International Journal of Information Security (2026) 25:103
https://doi.org/10.1007/s10207-026-01259-5

REGULAR CONTRIBUTION

Human-AI Integration in Cybersecurity: An Industry-Aligned Perspective on Incident Management

Jan Kincl[1,2] · **Marc T. P. Adam**[2] · **Tanja Pavleska**[1]

Received: 18 November 2025 / Accepted: 9 April 2026

Abstract

The integration of Artificial Intelligence (AI) into cybersecurity incident management has gained momentum amid rising threats and increasing operational complexity. While academic research has been widely analysed and found to predominantly address detection tasks and algorithmic performance, the industry perspective remains under-explored, with limited understanding of its practices and priorities. This paper presents a document analysis of a rich corpus of publicly available, industry-issued reports, to examine how AI is understood, deployed, and evaluated in real-world cybersecurity operations. By contextualising the well-established Technology-Human-Task-Context (THTC) framework to the cybersecurity domain, we identify key dimensions shaping AI integration, including task alignment, human oversight, operational constraints, and expected benefits. Our findings highlight critical gaps in current implementations, such as limited attention to recovery, governance, and task assignment, and emphasise the dual role of human experts as both controllers and beneficiaries. To address these gaps and support actionable system design, we propose a set of industry-aligned recommendations derived from a synthesis of the THTC framework and document analysis. These recommendations encompass AI capabilities, integration requirements, task alignment, outcomes, risk management, control mechanisms, and human factors. Our work offers a comprehensive foundation for aligning academic research with industry needs, guiding the development of AI-powered cybersecurity expert systems that are technically effective, ethically sound, and operationally viable.

Keywords Cybersecurity Incident Management · Artificial Intelligence · AI-Human Integration Recommendations · THTC Framework · Document Analysis · Academia-Industry Alignment

1 Introduction

The cybersecurity domain faces a growing number of incidents[1] alongside increasingly sophisticated threats, making the protection of digital assets increasingly critical in today's interconnected world. These challenges place immense pressure on Security Operation Centres (SOCs) teams and individuals responsible for safeguarding IT infrastructures, who often operate in high-pressure environments constrained by under-staffing, burnout, and limited support by operational automation [2]. In this context, artificial intelligence (AI) is widely recognised as both a threat and a transformative asset: while adversaries increasingly exploit AI to enhance the scale and sophistication of attacks [3], cybersecurity experts see the integration of AI into cybersecurity incident

✉ Jan Kincl
jan.kincl@uon.edu.au

Marc T. P. Adam
marc.adam@newcastle.edu.au

Tanja Pavleska
tanja.pavleska@ijs.si

[1] Laboratory for Open Systems and Networks, Jozef Stefan Institute, Ljubljana, Slovenia

[2] School of Computer and Information Sciences, University of Newcastle, Callaghan, NSW, Australia

[1] An *incident* is defined as "an unwanted or unexpected cybersecurity event, or a series of such events, that either has compromised business operations or has a significant probability of compromising business operations" [1].

Published online: 29 May 2026

management (CIM) as a key opportunity to improve the effectiveness and resilience of cybersecurity operations [4].

Despite the recognition and popularity of AI in cybersecurity research, several limitations persist in how it is studied and applied within the field. Multiple sources highlight a prevailing tendency of academic research to focus predominantly on detection-related problems, such as threat identification or anomaly detection, while other critical phases of cybersecurity incident management, particularly response and recovery, remain under-explored [5, 6]. Moreover, academic approaches often underestimate the importance of solution integrability and neglect the human element in cybersecurity operations [7].

In contrast, industry perspectives increasingly emphasise human-AI integration, where an AI expert system is designed to support and augment human operators, rather than replace them [8]. This divergence highlights a growing need to bridge the gap between academic and industry approaches, particularly in understand and improving the integration of AI into CIM. As WEF [9] asserted, "Focused industrial and academic research is needed to support this activity and develop the right research agenda" (p. 30). Understanding this shift is essential for guiding future research efforts and aligning priorities across both domains.

To support clearer exchange and collaboration between academia and industry, this study addresses the research problem of how AI is perceived and integrated into CIM by industry stakeholders. We approach this by conducting a document analysis of publicly available industry-issued literature, with the goal of identifying conceptual areas of AI integration. These insights are structured using the Technology-Human-Task-Context (THTC) framework, well-established framework in the domain of Human—Computer Interaction (HCI), which serves as the basis for establishing a conceptual model for AI integration grounded in industry practice.

The contributions of this paper are threefold. First, via a systematic analysis of industry-issued documents using the THTC framework, we structure the industry's perception, practices and recognised challenges of AI integration in CIM. Which enables the identification of conceptual focus, human-centric considerations, and under-explored areas. Second, we compare these insights with academic literature to highlight differences in research focus and uncover actionable gaps between research and practice. Finally, we propose a system of industry-synthesised recommendations intended to guide the development of AI-driven cybersecurity expert systems that are integrable, human-centric, and aligned with real-world operational needs.

2 Background and Related Work

This section provides the conceptual and theoretical foundations for our study, while also presenting the state-of-the-art approaches focused on the integration of AI technologies and human operators in CIM.

2.1 Extended Technology-Human-Task-Context Framework

We argue that integrating AI into CIM constitutes a case of socio-technical systems design in the broader HCI domain. Therefore, to structure our analysis, we adopt the widely established THTC framework proposed by Li and Zhang [10]. This framework recognises four areas influencing HCI: Technology, Human, Task and Context. It offers a lens for analysing complex socio-technical systems and the dependencies between human stakeholders, technology, and the contextual background and purpose of the interaction. Additionally, in line with more recent THTC adaptations that focused on mapping HCI effects for specific use cases [e.g.11], we extend the original framework with an *Outcome* dimension to provide a basic reference framework for mapping interactions between human and AI systems in cybersecurity.

Contextualised for the high-stakes and human-centred environments such as CIM, this approach allows us to recognise that AI technology does not operate in isolation, but is rather embedded in a complex interplay with: security expert roles, cognitive processes and interaction with computer systems (Human); operational workflows, decision structures and objectives of CIM (Task); regulatory and operational environments (Context); the technological characteristics of AI approaches that constrain or enable task execution (Technology); and the results of AI integration (Outcome).

This multidimensional framing directly aligns with the realities of cybersecurity operations, where human judgement, task specificity, technology capabilities and contextual constraints determine system success or failure. In the following sections, we briefly examine how existing literature reviews address the challenges and opportunities of AI in cybersecurity along the THTC framework dimensions.

2.2 Perspectives on AI in Cybersecurity

Numerous studies recognise the growing role of AI in cybersecurity. Sarker et al. [12] provides an overview of AI-based techniques for cybersecurity automation, such as Machine Learning (ML), Deep Learning (DL), Natural Language Processing (NLP), and knowledge representation. Similarly, Sankaram et al. [13] explores the transformative role of AI techniques, listing Supervised and Unsupervised Learning, Neural Networks, and Reinforcement Learning. Further-

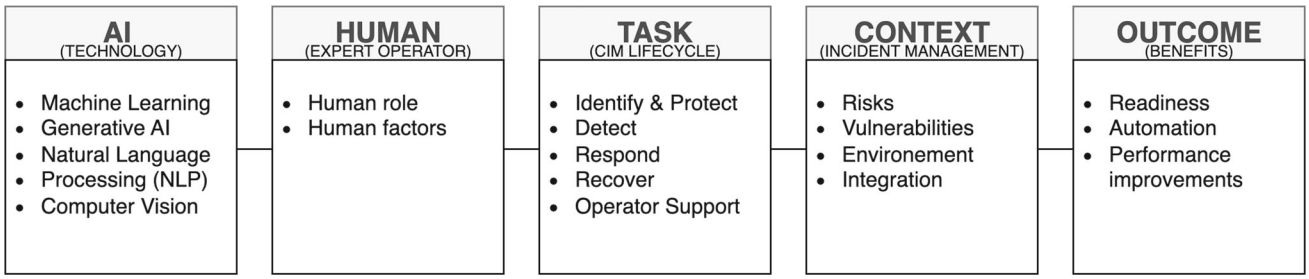

Fig. 1 Contextualised THTC Framework

more, Naik et al. [14] identifies directions in distributed AI approaches, such as multi-agent systems and expert systems relying on fuzzy logic. Overall, existing reviews focus on presenting taxonomies [e.g. [15]] of AI and ML approaches in cybersecurity. These taxonomies are often used to correlate AI approaches with specific cybersecurity tasks. For example, Ali et al. [15] identifies AI applications for intrusion detection, malware detection, and spam filtering, which is complemented by ransomware detection by [16] and insider threat detection using NLP [17]. Similarly, Jada and Mayayise [18] provides literature comparison in terms of AI roles in intrusion detection and incident prediction. Recent work also explores the role of large language models for vulnerability detection and related metrics [19]. Less frequently, tasks such as knowledge management [12], decision support [20], or expert systems [14] are also included among the AI-driven approaches to cybersecurity.

Beyond technology-task alignment, some literature revie ws focus on the vulnerabilities and limitations of AI-based systems. In that context, Li [21] highlights the sensitivity of AI models to data manipulation and data quality, whereas Goud [22] recognises the privacy concerns, transparency issues, and regulatory challenges related to AI-driven systems. Moreover, Ansari et al. [23] identifies and discusses the increased cost risks. Although several important studies have addressed some cybersecurity related AI risks, their overall coverage in the field remains relatively limited [18].

Existing reviews understand AI as a transformative force in cybersecurity, frequently recognising its role in improving threat detection and identification tasks [6, 22, 24]. Enhancements in performance [18], scalability, and readiness to face advanced adversarial threats are also commonly noted [25]. However, these benefits are often discussed in general terms, with limited attention to challenges in AI integration.

2.3 Human support and challenges in CIM

The role of human experts remains a central component of CIM, even as AI-driven tools increasingly support detection and response activities. Cybersecurity operations are inherently socio-technical, requiring continuous interaction between human expertise, technological systems, and organisational processes [26]. Human actors, including security analysts, incident responders, and threat hunters, play an essential role in interpreting system outputs, making decisions under uncertainty, and ensuring that security actions align with organisational priorities and risk tolerance [27].

Human involvement spans all phases of the CIM lifecycle [26]. In the identification and protection phases, experts are responsible for defining security policies, configuring detection mechanisms, and assessing system vulnerabilities. During the detection phase, human analysts validate alerts, distinguish false positives from genuine threats, and correlate signals across multiple data sources. This validation process is particularly important given the high volume of alerts generated by automated systems and the prevalence of alert fatigue in Security Operations Centres (SOCs) [28]. In the response phase, human actors make critical decisions regarding containment, mitigation, and escalation, often under time pressure and incomplete information. Finally, in the recovery phase, they conduct root cause analysis, coordinate system restoration, and integrate lessons learned into future defensive strategies. [29]

However, this human-centric nature of the CIM workflows also leads to constraints in the performance limits, dictated by the performance limits of the human operators themselves. Empirical studies show that SOCs often operate under conditions of high alert volumes, fragmented workflows, staff shortages, and limited automation support [30]. These challenges place substantial cognitive demand on analysts, often resulting in cognitive overload, increased error rates, and reduced decision quality. Moreover, prolonged exposure to such high-pressure environments contributes to affective strain, including elevated stress, frustration, and an increased risk of burnout risk [26, 31]. As a result, human performance becomes a critical factor influencing the effectiveness and reliability of incident management processes.

A complementary line of research examines CIM from the perspective of operational bottlenecks and workflow inefficiencies, focusing on how technological systems can better support human operators. Large-scale analyses of incident tickets and response workflows reveal persistent issues

such as incomplete service dependencies, ambiguous or low-context alerts, misrouted or repeatedly reassigned incidents, and delays in triage and mitigation [27, 32]. These findings emphasise that technological limitations are often intertwined with human decision-making challenges, particularly in environments characterised by uncertainty and information overload. Consequently, effective support systems must go beyond task automation and explicitly account for human roles within the process. This includes providing richer contextual information, reducing informational noise, improving visualisation and interpretability of system outputs, and offering actionable, decision-oriented guidance during complex investigations [33].

With the integration of AI into CIM, the role of humans is evolving rather than diminishing. Instead of acting solely as operators, humans increasingly function as supervisors, validators, and collaborators in human–AI systems [34]. They are responsible for interpreting AI-generated outputs, verifying recommendations, and intervening when automated decisions are uncertain or potentially incorrect. This human-in-the-loop approach is essential to mitigate risks such as automation bias, over-reliance on AI, and misinterpretation of model outputs [35, 36]. Maintaining appropriate levels of human oversight is therefore critical to ensuring accountability, trust, and effective decision-making in AI-supported cybersecurity environments.

Within the THTC framework adopted in this study, the human dimension interacts closely with technological capabilities, task requirements, and contextual constraints. Understanding how human expertise complements AI systems is essential for designing effective and resilient CIM processes. Rather than replacing human actors, AI technologies should be viewed as augmenting human capabilities, supporting analysts in managing complexity, reducing cognitive load, and improving overall incident response performance.

2.4 Industry AI integration alignment

Taken together, current findings indicate that CIM performance is shaped by intertwined cognitive, affective, and organisational pressures. While existing research identifies where humans struggle within incident workflows, only a few studies review AI approaches in cybersecurity with integration and human interaction in mind. Binbeshr et al. [37] analyse 38 studies considering the usability of their proposed approaches for Security Operations Centres. While this study recognises the cognitive processes in SOC, such as data processing and reacting to threats, it primarily focuses on the role of AI/ML approaches in fulfilling these cognitive tasks rather than on improved integration with human operators. Similarly, León et al. [38] proposes an expert-aware traffic-characterisation and anomaly-ranking system to assist proactive troubleshooting in SOC operations, and Yue et al. [39] presents a multi-objective intrusion-response framework for industrial control systems that selects response strategies across network and physical layers. Both studies consider deployment and integration within operational technology stacks, yet remain largely technology-centric, with limited human-in-the-loop evaluation and little attention to governance and operator authority. Khayat et al. [40] presents the technical capabilities of AI to elevate SOC performance in data acquisition, detection, and processing, but similarly focuses on architectural design for a technology stack and does not address human factors or interaction directly. The absence of human-centric considerations in AI integration was also noted by Tilbury and Flowerday [7], who explicitly highlight it as a key research challenge in the current state-of-the-art.

The predominant focus of academic studies on the technological aspects of AI and its alignment with detection-related tasks [6] stems from several inherent and methodological factors. Detection is the most computationally traceable and benchmarkable domain, supported by the availability of labelled datasets and standardised metrics, aligning with academic incentives for reproducibility and quantitative rigour. Academic research, often led by computer science disciplines, prioritises technical novelty over operational integration, with limited access to real-world SOC environments and human-centric workflows. This tool-centric and siloed approach discourages exploration of broader CIM lifecycle phases such as response and recovery. Additionally, publication norms often favour narrowly scoped, automatable tasks, further reinforcing the emphasis on detection at the expense of governance, integration, and human-AI collaboration.

In the effort to bridge these gaps, our study focuses on industry-issued literature to examine how AI integration,along with its benefits and barriers,is perceived by leading cybersecurity organisations. This approach allows us to provide a structured analysis that not only reflects the technical directions of AI, but also incorporates human roles, contextual constraints, and operational outcomes. To guide this analysis, we adopt and contextualise the THTC framework (see Figure 1), which enables a multidimensional mapping of AI integration across socio-technical layers. By doing so, we aim to support the development of more responsive and practically relevant AI solutions for CIM.

3 Methodology

We address our overarching research question by conducting a document analysis of publicly available, non-peer-reviewed industry-issued literature relevant to the use of AI in CIM. To guide the analysis, we follow the epistemological position of contextual constructivism, which assumes

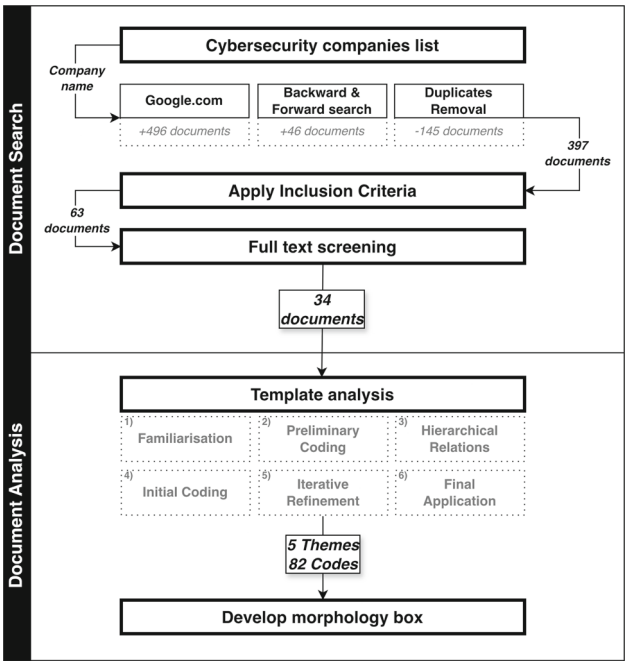

Fig. 2 Visualisation of document analysis methodology

that "there are always multiple interpretations to be made of any phenomenon, and that these depend upon the position of the researcher and the specific social context of the research" [[41], p. 4]. In line with this position, we adopt template analysis as it allows us to examine diverse perceptions and contexts within the selected documents, while also establishing a general understanding of the investigated domain [41].

The methodological procedure consisted of four key stages: (i) identification of relevant industry stakeholders, (ii) systematic document search using Google, (iii) application of selection criteria, and (iv) full-text review and coding. These steps are visualised in Figure 2.

3.1 Document corpus and search strategy

The document corpus was compiled through a systematic search for publicly available documents issued by industry stakeholders. In order to capture a wide range of industry perspectives, we conducted the systematic search of online documents using Google Search, following the approach of Chowdhury et al. [42]. We first identified 56 cybersecurity companies to drive the document search by merging results from: *"top AI cybersecurity companies list"* query. We then used this list to iteratively search for industry publications using the pattern: *"$company name$ + cybersecurity and AI and report and (2023 or 2024 or 2025) filetype:pdf"*. For each search query, we downloaded all documents from the first results page. We limited the time window to 2023–2025 to capture the immediate industry response to recent AI advances (such as generative AI[2]) and their implications for CIM, while keeping the dataset tractable. Importantly, the pattern was not strictly exclusive and several relevant pre-2023 documents (e.g., 2019–2022) were still included when they met the remaining criteria.

Table 1 Overview of analysed documents, classified by type and publication year

Document Type	2025	2024	2019–2023	Total
Company Research Reports	3	10	3	16
White Papers	1	8	1	10
Technology Viewpoints	1	1	0	2
Survey Results	0	4	0	4
Guidelines	0	1	0	1
Promotional Materials	1	0	0	1
Total	**6**	**24**	**4**	**34**

Note: Document types are classified using the GreyNet International taxonomy of grey literature (Available at: https://greynet.org/greysourceindex/documenttypes.html)

The initial search identified 496 documents, with an additional 46 manually added through backward and forward searches. After removing 145 duplicates, a total of 397 documents remained for screening. Documents were included in the analysis if they met the following criteria: (i) issued by an industry stakeholder (e.g., cybersecurity company, technology vendor, or professional organisation); (ii) publicly available in PDF format; (iii) relevant to CIM; (iv) addressed the use or implications of AI in cybersecurity; and (v) are published in English. The selected documents consist of grey literature such as white papers, reports, strategic outlooks, and best practice guidelines.

Out of the 397 screened documents, we excluded 334 for meeting one or more exclusion criteria (93 financial or market-oriented reports; 59 low AI appearance; 47 threat or technology forecast reports; 26 newsletter or magazine-style publications; 23 academic documents; 6 non-English), with the remaining 80 excluded items comprising short materials, transcripts, or other grey literature not addressing AI in cybersecurity incident management. The remaining 63 documents proceeded to full-text review. Of these, 34 were deemed relevant and included in the final analysis. Tables 1 2,3,4,5,6,7 provides an overview of the selected documents. Most were published in 2024 (24) and 2025 (6), with the remaining documents (4) spanning from 2019–2023.

3.2 Document analysis

In line with our epistemological position, we adopted the qualitative method of template analysis [41], focusing on

[2] ChatGPT was released on 30 November 2022.

establishing a hierarchical structure of recognised themes. The coding process was guided by an *a priori* template derived from the contextualised THTC framework (Highlighted in Fig. 1).

The first step of the analysis involved data familiarisation through skimming and close reading of the selected documents. Step 2 consisted of the preliminary coding using NVivo[3], applying the *a priori* template. This enabled establishing basic hierarchical relationships for the initial coding in step 3.

Step 4 involved developing an initial template based on a diverse subset of five documents, including two research reports, two survey studies, and one ethical guideline. Step 5 consisted of iterative application and refinement of the template as additional documents were incorporated. The structure was adjusted to reflect new themes and ensure comprehensive coverage. During this process, the coding structure was reorganised twice to merge overlapping codes and reduce complexity.

In Step 6, the finalised template was applied to the entire dataset. The coding structure was found to have converged, with no new themes emerging in the later stages of analysis, indicating that the template had reached sufficient saturation.

To organise and present the results, we utilised the concept of a *morphological box* [43], which allowed for a structured synthesis of the identified themes across the THTC framework dimensions. This process is presented in the following section.

4 Results

This section presents the results along the layers of the contextualised THTC framework. Specifically, Figure 3 synthesises the insights gained from the 34 analysed documents into a morphology that we created from thematic coding. We thereby expanded the original layers of the THTC framework with individual dimensions based on the factors that we identified in Section 2. Building on these dimensions, we then created sub-dimensions (e.g. Accountability) through the template analysis process. These represent the individual codes that group the documents in the dataset according to commonly recognised focus areas of integrating AI expert systems. In the following subsections, we elaborate on our findings for each thematic dimension and its sub-dimensions.

4.1 Context

Context was addressed by 26 documents (73.5%), making it the least represented of the five thematic layers. It encompasses the control measures and environmental considerations relevant to integrating AI technologies into CIM along the recognised sub-dimensions of *Governance* (22 documents, 64.7%) and *Risks* (24 documents, 70.5%).

Governance focuses on mechanisms for controlling and managing AI-based cybersecurity solutions. Among the identified sub-dimensions, *Auditing* stands out with a strong emphasis (18 documents, 81.8%), highlighting it as a key mechanism for controlling the integration and usage of AI for CIM. Thus, the industry frames auditing as a continuous process of monitoring and validation to ensure that AI systems meet operational objectives, team requirements, and resilience expectations. On the other hand, *Fairness* (36%) and *Legal Liability* (31%) emerge as the least-represented Governance sub-dimensions. Thereby, industry conceptualises fairness as the expectation that AI systems treat users and data equitably, supported by inclusive design practices and bias evaluations. By contrast, legal liability refers to the importance of assigning legal responsibility for AI actions, typically through regulatory compliance mechanisms and organisational safeguards - *"AI can offer significant advantages, but almost all CISOs surveyed (99.8%) believe there are multiple areas which require greater levels of regulation, particularly surrounding data privacy and protection and ethical use."* [D13].[4]

Finally, about half of the documents touch on the Governance sub-dimensions of *Accountability* (59%) and *Environment Understanding* (55%). Specifically, industry characterises accountability as the need to define responsibility for AI-driven cybersecurity systems across both development and deployment, with traceable and documented actions to support oversight and incident response. By contrast, environment understanding reflects industry's emphasis on aligning AI solutions with existing environments and workflows, ensuring a smooth integration that meets stakeholder needs.

Risks refer to concerns arising from the deployment of AI systems in cybersecurity operations. These risks are distinct from adversarial threats and focus on vulnerabilities introduced by the integration of AI technology into CIM itself. Thereby, industry puts a particular focus on *AI Introduced Vulnerability* (79%), capturing concerns about new risks introduced by AI deployment, such as model drift or data leakage [D16, D33], which require active mitigation. Further, about two-thirds of the industry documents are concerned about *Accuracy* (67%) and *Legal Risks* (67%). Thereby, the

[3] NVivo 14, developed by Lumivero, is a qualitative data analysis software. Available at: https://lumivero.com/products/nvivo/. Accessed: 30 May 2025.

[4] References in the format "[Dxx]" refer to the numbered industry publications available in Appendix Appendix B.

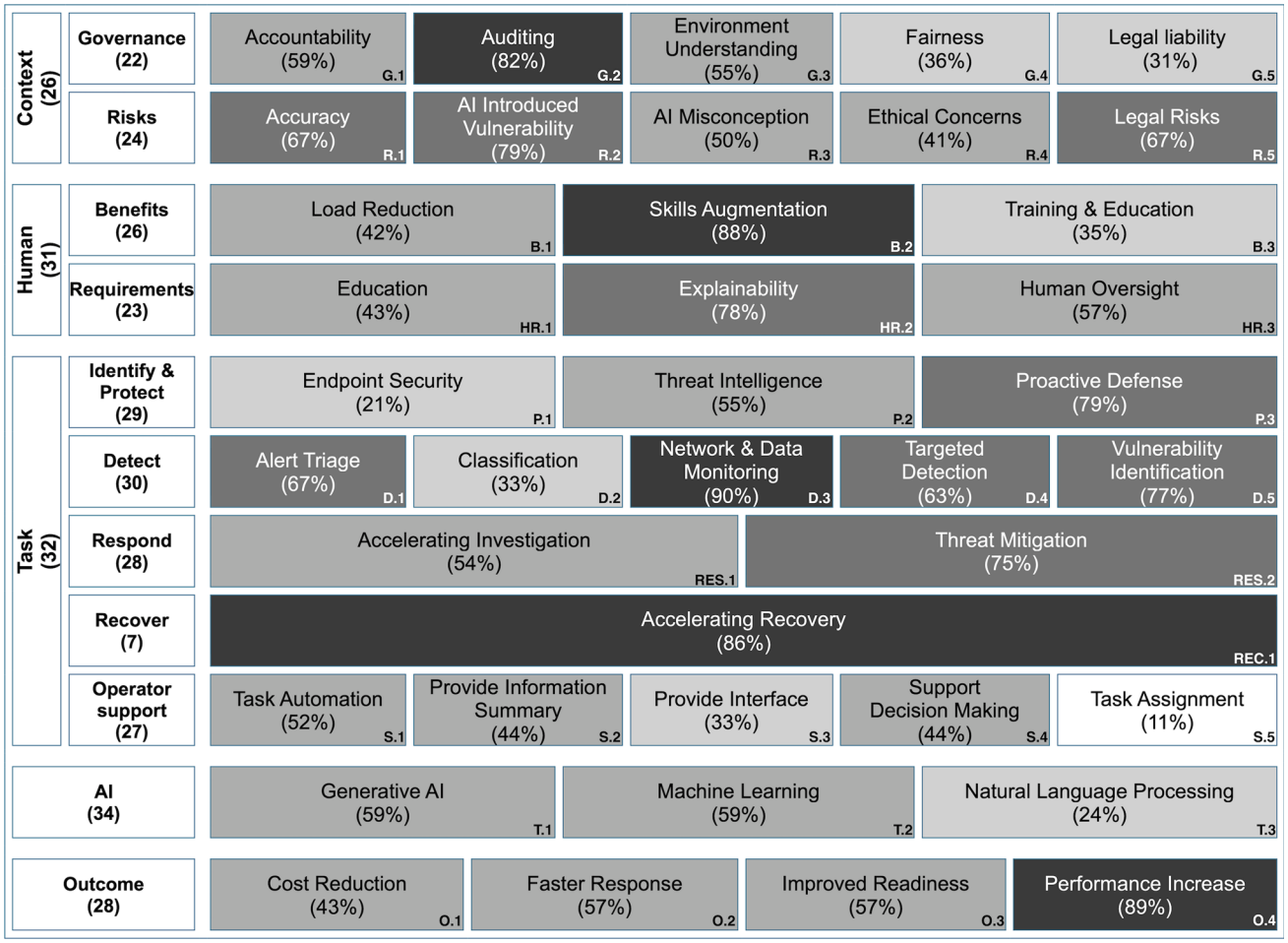

Fig. 3 Morphological box showing thematic coverage across the THTC framework from industry document analysis. Note: Colour-coded boxes indicate the proportion of coverage within each thematic layer. Percentages reflect the share of relevant documents per dimension (e.g., 32% of 22 documents address *Context–Governance*), not the full set of analysed documents

documents discuss accuracy in terms of maintaining reliable AI-human collaboration through well-defined performance metrics and ongoing monitoring. By contrast, legal risks are typically framed around data protection and compliance, with a strong focus on aligning AI systems with relevant regulatory standards.

Interestingly, the least emphasis in terms of risk is placed on *AI Misconception* (50%) and *Ethical Concerns* (41%). Specifically, the documents caution against unrealistic expectations or over-reliance on AI, which can lead to poor implementation and increased exposure to threats. Ethical concerns include issues such as bias, data privacy, and job displacement, which are seen as critical to address for responsible AI deployment - *"AI holds enormous potential to advance the way people live and work, but we must ensure that we apply these powerful tools ethically and sustainably."* [D27].

4.2 Human

Human layer was covered in 31 documents (91.1%). This layer encompasses documents providing perceptions on the implications of AI integration for cybersecurity professionals. Similarly, we structured the findings into two dimensions: *Human-Benefits* (76.4%), which addresses how experts can profit from the integration of AI technologies, and *Human-Requirements* (67.6%), which examines how their roles must adapt in response to the integration of these technologies.

Human-Benefits are discussed in terms of how AI supports and enhances the work of cybersecurity professionals. Overall, there is a strong industry consensus on the role of AI in *Skills Augmentation* (88%), where industry frames AI's role in enhancing decision-making capabilities, accelerating human investigations, and also as a possible solution to help address staffing and skill gaps - *"Cyber AI technology does not replace the human's function but rather serves to enhance it."* [D3]. Alongside this, industry recognises the potential

of AI to contribute to *Load Reduction* (42%), where AI is expected to take on selected tasks within CIM, thereby reducing the strain on cybersecurity experts. This is expected to free up professionals to focus on higher-priority activities and consequently contribute to improved team well-being. Finally, about a third of the documents describe AI's role in assisting with *Training & Education*, where AI contributes to dynamic learning, simulation, and testing. These capabilities of AI support skill acquisition and help maintain security awareness and posture.

Human-Requirements are discussed in terms of the evolving requirements and expectations imposed on cybersecurity professionals as AI becomes integrated into their workflows. In this regard, industry highlights a strong need for *Explainability* in AI technologies (78%), which is considered essential for enabling experts to audit AI decisions and maintain control over the automated process. Furthermore, explainability requirements are closely linked to accountability and transparency. A little over half of the documents (57%) recognise the need for *Human Oversight* of integrated AI technologies. Industry frames human oversight as a necessary safeguard in AI-assisted operations. Human experts are expected to supervise AI outputs to ensure that decisions remain accurate, ethical, and aligned with organisational goals - *"Given its relative novelty, it is crucial to keep humans involved in the decision-making process to ensure that actions are taken thoughtfully and appropriately rather than automatically initiating actions from the outset"* [D1]. Finally, parallel to the educational benefits, industry also recognises the introduced need for *Education* and further training (43%), where effective AI adoption is conditioned by the ability of cybersecurity professionals to understand AI systems and develop the required skillset for meaningful collaboration - "Security analysts, incident responders, and architects need to learn how to work with this new technology on a hands-on basis." [D5].

4.3 Task

The **Task** layer is the second most recognised within the dataset, with 32 documents addressing this area. Additionally, it is also the most detailed layer, having five dimensions recognised based on the adapted reference framework.

Identify & Protect use cases were covered in 29 documents (90%), making it the second most represented dimension of the Task layer, grouping tasks related to threat identification and prevention. Most prevalent is the recognition of AI's role in *Proactive Defence* (79%), where industry recognises the potential of AI technologies to transform the defence model from reactive to proactive by assisting with threat prediction, vulnerability identification, and improved adaptability through automated testing of security systems - *"AI provides a proactive solution, identifying threats before they can cause significant harm."* [D16]. Additionally, AI technology helps security teams with maintaining regulatory and policy compliance, and assists assessments and reporting. On the other hand, only a little over 20% of documents mentioned AI's role in *Endpoint Security*, where AI is deployed directly to the endpoint systems, enabling real-time monitoring, adaptive controls, and AI-powered malware protection. Last but not least, over half of the documents (55%) recognise the role of AI in *Threat Intelligence*, where AI can significantly reduce the workload of expert teams by assisting and automating threat hunting, information gathering, and generating actionable insights. Furthermore, with the ability to process vast datasets and correlate anomalies, AI helps security teams stay ahead of evolving threats with greater speed and precision.

Detect is the most covered dimension, with 30 documents (94%) providing insights across five recognised sub-dimensions. Usability of AI for *Networks & Data Monitoring* is the most frequently coded sub-dimension across the entire morphology, with 27 relevant documents. Industry conceptualises the role of AI in continuous monitoring and processing of large volumes of data with greater efficiency compared to human operators. This enhances infrastructure visibility and enables early detection of suspicious activities and system anomalies. Following monitoring, documents relate AI to the tasks of *Vulnerability Identification* (77%), *Alert Triage* (67%), and *Targeted Detection* (63%). Respectively, industry understands AI's role in automating the discovery of vulnerabilities and configuration errors, assisting security teams in managing and processing overwhelming volumes of alert data by filtering, and prioritising incidents based on severity and context, and using AI to detect specific types of incidents (such as malware, phishing, or insider threats) within monitored systems. In contrast, the capability of AI solutions to assist with *Classification* is described in only one third of the documents, presenting AI's potential to classify threats, anomalous behaviours, and data types into structured categories - *"Unsupervised machine learning has the potential to independently classify data and detect compelling patterns, instead of relying on knowledge of past threats."* [D3].

Respond & Recover dimensions exhibit the lowest sub-dimension granularity. While *Respond* is covered in 28 documents, *Recover* stands out as the least represented, appearing in only 7 documents.

Three quarters of documents recognise AI's role in *Threat Mitigation*, where, alongside detection, AI can automate the containment, mitigation, and response to identified vulnerabilities and detected incidents, reducing the impact of attacks by recommending or executing remediation steps. Alongside this, industry highlights the AI role for *Accelerating Investigation* (over 50% of documents), through automating data analysis, correlating monitored data, and generating incident

summaries - *"AI can use natural language processing to make decisions and extract the information needed during investigations."* [D17]. AI supports security teams in investigating incidents more efficiently, improving timely response and the quality of extracted insights.

Similar benefits are recognised in the case of *Accelerating Recovery*, where AI can support faster and more reliable recovery by optimising backup processes, automating remediation, and enabling system restoration - *"Post attack, our AI allows businesses to recover from cyber-attacks and get back to full operations faster and more confidently than a human team can alone."* [D7]. Accelerating post-incident analysis and investigation helps to orchestrate and accelerate recovery workflows. However, it is the only recognised sub-dimension for the recovery dimension, highlighting limited industry focus and perception.

The final Task dimension of **Operator Support** gathers recognised sub-dimensions which structure document insights on how AI can assist security teams in their daily operations. A little over 50% of documents present AI's role in *Task Automation*, where it can significantly reduce the workload of security teams by automating repetitive and time-consuming tasks, such as the previously mentioned alert triage. Both *Support Decision Making* and *Provide Information Summary* are covered by the same number of documents (44%), where, alongside previously mentioned processing, AI's role is to provide contextual insights and present analysts with higher-quality information, clear summaries of incidents or alerts, and actionable recommendations. This results in more informed decision-making and skillset development, particularly for junior analysts. Furthermore, beyond summarisation, industry presents AI's role in *Providing Interface*, where it acts as an interface between various tools and systems within the security workflows, offering more intuitive interactions and tailoring tools to specialised tasks, improving the utilisation of expert time and accessibility. Notably, *Task Assignment* stands out as the least represented, addressed in only 11% of the documents, which describe AI's role in direct assignment of tasks to team members - *"Assign incident response duties: AI can automatically assign engineers, based on expertise and availability, so they can better respond to an incident based on its nature."* [D2].

4.4 Technology – AI

AI technology represents the thematic layer covered by all documents, as its mention was one of the inclusion criteria for document selection. The understanding of the term *Artificial Intelligence* is limited within the analysed documents, with some referring to Artificial Intelligence only in a general sense (as "AI"). However, three particular AI subdomains were recognised within the documents.

Generative AI, covered in just under two thirds of the documents, is increasingly recognised as a tool to augment cybersecurity operations by automating content creation, testing procedures, incident summaries, and training materials. It is also understood as an intelligent interface in the form of chatbots, assisting operators with decision-making by managing and contextualising knowledge - *"Some security solutions come with AI chatbots that act as assistants to capacity-challenged security analysts."* [D2]. *Machine Learning*, covered by an identical proportion of documents (59%), is widely recognised as a key enabler for processing large volumes of data to detect threats, anomalies, and vulnerabilities. Industry often distinguishes between supervised and unsupervised learning approaches, alongside the broader subdomain of deep learning. Finally, connected to Generative AI, the sub-dimension of *Natural Language Processing* is recognised in roughly one quarter of the documents. It is described as enabling systems to interpret and generate human language, assisting with interaction or reporting - *"AI-driven natural language processing provides a clear explanation of the actions taken."* [D7].

4.5 Outcome

Outcomes of AI integration were discussed in 28 documents, making it the second least addressed thematic layer. Primarily, industry highlights AI's role in *Performance Increase* of CIM processes (89% of documents), where AI-based augmentation elevates the skill levels and capacity of security teams in fulfilling their roles - *"Gen AI revamps SecOps by enhancing the current SOC capabilities, aiding in automation, data interpretation, suggesting best practices."* [D1].

Industry focuses (57% of documents) on AI implications for *Improved Readiness*, connecting AI's role in monitoring, proactive defence, and skills augmentation with enabling security teams to face more advanced threats and strengthen overall cybersecurity posture. Moreover, together with improved readiness, 57% of documents also highlight the benefits of AI integration for *Faster Response*, where AI reduces the mean time to detect (MTTD) and respond (MTTR) to threats - *"Real-time incident response: AI tools can provide immediate responses to incidents, often faster than traditional human-led processes."* [D16]. Finally, *Cost Reduction* is the least frequently mentioned sub-dimension, with just under half of the documents recognising that AI-enabled automation improves resource allocation and helps address workforce shortages.

While industry widely recognises these benefits, their realisation depends on a clear understanding of the environmental factors that shape AI system deployment. Specifically, the interplay between the *Context* dimension, the evolving *Human* role, and the structure of the CIM process. These

dependencies are further examined in the co-occurrence analysis (Section 4.6), which synthesises the relationships between thematic layers and clarifies how industry perceives the role of cybersecurity experts when interacting with AI.

For additional and detailed statements aligned with the developed morphology box, we refer the reader to Appendix A, where they are presented in correspondence with the numbered sub-dimensions from the morphology (Figure 3). The list of analysed industry publications is provided in Appendix B. Finally, following the approach of [44], we provide an interactive online tool [5] for the morphology box, enabling filtering of results according to the morphology.

4.6 Conceptual Foundations for Human Role in AI-Driven Cybersecurity

During the coding process, we found that individual statements from the documents often linked to two or more morphology dimensions. To further explore these relationships, we compiled a co-occurrence matrix of the respective themes. As shown in the visualisation in Figure 4, the matrix highlights thematic areas that frequently appeared together and reveals dependencies between thematic domains. This shows how different dimensions, such as human roles, technology, and governance principles, interact in practice and shape the industry's conceptualisation of human-AI collaboration.

Building on this matrix, we identify two distinct clusters connected via the technology layer: the left-hand side links to governance-related codes relevant to AI integration, such as Accountability, Auditing, and Explainability, whereas the right-hand side connects to task-oriented applications and operational outcomes. Furthermore, the strength of association between individual nodes reflects the importance of each conceptual domain and its level of recognition from the industry perspective. For example, the strong links between Generative AI, Machine Learning, and individual tasks of CIM highlight how frequently these technological directions are acknowledged in recent industry literature.

Following overview outlines the conceptual directions in understanding the human role in AI-powered cybersecurity operations from industry perspective:

> ***Human as Controller*** Industry positions the human expert as responsible for the oversight and governance of AI technologies in cybersecurity operations. This role is underscored by the strong interconnection between the requirements of Explainability and Human Oversight with Auditing, Accountability, and Fairness from the Governance dimension.

> ***Human as Beneficiary*** Industry also frames the human expert as a beneficiary of AI integration, supported through enhanced task execution, operational outcomes, and skill augmentation. This is reflected in the co-occurrence of individual tasks, human benefits, and the outcomes of AI integration.

The co-occurrence patterns provide a structured view of how thematic dimensions and sub-dimensions interact in practice, providing a more in detail insight into how industry perceives AI integration. Additionally, it offers a foundation for identifying integration gaps and guiding the development of responsive AI solutions.

5 Recommendations for AI Integration in CIM

The preceding analysis used the THTC framework to structure the industry's perception of AI expert systems integration in CIM into a morphological box, capturing operational expectations, contextual constraints, and human-centric needs. Building on this structure, we present a set of industry-oriented recommendations for developing AI systems for CIM, organised according to the five contextualised layers of the THTC framework. In addition to operational requirements, we explicitly consider the ethical implications of AI integration, including trade-offs between performance gains and risks such as bias, over-reliance, and reduced human oversight.

The results suggest that industry pays limited attention to governance structures, ethical safeguards, and legal accountability, indicating a need for clearer integration policies within the *Context* layer. Within the *Human* layer, the industry clearly recognises the role of human experts as controllers, with a strong emphasis on explainability and oversight. This recognition reinforces the industry's conception of AI integration as a *human-in-the-loop* process. However, there are opportunities to further develop and apply AI for training and educational purposes. The *Task* layer reveals uneven coverage: while detection use cases and threat identification tasks are well represented, the *Respond* and *Recover* dimensions exhibit low granularity. Although response-related tasks are mentioned more frequently, the limited detail suggests a shallow understanding and highlights opportunities for further development. The potential of AI to assist with *Task Assignment* is also under-explored. In the *Technology* layer, frequent mentions of Generative AI reflect its rapid adoption, yet concerns about over-reliance and improper deployment persist. Finally, although the *Outcome* layer highlights benefits such as improved performance and cost reduction, their successful

[5] The interactive tool is available at: https://jkincl.github.io/interactive_labeling_DA_UON/

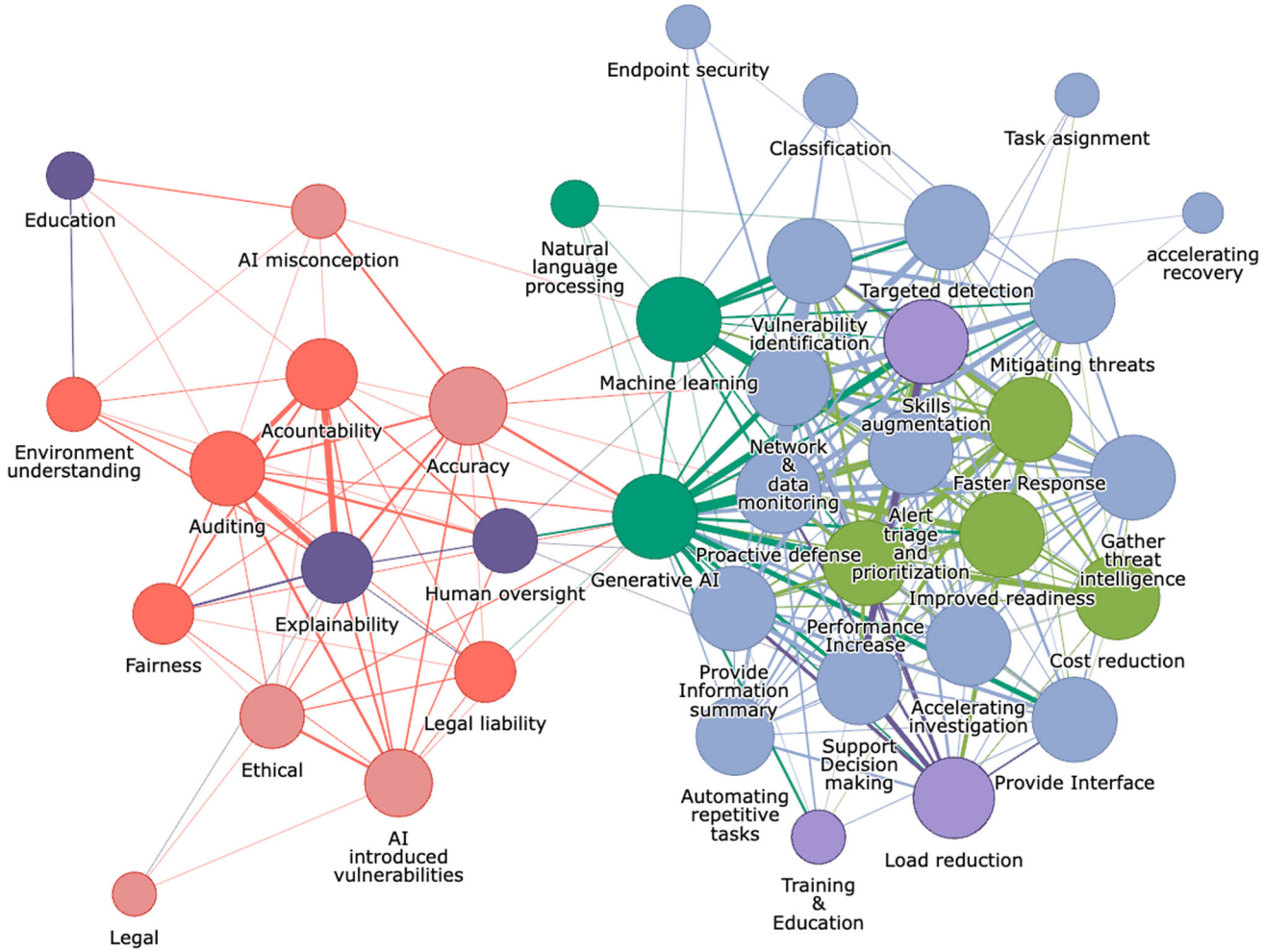

Fig. 4 Visualisation of co-occurrence matrix of morphology codes. Note: Figure is colour coded according to the five THTC framework layers; (1) Context - Red (Governance), Light Red (Risks), (2) Human - Purple (Requirements), Light Purple (Benefits), (3) Task - Blue, (4) Technology - Dark Green, (5) Outcome - Light Green; Node size reflects code frequency; edge thickness indicates co-occurrence strength

realisation depends on a clear understanding and alignment of operational and human factors.

We outline the following recommendations based on the identified gaps, connecting the principles and requirements identified during the analysis of industry perception. These recommendations can assist stakeholders in embedding AI capabilities into existing CIM workflows and provide guidance for the future development of AI systems for CIM.

RCM1 **Enable Auditability & Accountability** AI systems for CIM must enable full auditability and clearly assigned accountability from model development to operational use. The CIM team must be able to understand why an output was produced and use this information during analysis, decision-making, and reporting.
Integration consideration: meeting auditability requirements supports human control and confidence. Clear visibility of decisions and data use helps operators verify outputs, develop appropriate skills, and maintain trust in the system without slowing down their work.

RCM2 **Provide Governance & Risk Modelling by Design** AI systems must support governance processes already established within CIM teams, including policy adherence, emergency fallback options, and human override. Risk modelling should address not only technical risks (e.g., drift, poisoning, leakage) but also integration-related risks: what training operators need, how roles and responsibilities are affected by AI integration, and how tooling might be used incorrectly (e.g., over-reliance or detachment from the task).
Integration consideration: effective governance ensures that AI complements team practices rather

than disrupting them. Training and clear role definitions are essential for successful adoption.

RCM3 **Ensure Operational Integration & Compatibility:** AI systems must integrate with existing CIM tools, data formats, and workflows, and be adjustable to sector-specific and organisational constraints. The system should adapt to the team's operational context and maturity rather than forcing analysts to change how they work.
Integration consideration: AI must not introduce additional barriers, parallel workflows, or extra overhead. Its integration should streamline tasks, reduce fragmentation, and support efficient collaboration within the team.

RCM4 **Maintain Human-Centric Design & Oversight:** The primary purpose of AI integration in CIM is human augmentation. Interfaces and outputs must be understandable, practical, and suited to how analysts investigate, verify, and act. Human-in-the-loop oversight must remain central.
Integration consideration: usable explanations and clear interaction points help operators stay in control, maintain awareness, and build skills. AI must aim to support decision quality, reduce unnecessary load, and adapt to different experience levels within the team.

RCM5 **Ensure CIM Lifecycle & Goals Alignment:** AI capabilities should map onto clearly defined CIM lifecycle phases (e.g., Identify, Protect, Detect, Respond, Recover) and be modular to avoid overuse or misapplication. Different tasks may require different methods, and not all tasks benefit from automation to the same extent.
Integration consideration: aligning AI with team goals ensures that it supports actual workflows, including phases that are often underrepresented (such as response coordination or recovery).

RCM6 **Embed Legal and Ethical Compliance:** AI systems must comply with applicable regulatory and organisational requirements (e.g., GDPR, HIPAA, ISO/IEC 22989:2022 [45]). This includes data protection, purpose limitation, transparency, and documentation obligations, as well as ethical expectations around fairness and accountability.
Integration consideration: compliance safeguards not only protect the organisation but also ensure that analysts can use AI outputs confidently without legal or procedural ambiguity.

RCM7 **Support Resilience and Adaptive Defence:** AI systems deployed in CIM must remain stable under changing operational conditions, evolving threats, and updated organisational goals. They should handle drift, degradation, and adversarial pressures and be maintainable through updates and retraining.
Integration consideration: resilience includes the ability to adjust to new contexts, support updated workflows, and incorporate feedback from human operators. This ensures that the AI solution remains useful throughout changes in teams, tooling, or priorities.

The recommendations focus on providing actionable design considerations for improving the alignment of AI solutions with the practical realities of CIM. They are grounded in the results of the template analysis, which identified recurring themes and sub-dimensions that formed the morphology structure.

Explainability as a practical integration principle

While fully transparent and inherently interpretable AI models remain a significant technical challenge, our recommendation to adopt explainability in cybersecurity contexts does not assume the immediate availability of perfectly explainable systems. Instead, explainability should be understood as a spectrum of transparency-enhancing practices, including interpretation methods, confidence indicators, decision traceability, and structured audit logs. Even if complete algorithmic transparency proves unattainable, these mechanisms can meaningfully support accountability, human oversight, and regulatory compliance. In high-stakes cybersecurity environments, explainability therefore functions not as an absolute technical requirement, but as a risk-mitigation principle complemented by governance controls and human-in-the-loop decision-making.

The proposed recommendations span governance, human roles, task alignment, technological capabilities, and expect ed outcomes, and are mapped to the five thematic layers of the contextualised THTC framework. Figure 5 visualises the alignment with each recommendation linked to to the relevant thematic layer of the THTC framework based on its associated sub-dimensions.

This mapping illustrates how both the recommendations and the industry's operational expectations are distributed across the reference framework. The colour-coded structure also highlights the multidimensional nature of AI integration, showing how individual recommendations often span multiple layers. This visualisation supports both planning and implementation by helping practitioners identify relevant requirements, define system scope, and align design approaches with industry needs.

Ethical Implications of AI Integration in CIM

While the proposed integration specifications emphasise operational alignment and system design requirements, it is equally important to critically assess their broader ethical implications. AI-driven integration in CIM offers clear advantages, particularly in terms of improved efficiency,

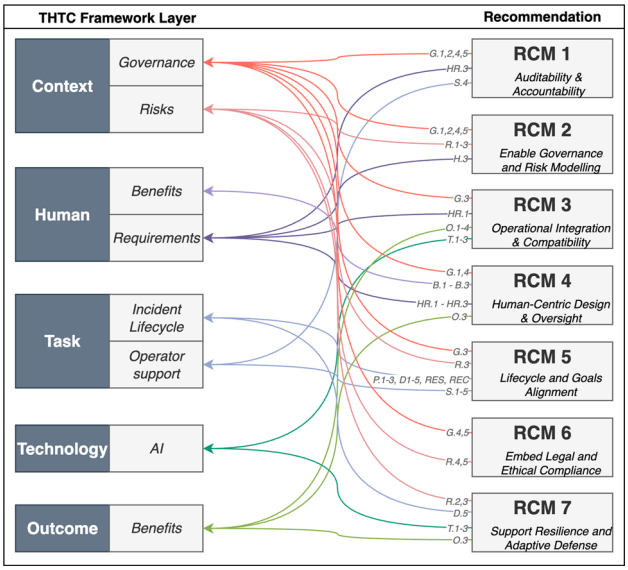

Fig. 5 Mapping between contextualised THTC framework and recommendations. Note: Connectors are colour coded according to the five THTC framework layers;(1) Context - Red (Governance), Light Red (Risks), (2) Human - Purple (Requirements), Light Purple (Benefits), (3) Task - Blue, (4) Technology - Dark Green, (5) Outcome - Light Green;

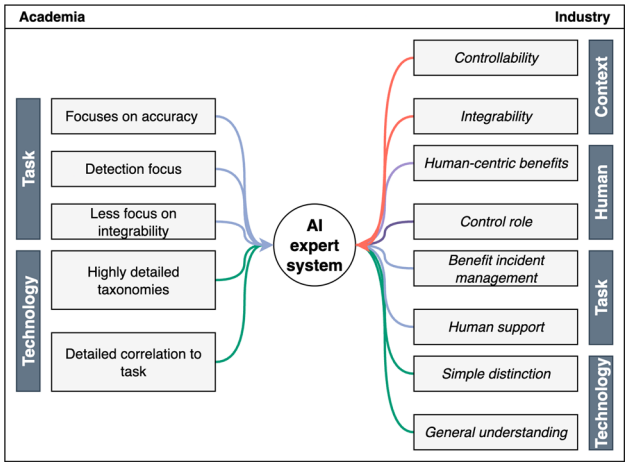

Fig. 6 Comparison of academia and industry perceptions on AI systems in CIM. Note: Connectors are colour coded according to the five THTC framework layers;(1) Context - Red (Governance), Light Red (Risks), (2) Human - Purple (Requirements), Light Purple (Benefits), (3) Task - Blue, (4) Technology - Dark Green, (5) Outcome - Light Green;

scalability, and faster response times, as reflected in the identified Outcome dimensions such as performance increase and improved readiness. These benefits can reduce cognitive load on analysts and enhance organisational resilience.

However, these advantages are accompanied by notable risks. As identified in the Context-Risks dimension, AI systems may introduce vulnerabilities such as biased decision-making, data quality dependencies, and potential misclassification of threats, which can negatively impact operational outcomes. Furthermore, the findings highlight concerns related to over-reliance on automation and misconceptions about AI capabilities, which may lead to reduced human vigilance and inappropriate trust in system outputs. Importantly, the integration of AI raises questions of accountability and human oversight. While industry emphasises the role of humans as controllers of AI systems, ensuring explainability and auditability, insufficient governance mechanisms may result in unclear responsibility for AI-driven actions and decisions. This is particularly critical in high-stakes cybersecurity contexts, where errors can have significant organisational consequences.

Therefore, effective AI integration must balance performance gains with safeguards that preserve human agency, ensure transparency, and mitigate ethical risks. This includes maintaining human-in-the-loop decision-making, addressing bias through continuous evaluation, and preventing over-automation that could erode expert judgement. By explicitly considering both benefits and drawbacks, the proposed integration framework supports a more responsible and ethically grounded deployment of AI in cybersecurity incident management.

6 Discussion

This study examined how the cybersecurity industry frames the integration of AI for cybersecurity incident management and what this implies for human–AI teaming, governance, and workflow fit. Through a template analysis on a diverse set of industry-issued documents, we identified themes, operational priorities and human-oriented risk posture changes that shape the deployment and evaluation of AI systems in practice. We compare academia and industry perspectives, summarise theoretical and practical contributions together with actionable recommendations grounded in the contextualised THTC framework.

6.1 Academia-Industry Alignment

Building on the insights from the template analysis and co-occurrence matrix, this subsection compares the industry focus and perspective with the academic focus outlined in Section 2.2. While both domains recognise the importance of AI integration in CIM, they differ in terms of priorities, conceptual framing, and evaluation criteria, which may result in misaligned research efforts. Figure 6 provides a simple comparison between academia and industry, illustrating the observed differences.

As stated by Kaur et al. [6] academic works often focus on detection issues or technical specificity. This is often reflected in the development of detailed taxonomies of AI technologies [e.g.15] and efforts to correlate specific algo-

rithms with particular CIM tasks. In contrast, the industry literature prioritises practical implementation concerns. Documents frequently omit technical specificity, referring to AI technologies in general terms and places greater emphasis on interoperability, explainability, governance requirements, evolving role of security operators, and seamless integration into existing workflows.

Despite these differences, both domains recognise a similar corpus of tasks in CIM, likely influenced by the widespread adoption of standardised frameworks such as NIST CSF [46]. The academic perspective remains more detail-oriented, while the industry perspective is guided by principles of integration. Both domains stand to benefit from closer alignment: industry could adopt more structured and detailed taxonomies, while academia could enhance the practical relevance of its research by addressing contextual constraints and incorporating human-centric design considerations.

6.2 Theoretical and Practical Contributions

To support both future development and better industry and academia alignment, the study makes three core contributions for researchers by clarifying how the findings translate into human–AI integration and the associated risk posture within CIM, thereby helping to bridge the gap between research and practice.

Industry posture and human role

First, the study provides a structured synthesis of the industry perspective (see Figure 3). Using template analysis, it identifies under-explored areas such as AI support for recovery and task assignment, followed by highlighting governance, contextual compatibility and integration challenges. Furthermore, the co-occurrence matrix shows that industry positions expert operators as controllers and beneficiaries when interacting with AI. In other words, industry treats humans as both responsible for oversight of AI and as direct recipients of augmentation. This sets the expectation that AI should fit existing processes and provide human-controllable safety measures, rather than create additional tasks for operators.

Human–AI integration

Second, our findings complement existing academic reviews by revealing key differences in focus and evaluation criteria. While academic work often prioritises novelty, industry places strong emphasis on operational integration, explainability, and human-in-the-loop design. This further confirms the importance of the limitations identified by Binbeshr et al. [37] and recent human–AI interaction studies [27], which call for a shift towards interactive AI, centring user-focused, human-in-the-loop design as crucial [47]. Consistent with the shift of human role for AI-augmented systems, our results emphasise decision traceability, usable explanations that support analyst judgement and learning, and the minimising of integration barriers, so that augmentation and human control can co-exist without introducing parallel workflows.

Risk posture and recommendations

Third, the findings are synthesised into a set of seven actionable recommendations. These recommendations not only consider the operational needs, principles, and constraints identified in the industry literature, but also reflect the risks related to human-AI integration when AI is used to augment human operation. We present the recommendations explicitly as *integration requirements* aligned with recognised human-centric principles (see Section 2.3) and the limitations highlighted by Tilbury and Flowerday [7], providing guidance for developing systems that are integrable, explainable, and responsive to real-world CIM environments. Furthermore, the recommendations offer a structured approach for mapping the CIM environment and informing system design across governance, human interaction, task alignment, technological capabilities, and expected outcomes. In terms of risk posture, the recommendations go beyond technical weaknesses (e.g., drift or hallucinations) and make explicit the human-role risks, such as: over-reliance, detachment from the task, skill atrophy, and the need for structured training during AI adoption-so that augmentation and human control can co-exist without introducing parallel workflows or operational burden. Taken together, the recommendations are intended to help researchers and practitioners align AI capabilities with practical team needs while safeguarding operator performance and accountability.

6.3 Limitations and Future Work

While this study provides a systematic overview of how AI is discussed and positioned in the cybersecurity industry, it has several limitations that should be considered when interpreting the findings. First, the analysis was limited to 34 publicly available, industry-issued documents. Although this corpus captures diverse viewpoints from different companies and sectors, it may not fully represent proprietary practices or internal decision-making processes that are not disclosed in public materials. Second, the study relied on qualitative coding within the adapted THTC framework, which, while allowing for rich thematic analysis, introduces the possibility of interpretive bias. Although cross-checking and iterative coding were applied, other researchers might arrive at slightly different categorisations or emphasis. Third, the focus on documents published between 2023 and 2025 means the results reflect a specific period of technological and market maturity; given the rapid evolution of AI capabilities, particularly in generative models, the industry's priorities and framing may shift significantly in the near future. Finally, while the THTC framework provided a robust analytical

structure, its application in this context was adapted for cybersecurity AI, which may require further refinement or validation when applied to other domains.

To address these limitations, future research may expand the dataset to include interviews, surveys, or observational studies with cybersecurity practitioners in order to offer deeper insight into lived experiences and operational constraints. Moreover, longitudinal analyses can be performed to track how industry discourse changes over time, particularly as AI technologies mature and regulatory landscapes evolve. This may lead to further extension of the analytical framework to also integrate quantitative performance metrics, governance maturity models, and cross-sectoral perspectives and enhance both the explanatory power and the practical applicability of the findings. Future work should evaluate human–AI integration not only by technical metrics but also by operator-centred measures (e.g., decision quality, task engagement, and training outcomes) in real SOC workflows. Finally, as the established industry perception shows limited consideration for human cognitive and affective dimensions in AI integration, more research efforts should be directed towards AI-assisted human management (such as task assignment), as well as the cognitive and emotional factors that shape how security professionals engage with AI systems. Such efforts would not only validate and enrich the results of current study, but will also support the development of AI systems that are better aligned with the complex socio-technical realities of cybersecurity incident management.

7 Conclusion

This study provided a structured synthesis of the industry perspective on AI expert systems integration into cybersecurity incident management (CIM). Using the adapted THTC framework as the analytical lens, we examined AI's role across technological, human, task, contextual, and outcome dimensions. The analysis revealed that while AI is widely acknowledged for its potential to enhance detection and certain automation capabilities, industry narratives also highlight the importance of human oversight, integration with existing workflows, and alignment with regulatory and operational contexts for successful human–AI integration in practice. The study identified notable gaps, including limited attention to recovery processes, comprehensive governance structures, and the full spectrum of incident management tasks. With that, this research contributes to a more holistic understanding of how AI is envisioned in practice and where future development should focus. Taken together, our results position AI not as a stand-alone solution for CIM practice but as *augmentation under human control*, with operator needs, governance instrumentation, and workflow alignment as top-priority requirements. Explainability should be treated as a spectrum (decision traceability, confidence indicators, post-hoc interpretation, audit logs) that mitigates risk even when full model transparency is not feasible. Accordingly, our recommendations highlight the human-AI integration requirements, reflecting the need for auditability, human governance, alignment with existing workflows, and necessary resilience. In doing so, they aim to help human teams adopt AI without introducing new barriers. We hope that the insights from our work can serve as a shared frame of reference for researchers and practitioners, helping ensure that AI adoption in cybersecurity is effective, responsible, and aligned with industry needs.

Acknowledgements Funding to support this research work was provided by: Slovenian Research Agency: research core funding No. P2-0037; and non-Commonwealth University of Newcastle scholarship.

Author Contributions Conceptualization: Jan Kincl, Marc T. P. Adam, Tanja Pavleska; Methodology: Jan Kincl, Marc T. P. Adam, Tanja Pavleska; Data curation: Jan Kincl; Formal analysis: Jan Kincl; Investigation: Jan Kincl; Validation: Jan Kincl, Marc T. P. Adam, Tanja Pavleska; Visualization: Jan Kincl; Writing - original draft: Jan Kincl; Writing - review & editing: Marc T. P. Adam, Tanja Pavleska; Resources: Marc T. P. Adam, Tanja Pavleska; Supervision: Marc T. P. Adam, Tanja Pavleska.

Data Availability No datasets were generated or analysed during the current study.

Declarations

Competing Interests The authors declare no competing interests.

Appendix A Example Statements

Context

Table 2 Selected statements from industry documents coded under the Context layer during template analysis

Layer	Dimension	Sub-Dimension	Statement
Context	Governance	Accountability	*"Establishing a dedicated team or department to oversee AI governance at the organizational level is crucial."* [D1]
			"The critical aspect of the plan is to communicate clear ownership across cross-functional teams within the enterprise." [D10]
			"Without properly documenting decisions and assigning responsibility, determining the liability for unexpected behavior or misuse might not be possible." [D26]
			"Controllable. Security teams should be able to decide on the role humans play in decision-making. They should also be able to customize models and set thresholds to guide how decisions are made." [D4]
		Auditing	*"Conduct regular reviews of your cybersecurity strategy and AI policies to adapt to evolving threats and technological advancements."* [D1]
Accountability			*"In the development cycle, there must be detailed audit of AI models. This will help enterprises address privacy and ethical issues early, thereby strengthening confidence among end consumers, stakeholders, and employees."* [D10]
			"Conduct regular cyber range exercises using adversarial techniques to try to breach the AI system. These exercises serve to both test and improve the resilience" [D2]
			"If the metrics do not measure the risk as intended, then the understanding of that risk will be incorrect, and mitigations may not be appropriately applied." [D26]
			"Testing and validation is crucial to ensuring accurate outcomes." [D7]
			"Organizations must also incorporate security testing, protection, and monitoring of their AI/ML models." [D30]
		Environment Understanding	*"Collaboration among IT teams, legal experts, business leaders, and other stakeholders within and outside the organization, pooling knowledge, experience and resources, is crucial."* [D1]
			"SOC teams look for tools that are designed to seamlessly fit into SOC analysts' existing workflows: 88% agreed that the adoption of solutions will be dependent on those solutions' ability to integrate seamlessly into established SecOps processes." [D11]
			"Integrating AI with existing security infrastructures and workflows can transform operations, bringing better solutions and insights. But it is a complex process, requiring thoughtful, strategic planning and execution to ensure it doesn't disrupt ongoing operations." [D2]
			"Cisco's AI Security Incident Collaboration Playbook will help coordinate AI security incident response between governments, industry peers, and global partners to drive toward a more secure future." [D29]
			"Understanding business context is essential for identifying the security needs of AI." [D27]
			"Personalize security for every organization, since risks depend on unique attributes like users, infrastructure, and assets" [D3]
			"AI can't replace humans, but humans can't replace AI, either. These solutions must include ways to securely integrate AI-based instruments into the corporate IT landscape." [D6]
		Fairness	*"Usage of AI for Cybersecurity should actively involve all the AI stakeholders, including security team members, SOC (Security Operations Center) analysts, threat hunters, privacy experts, users, developers, vendors, and business leaders"* [D10]
			"Gen AI raise important questions regarding data governance, intellectual property (IP), bias mitigation, and responsible utilization of AI-generated content." [D1]
			"In 2018 Cisco published our commitment to respect human rights in the design, development, and use of AI. In 2022, we formalized this commitment by launching our Responsible AI (RAI) Principles, which we operationalize through our RAI Framework." [D29]
			"Diverse datasets and continuous evaluation against bias are required to ensure fairness in AI models and equitable and accurate outcomes across different demographics and scenarios." [D2]

Table 2 continued

Layer	Dimension	Sub-Dimension	Statement
		Legal Liability	*"Companies must implement robust cybersecurity and regulatory compliance policies."* [D23]
			"If ownership or responsibility for development of the model is uncertain, regulators and others may have concerns about the model because it will not be clear who is - or should be - liable/responsible for problems with it or can answer questions about it. Users of models without clear ownership may find challenges with compliance with future AI regulation." [D26]
			"Organizations face significant regulatory hurdles in the implementation of Gen AI, especially for use cases related to cybersecurity." [D9]
			"Additionally, we need to introduce the appropriate level of governance in both development and usage to ensure trustworthy AI." [D27]
	Risks	Accuracy	*"Monitoring for model drift over time and recalibrating the models will ensure the output is reliable."* [D1]
			"It's easy to say a security product uses AI or ML. But it's not so easy to gather and analyze the huge amounts of data required to detect patterns, spot anomalies, and stay on top of the constantly changing threat environment." [D14]
			"AI models can inherit biases from the data they are trained on, leading to misclassification of threats or even overlooking certain types of attacks." [D16]
			"AI systems can misinterpret data or fail to recognize nuanced threats." [D19]
			"Data is central to AI-enhanced threat hunting, and that data - network traffic logs, user behavior, system logs, etc. - must be collected, consolidated, and cleaned before it can be analyzed." [D2]
			"AI threat detection models must be scrutinized to avoid skewed results." [D2]
			"Security professionals are wary of implementing AI due to concerns about data quality, transparency, data poisoning" [D20]
			"Any mislabeled data or human bias introduced can seriously compromise the ability of the system to correctly classify new activities." [D3]
			"If not applied responsibly, generative AI can cause confusion by hallucinating, where it references invented data, or by providing conflicting responses due to confirmation bias in the prompts written by different security team members." [D3]
		AI Introduced Vulnerability	*"However, the integration of AI into cybersecurity also introduces new challenges and risks, such as the potential for AI systems to be manipulated, creating vulnerabilities."* [D16]
			"Sensitive or confidential information may be uploaded into an AI model with little to no thought about the long-term implications." [D2]
			"Securing AI systems demands early mitigation, ongoing operational security, enterprise-level risk management, and frequent reassessment of vulnerabilities." [D27]
			"While AI holds the potential to deliver transformative advancements, it also brings unique vulnerabilities, such as data poisoning, model evasion attacks, and ethical concerns, which could compromise the integrity and security of AI systems." [D33]
		AI Misconception	*"On the other hand, there are persistent misunderstandings about what AI is, what it can do, and why choosing the right type of AI is so important. Only when those popular misconceptions have become far less widespread can our industry (cybersecurity) advance its effectiveness."* [D4]
			"Start with a compatibility assessment to point out technical challenges, including data formats and communication protocols. It may also help to adopt modular AI that be easily plugged into existing systems and AI tools that support leading standards for a more seamless integration." [D2]
			"Inappropriate selection and choice of the most appropriate AI-empowered digital transformation and cybersecurity solutions for the organisation's unique needs - leading to non-optimal implementation of IT investments, as well as human error in the usage and training of employees for optimal returns on investments and risk elimination." [D18]
			"The risk is that an organization may think that they need more technology and fewer experts. But the opposite is true. Automated systems lack the human intuition and context needed to evaluate the level of risk and the importance of a particular alert." [D2]

Table 2 continued

Layer	Dimension	Sub-Dimension	Statement
		Ethical Concerns	*"Other risks have an ethical nature and must be considered carefully so that the technology has a positive impact."* [D26]
			"The top three risks CISOs foresee from their own organizations using GenAI are the ethical & social implications, reliability of results/ misinformation, and data leakage." [D13]
		Legal Risks	*"AI systems handle large volumes of sensitive data. It is crucial to ensure the security and privacy of this data to prevent leaks and misuse. Companies must implement robust cybersecurity and regulatory compliance policies."* [D23]
			"There are also compliance issues - such as GDPR in the European Union - and data privacy concerns to consider ensuring that personal data is not processed without individual consent." [D2]
			"AI-related data privacy breaches are seen as a significant threat by 97% of surveyed professionals, with nearly two in five (37%) considering them very significant" [D28]
			"Most importantly, AI should be transparent, explainable, and privacy-preserving." [D4]

Note: This table presents statements coded under the Governance and Risk dimensions of the Context layer. Sub-dimensions include Accountability, Auditing, Environment Understanding, Fairness, Legal Liability, Accuracy, AI Introduced Vulnerability, AI Misconception, Ethical Concerns, and Legal Risks. D# refers to document identifiers listed in Table 7 in Appendix B

Human

Table 3 Selected statements from industry documents coded under the Human layer during template analysis

Layer	Dimension	Sub-Dimension	Statement
Human	Benefits	Load Reduction	*"The scalability of cyberattacks poses a significant challenge. However, we can use AI technologies to assist analysts in the Security Operations Center by swiftly searching multiple sources, advising on alert responses, and automating actions to handle high volumes more effectively."* [D1]
			"By crafting specific response playbooks, and optimizing workflows, AI also empowers security teams to efficiently prioritize, detect, and remediate issues" [D1]
			"Automating security tasks like vulnerability scanning and patching using AI can cut cost and errors. It lets human analysts to focus on more complex investigations and decisions" [D10]
			"Automated incident triage accelerates the early stages of incident response and allows security teams to focus on the most critical incidents first." [D17]
			"AI automates incident response playbooks, helping security teams efficiently handle various types of incidents. routine and repetitive tasks" [D17]
			"But with AI, security teams can focus on more strategic aspects of cybersecurity and leave the mundane tasks to AI and automation." [D2]
			"Defensive AI is becoming an integral part of the SOC, augmenting understaffed teams." [D5]
			"Through innovation, collaboration and responsible use of generative AI and agents, defenders will be positioned to take on cybersecurity's toughest challenges and work toward making the world safer for all" [D8]
		Skills Augmentation	*"These tools provide assistance that allows the development of generalist talent to a security analyst role"* [D1]
			"Adoption of AI can fill the increasing cybersecurity skill gap which has multiplied by 3.5 times in 8 years" [D8]
			"A similar proportion (90%) of respondents said GenAI is making it easier for the SOC team to communicate and grow their internal knowledge base." [D11]
			"AI-driven analytics identify new attack vectors, providing security teams with the knowledge to stay ahead of cybercriminals." [D16]
			"Actionable cyberthreat intelligence provides analysts with timely, relevant, and contextual insights into potential threats, enabling them to make informed decisions and take proactive measures to mitigate risks." [D2]
			"AI-based defensive tools show promise in improving the effectiveness of cybersecurity specialists." [D6]
			"Microsoft has invested heavily in AI to help SOCs upskill and operate at speeds beyond human capability to tackle threat actors. In a 2023 study we found that novice users were able to perform 26% faster and were 44% more accurate across all tasks when using Copilot for Security." [D8]
		Training & Education	*"AI-driven threat analysis provides the opportunity for security teams to learn and train in real-time, helping to reduce the skills gap"* [D8]
			"Makes them ideal (Large language models) for tasks like emulating sophisticated phishing attacks for preventative security" [D7]
			"Generative AI can enhance training content, boost trainee performance, enhance training retention, on-the-job training efficacy, and encourage continual learning of cyber defense skills and tactics." [D18]
	Requirements	Education	*"Additionally, 63% acknowledge the difficulty in integrating Gen AI into their existing security solutions due to talent limitations. Consequently, over half (51%) of organizations today are investing in comprehensive AI cybersecurity training programs."* [D1]
			"Security leaders should take steps to educate themselves and their teams on AI and how it can be used to improve their efforts and the solutions they purchase" [D12]

Table 3 continued

Layer	Dimension	Sub-Dimension	Statement
			"30% of all cybersecurity jobs are expected to require AI expertise by 2027." [D16]
			"Security analysts, incident responders, and architects need to learn how to work with this new technology on a hands-on basis." [D5]
			"Develop AI capabilities to combat AI-based attacks, recognizing that AI can augment, but not replace, human effort." [D6]
		Explainability	*"There is a risk that the decisions made based on complex probabilistic algorithms and huge quantities of data could lack "explainability", leaving the leaders accountable for them unable to verify or justify their correctness"* [D15]
			"(From solution description) The model editor ensures human users have visibility and understanding over the AI decision making. The various AI-powered capabilities show their work with clearly reported scores or explanations." [D3]
			"Most importantly, AI should be transparent, explainable, and privacy-preserving." [D4]
			"As AI becomes more widely adopted, explainable AI will become more critical than ever to clarify the decision-making roadmaps and outputs of other AI agents." [D7]
		Human Oversight	*"Human analysts will still be integral: Very few respondents (21%) associate autonomous security with eliminating human analysts."* [D11]
			"Security analysts' expertise is crucial for training systems, overseeing algorithms and models for ML and DL, and validating the output" [D14]
			"Always involve human analysts in validating AI findings." [D19]
			"Automated systems lack the human intuition and context needed to evaluate the level of risk and the importance of a particular alert." [D2]
			"AI is not capable of replacing human problem-solving and decision-making capabilities" [D6]

Note: This table presents statements coded under the Human layer. Sub-dimensions include Load Reduction, Skills Augmentation, Training & Education, Education, Explainability, and Human Oversight. D# refers to document identifiers listed in Table 7 in Appendix B

Task

Table 4 Selected statements from industry documents coded under the Task layer during template analysis

Layer	Dimension	Sub-Dimension	Statement
Task	Protect & Identify	Endpoint Security	*"AI anti-virus works slightly differently and uses a combination of methods to identify and destroy potentially harmful files."* [D24]
			"Automating threat detection/response (28%) and endpoint security (27%) are the most popular applications of AI." [D32]
		Threat Intelligence	*"However, we can use AI technologies to assist analysts in the Security Operations Center by swiftly searching multiple sources."* [D1]
			"The applied use of AI technologies is critical to data collection, analysis, correlation, and, ultimately, the formulation of that data into actionable intelligence." [D12]
			"Threat Intelligence: AI-driven analytics identify new attack vectors, providing security teams with the knowledge to stay ahead of cybercriminals." [D16]
			"Improve incident mitigation and response: leverage AI in threat hunting, analysis and resolution." [D21]
		Proactive Defence	*"There are numerous potential applications for generative AI, especially in enhancing proactive measures against attacks."* [D1]
			"AI is an essential tool to fight and protect against cyber threats. Forbes estimates 3 out of 4 enterprises across the globe have prioritized AI and machine learning in their IT budgets for cyber defense." [D10]
			"OpenAI's Chat GPT4 can be used to advance penetration testing" [D12]
	Detect	Alert Triage	*"While generative AI can handle a greater volume of events than manual processes, human oversight remains critical to verify conclusions periodically and ensure ethical considerations are upheld."* [D1]
			"A key benefit of AI is making your workforce more efficient. Machines never get tired or need rest; they work 24x7. They can identify patterns in massive amounts of data or alert streams to help security analysts and IT security professionals predict new emergent behaviors" [D13]
			"AI can identify, categorize, and prioritize security incidents based on their severity and potential impact on the organization, which reduces response time" [D17]
		Classification	*"Classifying, monitoring, and tracking data can be an extremely time-consuming exercise for security teams. However, AI can automate data classification"* [D20]
			"Instead of classifying an alert into a known set of categories, the differentiation is now built from all surrounding contextual information" [D8]
		Network & Data Monitoring	*"In cybersecurity, such agents operate autonomously and monitor network traffic, detect anomalies, respond to threats in real time, and actively search for threats without human intervention."* [D1]
			"When implemented properly, it can act like a team of threat researchers, who can filter through data and identify interesting patterns;" [D14]
			"AI monitors user and system behavior to identify unusual or suspicious activities, helping in the early detection of threats." [D17]
		Targeted Detection	*"Malware detection, classification and scoring of URLs and IPs, and phishing detection. In each case, ML and DL are working to bring measurable results."* [D14]

Table 4 continued

Layer	Dimension	Sub-Dimension	Statement
			"Autonomous detection and identification of malware, network anomalies and intrusions, spam and botnets" [D15]
			"AI can identify known phishing patterns and signatures, allowing it to recognize and flag suspicious emails. beyond known patterns" [D17]
			"By leveraging AI and deep learning for behavioral analysis, organizations can detect insider threats" [D2]
		Vulnerability Identification	*"AI enhances threat detection and response by rapidly analyzing vast amounts of data and identifying patterns and predicting potential breaches."* [D1]
			"Automating security tasks like vulnerability scanning and patching using AI" [D10]
			"AI to create malicious agents, application scanning solutions and penetration testers can use the same capability to find and remediate vulnerabilities" [D12]
	Respond & Recover	Accelerating Investigation	*"Hunting and query writing, incident response and investigations, alert handling, and more have gotten both more efficient and more effective thanks to GenAI tool usage."* [D11]
			"Enriched analytics to support human investigation and response" [D15]
			"Accelerating threat investigation and response" [D4]
			"So, once you found the potential threat and you've contained it intelligently to open up a window of opportunity to investigate it, then we want to use machine learning to help the security team with that investigation." [D24]
		Mitigating Threats	*"Automating security tasks like vulnerability scanning and patching using AI can cut cost and errors."* [D10]
			"In fact, the community should explore the value of automating security policies, detection and mitigation more broadly, using AI." [D15]
			"AI-powered patch management removes the herculean effort of manual patching to automate and streamline the patch management process." [D22]
			"There is strong agreement that AI-powered solutions will be better at stopping AI-powered threats (71% of respondents are confident in this), and there's also agreement (66%) that AI-powered solutions will be able to do so automatically." [D4]
			"Automated response. AI can automate responses to detected threats, quickly isolating affected systems and blocking malicious activities, reducing attackers' window of opportunity." [D6]
		Accelerating Recovery	*"There's near universal agreement that AI-powered cybersecurity solutions will greatly improve the ability of security teams to prevent, detect, respond to, and recover from threats. In fact, 95% of participants agree with the above statement."* [D5]
			"Potentially faster recovery from incidents, for example, through the use of self-regenerating networks to reinstate pre-compromise states" [D15]
			"In parallel, cyber defenders are harnessing AI to enhance cybersecurity capabilities, facilitating wider prevention, more accurate threat detection, autonomous remediation and more rapid and effective incident response." [D27]

Table 4 continued

Layer	Dimension	Sub-Dimension	Statement
	Operator Support	Task Automation	*"To begin, organizations can automate complex, time intensive and redundant activities, which can enhance efficiency and reduce errors."* [D10]
			"AI is also being used to support human defenders by augmenting and automating tasks usually performed by analysts" [D15]
			"Properly implemented, AI can multiply productivity by automating repetitive tasks, scanning logs, tracking data, detecting anomalies in the environment, and more." [D20]
		Provide Information Summary	*"Gen AI can further help in interpreting complex regulations and producing detailed reports required for compliance."* [D1]
			"More accurate reports and analyses of data and network traffic for enhanced system observability." [D18]
			"Creating a report for the security team that looks like the sort of thing that would be the result of 8 or 10 hours work from a junior analyst. So ultimately, we're helping security teams to be a lot leaner, a lot more efficient and helping them to scale their operations to a far greater degree" [D24]
			"It can also be used to summarize as part of the reporting process" [D3]
		Provide Interface	*"Through prompts, analysts can classify, synthesize, and summarize these insights in an intuitive way and preferred formats (e.g., translate attack graphs to human-readable explanations)"* [D1]
			"SIEM solutions also utilize GPT technology and natural language processing (NLP) to create a more informed and guided experience for security operations center personnel." [D12]
			"An AI assistant not only transforms how analysts view their jobs, but it can also empower them: New analysts can learn from data-driven insights, while experienced analysts can focus on more important tasks" [D2]
			"Improve integrations between their tools" [D4]
		Support Decision Making	*"In fact, a study by MIT showed how the "human-in-the-loop" approach to AI outperformed AI alone, and humans alone, in attack detection. "The key is to leverage the expertise you have (or your vendor has) to work smarter and faster"."* [D14]
			"Gen AI can support decision-making, enabling swift action and providing valuable support for security analysts" [D1]
			"AI-enabled security platforms use deep contextual data processing to answer questions, provide recommendations and direction, hypothesize, and formulate possible answers based on available evidence." [D2]
			"AI no longer just automates repetitive tasks but also actively participates in decision-making, provides strategic insights, and collaborates with human employees" [D23]
		Task Assignment	*"AI can assess the priority of a given item based on how similar items were prioritized in the past."* [D8]
			"Enables security teams to focus on the most critical issues, but it also maximizes the effectiveness of remediation efforts." [D22]

Note: This table presents statements coded under the Task layer. Sub-dimensions include Endpoint Security, Threat Intelligence, Proactive Defence, Alert Triage, Classification, Network & Data Monitoring, Targeted Detection, Vulnerability Identification, Accelerating Investigation, Mitigating Threats, Accelerating Recovery, Task Automation, Provide Information Summary, Provide Interface, Support Decision Making, and Task Assignment. D# refers to document identifiers listed in Table 7 in Appendix B.

Technology

Table 5 Selected statements from industry documents coded under the Technology layer during template analysis

Layer	Dimension	Sub-Dimension	Statement
Technology	-	Machine Learning	*"SIEM uses supervised and unsupervised machine learning (ML) models to perform sophisticated linear regression, including support vector regression, Gaussian process regression, and decision tree regression."* [D1]
			"The next evolution, deep learning (DL), allows machines to use techniques that more closely simulate human decision-making." [D14]
			"Predictive analysis: machine learning algorithms analyze historical data to predict potential future threats." [D17]
		Generative AI	*"There are numerous potential applications for generative AI, especially in enhancing proactive measures against attacks."* [D1]
			"CISOs have recognized the benefits, with 91% expressing excitement over the prospects and opportunities GenAI and AI will bring to their organization." [D13]
		Natural Language Processing	*"AI can identify known phishing patterns and signatures, allowing it to recognize and flag suspicious emails."* [D17]

Note: This table presents statements coded under the Technology layer. Sub-dimensions include Machine Learning, Generative AI, and Natural Language Processing. D# refers to document identifiers listed in Table 7 in Appendix B

Outcome

Table 6 Selected statements from industry documents coded under the Outcome layer during template analysis

Layer	Dimension	Sub-Dimension	Statement
Outcome	-	Cost Reduction	*"Infinity AI Copilot addresses the growing global shortage of cyber security practitioners by boosting the efficiency and effectiveness of security teams."* [D21]
			"AI presents an opportunity to both improve the accuracy and effectiveness of the analysis and do so in a highly cost-efficient way." [D24]
			"It reflects the hope that AI technologies can be a force multiplier for overworked security teams, making them more efficient and productive. This outcome would go a long way toward mitigating the cybersecurity skills shortage that has plagued IT groups for many years" [D25]
		Faster Response	*"It can reduce MTTD and MTTR and increase analyst productivity. Instead of babysitting alerts that don't amount to anything, they can get alerts for only high priority threats that require human critical thinking skills."* [D2]
			"Not only does automated patching boost network security, but it's also significantly faster and more efficient, making it much easier to stay up to date with patches." [D22]
			"Faster response to threats and incidents is the top benefit it pros expect from deploying AI" [D17]
		Improved Readiness	*"This approach also supports compliance with regulatory requirements and fosters a proactive security culture."* [D1]
			"AI systems can continuously learn and adapt to new threats and attack methods, offering a dynamic defense against evolving threats." [D10]
			"Refinement of cyber deception to proactively create environments that are difficult for attackers to operate in" [D15]
		Performance Increase	*"ML gives us the ability to magnify the ability of humans, merging the abilities of multiple experts into something that is much greater than the sum of the parts."* [D14]
			"Improves system performance and reliability as compared to non-AI-enhanced solutions." [D18]
			"AI and automation help analysts reduce their workloads by eliminating manual errors, streamlining processes, refocusing their efforts" [D2]

Note: This table presents statements coded under the Outcome layer. Sub-dimensions include Cost Reduction, Faster Response, Improved Readiness, and Performance Increase. D# refers to document identifiers listed in Table 7 in Appendix B

Appendix B Used Industry Publications

Table 7 List of analysed industry-issued publications

Code	Title	Institution	Reference
D1	New Defenses, New Threats: What AI and Gen AI Bring to Cybersecurity	Capgemini Research Institute	[48]
D2	AI: The Good, Bad and Opportunity – Standard Solutions Guide	TD SYNNEX	[8]
D3	The AI Arsenal	Darktrace	[3]
D4	The State of AI Cyber Security 2024	Darktrace	[49]
D5	The State of AI Cybersecurity 2025	Darktrace	[50]
D6	AI in Cybersecurity	Arthur D. Little	[4]
D7	The CISO's Guide to Cyber AI	Darktrace	[51]
D8	Microsoft Digital Defense Report 2024	Microsoft	[2]
D9	Top Tech Trends 2025: AI Powered Everything	Capgemini Research Institute	[52]
D10	Infosys Playbook: AI-First Cybersecurity for Enterprises	Infosys	[53]
D11	AI Inflection Point	Enterprise Strategy Group, commissioned by SentinelOne	[54]
D12	Use Artificial Intelligence to Combat Cyberthreats	Fortinet	[55]
D13	The Mind of the CISO: Decoding the GenAI Impact	Trellix	[56]
D14	Demystifying AI in Cybersecurity	Webroot	[57]
D15	Future Series: Cybersecurity, Emerging Technology and Systemic Risk	World Economic Forum in collaboration with University of Oxford	[9]
D16	Cybersecurity and AI	Skytech Cybercloud	[58]
D17	Securing Tomorrow: A Guide to the Role of AI in Cybersecurity	Barracuda Networks	[59]
D18	Cybersecurity in the Age of AI	Barracuda Networks	[60]
D19	Impact of Artificial Intelligence on Criminal and Illicit Activities	U.S. Department of Homeland Security	[61]
D20	AI Trends and Security Insights for the C-Suite	CXO Revolutionaries, sponsored by Zscaler	[62]
D21	Cyber Security Report 2024	Check Point Research	[63]
D22	The Fight for Cyber Resilience	TDSynnex and CyberSolv	[64]
D23	2025 Digital Trends	Softtek	[65]
D24	Global AI Report 2020	DrakeStar	[66]
D25	2024 Cyberthreat Defense Report	CyberEdge Group	[67]
D26	Foundation Models: Opportunities, Risks and Mitigations	IBM AI Ethics Board	[68]
D27	Artificial Intelligence and Cybersecurity: Balancing Risks and Rewards	World Economic Forum in collaboration with the Global Cyber Security Capacity Centre, University of Oxford	[69]

Table 7 continued

Code	Title	Institution	Reference
D28	2024 Cybersecurity Assessment Report	Bitdefender	[70]
D29	FY24 Purpose Report	Cisco Systems, Inc.	[71]
D30	Counter-AI Offensive Tools and Techniques	Cybersecurity & Information Systems Information Analysis Center	[72]
D31	2024 Global Networking Trends Report	Cisco Systems, Inc.	[73]
D32	State of Cybersecurity 2024	ISACA	[74]
D33	AI and Cybersecurity	Coalition for Cybersecurity in Asia-Pacific	[75]
D34	Global Cybersecurity Outlook 2025	World Economic Forum in collaboration with Accenture	[76]

Note: This table presents the list of industry-issued documents analysed in the study. Each entry is assigned an identifier (D#), which is used throughout the paper to attribute statements and insights to specific sources. These documents were selected based on relevance to AI integration in cybersecurity incident management and were coded during template analysis

References

1. ASD. Information security manual: Guidelines for cybersecurity incidents. Technical report, Australian Signals Directorate, Canberra, Australia, March (2025). URL https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/ism/cybersecurity-guidelines/guidelines-cybersecurity-incidents
2. Microsoft. Microsoft digital defense report (2024). Technical report, Microsoft, 2024. URL https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024. Accessed: 2025-05-29
3. Darktrace. The ai arsenal. Technical report, Darktrace, (2025). URL https://www.darktrace.com/resources/the-ai-arsenal. Accessed: 2025-05-29
4. Scherr, M., Stepanov, I., Bryzhytska, D., Jablonski, P., Papadopoulos, M., Teixeira, T.: Ai in cybersecurity. Technical report, Arthur D. Little, (2024). URL https://www.adlittle.com/en/insights/viewpoints/ai-cybersecurity. Accessed: 2025-05-29
5. Lohn, A., Knack, A., Burke, A., Jackson, K.: Autonomous cyber defense: A roadmap from lab to ops. Technical report, Centre for Emerging Technology and Security (CETaS) (2023)
6. Kaur, R., Gabrijelčič, D., Klobučar, T.: Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, 97:101804, September (2023). ISSN 15662535. https://doi.org/10.1016/j.inffus.2023.101804
7. Tilbury, J., Flowerday, S.: Humans and automation: Augmenting security operation centers. *Journal of Cybersecurity and Privacy*, 4(3):388–409, July (2024). ISSN 2624-800X. https://doi.org/10.3390/jcp4030020
8. TDSYNNEX. Ai: The good, bad and opportunity – standard solutions guide. Technical report, TD SYNNEX, September 2024. URL https://www.tdsynnex.com/na/us/advancedsolutions/cybersecurity/. Accessed: 2025-05-29
9. WEF. Future series: Cybersecurity, emerging technology and systemic risk. Technical report, World Economic Forum in collaboration with University of Oxford, November 2020. URL https://www3.weforum.org/docs/WEF_Future_Series_Cybersecurity_emerging_technology_and_systemic_risk_2020.pdf. Accessed: 2025-05-29
10. Li, N., Zhang, P.: The intellectual development of human-computer interaction research: A critical assessment of the MIS literature (1990-2002). *Journal of the Association for Information Systems*, 6, (2005). ISSN 1536-9323. https://doi.org/10.17705/1jais.00070
11. Seitz, J., Benke, I., Heinzl, A., Maedche, A.: The impact of video meeting systems on psychological user states: a state-of-the-art review. *International Journal of Human-Computer Studies*, 182:103178, (2024). ISSN 1071-5819. https://doi.org/10.1016/j.ijhcs.2023.103178
12. Sarker, I.H., Furhad, M.H., Nowrozy, R.: Ai-driven cybersecurity: An overview, security intelligence modeling and research directions. *SN Computer Science*, 2(3):173, May (2021). ISSN 2662-995X, 2661-8907https://doi.org/10.1007/s42979-021-00557-0
13. Sankaram, M., Roopesh, M., Rasetti, S., Nishat, N.: A comprehensive review of artificial intelligence applications in enhancing cybersecurity threat detection and response mechanisms. *Global Mainstream Journal of Business, Economics, Development & Project Management*, 3(05):1–14, Jul. (2024). https://doi.org/10.62304/jbedpm.v3i05.180
14. Naik, B., Mehta, A., Yagnik, H., Shah, M.: The impacts of artificial intelligence techniques in augmentation of cybersecurity: a comprehensive review. *Complex & Intelligent Systems*, 8(2):1763–1780, April (2022). ISSN 2199-4536, 2198-6053. https://doi.org/10.1007/s40747-021-00494-8
15. Ali, R., Ali, A., Iqbal, F., Masood Khattak, A., Aleem, S.: A systematic review of artificial intelligence and machine learning techniques for cyber security. In Yuan Tian, Tinghuai Ma, and Muhammad Khurram Khan, editors, *Big Data and Security*, volume 1210, pages 584–593. Springer Singapore, Singapore, (2020). ISBN 978-981-15-7529-7 978-981-15-7530-3. https://doi.org/10.1007/978-981-15-7530-3_44
16. Kamruzzaman, M., Bhuyan, M.K., Hasan, R., Farjana Farabi, S., Nilima, S.I., Azhad Hossain, M.: Exploring the landscape: A systematic review of artificial intelligence techniques in cybersecurity. In *2024 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI)*, pages 01–06, Beijing, China, October 2024. IEEE. ISBN 979-8-3503-4983-2. https://doi.org/10.1109/CCCI61916.2024.10736474
17. Kundiya, K., Haribhakta, Y.: A systematic review on insider threat detection using natural language processing. Int. J. Inf. Secur. **24**(6), 227 (2025). https://doi.org/10.1007/s10207-025-01145-6
18. Jada, I., Mayayise, T.O.: The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. *Data and Information Management*, 8(2):100063,

June (2024). ISSN 25439251. https://doi.org/10.1016/j.dim.2023.100063
19. Far, S.M.T., Feyzi, F.: Large language models for software vulnerability detection: a guide for researchers on models, methods, techniques, datasets, and metrics. Int. J. Inf. Secur. **24**(2), 78 (2025). https://doi.org/10.1007/s10207-025-00992-7
20. Akhtar, M., Feng, T.: An overview of the applications of artificial intelligence in cybersecurity. *EAI Endorsed Transactions on Creative Technologies*, 8(29):172218, December (2021). ISSN 2409-9708. https://doi.org/10.4108/eai.23-11-2021.172218
21. Li, J.: Cyber security meets artificial intelligence: a survey. Frontiers of Information Technology & Electronic Engineering **19**, 1462–1474 (2019). https://doi.org/10.1631/FITEE.1800573
22. Goud, S.N.G.: Review on harnessing artificial intelligence: A paradigm shift in cybersecurity for a safer digital future. International Journal for Research in Applied Science and Engineering Technology, 12(12), 412–416, (2024). ISSN 23219653. https://doi.org/10.22214/ijraset.2024.65782
23. Farheen Ansari, M., Dash, B., Sharma, P., Yathiraju, N.: The impact and limitations of artificial intelligence in cybersecurity: A literature review. *IJARCCE*, 11:81–90, 10 (2022). https://doi.org/10.17148/IJARCCE.2022.11912
24. Abdullahi, M., Mohamed, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L., Jadid Abdulkadir, S.: Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review. Electronics **11**, 1–27 (2022). https://doi.org/10.3390/electronics11020198
25. Morovat, K., Panda, B.: A survey of artificial intelligence in cybersecurity. In *2020 International Conference on Computational Science and Computational Intelligence (CSCI)*, pages 109–115, Las Vegas, NV, USA, December (2020). IEEE. ISBN 978-1-7281-7624-6. https://doi.org/10.1109/CSCI51800.2020.00026
26. Kincl, J., Adam, M.T. P., Pavleska, T.: The role of human factors in cybersecurity incident management. In *HCI for Cybersecurity, Privacy and Trust*, volume 15814 of *Lecture Notes in Computer Science*, pages 35–53. Springer Nature Switzerland, Cham, (2025). https://doi.org/10.1007/978-3-031-92833-8_3
27. Chen, Z., Kang, Y., Li, L., Zhang, X., Zhang, H., Xu, H., Zhou, Y., Yang, L., Sun, J., Xu, Z., Dang, Y., Gao, F., Zhao, P., Qiao, B., Lin, Q., Zhang, D., Lyu, M.R.: Towards intelligent incident management: why we need it and how we make it. In *Proceedings of the 28th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, ESEC/FSE 2020, page 1487–1497, New York, NY, USA, (2020). Association for Computing Machinery. ISBN 9781450370431. https://doi.org/10.1145/3368089.3417055
28. Tariq, S., Baruwal Chhetri, M., Nepal, S., Paris, C.: Alert fatigue in security operations centres: Research challenges and opportunities. *ACM Comput. Surv.*, 57(9), April (2025). ISSN 0360-0300. https://doi.org/10.1145/3723158
29. Forum of Incident Response and Security Teams. First services framework:team types within the context of services frameworks. Technical report, FIRST, 2025. URL https://www.first.org/standards/frameworks/csirts/FIRST-services-framework-team-types-v1.2.pdf
30. Wakefield Research. 2022 devo soc performance report. Technical report, Devo, (2022). URL https://www.devo.com/resources/analyst-research/2022-devo-soc-performance-report/
31. Nepal, S., Hernandez, J., Lewis, R., Chaudhry, A., Houck, B., Knudsen, E., Rojas, R., Tankus, B., Prafullchandra, H., Czerwinski, M.: Burnout in cybersecurity incident responders: Exploring the factors that light the fire. *Proceedings of the ACM on Human-Computer Interaction*, 8:1–35, (2024). ISSN 2573-0142. https://doi.org/10.1145/3637304
32. Mandal, A., Agarwal, S., Malhotra, N., Sridhara, G., Ray, A., Swarup, D.: Improving it support by enhancing incident management process with multi-modal analysis. In Sami Yangui, Ismael Bouassida Rodriguez, Khalil Drira, and Zahir Tari, editors, *Service-Oriented Computing*, pages 431–446. Springer International Publishing, (2019). ISBN 978-3-030-33702-5
33. Palma, A., Angelini, M.: Impavid: Enhancing incident management process compliance assessment with visual analytics. *Computers & Graphics*, 130:104243, 2025. ISSN 0097-8493. https://doi.org/10.1016/j.cag.2025.104243. URL https://www.sciencedirect.com/science/article/pii/S0097849325000846
34. Steyvers, M., Kumar, A.: Three challenges for ai-assisted decision-making. Perspect. Psychol. Sci. **19**(5), 722–734 (2024). https://doi.org/10.1177/17456916231181102
35. Parasuraman, R., Sheridan, T.B., Wickens, C.D.: A model for types and levels of human interaction with automation. IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans **30**(3), 286–297 (2000). https://doi.org/10.1109/3468.844354
36. Romeo, G., Conti, D.: Exploring automation bias in human-ai collaboration: a review and implications for explainable ai. AI & Society **41**(1), 259–278 (2026). https://doi.org/10.1007/s00146-025-02422-7
37. Binbeshr, F., Imam, M., Ghaleb, M., Hamdan, M., Abdul Rahim, M., Hammoudeh, M.: The rise of cognitive SOCs: A systematic literature review on ai approaches. *IEEE Open Journal of the Computer Society*, 6:360–379, (2025). ISSN 2644-1268. https://doi.org/10.1109/OJCS.2025.3536800
38. León, A., Perdices, D., García-Dorado, J.L., Ramos, J., Aracil, J.: An expert-aware markovian system for end-user proactive troubleshooting in the network and security operations center. Expert Syst. Appl. **276**, 127072 (2025). https://doi.org/10.1016/j.eswa.2025.127072
39. Yue, Y., Zhao, D., Zhou, Y., Xu, L., Tang, Y., Peng, H.: An intrusion response approach based on multi-objective optimization and deep q network for industrial control systems. Expert Syst. Appl. **272**, 126664 (2025). https://doi.org/10.1016/j.eswa.2025.126664
40. Khayat, M., Barka, E., Serhani, M.A., Sallabi, F., Shuaib, K., Khater, H.M.: Empowering security operation center with artificial intelligence and machine learning-a systematic literature review. IEEE Access **13**, 19162–19197 (2025). https://doi.org/10.1109/ACCESS.2025.3532951
41. Brooks, J., McCluskey, S., Turley, E., King, N.: The utility of template analysis in qualitative psychology research. Qual. Res. Psychol. **12**(2), 202–222 (2015). https://doi.org/10.1080/14780887.2014.955224
42. Chowdhury, N.H., Adam, M.T.P., Teubner, T.: Rushing for security: a document analysis on the sources and effects of time pressure on organizational cybersecurity. Information & Computer Security **31**(4), 504–526 (2023). https://doi.org/10.1108/ICS-01-2021-0013
43. Zwicky, F.: Discovery, Invention, 1st edn. Research Through the Morphological Approach. Macmillan, New York, USA (1969)
44. Knaeble, M., Nadj, M., Germann, L., Maedche, A.: Tools of trade of the next blue-collar job? antecedents, design features, and outcomes of interactive labeling systems. In *Proceedings of the 31st European Conference on Information Systems (ECIS)*, Kristiansand, Norway, (2023). https://aisel.aisnet.org/ecis2023_rp/373
45. ISO. Iso/iec 22989:2022 – information technology – artificial intelligence – artificial intelligence concepts and terminology. Technical report, International Organization for Standardization, July 2022. URL https://www.iso.org/standard/74296.html
46. NIST. The nist cybersecurity framework (csf) 2.0. Technical report, National Institute of Standards and Technology, (2024)
47. Raees, M., Meijerink, I., Lykourentzou, I., Khan, V.-J., Papangelis, K.: From explainable to interactive ai: A literature review on current trends in human-ai interaction. *International Journal of Human-Computer Studies*, 189:103301, (2024). ISSN 1071-

5819. https://doi.org/10.1016/j.ijhcs.2024.103301. URL https://www.sciencedirect.com/science/article/pii/S1071581924000855
48. Capgemini. New defenses, new threats: What ai and gen ai bring to cybersecurity. Technical report, Capgemini Research Institute, November 2024. URL https://www.capgemini.com/wp-content/uploads/2024/11/CRI_AI-and-gen-AI-in-cybersecurity_15112024.pdf. Accessed: 2025-05-29
49. Darktrace. The state of ai cyber security 2024. Technical report, Darktrace, 2024. URL https://www.darktrace.com/resources/state-of-ai-cyber-security-2024. Accessed: 2025-05-29
50. Darktrace. The state of ai cybersecurity 2025. Technical report, Darktrace, 2025. URL https://www.darktrace.com/the-state-of-ai-cybersecurity-2025. Accessed: 2025-05-29
51. Darktrace. The ciso's guide to cyber ai. Technical report, Darktrace, 2024. URL https://www.darktrace.com/resources/the-cisos-guide-to-cyber-ai. Accessed: 2025-05-29
52. Capgemini. Top tech trends 2025: Ai powered everything. Technical report, Capgemini Research Institute, 2025. URL https://www.capgemini.com/insights/research-library/top-tech-trends-2025. Accessed: 2025-05-29
53. Infosys. Infosys playbook: Ai-first cybersecurity for enterprises. Technical report, Infosys, 2024. URL https://www.infosys.com/services/cyber-security/documents/ai-first-cybersecurity.pdf. Accessed: 2025-05-29
54. SentinelOne. Ai inflection point. Technical report, Enterprise Strategy Group, commissioned by SentinelOne, 2024. URL https://www.sentinelone.com/lp/esg-genai/. Accessed: 2025-05-29
55. Fortinet. Use artificial intelligence to combat cyberthreats. Technical report, Fortinet, September 2024. URL https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-ai-combat-cyberthreats.pdf. Accessed: 2025-05-29
56. Trellix. The mind of the ciso: Decoding the genai impact. Technical report, Trellix, (2024). URL https://www.trellix.com/en-au/solutions/mind-of-the-ciso-decoding-the-genai-impact/. Accessed: 2025-05-29
57. Webroot. Demystifying ai in cybersecurity. Technical report, Webroot, (2019). URL https://www-cdn.webroot.com/3815/7470/9219/CyberEdge_Webroot_Demystifying_AI_WP.pdf. Accessed: 2025-05-29
58. Skytech. Cybersecurity and ai. Technical report, Skytech Cybercloud, (2024). URL https://skytechdigital.ae/wp-content/uploads/2024/12/Cybersecurity-and-AI-E-Book.pdf. Accessed: 2025-05-29
59. Barracuda. Securing tomorrow: A guide to the role of ai in cybersecurity. Technical report, Barracuda Networks, February (2024). URL https://assets.barracuda.com/assets/docs/dms/ciso-guide-ai-cybersecurity-ebook.pdf. Accessed: 2025-05-29
60. Barracuda. Cybersecurity in the age of ai. Technical report, Barracuda Networks, (2024). URL https://s3.ap-southeast-1.amazonaws.com/cdn.thinklogicmarketing.com/CybersecAsia/eGuides/Barracuda+eGuide_April+1.pdf. Accessed: 2025-05-29
61. DHS. Impact of artificial intelligence on criminal and illicit activities. Technical report, U.S. Department of Homeland Security, (2024). URL https://www.dhs.gov/sites/default/files/2024-10/24_0927_ia_aep-impact-ai-on-criminal-and-illicit-activities.pdf. Accessed: 2025-05-29
62. Zscaler. Ai trends and security insights for the c-suite. Technical report, CXO Revolutionaries, sponsored by Zscaler, (2024). URL https://www.zscaler.com/resources/industry-reports/zscaler-cxorevs-report-ai-trends-security-insights.pdf. Accessed: 2025-05-29
63. CheckPoint. Cyber security report 2024. Technical report, Check Point Research, (2024). URL https://www.checkpoint.com/resources/report-3854/report--cyber-security-report-2024. Accessed: 2025-05-29
64. TDSynnex. The fight for cyber resilience. Technical report, TDSynnex and CyberSolv, (2024). URL https://www.tdsynnex.com/na/us/cybersolv/wp-content/uploads/sites/10/2024/06/The-Fight-for-Cyber-Resilience.pdf. Accessed: 2025-05-29
65. Softtek. 2025 digital trends. Technical report, Softtek, (2024). URL https://www.softtek.com/digital-trends-2025. Accessed: 2025-05-29
66. DrakeStar. Global ai report (2020). Technical report, DrakeStar, October 2020. URL https://www.drakestar.com/research/global-ai-report-2020. Accessed: 2025-05-29
67. CyberEdge. 2024 cyberthreat defense report. Technical report, CyberEdge Group, (2024). URL https://cyberedgegroup.com/wp-content/uploads/2024/05/CyberEdge-2024-CDR-Report-v1.0.pdf. Accessed: 2025-05-29
68. IBM. Foundation models: Opportunities, risks and mitigations. Technical report, IBM AI Ethics Board, May (2024). URL https://www.ibm.com/downloads/documents/us-en/10a99803d8afd656. Accessed: 2025-05-29
69. WEF. Artificial intelligence and cybersecurity: Balancing risks and rewards. Technical report, World Economic Forum in collaboration with the Global Cyber Security Capacity Centre, University of Oxford, January (2025). URL https://reports.weforum.org/docs/WEF_Artificial_Intelligence_and_Cybersecurity_Balancing_Risks_and_Rewards_2025.pdf. Accessed: 2025-05-29
70. Bitdefender. 2024 cybersecurity assessment report. Technical report, Bitdefender, (2024). URL https://www.bitdefender.com/content/dam/bitdefender/business/campaign/2024-Assessment-Report.pdf. Accessed: 2025-05-29
71. Cisco. Fy24 purpose report. Technical report, Cisco Systems, Inc., (2024). URL https://www.cisco.com/site/us/en/about/purpose/fy24-report/index.html. Accessed: 2025-05-29
72. CSIAC. Counter-ai offensive tools and techniques. Technical report, Cybersecurity & Information Systems Information Analysis Center, (2024). URL https://csiac.dtic.mil/wp-content/uploads/2024/02/TI-Response-Report_CSIAC_Counter-AI-Offensive-Tools_272024.pdf. Accessed: 2025-05-29
73. Cisco. 2024 global networking trends report. Technical report, Cisco Systems, Inc., (2024). URL https://www.cisco.com/c/dam/global/en_uk/solutions/enterprise-networks/2024-global-networking-trends.pdf. Accessed: 2025-05-29
74. ISACA. State of cybersecurity 2024. Technical report, ISACA, October (2024). URL https://www.isaca.org/resources/reports/state-of-cybersecurity-2024. Accessed: 2025-05-29
75. CCAPAC. Ai and cybersecurity. Technical report, Coalition for Cybersecurity in Asia-Pacific, (2024). URL https://ccapac.asia/wp-content/uploads/2024/10/CCAPAC-2024-Report.pdf. Accessed: 2025-05-29
76. WEF. Global cybersecurity outlook 2025. Technical report, World Economic Forum in collaboration with Accenture, January (2025). URL https://www.weforum.org/publications/global-cybersecurity-outlook-2025/. Accessed: 2025-05-29