POSTPRINT VERSION. The final version is published here :
Le, T. D., Le Dinh, T. et Uwizeyemungu, S. (2025). A cybersecurity framework for enhancing Small and medium-sized enterprises (SMEs) security posture using user behaviour analytics. Enterprise Information Systems (p. 2529282): Taylor & Francis. doi: https://doi.org/10.1080/17517575.2025.2529282

A Cybersecurity Framework for Enhancing Small and Medium-sized Enterprises (SMEs) Security Posture Using User Behaviour Analytics

Tran Duc Le[a], Thang Le Dinh[b] and Sylvestre Uwizeyemungu[b]

[a]University of Wisconsin-Stout, Menomonie, Wisconsin, USA, Email: let@uwstout.edu
[b]Université du Québec à Trois-Rivières, Trois-Rivières, Québec, Canada, Email: thang.ledinh@uqtr.ca, sylvestre.uwizeyemungu@uqtr.ca

ARTICLE HISTORY
Compiled July 7, 2025

ABSTRACT
Small and Medium-sized Enterprises (SMEs) are increasingly targeted by complex cyber threats yet often lack tailored, advanced cybersecurity measures. This research fills a critical gap by introducing a novel cybersecurity framework designed to make sophisticated user behaviour analytics practical, accessible, and impactful for these enterprises, thereby aiming to significantly enhance their cyber resilience. The framework is distinctively structured with a multi-layered approach, leverages user behaviour analytics aligned with the NIST Cybersecurity Framework (NIST CSF), and uniquely integrates with the existing TRIVI customer intelligence model. Advanced data analytics and a proposed cloud-based implementation using tools like the Elastic Stack underpin the solution. The primary contributions offer considerable advantages for SMEs: (1) A multi-layered cybersecurity framework specifically tailored to SME needs and resource levels, leveraging user behaviour data to enable practical proactive threat detection. (2) Novel integration with the TRIVI business intelligence framework, allowing for the efficient transformation of existing data into enriched security intelligence. (3) Demonstrated alignment of the framework's layers with all five NIST CSF core functions, providing SMEs a standards-based path to systematically improve their security posture and aid compliance. (4) A proposed cost-effective and scalable cloud implementation model, designed to make advanced cybersecurity analytics financially and technically accessible. These aspects deliver superior SME accessibility and a stronger user behaviour focus compared to many traditional SIEM solutions. Ultimately, the framework establishes a vital blueprint for SMEs to effectively harness user behaviour data, thereby strengthening their cyber resilience, supporting business continuity, and enhancing competitiveness in a challenging digital landscape. Future work will concentrate on the implementation, assessment, and enhancement of this framework across diverse SME segments, underscoring the continuous significance of such cybersecurity advancements for SME sustainability and growth.

KEYWORDS
Cybersecurity Analytic; User Behaviour Analytics; SMEs; NIST; TRIVI

1. Introduction

In the current digital age, when cooperation with customers and business partners via online transactions and communications has become the norm, cybersecurity is a

Corresponding author: Tran Duc Le. Email: let@uwstout.edu growing concern for all businesses (Williquette 2019; Olayinka and Win 2022). While cybersecurity is a critical concern for all businesses, the impact of cyber threats can be disproportionately severe for Small and Medium-sized Enterprises (SMEs), which often have fewer resources and less specialized expertise to dedicate to cybersecurity defenses compared to larger organizations (Ozkan and Spruit 2020; Jahankhani, Meda, and Samadi 2022). Without adequate cybersecurity measures in place, SMEs are more vulnerable to cyber-attacks and data breaches, which can have devastating consequences for their operations and reputation (Chidukwani, Zander, and Koutsakis 2022; Fernandez De Arroyabe and Fernandez de Arroyabe 2023). The increased exposure underlines the need for stringent cybersecurity protocols or procedures to protect their digital resources and uphold the trust of their customers.

User behaviours significantly shape cybersecurity outcomes and often serve as a primary determinant of a system's vulnerability or resilience (Moustafa and Bello 2021; Kannelønning and Katsikas 2023). These behaviours span a range of actions and habits related to users' interaction with technology and digital platforms (El Haddad, Shahab, and Aïmeur 2018; Acton, Datta, and Hughes 2023). In a technical context, these behaviour data include but are not limited to system logins, network and application interactions, and are often documented in log files (Wu, Tang, and Pan 2022; Jackson, Crowston, and Østerlund 2018). Occasionally, this data category is referred to as **user and entity behaviour data** (Shashanka, Shen, and Wang 2016; Khaliq, Tariq, and Masood 2020). From now on, for the sake of simplicity, it shall be referred to as **user behaviour data**.

On the business side, user behaviours involve web browsing habits, online shopping preferences, and transaction details (Liu et al. 2021; Hong and Furnell 2021). These behaviours expand the data scope, requiring protection, as they typically involve exchanging and storing personal user information (Zhao et al. 2019). The absence of robust measures to supervise and control the potential risks linked with user behaviours leaves the digital infrastructure of many SMEs open to a plethora of cyber threats.

The primary objective of this research is to design a robust and data-driven framework that leverages user behaviour data to enhance cybersecurity in SMEs. Drawing inspiration from the TRIVI framework (Le Dinh et al. 2022), initially conceptualised for enhancing customer intelligence in SMEs, the study proposes to extend it with additional modules that harness user behaviour data to enhance cybersecurity. The data collected through the TRIVI framework, mainly the user behaviour information related to web browsing habits, online shopping preferences, and transaction details, will also serve as part of the inputs for our proposed framework. Moreover, by integrating advanced analytical techniques and machine learning algorithms, this study aspires to construct a robust, data-driven framework that enables SMEs to predict, prevent, and mitigate cyber threats effectively.

In addition, the proposed solution is aligned with the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) (Pascoe 2023). By adopting the NIST framework as the foundation for the solution, this study ensures compatibility with established best practices and facilitates a shared understanding of cybersecurity challenges. This alignment is particularly advantageous for SMEs, enabling them to leverage user behaviour data effectively, maintain resilience against cyber threats, and seamlessly integrate within the broader cybersecurity ecosystem.

The main contributions of this research include:

- A cybersecurity framework tailored for SMEs, featuring a multi-layered archi-

tecture (Data, Analytics, Reporting, Decision) with dedicated modules (e.g., Collection, Standardization, Threat Detection, Security Analysis, Visualization, Recommendation) designed to systematically process user behaviour data for security insights;
- Integration with the established TRIVI framework to enhance its specific customer intelligence capabilities into general business intelligence capabilities;
- Alignment of the framework with the NIST CSF to ensure adherence to industry best practices and facilitate seamless integration;
- A cloud-based implementation strategy as a sample realisation to ensure accessibility and cost-effectiveness for SMEs.

The remainder of this paper is structured as follows. Section 2 provides a literature review of the research context. Section 3 delves into the specific types and sources of user behaviour data considered in the proposed framework. Section 4 presents the methodology, detailing the Cybersecurity Behaviour Analysis Triad (CBAT) that forms the framework's foundation. Section 5 elaborates on the framework development, discussing the multi-layered approach and individual modules. Section 6 demonstrates the alignment of the proposed framework with the NIST CSF. Section 7 outlines the technical implementation and cloud deployment strategy using the Elastic Stack. Section 8 discusses the advantages of the proposed framework over traditional Security Information and Event Management (SIEM) solutions, strategies for implementation and evaluation, and potential challenges. Finally, Section 9 concludes the paper, summarising the essential findings and outlining future research directions.

2. Literature Review

2.1. *Cybersecurity Challenges in SMEs*

Resource constraints are one of the most significant challenges SMEs face in developing robust cybersecurity measures (Kandpal et al. 2023). Kabanda et al. (Kabanda, Tanner, and Kent 2018) highlight that SMEs struggle with internal factors such as budget, management support, and attitudes towards cybersecurity, which limit their ability to implement effective cybersecurity practices. These constraints not only hinder the adoption of advanced cybersecurity technologies (Trantidou et al. 2022) but also affect the overall cybersecurity culture (Sutton and Tompson 2025) within the organisation, making SMEs susceptible to various online threats (Heikkilä et al. 2016; El Haddad, Shahab, and Aïmeur 2018; Le, Le-Dinh, and Uwizeyemungu 2024).

In addition, the **lack of tailored cybersecurity methodologies** that address SMEs' specific needs and capabilities further complicates their cybersecurity efforts. Kavakli et al. (Kavakli, Loucopoulos, and Skourtis 2022) emphasised the absence of appropriate guidelines catering to SME requirements and proposed a Requirements Engineering (RE) methodology to bridge this gap. This approach underscores the necessity for SMEs to implement cybersecurity frameworks that are effective and feasible, considering their limited resources.

Moreover, the **readiness** of SMEs to tackle cybersecurity threats is another area of concern (Mitrofan, Cruceru, and Barbu 2020; White et al. 2022). Perozzo et al. (Perozzo, Zaghloul, and Ravarini 2022) introduce a CyberSecurity Readiness Model for SMEs based on a Socio-Technical perspective, acknowledging that SMEs are among the most vulnerable and least mature regarding cybersecurity resilience. This model provides a structured approach to assessing and enhancing SMEs' readiness to prevent and manage cyber-attacks, focusing on cybersecurity's technological and organisational dimensions. Rawindaran (Rawindaran 2023) underscores the lack of cybersecurity **awareness and skills issues** within SMEs, noting that despite the heightened risk of cyber incidents, a significant gap exists in cybersecurity knowledge and preparedness. This gap hinders effective cyber risk management and exacerbates vulnerabilities to phishing, ransomware, and other cyber-attacks (MacColl et al. 2023).

Applying machine learning and artificial intelligence in threat hunting and cybersecurity poses both an opportunity and a challenge for SMEs. While such technologies offer advanced capabilities in detecting and mitigating cyber threats, SMEs often **lack the technical expertise** and resources to implement and manage these technologies effectively (Lozano, Llopis, and Domingo 2023; Kent, Tanner, and Kabanda 2016; Nagahawatta et al. 2021). Furthermore, strategic management approaches to digitalisation, including adopting cybersecurity governance frameworks, remain underutilised in SMEs (Rawindaran et al. 2023).

2.2. *Cybersecurity Attempts in the Context of User Behaviour*

User behaviour plays a crucial role in the cybersecurity risk profile of SMEs (Alsharida et al. 2023). Personality traits of SME clients, and employees significantly impact their cybersecurity behaviours, influencing decision-making processes related to security practices and thereby affecting the enterprise's overall security risk (Kalhoro et al. 2022). The level of preparation and investment in cybersecurity measures is directly affected by user behaviour, rendering vulnerable companies more susceptible to cyber threats in the dynamic online environment (Mitrofan, Cruceru, and Barbu 2020; Kim et al. 2019; Sahoo and Gupta 2019; Moallem 2024).

Implementing user behaviour data within SMEs offers a proactive stance against cyber threats. Recent studies (Mihailescu et al. 2023; Folino, Otranto Godano, and Pisani 2023; AlQadheeb, Bhattacharyya, and Perl 2022) demonstrate that user behaviour analytic technologies can effectively detect unusual behaviour patterns or anomaly detection, thereby flagging potential security incidents before they escalate into full-blown attacks. For instance, its application in detecting and managing cyber vulnerabilities gives enterprises a robust solution for enhancing their cyber defences, highlighting its pivotal role in cybersecurity risk management (Olaniyan, Rakshit, and Vajjhala 2023; Singh, Krishnaswamy, and Zhang 2022). Besides, user behaviour analytics also become critical in identifying insider threats (Sav and Magar 2020), leveraging user and entity activity mapping, profiling techniques, and risk score calculations to detect abnormal behaviours indicative of potential security breaches (Khaliq, Tariq, and Masood 2020).

Furthermore, Alshehri et al. (Alshehri et al. 2023) contribute to this discussion by proposing a framework that integrates machine learning with user behaviour analytics for cyberattack detection. Adding another dimension to this discussion, Siming et al. (Chen et al. 2018) explore the complexity of user behaviour analysis in cybersecurity by developing a visual exploration tool for identifying user behaviour patterns. This approach facilitates understanding why certain behaviours are considered anomalous, pointing towards the need for cybersecurity frameworks to incorporate visual analytics for better anomaly detection.

Moreover, the study by King et al. (King et al. 2018) addresses the characterisation of maliciousness within cybersecurity risk frameworks. By proposing a Human Factors risk framework, this study emphasises the need to understand the human elements contributing to cyber vulnerabilities, including the analysis of malicious intent behind user behaviours.

Research by Li et al. (Li et al. 2019) demonstrates that a clear understanding of organisational cybersecurity policies boosts employees' threat appraisal capabilities and coping appraisal abilities, positively affecting their compliance behaviour. This finding suggests that SMEs must prioritise disseminating information about cybersecurity policies across all organisational levels to mitigate user behaviour risks.

In the context of e-commerce, Abtahi et al. (Abtahi, Farhana, and Hasan 2023) demonstrate how SMEs confront cybersecurity challenges as they transition to online platforms. In addition, the role of user behaviour in cybersecurity for SMEs is highlighted by Elkhannoubi and Belaissaoui (Elkhannoubi and Belaissaoui 2016). Their work emphasises that even robust cybersecurity strategies can be undermined by inadequate user behaviour, advocating for developing user charters or guidelines that specifically address and regulate behaviour in the digital environment. Moore's research on SMEs' strategies suggests combating external cybersecurity threats by analysing the routine activities of users (Moore 2023). According to this study, SMEs can identify vulnerabilities and implement targeted strategies to protect their digital assets and information.

Fatema Rashid et al. (Rashid and Miri 2021) presented an approach to anomaly detection that minimises privacy breaches while maintaining the efficacy of behaviour analytics by using differentially private data. Integrating differential privacy into user behaviour data ensures data privacy and accuracy in anomaly detection, offering a cost-effective solution for SMEs concerned with security and privacy.

Zhao (Zhao 2023) focuses on detecting browser fingerprinting through user behaviour analysis. This study suggests areas where cybersecurity frameworks could be improved to protect against such threats, highlighting the importance of adapting to new cyber threats through a deeper understanding of user behaviour.

Further exploring the integration of machine learning with behavioral analytics, Shivappa and Shetty (Shivappa and D 2024) proposed an architecture for anomaly detection in network traffic flow by analyzing user behavior. Their approach involved pre-processing API access behavior data, performing correlation analysis to understand user patterns, and applying several machine learning algorithms - including Logistic Regression, K-Nearest Neighbors, Decision Tree, and Random Forest - for both binary (normal/abnormal) and multi-class classification of anomalies. A key finding of their work was the superior performance of the Random Forest algorithm, which achieved very high accuracy in identifying both general anomalies and specific attack types on their datasets. This study underscores the potential of specific machine learning pipelines in effectively modeling user behavior for robust cyber threat detection from network traffic data.

Recently, further advancing User and Entity Behaviour Analytics (UEBA) methodologies, Fuentes et al. (Fuentes et al. 2025) have introduced an explainable anomaly detection framework centered around Deep Autoencoders. A notable aspect of their research is the integration of Doc2Vec for processing textual features, such as command line arguments or process execution lists, in conjunction with numerical data to construct comprehensive behavioral profiles. Their framework was evaluated using real-world data from a financial institution along with synthetic anomalies derived from actual attack scenarios, showing effective detection capabilities. A key emphasis of their work was on the explainability of the detection process, utilizing per-feature reconstruction errors from the autoencoder to help pinpoint the specific behaviors contributing to an anomaly score. This study highlights the potential of deep learning techniques not only to accurately identify anomalies within a UEBA context but also to offer interpretable insights valuable for security analysts.

Despite numerous attempts to propose solutions leveraging user behaviour data to enhance the cybersecurity capabilities of SMEs, there remains a significant research gap related to this topic:

- Although user behaviour can bolster cybersecurity, current frameworks are not always tailored to SMEs (Yigit Ozkan and Spruit 2023), nor do they fully leverage these insights for smaller businesses (Moustafa and Bello 2021; van Haastrecht et al. 2021);
- There is a need for frameworks that emphasise both social and technical factors influencing cybersecurity toward human-centric cybersecurity practices (Perozzo, Zaghloul, and Ravarini 2022; Malatji, Von Solms, and Marnewick 2019);
- Existing studies focus on technical aspects, neglecting theoretical and cultural influences (Rahman et al. 2021);
- Utilising intelligent software with machine learning to combat cyber threats is underexplored (Rawindaran, Jayal, and Prakash 2022).

While the preceding discussion highlighted various attempts to utilize user behaviour analytics (UBA) in cybersecurity, Table 1 offers a comparative summary of selected representative studies. This comparison helps to illustrate the different facets explored in prior research.

Acknowledging these identified shortcomings and building upon the foundational contributions from the existing literature, this research directly seeks to bridge these critical gaps. Specifically, the current study proposes a novel, multi-layered cybersecurity framework meticulously designed for the unique operational context and resource constraints of SMEs. It aims to provide a practical and accessible solution by deeply integrating user behaviour analytics, innovatively leveraging existing business intelligence through the TRIVI framework, aligning with the NIST CSF for a standardized approach, and proposing a cost-effective cloud-based implementation model. This holistic approach directly targets the identified needs for SME-tailored, human-centric, and analytically robust cybersecurity measures that are currently underexplored or not cohesively addressed in existing solutions for smaller enterprises.

2.3. *Theoretical Background*

At its core, the process of analysing collected data to enhance cybersecurity within any given enterprise is called cybersecurity analytics (Janeja 2022; Anand, Chirputkar, and Ashok 2023). In other words, cybersecurity analytics involves collecting, analysing, and interpreting data to identify and mitigate security threats and risks in the digital environment of an organisation (Rajasekar, Premalatha, and Dhanaraj 2022; Borges Amaro et al. 2022). It encompasses the utilisation of various tools, techniques, and technologies to gain insights into potential vulnerabilities, malicious activities, and security breaches. While larger corporations typically possess the necessary resources to invest in comprehensive SIEM solutions (González-Granadillo, González-Zarzosa, and Diaz 2021), SMEs often face budgetary constraints and expertise limitations (Jahankhani, Meda, and Samadi 2022; Heidt, Gerlach, and Buxmann 2019).

Table 1.: Comparative analysis of selected works using user behaviour analytics

Study	**Objective**	**Approach**	**Contributions**
Mihailescu et al. (2023); Folino et al. (2023)	Anomaly detection via UBA	User behaviour analytic technologies for flagging potential security incidents	Demonstrate effectiveness in detecting unusual patterns/potential incidents.
Sav & Magar (2020); Khaliq et al. (2020)	Insider threat detection	User/entity activity mapping, profiling, risk scores	Show UBA's criticality in identifying insider threats via abnormal behaviour.
Alshehri et al. (2023)	Cyberattack detection	Framework integrating machine learning with UBA	Proposed machine learning with UBA approach for improved detection accuracy.
Siming et al. (2018)	Understanding anomalous behaviour	Visual exploration tool	Facilitate understanding why behaviour is anomalous via visualization.
King et al. (2018)	Characterizing maliciousness in risk frameworks	Human factors risk framework	Emphasize understanding human elements & malicious intent in risk assessment.
Elkhannoubi et al. (2016)	User behaviour impact on strategy effectiveness in SMEs	Advocated user charters/guidelines	Emphasized behaviour can undermine strategies; need for guidelines in SMEs.
Moore (2023)	SME strategies against external threats	Analysis of routine user activities	Suggest routine activity analysis can help SMEs identify vulnerabilities.
Rashid & Miri (2021)	Privacy-preserving anomaly detection	UBA using differentially private data	Offer cost-effective anomaly detection while enhancing data privacy.
Zhao (2023)	Detecting browser fingerprinting	Flow-centric analysis with UBA	Suggest UBA can detect specific modern threats like fingerprinting.
Shivappa and Shetty (2024)	Detecting network traffic anomalies	Utilizing pre-processing of API access behavior data	Proposed an ML-driven architecture for behavioral modeling to enhance cybersecurity threat detection.
Fuentes et al. (2025)	Threat detection	Employing Deep Autoencoders to model normal behavior	Presented an explainable UEBA framework that effectively combines Deep Autoencoders with Doc2Vec.

Commercial solutions such as Splunk[1], AlienVault[2], Solarwinds[3], LogRhythm SIEM[4], and QRadar[5] are among the renowned solutions that leverage advanced analytics to facilitate threat detection. However, the cost of these sophisticated tools often places them beyond the reach of SMEs.

In the architecture of a cybersecurity analytic solution, four primary modules form the backbone of its functionality: Anomaly Detection (Elsayed and Zulkernine 2020), Threat Intelligence (Samtani et al. 2020), Incident Response (Naseer et al. 2024), and User Behaviour Analytics (Salitin and Zolait 2018).

Anomaly Detection

This module identifies behaviours or activities that deviate from established patterns or norms within a system or network (Xi et al. 2018). The module relies on sophisticated algorithms and techniques to detect potential threats, such as unusual login attempts, abnormal data transfers, or uncharacteristic user behaviours.

Threat Intelligence

This module leverages external and internal data to recognise and predict evolving threat landscapes. It includes gathering, processing, and disseminating information about emerging threats and cyber-attack tactics (Sonwani et al. 2022). Its primary purpose is to provide information and insights about potential cyber threats, including their tactics, techniques, and procedures (TTPs) (Saeed et al. 2023b).

Incident Response

This module facilitates swift and efficient response procedures upon detecting a security event or incident (Kävrestad, Birath, and Clarke 2024). It is responsible for alert generation, incident categorisation, prioritisation, and orchestration of necessary response activities (Renners, Heine, and Rodosek 2017).

User Behaviour Analytics

It supplements the capabilities of the Anomaly Detection module (Landauer et al. 2022; Khan, Khan, and Arshad 2022). This relatively new component uses machine learning, deep learning, and statistical analyses to detect when a user or machine significantly deviates from normal behaviour, providing another layer of anomaly detection (Khaliq, Tariq, and Masood 2020; Rashid and Miri 2021).

2.4. *A Brief Review on the TRIVI Framework*

Developed by Thang Le Dinh et al., the TRIVI framework (Le Dinh et al. 2022) is not merely a theoretical construct but a practically oriented guideline designed to assist SMEs in constructing robust Customer Intelligence Systems (CIS). It emphasises the application of business analytics to extract valuable insights from extensive datasets, thereby fostering value creation in the era of big data.

The strength of TRIVI lies in guiding SMEs toward:

- **Identifying Valuable User Data:** TRIVI encourages identifying various types of user data that can provide insights into customer behaviour, preferences, and expectations. This identification process is crucial for SMEs to ensure they collect data that can lead to actionable intelligence;
- **Data Utilisation for Customer Intelligence:** The framework provides a

[1] https://www.splunk.com/

[2] https://cybersecurity.att.com/

[3] https://www.solarwinds.com/security-event-manager

[4] https://logrhythm.com/

[5] https://www.ibm.com/products/qradar-siem

structured approach for transforming user data into customer intelligence. This intelligence can inform several facets of business strategy, such as personalised marketing campaigns, product development, and customer service enhancements;

- **Prioritising Data Sources:** TRIVI helps SMEs prioritise data sources that are most relevant to their specific business needs. It ensures that SMEs focus their efforts on analysing data that will provide the most significant return on investment;
- **Sustainable Competitive Advantage:** SMEs can build a sustainable competitive advantage by leveraging user data to understand and predict customer behaviour. The insights gained from this data can be used to tailor experiences, foster loyalty, and ultimately drive growth.

While TRIVI focuses on deriving customer intelligence, many of its data sources and techniques can be adapted for cybersecurity purposes in our research. This adaptation can particularly help enhance specific customer intelligence into more general user intelligence.

Specifically, TRIVI considers various sources to collect user behaviour data:

- Web data, such as browsing habits, shopping preferences, and transactions from e-commerce sites;
- Social media data, including likes, shares, and comments reflecting user preferences;
- Mobile app usage logs, which record user interactions.

The key relevance is TRIVI's ability to aggregate heterogeneous user behaviour data from users' digital interactions with systems and applications. While TRIVI analyses this data for marketing insights, the study adapts it to the proposed framework for security analytics in a more general way, covering different business insights.

For instance, web browsing habits, historical purchases, and application interactions can reveal potential security threats and vulnerable user behaviours. Analysing patterns can uncover risks, compromised accounts, and data exfiltration channels.

In summary, TRIVI demonstrates how diverse user behaviour data from digital systems can be harvested and intelligently analysed. By redirecting this approach to analyse user behaviours for cybersecurity, we can build a practical framework tailored for SMEs.

3. User Behaviour Data

In this proposed framework, there are two sources of user behaviour data: (i) Data related to business and obtained from the TRIVI, such as web browsing habits, online shopping preferences, and transaction details, and (ii) Data collected (called user behaviour logs) from different data sources related to the behaviour of the users, such as applications, systems, and networks (Dumais et al. 2014).

User behaviour logs in an SME typically record various user activities within the company's systems, networks, or applications. These logs can be crucial in understanding how users interact with systems, identifying potential security threats, and improving user experience. Below are some examples of the types of information that might be recorded in user behaviour logs:

- *Login and Logout times:* This can help track user activity and can be used to identify any unusual behaviour, such as logging in at odd hours;

- *IP addresses:* Logging users' IP addresses can help identify the location from which systems are being accessed, which could be necessary for security purposes;
- *Access to sensitive data:* Logs can be used to track who accessed what data and when. It is essential for compliance and security purposes;
- *Changes made to data or systems:* Any changes made to the system or data should be logged, including what was changed, who made the change, and when the change was made;
- *Error logs:* Any user-generated errors should be logged, including details of the error and when it occurred;
- *Email and communication logs:* Details of sent and received emails, chat messages, or other forms of communication can be logged;
- *File transfers and downloads:* If the SME handles many file transfers or allows downloads, logging these can provide a record of what information is being moved around and by whom;
- *Web browsing history:* Depending on the nature of the SME, keeping logs of the clients' and employees' web browsing history while using company devices or networks is also necessary.

Table 2 summarises data types and sources related to user behaviour in the proposed framework.

Table 2.: User behaviour data sources and types

From TRIVI	**User Behaviour Data**	
Web Analytic Data	Application	Web access/error logs
		Email Logs
Web Browsing Habits		Mobile App Logs
		Installation/Update Logs
User Activity Logs		Error Logs
	System	Authentication Records
Online Shopping Preferences		System Events
		File Access Logs
Transaction Data		Privileged Access Logs
	Network	Traffic Logs
User-generated Content		Connection Logs
		IDS/IPS Alerts

4. Methodology

This study adopts socio-technical principles to address the complexity of cybersecurity in SMEs. The Socio-Technical Systems Cybersecurity Framework (STS-CF) proposed by Malatji et al. (Malatji, Von Solms, and Marnewick 2019) serves as the conceptual foundation. STS-CF posits that effective cybersecurity emerges from the dynamic interplay among technology, processes, and people, ensuring that human-centric factors (e.g., behaviors, organizational culture) receive as much attention as

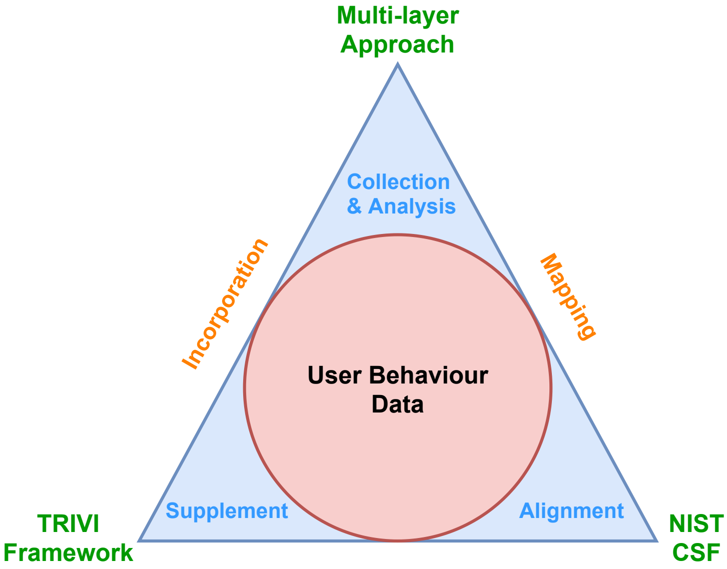

Figure 1.: Cybersecurity Behaviour Analysis Triad.

technical controls.

From an STS-CF perspective, cybersecurity risk must be viewed not solely as a technology challenge but also as a sociological one, requiring organizations to align staff awareness, workflow processes, and governance structures. While STS-CF provides a strong theoretical underpinning, its broad scope can be daunting for SMEs seeking a more focused roadmap. Hence, a specialized approach tailored to smaller, resource-constrained environments is necessary to realize the full potential of socio-technical cybersecurity measures. To this end, we propose the Cybersecurity Behavior Analysis Triad (CBAT), a conceptual framework designed to integrate key components of STS theory into a cohesive and actionable methodology for SME cybersecurity enhancement. The CBAT is presented in Figure 1. The CBAT triad encapsulates a multi-layer approach with the robust capabilities of the TRIVI Framework, all while aligning with the comprehensive security guidelines of the NIST Cybersecurity Framework. The crux of CBAT is user behaviour data, which acts as the nucleus, driving the responsiveness of the cybersecurity framework.

Multi-layer Approach

The Multi-layer Approach forms a vertex of the CBAT, emphasising the stratified nature of cybersecurity measures. It comprises various layers. Each layer is dedicated to a particular aspect of user behaviour data handling—from collection and storage to analysis and action. This approach acknowledges that data-driven insights are crucial for proactive defence mechanisms and ensures that cybersecurity strategies are comprehensive and adaptive.

TRIVI Framework

The TRIVI Framework is another vertex of the CBAT, representing the foundation of SMEs' customer intelligence systems. This framework is adept at collecting and aggregating vast amounts of user behaviour data to glean valuable business insights. The CBAT leverages the TRIVI Framework's existing infrastructure and analytical prowess, extending its capabilities from a business analytics tool into a sentinel for cybersecurity.

NIST Cybersecurity Framework

The NIST CSF, comprising the Identify, Protect, Detect, Respond, and Recover functions, is the third vertex of the CBAT. This internationally recognised framework offers a high-level strategic view of the organisation's approach to managing and mitigating cybersecurity risks. The proposed framework will align closely with the NIST CSF, ensuring the proposed cybersecurity measures adhere to industry standards and best practices.

User Behaviour Data

At the heart of the CBAT is User Behaviour Data — the crucial element that informs and drives the entire methodology. It encompasses the digital footprints left by users as they interact with SMEs' systems, networks, websites, and other entities. CBAT harnesses detailed insights into user behaviour patterns by focusing on this data, enabling it to detect and analyse anomalies indicative of potential cybersecurity threats.

Interrelationships within the CBAT

- **Incorporation:** This relationship denotes the seamless integration of the Multi-layer Approach with the TRIVI Framework. The incorporation process ensures that the proposed framework benefits from the strengths of both approaches.
- Mapping: The CBAT maps its Multi-layer Approach onto the NIST CSF, ensuring that each layer corresponds to one or more of its core functions. This meticulous mapping guarantees that our framework's comprehensive approach aligns with the NIST CSF's best practices.
- **Data Collection and Analysis:** This relation signifies the critical data collection and analysis processes within the Multi-layer Approach. It underscores the importance of gathering extensive user behaviour data and subjecting it to rigorous analysis to inform the security measures implemented across the framework's multiple layers.
- **Supplement:** The TRIVI Framework serves to supplement User Behaviour Data. A more comprehensive user behaviour profile is constructed by infusing the TRIVI Framework's existing data with the log datasets. This enriched data repository significantly enhances the predictive power of the proposed framework, allowing for a more sophisticated analysis of behaviour patterns, identification of aberrant activities, and the implementation of more accurate and timely security interventions.
- **Alignment:** The alignment between the NIST CSF and User Behaviour Data emphasises that the data-driven insights are leveraged following the NIST CSF guidelines. It ensures that the behaviour analytics are insightful and conform to established cybersecurity protocols.

5. Framework Development

The framework is conceptualized using a bottom-up approach (Figure 2), comprising four key layers: Data Layer, Analytics Layer, Reporting Layer, and Decision Layer. These layers are designed to be interactive and dynamic, where the output of one layer serves as the input for the subsequent layer. This structure ensures a continuous and logical flow of information, fostering an environment of constant learning and adaptation crucial for effective cybersecurity. Several modules within these layers build upon the existing data analytics features of the TRIVI framework to extract security-related insights, while additional modules are incorporated specifically to harness user behaviour logs and drive cyber threat prediction and mitigation. Within each layer reside distinct modules, each executing a specific function, some inspired by TRIVI and others newly introduced for SME cybersecurity needs.

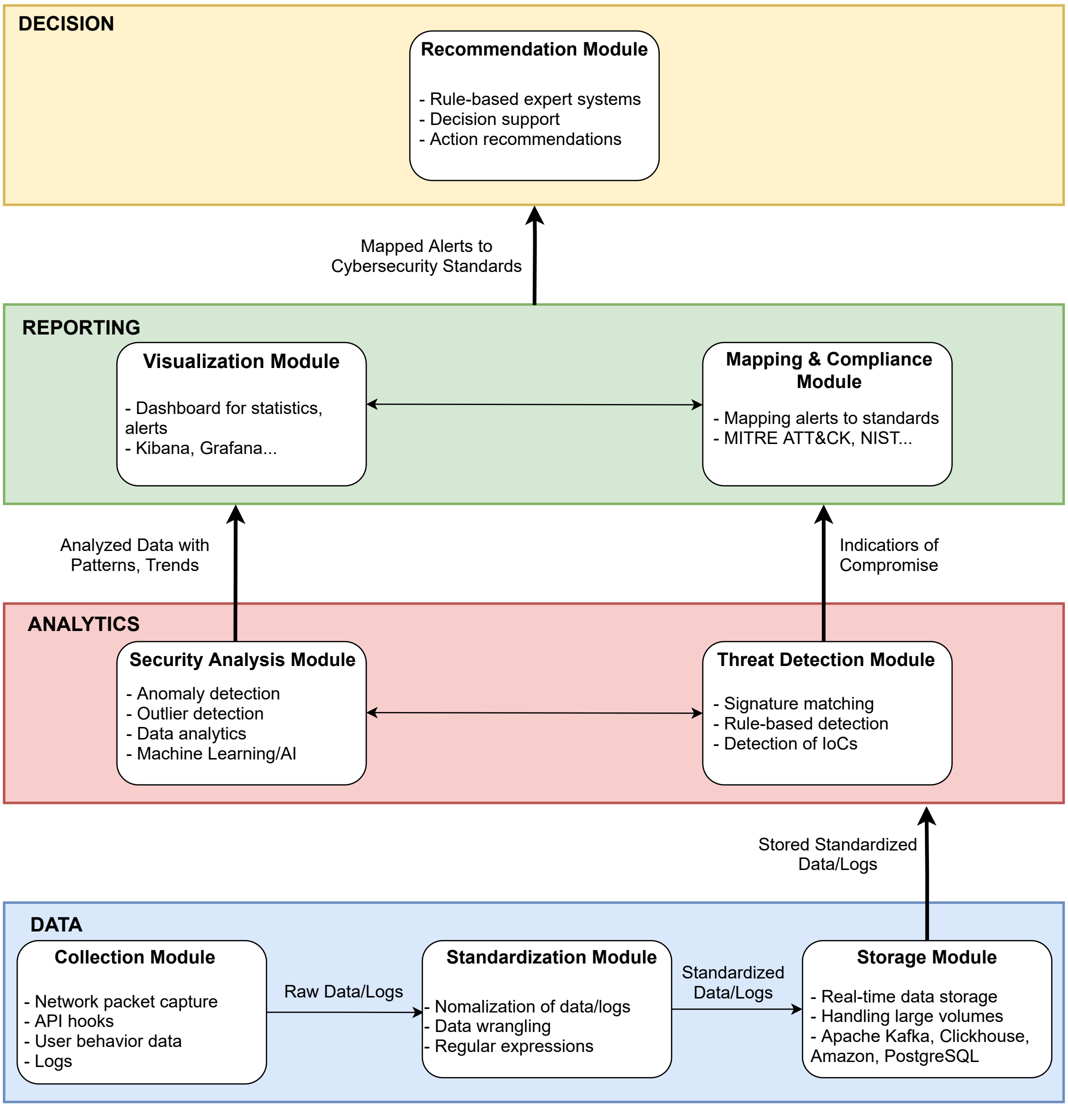

Figure 2.: A bottom-up approach for the framework development.

5.1. *Data Layer*

At the base, the Data Layer establishes the framework's foundation, responsible for handling all aspects of data acquisition and preparation. It comprises three interconnected modules: *Collection, Standardization,* and *Storage.*

Collection Module

As the foundational component of the Data Layer, the Collection Module is responsible for the comprehensive ingestion of raw data from a wide array of sources across the SME's digital environment. Its primary function, as illustrated in Figure 2, is to gather diverse data streams that capture user activities and system events, focusing particularly on user behaviour data and various types of log files.

The inputs to this module are intentionally broad to ensure holistic visibility, potentially including (but not limited to):

- **Network Packet Capture:** Intercepting network traffic to analyze communication patterns and data flows.
- **API Hooks:** Tapping into application programming interfaces to monitor interactions between software components or user actions within applications.
- **User Behavior Data:** Gathering information related to user interactions with systems, which might include authentication records, file access patterns, or application usage logs. This complements the business-centric user data sourced via the TRIVI framework (like web browsing habits or transaction details), providing a fuller picture of user actions.
- **Logs:** Collecting event logs from operating systems, servers, applications, databases, security appliances (like firewalls or Intrusion Detection Systems - IDS/IPS alerts), and mobile devices.

Systematically collecting these varied data types is important for enabling downstream monitoring and analysis, particularly to detect anomalies that might indicate insider threats, compromised user credentials, unusual account activity, or other security risks. It should be noted that data privacy concerns are a key challenge in implementing the framework, particularly the legal and ethical considerations surrounding user behaviour data collection under regulations like GDPR[6]. Given the sensitivity of user behaviour data, it is imperative that clear policies regarding data collection are established and communicated, and that proper user notice and consent mechanisms are implemented in adherence to privacy regulations. It is important to distinguish this module's function from the data sourcing inherent in the TRIVI model; while TRIVI provides valuable user intelligence from a business perspective, this Collection Module focuses on gathering the raw technical logs and event data essential for security monitoring.

The module must be engineered to robustly handle large volumes of data, often arriving at high velocity (real-time), stemming from potentially hundreds or thousands of diverse sources across the SME's infrastructure. This data is inherently heterogeneous, arriving in various formats (structured, semi-structured, and unstructured). Example implementation mechanisms could involve deploying lightweight agents (like Elastic Beats), configuring system logging protocols (e.g., Syslog), or integrating directly with cloud service APIs.

The output of this module is a stream or repository of Raw Data/Logs, which is then directed to the subsequent stage – the Standardization Module. There, this raw, multi-formatted data undergoes necessary transformation and normalization processes to prepare it for effective storage, analysis, and interpretation in the framework's subsequent layers.

Standardisation Module

Positioned immediately after the Collection Module, the Standardisation Module receives the continuous flow of heterogeneous raw data and logs gathered from diverse sources. Its function is to process this inconsistent input into a standardised, structured, and normalised format that is optimized for efficient storage and, crucially, effective analysis by the subsequent Analytics Layer.

Standardisation is a pivotal step because raw logs and event data often vary sig-

[6] https://gdpr-info.eu/

nificantly in format, structure, and content depending on their source system or application. This module tackles the challenge of reconciling these differences, removing inconsistencies related to aspects like timestamp formats, units of measurement, data encoding, or field naming conventions. By transforming the data into a uniform structure, it becomes significantly more suitable for reliable comparison, correlation, and algorithmic analysis. Furthermore, working with standardised data dramatically simplifies the processes within the Storage and Analytics layers, which is particularly advantageous when dealing with the large data volumes typical in security monitoring.

As indicated in Figure 2, the standardisation process within this module employs a combination of techniques (but not limited to):

- **Log Parsing** (Zhang et al. 2023): This involves applying parsers, often based on regular expressions (Hameed and Naumann 2020), to dissect unstructured or semi-structured log messages and extract key-value pairs (e.g., identifying and extracting fields like timestamp, source IP, destination IP, user ID, event type, status code, etc.).
- **Normalisation:** This focuses on bringing disparate data points into a common representation. Examples include converting all timestamps to a single format (e.g., UTC), mapping varied event severity labels (like "High", "Severe", "Critical") to a consistent taxonomy, or standardizing units (e.g., converting all data sizes to bytes).
- **Data Wrangling and Validation:** This includes tasks such as cleaning the data (e.g., handling missing fields, correcting obvious errors), validating data types (ensuring that an IP address field contains a valid IP), and potentially restructuring the data for analytical convenience.

By applying these techniques, the module handles the variety of incoming data formats and transforms them into a consistent, structured format (e.g., JSON objects adhering to a predefined schema) that is significantly easier to work with in the subsequent layers.

The final output from the Standardisation Module is a stream of Standardised Data/Logs. This clean, structured, and potentially enriched data is then passed directly to the Data Storage Module for efficient persistence and retrieval.

Storage Module

The Storage Module serves as the central repository within the Data Layer, responsible for the secure, reliable, and cost-effective persistence of the standardised logs and data processed and received from the Standardization Module. A key challenge for this module is handling potentially large amounts of continuously generated data, which requires capabilities for both real-time streaming data ingestion and efficient storage of historical logs at scale. Crucially, these stored data must be easily and efficiently accessible to the subsequent Analytics Layer, which is heavily dependent on this repository to identify emerging threats, perform complex security analyses, and understand long-term patterns.

To meet these diverse requirements (high-volume ingestion, real-time querying, historical analysis, scalability, cost-efficiency), a hybrid approach leveraging multiple storage technologies is often optimal, as suggested by the examples in Figure 2 and the implementation discussion in Section 7:

- **Streaming/Buffering:** Technologies like *Apache Kafka*[7] can serve as a durable,

[7] https://kafka.apache.org/

high-throughput buffer for incoming real-time data streams, decoupling ingestion from processing, and preventing data loss during peak loads before data land in the primary storage or analytics engine.

- **Primary Analytics Store:** A powerful search and analytics engine like *Elasticsearch*[8] is often used as the primary store. It excels at indexing semi-structured log data and providing near-real-time search, aggregation, and analytical capabilities needed by the Analytics Layer.
- **Cost-Effective Historical Storage:** For long-term retention of logs required for compliance or infrequent forensic analysis, cloud object storage such as *Amazon S3*[9] offers a highly scalable and cost-effective solution (often referred to as 'cold' storage). Data can be tiered off to object storage from the primary analytics store based on age or relevance.
- **Structured/Relational Querying:** In some cases, traditional Relational databases such as *PostgreSQL*[10] might be used alongside other systems, perhaps to store metadata, configuration information, or specific aggregated results where structured querying via SQL is advantageous.
- **Specialized Analytical Databases:** For very large-scale analytical tasks or specific performance needs, columnar databases like *ClickHouse* or data warehouses like *Amazon Redshift* could complement the primary storage, offering optimized performance for complex analytical queries.

As data accumulates, the Storage Module ensures that both storage and retrieval mechanisms remain efficient and performant. Ultimately, the Storage Module provides a well-managed, queryable interface to the stored standardised data/logs. This readily accessible data serves as the essential input fuel for both the Threat Detection Module and the Security Analysis Module within the Analytics Layer, enabling them to perform their respective security functions. The implementation of data processing techniques must adhere to strict regulations regarding customer and user information policies.

5.2. *Analytics Layer*

Positioned strategically above the Data Layer, the Analytics Layer serves as the core intelligence engine of the framework. It receives the Stored Standardised Data/Logs from the Storage Module as its primary input. This layer's fundamental purpose is to scrutinize this prepared data to unearth potential cybersecurity threats, risks, and anomalous activities. To achieve comprehensive coverage against both known and unknown threats, it comprises two distinct yet interconnected modules: the *Threat Detection Module* and the *Security Analysis Module*. These modules often operate in parallel, analyzing the same data streams but applying different techniques to achieve complementary security objectives.

Threat Detection Module

The Threat Detection Module acts as the framework's first line of defense against recognized malicious activity. Operating on the stored standardised data/logs, it employs established techniques primarily focused on identifying threats that match predefined patterns or violate explicit security rules. The key methods include:

[8] https://www.elastic.co/

[9] https://aws.amazon.com/s3/

[10] https://www.postgresql.org/

- **Signature Matching:** This technique involves comparing attributes within the log data (such as file hashes, IP addresses, domain names, known malicious strings) against extensive databases of Indicators of Compromise (IOCs). These IOCs represent signatures of known malware, attack infrastructure, or malicious tools derived from threat intelligence feeds and historical incident data. By scanning for these high-fidelity IOC signatures, this module can quickly and accurately flag instances of known threats with a high degree of confidence. Matches often trigger immediate alerts signifying potentially severe ongoing attacks.
- **Rule-Based Detection:** Complementing signature matching, this involves defining custom security rules based on organizational policies or known suspicious sequences of events. These rules typically follow logical conditions (e.g., "*IF login from new country occurs < 1 hour after login from office AND sensitive data access attempted THEN alert*"). Examples include rules detecting impossible travel scenarios (logins from geographically distant locations in a short time), the use of specific risky commands, multiple failed login attempts followed by success, or unauthorized port scanning activity. Rules can encode both individual event conditions and correlated behaviours across multiple data points to identify violations or complex, predefined attack steps.

The primary output of this module consists of high-priority alerts and identified Indicators of Compromise, which are passed upwards to the Reporting Layer, particularly feeding into the Mapping & Compliance Module for contextualization against frameworks like MITRE ATT&CK (Ahmed et al. 2022). While effective against known threats, this module is inherently limited in its ability to detect novel, zero-day, or sophisticated polymorphic attacks that lack known signatures or predefined rules.

Security Analysis Module

The Security Analysis Module acts as a vital counterpart to Threat Detection, focusing on uncovering novel threats, subtle anomalies, and deviations from normal behaviour that signature- or rule-based methods might miss. It also operates on the stored standardised data/logs received from the Storage Module but employs more sophisticated analytical techniques to find hidden patterns, trends, and outliers indicative of potential security concerns. Its core capability lies in establishing baselines of normal activity (for users, systems, network traffic) and then identifying significant deviations.

By leveraging advanced technologies such as Machine Learning (ML) (Thomas, P. Vijayaraghavan, and Emmanuel 2020) and Artificial Intelligence (AI) (Leenen and Meyer 2021), often incorporating principles of User Behaviour Analytics (UBA), this module can process vast datasets more effectively than manual analysis. It excels at uncovering complex, previously unseen patterns or subtle correlations that might signal sophisticated attacks or insider threats. Examples of its application include: clustering user activity to spot individuals whose behaviour significantly differs from their peer group (potential insider threat or compromised account), or using sequence mining to detect anomalous transitions in system states or user workflows (e.g., unusual command sequences indicating lateral movement). Deep learning models can further enhance capabilities in areas like automated threat categorization and alert prioritization based on learned risk factors.

Key techniques and approaches employed by this module include (but not limited to):

- **Anomaly/Outlier Detection:** Using statistical methods or unsupervised ML

algorithms (like clustering, e.g., k-Means) to identify data points, events, or user behaviours that significantly deviate from established norms or peer group behaviour. This is fundamental for detecting unusual activity without prior knowledge of the threat.
- **Behavioural Baselining:** Establishing dynamic profiles of normal behaviour for users, entities (servers, endpoints), and network traffic, and then detecting deviations from these learned baselines.
- **Predictive Modelling:** Employing supervised ML algorithms (classification like random forests or neural networks) trained on labeled historical data to categorize new events as benign or malicious, often capable of detecting complex attack patterns missed by simpler methods.
- **Pattern and Sequence Analysis:** Utilizing techniques like sequence mining to uncover suspicious or atypical sequences of actions or events that violate expected workflows, potentially indicating tactics like lateral movement or privilege escalation.
- **Advanced ML/DL:** Leveraging deep learning for tasks like complex feature extraction from raw logs or sophisticated threat classification based on subtle data characteristics.
- **Threat Intelligence Integration:** Incorporating third-party threat intelligence feeds not just for known IOCs (as in Threat Detection) but also to enrich ML models with information on emerging Tactics, Techniques, and Procedures (TTPs) and zero-day vulnerabilities, facilitating a continuous learning cycle.

The outputs of this module are diverse, including actionable threat analytics, alerts ranked by risk score, dashboards visualizing anomalies and trends, and watchlists highlighting suspicious users or entities requiring further investigation. This module provides a crucial anomaly detection capability, significantly augmenting the defenses provided by the Threat Detection module by surfacing hidden or novel threats. Once analysis is complete, these findings (Analyzed Data with Patterns, Trends) are passed to the Reporting Layer for visualization and further contextualization.

Security Analysis Module

The Security Analysis Module acts as a vital counterpart to Threat Detection, focusing on uncovering novel threats, subtle anomalies, and deviations from normal behaviour that signature- or rule-based methods might miss. This capability is central to the framework's aim of addressing potential false negatives that can arise from relying solely on detection of known threats. It also operates on the stored standardised data/logs received from the Storage Module but employs more sophisticated analytical techniques to find hidden patterns, trends, and outliers indicative of potential security concerns. Its core capability lies in establishing baselines of normal activity (for users, systems, network traffic) and then identifying significant deviations.

By leveraging advanced technologies such as Machine Learning (ML) (Thomas, P. Vijayaraghavan, and Emmanuel 2020) and Artificial Intelligence (AI) (Leenen and Meyer 2021), often incorporating principles of User Behaviour Analytics (UBA), this module is envisioned to process vast datasets more effectively than manual analysis, which can be particularly beneficial for SMEs with limited analytical resources. It aims to excel at uncovering complex, previously unseen patterns or subtle correlations that might signal sophisticated attacks or insider threats. While these advanced techniques are proposed to significantly enhance threat detection, the framework design acknowledges the potential for generating false positives. Consequently, design considerations for managing alert accuracy and volume are integral to this module's proposed operation. Examples of its application include: clustering user activity to spot individuals whose behaviour significantly differs from their peer group (potential insider threat or compromised account), or using sequence mining to detect anomalous transitions in system states or user workflows (e.g., unusual command sequences indicating lateral movement). Deep learning models could further enhance capabilities in areas like automated threat categorization and alert prioritization based on learned risk factors.

Key techniques and approaches proposed for this module include (but are not limited to):

- **Anomaly/Outlier Detection:** Using statistical methods or unsupervised ML algorithms (like clustering, e.g., k-Means) to identify data points, events, or user behaviours that significantly deviate from established norms or peer group behaviour. This is fundamental for detecting unusual activity without prior knowledge of the threat.
- **Behavioural Baselining:** Establishing dynamic profiles of normal behaviour for users, entities (servers, endpoints), and network traffic, and then detecting deviations from these learned baselines.
- **Predictive Modelling:** Employing supervised ML algorithms (classification like random forests or neural networks) trained on labeled historical data to categorize new events as benign or malicious, potentially capable of detecting complex attack patterns missed by simpler methods.
- **Pattern and Sequence Analysis:** Utilizing techniques like sequence mining to uncover suspicious or atypical sequences of actions or events that violate expected workflows, potentially indicating tactics like lateral movement or privilege escalation.
- **Advanced ML/DL:** Leveraging deep learning for tasks like complex feature extraction from raw logs or sophisticated threat classification based on subtle data characteristics.
- **Threat Intelligence Integration:** Incorporating third-party threat intelligence feeds not just for known IOCs (as in Threat Detection) but also to enrich ML models with information on emerging TTPs and zero-day vulnerabilities, proposed to facilitate a continuous learning cycle.

The outputs of this module are envisioned to be diverse, including actionable threat analytics, alerts that can be prioritized using a proposed risk scoring mechanism, dashboards for visualizing anomalies, and watchlists for suspicious entities. A key design goal for this module is to surface hidden or novel threats, thereby aiming to reduce false negatives inherent in simpler detection approaches. Simultaneously, the framework proposes several considerations for managing potential false positives that may arise from its advanced analytical techniques and for enhancing overall detection accuracy. For example, it is proposed that risk scoring (Jalalvand et al. 2024) could assist SMEs in focusing on critical alerts, and that detection algorithm sensitivity could be configurable, allowing organizations to balance detection thoroughness with their operational capacity and risk appetite. Moreover, a human-in-the-loop approach (Ruengsurat et al. 2025) is suggested, where SME personnel could validate key alerts, providing valuable feedback. Such feedback, alongside automated learning from threat intelligence, would be part of a proposed continuous refinement process. This iterative feedback loop, ideally incorporating validated insights from the Reporting and Decision Layers, is considered important for progressively improving the accuracy of the

Security Analysis Module. Enhanced accuracy, in turn, supports more reliable identification of true threats (further reducing false negatives that even advanced systems might initially miss) while also minimizing distracting false alarms. Once analysis and initial prioritization are complete, these findings (Analyzed Data with Patterns, Trends) are passed to the Reporting Layer for visualization and further contextualization.

5.3. *Reporting Layer*

Serving as the crucial interface between the technical analysis performed in the Analytics Layer and the actionable guidance provided by the Decision Layer, the Reporting Layer focuses on visualising and contextualising the diverse outputs received. This layer takes Indicators of Compromise (primarily from Threat Detection) and Analyzed Data with Patterns, Trends (primarily from Security Analysis) as its main inputs. Its objective is to translate these potentially complex findings into formats easily understood by human analysts, security managers, and other stakeholders. This layer comprises two essential modules: the *Visualization Module* and the *Mapping & Compliance Module.*

Visualisation Module

The Visualization Module is primarily responsible for transforming the analytical findings, especially the patterns and trends identified by the Security Analysis Module, into intuitive and accessible visual representations. The goal is to enable stakeholders to quickly grasp key threat events, monitor ongoing security trends, understand the overall risk posture, and identify areas requiring attention without needing to sift through raw data. To achieve this, it leverages data visualisation tools and techniques to build interactive dashboards, graphs, charts, and reports.

Key outputs often include:

- **Threat Summary Dashboards:** Aggregating detected threats and alerts, potentially categorized by severity, attack vector (e.g., phishing, malware, exploit), targeted assets, or geographical origin.
- **User Behaviour Dashboards:** Tracking user activity levels, login patterns, resource access, and risk scores, specifically designed to highlight outliers or anomalous behaviour profiles.
- **Network Analytics Dashboards:** Providing visibility into network traffic patterns, identifying unusual connections, visualizing data flows between internal and external entities, and highlighting potential reconnaissance or exfiltration activity.
- **Trend Analysis Displays:** Utilizing tools to visualize metrics over time, helping to spot gradual changes or emerging patterns in threat activity or system behaviour.

Real-time streaming dashboards allow for continuous monitoring of critical security metrics, while automated scheduled reports and alerts provide periodic summaries or immediate notifications of significant events to relevant personnel.

Mapping & Compliance Module

While the Visualization Module focuses on presenting what is happening, the Mapping & Compliance Module adds crucial context, explaining why it might be happening and what it means in a broader security context. It primarily processes the Indicators of Compromise and alerts generated by the Analytics Layer, enriching them by correlating them against external knowledge bases, known adversary behaviours, and regulatory standards. As shown in Figure 2, it focuses on mapping alerts to standards like MITRE ATT&CK and NIST CSF. Its key functions include:

- **Threat Intelligence Correlation:** Matching technical indicators (file hashes, IP addresses, domains, email subjects) extracted by the Analytics Layer against threat intelligence feeds. This links observed activity to known adversary groups, ongoing campaigns, specific malware families, and their documented Tactics, Techniques, and Procedures.
- **Adversary Tactic/Technique Identification:** Correlating observed attack patterns and behaviours (e.g., sequences of events identified by the Security Analysis module) with the MITRE ATT&CK framework. This helps understand the adversary's likely intent, sophistication, and potential next steps in the attack lifecycle.
- **Vulnerability Contextualization:** Tagging detected threats or compromised assets with related Common Vulnerabilities and Exposures (CVEs). This links the threat activity to specific software flaws that may have been exploited, highlighting necessary patching or remediation actions.
- **Compliance Reporting:** Generating reports that document the detected security events and the framework's monitoring activities, often mapping these findings to specific controls or requirements within compliance frameworks like the NIST Cybersecurity Framework, ISO 27001, or others relevant to the SME. This assists in demonstrating due diligence and security posture to auditors or regulators.

Together, these two modules process the outputs of the Analytics Layer, transforming technical findings into visualized trends and contextualized, standards-aligned alerts. The resulting output, as Mapped Alerts to Cybersecurity Standards, provides the necessary intelligence, priority, and context for the Decision Layer to determine appropriate responses.

5.4. *Decision Layer*

Positioned at the apex of the framework, the Decision Layer represents the culmination of the data processing pipeline. It receives the contextualized and prioritized intelligence, represented as Mapped Alerts to Cybersecurity Standards, from the Reporting Layer. This layer's role is to translate these insights into specific, actionable recommended courses of action designed to mitigate identified threats, recover from incidents, and proactively reinforce the SME's cyber defenses. It contains the central *Recommendation Module.*

Recommendation Module

The Recommendation Module, potentially leveraging capabilities inherited from the TRIVI framework, acts as the framework's "brain" for response guidance. It takes the mapped alerts and enriched findings from the Reporting Layer as input. Its core purpose is to suggest the most appropriate response measures for the diverse security events and risks uncovered by the preceding layers. This goes beyond simple alerting to provide concrete guidance tailored to the SME's specific situation.

To generate these recommendations, the module employs several approaches:

- **Rule-Based Expert Systems:** It utilizes predefined rules that encode organizational security policies, industry best practices, and accumulated operational

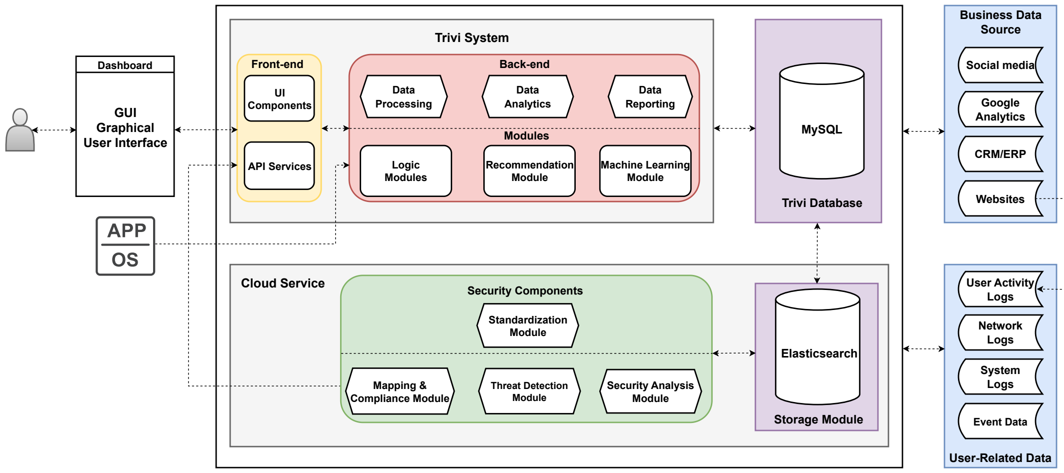

Figure 3.: Integration of the proposed framework into the TRIVI framework.

experience into structured logic trees (e.g., *”IF alert type is ’ransomware detected’ AND asset criticality is ’High’ THEN recommend ’isolate endpoint immediately’ AND ’initiate backup recovery plan’”*). These rules incorporate key risk factors like threat severity, potential impact, and the criticality of affected assets to determine appropriate actions. Examples include rules dictating steps like resetting user credentials following anomalous logins, isolating compromised endpoints exhibiting data exfiltration patterns, blocking malicious IP addresses at the firewall, or initiating specific incident response playbooks.

- **Decision Support Systems:** Beyond static rules, the module utilizes decision support capabilities to provide more contextual recommendations. This allows for tailoring suggestions by considering dynamic factors such as the SME’s overall security maturity level, its tolerance for business disruption during remediation, specific regulatory constraints, and its current preparedness level (e.g., availability of backups).
- **Machine Learning (Potentially):** Leveraging ML capabilities (potentially inherited from TRIVI or implemented using tools like those mentioned in Section 7.2) could further enhance recommendations by learning from past incidents and responses to identify optimal mitigation strategies based on complex patterns.

Figure 3 presents the idea of integrating the proposed framework into TRIVI by inheriting some TRIVI modules.

When integrating the proposed framework into the existing TRIVI framework, most modules could be deployed on the cloud through the Cloud Service component inherited from TRIVI. Furthermore, a new Storage Module must be designed to collect and store the diverse data types, especially the raw and normalised log files. The *MySQL* database in TRIVI, containing business data sources and user behaviour data, could be connected to this new Storage Module to create a consolidated data lake. Furthermore, several TRIVI modules, like the Machine Learning, Data Analytics, and Recommendation modules, could be efficiently leveraged for security analysis.

These recommendations can be presented to security analysts or executives for manual execution or, in some cases, trigger automated workflows through integration with IT Service Management platforms. Ultimately, the Recommendation Module serves as the decisive point, providing SMEs with the tailored guidance needed to effectively protect their digital assets, respond to incidents efficiently, and continuously

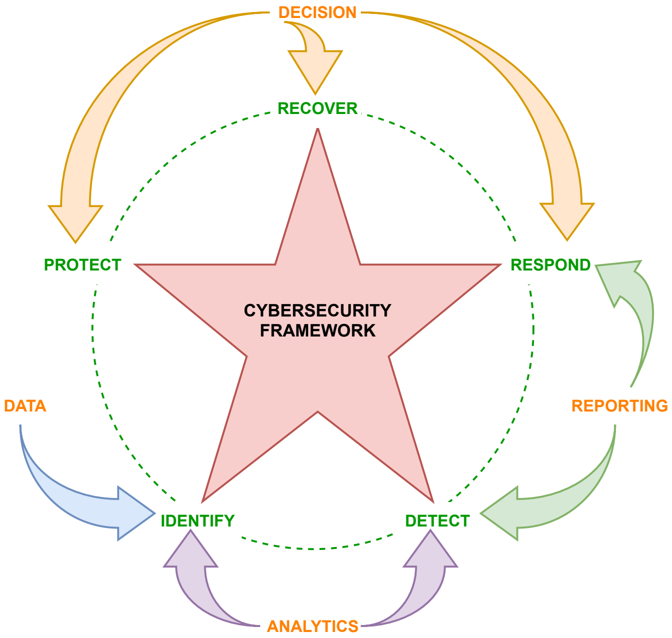

Figure 4.: Alignment with the NIST cybersecurity framework.

enhance their overall cybersecurity posture.

6. Alignment with The NIST CSF Framework

In order to demonstrate the consistency and completeness of the proposed multi-layered framework for cybersecurity, this framework can be effectively aligned with the five core functions of the NIST CSF framework: *Identify, Protect, Detect, Respond,* and *Recover*. Each layer of the framework corresponds to one or more of these functions based on the specific activities and objectives they encompass (Figure 4). The following in-depth analysis elucidates the alignment between the proposed framework and the NIST CSF.

Data Layer – Identify Mapping

- The ***Data Layer*** serves as the foundation for cybersecurity risk management. It involves identifying the resources (such as user behaviour data and log files) that need to be protected and analysed. Activities in this layer correspond to the ***Identify*** function by collecting and standardising raw data, which is crucial for understanding the resources and the related cybersecurity risks.

Analytics Layer – Detect Mapping

- The ***Identify*** aspect comes from analysing the standardised data to understand normal behaviour and potential vulnerabilities within the system. This insight is essential for risk identification and management.
- The ***Detect*** function is served primarily through the Threat Detection Module, which applies various techniques to identify potential threats, and the Security Analysis Module, which uses advanced technologies (eg. Machine Learning, Deep Learning, Natural Language Processing, or Graph Analytics) to analyse patterns

and detect anomalies.

Reporting Layer – Detect & Respond Mapping

- The ***Detect*** function is enhanced by visualising the analytics outcomes. The Visualization Module makes data understandable and accessible through interactive dashboards. It directly supports identifying cybersecurity events that may otherwise go unnoticed.
- The ***Respond*** function is initiated here as the Mapping & Compliance Module adds context to the detected threats and provides information necessary for developing the initial response to cybersecurity events. It includes mapping the threats to known adversarial tactics and understanding the implications in terms of compliance.

Decision Layer – Respond, Recover, Protect Mapping

- The ***Protect*** function, represented by the Recommendation Module, suggests preventive measures to safeguard against detected threats.
- The ***Respond*** function is further incorporated as this layer outlines the actions to respond to detected cybersecurity events. Recommendations are given for immediate response activities to contain and mitigate the impacts of incidents.
- Lastly, the ***Recover*** function is evident as the framework guides recovery strategies to restore impaired services and capabilities after an incident.

To summarise, each layer in the framework not only contributes to one particular NIST function but also overlaps with others, reflecting the integrated and interconnected nature of cybersecurity activities. The layers are steps in a continuous process that starts with identifying what needs to be protected, detecting when something has gone wrong, responding to that incident, and then recovering from it. This mapping shows the depth and breadth of activities within each layer and how they correspond to the NIST Cybersecurity Framework.

7. Technical Implementation and Cloud Deployment

In order to highlight the applicability and appropriateness of the framework, this section discusses the technical implementation with a focus on cloud deployment for SMEs. Integrating technical solutions and cloud services has become essential for SMEs in today's cybersecurity landscape. Cloud services offer scalability, flexibility, and built-in security features, making them attractive for SMEs (Lacity and Reynolds 2014). Open-source solutions, such as the Elastic Stack[11], present an ideal fit for SMEs with its modular architecture combining scalable log management, search, and analytics capabilities. They provide additional advantages with their transparency, flexibility, and community-driven improvements. These platforms enable SMEs to tailor their cybersecurity measures to their specific needs while benefiting from regular updates and enhancements. This section will discuss the practical implementation aspect of these solutions and their deployment in a cloud environment within the context of our proposed framework. *It should be noted that the technical implementation presented herein serves* ***merely as a sample****.* The provision of a prototype or a practical application is out of the scope of this research. Furthermore, SMEs can adopt any cloud

[11] https://www.elastic.co/

service instead of Elastic Stack.

7.1. *Cloud Services and Elastic Stack*

The open-source Elastic Stack (ELK Stack) presents a technology suite for cloud-based log analytics (Poenaru and Ciobanu-Zabet 2020). It combines scalable search and analytics capabilities via four main components:

- **Elasticsearch** is a search and analytics engine providing real-time and data analysis. It is designed to work with large volumes of data and return query results in near real-time;
- **Logstash** is a flexible data ingestion pipeline for collecting, parsing, transforming, and routing logs from myriad sources into *Elasticsearch. Logstash* offers numerous input, output, filter, and codec plugins for diverse integrations;
- **Kibana** is a visualisation layer that provides dashboards and a Graphical User Interface (GUI) for exploring data indexed in *Elasticsearch.* It enables real-time monitoring and tailored visuals;
- **Beats** is a lightweight data shipper that can be installed on hundreds or thousands of machines to forward logs and metrics into the *Elastic Stack.* For example, Filebeat forwards log files, while *Metricbeat* ships system and service metrics.

7.2. *Cloud-based Implementation of Modules*

This subsection delineates the realisation of the framework's modules by harnessing the expansive capabilities of the Elastic Stack hosted in a cloud environment tailored for SMEs. Figure 5 presents the implementation flow for this cloud-based approach.

For the **Collection Module**, the lightweight data shippers in ***Elastic's Beats*** family are utilised, such as ***Filebeat*** for forwarding logs from endpoints and ***Metricbeat*** for collecting system and service metrics. ***Packetbeat*** is used to capture network traffic, and ***Heartbeat*** is employed to monitor service uptime. These provide comprehensive coverage of machine, network, and application data flows. ***Beats*** are the primary data collectors, forwarding data to ***Logstash***. ***Logstash***'s input plugins can aggregate disparate data streams.

The **Standardization Module** leverages ***Logstash's*** versatile data processing pipeline to parse, normalise, and transform the raw data into unified formats consumable by downstream modules. Techniques like ***Grok patterns***, ***date filtering***, and ***geoIP filters*** are applied to normalise timestamps and geographical locations and ensure uniformity. Custom Logstash configurations encode validation logic and business rules.

The **Storage Module** leverages ***Elasticsearch*** as a distributed, scalable data store that provides features such as indexing, document APIs, SQL support, and aggregations to power data management. It can be integrated with *S3 repositories* for cloud storage, while the SQL plugin enables relational operations.

In practice, alternative database technologies such as *Apache Kafka, ClickHouse, Amazon Redshift,* and *PostgreSQL* could potentially be utilised for the framework's data storage needs. These database systems offer advantages for handling large volumes of heterogeneous data. They could be integrated with the rest of the *Elastic Stack* components to realise other modules like analytics and visualisation. For instance, a high-throughput message queue like *Kafka* could collate real-time data streams

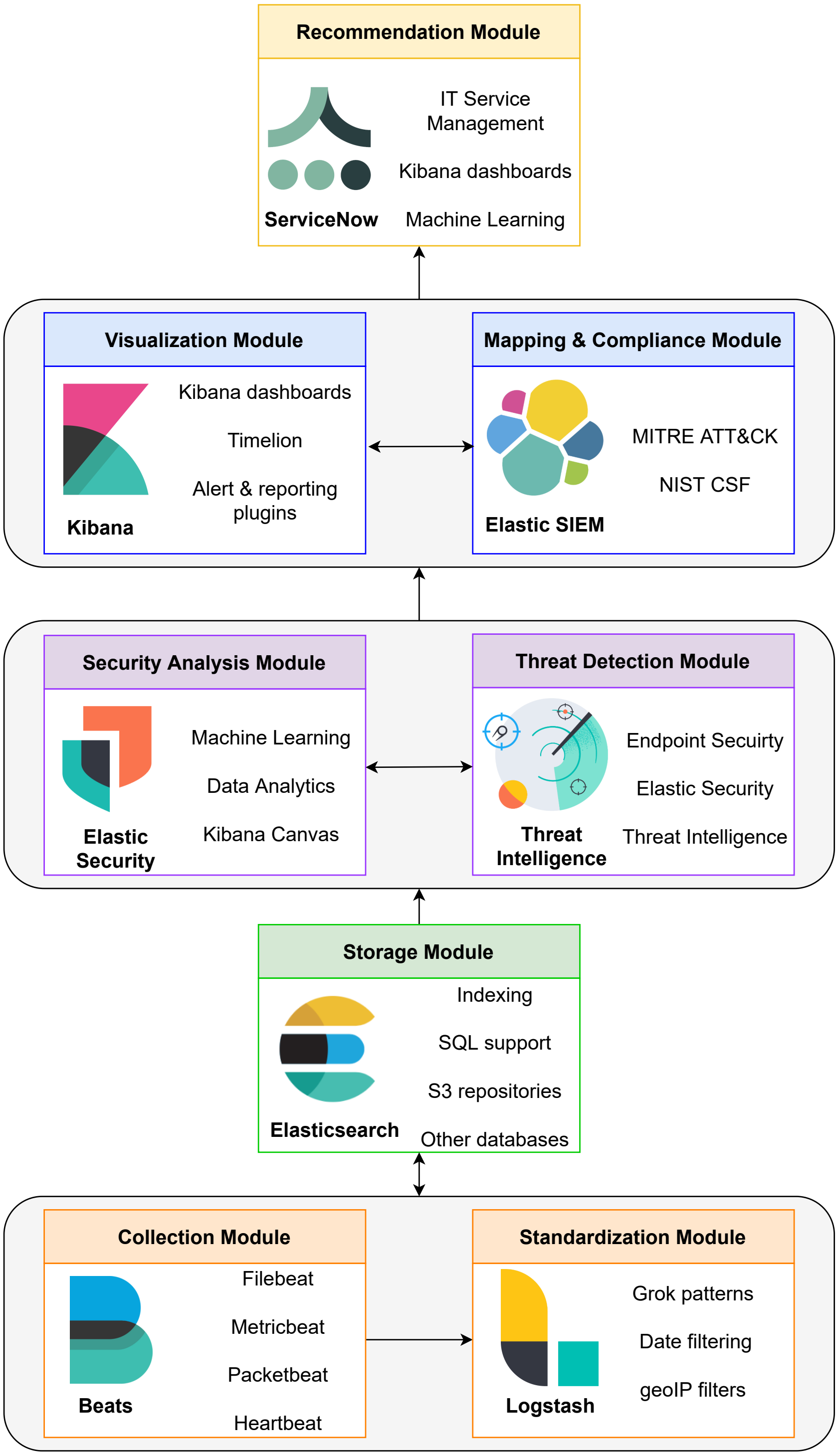

Figure 5.: Cloud-based implementation flow.

before loading them into *Elasticsearch* for search and analytics. Similarly, a robust analytic database like *Redshift* could complement *Elasticsearch* by providing SQL capabilities for structured queries. A multi-model solution like *ClickHouse* combines the strengths of row, column, and time-series data storage, amenable to security analytics. By thoughtfully integrating complementary databases with the Elastic Stack, the storage layer can be optimised for diverse data types and use cases while retaining interoperability across the modular framework. The choice of databases would depend on the specific data profiles, infrastructure constraints, and performance requirements.

The **Threat Detection Module** benefits from ***Elastic's SIEM*** applications, offering curated detections aligned with established threat frameworks. ***Endpoint Security*** provides prebuilt anomaly detection rules, and custom detection rules are encoded with *Logstash* filters. ***Elastic Security*** allows for integration with various external threat intelligence providers. These integrations can automatically ingest, normalise, and correlate threat intelligence data with event data in real-time. This feature enables analysts to view detailed information about threats, such as IOCs, directly within the security application, enhancing their ability to rapidly identify, investigate, and respond to threats.

For the **Security Analysis Module**, Elasticsearch's cutting-edge analytics tooling, including machine learning and data frame analytics, can be employed for sophisticated modelling. The ***Kibana Canvas*** workbench is also used to create machine learning models, and the outputs from these models are visualised in *Kibana.*

The **Visualization Module** is enabled by ***Kibana's*** dashboards, graphs, and User Interface (UI). ***Timelion*** visualises time-series data. ***Alerting and reporting plugins*** are utilised to deliver notifications.

For the **Mapping & Compliance Module**, ***Elastic SIEM*** includes event correlation capabilities that link different events and alerts based on common indicators, such as IP addresses or user names. It helps to provide context around security incidents and can assist in mapping alerts to cybersecurity standards like MITRE ATT&CK or NIST CSF. Custom ***Logstash filters*** are developed to implement standards mapping.

Finally, while the **Recommendation Module** primarily derives from the preexisting TRIVI Framework, it is noteworthy to mention that certain aspects of this module can be enhanced and efficiently operationalised through the strategic deployment of cloud services. This module combines predictive analytics and decision systems to offer strategic guidance. Machine Learning algorithms identify mitigation measures. It can integrate with IT Service Management (ITSM) and SIEM tools like ***ServiceNow***, which use Elastic apps to trigger responses. ***Kibana*** dashboards surface alerts for recommended actions.

This application of the multifaceted Elastic Stack demonstrates a comprehensive realisation of the framework in the cloud to deliver integrated cybersecurity capabilities purpose-built for resource-constrained SME environments.

8. Discussions

8.1. *Advantages of An SME-Specific Cybersecurity Framework over Traditional SIEM Solutions*

First and foremost, it is imperative to acknowledge that SIEM solutions currently available in the market, such as *Splunk, IBM QRadar,* and *LogRhythm*, operate with a high degree of efficacy and offer many auxiliary features. However, it is critical to note that these solutions predominantly cater to larger enterprises characterised by substantial scale and necessitate considerable investment in terms of both resources and operational costs. In contrast, the proposed framework, potentially constructed as an open-source solution utilising the *Elastic Stack*, primarily addresses the unique needs of SMEs. This focus is manifested through emphasising cost-efficiency and simplifying system deployment and management, making cybersecurity more accessible and manageable for SMEs. This discussion distils the proposed framework's unique advantages, which are not commonly found in or are distinctively different from popular SIEM solutions. Table 3 presents some essential contributions of the proposed framework to the SME-Specific cybersecurity solutions.

Table 3.: Essential advantages of the proposed framework

Feature	**Proposed Framework**	**Traditional SIEM Solutions**
Integration with Business Intelligence	Integrates with the TRIVI framework for deep insights into user behaviour, web habits, and shopping preferences	Limited integration; focuses mainly on security logs and network data
Tailored for SMEs	Designed specifically for SMEs, considering cost, resource limitations, and scalability	Often tailored for larger enterprises with significant resources
Tailored for User Behaviour Analytics	Specifically designed to leverage user behaviour data for nuanced threat detection within SME contexts	Features present but not as focused or detailed for specific contexts
Cloud-Based Scalability and Cost Efficiency	Open-source cloud-service design for SME cost-efficiency and scalability	Cloud options are available but may not be optimised for SME efficiency
Ease of use	The framework is designed for easy deployment and use	Usually requires an IT team and extensive expertise

8.2. *Strategy for Implementation and Evaluation*

Adopting a resource-efficient strategy that does not require extensive expertise is crucial to ensure the successful implementation and evaluation of the proposed framework in SMEs. The following guideline based on the Deming Cycle (Plan–Do–Check–Act) (Jagusiak-Kocik 2017) – a model widely recognized for its emphasis on continuous improvement and iterative refinement – is designed to facilitate SMEs in independently conducting the implementation and future evaluation of the cybersecurity framework. However, because SMEs typically face tighter budget constraints and less specialized staff, we modify certain elements of the PDCA approach to better align with our research objectives and practical realities.

Implementation Strategy

- **Step 1:** Framework Customization
  - *Tailor to Needs*: Start by identifying critical digital assets and the needs of SMEs
  - *Pilot Testing*: Run a small-scale pilot test to identify potential issues and make necessary adjustments
  - *Resource Allocation*: Allocate available resources efficiently, focusing on high-impact areas identified in the risk assessment
- **Step 2:** Implementation
  - *Phased Approach*: Implement the framework in phases, starting with core

components such as the collection module and threat detection systems, and make adjustments as needed
    - *Training and Awareness*: Conduct training sessions for employees to raise awareness about cybersecurity best practices and how to use the new system
    - *Assign Roles*: Define roles and responsibilities related to the operation
    - *Technical Setup*: Deploy the necessary tools and technologies, ensuring they are configured correctly and integrated with existing systems
- **Step 3:** Operationalisation
    - *Monitoring*: Establish procedures for the continuous monitoring of cybersecurity threats and system performance
    - *Response Protocols*: Develop and document incident response protocols to ensure swift action in case of a security breach
    - *Regular Updates*: Schedule regular updates and maintenance checks for cybersecurity tools and systems to protect against new threats

Evaluation Strategy

- **Step 1:** Define Metrics
    - *Effectiveness Metrics*: Define clear metrics for evaluating the framework's effectiveness, such as mean time to detect (MTTD), mean time to respond (MTTR), anomaly detection rate, or accuracy
    - *User Feedback*: Include metrics for user satisfaction and system usability to ensure the framework supports, rather than hinders business operations
- **Step 2:** Survey
    - Distribute regular *surveys* to collect feedback from employees on the system's usability and any issues they encounter
- **Step 3:** Analysis and Review
    - *Regular Reviews*: Schedule regular review sessions to analyse feedback information and assess the framework's performance against defined metrics
    - *Adjustments*: Use the insights gained from the analysis to make necessary adjustments to the framework or its implementation
- **Step 4:** Document Everything
    - *Maintain Records*: Keep detailed records of the implementation process, data collected, feedback, and changes made
- **Step 5:** Continuous Improvement
    - *Iterative Process*: Treat the evaluation process as iterative, continually seeking ways to improve the cybersecurity posture
    - *Share Findings*: Regularly share the evaluation outcomes with stakeholders to demonstrate progress and value

8.3. *Challenges in Implementing the Proposed Framework in SMEs*

Despite targeting technical simplification to accommodate SMEs with limited human and financial resources, SMEs still face challenges in implementing the proposed framework. These challenges are presented in Table 4 below.

Table 4.: Challenges in implementing the proposed framework in SMEs

Challenge	Description	Mitigation Strategies
Complexity in Implementation	Despite efforts to simplify the technical aspects for SMEs with limited resources, initial technical support is crucial for system deployment and user training (Carías et al. 2020)	Offer initial and ongoing technical support, develop step-by-step guides for system deployment, and provide comprehensive training programs to empower SMEs with the knowledge and skills required for effective utilisation. Maximise the automation
Data Privacy Concerns	Collecting user behaviour data raises legal and ethical considerations, necessitating strict adherence to data protection laws (Benjamin et al. 2024)	Establish clear data collection policies, implement robust protection measures, and ensure legal compliance
False Positives Management	Advanced analytics may generate false positives, leading to unnecessary alerts and resource consumption (Mohan et al. 2024)	Continuously refine intelligence models and establish efficient alert management processes
Integration with Existing Systems	Integrating the framework with existing IT infrastructure without disrupting operations can be challenging (Handri, Indra Sensuse, and Tarigan 2024)	Additional resource expenditure for a seamless transition
Continuous Update Requirement	The rapid evolution of cybersecurity threats requires the framework to be regularly updated, which can be burdensome for SMEs (Saeed et al. 2023a)	Automate update processes and provide clear guidelines for managing updates
Cultural Shifts	Adopting a proactive, data-driven approach to cybersecurity requires changing the mindset and operations (Benjamin et al. 2024)	Promote awareness and understanding of proactive cybersecurity measures among staff and management

9. Conclusions

This research proposes a novel, data-driven cybersecurity framework tailored specifically for SMEs to enhance their security posture by leveraging user behaviour analytics. The framework is meticulously aligned with the NIST CSF, ensuring its adherence to industry best practices and standards.

The proposed framework adopts a multi-layered approach comprising four interconnected layers: Data, Analytics, Reporting, and Decision. Each layer contains multiple modules that collectively map to the five core functions of the NIST CSF: Identify, Protect, Detect, Respond, and Recover. This alignment ensures a comprehensive and structured approach to cybersecurity that addresses the unique challenges SMEs face.

A key strength of the framework lies in its integration with the TRIVI framework, an established model for customer intelligence systems in SMEs. By leveraging the data collection and analytics capabilities of TRIVI, the proposed framework gains access to a rich repository of user behaviour data, including web browsing habits, online shopping preferences, and transaction details. This data, combined with the user behaviour logs from systems, networks, and applications collected by the framework itself, provides a comprehensive view of user activities, enabling the detection of potential security threats and anomalies.

The framework employs advanced data analytics techniques, such as machine learning, artificial intelligence, and statistical analysis, to extract actionable insights from the collected user behaviour data. These insights are visualised through interactive dashboards and reports, facilitating straightforward interpretation and decision-making by SMEs. The Recommendation Module, inherited from the TRIVI framework, provides SMEs with clear, actionable guidance on mitigating identified threats and reinforcing their cyber defences aligned with industry standards like NIST and MITRE ATT&CK.

In order to ensure the framework's accessibility and cost-effectiveness for SMEs, a cloud-based implementation using the Elastic Stack is proposed. This open-source solution offers scalability, flexibility, and built-in security features, making it an ideal choice for SMEs with limited resources and expertise.

The proposed framework offers several advantages over traditional SIEM solutions, including its tailored design for SMEs, integration with business intelligence through TRIVI, and focus on user behaviour analytics. However, challenges such as implementation complexity, data privacy concerns, and the need for continuous updates must be addressed through strategic planning and resource allocation. These can be addressed through phased implementation, strong data governance, and change management. The framework methodology establishes a blueprint for SMEs to unlock value from existing user behaviour data in a viable and scalable manner.

In future work, a prototype of the proposed cybersecurity framework utilising cloud services, as initially suggested, will be deployed. Experimental trials will be conducted across diverse SMEs in various sectors to evaluate the framework's practical effectiveness and adaptability. Furthermore, enhancing the framework's capabilities in malware detection and ensuring seamless integration with prevalent legacy systems within SMEs will be prioritised, representing significant research opportunities. Exploring advanced deep learning techniques will also be considered to provide a more comprehensive defence mechanism. Considering the influence of cultural differences on user behaviour and the framework's effectiveness across diverse regions. As cyber threats evolve, the necessity and relevance of cybersecurity frameworks, particularly those leveraging user behaviour analytics, will become increasingly critical for SMEs operating with limited resources. This continuous development aims to fortify SMEs' resilience against cyber threats, supporting their sustainable growth in the digital economy.

Disclosure statement

The authors report there are no competing interests to declare.

Acknowledgement

This research has received no external funding.

References

Abtahi, Ahanaf Tahmid, Nazia Farhana, and Md Mehedi Hasan. 2023. "A Study on the Impact of E-Commerce Adoption for Enhancing Supply Chain Efficiency in Bangladesh SMEs." *Business and Economics in Developing Countries* 1 (1): 29–33. https://doi.org/10.26480/bedc.01.2023.29.33.

Acton, Thomas, Pratim Milton Datta, and Martin Hughes. 2023. "Phantom or Menace: User Behaviors in Cybersecurity." In *2022 Cyber Research Conference-Ireland (Cyber-RCI)*, 1–4. IEEE.

Ahmed, Mohamed, Sakshyam Panda, Christos Xenakis, and Emmanouil Panaousis. 2022. "MITRE ATT&CK-driven cyber risk assessment." In *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 1–10.

AlQadheeb, Arwa, Siddhartha Bhattacharyya, and Samuel Perl. 2022. "Enhancing cybersecurity by generating user-specific security policy through the formal modeling of user behavior." *Array* 14: 100146. https://doi.org/10.1016/j.array.2022.100146.

Alsharida, Rawan A., Bander Ali Saleh Al-rimy, Mostafa Al-Emran, and Anazida Zainal. 2023. "A systematic review of multi perspectives on human cybersecurity behavior." *Technology in Society* 73: 102258. https://doi.org/10.1016/j.techsoc.2023.102258.

Alshehri, Abdullah, Nayeem Khan, Ali Alowayr, and Mohammed Yahya Alghamdi. 2023. "Cyberattack Detection Framework Using Machine Learning and User Behavior Analytics." *Computer Systems Science & Engineering* 44 (2). https://doi.org/10.32604/csse.2023.026526.

Anand, Abhishek, Abhijit Chirputkar, and P Ashok. 2023. "Mitigating Cyber-Security Risks using Cyber-Analytics." In *2023 7th International Conference on Trends in Electronics and Informatics (ICOEI)*, 630–635. IEEE.

Benjamin, Lucky Bamidele, Ayodeji Enoch Adegbola, Prisca Amajuoyi, Mayokun Daniel Adegbola, and Kudirat Bukola Adeusi. 2024. "Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies." *Global Journal of Engineering and Technology Advances* 19 (2): 134–153. https://doi.org/10.30574/gjeta.2024.19.2.0084.

Borges Amaro, Lucas José, Bruce William Percilio Azevedo, Fabio Lucio Lopes de Mendonca, William Ferreira Giozza, Robson de Oliveira Albuquerque, and Luis Javier García Villalba. 2022. "Methodological framework to collect, process, analyze and visualize cyber threat intelligence data." *Applied Sciences* 12 (3): 1205. https://doi.org/10.3390/app12031205.

Carías, Juan Francisco, Marcos RS Borges, Leire Labaka, Saioa Arrizabalaga, and Josune Hernantes. 2020. "Systematic approach to cyber resilience operationalization in SMEs." *IEEE access* 8: 174200–174221. https://doi.org/10.1109/ACCESS.2020.3026063.

Chen, Siming, Shuai Chen, Natalia Andrienko, Gennady Andrienko, Phong H. Nguyen, Cagatay Turkay, Olivier Thonnard, and Xiaoru Yuan. 2018. "User Behavior Map: Visual Exploration for Cyber Security Session Data." In *2018 IEEE Symposium on Visualization for Cyber Security (VizSec)*, October. IEEE.

Chidukwani, Alladean, Sebastian Zander, and Polychronis Koutsakis. 2022. "A survey on the cyber security of small-to-medium businesses: Challenges, research focus and recommendations." *IEEE Access* 10: 85701–85719. https://doi.org/10.1109/ACCESS.2022.3197899.

Dumais, Susan, Robin Jeffries, Daniel M. Russell, Diane Tang, and Jaime Teevan. 2014. *Understanding User Behavior Through Log Data and Analysis*, 349–372. Springer New York.

El Haddad, Ghada, Amin Shahab, and Esma Aïmeur. 2018. "Exploring User Behavior and Cybersecurity Knowledge-An experimental study in Online Shopping." In *2018 16th Annual Conference on Privacy, Security and Trust (PST)*, 1–10. IEEE.

Elkhannoubi, HB, and Mustapha Belaissaoui. 2016. "User's Behavior Influence on Cyber security Strategy Effectiveness." *International Journal of Ad-vanced Engineering Research and Sci-ence (IJAERS)* 3 (10): 188–196. https://doi.org/10.22161/ijaers/3.10.30.

Elsayed, Marwa A, and Mohammad Zulkernine. 2020. "PredictDeep: security analytics as a service for anomaly detection and prediction." *IEEE Access* 8: 45184–45197.

https://doi.org/10.1109/ACCESS.2020.2977325.

Fernandez De Arroyabe, Ignacio, and Juan Carlos Fernandez de Arroyabe. 2023. "The severity and effects of Cyber-breaches in SMEs: a machine learning approach." *Enterprise Information Systems* 17 (3): 1942997. https://doi.org/10.1080/17517575.2021.1942997.

Folino, Gianluigi, Carla Otranto Godano, and Francesco Sergio Pisani. 2023. "An ensemble-based framework for user behaviour anomaly detection and classification for cybersecurity." *The Journal of Supercomputing* 79 (11): 11660–11683. https://doi.org/10.1007/s11227-023-05049-x.

Fuentes, Javier, Ignacio Ortega-Fernandez, Nerea M. Villanueva, and Marta Sestelo. 2025. "Cybersecurity threat detection based on a UEBA framework using Deep Autoencoders." *arXiv preprint arXiv:2505.11542* https://doi.org/10.48550/arXiv.2505.11542.

González-Granadillo, Gustavo, Susana González-Zarzosa, and Rodrigo Diaz. 2021. "Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures." *Sensors* 21 (14): 4759. https://doi.org/10.3390/s21144759.

Hameed, Mazhar, and Felix Naumann. 2020. "Data Preparation: A Survey of Commercial Tools." *ACM SIGMOD Record* 49 (3): 18–29. https://doi.org/10.1145/3444831.3444835.

Handri, Eko Yon, Dana Indra Sensuse, and Avinanta Tarigan. 2024. "Developing an Agile Cybersecurity Framework With Organizational Culture Approach Using Q Methodology." *IEEE Access* 12: 108835–108850. https://doi.org/10.1109/access.2024.3432160.

Heidt, Margareta, Jin P Gerlach, and Peter Buxmann. 2019. "Investigating the security divide between SME and large companies: How SME characteristics influence organizational IT security investments." *Information Systems Frontiers* 21: 1285–1305. https://doi.org/10.1007/s10796-019-09959-1.

Heikkilä, Marjo, Anita Rättyä, Sakari Pieskä, and Joni Jämsä. 2016. "Security challenges in small-and medium-sized manufacturing enterprises." In *2016 International Symposium on Small-scale Intelligent Manufacturing Systems (SIMS)*, 25–30. IEEE.

Hong, Yuxiang, and Steven Furnell. 2021. "Understanding cybersecurity behavioral habits: Insights from situational support." *Journal of Information Security and Applications* 57: 102710. https://doi.org/10.1016/j.jisa.2020.102710.

Jackson, Corey Brian, Kevin Crowston, and Carsten Østerlund. 2018. "Did they login?: Patterns of Anonymous Contributions in Online Communities." *Proceedings of the ACM on Human-Computer Interaction* 2 (CSCW): 1–16. https://doi.org/10.1145/3274346.

Jagusiak-Kocik, Marta. 2017. "PDCA cycle as a part of continuous improvement in the production company-a case study." *Production engineering archives* 14 (14): 19–22. https://doi.org/10.30657/pea.2017.14.05.

Jahankhani, Hamid, Lakshmi N. K. Meda, and Mehrdad Samadi. 2022. *Cybersecurity Challenges in Small and Medium Enterprise (SMEs)*, 1–19. Springer International Publishing.

Jalalvand, Fatemeh, Mohan Baruwal Chhetri, Surya Nepal, and Cecile Paris. 2024. "Alert Prioritisation in Security Operations Centres: A Systematic Survey on Criteria and Methods." *ACM Computing Surveys* 57 (2): 1–36. https://doi.org/10.1145/3695462.

Janeja, Vandana P. 2022. *Data Analytics for Cybersecurity.* Cambridge University Press.

Kabanda, Salah, Maureen Tanner, and Cameron Kent. 2018. "Exploring SME cybersecurity practices in developing countries." *Journal of Organizational Computing and Electronic Commerce* 28 (3): 269–282. https://doi.org/10.1080/10919392.2018.1484598.

Kalhoro, Shadab, Ramesh Kumar Ayyasamy, AbdulKarim Kanaan Jebna, Anam Kalhoro, Kesavan Krishnan, and Suresh Nodeson. 2022. "How Personality Traits Impacts on Cyber Security Behaviors of SMEs Employees." In *2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, November, 635–641. IEEE.

Kandpal, Saral, Sachin Bhatt, Lalit Mohan, Amit Patwal, and Pushpendra Kumar. 2023. "Cyber Security Implementation Issues in Small to Medium-sized Enterprises (SMEs) and their Potential Solutions: A Comprehensive Analysis." In *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, July, 1–5. IEEE.

Kannelønning, Kristian, and Sokratis K Katsikas. 2023. "A systematic literature review of how cybersecurity-related behavior has been assessed." *Information & Computer Security* 31 (4): 463–477. https://doi.org/10.1108/ics-08-2022-0139.

Kavakli, Evangelia, Pericles Loucopoulos, and Yannis Skourtis. 2022. "Capability oriented RE for Cybersecurity and Personal Data Protection: Meeting the challenges of SMEs." In *2022 IEEE 30th International Requirements Engineering Conference Workshops (REW)*, 244–249. IEEE.

Kent, Cameron, Maureen Tanner, and Salah Kabanda. 2016. "How South African SMEs address cyber security: The case of web server logs and intrusion detection." In *2016 IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech)*, 100–105. IEEE.

Khaliq, Salman, Zain Ul Abideen Tariq, and Ammar Masood. 2020. "Role of user and entity behavior analytics in detecting insider attacks." In *2020 International Conference on Cyber Warfare and Security (ICCWS)*, 1–6. IEEE.

Khan, Muhammad Zunair Ahmed, Muhammad Mubashir Khan, and Junaid Arshad. 2022. "Anomaly detection and enterprise security using user and entity behavior analytics (UEBA)." In *2022 3rd International Conference on Innovations in Computer Science & Software Engineering (ICONICS)*, 1–9. IEEE.

Kim, Euiyoung, JungKyoon Yoon, Jieun Kwon, Tiffany Liaw, and Alice M Agogino. 2019. "From innocent irene to parental patrick: Framing user characteristics and personas to design for cybersecurity." In *Proceedings of the Design Society: International Conference on Engineering Design*, Vol. 1, 1773–1782. Cambridge University Press.

King, Zoe M, Diane S Henshel, Liberty Flora, Mariana G Cains, Blaine Hoffman, and Char Sample. 2018. "Characterizing and measuring maliciousness for cybersecurity risk assessment." *Frontiers in psychology* 9: 290575. https://doi.org/10.3389/fpsyg.2018.00039.

Kävrestad, Joakim, Marcus Birath, and Nathan Clarke. 2024. *Incident Response*, 61–67. Springer.

Lacity, Mary C, and Peter Reynolds. 2014. "Cloud services practices for small and medium-sized enterprises." *MIS Quarterly Executive* 13 (1).

Landauer, Max, Florian Skopik, Georg Höld, and Markus Wurzenberger. 2022. "A User and Entity Behavior Analytics Log Data Set for Anomaly Detection in Cloud Computing." In *2022 IEEE International Conference on Big Data (Big Data)*, 4285–4294. IEEE.

Le, Tran Duc, Thang Le-Dinh, and Sylvestre Uwizeyemungu. 2024. "Search engine optimization poisoning: A cybersecurity threat analysis and mitigation strategies for small and medium-sized enterprises." *Technology in Society* 102470. https://doi.org/10.1016/j.techsoc.2024.102470.

Le Dinh, Thang, Thi My Hang Vu, Nguyen Anh Khoa Dam, and Chan Nam Nguyen. 2022. "Trivi: A conceptual framework for customer intelligence systems for small and medium-sized enterprises." In *2022 Pacific Asia Conference on Information Systems (PACIS)*, 177.

Leenen, Louise, and Thomas Meyer. 2021. *Artificial intelligence and big data analytics in support of cyber defense*, 1738–1753. IGI Global.

Li, Ling, Wu He, Li Xu, Ivan Ash, Mohd Anwar, and Xiaohong Yuan. 2019. "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior." *International Journal of Information Management* 45: 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017.

Liu, Shangsong, Di Peng, Haotian Zhu, Xiaolin Wen, Xinyi Zhang, Zhenghao Zhou, and Min Zhu. 2021. "MulUBA: multi-level visual analytics of user behaviors for improving online shopping advertising." *Journal of Visualization* 24 (6): 1287–1301. https://doi.org/10.1007/s12650-021-00771-1.

Lozano, Mario Aragonés, Israel Pérez Llopis, and Manuel Esteve Domingo. 2023. "Threat hunting architecture using a machine learning approach for critical infrastructures protection." *Big Data and Cognitive Computing* 7 (2): 65. https://doi.org/10.3390/bdcc7020065.

MacColl, Jamie, James Sullivan, Jason RC Nurse, Gareth Mott, Sarah Turner, Edward Cartwright, and Anna Cartwright. 2023. "Cyber Insurance and the Ransomware Challenge." *Royal United Services Institute (RUSI)* .

Malatji, Masike, Sune Von Solms, and Annlizé Marnewick. 2019. “Socio-technical systems cybersecurity framework.” *Information & Computer Security* 27 (2): 233–272. https://doi.org/10.1108/ICS-03-2018-0031.

Mihailescu, Marius Iulian, Stefania Loredana Nita, Marius Rogobete, and Valentina Marascu. 2023. “Unveiling Threats: Leveraging User Behavior Analysis for Enhanced Cybersecurity.” In *2023 15th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, 01–06. IEEE.

Mitrofan, Andrei-Laurențiu, Elena-Veronica Cruceru, and Andreea Barbu. 2020. “Determining the main causes that lead to cybersecurity risks in SMEs.” *Business Excellence & Management* 10 (4). https://doi.org/10.24818/beman/2020.10.4-03.

Moallem, Abbas. 2024. *Human Behavior in Cybersecurity Privacy and Trust*, 77–107. CRC Press.

Mohan, Rathish, Abhishek Vajpayee, Srikanth Gangarapu, and Vishnu Vardhan Reddy Chilukoori. 2024. “Mitigating Complex Cyber Threats: An Integrated Multimodal Deep Learning Framework for Enhanced Security.” *International Journal for Research in Applied Science and Engineering Technology* 12 (9): 1108–1117. https://doi.org/10.22214/ijraset.2024.64150.

Moore, Kevin E. 2023. “Analyzing Small Business Strategies to Prevent External Cybersecurity Threats.” Walden University. Thesis.

Moustafa, Ahmed A, and Abubakar Bello. 2021. “The role of user behaviour in improving cyber security management.” *Frontiers in Psychology* 12: 561011. https://doi.org/10.3389/fpsyg.2021.561011.

Nagahawatta, Ruwan, Sachithra Lokuge, Matthew Warren, and Scott Salzman. 2021. “Cybersecurity Issues and Practices in a Cloud Context: A Comparison Amongst Micro, Small and Medium Enterprises.” In *Australasian Conference on Information Systems 2021 (ACIS)*, 45.

Naseer, Humza, Kevin Desouza, Sean B Maynard, and Atif Ahmad. 2024. “Enabling cybersecurity incident response agility through dynamic capabilities: the role of real-time analytics.” *European Journal of Information Systems* 33 (2): 200–220. https://doi.org/10.1080/0960085X.2023.2257168.

Olaniyan, Rahma, Sandip Rakshit, and Narasimha Rao Vajjhala. 2023. *Application of user and entity behavioral analytics (UEBA) in the detection of cyber threats and vulnerabilities management*, 419–426. Springer.

Olayinka, Olakunle, and Thomas Win. 2022. *Cybersecurity and Data Privacy in the Digital Age: Two Case Examples*, 117–131. IGI Global.

Ozkan, Bilge Yigit, and Marco Spruit. 2020. “Assessing and improving cybersecurity maturity for SMEs: Standardization aspects.” *arXiv preprint arXiv:2007.01751* .

Pascoe, Cherilyn E. 2023. “Public Draft: The NIST Cybersecurity Framework 2.0.” *National Institute of Standards and Technology* .

Perozzo, Haiat, Fatema Zaghloul, and Aurelio Ravarini. 2022. “CyberSecurity readiness: a model for SMEs based on the socio-technical perspective.” *Complex systems informatics and modeling quarterly* (33): 53–66. https://doi.org/10.7250/csimq.2022-33.04.

Poenaru, Robert, and Dragos Ciobanu-Zabet. 2020. “Elk stack–improving the computing clusters at dfcti through log analysis.” In *2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, 1–8. IEEE.

Rahman, Tashfiq, Rohani Rohan, Debajyoti Pal, and Prasert Kanthamanon. 2021. “Human Factors in Cybersecurity: A Scoping Review.” In *The 12th International Conference on Advances in Information Technology*, IAIT2021, June. ACM.

Rajasekar, Vani, J. Premalatha, and Rajesh Kumar Dhanaraj. 2022. *Security analytics*, 333–354. Elsevier.

Rashid, Fatema, and Ali Miri. 2021. “User and Event Behavior Analytics on Differentially Private Data for Anomaly Detection.” In *2021 7th IEEE Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, May, 81–86. IEEE.

Rawindaran, Nisha. 2023. "Impact of cyber security awareness in small, medium enterprises (SMEs) in Wales." Cardiff Metropolitan University. Thesis.

Rawindaran, Nisha, Ambikesh Jayal, and Edmond Prakash. 2022. "Exploration of the Impact of Cybersecurity Awareness on Small and Medium Enterprises (SMEs) in Wales Using Intelligent Software to Combat Cybercrime." *Computers* 11 (12): 174. https://doi.org/10.3390/computers11120174.

Rawindaran, Nisha, Liqaa Nawaf, Suaad Alarifi, Daniyal Alghazzawi, Fiona Carroll, Iyad Katib, and Chaminda Hewage. 2023. "Enhancing Cyber Security Governance and Policy for SMEs in Industry 5.0: A Comparative Study between Saudi Arabia and the United Kingdom." *Digital* 3 (3): 200–231. https://doi.org/10.3390/digital3030014.

Renners, Leonard, Felix Heine, and Gabi Dreo Rodosek. 2017. "Modeling and learning incident prioritization." In *2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, September, 398–403. IEEE.

Ruengsurat, Satida, Jaimai Eawsivigoon, Vidchaphol Sookplang, Karin Sumongkayothin, Prarinya Siritanawan, Razvan Beuran, and Kotani Kazunori. 2025. "Human-in-the-Loop for Machine Learning in Offensive Cybersecurity." In *2025 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, February, 0331–0336. IEEE.

Saeed, Saqib, Salha A Altamimi, Norah A Alkayyal, Ebtisam Alshehri, and Dina A Alabbad. 2023a. "Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations." *Sensors* 23 (15): 6666. https://doi.org/10.3390/s23156666.

Saeed, Saqib, Sarah A. Suayyid, Manal S. Al-Ghamdi, Hayfa Al-Muhaisen, and Abdullah M. Almuhaideb. 2023b. "A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience." *Sensors* 23 (16): 7273. https://doi.org/10.3390/s23167273.

Sahoo, Somya Ranjan, and Brij Bhooshan Gupta. 2019. "Classification of various attacks and their defence mechanism in online social networks: a survey." *Enterprise Information Systems* 13 (6): 832–864. https://doi.org/10.1080/17517575.2019.1605542.

Salitin, Manya Ali, and Ali Hussein Zolait. 2018. "The role of User Entity Behavior Analytics to detect network attacks in real time." In *2018 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, November, 1–5. IEEE.

Samtani, Sagar, Maggie Abate, Victor Benjamin, and Weifeng Li. 2020. *Cybersecurity as an Industry: A Cyber Threat Intelligence Perspective*, 135–154. Springer International Publishing.

Sav, Ujwala, and Ganesh Magar. 2020. *Insider Threat Detection Based on Anomalous Behavior of User for Cybersecurity*, 17–28. Springer Singapore.

Shashanka, Madhu, Min-Yi Shen, and Jisheng Wang. 2016. "User and entity behavior analytics for enterprise security." In *2016 IEEE International Conference on Big Data (Big Data)*, December, 1867–1874. IEEE.

Shivappa, Pranitha Kedambady, and Pushparaj Shetty D. 2024. "An Approach for Integrating Behavioral Analytics and Machine Learning for Enhanced Cybersecurity." In *2024 4th Asian Conference on Innovation in Technology (ASIANCON)*, August, 1–6. IEEE.

Singh, Nitin, Venkataraghavan Krishnaswamy, and Justin Zuopeng Zhang. 2022. "Intellectual structure of cybersecurity research in enterprise information systems." *Enterprise Information Systems* 17 (6). https://doi.org/10.1080/17517575.2022.2025545.

Sonwani, Himanshu, Mohit Divya, Anurag Dhawan, Arpit Mantri, and Harish Kumar. 2022. "A Comprehensive Study on Threat Intelligence Platform." In *2022 International Conference on Communication, Computing and Internet of Things (IC3IoT)*, 1–5. IEEE.

Sutton, Anna, and Lisa Tompson. 2025. "Towards a cybersecurity culture-behaviour framework: A rapid evidence review." *Computers & Security* 148: 104110. https://doi.org/10.1016/j.cose.2024.104110.

Thomas, Tony, Athira P. Vijayaraghavan, and Sabu Emmanuel. 2020. *Machine Learning Ap-*

proaches in Cyber Security Analytics. Springer Singapore.

Trantidou, Tatiana, George Bravos, Philippe Valoggia, Ioannis Skourtis, Manolis Falelakis, Kostas Poulios, Ilias Spais, et al. 2022. "SENTINEL - Approachable, tailor-made cybersecurity and data protection for small enterprises." In *2022 IEEE International Conference on Cyber Security and Resilience (CSR)*, July, 112–117. IEEE.

van Haastrecht, Max, Bilge Yigit Ozkan, Matthieu Brinkhuis, and Marco Spruit. 2021. "Respite for SMEs: A Systematic Review of Socio-Technical Cybersecurity Metrics." *Applied Sciences* 11 (15): 6909. https://doi.org/10.3390/app11156909.

White, Gareth R. T., Robert A. Allen, Anthony Samuel, Ahmed Abdullah, and Robert J. Thomas. 2022. "Antecedents of Cybersecurity Implementation: A Study of the Cyber-Preparedness of U.K. Social Enterprises." *IEEE Transactions on Engineering Management* 69 (6): 3826–3837. https://doi.org/10.1109/tem.2020.2994981.

Williquette, Joel F. 2019. *Cybersecurity Concerns in International Business*, 1690–1702. IGI Global.

Wu, Nan, Xueming Tang, and Ying Pan. 2022. "Log filtering method based on user behaviors." *Journal of Physics: Conference Series* 2253 (1): 012014. https://doi.org/10.1088/1742-6596/2253/1/012014.

Xi, Xiangyu, Tong Zhang, Wei Ye, Zhao Wen, Shikun Zhang, Dongdong Du, and Qing Gao. 2018. "An Ensemble Approach for Detecting Anomalous User Behaviors." *International Journal of Software Engineering and Knowledge Engineering* 28 (11n12): 1637–1656. https://doi.org/10.1142/s0218194018400211.

Yigit Ozkan, Bilge, and Marco Spruit. 2023. "Adaptable security maturity assessment and standardization for digital SMEs." *Journal of Computer Information Systems* 63 (4): 965–987. https://doi.org/10.1080/08874417.2022.2119442.

Zhang, Tianzhu, Han Qiu, Gabriele Castellano, Myriana Rifai, Chung Shue Chen, and Fabio Pianese. 2023. "System Log Parsing: A Survey." *IEEE Transactions on Knowledge and Data Engineering* 1–20. https://doi.org/10.1109/tkde.2022.3222417.

Zhao, Peihai, Zhijun Ding, Mimi Wang, and Ruihao Cao. 2019. "Behavior Analysis for Electronic Commerce Trading Systems: A Survey." *IEEE Access* 7: 108703–108728. https://doi.org/10.1109/access.2019.2933247.

Zhao, Rui. 2023. "FProbe: The Flow-Centric Detection and a Large-Scale Measurement of Browser Fingerprinting." In *2023 32nd International Conference on Computer Communications and Networks (ICCCN)*, July, 1–10. IEEE.