Adoption of Cyber Threat Intelligence in organizations: a systematic literature review

Patrick Shirazi
University of Skövde
patrick.shirazi@his.se

Abstract

In today's rapidly evolving cyber threat landscape, cyber threat intelligence (CTI) has become a vital component of the organization's cybersecurity ecosystem. While a body of research has explored various technical aspects of CTI, such as data processing and CTI sharing, the adoption[1] of CTI within organizations remains underresearched. This paper presents a systematic literature review (SLR) aimed at identifying the key factors influencing CTI adoption in organizations. A total of 17 factors were identified and categorized into the people, process, and technology (PPT) framework, comprising three people-related factors, nine process-related factors, and five technology-related factors. The findings highlight the critical role of business maturity, process integration, competence development, and technical capabilities in facilitating successful CTI adoption within organizations.

1. Background

Threat intelligence is the evidence-based knowledge that provides context, mechanisms, indicators, implications, and actionable advice about existing or emerging threats to assets, helping inform decisions on how to respond (McMillan, 2023). In an organization, conducting threat intelligence means transforming collected data and information regarding cyber threat actors, including their intentions and capabilities, into a product that can be used in decision-making processes (Ainslie et al., 2023). This acquisition of intelligence is performed via four main steps: collect, process, analyze, and disseminate (Lundgren & Padyab, 2023).

Literature review is a crucial first step in understanding the adoption of CTI in organizations because it synthesizes existing knowledge, identifies key factors influencing adoption, and highlights gaps in research. Without this foundational understanding, primary data collection could be limited by biases, such as organizations reporting only their specific use cases or overlooking broader trends. Additionally, academic literature provides insights from multiple studies, methodologies, and contexts, reducing the risk of over-reliance on anecdotal evidence. A well-conducted review enables the formulation of more precise research questions and hypotheses, which can later be tested through direct data collection in organizations.

Although organizations recently have increasingly relied on cyber threat intelligence (CTI) as a tool to enhance their cybersecurity posture against rising cyber threats (Samtani et al., 2020; Wagner et al., 2019), it is shown that the rate of CTI adoption in organizations is still low and mainly dominated within information technology (IT) operations. Besides, CTI literature within organizations is predominantly focused on technological aspects, which indicates a knowledge gap since CTI process is not just about technology (Ainslie et al., 2023). The number of other CTI literature reviews focusing on organizational adoption is limited. Furthermore, existing CTI reviews mainly emphasize areas other than CTI adoption, such as decision-making processes (Ainslie et al., 2023), technical CTI sharing mechanisms (Wagner et al., 2019), management (Lundgren & Padyab, 2023), and various technical aspects (Tounsi & Rais, 2018). Other CTI reviews, however, focused on inherent CTI process challenges and opportunities regardless of their adoption and implementation in organizational contexts (Abu et al.,

[1] In this paper, adoption is conceptualized as the decision-making process through which an organization commits to and utilizes an innovation, while practice and implementation refer to the process of applying or integrating that innovation within a specific organizational context (Allen et al., 2017).

2018; Jesus et al., 2024). Aside from literature reviews, there are also few studies on organizational adoption of CTI, such as an action research on CTI adoption in commercial organizations (Kotsias et al., 2023) and value of CTI function (Berndt & Ophoff, 2020).

There are also other studies in limited scopes and not the entire CTI process. For instance, Gong investigated the obstacles to adopting two main interoperability standards for CTI sharing: Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII) (N. Gong, 2019). While numerous studies have explored various barriers and opportunities associated with CTI, research specifically focusing on its adoption within organizations remains limited. Even among the few studies available, the number of comprehensive investigations into CTI adoption across diverse types of organizations is limited. For instance, Ainslie et al. studied CTI for security decision-making in organizations and categorized their findings into three disciple-specific angles: technology, information sharing, and organization practice (Ainslie et al., 2023). A significant gap raised by Ainslie et al. is the need for more research on organizational practice perspectives as the current literature is dominated by technical perspectives. In the same direction, a notable example is the study by Kotsias et al., which analyzed CTI adoption as a service within a single commercial organization (Greenback) using the People, Process, and Technology (PPT) framework (Kotsias et al., 2023).

The research questions are derived from the need to systematically identify and categorize the key factors influencing CTI adoption. Given the complexity of CTI adoption in organizations, we adopt the PPT framework as a guiding structure. This well-established framework ensures a comprehensive investigation by addressing the human, procedural, and technological dimensions separately. Each research question is formulated to explore one of these three categories in depth, allowing us to identify barriers, opportunities, and influencing factors specific to each domain. While this section introduces these questions, the remainder of the paper implicitly addresses them through the structured literature review and analysis.

RQ1: What are the business and process factors that impact CTI adoption in an organization?

RQ2: What are the technical limitations, challenges, and opportunities for CTI adoption?

RQ3: What human factors have an impact on CTI adoption?

By synthesizing existing knowledge, our study will provide a more comprehensive understanding of the factors impacting CTI adoption in organizations, contributing. It also enables various practitioners to address these factors in their implementation of CTI solutions. Besides, the results open the horizons for regulatory bodies to cover them in their policies.

As mentioned earlier, People, Process, Technology (PPT) as a globally recognized framework for process improvements in organizations is used in this paper. Although the origin of this classification is not clear, it has been introduced since 1964 (Prodan et al., 2015). The PPT framework provides a comprehensive approach to managing changes prompted by digital technologies by considering the relationships between the three factors: people, process, and technology. By holistically understanding the three factors, organizations can navigate the complexities of digital transformation, which enables successful technology implementation and increases business performance (Satwekar et al., 2024). PPT has been widely used in information systems such as adopting CTI in a commercial organization (Kotsias et al., 2023), discerning and categorizing cloud security issues (Ghaffari et al., 2019), identifying cybersecurity challenges in organizations (Teoh et al., 2018), and application modeling for information systems risk management in small and medium enterprises (Javaid & Iqbal, 2017) and digital transformation (Taher, 2023).

The rest of the paper is organized as follows: Section 2 describes the steps of the method to conduct the systematic review. Section 3 analyses the results of the research and organizes them into three distinct categories of PPT. Section 4 discusses the findings and elaborates on future research directions. Lastly, Section 5 concludes the paper.

2. Research Methodology

In this study, the Webster & Watson (Webster & Watson, 2002) protocol was employed to guide the systematic literature review process. This protocol offers a structured approach to identifying, selecting, and assessing relevant research studies and has been widely used in information systems. The databases were selected based on their indexing of high-quality, peer-reviewed research in information systems. IEEE Xplore was included for its strong coverage of technical aspects, while Scopus and Web of Science were chosen for their broad, multidisciplinary scope. Other sources, such as ACM, were not added to

avoid redundancy in technical coverage, and Google Scholar was excluded due to its inclusion of non-peer-reviewed materials. To ensure the search query covers the various aspects of the research questions, a combination of three major concepts needs to be included: CTI, Adoption, and Organization. Since each keyword has common alternatives, the following search query is selected. Figure 1 demonstrates the research query.

```
("Cyber threat intelligence" OR "Cyber threat hunting" OR "Cyber threat modelling" OR "Cyber threat modeling" OR "Cyber threat analysis" OR "Cyber threat detection" OR "Adversary intelligence“)  AND  (Direction OR Planning OR Gathering OR Collection OR Sharing OR Dissemination  OR Process OR Processing OR Analysis OR Analyzing OR Feedback)  AND  (Organization OR Organizations OR Corporate OR Corporates OR Corporation OR Company OR Companies OR Business OR Businesses OR Enterprise OR Enterprises OR Management OR Regulatory OR Compliance OR Commercial)
```

Figure 1 The search query including terms to cover CTI adoption in organizations.

The inclusion criteria focus on academic, peer-reviewed content from journals and conference proceedings that explicitly address CTI adoption in an organizational context and are written in English. To ensure relevance to recent developments in organizational practices, we limited the timeframe to studies published between 2014 and 2024. Papers were excluded if they focused exclusively on CTI outside the organizational context such as algorithm development or purely technical advancements. Furthermore, papers that lacked a clear organizational focus or did not explicitly discuss CTI adoption within organizations are excluded as well as those who were non-peer-reviewed, such as white papers, book chapters, or unpublished manuscripts. This approach significantly reduced the pool of papers by filtering out studies that, while related to CTI, did not contribute to understanding its adoption within organizations.

The initial search query and criteria applied across databases returned 914 results. After removing 365 duplicates, 549 unique records remained. During the initial screening phase, titles, keywords, and abstracts were reviewed against the inclusion criteria, leading to the exclusion of 232 papers. The remaining papers underwent full-text screening, resulting in 199 additional exclusions and leaving 37 relevant articles. Through reference checks and snowballing techniques, 26 more articles were identified, bringing the final total to 63 articles. Next, each selected article underwent a full-text review, where data relevant to the research questions were extracted. All statements are categorized into three areas of people, process, and technology. Figure 2 demonstrates the paper selection process.

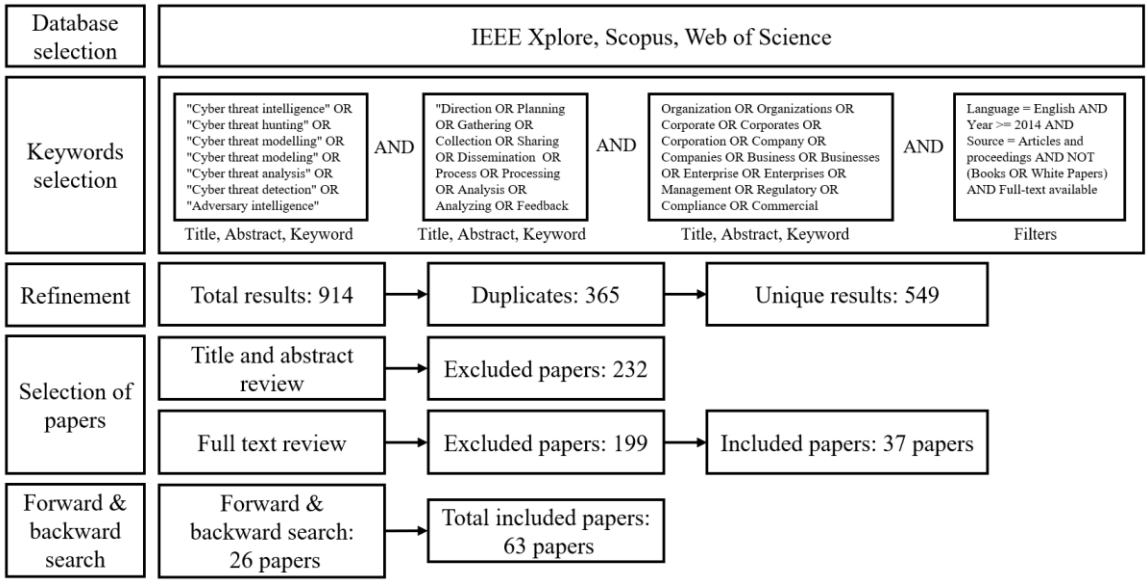

Figure 2 Paper selection process using Webster & Watson method.

A concept matrix is used to organize and analyze the results according to Webster & Watson protocol. The matrix helped to identify key concepts and themes emerging from the body of research and map them against the reviewed articles. A thematic analysis based on Braun and Clarke was conducted to remove duplicates and consolidate findings (Braun & Clarke, 2006). The results are further categorized into PPT dimensions: People dimension consists of knowledge, competence, motivation, engagement of human factor (Prodan et al., 2015); Process as a “set of interrelated or interacting activities that use inputs to deliver an intended result.” (ISO 9000:2015, 2015) and Technology, as systems that integrate

techniques, activities, tools, and artifacts within social contexts, influencing human activity, institutions, and cultural environments (David M. Kaplan, 2003).

3. Results

In this review, the body of literature is examined and organized into three primary categories based on research questions. Each of the following sections corresponds to one of these research questions.

3.1 People Factors

Existing literature emphasizes the importance of skills and training of CTI analysts in determining the perceived value and effectiveness of CTI implementations. For instance, the efficiency of utilizing shared threat intelligence is increased while having well-trained analysts (Miazi et al., 2017; Zibak & Simpson, 2018). Miazi et al. (2017) indicated the knowledge gap as a barrier to threat-hunting implementation, noting that security experts often lack proficiency in data analytics, while data analytics professionals, in turn, lack expertise in cybersecurity. A root cause for this issue is the absence of threat hunting as an integral component of cybersecurity education for security professionals. (Miazi et al., 2017). The knowledge gap has also been recognized as an operational challenge in CTI adoption. For instance, in a case study examining CTI sharing in developing countries, Alkalabi et al. (2021) identify a lack of employee expertise in handling threat intelligence as one of the three primary operational barriers (Alkalabi et al., 2021).

Similarly, other studies have highlighted the knowledge gap as a barrier to identifying relevant CTI (Xu et al., 2020), as well as a contributing factor to the disconnect between technologists and intelligence specialists (Ainslie et al., 2023). Moreover, this gap presents challenges in the integration of Artificial Intelligence (AI) in cybersecurity applications (Aldasoro et al., 2024). The issue is particularly distinct among Small and Medium Enterprises (SMEs), which often possess limited cybersecurity knowledge and resources, making them more vulnerable to cyber threats (van Haastrecht et al., 2021). One specific example of this knowledge gap is the limited awareness of the Traffic Light Protocol (TLP) outside of the technical CTI community, which directly impacts CTI sharing when adherence to TLP guidelines is required (Bromander et al., 2021). Additionally, the adoption of certain CTI standards presents further challenges due to the considerable time and effort required for implementation. For instance, STIX needs a considerable learning curve, requiring personnel to undertake training to effectively integrate it into CTI processes (N. Gong, 2019).

In a study, Zibak et al. (2021) adopted a success model for CTI management platforms and they addressed the importance of the user satisfaction concept which is based on content quality, system quality, service quality, and perceived trust (Zibak et al., 2021). Given the diverse range of users, from operational staff to decision-makers, they argue that addressing user requirements and ensuring satisfaction can impact the adoption of CTI platforms. Additionally, user satisfaction embraces perceived trust in these platforms, which can be strengthened through security measures and compliance with regulations such as the General Data Protection Regulation (GDPR), thereby encouraging user engagement (Zibak et al., 2021). The literature also highlights challenges related to user adoption of CTI processes. For instance, Kotsias et al. (2023) identify reluctance among users to adopt new CTI implementations as a potential barrier (Kotsias et al., 2023). Table 1 provides a summary of people factors influencing CTI adoption.

Table 1 People factors on CTI adoption

Factor	Description
Skills and competence	Gaps between technical and intelligence teams can undermine the effectiveness of CTI. A lack of expertise in relevant standards and regulations can impair the utilization and interoperability of CTI, while also constraining the accurate interpretation and practical application of its insights.
User satisfaction and trust	Meeting users' requirements can enhance user satisfaction, trust, and engagement.
User unwillingness to adopt new processes	Resistance to adopting new CTI processes remains a significant challenge for organizations, potentially delaying the effective implementation of CTI implementations.

3.2 Process Factors

A primary barrier to the adoption of CTI in organizations is the lack of consensus on CTI definitions, key terms, and vocabulary (Ainslie et al., 2023; Alkalabi et al., 2021; N. Gong, 2019; Xiong &

Lagerström, 2019; Zibak & Simpson, 2019b). Effective CTI implementations must be accessible, reliable, relevant to the business context, accurate, and enriched with sufficient contextual information (Amato et al., 2021; Kotsias et al., 2023; van Haastrecht et al., 2021). To enhance decision-making and mitigate cyber threats, CTI should be integrated into board agendas and aligned with overall business processes (Aliyu et al., 2020). The transformation of shared intelligence into actionable insights can be facilitated through expert evaluations and production rules, further reinforcing the value of CTI (van Haastrecht et al., 2021). Additionally, aligning CTI with organizational risk assessment processes is essential for its effective implementation (Sauerwein et al., 2018).

The relevance of CTI to the business context has been recognized in the literature (Wagner et al., 2017; Xu et al., 2019). Ensuring this relevance requires organizations to continuously adapt CTI implementations in response to changes in their business environment (Xu et al., 2019). However, a case study on CTI adoption revealed challenges in its practical application. While CTI provides operational and tactical benefits, it often lacks strategic value for end-users (Kotsias et al., 2023). Furthermore, CTI frequently fails to reach key stakeholders, such as executive decision-makers, and its utilization is often driven by necessity rather than being perceived as a business priority. This limitation contributes to a lack of trust in CTI among senior stakeholders, further hindering its widespread adoption (Kotsias et al., 2023).

Organizational maturity is a critical factor influencing the adoption and effectiveness of CTI and has been examined across multiple dimensions, including the establishment of processes, technological infrastructure, and investment in CTI capabilities (Amato et al., 2021). For instance, in a survey on CTI sharing, half of the respondents assessed their organization's information-sharing program as immature, highlighting a gap in organizational readiness (Zibak & Simpson, 2019b).

The development of in-house competencies is identified in literature as a key strategy for enhancing organizational maturity. Investing in internal expertise, processes, and technology is recommended as a means to reduce reliance on fully outsourced services or standalone CTI specialists (Amato et al., 2021; Kotsias et al., 2023). This need for internal capability is further emphasized by ongoing standardization challenges in the industry, which can hinder the consistent adoption of CTI implementations across organizations. These challenges appear due to the absence of universal standards and interoperability issues stemming from variations in standards used by different entities (Alkalabi et al., 2021; Basha et al., 2023; Keim & Mohapatra, 2022; Sullivan & Burger, 2017).

A mixed-method study on the barriers to adopting STIX and TAXII standards found that government agencies, security technology vendors, military sectors, research and development institutions, and consulting firms are among the primary adopters, while adoption remains limited in the education sector and nonexistent in retail and energy industries (N. Gong, 2019). The study indicates that the implementation of these standards improves multiple aspects of CTI, including structured relationship data sharing, data restriction capabilities, structured documentation markup, and interoperability. However, significant adoption barriers persist, such as the complexity of the initial setup, the learning curve, organizational compatibility, comprehension of cyber threat terminology, and inconsistencies in data notation (N. Gong, 2019).

Evaluating CTI implementation in organizations presents challenges, particularly due to the lack of tangible metrics such as return on investment (ROI) (Ainslie et al., 2023; Kotsias et al., 2023; Zibak & Simpson, 2018). Other key evaluation factors identified in the literature include timeliness, sensitivity, originality, and impact (Griffioen et al., 2020).

Krasznay and Gyebnár (2021) conducted a case study in which they developed an industry-specific CTI feed for Industrial Control Systems and Operational Technology (ICS/OT) networks, with a particular focus on the electricity sector. This initiative was part of establishing an Intelligence Sharing and Analysis Center (ISAC) for the Hungarian Energy and Public Utility Regulatory Authority, aiming to implement both human-readable and repository-based intelligence. A key challenge identified in their study was the absence of clear technical requirements and specifications for the information-sharing platform, which hindered its implementation (Krasznay & Gyebnár, 2021).

Financial constraints also pose a barrier to CTI adoption, as CTI solutions and services require funding from organizations. However, establishing long-term CTI implementations and advancing intelligence sharing among organizations can help mitigate these financial burdens by distributing costs more effectively (Alkalabi et al., 2021). Furthermore, aligning security investments with business continuity plans can enhance the strategic allocation of financial resources, ensuring more sustainable security expenses (Alkalabi et al., 2021; Zibak & Simpson, 2019a). Leadership endorsement is another critical

factor, as securing executive support and adequate financial backing is essential for developing the necessary CTI capabilities (Ainslie et al., 2023; Kotsias et al., 2023).

Another concern regarding CTI adoption is the reluctance of businesses to share threat intelligence due to issues related to confidentiality, privacy, legal uncertainties, and the potential risk of reputational damage. CTI data often contains sensitive information, including personally identifiable information (PII), financial records, and proprietary organizational data, which raises concerns about data protection and compliance (Albakri et al., 2018; Alkalabi et al., 2021; Basha et al., 2023; Chantzios et al., 2019; Skopik et al., 2016; Sullivan & Burger, 2017). These challenges specifically stand out when intelligence data must be shared across jurisdictions, as legal frameworks and regulatory requirements vary across countries and industries (Sullivan & Burger, 2017).

A survey conducted across 61 organizations found that 41% of respondents agreed or strongly agreed that the risk of violating privacy and antitrust laws could impede threat intelligence sharing (Zibak & Simpson, 2019a). Nevertheless, regulatory frameworks such as the General Data Protection Regulation (GDPR) recognize the public interest in cybersecurity, which can sometimes override privacy concerns and facilitate business-to-business data sharing (Sullivan & Burger, 2017). One potential solution is the deidentification of data, although this approach can result in partial data loss and reduce the overall effectiveness of the shared intelligence (S. Gong & Lee, 2020). For organizations implementing automated CTI sharing, additional challenges rise in synchronizing and orchestrating multiple processes effectively (Wagner et al., 2017). A summary of process factors is presented in Table 2.

Table 2 Process factors of CTI adoption

Factor	Description
CTI relevance to business	CTI must be relevant, precise, enriched, and tailored to the organization's business context.
Integration with business processes	Integrating CTI into business processes enhances decision-making and ensures that security measures align with organizational risk assessments.
Organizational maturity	Mature CTI implementations require established processes, appropriate technologies, and sustained investment in CTI tools. Developing in-house CTI expertise can enhance maturity and reduce the dependency on outsourced services, leading to long-term sustainability.
Standardization	Standardization can enhance CTI adoption by addressing challenges posed by immature automation and inconsistent processes. Standards such as STIX can facilitate data exchange and reduce uncertainties, enabling more effective CTI implementation, though their adoption requires considerable effort and adherence to established requirements.
CTI evaluation	Evaluating CTI effectiveness is challenging due to a lack of tangible metrics, such as ROI.
Leadership endorsement	The successful adoption of CTI relies on leadership endorsement and financial investment to develop necessary capabilities.
Trust issues in CTI sharing	Organizations are frequently hesitant to share CTI due to concerns about privacy, legal implications, and reputational risks, particularly when data includes PII or sensitive financial data.
Excessive costs	The excessive costs associated with CTI solutions present a challenge that could be improved through collaborative CTI sharing among organizations.
Resource constraints	Limited resources and staffing shortages can hinder an organization’s ability to proactively respond to cyber threats.

3.3 Technology Factors

Literature highlights the challenge of manual processes in CTI implementations. A systematic literature review on threat modeling by Xiong and Lagerström (2019) found that most threat modeling processes are still conducted manually, with limited validation mechanisms (Xiong & Lagerström, 2019). Similarly, studies indicate that Threat Intelligence Platforms (TIPs) lack essential capabilities, such as filtering CTI based on relevance and risk priority, requiring practitioners to manually correct, evaluate, analyze, and interpret the data (Bromander et al., 2021; van Haastrecht et al., 2021; Wagner et al., 2017). Additionally, the manual selection of relevant security feeds extends response times and increases the risk of missing critical opportunities for effective mitigation (Arikkat et al., 2024). The need for automation has been widely discussed as a solution to address challenges such as human error and processing delays (Amato et al., 2021; Berndt & Ophoff, 2020; Wagner et al., 2019; Zibak & Simpson, 2018). Automation can also improve the speed and efficiency of intelligence exchange (Sullivan & Burger, 2017). However, developing these capabilities requires considerable time and resources, posing an additional challenge for organizations seeking to implement them (Chantzios et al., 2019).

Data quality is a critical concern in literature on CTI. In a case study on CTI challenges in Saudi Arabia, Alkalabi et al. (2021) identified the absence of a centralized system for CTI exchange, the lack of standardized data formats and taxonomy, and difficulties in establishing secure communication

channels as primary barriers to CTI sharing. (Alkalabi et al., 2021). One of the primary causes of data inconsistency is the existence of multiple representations of the same CTI data (Bromander et al., 2021). Some organizations enrich CTI data using flexible standards such as STIX; however, this can create interoperability challenges for other organizations attempting to consume shared data (Bromander et al., 2021). Sauerwein et al. (2019) categorize CTI data sources into six key dimensions: type of information, integrability, timeliness, originality, type of source, and trustworthiness. Their study highlights that a significant portion of CTI data sources focus on vulnerabilities (Sauerwein et al., 2019). Handling incomplete and imprecise raw data remains a challenge, particularly when data is gathered from public sources, which often contain unstructured content, originates from unverified providers, or include deliberately manipulated information (S. Gong & Lee, 2020; Sauerwein et al., 2019). Xu et al. (2020) emphasize that "information in real-world systems is usually vague, imprecise, inconsistent, and incomplete", further complicating CTI processing and analysis (Xu et al., 2020, p. 1).

Advancements in data collection techniques, such as the development of custom crawlers and machine learning models, enhance the ability to filter relevant data efficiently (Arikkat et al., 2024). However, integrating this data into organizational workflows is further complicated by the limitations of software interfaces, such as Application Programming Interfaces (APIs), which often provide only basic search functionalities (Sauerwein et al., 2019). Additional constraints exist within CTI platforms, including restricted customization options, challenges in stream aggregation, and filtering limitations (Sillaber et al., 2016). The timeliness of CTI feeds is another factor affecting data quality. Delays in updating threat intelligence reduce its effectiveness, as real-time information is essential for proactive threat mitigation. A study evaluating 24 open-source CTI feeds containing 1.38 million indicators found that, on average, it takes up to 21 days for an indicator of compromise to be included in a CTI feed, limiting its usefulness in mitigating threats (Griffioen et al., 2020). The same study also highlights geographic biases in CTI feeds, which may affect the relevance of threat detection for organizations outside specific regions. Additionally, not all CTI feed data is original, as some sources rely on repackaging, aggregation, and curation rather than directly producing new intelligence (Griffioen et al., 2020). To improve data reliability, some researchers propose implementing user-feedback mechanisms, such as reliability scoring, to validate CTI information and enhance trustworthiness (S. Gong & Lee, 2020; Sauerwein et al., 2019). Normalization and consolidation, supported by advanced analytics and data linkage, can further address data inconsistency issues (Brown et al., 2015).

Automated mechanisms, such as the Malware Information Sharing Platform (MISP), have been proposed as solutions to improve the quality of shared CTI (Kotsias et al., 2023; Mundt & Baier, 2022; van Haastrecht et al., 2021; Zibak et al., 2021). Additionally, integrating data processing and analytics capabilities within TIPs can facilitate the generation of actionable intelligence, differentiating data aggregators from data processors (Zibak et al., 2021).

Managing large datasets to identify relevant vulnerabilities remains a significant challenge due to the increasing volume of cyber threat data (Sadlek et al., 2022). The complexity of processing diverse information sources imposes additional demands on organizations in terms of time and effort (Amato et al., 2021; Arikkat et al., 2024; Sadlek et al., 2022; van Haastrecht et al., 2021; Voutilainen & Kari, 2020). As cyber threats become more sophisticated and automated, CTI implementations must incorporate appropriate service architectures, including automation and orchestration, to enhance efficiency (Sullivan & Burger, 2017). False positives and imprecise data further complicate CTI integration (Sadlek et al., 2022), particularly when unstructured data must be reconciled with existing threat intelligence repositories (Husari et al., 2017; Rahman et al., 2023; Sauerwein et al., 2019). Additionally, shared CTI data often lacks necessary contextual information, limiting its practical utility (van Haastrecht et al., 2021). In this regard, the application of Artificial Intelligence (AI) and Natural Language Processing (NLP) in CTI has been identified to help process large volumes of data, extract intelligence from human-readable sources, and reduce manual workload (Basha et al., 2023; Husari et al., 2017; Sadlek et al., 2022). Moreover, the implementation of advanced visualization techniques can support the analysis of diverse CTI datasets, improving situational awareness and decision-making (Brown et al., 2015). A summary of technology factors is provided in Table 3.

Table 3 Technology factors of CTI adoption

Factor	Description
Interoperability	The lack of standardization and interoperability across organizations results in inconsistent CTI data usage, as differing standards and representations of the same data lead to compatibility challenges.
Data quality	The effectiveness of CTI is compromised by incomplete, imprecise, biased, or manipulated data from untrustworthy sources, delays in feed updates, and challenges in managing large volumes of heterogeneous data, including false positives and unstructured formats. Enhancing CTI relevance and trustworthiness requires more

	frequent updates, feedback mechanisms to validate data accuracy, and consolidation of data into unified formats through advanced analytics. Additionally, relying on original feeds helps mitigate biases introduced by intermediate processors, improving interoperability and data quality.
TIP capabilities	Effective CTI systems depend on robust service designs with automation and orchestration capabilities, yet their efficiency is hindered by limited search and integration functionalities in software interfaces, such as APIs. The lack of centralized systems, standardized data formats, and secure communication channels further obstruct inter-organizational CTI sharing. Enhanced visualization tools, automation, and standardized platforms facilitate better insights, decision-making, and streamlined data sharing and processing, thereby improving CTI quality.
Data processing and analytics	Integrating data processing and analytics capabilities within CTI platforms enhances intelligence generation by distinguishing between raw data aggregation and actionable insights. Custom crawlers and machine learning models improve data collection and filtering, enabling more effective identification of relevant information. Additionally, the use of AI, big data, text mining, and NLP technologies automates the extraction of CTI from human-readable sources, reducing the need for manual processing and effort.
Automation	Automation is essential for effective CTI sharing, as it mitigates challenges such as human error and processing delays. While TIPs often rely on manual processing and expert interpretation to produce actionable outputs, automation remains necessary despite difficulties in achieving synchronization and orchestration across diverse processes.

4. Discussion

This SLR identifies and synthesizes the key factors influencing the adoption of CTI in organizations, focusing on the people, process, and technology dimensions. While the findings offer novel insights, they also expose considerable gaps in the existing body of literature. These findings are consistent with prior research (Abu et al., 2018; Ainslie et al., 2023; Lundgren & Padyab, 2023), emphasizing the integration of cybersecurity initiatives with organizational goals and strategies. However, this study advances existing knowledge by providing a holistic exploration of CTI adoption through the interconnected lenses of people, processes, and technology. This multidimensional perspective enables a more comprehensive understanding of the organizational dynamics shaping CTI integration.

People factors stand out as a critical yet underrepresented dimension in existing literature. Prior studies like (Kotsias et al., 2023) often conceptualize people's involvement in CTI adoption narrowly, focusing on “users” rather than exploring deeper aspects such as expertise, competence, and organizational culture. The findings expand this understanding, emphasizing the importance of the expertise of people as a cornerstone of successful CTI adoption. This perspective emphasizes the need for a more sophisticated exploration of people’s dimensions in cybersecurity implementations. In this regard, future studies can explore whether there is a causal relationship between enhancing people factors and CTI adoption.

Previous surveys have primarily concentrated on technological barriers to CTI application within organizations (Tounsi & Rais, 2018) or specific aspects such as challenges in CTI (Brown et al., 2015; Skopik et al., 2016; Wagner et al., 2019) and issues related to data quality (Sillaber et al., 2016). In contrast, the findings of this paper emphasize the significance of aligning CTI initiatives with broader business characteristics such as strategy and business context and the critical role of the people factor.

Organizational maturity stands out as an underexplored factor in the existing CTI adoption literature. This gap becomes particularly visible as the literature extensively addresses various aspects of process improvement, such as automation and process efficiency (Ainslie et al., 2023; Aliyu et al., 2020; Kotsias et al., 2023), yet pays limited attention to the role of organizational maturity in shaping CTI adoption.

The analysis identifies unique CTI-specific factors, such as CTI metrics and trust, while the remaining process factors, including leadership endorsement and barriers to CTI sharing, align with general cybersecurity practice considerations. These findings reinforce prior research on factors contributing to the successful adoption of CTI within a cybersecurity ecosystem.

Several factors exhibit bidirectional overlap or influence on others. For instance, people's skills and competence can directly affect an organization's in-house capabilities and overall maturity. Similarly, the data quality factor impacts other elements, such as CTI evaluation and trust issues in CTI sharing. This requires more in-depth investigation beyond the scope of our current literature review. Since the bidirectional influences we identified emerge as insights from the synthesis rather than explicit findings in the literature, further empirical validation with practitioners would be necessary to ensure accuracy and avoid speculative bias. This presents an opportunity for future research, where practitioner input and additional studies could help map these relationships more systematically.

This SLR highlights several technical challenges to CTI adoption, including gaps in standardization, limitations in TIPs, and barriers to effective CTI sharing. Among these, data quality emerges as the most frequently cited challenge, often originating from unstructured CTI data sources that lack standardization and proper pre-processing. Advanced technologies, such as generative AI and machine learning, are identified in the literature as promising solutions to mitigate these data quality issues (Sadlek et al., 2022; Samtani et al., 2020). These findings have important practical implications for organizations adopting CTI. By aligning CTI initiatives with business objectives and investing in people expertise, organizations can significantly improve the effectiveness of their cybersecurity efforts.

This study is constrained by the limited number of databases (IEEE, Web of Science, and Scopus); however, including additional sources in future research could enrich the literature base and provide a broader perspective.

The study of the interaction between the elements of people, processes, and technology fell out of the scope of this review. However, understanding how these dimensions influence each other during CTI adoption is a fruitful avenue for future research. Future research should prioritize empirical investigations, including longitudinal studies, to examine the evolution of CTI implementations over time and their long-term impact on organizational cybersecurity. Additionally, studies focusing on industry-specific factors, such as regulatory requirements in critical infrastructure sectors, would provide valuable insights. Expanding the body of use-case studies with empirical data is essential for developing actionable guidelines and best practices.

5 Conclusion

This systematic literature review examined the factors influencing the adoption of CTI in organizational environments. The findings reveal that CTI adoption is a multifactorial challenge shaped by three key factors: people, process, and technology. Alignment with organizational goals, the quality of CTI data, and the availability of skilled personnel were identified as pivotal factors for successful implementation. Tailoring these elements to an organization's specific context is critical for addressing existing gaps and ensuring effective CTI adoption. However, significant barriers, such as gaps in organizational maturity, people competence, and limited empirical research, persist. Future research should prioritize use-case studies and empirical investigations to advance the field and provide actionable insights for organizations. Addressing these gaps could help the development of more effective CTI strategies, strengthening the ability of organizations to navigate emerging cybersecurity threats.

References

Abu, M. S., Selamat, S. R., Ariffin, A., & Yusof, R. (2018). Cyber Threat Intelligence – Issue and Challenges. *Indonesian Journal of Electrical Engineering and Computer Science*, *10*(1), Article 1. https://doi.org/10.11591/ijeecs.v10.i1.pp371-379

Ainslie, S., Thompson, D., Maynard, S., & Ahmad, A. (2023). Cyber-threat intelligence for security decision-making: A review and research agenda for practice. *Computers & Security*, *132*, 103352. https://doi.org/10.1016/j.cose.2023.103352

Albakri, A., Boiten, E., & De Lemos, R. (2018). Risks of Sharing Cyber Incident Information. *Proceedings of the 13th International Conference on Availability, Reliability and Security*, 1–10. https://doi.org/10.1145/3230833.3233284

Aldasoro, I., Doerr, S., Gambacorta, L., Notra, S., Oliviero, T., & Whyte, D. (2024). Generative Artificial Intelligence and Cyber Security in Central Banking. *Journal of Financial Regulation*, fjae008. https://doi.org/10.1093/jfr/fjae008

Aliyu, A., He, Y., Yevseyeva, I., & Luo, C. (2020). Cyber Security Decision Making Informed by Cyber Threat Intelligence (CYDETI): IEEE CNS 20 Poster. *2020 IEEE Conference on Communications and Network Security (CNS)*, 1–2. https://doi.org/10.1109/CNS48642.2020.9162162

Alkalabi, W., Simpson, L., & Morarji, H. (2021). Barriers and Incentives to Cybersecurity Threat Information Sharing in Developing Countries: A Case Study of Saudi Arabia. *Proceedings of the 2021 Australasian Computer Science Week Multiconference*, 1–8. https://doi.org/10.1145/3437378.3437391

Allen, J. D., Towne, S. D., Maxwell, A. E., DiMartino, L., Leyva, B., Bowen, D. J., Linnan, L., & Weiner, B. J. (2017). Measures of organizational characteristics associated with adoption and/or implementation of innovations: A systematic review. *BMC Health Services Research*, *17*(1), 591. https://doi.org/10.1186/s12913-017-2459-x

Amato, G., Ciccarone, S., Digregorio, P., & Natalucci, G. (2021). *A Service Architecture for an Enhanced Cyber Threat Intelligence Capability*. Italian Conference on Cybersecurity.

https://www.semanticscholar.org/paper/A-Service-Architecture-for-an-Enhanced-Cyber-Threat-Amato-Ciccarone/a0e045567f509f2fdabdc70ed6f927e6c4e2ce9c

Arikkat, D. R., P., V., K.a., R. R., Nicolazzo, S., Nocera, A., Timpau, G., & Conti, M. (2024). OSTIS: A novel Organization-Specific Threat Intelligence System. *Computers & Security*, *145*, 103990. https://doi.org/10.1016/j.cose.2024.103990

Basha, C. B., Aggarwal, S., Esanmurodova, N., Alabdeli, H., Tiwari, A., Sathi, G., & Ritwika, S. (2023). Fostering Effective Cyber Threat Intelligence Sharing: Overcoming Challenges and Implementing Best Practices. *2023 International Conference for Technological Engineering and Its Applications in Sustainable Development (ICTEASD)*, 177–182. https://doi.org/10.1109/ICTEASD57136.2023.10585133

Berndt, A., & Ophoff, J. (2020). Exploring the Value of a Cyber Threat Intelligence Function in an Organization. In L. Drevin, S. Von Solms, & M. Theocharidou (Eds.), *Information Security Education. Information Security in Action* (pp. 96–109). Springer International Publishing. https://doi.org/10.1007/978-3-030-59291-2_7

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Bromander, S., Swimmer, M., Muller, L. P., Jøsang, A., Eian, M., Skjøtskift, G., & Borg, F. (2021). Investigating Sharing of Cyber Threat Intelligence and Proposing A New Data Model for Enabling Automation in Knowledge Representation and Exchange. *Digital Threats*, *3*(1), 6:1-6:22. https://doi.org/10.1145/3458027

Brown, S., Gommers, J., & Serrano, O. (2015). From Cyber Security Information Sharing to Threat Management. *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, 43–49. https://doi.org/10.1145/2808128.2808133

Chantzios, T., Koloveas, P., Skiadopoulos, S., Kolokotronis, N., Tryfonopoulos, C., Bilali, V.-G., & Kavallieros, D. (2019). The Quest for the Appropriate Cyber-threat Intelligence Sharing Platform: *Proceedings of the 8th International Conference on Data Science, Technology and Applications*, 369–376. https://doi.org/10.5220/0007978103690376

David M. Kaplan. (2003). *Ricoeur's Critical Theory*. SUNY Press. https://libraryproxy.his.se/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=112744&site=ehost-live

Ghaffari, F., Gharaee, H., & Arabsorkhi, A. (2019). Cloud Security Issues Based on People, Process and Technology Model: A Survey. *2019 5th International Conference on Web Research (ICWR)*, 196–202. https://doi.org/10.1109/ICWR.2019.8765295

Gong, N. (2019). Barriers to Adopting Interoperability Standards for Cyber Threat Intelligence Sharing: An Exploratory Study. In K. Arai, S. Kapoor, & R. Bhatia (Eds.), *Intelligent Computing* (pp. 666–684). Springer International Publishing. https://doi.org/10.1007/978-3-030-01177-2_49

Gong, S., & Lee, C. (2020). BLOCIS: Blockchain-Based Cyber Threat Intelligence Sharing Framework for Sybil-Resistance. *Electronics*, *9*(3), Article 3. https://doi.org/10.3390/electronics9030521

Griffioen, H., Booij, T., & Doerr, C. (2020). Quality Evaluation of Cyber Threat Intelligence Feeds. In M. Conti, J. Zhou, E. Casalicchio, & A. Spognardi (Eds.), *Applied Cryptography and Network Security* (pp. 277–296). Springer International Publishing. https://doi.org/10.1007/978-3-030-57878-7_14

Husari, G., Al-Shaer, E., Ahmed, M., Chu, B., & Niu, X. (2017). TTPDrill: Automatic and Accurate Extraction of Threat Actions from Unstructured Text of CTI Sources. *Proceedings of the 33rd Annual Computer Security Applications Conference*, 103–115. https://doi.org/10.1145/3134600.3134646

ISO 9000:2015. (2015). *ISO 9000:2015(en), Quality management systems—Fundamentals and vocabulary*. https://www.iso.org/obp/ui/#iso:std:iso:9000:en

Javaid, M. I., & Iqbal, M. M. W. (2017). A comprehensive people, process and technology (PPT) application model for Information Systems (IS) risk management in small/medium enterprises (SME). *2017 International Conference on Communication Technologies (ComTech)*, 78–90. https://doi.org/10.1109/COMTECH.2017.8065754

Jesus, V., Bains, B., & Chang, V. (2024). Sharing Is Caring: Hurdles and Prospects of Open, Crowd-Sourced Cyber Threat Intelligence. *IEEE Transactions on Engineering Management*, *71*, 6854–6873. IEEE Transactions on Engineering Management. https://doi.org/10.1109/TEM.2023.3279274

Keim, Y., & Mohapatra, A. K. (2022). Cyber threat intelligence framework using advanced malware forensics. *International Journal of Information Technology*, *14*(1), 521–530. https://doi.org/10.1007/s41870-019-00280-3

Kotsias, J., Ahmad, A., & Scheepers, R. (2023). Adopting and integrating cyber-threat intelligence in a commercial organisation. *European Journal of Information Systems*, *32*(1), 35–51. https://doi.org/10.1080/0960085X.2022.2088414

Krasznay, C., & Gyebnár, G. (2021). Possibilities and Limitations of Cyber Threat Intelligence in Energy Systems. *2021 13th International Conference on Cyber Conflict (CyCon)*, 171–188. https://doi.org/10.23919/CyCon51939.2021.9468289

Lundgren, M., & Padyab, A. (2023). A Review of Cyber Threat (Artificial) Intelligence in Security Management. In T. Sipola, T. Kokkonen, & M. Karjalainen (Eds.), *Artificial Intelligence and Cybersecurity: Theory and Applications* (pp. 29–45). Springer International Publishing. https://doi.org/10.1007/978-3-031-15030-2_2

McMillan, R. (2023). *Definition: Threat Intelligence*. Gartner. https://www.gartner.com/en/documents/2487216

Miazi, M. N. S., Pritom, M. M. A., Shehab, M., Chu, B., & Wei, J. (2017). The Design of Cyber Threat Hunting Games: A Case Study. *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, 1–6. https://doi.org/10.1109/ICCCN.2017.8038527

Mundt, M., & Baier, H. (2022). Towards Mitigation of Data Exfiltration Techniques Using the MITRE ATT&CK Framework. In P. Gladyshev, S. Goel, J. James, G. Markowsky, & D. Johnson (Eds.), *Digital Forensics and Cyber Crime* (pp. 139–158). Springer International Publishing. https://doi.org/10.1007/978-3-031-06365-7_9

Prodan, M., Prodan, A., & Purcarea, A. A. (2015). Three New Dimensions to People, Process, Technology Improvement Model. In A. Rocha, A. M. Correia, S. Costanzo, & L. P. Reis (Eds.), *New Contributions in Information Systems and Technologies* (pp. 481–490). Springer International Publishing. https://doi.org/10.1007/978-3-319-16486-1_47

Rahman, M. R., Mahdavi-Hezaveh, R., & Williams, L. (2023). What are the attackers doing now? Automating cyber threat intelligence extraction from text on pace with the changing threat landscape: A survey. *ACM Computing Surveys*, *55*(12), 1–36. https://doi.org/10.1145/3571726

Sadlek, L., Čeleda, P., & Tovarňák, D. (2022). Current Challenges of Cyber Threat and Vulnerability Identification Using Public Enumerations. *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 1–8. https://doi.org/10.1145/3538969.3544458

Samtani, S., Abate, M., Benjamin, V., & Li, W. (2020). Cybersecurity as an Industry: A Cyber Threat Intelligence Perspective. In T. J. Holt & A. M. Bossler (Eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 135–154). Springer International Publishing. https://doi.org/10.1007/978-3-319-78440-3_8

Satwekar, A., Miozza, M., Abbattista, C., Palumbo, S., & Rossi, M. (2024). Triad of Digital Transformation: Holistic Orchestration for People, Process, and Technology. *IEEE Transactions on Engineering Management*, *71*, 7815–7831. IEEE Transactions on Engineering Management. https://doi.org/10.1109/TEM.2024.3384995

Sauerwein, C., Pekaric, I., Felderer, M., & Breu, R. (2019). An analysis and classification of public information security data sources used in research and practice. *Computers & Security*, *82*, 140–155. https://doi.org/10.1016/j.cose.2018.12.011

Sauerwein, C., Sillaber, C., & Breu, R. (2018). Shadow Cyber Threat Intelligence and Its Use in Information Security and Risk Management Processes. *MKWI*, 1333–1344. https://www.researchgate.net/profile/Clemens-Sauerwein-2/publication/358425641_Shadow_Cyber_Threat_Intelligence_and_Its_Use_in_Information_Security_and_Risk_Management_Processes/links/62022da400a69e030648feec/Shadow-Cyber-Threat-Intelligence-and-Its-Use-in-Information-Security-and-Risk-Management-Processes.pdf

Sillaber, C., Sauerwein, C., Mussmann, A., & Breu, R. (2016). Data Quality Challenges and Future Research Directions in Threat Intelligence Sharing Practice. *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*, 65–70. https://doi.org/10.1145/2994539.2994546

Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, *60*, 154–176. https://doi.org/10.1016/j.cose.2016.04.003

Sullivan, C., & Burger, E. (2017). "In the public interest": The privacy implications of international business-to-business sharing of cyber-threat intelligence. *Computer Law & Security Review*, *33*(1), 14–29. https://doi.org/10.1016/j.clsr.2016.11.015

Taher, A. (2023). Stakeholders' opinions support the people-process-technology framework for implementing digital transformation in higher education. *Technology, Pedagogy and Education*, *32*(5), 555–567. https://doi.org/10.1080/1475939X.2023.2248134

Teoh, C. S., Kamil Mahmood, A., & Dzazali, S. (2018). Cyber Security Challenges in Organisations: A Case Study in Malaysia. *2018 4th International Conference on Computer and Information Sciences (ICCOINS)*, 1–6. https://doi.org/10.1109/ICCOINS.2018.8510569

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, *72*, 212–233. https://doi.org/10.1016/j.cose.2017.09.001

van Haastrecht, M., Golpur, G., Tzismadia, G., Kab, R., Priboi, C., David, D., Răcătăian, A., Baumgartner, L., Fricker, S., Ruiz, J. F., Armas, E., Brinkhuis, M., & Spruit, M. (2021). A Shared Cyber Threat Intelligence Solution for SMEs. *Electronics*, *10*(23), Article 23. https://doi.org/10.3390/electronics10232913

Voutilainen, J., & Kari, M. (2020, June 26). Strategic Cyber Threat Intelligence: Building the Situational Picture with Emerging Technologies. *Proceedings of the 19th European Conference on Cyber Warfare*. The 19th European Conference on Cyber Warfare. https://doi.org/10.34190/EWS.20.030

Wagner, T. D., Mahbub, K., Palomar, E., & Abdallah, A. E. (2019). Cyber threat intelligence sharing: Survey and research directions. *Computers & Security*, *87*, 101589. https://doi.org/10.1016/j.cose.2019.101589

Wagner, T. D., Palomar, E., Mahbub, K., & Abdallah, A. E. (2017). Relevance Filtering for Shared Cyber Threat Intelligence (Short Paper). In J. K. Liu & P. Samarati (Eds.), *Information Security Practice and Experience* (pp. 576–586). Springer International Publishing. https://doi.org/10.1007/978-3-319-72359-4_35

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, *26*(2), xiii–xxiii.

Xiong, W., & Lagerström, R. (2019). Threat modeling – A systematic literature review. *Computers & Security*, *84*, 53–69. https://doi.org/10.1016/j.cose.2019.03.010

Xu, Y., Yang, Y., & He, Y. (2019). A Business Process Oriented Dynamic Cyber Threat Intelligence Model. *2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, 648–653. https://doi.org/10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00147

Xu, Y., Yang, Y., & He, Y. (2020). A Representation of Business Oriented Cyber Threat Intelligence and the Objects Assembly. *2020 10th International Conference on Information Science and Technology (ICIST)*, 105–113. https://doi.org/10.1109/ICIST49303.2020.9202271

Zibak, A., Sauerwein, C., & Simpson, A. (2021). A success model for cyber threat intelligence management platforms. *Computers & Security*, *111*, 102466. https://doi.org/10.1016/j.cose.2021.102466

Zibak, A., & Simpson, A. (2018). Can We Evaluate the Impact of Cyber Security Information Sharing? *2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, 1–2. https://doi.org/10.1109/CyberSA.2018.8551462

Zibak, A., & Simpson, A. (2019a). Cyber Threat Information Sharing: Perceived Benefits and Barriers. *Proceedings of the 14th International Conference on Availability, Reliability and Security*, 1–9. https://doi.org/10.1145/3339252.3340528

Zibak, A., & Simpson, A. (2019b). Towards Better Understanding of Cyber Security Information Sharing. *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, 1–8. https://doi.org/10.1109/CyberSA.2019.8899697