniawan. 2022. Predicting confidentiality, integrity, and availability from SQL injection payload. In *2022 International Conference on Information Management and Technology (ICIMTech)*. IEEE, 600–605.

[137] Mohammed Saleh Ali Muthanna, Reem Alkanhel, Ammar Muthanna, Ahsan Rafiq, and Wadhah Ahmed Muthanna Abdullah. 2022. Towards SDN-enabled, intelligent intrusion detection system for internet of things (IoT). *IEEE Access* 10 (2022), 22756–22768.

[138] Joonwoo Myung, Youngmin Ko, Taewoong Kwon, Jun Lee, Kyuil Kim, and Jungsuk Song. 2023. Intrusion detection systems based on machine learning using feature expansion methods. In *2023 18th Asia Joint Conference on Information Security (AsiaJCIS)*. IEEE, 32–38.

[139] Azqa Nadeem, Sicco Verwer, Stephen Moskal, and Shanchieh Jay Yang. 2021. Alert-driven attack graph generation using s-pdfa. *IEEE Transactions on Dependable and Secure Computing* 19, 2 (2021), 731–746.

[140] Carlos Natalino, Marco Schiano, Andrea Di Giglio, and Marija Furdek. 2022. Root cause analysis for autonomous optical network security management. *IEEE Transactions on Network and Service Management* 19, 3 (2022), 2702–2713.

[141] Mohamed Naveen and Suman De. 2022. Efficient digital assistant workflow for ticket monitoring and dispatching. In *2022 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON)*. IEEE, 1–6.

[142] Samuel Ndichu, Tao Ban, Takeshi Takahashi, and Daisuke Inoue. 2021. A machine learning approach to detection of critical alerts from imbalanced multi-appliance threat alert logs, Y. Chen, H. Ludwig, Y. Tu, U. Fayyad, X. Zhu, X. Hu, S. Byna, X. Liu, J. Zhang, S. Pan, V. Papalexakis, J. Wang, A. Cuzzocrea, and C. Ordonez (Eds.). *2021 IEEE INTERNATIONAL CONFERENCE ON BIG DATA (BIG DATA)*, 2119–2127. DOI: https://doi.org/10.1109/BigData52589.2021.9671956 9th IEEE International Conference on Big Data (IEEE BigData), ELECTR NETWORK, DEC 15-18, 2021.

[143] Samuel Ndichu, Tao Ban, Takeshi Takahashi, and Daisuke Inoue. 2022. Critical-threat-alert detection using online machine learning. In *2022 IEEE International Conference on Big Data (Big Data)*. IEEE, 3007–3014.

[144] Samuel Ndichu, Tao Ban, Takeshi Takahashi, and Daisuke Inoue. 2022. Security-alert screening with oversampling based on conditional generative adversarial networks. In *2022 17th Asia Joint Conference on Information Security (AsiaJCIS)*. IEEE, 1–7.

[145] Samuel Ndichu, Tao Ban, Takeshi Takahashi, and Daisuke Inoue. 2023. Machine learning–based security alert screening with focal loss. In *2023 IEEE International Conference on Big Data (BigData)*. IEEE, 3043–3052.

[146] Euclides Carlos Pinto Neto, Sajjad Dadkhah, and Ali A Ghorbani. 2022. Collaborative DDoS detection in distributed multi-tenant IoT using federated learning. In *2022 19th Annual International Conference on Privacy, Security & Trust (PST)*. IEEE, 1–10.

[147] Subash Neupane, Jesse Ables, William Anderson, Sudip Mittal, Shahram Rahimi, Ioana Banicescu, and Maria Seale. 2022. Explainable intrusion detection systems (x-ids): A survey of current methods, challenges, and opportunities. *IEEE Access* 10 (2022), 112392–112415.

[148] Quoc Phong Nguyen, Kar Wai Lim, Dinil Mon Divakaran, Kian Hsiang Low, and Mun Choon Chan. 2019. Gee: A gradient-based explainable variational autoencoder for network anomaly detection. In *2019 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 91–99.

[149] Taishi Nishiyama, Atsutoshi Kumagai, Kazunori Kamiya, and Kenji Takahashi. 2020. SILU: Strategy involving large-scale unlabeled logs for improving malware detector. *2020 IEEE SYMPOSIUM ON COMPUTERS AND COMMUNICATIONS (ISCC)*, 524–530. 25th IEEE Symposium on Computers and Communications (ISCC), Rennes, FRANCE, JUL 07-10, 2020.

[150] Francesco Nocera, Simone Demilito, Piergiorgio Ladisa, Marina Mongiello, Awais Aziz Shah, Jawad Ahmad, and Eugenio Di Sciascio. 2022. A user behavior analytics (uba)-based solution using lstm neural network to mitigate ddos attack in fog and cloud environment. In *2022 2nd International Conference of Smart Systems and Emerging Technologies (SMARTTECH)*. IEEE, 74–79.

[151] Ridwan Nur Wibowo, Parman Sukarno, and Erwid Musthofa Jadied. 2019. NSL-KDD Dataset. https://api.semanticscholar.org/CorpusID:198166203

[152] Håvard Jakobsen Ofte and Sokratis Katsikas. 2023. Understanding situation awareness in SOCs, a systematic literature review. *Computers & Security* 126 (2023), 103069.

[153] Talha Ongun, Oliver Spohngellert, Benjamin Miller, Simona Boboila, Alina Oprea, Tina Eliassi-Rad, Jason Hiser, Alastair Nottingham, Jack Davidson, and Malathi Veeraraghavan. 2021. PORTFILER: Port-level network profiling for self-propagating malware detection. In *2021 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 182–190.

[154] Alina Oprea, Zhou Li, Robin Norris, and Kevin Bowers. 2018. Made: Security analytics for enterprise threat detection. In *Proceedings of the 34th Annual Computer Security Applications Conference*. 124–136.

[155] Alina Oprea, Zhou Li, Robin Norris, and Kevin Bowers. 2018. MADE: Security analytics for enterprise threat detection. *Proceedings of the 34th Annual Computer Security Applications Conference*, 124–136. DOI: https://doi.org/10.1145/3274694.3274710

[156] Riccardo Orizio, Satyanarayana Vuppala, Stylianos Basagiannis, and Gregory Provan. 2020. Towards an explainable approach for insider threat detection: Constraint network learning. In *2020 International Conference on Intelligent Data Science Technologies and Applications (IDSTA)*. IEEE, 42–49.

[157] Matthew J. Page, Joanne E. McKenzie, Patrick M. Bossuyt, Isabelle Boutron, Tammy C. Hoffmann, Cynthia D. Mulrow, Larissa Shamseer, Jennifer M. Tetzlaff, Elie A. Akl, Sue E. Brennan, Roger Chou, Julie Glanville, Jeremy M. Grimshaw, Asbjørn Hróbjartsson, Manoj M Lalu, Tianjing Li, Elizabeth W Loder, Evan Mayo-Wilson, Steve McDonald, Luke A. McGuinness, Lesley A. Stewart, James Thomas, Andrea C. Tricco, Vivian A. Welch, Penny Whiting, and David Moher. 2021. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ* 372 (2021). DOI: https://doi.org/10.1136/bmj.n71 arXiv:https://www.bmj.com/content/372/bmj.n71.full.pdf

[158] Cheolhee Park, Jonghoon Lee, Youngsoo Kim, Jong-Geun Park, Hyunjin Kim, and Dowon Hong. 2022. An enhanced AI-based network intrusion detection system using generative adversarial networks. *IEEE Internet of Things Journal* 10, 3 (2022), 2330–2345.

[159] Uduwarage Nipun Akalanka Perera, Shanith Rathnayaka, ND Perera, WW Madushanka, and Amila Nuwan Senarathne. 2021. The next gen security operation center. In *2021 6th International Conference for Convergence in Technology (I2CT)*. IEEE, 1–9.

[160] Vihanga Heshan Perera, Amila Nuwan Senarathne, and Lakmal Rupasinghe. 2019. Intelligent soc chatbot for security operation center. In *2019 International Conference on Advancements in Computing (ICAC)*. IEEE, 340–345.

[161] Sergio Iglesias Pérez, Santiago Moral-Rubio, and Regino Criado. 2021. A new approach to combine multiplex networks and time series attributes: Building intrusion detection systems (IDS) in cybersecurity. *Chaos, Solitons & Fractals* 150 (2021), 111143.

[162] Aditya Pingle, Aritran Piplai, Sudip Mittal, Anupam Joshi, James Holt, and Richard Zak. 2020. RelExt: Relation extraction using deep learning approaches for cybersecurity knowledge graph improvement. *Proceedings of the 2019 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, 879–886. DOI: https://doi.org/10.1145/3341161.3343519

[163] Alfan Presekal, Alexandru Ştefanov, Vetrivel Subramaniam Rajkumar, and Peter Palensky. 2023. Cyber forensic analysis for operational technology using graph-based deep learning. In *2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE, 1–7.

[164] Medha Pujari, Bhanu Prakash Cherukuri, Ahmad Y Javaid, and Weiqing Sun. 2022. An approach to improve the robustness of machine learning based intrusion detection system models against the carlini-wagner attack. In *2022 IEEE International Conference on Cyber Security and Resilience (CSR)*. IEEE, 62–67.

[165] Áron Puskás, Eszter Kail, Szandra Laczi, and Anna Bánáti. 2023. Neural network-based log analysis methods for 5G network. In *2023 IEEE 21st Jubilee International Symposium on Intelligent Systems and Informatics (SISY)*. IEEE, 000589–000594.

[166] Malik Qasaimeh, Rand Abu Hammour, Muneer Bani Yassein, Raad S Al-Qassas, Juan Alfonso Lara Torralbo, and David Lizcano. 2022. Advanced security testing using a cyber-attack forecasting model: A case study of financial institutions. *Journal of Software: Evolution and Process* 34, 11 (2022), e2489.

[167] Petar Radanliev. 2024. Digital security by design. *Security Journal* 37, 4 (2024), 1640–1679.

[168] Petar Radanliev. 2024. Integrated cybersecurity for metaverse systems operating with artificial intelligence, blockchains, and cloud computing. *Frontiers in Blockchain* 7 (2024), 1359130.

[169] Priyanka Ranade, Aritran Piplai, Anupam Joshi, and Tim Finin. 2021. Cybert: Contextualized embeddings for the cybersecurity domain. In *2021 IEEE International Conference on Big Data (Big Data)*. IEEE, 3334–3342.

[170] Ruby Rani, Gregory Epiphaniou, and Carsten Maple. 2023. Reinforcement learning-based alert prioritisation in security operation centre: A framework for enhancing cybersecurity in the digital economy. In *International Conference on AI and the Digital Economy (CADE 2023)*, Vol. 2023. IET, 151–157.

[171] Madhu Raut, Sunita Dhavale, Amarjit Singh, and Atul Mehra. 2020. Insider threat detection using deep learning: A review. In *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)*. IEEE, 856–863.

[172] Christopher Redino, Dhruv Nandakumar, Robert Schiller, Kevin Choi, Abdul Rahman, Edward Bowen, Aaron Shaha, Joe Nehila, and Matthew Weeks. 2022. Zero day threat detection using graph and flow based security telemetry. In *2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*. IEEE, 655–662.

[173] Matteo Repetto. 2023. Adaptive monitoring, detection, and response for agile digital service chains. *Computers & Security* 132 (2023), 103343.

[174] Gilad Rosenthal, Ofir Erets Kdosha, Kobi Cohen, Alon Freund, Avishay Bartik, and Aviv Ron. 2020. ARBA: Anomaly and reputation based approach for detecting infected IoT devices. *IEEE Access* 8 (2020), 145751–145767.

[175] Kevin A Roundy, Acar Tamersoy, Michael Spertus, Michael Hart, Daniel Kats, Matteo Dell'Amico, and Robert Scott. 2017. Smoke detector: Cross-product intrusion detection with weak indicators. In *Proceedings of the 33rd Annual Computer Security Applications Conference*. 200–211.

[176] Stuart Russell and Peter Norvig. 2021. Artificial Intelligence: A Modern Approach (4th ed.). Prentice Hall.

[177] Stanisław Saganowski. 2020. A three-stage machine learning network security solution for public entities. In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, 1097–1104.

[178] Sagar Samtani, Hongyi Zhu, and Hsinchun Chen. 2020. Proactively identifying emerging hacker threats from the dark web: A diachronic graph embedding framework (d-gef). *ACM Transactions on Privacy and Security (TOPS)* 23, 4 (2020), 1–33.

[179] José Carlos Sancho, Andrés Caro, Mar Ávila, and Alberto Bravo. 2020. New approach for threat classification and security risk estimations based on security event management. *Future Generation Computer Systems* 113 (2020), 488–505.

[180] Vita Santa Barletta, Danilo Caivano, Mirko De Vincentiis, Anibrata Pal, and Francesco Volpe. 2023. Automotive knowledge base for supporting vehicle-SOC analysts. In *2023 IEEE International Conference on Metrology for eXtended Reality, Artificial Intelligence and Neural Engineering (MetroXRAINE)*. IEEE, 960–965.

[181] Daniel Schlette, Marco Caselli, and Günther Pernul. 2021. A comparative study on cyber threat intelligence: The security incident response perspective. *IEEE Communications Surveys & Tutorials* 23, 4 (2021), 2525–2556.

[182] Hichem Sedjelmaci. 2020. Attacks detection approach based on a reinforcement learning process to secure 5g wireless network. In *2020 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, 1–6.

[183] Hichem Sedjelmaci. 2022. Attacks detection and decision framework based on generative adversarial network approach: Case of vehicular edge computing network. *Transactions on Emerging Telecommunications Technologies* 33, 10 (10 2022), e4073. DOI: https://doi.org/10.1002/ett.4073

[184] Hichem Sedjelmaci, Fateh Guenab, Aymen Boudguiga, and Yohann Petiot. 2018. Cooperative security framework for CBTC network. In *2018 IEEE International Conference on Communications (ICC)*. IEEE, 1–6.

[185] Ömer Sen, Philipp Malskorn, Simon Glomb, Immanuel Hacker, Martin Henze, and Andreas Ulbig. 2023. An approach to abstract multi-stage cyberattack data generation for ml-based ids in smart grids. In *2023 IEEE Belgrade PowerTech*. IEEE, 01–10.

[186] Giuseppe Settanni, Yegor Shovgenya, Florian Skopik, Roman Graf, Markus Wurzenberger, and Roman Fiedler. 2017. Acquiring cyber threat intelligence through security information correlation. In *2017 3rd IEEE International Conference on Cybernetics (CYBCONF)*. IEEE, 1–7.

[187] Ankit Shah, Arunesh Sinha, Rajesh Ganesan, Sushil Jajodia, and Hasan Cam. 2020. Two can play that game: An adversarial evaluation of a cyber-alert inspection system. *ACM Transactions on Intelligent Systems and Technology (TIST)* 11, 3 (2020), 1–20.

[188] Deepesh Shahjee and Nilesh Ware. 2022. Integrated network and security operation center: A systematic analysis. *IEEE Access* 10 (2022), 27881–27898.

[189] Iman Sharafaldin, Arash Habibi Lashkari, Ali A Ghorbani, et al. 2018. Toward generating a new intrusion detection dataset and intrusion traffic characterization. *ICISSp* 1 (2018), 108–116.

[190] Iman Sharafaldin, Arash Habibi Lashkari, Saqib Hakak, and Ali A Ghorbani. 2019. Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy. In *2019 International Carnahan Conference on Security Technology (ICCST)*. IEEE, 1–8.

[191] Haroon Sheikh, Corien Prins, and Erik Schrijvers. 2023. Artificial intelligence: Definition and background. In *Mission AI: The New System Technology*. Springer, 15–41.

[192] Toshiki Shibahara, Hirokazu Kodera, Daiki Chiba, Mitsuaki Akiyama, Kunio Hato, Ola Söderström, Daniel Dalek, and Masayuki Murata. 2019. Cross-vendor knowledge transfer for managed security services with triplet network. *Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security*, 59–69. DOI: https://doi.org/10.1145/3338501.3357367

[193] Lijian Sun, Yun Zhou, Yanjuan Wang, Cheng Zhu, and Weiming Zhang. 2020. The effective methods for intrusion detection with limited network attack data: Multi-task learning and oversampling. *IEEE Access* 8 (2020), 185384–185398.

[194] Hatma Suryotrisongko, Yasuo Musashi, Akio Tsuneda, and Kenichi Sugitani. 2022. Robust botnet DGA detection: Blending XAI and OSINT for cyber threat intelligence sharing. *IEEE Access* 10 (2022), 34613–34624.

[195] Zarrin Tasnim Sworna, Muhammad Ali Babar, and Anjitha Sreekumar. 2023. IRP2API: Automated mapping of cyber security incident response plan to security tools' APIs. In *2023 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER)*. IEEE, 546–557.

[196] Zarrin Tasnim Sworna, Chadni Islam, and Muhammad Ali Babar. 2023. APIRO: A framework for automated security tools API recommendation. *ACM Trans. Softw. Eng. Methodol.* 32, 1 (2 2023), 1–42. https://doi.org/10.1145/3512768

[197] Mateusz Szczepański, Michał Choraś, Marek Pawlicki, and Rafał Kozik. 2020. Achieving explainability of intrusion detection system by hybrid oracle-explainer approach. In *2020 International Joint Conference on Neural Networks (IJCNN)*. IEEE, 1–8.

[198] Baoming Tang, Qiaona Hu, and Derek Lin. 2017. Reducing false positives of user-to-entity first-access alerts for user behavior analytics. In *2017 IEEE International Conference on Data Mining Workshops (ICDMW)*. IEEE, 804–811.

[199] Paul Theron, Alexander Kott, Martin Drašar, Krzysztof Rzadca, Benoît LeBlanc, Mauno Pihelgas, Luigi Mancini, and Agostino Panico. 2018. Towards an active, autonomous and intelligent cyber defense of military systems: The NATO AICA reference architecture. In *2018 International Conference on Military Communications and Information Systems (ICMCIS)*. IEEE, 1–9.

[200] Hauton Tsang, Mohammad A Salahuddin, Noura Limam, and Raouf Boutaba. 2023. Meta-ATMoS+: A meta-reinforcement learning framework for threat mitigation in software-defined networks. In *2023 IEEE 48th Conference on Local Computer Networks (LCN)*. IEEE, 1–9.

[201] Andrea Tundis, Samuel Ruppert, and Max Mühlhäuser. 2022. A feature-driven method for automating the assessment of osint cyber threat sources. *Computers & Security* 113 (2022), 102576.

[202] Uğur Ünal and Hasan Dağ. 2022. Anomalyadapters: Parameter-efficient multi-anomaly task detection. *IEEE Access* 10 (2022), 5635–5646.

[203] Uğur Ünal, Ceyda Nur Kahya, Yaprak Kurtlutepe, and Hasan Dağ. 2021. Investigation of cyber situation awareness via SIEM tools: A constructive review. In *2021 6th International Conference on Computer Science and Engineering (UBMK)*. IEEE, 676–681.

[204] Rohit Valecha, Pranali Mandaokar, and H Raghav Rao. 2021. Phishing email detection using persuasion cues. *IEEE Transactions on Dependable and Secure Computing* 19, 2 (2021), 747–756.

[205] Thijs Van Ede, Hojjat Aghakhani, Noah Spahn, Riccardo Bortolameotti, Marco Cova, Andrea Continella, Maarten van Steen, Andreas Peter, Christopher Kruegel, and Giovanni Vigna. 2022. Deepcase: Semi-supervised contextual analysis of security events. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 522–539.

[206] Meble Varghese and M Victor Jose. 2022. Optimal trained deep maxout model for intrusion detection in cloud. In *2022 International Conference on Automation, Computing and Renewable Systems (ICACRS)*. IEEE, 1220–1227.

[207] Seba Anna Varghese, Alireza Dehlaghi Ghadim, Ali Balador, Zahra Alimadadi, and Panos Papadimitratos. 2022. Digital twin-based intrusion detection for industrial control systems. In *2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*. IEEE, 611–617.

[208] Sridhar Venkatesan, Harshvardhan Sikka, Rauf Izmailov, Ritu Chadha, Alina Oprea, and Michael J De Lucia. 2021. Poisoning attacks and data sanitization mitigations for machine learning models in network intrusion detection systems. In *MILCOM 2021-2021 IEEE Military Communications Conference (MILCOM)*. IEEE, 874–879.

[209] Manfred Vielberth, Fabian Böhm, Ines Fichtinger, and Günther Pernul. 2020. Security operations center: A systematic study and open challenges. *IEEE Access* 8 (2020), 227756–227779.

[210] Quang Hieu Vu, Dymitr Ruta, and Ling Cen. 2019. Gradient boosting decision trees for cyber security threats detection based on network events logs. In *2019 IEEE International Conference on Big Data (Big Data)*. IEEE, 5921–5928.

[211] AM Vulfin. 2023. Detection of network attacks in a heterogeneous industrial network based on machine learning. *Programming and Computer Software* 49, 4 (2023), 333–345.

[212] Yatin Wadhawan and Clifford Neuman. 2018. Rl-bags: A tool for smart grid risk assessment. In *2018 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE)*. IEEE, 7–14.

[213] Tian Wang, Chen Zhang, Zhigang Lu, Dan Du, and Yaopeng Han. 2019. Identifying truly suspicious events and false alarms based on alert graph. In *2019 IEEE International Conference on Big Data (Big Data)*. IEEE, 5929–5936.

[214] Xuren Wang, Rong Chen, Binghua Song, Jie Yang, Zhengwei Jiang, Xiaoqing Zhang, Xiaomeng Li, and Shengqin Ao. 2021. A method for extracting unstructured threat intelligence based on dictionary template and reinforcement learning. In *2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*. IEEE, 262–267.

[215] Yifeng Wang, Yuanbo Guo, and Chen Fang. 2022. An end-to-end method for advanced persistent threats reconstruction in large-scale networks based on alert and log correlation. *Journal of Information Security and Applications* 71 (2022), 103373.

[216] Arkadiusz Warzyński, Patryk Schauer, and Łukasz Falas. 2021. Regional center of cybersecurity anomaly detection module efficiency in network monitoring scenarios. In *2021 IEEE 30th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*. IEEE, 107–112.

[217] Łukasz Wawrowski, Marcin Michalak, Andrzej Białas, Rafał Kurianowicz, Marek Sikora, Mariusz Uchroński, and Adrian Kajzer. 2021. Detecting anomalies and attacks in network traffic monitoring with classification methods and XAI-based explainability. *Procedia Computer Science* 192 (2021), 2259–2268.

[218] Peilun Wu and Hui Guo. 2022. Holmes: An efficient and lightweight semantic based anomalous email detector. In *2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, 1360–1367.

[219] Peilin Wu, Jinlei Li, Yan Meng, and Haojin Zhu. 2019. An ensemble approach for suspicious traffic detection from high recall network alerts. In *2019 IEEE International Conference on Big Data (Big Data)*. IEEE, 5937–5944.

[220] Shuning Wu, Joel Fulton, Ningwei Liu, Charles Feng, and Ligang Zhang. 2019. Risky host detection with bias reduced semi-supervised learning. *Proceedings of the 2019 International Conference on Artificial Intelligence and Computer Science*, 34–40. DOI: https://doi.org/10.1145/3349341.3349365

[221] Anli Yan, Zhenxiang Chen, Riccardo Spolaor, Shuaishuai Tan, Chuan Zhao, Lizhi Peng, and Bo Yang. 2020. Network-based malware detection with a two-tier architecture for online incremental update. In *2020 IEEE/ACM 28th International Symposium on Quality of Service (IWQoS)*. IEEE, 1–10.

[222] Huiran Yang, Jiaqi Kang, Yueyue Dai, Jiyan Sun, Yan Zhang, Huajun Cui, and Can Ma. 2023. LActDet: An automatic network attack activity detection framework for multi-step attacks. In *2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, 676–685.

[223] Huiran Yang, Yan Zhang, Yueyue Dai, Jiyan Sun, Huajun Cui, Can Ma, and Weiping Wang. 2023. CACluster: A clustering approach for IoT attack activities based on contextual analysis. In *2023 IEEE 29th International Conference on Parallel and Distributed Systems (ICPADS)*. IEEE, 1809–1816.

[224] Jin Yang, Tao Li, Gang Liang, Wenbo He, and Yue Zhao. 2019. A simple recurrent unit model based intrusion detection system with DCGAN. *IEEE Access* 7 (2019), 83286–83296.

[225] Zhen Yang, Xiaodong Liu, Tong Li, Di Wu, Jinjiang Wang, Yunwei Zhao, and Han Han. 2022. A systematic literature review of methods and datasets for anomaly-based network intrusion detection. *Computers & Security* 116 (2022), 102675.

[226] Waleed A. Yousef, Issa Traoré, and William Briguglio. 2022. Classifier calibration: with application to threat scores in cybersecurity. *IEEE Transactions on Dependable and Secure Computing* 20, 3 (2022), 1994–2010.

[227] Syed Rameem Zahra, Mohammad Ahsan Chishti, Asif Iqbal Baba, and Fan Wu. 2022. Detecting Covid-19 chaos driven phishing/malicious URL attacks by a fuzzy logic and data mining based intelligence system. *Egyptian Informatics Journal* 23, 2 (2022), 197–214.

[228] Jun Zengy, Xiang Wang, Jiahao Liu, Yinfang Chen, Zhenkai Liang, Tat-Seng Chua, and Zheng Leong Chua. 2022. Shadewatcher: Recommendation-guided cyber threat analysis using system audit records. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 489–506.

[229] Fengli Zhang, Philip Huff, Kylie McClanahan, and Qinghua Li. 2020. A machine learning-based approach for automated vulnerability remediation analysis. In *2020 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 1–9.

[230] Yizhe Zhang, Hongying Dong, Alastair Nottingham, Molly Buchanan, Donald E Brown, and Yixin Sun. 2023. Global analysis with aggregation-based beaconing detection across large campus networks. In *Proceedings of the 39th Annual Computer Security Applications Conference*. 565–579.

[231] Ziani Zineb, Emad Nahid, and Bouaziz Ahmed. 2023. A novel approach to parallel anomaly detection: Application in cybersecurity. In *2023 IEEE International Conference on Big Data (BigData)*. IEEE, 3574–3583.

## Appendices

### A Data Availability

In accordance with the principles of transparency and open collaboration, all data and supplementary materials which are not included within the paper for brevity are available upon request. Interested parties can obtain these materials by reaching out to the corresponding author. The sharing of data and materials will be facilitated to support the replication and validation of findings, foster scholarly dialogue, and encourage further research inquiries. Requests for materials will be considered on a case-by-case basis, with the intent of ensuring their appropriate use. Please provide a brief description of the intended use or purpose for which you are requesting the materials. We are committed to promoting transparency and collaboration, and will endeavor to respond to requests promptly.

### B Additional Information

In this section includes supplementary information for the survey.

### B.1 Registration and Protocol

This review is not registered and no protocol has been prepared.

### B.2 Support

No specific financial support was received for this survey.

### B.3 Competing Interests

Authors have no competing interests.

Received 4 February 2025; revised 7 May 2025; accepted 18 May 2025