electronics

MDPI

Review

Cybersecurity Analytics for the Enterprise Environment: A Systematic Literature Review

Tran Duc Le [1,*], Thang Le-Dinh [2] and Sylvestre Uwizeyemungu [3]

[1] Department of Mathematics, Statistics & Computer Science, University of Wisconsin-Stout, Menomonie, WI 54751, USA
[2] Department of Marketing and Information Systems, Université du Québec à Trois-Rivières, Trois-Rivières, QC G9A 5H7, Canada; thang.ledinh@uqtr.ca
[3] Department of Accounting, Université du Québec à Trois-Rivières, Trois-Rivières, QC G9A 5H7, Canada; sylvestre.uwizeyemungu@uqtr.ca
* Correspondence: let@uwstout.edu

Abstract: The escalating scale and sophistication of cyber threats compel enterprises to urgently adopt data-driven security analytics. This systematic literature review, adhering to the PRISMA protocol, rigorously synthesizes current knowledge by analyzing 65 peer-reviewed studies (2013–2023) from six major databases on enterprise-level cybersecurity analytics. Our findings reveal a significant industry-wide transition from traditional signature-based tools towards advanced cloud-enabled, big-data and artificial intelligence-powered techniques, where machine learning and graph-based models are increasingly prominent in recent works. While large organizations in finance, Information and Communication Technology, and critical utilities spearhead adoption, dedicated research focusing on small and medium-sized enterprises (SMEs) remains notably limited. Ten thematic observations encapsulate key adoption drivers, an evolving preference for proactive and predictive security strategies, the critical role of heterogeneous log and network data, and persistent implementation challenges-notably data integration, skills shortages, and cost. Furthermore, this review identifies crucial open research avenues, including the development of real-time scalable analytics, unified policy languages, and critically needed SME-oriented solutions. Collectively, these insights provide a robust evidence base to inform future research trajectories and guide the practical deployment of effective cybersecurity analytics in diverse enterprise settings.

Keywords: cybersecurity analytics; PRISMA; enterprise security; systematic literature review

check for updates

Academic Editors: Seokjoo Shin and Domenico Rosaci

Received: 30 April 2025
Revised: 22 May 2025
Accepted: 29 May 2025
Published: 31 May 2025

Citation: Le, T.D.; Le-Dinh, T.; Uwizeyemungu, S. Cybersecurity Analytics for the Enterprise Environment: A Systematic Literature Review. *Electronics* **2025**, *14*, 2252. https://doi.org/10.3390/electronics14112252

1. Introduction

In today's quickly changing digital world, enterprises confront an expanding number of security risks and vulnerabilities [1]. Cyberattacks have increased dramatically due to the increasing use of new technologies such as cloud computing [2], mobile devices [3], and the Internet of Things (IoT) [4]. This leads to new difficulties for enterprises in protecting their resources and data. Distributed Denial of Service (DDoS) attacks, phishing attacks, malware attacks, theft of sensitive data, or even threats from within enterprises are the most dangerous threats to enterprises [5]. These threats can cause financial losses, reputational damage, and loss of user data [6]. Companies need comprehensive security solutions to maintain stable company operations, ensure customer trust, and raise security awareness [7].

Traditional security tools such as firewalls [8], intrusion detection systems [9], and antivirus software have been shown to be ineffective against persistent and sophisticated cyberattacks [10]. To access sensitive information without permission, adversaries continue to create new techniques and methods, exploit zero-day vulnerabilities [11], and leverage social engineering [12] for unauthorized access to sensitive information. Cybersecurity analytics [13,14] has evolved as a significant component in enterprise security strategy in order to react to these complex threats. Consequently, the escalating challenge posed by such advanced threats, notably Advanced Persistent Threats (APTs) that circumvent traditional security, underscores the critical need for a comprehensive review to consolidate current knowledge on the efficacy and evolution of cybersecurity analytics in enterprise defense.

Using sophisticated data analysis techniques [15], cybersecurity analytics can help companies identify, assess, and respond to potential threats more efficiently and quickly [16]. This solution identifies and mitigates possible hazards by collecting, processing, and analyzing security-related data [17,18].

Despite the growing interest in cybersecurity analysis methodologies, a conspicuous lack of clarity regarding their efficacious application within the enterprise context persists. Many barriers such as encompassing budgetary limitations, a dearth of requisite technical expertise, and persistent data privacy concerns contribute to the deployment process's complexities [19]. There appears to be a noticeable scarcity of methodical endeavors through which to synthesize and consolidate knowledge from individual studies dispersed across the domain. This circumstance underscores a prominent knowledge gap and accentuates the necessity of a systematic literature review (SLR). An SLR of this nature would foster a holistic viewpoint on cybersecurity analytics within the enterprise milieu, weaving together disparate strands of knowledge to produce a comprehensive, unified understanding of the field.

The motivation for conducting a systematic literature review on cybersecurity analytics for enterprise environments is threefold. First, it provides complete and insightful information on trends and changes that have occurred in developing and implementing cybersecurity analytics solutions in an enterprise context. Next, it helps businesses to have more information about the cutting-edge methods, tools, frameworks, applications, and deployment strategies used in the field. As a result, it enables them to make informed choices when applying cybersecurity analytics solutions. Finally, this review emphasizes the field's significant challenges and gaps and encourages more research and development activities.

This review focuses on studies explicitly addressing cybersecurity analytics in the enterprise context and on research that can be extrapolated to this context. It aims to provide a complete and up-to-date synthesis of the security analysis literature for enterprises to inform both researchers and practitioners in this field.

2. Delving into Security Analytics

Before delving into security analytics, it is important to note that, within the scope of this research, the terminologies "*cybersecurity analytics* " and "*security analytics*" are employed synonymously to denote identical concepts. Henceforth, for the sake of simplicity, the term "*security analytics*" will be predominantly employed.

The cybersecurity landscape is in constant flux, dynamically evolving to meet the new challenges of an increasingly digitized world. At the heart of this evolution is security analytics, a potent blend of data-driven techniques and methodologies designed to strengthen an organization's cybersecurity structure [20]. It systematically involves collecting security-related data from diverse sources, meticulously processing this data to ensure quality and relevance (e.g., through cleansing, normalization, and enrichment), and then analyzing the refined data to identify patterns, trends, and anomalies. These analytical outcomes indicate potential threats or vulnerabilities within an organization's information systems, thereby enabling better-informed, proactive decision making and more effective risk mitigation [16–18,21].

This section provides an overview of security analytics, including its primary purposes and the typical data lifecycle it involves, before discussing the key challenges associated with its implementation and the motivation for this review.

Purposes of Security Analytics

Security analytics holds the potential to serve multiple purposes [14,22], including **detecting intrusions** (to identify anomalous activity that may indicate an intrusion), **investigating incidents** (to determine the root cause and identify the attacker), **responding to incidents** (by providing information on the affected systems and users), and **preventing future incidents** (by identifying vulnerabilities and recommending mitigation measures).

The Security Analytics Data Lifecycle

Key activities and techniques integral to the efficacy and application of security analytics encompass various stages from initial data gathering through processing to eventual analysis [15,23]. This lifecycle is critical in fortifying an organization's cybersecurity landscape.

The process typically begins with **data gathering** from diverse sources, including network traffic, system logs, user activity records, and external threat intelligence feeds. The aim is to achieve a comprehensive view of the organization's cybersecurity state to aid in accurate threat detection. Subsequently, this raw data undergoes meticulous **data preprocessing** to ensure its quality and relevance for analysis. Common preprocessing steps include data cleansing (to remove errors or inconsistencies), normalization (to bring data into a common format), and enrichment (to add contextual information).

Key Challenges in Implementation

While strategically leveraging data through analytics can significantly bolster an enterprise's cybersecurity posture and threat response capabilities, its practical implementation is often fraught with challenges [19]. Understanding the practical impediments organizations encounter—whether technical, organizational, or financial—is instrumental for advancing the field. Furthermore, defining and accessing the most valuable data sources and types within specific enterprise contexts remains an essential facet requiring ongoing exploration and research.

Research motivation

As we delve into security analytics, we aim to highlight its multiple applications, unravel the technicalities of its deployment, and identify gaps in current research and promising opportunities for future exploration. Recognizing that the journey of security analytics is far from linear, it is crucial to elucidate how its adoption and application have transformed over time. As a multidimensional concept, it has permeated many industries, sectors, and domains—but to what extent and where has its impact been most profoundly felt? Moreover, it is paramount that we continue to evaluate and re-imagine how data-centric methodologies can be harnessed more effectively. Thus, we must constantly re-evaluate the models, methods, and frameworks underpinning security analytics.

3. Research Methodology

This study uses the widely recognized systematic review methodology known as PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) [24], which has been extensively utilized in a range of reputable journal publications for conducting systematic literature reviews [25–29]. This methodology follows a systematic approach, encompassing four main phases, each with specific activities designed to ensure a comprehensive and transparent review process: identification, screening, judgement of eligibility, and data extraction and synthesis.

This study's SLR formulated research questions based on the identified security analytics challenges and the underlying motivation.

The primary research questions of this review are as follows:

- **RQ1:** How has the adoption of security analytics in enterprises evolved over time?
- **RQ2:** In which industries, fields, domains, or sectors are enterprises most actively adopting and utilizing security analytics?
- **RQ3:** What techniques, methods, models, and frameworks are enterprises employing to implement and optimize security analytics?
- **RQ4:** Which data sources and data types are integral to security analytics within an enterprise context?
- **RQ5:** What are the barriers faced by enterprises in implementing security analytics?
- **RQ6:** What are the research gaps and future research opportunities in enterprise security analytics?

Figure 1 illustrates the interrelation between research questions and their respective correlations with the primary tasks of cybersecurity analytics within the enterprise context.

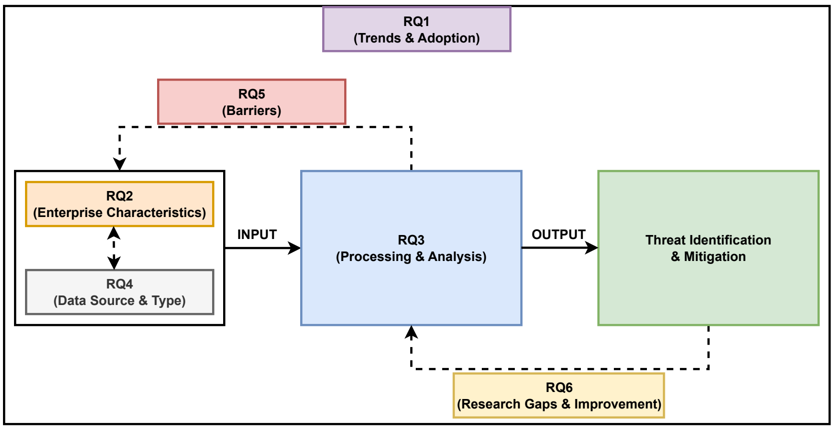

Figure 1. Relationship between research questions and cybersecurity analytics tasks in the enterprise context.

As mentioned in Section 2, RQ1 and RQ2 are related to the purposes of cybersecurity analytics. Thus, RQ3 and RQ4 are concerned with data processing. Finally, RQ5 deals with key challenges, and RQ6 is related to the research's motivation. A flow diagram based on PRISMA with all the detailed information and statistics is depicted in Figure 2.

In the following sections, we detail different literature review activities, including identification, screening, eligibility, and backward and forward searches.

3.1. Identification

Search Strategy

This study gathered research articles from the following digital databases: *IEEE Xplore*, *Scopus*, *Web of Science*, *ScienceDirect*, *ACM Digital Library*, and *Proquest*. The choice of the database took into account its scope and relevance in academia. *IEEE Xplore* is the leading academic database in engineering and computer science (https://paperpile.com/g/academic-research-databases/ (accessed on 29 April 2025)). *Scopus* is an online abstract and indexing service provided through *Elsevier*. *Web of Science*, *ScienceDirect*, *ACM Digital Library*, and *Proquest* are well-known databases providing access to a wide range of academic literature. Researchers commonly use these databases because they provide access to high-quality, peer-reviewed articles and other academic resources.

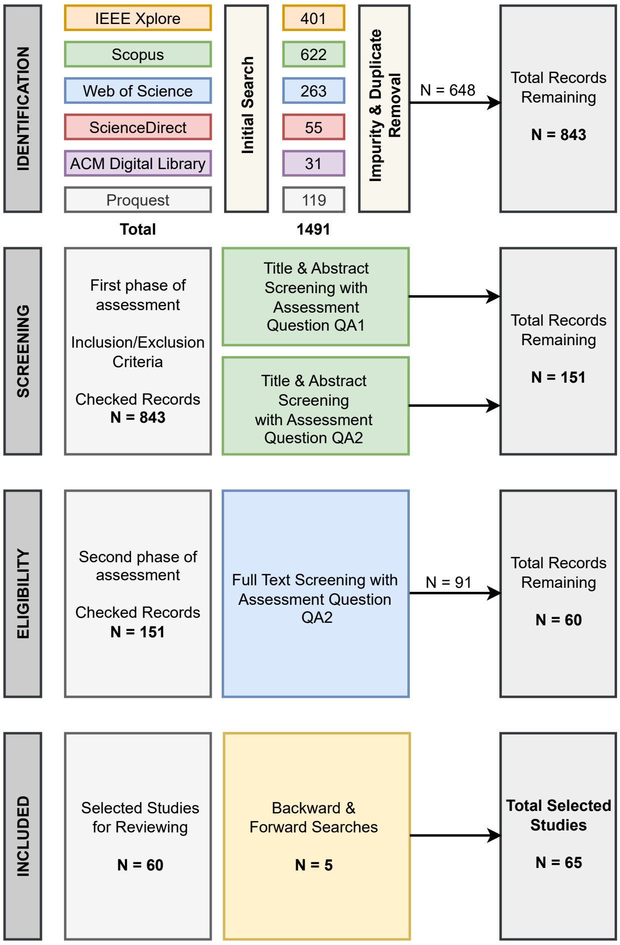

Figure 2. PRISMA-2020 flow diagram indicating a step-by-step process of identifying and selecting the studies.

A tripartite grouping of keywords was employed in the titles, keywords, or abstracts of potential articles to ensure comprehensive and systematic inclusion of pertinent literature in this review. This grouping directly aligns with this study's main research questions and aims. **The first group** of keywords focused on the core theme of the review—security analytics. It included the following terms: (*"cybersecurity analytic*" OR "cybersecurity analysis" OR "security analytic*" OR "security analysis"*). These terms reflect the investigation of RQ1, RQ2, and RQ6, which explore the evolution, industry-specific adoption, and future research avenues in enterprise security analytics, respectively.

The second group aimed to capture the various ways that security analytics is implemented and optimized in enterprises. Therefore, the second group included (*"technique*" OR "platform*" OR "framework*" OR "method*" OR "model*" OR "approach*" OR "data *"*). These terms resonate with RQ3 and RQ4, investigating the specific techniques, methods, models, and frameworks employed in security analytics, as well as the data sources and types integral to this domain.

The third group was designed to ensure that the literature selected was relevant to the enterprise context. It included (*"enterprise*" OR "firm*" OR "compan*" OR "business*"*). This group helped to delve into RQ5 and RQ6, addressing the barriers faced by enterprises in implementing security analytics. It also tied in with our research aim to identify the impact and applications of security analytics across different sectors.

Table 1 presents the search results. It is important to note that the search results were constrained by the time at which this study was conducted. In total, 1491 potentially relevant publications were identified.

Table 1. Search results from major databases.

Database	ID	Total
ACM Digital Library	DB01	31
IEEE Xplore	DB02	401
Proquest	DB03	119
ScienceDirect	DB04	55
Scopus	DB05	622
Web of Science	DB06	263
Total		**1491**

Study Selection

In order to identify relevant studies within the scope of the research field under consideration, specific criteria for inclusion and exclusion were established.

- **Inclusion Criteria** included
  - InC01. Studies published in the last ten years, between 2013 and 2023;
  - InC02. Studies published in conferences and journals;
  - InC03. Studies that are written in English.
- **Exclusion Criteria** included
  - ExC01. Studies published before 2013;
  - ExC02. Studies that are published in non-peer-reviewed sources;
  - ExC03. Studies that are not written in English;
  - ExC04. Studies published in preprint platforms;
  - ExC05. Studies for which the full text is not available;
  - ExC06. Studies in which none of the phrases from the above searching groups were included in the title or abstract;
  - ExC07. Studies that are a survey or a review.

The selection of the 2013–2023 publication window (InC01) was deliberate, aiming to capture the most relevant decade reflecting the maturation and widespread adoption of key technologies that fundamentally reshaped enterprise security analytics. This period encompasses the significant rise of Big Data analytics, the increased migration of enterprises to cloud computing environments facilitating large-scale data processing, and the notable shift towards employing machine learning and artificial intelligence techniques, as identified by our findings (see Section 4.1, Ob2). Focusing on this timeframe ensures that the review concentrates on contemporary approaches and challenges pertinent to the current state of the art in a rapidly evolving field, excluding earlier foundational work that may rely on significantly different technological underpinnings. Furthermore, our search concluded with publications up to the end of December 2023. While the manuscript preparation and review process extended into 2025, this defined cutoff date is necessary to ensure a consistent and replicable dataset for analysis. Additionally, delays in database indexing mean that the most recent publications (from 2024 and early 2025) may not have been fully available or indexed at the time the systematic search and screening were finalized, ensuring that the 2013–2023 window represents the most comprehensive dataset achievable at the point of analysis commencement.

It should be noted that during the search process (as shown in Table 1), specific inclusion and exclusion criteria were incorporated to reduce the number of publications requiring scrutiny. Nonetheless, these criteria were still manually employed to screen and eliminate studies that did not meet the requirements, given that specific databases lacked sufficient filters for searching.

All selected research articles were saved in *EndNote version 21.5* (https://endnote.com/ (accessed on 29 April 2025)), a piece of reference management software for scholarly publications.

Removal of Duplicate Records

In this step, we employed the “*Find Duplicates*” function in *EndNote* to eliminate duplicated records, resulting in 1150 remaining records. However, due to variations in the information fields of papers from different database sources, *EndNote* might miss some duplicate papers. To ensure the uniqueness of each record, we conducted a manual double-check. Furthermore, records representing general content, table of contents, or cover pages of conferences were also removed. After completing this step, the remaining number of records was 843. Lastly, the “*Find Reference Updates*” feature in *EndNote* was utilized to guarantee the inclusion of the final versions of all records.

3.2. Study Selection Process

The study selection process was conducted in multiple stages, adhering to the PRISMA guidelines [24], and involved screening, eligibility assessment, and supplementary searches. This process aimed to identify all peer-reviewed studies directly relevant to cybersecurity analytics in enterprise environments published between 2013 and 2023. The entire study selection procedure, from the initial screening of titles and abstracts through to the full-text review for final inclusion, was conducted by a team of three researchers. To ensure consistency in the application of selection criteria and to resolve any ambiguities encountered during the evaluation of papers, a consensus-based approach was employed. In cases where consensus could not be reached through discussion, the first author made the final determination for inclusion or exclusion.

3.2.1. Screening Stage (Title and Abstract Review)

After the initial database search yielded 1491 potentially relevant publications (as detailed in Table 1), an initial screening based on titles and abstracts was performed to remove studies that were clearly irrelevant. This crucial step helped to narrow down the corpus to a more manageable set for full-text assessment. During this stage, two key relevance assessment questions, derived from our research scope, were applied:

- **Relevance Question 1 (RQ1$_{screen}$):** Does the title or abstract contain keywords from both our first search group (cybersecurity/security analytics terms) AND our third search group (enterprise context terms)?
- **Relevance Question 2 (RQ2$_{screen}$):** Does the title or abstract indicate that the study’s primary focus is on security analytics specifically for an enterprise, organizational, or business context?

Studies had to satisfy both RQ1$_{screen}$ and RQ2$_{screen}$, alongside the general inclusion criteria (e.g., language, year), to proceed. This screening process resulted in the exclusion of 692 records. Consequently, 151 records remained for full-text eligibility assessment.

3.2.2. Eligibility Stage (Full-Text Review)

In this phase, the full texts of the 151 remaining studies were thoroughly assessed. The primary aim was to confirm their direct relevance to the review’s research questions and ensure they met all predefined inclusion criteria. The key relevance assessment question applied here was as follows:

- **Relevance Question 3 (RQ3$_{full\text{-}text}$):** Based on the full text, does the study substantively address security analytics within an enterprise context, providing insights relevant to our research questions (e.g., regarding techniques, frameworks, data, challenges, or future directions)?

Each study was evaluated against RQ3$_{full\text{-}text}$ and the complete set of inclusion/exclusion criteria. This detailed review ensured that only the most relevant studies were included. Following this rigorous assessment, 91 records were excluded, primarily due to a lack of direct relevance to the enterprise security analytics context upon full-text review or insufficient detail pertinent to our research questions. This resulted in 60 studies proceeding to data extraction (the flow of studies is illustrated in the PRISMA diagram in Figure 2). These selected studies are denoted by the symbol "*S*" (e.g., S1, S2, S3).

3.2.3. Backward and Forward Searches (Snowballing)

To further ensure comprehensive coverage and mitigate the risk of missing relevant publications, a snowballing technique, encompassing both backward (examining reference lists of included studies) and forward (identifying studies that cited the included studies) searches [30], was conducted on the 60 studies identified. Any new studies retrieved through this method underwent the same rigorous screening, eligibility, and quality appraisal process described above. Through this snowballing process, an additional five relevant studies were identified and included. These studies are denoted by the symbol "*A*" (e.g., A1, A2, A3, A4, A5).

3.2.4. Quality Appraisal

The primary objective of this systematic literature review was to comprehensively map the existing research landscape, identifying key themes, prevalent challenges, and future research directions in enterprise security analytics. Accordingly, our quality appraisal process was designed to ensure the relevance, clarity, and utility of the included studies for achieving these mapping objectives. All selected studies were peer-reviewed journal articles or full conference papers, which provided an inherent baseline of academic rigor.

During the full-text eligibility assessment, beyond confirming direct topical relevance to our research questions (as per RQ3$_{full\text{-}text}$), our team actively assessed each study based on the following considerations:

- **Clarity of Contribution:** the extent to which the study's objectives, methodology, and findings were clearly presented and understandable.
- **Sufficiency of Detail:** whether the study provided adequate detail to allow for the extraction of relevant data pertaining to our review's specific research questions (e.g., on techniques, frameworks, data sources, and challenges).
- **Direct Contribution to Review Objectives:** the degree to which the study made a discernible and substantive contribution to the understanding of enterprise security analytics in line with the aims of this review.

Studies that were found to be significantly lacking in clarity, provided insufficient detail for meaningful data extraction, or did not offer a discernible contribution to the specific focus areas of this review were excluded during the eligibility phase.

While a formal critical appraisal of the intrinsic methodological soundness of each primary study using a standardized checklist (e.g., CASP, AMSTAR) for scoring or as an independent exclusion criterion was not performed, our multi-faceted eligibility and appraisal process ensured that the final set of 65 studies was robust, relevant, and of sufficient quality to address the comprehensive mapping objectives of this systematic literature review.

3.3. Characteristics of Included Studies

Of 65 selected studies, 48 were from conferences, and 17 were from journals (see Table A1). The three years when the most studies had been published were 2015, 2016, and 2020. Figure 3 shows the number of studies published and their types by year.

Despite fluctuations and a recent decrease in published studies from 2013 to 2023 in security analytics within an enterprise context, this should not be seen as diminishing interest. Instead, the field is transitioning from "burgeoning" to "emerging". The drop in studies may reflect the field's complexities, necessitating deeper research and potentially longer publication times. Concurrently, this field remains promising and shows vast unexplored potential, as indicated by gaps in areas like methodological approaches, data source integration, visualization, real-time analysis, and scalability and performance. The recent decrease may suggest a shift in research focus towards these comprehensive studies, affirming the relevance and importance of ongoing research in this domain.

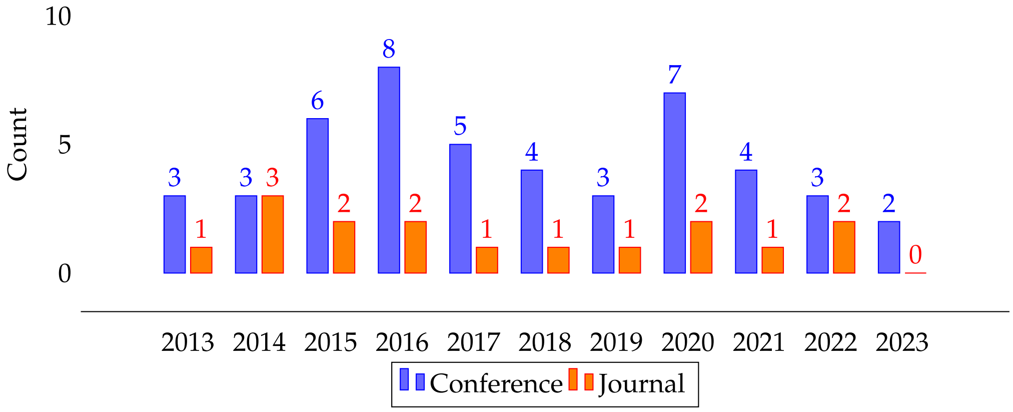

Figure 3. Annual distribution and type of 65 primary studies on enterprise security analytics (2013–2023). The trend indicates initial growth followed by fluctuations and a recent decrease, possibly reflecting a shift in research focus towards more complex studies in an emerging field.

4. Results and Analysis

This section presents the findings and interpretation of results derived from the systematic literature review (see the Supplementary Materials), structured around the six research questions proposed earlier to delineate the current state of cybersecurity analytics in enterprise environments. The analysis aims to provide a comprehensive understanding of prevailing trends, adopted methodologies, and persistent challenges.

4.1. The Adoption and Evolution of Security Analytics in Enterprises (RQ1)

This subsection addresses the first research question (RQ1) by examining the adoption trajectory of security analytics within enterprises. It highlights key evolutionary patterns and identifies the primary catalysts shaping its current landscape. Our systematic review of 65 studies (2013–2023) revealed that enterprise adoption of security analytics is not merely a trend but a strategic response to a confluence of evolving pressures and technological advancements.

Observation 1 (Ob1): Multifaceted Drivers Necessitate Advanced Security Analytics

The impetus for enterprises to adopt and advance their security analytics capabilities is driven by a complex interplay of factors. These are not isolated pressures but interconnected elements spanning the threat landscape, business operational demands, and the pervasive influence of data-intensive technologies. Understanding these drivers is crucial for contextualizing the shift towards more sophisticated analytical approaches.

Ob1.1 The Evolving Landscape of Threats and the Limitations of Traditional Defenses

A primary driver identified across numerous studies is the escalating sophistication, volume, and persistence of cyber threats, which increasingly render traditional, signature-based security measures inadequate.

- **Elaboration and Evidence:** Enterprises are confronted with an increasingly dynamic threat environment, characterized by the evolving behaviors of malicious actors [31] and the diverse impacts of varying attack vectors [32]. A significant accelerator in this context is the documented surge in APTs, which are designed to bypass conventional defenses [33]. Compounding this, traditional security methodologies often fail to adequately translate high-level security needs into concrete, implementable security requirements [34]. Furthermore, a recurrent theme is that existing security solutions are frequently not designed holistically, leading to fragmented defenses [35]. The inherent complexity and continuous changeability of modern business processes further exacerbate these vulnerabilities [36].
- **Analysis:** The failure of legacy systems to counter advanced threats effectively creates significant security gaps, exposing organizations to severe financial, operational, and reputational damage. This necessitates a fundamental shift from purely reactive defense postures to strategies emphasizing proactive threat anticipation and predictive analytics. The core implication is the urgent need for security analytics solutions capable of discerning complex attack patterns, identifying subtle anomalies indicative of compromise [37], and adapting dynamically to new adversarial techniques. This also calls for proactive breach detection mechanisms [38].
- **Trends and Challenges:** This driver directly fuels the industry-wide transition towards AI-powered techniques, particularly machine learning and deep learning, for advanced threat detection, behavioral analysis, and predictive security. Key technological trends responding to this include the development of sophisticated Security Information and Event Management (SIEM) systems, Endpoint Detection and Response (EDR), and Network Detection and Response (NDR) solutions that leverage these analytical capabilities [39]. However, a significant challenge lies in developing and maintaining analytics models that can keep pace with the rapid evolution of adversarial Tactics, Techniques, and Procedures (TTPs) and the sheer volume of threat intelligence [40].

Ob1.2 Business Imperatives: Efficiency, Cost-Effectiveness, and Strategic Security Alignment

Beyond the pressures of direct threats, the adoption of security analytics is strongly influenced by fundamental business imperatives, including the demand for greater operational efficiency, cost-effectiveness, and the strategic alignment of cybersecurity with broader corporate objectives.

- **Elaboration and Evidence:** A consistent theme in the literature is the organizational need for security approaches that offer high performance and enhanced efficiency [41]. This is often championed by decision makers who are tasked with integrating security analytics into the overarching business strategy [42], a process that inherently involves navigating the challenge of balancing robust security measures with budgetary constraints [43]. The dynamic nature of business operations also demands more agile and responsive security frameworks [36].
- **Analysis:** In the contemporary enterprise, cybersecurity is increasingly viewed not merely as an IT overhead but as a critical enabler of business continuity, trust, and innovation. Inefficient or overly costly security measures can drain resources, impede agility, and ultimately hinder competitive advantage. The core implication is a demand for security analytics that not only improve threat detection and response times but also optimize security operations, automate routine tasks, and provide clear metrics to demonstrate value and inform strategic investment decisions.
- **Trends and Challenges:** These business drivers are accelerating the adoption of Security Orchestration, Automation, and Response (SOAR) platforms, which aim to streamline security workflows by integrating analytics with automated response

actions [44]. The pursuit of efficiency also encourages the use of cloud-native security analytics platforms that offer scalability and potentially lower total cost of ownership. Challenges in this domain include effectively quantifying the return on investment (ROI) for security analytics, ensuring that automated responses do not inadvertently disrupt business processes, and seamlessly integrating security analytics into diverse and often siloed enterprise IT environments [13].

Ob1.3 Proliferation of Big Data and the Rise of Advanced Analytical Techniques

The explosion in data volume, velocity, and variety within enterprise environments, coupled with the maturation of machine learning and other advanced analytical techniques, constitutes a third major driver for the adoption of specialized security analytics.

- **Elaboration and Evidence:** Enterprises today must contend with analyzing vast volumes of often unstructured or semi-structured data, such as text logs from myriad systems [45], and navigate the inherent security risks associated with managing these large-scale Big Data environments [46]. A common operational pain point is the high number of false positive alerts generated by simpler tools and the extensive analysis times required when dealing with heterogeneous data sources [47]. Concurrently, with the growing reliance on machine learning (ML) for various business functions, there is a corresponding need for robust security analyses specifically tailored for, and sometimes applied to, these ML systems themselves [48].
- **Analysis:** The mere collection and storage of massive datasets provide little security value without the ability to extract timely, actionable intelligence. The inability to effectively process and analyze this "data deluge" can lead to missed critical alerts, delayed incident response, and significant analyst fatigue. This underscores a critical demand for advanced data-processing architectures, scalable analytical platforms, and the application of sophisticated models (including ML and deep learning (DL)) capable of uncovering hidden patterns and anomalies within complex datasets. The goal is to transform raw security data into strategic insights.
- **Trends and Challenges:** This directly underpins the widespread move towards dedicated Big Data security analytics platforms, often leveraging cloud infrastructure for its scalability and processing power. The application of ML/AI for User and Entity Behavior Analytics (UEBA), advanced threat hunting, and fraud detection are prominent examples of this trend. However, significant challenges persist, including ensuring data quality and consistency from diverse sources, the "black-box" nature of some ML models (driving research into Explainable AI for security), the persistent shortage of cybersecurity professionals with data science skills, and the need to make complex analytics outputs more accessible and user-friendly, potentially through advanced visual tools [49].

In essence, these interconnected driving factors—spanning the evolving threat landscape, core business requirements, and the transformative impact of Big Data and AI—collectively compel enterprises to continuously enhance their security analytics capabilities. This understanding forms the basis for exploring how organizations are operationalizing these analytics, the specific techniques being employed, and the challenges they encounter, which will be detailed in subsequent sections.

Observation 2 (Ob2): A Progressive Technological Shift Towards Data-Driven and Intelligent Security Analytics

The evolution of security analytics within enterprise settings is intrinsically linked to and propelled by significant technological advancements. Our review indicates a clear trajectory away from traditional, often manual, security measures towards more automated, data-intensive, and intelligent analytical capabilities. This technological shift is not merely about adopting new tools but reflects a fundamental change in how organizations approach threat detection, response, and overall cyber risk management. Many selected studies highlight the strategic utilization of cutting-edge technologies such as Big Data, cloud computing, and artificial intelligence (AI)—including its subfields ML and DL—to enhance security analytics capabilities [50,51]. The prominence of these technologies in the reviewed literature is illustrated in Figure 4.

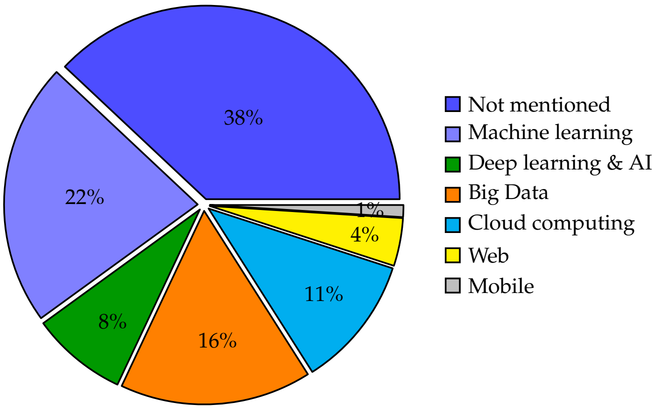

Figure 4. Distribution of primary technologies cited in the reviewed enterprise security analytics literature (N = 65 studies). The chart underscores the foundational role of machine learning, Big Data, and cloud computing, while also noting a significant portion of studies that did not focus on a specific underlying technology. Some studies incorporate multiple technologies.

As Figure 4 demonstrates, machine learning (22 studies), Big Data (16 studies), and cloud computing (11 studies) are the most frequently cited technologies, forming the core of modern enterprise security analytics. The "Not mentioned" category (38 studies) suggests that a substantial number of studies might focus on higher-level frameworks, threat types, or organizational aspects rather than specific technological implementations, or that the technology is implied (e.g., general "security analysis"). Research focusing on mobile platforms within enterprise security analytics [47,52] appears less prevalent (with 1 study explicitly tagged), though mobile security data could be ingested by broader systems. The following discussion explores the evolution and interplay of these key technologies, highlighting their impact on security analytics practices.

Ob2.1 Foundational Layers: Cloud Computing and Big Data Ecosystems

The initial significant shift observed is the adoption of cloud computing and Big Data technologies, which together provide the scalable infrastructure and data-processing capabilities essential for advanced security analytics.

- **Elaboration and Evidence (Cloud Computing):** The migration to cloud computing for security analytics reflects broader enterprise adoption driven by the pursuit of operational efficiency, scalability, and perceived cost-effectiveness [46,52–59]. As organizations increasingly entrust their data and applications to cloud environments, significant practical concerns regarding the comprehensive protection of sensitive assets against sophisticated external and internal threats emerge [53]. These concerns, such as ensuring data privacy and meeting complex compliance mandates in shared infrastructures, understandably lead some clients to hesitate in relocating their most sensitive data to the cloud [53]. This evolving landscape has spurred significant interest in leveraging dedicated cloud-native security analytics to detect complex attacks within virtualized and containerized infrastructures [56]. Modern cloud-based security analytics solutions offer the technical ability to ingest and analyze vast data volumes from diverse, distributed sources—including network logs, endpoint data, and cloud application telemetry—often in near real time to support rapid threat detection and response [38,60].

- **Elaboration and Evidence (Big Data):** Concurrent with, and often underpinning cloud adoption, the strategic focus in security analytics has decisively broadened from rudimentary data storage to the advanced processing and contextual analysis of "Big Data". This practically entails managing and deriving actionable intelligence from the escalating volume, velocity, and variety of security-relevant data streams [37,46,56,57,60–68]. Enterprises now recognize that robust Big Data capabilities are not merely advantageous but practically indispensable for identifying subtle attack patterns, anomalous behaviors, and complex correlations across heterogeneous datasets that may indicate sophisticated security breaches or ongoing, low-and-slow attacks [37].
- **Analysis:** Cloud computing provides the elastic, dynamically scalable, and potentially cost-effective infrastructural backbone essential for resource-intensive security analytics operations. Simultaneously, Big Data technologies furnish the critical tools and platforms to ingest, efficiently store, and process the massive and diverse datasets required for achieving comprehensive threat visibility and enabling deep forensic capabilities. Their synergy facilitates a crucial shift from traditionally siloed, often capacity-constrained, on-premises security monitoring paradigms towards more centralized, scalable, and potentially more effective enterprise-wide analytics. The foremost practical implication is the enhanced ability to perform significantly deeper, broader, and more context-aware analyses than previously feasible, thereby laying the critical groundwork for more intelligent and proactive security operations. However, realizing this potential practically requires significant upfront planning for data governance, security, and cost management, alongside the development of new skill sets within security teams to manage and leverage these complex, distributed environments. The transition also introduces limitations such as increased dependency on provider infrastructure and the potential for new attack surfaces specific to cloud and Big Data platforms if not adequately secured.
- **Trends and Challenges:** This foundational layer of cloud and Big Data infrastructure supports the deployment of advanced SIEM systems, the creation of security data lakes for flexible analytics, and the adoption of cloud-native security monitoring and response tools. However, its real-world application is fraught with persistent practical challenges and limitations that enterprises must navigate.
    - **Data Security, Sovereignty, and Compliance:** Managing data security and ensuring sovereignty in multi-cloud or hybrid environments presents significant operational complexity, particularly for global enterprises facing differing regional data protection regulations (e.g., GDPR, CCPA) [53]. Ensuring compliance when data traverses multiple jurisdictions or is managed by third-party providers requires robust contractual agreements and continuous auditing, which can be resource-intensive.
    - **Data Quality, Integration, and Interoperability:** Ensuring high data quality and achieving seamless interoperability among diverse security data sources (e.g., legacy systems, modern IoT devices, and cloud services) remains a major hurdle [37]. Poor data quality can lead to inaccurate analytics and an increase in false positives, diminishing trust in the system. The lack of standardized data formats (an issue addressed by initiatives like SysFlow) often necessitates complex and costly data integration efforts, diverting resources from actual analysis.
    - **Cost Management and Control:** While the cloud can offer cost-effectiveness, enterprises face challenges in controlling escalating data storage volumes, processing workloads, and, in particular, network egress fees. The specialized nature of many advanced analytics tools and platforms also adds to licensing and operational costs, requiring careful financial planning and justification of ROI.

  - **Specialized Skills Gap:** A critical practical limitation is the pervasive shortage of personnel possessing the requisite blend of skills in cybersecurity, cloud engineering, Big Data analytics, and data science needed to design, deploy, manage, and interpret the outputs of these complex ecosystems effectively [56]. This skills gap can significantly delay adoption or limit the utility of implemented solutions.
  - **Actionable Insights from Data:** While the infrastructure facilitates the collection and processing of vast data, including web-based sources [63,69], a key challenge lies in transforming this data into genuinely actionable insights for security teams. Advanced visualization and user-centered design of analytics interfaces [49,53] are crucial for enabling analysts to effectively explore data, understand alerts, and make timely decisions, but developing such interfaces requires specific expertise and iterative refinement.

Ob2.2 The Intelligence Layer: Artificial Intelligence—Machine Learning and Deep Learning

Building upon the data foundation provided by Big Data and cloud computing, the most impactful recent technological evolution is the increasing application of AI, particularly its subfields ML and DL, to imbue security analytics with greater intelligence, automation, and predictive power.

- **Elaboration and Evidence (Machine Learning):** As a core subset of AI, ML has emerged as a demonstrably powerful approach through which to address the formidable challenge of extracting meaningful and actionable insights from the large, diverse, and complex datasets generated within modern enterprise environments [41,60,70]. ML algorithms are designed to automatically uncover intricate patterns, learn from historical security data (including both malicious and benign activities), and identify subtle anomalies that may deviate from established normal behavior, proving particularly effective when applied to large-scale datasets [47,71,72]. A key **practical advantage** over traditional, static rule-based systems, which can quickly become outdated and ineffective against rapidly evolving cyber threats [73], is the ability of ML models to be continuously updated and retrained. This adaptability enables them to potentially detect emerging threats and novel attack patterns for which explicit signatures do not yet exist. ML is especially crucial for advancing predictive analytics capabilities within enterprises, allowing them to move beyond reactive defense by anticipating potential security threats and proactively implementing targeted defensive measures [37,38,48,49,58,66,74–76]. This transition represents a natural and necessary progression in maximizing the strategic value of security-related data for enhanced enterprise defense [56].
- **Elaboration and Evidence (Deep Learning):** DL, a more advanced and specialized subset of ML (and thus AI), represents a further cutting edge in the evolution of security analytics, as evidenced by its application in several reviewed studies targeting complex security challenges [57,65,77–80]. DL models, such as multi-layered neural networks, have demonstrated superior performance, particularly in handling highly complex, high-dimensional, and often unstructured or semi-structured data types prevalent in cybersecurity (e.g., raw network packet data, system call sequences, and free-text incident logs) [65,78]. A significant practical benefit of many DL architectures is their inherent ability to perform automatic feature extraction from raw data. This alleviates the need for manual feature engineering, which is often a complex, time-consuming, and expertise-intensive task for security analysts. With sufficient relevant data for training, DL techniques can achieve higher accuracy and better generalization than many traditional ML methods [77]. This enhanced accuracy is critically important in the security domain, where the consequences of both false positives (leading to alert fatigue and wasted investigative effort) and false negatives (resulting in missed

detections of actual threats) can be severe for an enterprise [57]. The capacity of DL models to continuously learn and adapt from new data makes them particularly effective for developing proactive, predictive, and dynamic security analytics solutions capable of addressing novel and evolving adversarial tactics [79,80].

- **Analysis:** The integration of AI, encompassing both ML and DL, into enterprise security analytics signifies a fundamental paradigm shift. It propels security operations beyond merely detecting known, signatured threats towards the more ambitious goals of identifying "unknown unknowns"—previously unseen attack patterns or vulnerabilities—and anticipating future adversarial campaigns. A core practical implication for enterprises is the empowerment of their security teams to adopt a more proactive stance, which can lead to tangible benefits such as reduced incident response times, minimized breach impact, and a stronger overall security posture. The capability of these AI-driven technologies to analyze security-related data at a scale and speed far surpassing human analytical capabilities is transformative for Security Operations Centers (SOCs), enabling them to better cope with the overwhelming volume of modern security telemetry. However, this transformative potential comes with practical limitations and considerations. While AI can enhance autonomy, its deployment necessitates robust validation processes and human oversight to prevent erroneous automated actions that could disrupt critical business operations or lead to misallocation of security resources. Furthermore, the promise of identifying "unknown unknowns" requires careful management of expectations, as the discovery and validation of genuinely novel threats remain complex and resource-intensive, with a persistent risk of misinterpreting anomalies.
- **Trends and Challenges:** This intelligence layer is increasingly driving the development and adoption of advanced security technologies such as UEBA, sophisticated Network Traffic Analysis (NTA) solutions, SOAR platforms, and next-generation antivirus/endpoint protection (NGAV/EPP) systems. However, the widespread and effective adoption of AI in enterprise security is not without significant practical challenges and limitations:
  - **Data Requirements and Quality:** A primary hurdle is the critical need for large volumes of high-quality, relevant, and appropriately labeled datasets for training effective supervised ML and DL models. In practice, acquiring, preparing, and maintaining such datasets is a substantial undertaking for most enterprises, demanding significant investment in data infrastructure, governance, and specialized personnel. The scarcity of labeled data for novel or zero-day attacks poses a particular challenge for supervised learning paradigms.
  - **The "Black-Box" Problem:** The "black-box" nature of many complex ML/DL models, where the reasoning behind their predictions is not easily understandable by human analysts, presents a serious real-world limitation [81]. This lack of interpretability can hinder trust, slow down adoption, and make it difficult for SOC analysts to validate alerts or for engineers to debug and refine models, potentially leading to critical alerts being overlooked or misunderstood.
  - **Adversarial AI Attacks:** ML models themselves can be targets of sophisticated adversarial attacks (e.g., data poisoning and evasion attacks), where attackers manipulate input data to cause misclassification or evade detection. This vulnerability is a growing practical concern for enterprises, as it means that AI-driven security systems can be subverted, undermining their reliability and effectiveness.
  - **Specialized Skills Gap:** There remains a significant and persistent skills gap. Data scientists and ML engineers who also possess deep cybersecurity domain expertise are lacking [81]. **Practically**, this means many enterprises struggle to hire,

develop, and retain the talent necessary to build, deploy, manage, and critically evaluate these advanced AI-driven security analytics solutions, often leading to reliance on third-party vendors or underutilization of the technology's potential.

- **Integration and Operationalization Complexity:** Integrating advanced AI analytics into existing security workflows and IT infrastructure can be complex and disruptive. Ensuring that AI-generated insights are effectively operationalized—that is, translated into timely and appropriate security actions—requires careful planning, process re-engineering, and often, significant changes to existing SOC procedures.

Ensuring a clear conceptual hierarchy wherein ML and DL are understood as integral components of the broader AI field with specific strengths and weaknesses is important for consistent understanding and strategic development within the cybersecurity domain.

Table 2 summarizes the primary impacts of these key technologies on cybersecurity analytics within the enterprise context.

Table 2. Key technologies and their transformative impacts on enterprise cybersecurity analytics.

Technology	Impact on Cybersecurity Analytics
Cloud Computing	Provides scalable and flexible infrastructure for hosting data-intensive analytics; enables efficient network monitoring, real-time threat detection, and supports business continuity.
Big Data	Enables the ingestion, storage, and processing of vast and diverse security data volumes; facilitates the extraction of actionable insights for comprehensive threat detection and mitigation.
Web Technologies	Serve as a critical data source (e.g., weblogs, application data) and a platform for delivering interactive security dashboards, visualizations, and real-time alerts for timely incident response.
Machine Learning (AI Subset)	Empowers automated detection of complex patterns, anomalies, and suspicious behaviors from large datasets; facilitates predictive analytics for early threat identification and proactive defense.
Deep Learning (AI Subset)	Handles highly complex, unstructured, and high-dimensional data; enables automatic feature engineering and continuous model adaptation for more accurate and proactive threat intelligence.

In conclusion, the technological landscape of enterprise security analytics is characterized by a dynamic and progressive integration of capabilities. From the foundational scalability offered by cloud computing and Big Data to the advanced intelligence furnished by machine learning and deep learning, this evolution reflects a relentless pursuit of more effective, efficient, and proactive strategies to combat the ever-advancing sophistication of cyber threats. This ongoing technological shift underscores the centrality of data and intelligence in modern cybersecurity paradigms.

Observation 3 (Ob3): The Imperative for a Holistic, Business-Integrated Approach to Security Analytics

Our systematic literature review reveals a growing recognition that traditional security analytics, often confined to purely technical dimensions, are increasingly insufficient to address the complex, interconnected nature of modern enterprise operations and their associated cyber risks [36,82]. This highlights a significant thematic observation: the imperative to evolve towards a holistic approach that intrinsically marries security analytics with overarching business realities, objectives, and processes [35,83].

- **Elaboration and Evidence:** A holistic approach to security analytics, as conceptualized within the reviewed literature, intentionally transcends purely technical threat detection. It advocates for an integrated methodology that systematically considers multiple organizational perspectives and critical influencing factors. In practice, this involves extending the purview of security analytics beyond the mere identification of technical vulnerabilities to also critically examine the intricate workings of core business processes, including their operational efficiency drivers [38,84], overarching strategic corporate objectives, and the continuously evolving regulatory compliance landscapes [34,85]. A recurring theme in the reviewed studies is that as business processes inevitably grow in complexity—driven by rapid technological advancements (e.g., the proliferation of interconnected IoT devices and sprawling cloud service dependencies) and dynamic market demands—the enterprise attack surface and potential threat vectors consequently become more multifaceted and deeply embedded within these operational processes [31–33,86]. This escalating complexity necessitates a security strategy that is not only comprehensive in its coverage but also inherently adaptive to change. The literature suggests that adopting such a holistic approach provides a vital context-centric perspective [57], thereby enabling the development and deployment of security measures that are more precisely tailored to unique business needs and specific risk appetites.

It is important to note a key observation from our review: while the surveyed literature strongly and consistently advocates for the *need* for holistic security analytics, and several studies propose valuable conceptual frameworks or models aiming in this direction, there is a less pronounced emphasis on empirical studies that rigorously validate the superior effectiveness or measurable ROI of specific, named holistic frameworks when compared directly with more traditional, purely technical security solutions within diverse enterprise settings. This suggests a significant practical gap and a crucial area for future research focused on the demonstrable implementation benefits and quantifiable outcomes of comprehensive holistic models.

- **Analysis:** The core critique of traditional, siloed security analytics is its inherent practical limitation, that is, a tendency to generate a narrow, technically focused view of risk that is often disconnected from the actual or potential business impact. In real-world terms, this disconnect can lead to misaligned security controls (e.g., over-investing in low-impact areas while under-resourcing critical business functions), inefficient allocation of scarce security resources, unintended disruption to critical business operations during incident response, and, ultimately, a diminished overall security posture despite significant technical efforts. Conversely, a genuinely holistic approach seeks to transform cybersecurity from being perceived merely as a cost center or a purely technical support function into a strategic business enabler that contributes to organizational resilience and trustworthiness. The practical implications of successfully adopting such an integrated approach are profound, though challenging to achieve.
  - It necessitates enhanced and sustained cross-departmental collaboration, actively breaking down entrenched silos between IT/security teams and various business units (e.g., finance, operations, legal). Practically, this requires strong leadership commitment, clear communication channels, and often, a cultural shift towards shared responsibility for security.
  - It calls for the cultivation or acquisition of cybersecurity professionals who possess not only deep technical expertise but also strong business acumen, risk management understanding, and effective communication skills to engage with diverse stakeholders. Finding or developing such hybrid talent is a significant practical challenge for many organizations.
  - It demands the development, implementation, and consistent tracking of security metrics that resonate with business leaders and clearly demonstrate the value of security investments in terms of tangible risk reduction, operational continuity,

    and business enablement [35]. Defining these metrics and collecting the necessary data can be a complex practical undertaking.
  - It implies a strategic organizational shift towards comprehensive and integrated risk management frameworks (e.g., systematically integrating cybersecurity risk into broader Enterprise Risk Management—ERM programs) that inherently consider business context, impact tolerance, and strategic objectives in all security decision making.
- **Trends and Challenges:** The drive towards a more holistic perspective in security analytics aligns with and is supported by several important technological and conceptual trends, while also facing significant **practical challenges and limitations** in its implementation:
  - **Supporting Trends:** The development and adoption of Governance, Risk, and Compliance (GRC) platforms aim to provide an integrated view and management of these interconnected domains, thereby facilitating a more holistic approach to enterprise risk. The increasing emphasis within modern system development on "Security by Design" and "Privacy by Design" principles inherently requires a proactive, holistic understanding of business processes and data flows from the earliest stages. Furthermore, advancements in AI-driven analytics are leading to more context-aware security tools, such as UEBA, which can better understand user roles and typical business functions and flag meaningful deviations from normal operational patterns.
  - **Persistent Real-World Challenges:**
    - A primary limitation is bridging the persistent communication and cultural gap that often exists between highly technical security teams and more business-focused operational units. Overcoming differing priorities and vocabularies requires concerted effort.
    - Developing meaningful, quantifiable metrics that effectively translate technical security outcomes (e.g., vulnerabilities patched, incidents contained) into demonstrable business value (e.g., risk reduction in monetary terms and protection of revenue streams) remains a complex practical task.
    - The inherent complexity of accurately modeling diverse, dynamic, and often opaque business processes, along with their intricate IT dependencies and associated security risks, can be a daunting implementation hurdle.
    - As noted earlier, the lack of widely adopted, standardized holistic frameworks and the difficulty in empirically demonstrating the direct ROI of a holistic approach compared to purely technical interventions can significantly hinder its adoption and investment justification in practice.
    - Moreover, implementing a truly holistic security strategy often involves higher initial and ongoing investment in terms of time, skilled resources, and significant organizational change management, creating a substantial practical barrier, especially for resource-constrained organizations.

In summary, Observation 3 underscores a pivotal shift in perspective: effective enterprise security analytics in the modern era must be deeply interwoven with the fabric of the business itself. This holistic integration is crucial for developing resilient, adaptive, and context-aware security strategies that not only protect assets but also support and enhance core business objectives.

4.2. The Landscape of Enterprise Security Analytics Adoption Across Industries and Sectors (RQ2)

This subsection addresses RQ2 by examining the distribution and focus of security analytics adoption across various industries, enterprise types, and operational sectors, as identified in the reviewed literature.

Observation 4 (Ob4): Concentrated Adoption in Large, Critical Sectors with a Notable Research Gap for SMEs

Our systematic review indicates that while the adoption of security analytics is present across a range of industries, its application and associated research are notably concentrated in large-scale enterprises and within sectors deemed critical, such as Information and Communication Technology (ICT), financial services, and utilities. Conversely, there is a significantly less pronounced research focus on the specific security analytics needs and adoption patterns within SMEs. Table 3 provides a detailed breakdown of security analytics adoption by industry and enterprise size as reflected in the selected studies.

Table 3. Security Adoption of analytics across industries and enterprise size.

Targeted Industry/Sector/Domain/Field	Size of Enterprise	Studies
ICT and Related Fields	Large-scale	[41]
	Any	[45,78,87–89]
Financial Services (including Online Banking) and Government Institutions	Large-scale	[35,61,66,90]
	Any	[74,91]
Industrial Control and Security Systems	Large-scale	[92]
Utilities (Power, Fuel, Energy)	Any	[42,84]
Health Systems	Any	[83]
Smart Infrastructures and Systems (including IoT, IIoT, Cyber–Physical Systems, Smart Grid)	Any	[76,93]
	SME	[58]
Not mentioned	Large-scale	[37,38,47,55,57,64,68,70,71,75,77,94]
	SME	[49,95]
	Any	[46,48,56,65,67,80,86,96,97]

- **Elaboration & Evidence:** As detailed in Table 3, the adoption of security analytics is notably concentrated in large-scale enterprises, particularly within the ICT sector [41], financial services and government institutions [35,61,66,90], and industrial control systems (ICS) environments [92]. For enterprises where specific size was not a primary focus or findings were deemed broadly applicable (“Any” size), adoption remains prominent in critical utilities (power, fuel, energy) [42,84], financial services [74,91], ICT and related fields (e.g., telecommunications, software development) [45,78,87–89], health systems [83], and increasingly in emerging smart infrastructures (including IoT and Cyber–Physical Systems) [76,93]. A substantial number of the reviewed studies that targeted large enterprises [37,38,47,55,57,64,68,70,71,75,77,94] or were applicable to “Any” enterprise size [46,48,56,65,67,80,86,96,97] did not specify a narrow industry focus. This suggests either the perceived general applicability of the discussed analytics solutions and foundational techniques or a primary research focus on the techniques themselves rather than their sector-specific nuances.

  Critically, our review reveals that only a small fraction of the selected literature (three studies: [58] focusing on Smart Infrastructures/IIoT and [49,95] focusing on non-sector-specific contexts) explicitly centers on the unique security analytics needs and adoption contexts of SMEs. Study [58], for instance, explores Security as a Service (SECaaS) tailored for SMEs operating in the Industrial Internet of Things (IIoT) domain, highlighting a potential service delivery model more attuned to their resource constraints. This starkly limited representation of SMEs in the research landscape underscores a significant practical gap; despite their collective economic importance and recognized vulnerability to a wide array of cyber threats, the development and academic investigation of tailored security analytics solutions for this segment appear considerably underdeveloped.

- **Analysis:** The observed concentration of security analytics adoption and associated research primarily within large enterprises and critical sectors can be attributed to several interconnected practical drivers and realities:
  - **Resource Availability and Operational Complexity:** Large organizations typically possess substantially greater financial and dedicated human resources, enabling them to invest in sophisticated, often expensive, analytics platforms and the specialized personnel required to manage them. They also tend to operate more extensive and complex IT/OT environments, generating vast volumes of data that both necessitates and benefits from advanced analytical capabilities for effective oversight and threat detection.
  - **Elevated Risk Profile and Potential Impact:** These larger entities are often high-value, high-visibility targets for sophisticated cyberattacks. In practical terms, a security breach can lead to catastrophic financial losses, severe reputational damage, erosion of customer trust, and widespread operational disruption (e.g., in financial systems [35,66,90] or industrial control environments [92]). This heightened risk calculus mandates proactive and advanced security measures, including robust analytics.
  - **Stringent Regulatory and Compliance Pressures:** Critical sectors such as finance, healthcare [83], and utilities [42,84] frequently operate under stringent and evolving regulatory and compliance mandates (e.g., PCI DSS, HIPAA, NERC CIP). These obligations often compel the implementation of comprehensive security monitoring, auditing, and reporting capabilities, for which security analytics are increasingly indispensable.

The practical implications of these skewed adoption and research patterns are significant and multifaceted. Firstly, the predominance of research focused on large-enterprise contexts may result in security analytics solutions, frameworks, and best practices that are not readily adaptable, affordable, or practically implementable for SMEs. Solutions may assume the availability of large, dedicated security teams, extensive historical datasets for model training, or complex integration capabilities that are often absent in smaller organizations. This directly exacerbates the cybersecurity vulnerability of SMEs, which frequently lack the internal expertise, financial resources, and operational capacity of their larger counterparts, making them attractive, softer targets for attackers. Secondly, while highly specialized, sector-specific analytics are vital (e.g., for ICS environments with unique operational technologies and threat models), the large number of studies with a "Not mentioned" industry focus suggests a substantial body of work on foundational analytics techniques. However, a practical challenge remains in effectively translating these general techniques into actionable, sector-specific guidance and configurations for practitioners in diverse fields. The pronounced SME gap, therefore, implies a pressing real-world need for focused research and development into scalable, cost-effective, and user-friendly security analytics solutions, explicitly tailored to the distinct operational realities, resource constraints, and prevalent threat landscapes faced by smaller organizations.

- **Trends and Challenges:**
  - **Supporting Trends for Broader, More Equitable Adoption:** The increasing availability of cloud-based security analytics platforms and SECaaS models [58] offers a promising pathway through which to make advanced analytical capabilities

more accessible and affordable to a wider range of organizations, including SMEs. These models can practically reduce the need for significant upfront infrastructure investment and specialized in-house management expertise. Concurrently, the ongoing development of AI-powered analytics aims to automate more complex detection, analysis, and response tasks, potentially lowering the skills barrier for adoption and making sophisticated tools more usable by teams with limited data science experience. Furthermore, there is a growing trend towards industry-specific threat intelligence sharing and the formation of collaborative platforms (e.g., Information Sharing and Analysis Centers—ISACs). These initiatives can significantly enrich security analytics with relevant, contextual threat data, a practical benefit that can enhance the effectiveness of analytics for all participating organizations, including SMEs within those sectors.

– **Persistent Real-World Challenges and Limitations:** Despite positive trends, significant hurdles remain. The primary practical challenge for SMEs continues to be the often-prohibitive cost and perceived operational complexity of implementing and managing effective security analytics tools, compounded by a persistent general shortage of affordable cybersecurity talent. For organizations of all sizes, real-world difficulties include the technical complexities of integrating analytics solutions with diverse, often siloed, IT and Operational Technology (OT) systems; ensuring consistent data quality and governance across disparate sources; and effectively managing the sheer volume of alerts generated to avoid analyst fatigue and ensure critical threats are prioritized. Developing truly sector-specific analytics that deeply understand unique industrial protocols (e.g., in manufacturing or medical systems), specific regulatory requirements, and distinct business process risks is a continuous and resource-intensive effort. The "Not mentioned" category regarding industry application in many studies (see Table 3) might also point to an ongoing practical challenge in translating general academic research findings into clear, actionable, sector-specific guidance for practitioners. Finally, a key design and market limitation is ensuring that sophisticated analytics solutions can scale down effectively for smaller organizations or those with less mature security programs, without losing essential functionality or becoming overly simplistic. Addressing these multifaceted challenges is critical for democratizing effective security analytics across the entire enterprise spectrum.

In essence, Observation 4 highlights that while security analytics is recognized as vital across the board, its current in-depth adoption and research footprint are skewed towards larger organizations in critical industries. Bridging the gap for SMEs and ensuring the continued development of effective, adaptable analytics for all sectors remain key priorities for both researchers and practitioners.

4.3. Technical Aspects of the Implementation and Optimization of Security Analytics in Enterprises (RQ3)

This subsection addresses RQ3 by dissecting the various data-processing and analysis techniques employed in enterprise security analytics, as identified in the reviewed literature. Table 4 categorized studies by these techniques; this analysis synthesizes that information.

Table 4. Selected studies on security analytics in the enterprise context.

Study	Framework, Platform, Prototype	Analysis Techniques	Method	Model	Tool	Name	Type of Analysis	Strategy
S1 [41] Cheng_2013	✓	In-memory data management	–	–	–	SAL	Mix	Proactive & Reactive
S2 [42] Holm_2013	–	Modelling language	–	–	✓	CySeMoL	Quantitative	Proactive
S3 [43] Purboyo_2013	–	Visualisation	✓	✓	–	–	Mix	Proactive
S4 [31] Wang_2013	–	Game theory & Stochastic	✓	✓	–	ADSGN	Quantitative	Proactive
S5 [32] Abraham_2014	–	Absorbing Markov chains & Attack graph	–	✓	–	–	Quantitative	Predictive
S6 [34] Ahmed_2014	–	Role-based access control (RBAC)	✓	–	–	SREBP	–	Proactive
S7 [33] Brewer_2014	–	Multi-dimensional behavioural analytics	✓	–	–	–	Mix	Proactive & Predictive
S8 [35] Li_2014	✓	Three-layer conceptual model	✓	–	–	–	–	Proactive
S9 [36] Rieke_2014	–	Model-based	–	✓	–	–	Qualitative	Predictive
S10 [91] Xin_2014	–	STRIDE threat model & Threat tree analysis	✓	✓	–	–	Qualitative	Proactive
S11 [98] Abraham_2015	✓	Attack graph & Stochastic modelling	–	✓	–	Non-homogeneous Markov Model	Quantitative	Predictive
S12 [87] Cai_2015	✓	Analytic Hierarchy Process (AHP)	–	✓	–	IBN	Mix	Proactive
S13 [53] Hussein_2015	✓	Virtualised honeypot & Covariance matrix	✓	–	–	–	Quantitative	Proactive & Reactive
S14 [83] Rieke_2014	–	Compliance monitoring & Model-based behavior prediction	–	✓	–	PSA@R	Qualitative	Predictive
S15 [61] Stepanova_2015	✓	Ontology-based automated penetration testing	✓	–	✓	–	Mix	Proactive
S16 [82] Valja_2015	–	Attack graph-based	–	✓	–	Extension of P^{2}CySeMoL	Quantitative	Proactive
S17 [85] Alsaleh_2016	✓	Extensible Configuration Checklist Description Format (XCCDF) & vulnerability scoring systems	–	✓	–	–	Quantitative	Proactive
S18 [71] Baluda_2016	✓	Grubbs' test, Support Vector Machine & Automata-based behavioral modeling	–	–	✓	EMMA	Quantitative	Detective
S19 [88] Jenab_2016	–	Flow-graph concept & Markovian method	–	✓	–	–	Quantitative	Detective & Predictive
S20 [99] Kim_2016	✓	Problem domain ontology	✓	–	–	–	–	Proactive
S21 [62] Kotenko_2016	–	Attack graph & Security metric calculation	–	–	–	–	Quantitative	–
S22 [90] Naik_2016	–	Computational Intelligence, Windows batch programming & R language	✓	–	–	–	Quantitative	Predictive
S23 [54] Niu_2016	✓	Collecting common security problems & Building a knowledge base	–	✓	–	–	Qualitative	Proactive

Table 4. *Cont.*

Study	Framework, Platform, Prototype	Analysis Techniques	Method	Model	Tool	Name	Type of Analysis	Strategy
S24 [100] Ou_2016	✓	Graph generation algorithms & Customized reasoning algorithms	–	✓	–	–	Quantitative	Predictive
S25 [89] Valja_2016	–	Graph-based attack & Enterprise architecture language	✓	–	–	CySeMoL-ArchiMate	Quantitative	Proactive
S26 [94] Buyukkayhan_2017	–	Endpoint monitoring and clustering & Outlier detection	✓	–	–	–	Quantitative	Detective & Proactive
S27 [96] Kato_2017	–	Attack tree	✓	–	–	–	Quantitative	Proactive
S28 [70] Lagerstrom_2017	–	Threat modeling, domain-specific language (DSL) & Reinforcement learning	✓	–	✓	–	–	Proactive
S29 [95] Nguyen_2017		Uncertain graphs	✓	–	–	–	Quantitative	Proactive
S30 [47] Sapegin_2017	✓	In-memory data storage, misuse detection, query-based analytics, and anomaly detection	–	–	–	REAMS	Quantitative	–
S31 [55] Zhu_2017	✓	Behaviour path restoration	✓	–	–	–	Mix	Detective & Proactive
S32 [45] Cinque_2018	–	Topic-modeling technique, Latent Dirichlet Allocation (LDA)	✓	–	–	–	Mix	Detective
S33 [101] Sion_2018	✓	Threat modeling, risk analysis, & Design decisions	✓	–	–	TMaRA	Mix	Proactive & Predictive
S34 [56] Win_2018	✓	Graph-based event correlation & Logistic regression	✓	–	–	BDSA	Quantitative	Proactive & Detective
S35 [102] Wu_2018	–	OpenVAS, Ontology- & Graph-based approach	✓	–	–	–	Qualitative	Proactive & Detective
S36 [63] Lai_2019	–	Self-organizing Maps, Fuzzy c-means & t-SNE algorithms	✓	✓	–	–	Quantitative	Detective
S37 [73] Padmanaban_2019	–	Probabilistic arithmetic automata & SVM	–	✓	–	–	Quantitative	Detective
S38 [60] Sharma_2019	✓	Hive queries, k-algorithm & SVM	–	–	–	ANSA	Quantitative	Detective
S39 [72] Ahmed_2020	✓	Apache spark framework & Customized machine learning	–	–	–	SAD-F	Quantitative	Proactive & Detective
S40 [52] Alavizadeh_2020	✓	Virtual Machine Live Migration (VM-LM)	–	–	–	–	Quantitative	Proactive
S41 [77] Chowdhary_2020	✓	Deep-Q Network and domain-specific transition matrix & Attack graph	–	–	–	ASAP	Mix	Proactive
S42 [57] Elsayed_2020	✓	Monitoring systems with graph analytics & Graph convolutional neural network (GCN)	–	–	–	PredictDeep	Quantitative	Detective & Predictive

Table 4. *Cont.*

Study	Framework, Platform, Prototype	Analysis Techniques	Method	Model	Tool	Name	Type of Analysis	Strategy
S43 [93] Ivanov_2020	–	Attack graphs & Calculation of security indicators	✓	–	–	–	Quantitative	Proactive & Detective
S44 [84] Nashivochnikov_2020	✓	Data analysis	–	–	–	–	Quantitative	Proactive, Detective & Predictive
S45 [78] Sundararaj_2020	–	Process mining & Natural language processing	✓	–	–	–	Mix	Detective
S46 [64] Taylor_2020	–	Data representation	–	–	✓	SysFlow	Mix	Detective
S47 [65] Wu_2020	–	Spatio-temporal characteristics	–	✓	–	–	Quantitative	Detective & Predictive
S48 [92] Zhang_2020	–	Attack graph-based & Graph database	✓	–	–	–	Quantitative	Proactive
S49 [79] Aquino_2021	✓	Processing historical behavior of attacks	✓	–	–	–	Mix	Predictive
S50 [58] Empl_2021	✓	Threat modeling and complex event processing	–	–	–	–	–	Detective, Proactive & Predictive
S51 [86] Kumar_2021	✓	Stochastic timed automata and statistical model-checking	–	✓	–	ECKC	Quantitative	Proactive
S52 [46] Rosado_2021	–	MARISMA methodology & eMARISMA tool	✓	–	✓	MARISMA-BiDa	Mix	Proactive
S53 [74] Vassilev_2021	✓	Ontology & Knowledge graphs	–	–	–	–	Qualitative	All
S54 [80] Chen_2022	–	Word2Vec, N-Gram model	✓	✓	–	–	Mix	Proactive
S55 [66] Chun_2022	–	Behaviour-based intelligence	✓	–	–	–	Quantitative	Detective, Reactive & Predictive
S56 [75] Ndichu_2022	✓	Online supervised learning	–	–	–	–	Quantitative	Detective & Predictive
S57 [97] Sonmez_2022	✓	MITRE ATT&CK framework, CAPEC, CWE	–	–	✓	Attack Dynamics	Quantitative	Detective & Proactive
S58 [48] Zou_2022	–	AISC graph, two-layer MLSD graph	✓	–	ML-SSA	–	Quantitative	Proactive
S59 [76] Efiong_2023	–	Machine learning	–	✓	–	–	Quantitative	Detective & Predictive
S60 [59] Vassilev_2023	✓	Threat intelligence	–	–	–	–	Mix	Detective
A1 [67] Early_2015	–	Data analytics	✓	–	–	–	Quantitative	Proactive & Predictive
A2 [37] Puri_2015	–	Graph analytics & Data mining	✓	–	–	–	Quantitative	Detective & Predictive
A3 [38] Li_2016	✓	Behaviour profiling & Statistical analysis	–	–	–	–	Quantitative	Proactive & Predictive
A4 [49] Ulmer_2018	✓	Visualization and clustering & User-centered design	–	–	✓	–	Mix	Detective & Predictive
A5 [68] Chernova_2019	✓	Correlation analysis	–	–	–	–	Quantitative	Detective, Reactive & Proactive

Observation 5 (Ob5): Predominance of Machine Learning and Graph-Based Approaches Amidst a Diverse Range of Analysis Techniques

Our review reveals the application of a diverse array of processing and analysis techniques. While multiple methodologies are utilized, there is a clear gravitation towards machine learning and computational intelligence (MLCI) and graph-based approaches (GBAs). This trend underscores the industry's response to escalating cyber threat complexity, demanding data-intensive, interconnected, and intelligent analytical methods. Other specialized techniques, including Behavioral Analysis and Profiling (BAP), various Modeling Techniques (MTs), and Ontologies and Knowledge Graphs (OKGs), also play crucial, often complementary, roles. Foundational Data Management and Representation (DMR) techniques further underpin the efficacy of these analytical methods.

The primary categories of analysis techniques identified are discussed below, highlighting their prevalence, core concepts, implications, and connection to broader technological trends.

- **Machine Learning and Computational Intelligence (MLCI):** This was the most prominent category of analytical techniques identified, being central to the methodologies of 12 reviewed studies [56,57,60,63,71–73,75–77,80,90].
  - **Elaboration and Evidence:** MLCI, as presented in the literature, encompasses a range of computational models, statistical analysis methods, and machine learning algorithms applied to security data for tasks such as threat detection, classification, and predictive decision making. Examples from the reviewed studies include the application of Support Vector Machines (SVMs) for intrusion detection and malware classification, aiming to distinguish malicious from benign activities [60,71]; the use of Deep-Q Networks (DQNs), which combine Q-learning with deep learning, for optimizing incident response strategies [77]; the deployment of Latent Dirichlet Allocation (LDA) and N-Gram models for text-based anomaly detection and deriving threat intelligence from unstructured log data [45,80]; and the utilization of ensemble learning methods like boosting to improve predictive accuracy for threat identification [76]. It is important to note that while these studies report varying degrees of success, their practical validity and reliability in broader enterprise contexts often depend on the specific datasets used for training/testing and the experimental conditions, necessitating careful evaluation before widespread real-world deployment.
  - **Analysis:** The observed dominance of MLCI in the reviewed literature stems from its inherent capabilities to process vast and complex security data volumes, automatically learn intricate patterns indicative of known and potentially unknown threats, detect subtle anomalies that might evade traditional rule-based systems, and make predictions about future security events. These capabilities can translate into significant practical benefits for enterprises, such as enhanced efficiency in security operations through automation, improved detection rates for novel and evasive threats, and better prioritization of alerts. However, the adoption and operationalization of MLCI in enterprise security are fraught with substantial practical challenges and limitations:
    - A **critical dependency on large volumes of high-quality, representative training data** is a major operational limitation. Enterprises often struggle with the practicalities of collecting, cleaning, labeling (especially for supervised learning), and maintaining such datasets. Biased, incomplete, or outdated training data can lead to poorly performing models, increased false positives/negatives, and even discriminatory or unfair outcomes in real-world security applications (e.g., in user behavior analytics).

        - The **susceptibility of ML models to adversarial attacks**—where malicious actors intentionally craft inputs to evade detection (evasion attacks) or manipulate training data to compromise model integrity (poisoning attacks)—is a severe real-world limitation. This means the ML systems themselves can become an attack surface, requiring dedicated defensive strategies and robust validation, which adds to their operational complexity.
        - The **need for specialized data science and cybersecurity expertise** to develop, deploy, manage, and interpret MLCI solutions creates a significant skills gap. Practically, many organizations find it costly and difficult to acquire and retain talent with this hybrid skillset, potentially leading to over-reliance on third-party solutions (which may lack transparency) or an inability to fully leverage the potential of ML technologies.
    - **Trends and Challenges:** Key technological trends aim to address some of these limitations. There is increasing adoption of deep learning for more complex, high-dimensional data, though this often intensifies the data and explainability challenges. Research into Explainable AI (XAI) is critical for building trust and making ML outputs more transparent and actionable for security practitioners. The development of automated ML (AutoML) tools seeks to lower the technical barrier for model development, potentially making ML more accessible to enterprises with limited in-house data science capabilities; however, their practical limitation lies in potentially producing less optimized or generalizable models for highly specific cybersecurity tasks compared to expert-driven approaches. Ongoing real-world challenges that significantly impact the effectiveness and reliability of MLCI in enterprises include
        - **Managing data and concept drift:** Security threats and enterprise environments constantly evolve, causing ML models trained on historical data to degrade in performance over time. Practically, this necessitates continuous monitoring, frequent retraining, and robust MLOps (machine learning operations) practices, which represent a significant and ongoing operational overhead.
        - **Preventing model poisoning and ensuring model robustness:** Protecting the integrity of training data and developing models resilient to adversarial manipulation are crucial for maintaining the reliability of ML-based security defenses.
        - **Reducing alert fatigue from false positives:** Despite the sophistication of ML, poorly tuned models or those affected by data drift can still generate a high volume of false alarms. This remains a persistent practical issue, potentially overwhelming security teams and leading to genuine threats being overlooked if not carefully managed through continuous model evaluation and threshold tuning.
        - **Bridging the cybersecurity–data science skills gap:** This remains a fundamental constraint limiting the widespread and effective adoption and innovative application of MLCI in many enterprise security programs.
- **Graph-Based Approaches:** These techniques were significantly featured in 9 studies [32,48,62,77,82,89,92,93,98].
    - **Elaboration and Evidence:** GBAs leverage graph theory to construct models of enterprise environments, representing entities (e.g., network assets, users, applications, vulnerabilities) as nodes and their relationships (e.g., connectivity, access rights, dependencies) as edges. This structure facilitates the analysis of complex attack pathways, systemic dependencies, and potential incident propa-

gation routes. Examples from the reviewed literature include the development and application of attack graphs to model potential multi-step attack scenarios and identify critical choke points [82,92]; the combination of Markov chains with GBAs to enable predictive modeling of attack progression and likelihood [32]; and the design of specialized graph structures like the adversarial influence and susceptibility graphs (AISC graphs) for conducting comprehensive defense posture and vulnerability analysis [48]. While these studies demonstrate the utility of GBA for specific security analyses, it is important to recognize that the practical validity and reliability of such models in real-world enterprise settings are heavily contingent on the accuracy and completeness of the data used to construct the graph and the underlying assumptions about entity interactions. Translating the full, dynamic complexity of large-scale enterprise networks into an accurate and maintainable graph model remains a significant endeavor.

- **Analysis:** GBAs offer a powerful visual and analytical paradigm that can significantly enhance an enterprise's understanding of complex interdependencies and systemic risks. Practically, they are invaluable for attack path analysis, enabling security teams to visualize how attackers might traverse the network to reach critical assets, and for vulnerability management, by helping to prioritize remediation efforts based on exploitability and potential impact. This visual and relational context can lead to more informed and proactive security decision making. However, the practical application of GBA in enterprises faces notable limitations and challenges.
  * **Complexity of Construction and Maintenance:** Constructing and, more critically, maintaining accurate, large-scale security graphs is a complex and often computationally intensive task. The initial data collection, entity discovery, relationship mapping, and vulnerability attribution can require significant effort and integration with multiple data sources. In highly dynamic enterprise environments where assets, configurations, and software versions change frequently, keeping the graph model current is a continuous operational challenge. An outdated graph quickly loses its analytical value and can lead to misleading conclusions.
  * **Scalability for Large Enterprises:** As enterprise networks grow, the size and complexity of the corresponding security graphs can become immense. Scalability, in terms of graph storage, processing power required for complex queries (e.g., pathfinding, centrality analysis), and timely updates, can be a significant practical concern. For very large organizations, this may necessitate investment in specialized (and potentially expensive) graph database technologies or distributed processing frameworks.
  * **Data Quality and Completeness Dependencies:** The utility of any GBA is fundamentally dependent on the quality, accuracy, and completeness of the input data used to build the graph. Incomplete asset inventories, inaccurate vulnerability information, or missing relationship data can lead to an incomplete or misleading representation of the actual attack surface, thereby limiting the real-world reliability of the analysis.
- **Trends and Challenges:** Current trends in GBA for security include the integration of GBA with machine learning (ML) techniques for dynamic graph analysis, aiming to automatically detect anomalies or predict changes within graph structures that might indicate emerging threats (as seen in approaches like [77]). This has the practical implication of potentially making graphs more adaptive and responsive to evolving conditions, but also introduces the inherent complexities

of ML (e.g., data requirements and interpretability). Another trend is the development of graph databases specifically optimized for handling the scale and query patterns of security-related data, which could alleviate some scalability concerns. Despite these advancements, significant real-world challenges persist.

- **Achieving Real-Time Graph Analytics at Enterprise Scale:** Many critical security use cases, such as detecting an ongoing attack as it propagates or assessing the immediate impact of a new high-severity vulnerability, require real-time or near real-time analytical capabilities. The computational cost of continuously updating and performing complex queries on massive graphs in real time remains a major technical and practical hurdle for most enterprises.
- **Standardizing Graph Modeling Approaches for Security:** The lack of widely adopted, standardized schemas, ontologies, or modeling languages for representing security-relevant entities and relationships in graphs makes it difficult to share graph models, compare results effectively across different GBA tools or research studies, and seamlessly integrate GBA with other security information systems. Practically, this fragmentation hinders interoperability and the development of a mature ecosystem of reusable GBA components and benchmarks.

- **Behavioral Analysis and Profiling:** This category of analytical techniques was prominent in six of the reviewed studies [33,47,55,66,79,94].
    - **Elaboration and Evidence:** BAP focuses on understanding, modeling, and ultimately predicting the actions and patterns of behavior exhibited by users, systems, network entities, and potential attackers. The reviewed literature showcases techniques such as Multi-Dimensional Behavioral Analytics, which considers diverse aspects like login frequency, resource access patterns, and data transfer volumes to build comprehensive profiles [33]; the analysis of historical attack behaviors and attacker Tactics, Techniques, and Procedures to predict future threat vectors or campaign characteristics [79]; and the application of behavior-based intelligence, which models past legitimate behavior to identify statistically significant anomalies potentially indicative of compromise or insider activity [66]. The practical reliability of BAP techniques often hinges on the quality and granularity of the data sources used for profiling (e.g., endpoint logs, network traffic, application logs), the sophistication of the anomaly detection algorithms employed, and, critically, the stability and predictability of what constitutes “normal” behavior within the monitored environment.
    - **Analysis:** The increasing adoption of BAP in enterprises reflects a strategic shift towards detecting threats, such as insider threats and APTs, that are specifically designed to evade traditional signature-based defenses, often by mimicking legitimate user or system behavior. BAP enables more user-centric and context-aware security monitoring. This can lead to more accurate threat identification by tailoring detection to individual user roles, responsibilities, and typical activity patterns, thereby potentially reducing the high volume of false positives often associated with generic security rules. It also provides rich contextual data crucial for forensic investigations. However, the implementation of BAP is accompanied by significant practical limitations.
        - **Establishing and Maintaining Accurate Behavioral Baselines:** This is arguably the most substantial challenge. In large, diverse, and dynamic enterprise environments with evolving job roles, frequent personnel changes, and new application deployments, “normal” behavior is a constantly moving

target. The initial baselining period required to learn these norms can be lengthy and resource-intensive. More importantly, maintaining the accuracy of these baselines necessitates continuous learning, adaptation, and periodic re-evaluation, which is computationally demanding and operationally complex. Failure to do so in practice leads to degraded model performance, resulting in either excessive false positive alerts or, conversely, missed detections of genuine threats.

    - **Data Volume and Granularity Requirements:** Effective BAP often requires the collection and analysis of vast quantities of granular data from multiple sources. This presents challenges related to data storage, processing power, and the potential performance impact on monitored systems or networks.
    - **Privacy and Ethical Considerations:** The detailed collection and analysis of user and system behavior data inherently raise significant privacy concerns. Enterprises must practically navigate complex legal frameworks (e.g., GDPR, CCPA, and local labor laws concerning employee monitoring) and ethical considerations. Implementing BAP necessitates the development of clear governance policies, ensuring transparency with users regarding what data is collected and for what purpose (where appropriate and legally required), employing robust data anonymization or pseudonymization techniques when feasible, and implementing stringent access controls and audit trails to prevent misuse of sensitive behavioral data. These considerations can significantly influence the scope and methodology of BAP deployment.

  - **Trends and Challenges:** BAP is a core technological component of modern UEBA platforms and is increasingly being integrated with Identity and Access Management (IAM) systems. This integration has the practical implication of enabling more dynamic, risk-based authentication and adaptive access controls (e.g., requiring step-up authentication or restricting access if a user's behavior suddenly deviates significantly from their established profile). Despite these advancements, several persistent real-world challenges limit the universal effectiveness and ease of BAP deployment:

    - **Minimizing False Positives and Alert Fatigue:** While BAP aims for higher accuracy, poorly tuned systems, inadequate baselining, or a failure to account for legitimate behavioral variances can still generate a high number of false positive alerts. This remains a critical operational challenge, as it can overwhelm SOC analysts, leading to alert fatigue, a loss of trust in the BAP system, and ultimately, the risk of genuine threats being overlooked.
    - **Adapting Baselines to Dynamic Organizational Contexts:** As noted, effectively and efficiently adapting behavioral baselines to reflect legitimate changes in user roles, responsibilities, business processes, and IT systems is an ongoing practical and technical hurdle. This requires sophisticated adaptive algorithms and potentially significant computational resources for continuous model retraining and validation.
    - **Ethical Implications of Continuous Monitoring and Potential for Misinterpretation:** Beyond legal privacy compliance, the continuous monitoring inherent in BAP raises broader ethical questions about workplace surveillance and the potential for misinterpretation of automatically flagged "anomalies", which could unfairly impact individuals. Enterprises must carefully balance legitimate security needs with their ethical obligations to employees, ensuring fairness, transparency, and mechanisms for redress. This often

necessitates clear communication strategies and robust oversight of BAP system outputs and subsequent actions.

- **Modeling Techniques:** Various modeling techniques were explored in six of the reviewed studies [36,42,58,91,97,101].
    - **Elaboration and Evidence:** This category encompasses conceptual or mathematical representations of systems, threats, or security processes, designed to facilitate understanding, risk assessment, and prediction. Examples from the literature include general threat modeling methodologies, the application of the STRIDE threat model (STRIDE is a model of threats developed at Microsoft, used to identify and categorize potential threats to a system. See https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats (accessed on 29 April 2025)), leveraging the MITRE ATT&CK framework for describing adversary tactics and techniques, and model-based behavior prediction.
    - **Analysis:** MT provides structured methodologies that can aid enterprises in proactively identifying system vulnerabilities and understanding potential attack vectors. Frameworks like MITRE ATT&CK offer a valuable common lexicon, improving communication within the cybersecurity community and enabling more consistent threat intelligence sharing. The primary practical implication is a more systematic and potentially proactive approach to risk management. However, a key limitation is that all models are abstractions and may not capture the full complexity or dynamic nature of real-world enterprise environments. This necessitates continuous, resource-intensive updating to maintain their relevance and accuracy, failing which they risk providing a false sense of security or misdirecting defensive efforts.
    - **Trends and Challenges:** A strong trend is the increasing operationalization of the MITRE ATT&CK framework within security operations for detection engineering, threat hunting, and incident response. Automated tools are also more frequently used to support the threat modeling process, offering efficiency gains. The primary challenges lie in keeping these models continuously updated in parallel with the rapidly evolving threat landscape and the organization's own IT changes. Furthermore, effectively integrating model outputs into the broader security analytics lifecycle (e.g., linking threat model findings to SIEM alert correlation or SOAR playbook triggers) remains an issue requiring careful planning and technical integration.
- **Ontologies and Knowledge Graphs:** These methods, employing structured knowledge frameworks, were discussed in four of the reviewed studies [61,74,99,102].
    - **Elaboration and Evidence:** OKG techniques utilize formal, structured representations of knowledge—defining entities, their properties, and the relationships between them—to enhance security analysis and reasoning. Examples include Ontology-Based Automated Penetration Testing, where ontologies guide the selection and application of testing tools [61], and the use of knowledge graphs to map security-relevant entities (e.g., assets, vulnerabilities, threat actors, TTPs) and their interconnections for advanced threat detection and incident response [74]. The effectiveness of OKG-driven security analytics is highly dependent on the quality, completeness, and consistency of the underlying ontology or knowledge graph, as well as the sophistication of the reasoning engines applied to them.
    - **Analysis:** OKGs offer the potential for richer semantic understanding of complex security data, improved automated reasoning capabilities, and enhanced automation of security tasks. They can help to integrate diverse data sources into

a unified model and provide a more holistic, context-aware view of the enterprise security landscape. However, the limitations are the significant complexity and substantial effort involved in developing, meticulously maintaining, and continuously populating comprehensive security ontologies and knowledge graphs. This requires specialized expertise (e.g., ontologists, knowledge engineers, cybersecurity domain experts), considerable time investment, and robust governance processes, making the ROI difficult to justify for some organizations.

  - **Trends and Challenges:** Emerging trends involve leveraging natural language processing (NLP) and large language models (LLMs) to assist in the semi-automated construction and querying of security knowledge graphs, potentially reducing the manual effort involved. Efforts towards creating standardized security ontologies also aim to improve interoperability and reusability. Despite these trends, significant challenges with interoperability between different OKG systems and ensuring the scalability of these complex structures for large, dynamic enterprise environments persist, limiting broader adoption.

- **Foundational Data Management and Representation Techniques:** While not strictly analysis techniques themselves, effective DMR practices, highlighted in studies such as [41,47,64] (three studies focusing on these aspects), are crucial enablers for any advanced security analytics.
  - **Elaboration and Evidence:** This category includes critical infrastructure components such as In-Memory Data Management for accelerated data processing and enabling real-time analytics crucial for timely incident response [41,47], as well as effective data representation techniques, including advanced visualization methods, for formatting and presenting complex security data in ways that aid human interpretation and pattern identification [64]. The choice of DMR techniques involves trade-offs regarding cost, performance, scalability, and implementation complexity.
  - **Analysis:** Efficient DMR is fundamental to the overall performance, reliability, and utility of any enterprise security analytics system. Practically, slow data access, poor data quality, or ineffective visualization can severely hamper threat detection, incident investigation, and response capabilities, regardless of the sophistication of the analytical algorithms employed. The clear implication is that strategic investment in robust data infrastructure (including storage, processing, and integration capabilities) and user-centric visualization tools is as critical to successful security analytics as the analytical models themselves. A key limitation for some organizations can be the cost and complexity associated with implementing and maintaining state-of-the-art DMR infrastructure and acquiring the necessary data engineering skills.
  - **Trends and Challenges:** Current trends include the increasing adoption of big data platforms (e.g., data lakes, data lakehouses) specifically for security data to handle volume and variety, alongside advanced interactive visualization tools designed to make complex data more accessible to analysts. Persistent challenges involve managing the sheer scale of security data generated daily, ensuring consistent data quality and governance across diverse sources, and effectively presenting complex analytical outputs in an intuitive, actionable, and timely manner for often overburdened security analysts.

In summary, the landscape of security analytics techniques is dominated by MLCI and GBA, driven by their power in handling complex, large-scale data and modeling intricate relationships inherent in modern cyber threats. The increasing prominence of BAP highlights a shift towards understanding user and entity behaviors, while MT and

OKG provide structured and semantic depth. These trends suggest a move towards more intelligent, interconnected, and context-aware security analytics. Future advancements will likely focus on hybrid approaches, combining the strengths of these diverse techniques—for instance, MLCI with BAP for nuanced anomaly detection or GBA with OKG for comprehensive, semantically enriched security posture analysis—to build more resilient and adaptive enterprise defense mechanisms. The continuous evolution of these techniques is essential to keep pace with the ever-advancing capabilities of cyber adversaries.

Observation 6 (Ob6): The Complementary Roles of Quantitative and Qualitative Analysis, with Opportunities for Increased Mixed-Methods Integration

Our review indicates that enterprise security analytics research utilizes both quantitative and qualitative methodologies to assess and understand cyber threats, vulnerabilities, and incidents [103]. Quantitative analysis, focusing on numerical data and statistical evaluation, appears frequently for measuring security events and control effectiveness. Qualitative analysis provides essential contextual understanding and insight into complex, non-numerical aspects. While both are valued, the explicit adoption of mixed-methods approaches, integrating the strengths of both, was less commonly highlighted in the reviewed studies, suggesting a potential avenue for developing more holistic and robust research findings in the field.

- **Quantitative Analysis in Security Analytics:**
    - **Elaboration and Evidence:** This approach centers on the use of numerical data, statistical methods [86], and computational techniques to measure [57], quantify, and objectively evaluate security-related phenomena [92]. It often involves analyzing metrics such as the frequency and impact of security incidents [32], the financial cost of breaches, or the performance of security controls [38]. For instance, studies have employed Game Theory and stochastic modeling to quantify outcomes of security strategies [31], or computational intelligence and programming languages like R to develop a numerical understanding of threats [90].
    - **Analysis:** Quantitative analysis is vital for enterprises to prioritize risks, justify security investments, allocate resources effectively, and make data-driven operational decisions. Its strengths lie in its objectivity, potential for automation, and the comparability of results. However, its effectiveness can be limited by the need for large volumes of high-quality data and an inability to fully capture nuanced, unmeasurable, or emergent aspects of security concerns, such as attacker intent or the subtleties of human behavior [90]. An over-reliance on purely quantitative metrics can sometimes lead to a narrow understanding of a complex and dynamic threat landscape.
    - **Trends and Challenges:** The trend towards Big Data analytics and AI/ML (as discussed in Observation 5) heavily fuels quantitative security analysis by enabling the processing of vast datasets for anomaly detection, predictive risk scoring, and automated response. Challenges include ensuring the quality and integrity of input data for these models, avoiding “metric fixation”, managing alert fatigue from purely quantitative systems, and developing quantitative models that are truly representative of real-world security effectiveness.
- **Qualitative Analysis in Security Analytics:**
    - **Elaboration and Evidence:** Qualitative analysis emphasizes subjective information, in-depth contextual understanding, and expert judgment [103]. It involves gathering and interpreting non-numerical data such as textual descriptions from incident reports, interview data with security personnel, observational studies of security operations [102], or detailed case studies. Examples include model-based

qualitative analysis to understand threat intricacies [36] and the use of threat modeling frameworks like STRIDE combined with threat tree analysis to explore vulnerabilities [91].

  - **Analysis:** This approach is invaluable for uncovering hidden patterns, understanding the "why" behind security events, exploring behavioral indicators, identifying emerging threats not yet quantifiable [74], and assessing the usability and practical effectiveness of security processes. It provides richness and depth that quantitative data alone cannot. However, qualitative findings can be subject to researcher interpretation and potential biases, may be more time-consuming to collect and analyze, and are often less generalizable than quantitative results. For enterprises, qualitative insights are crucial for developing targeted training, refining incident response plans based on real-world scenarios, and understanding the socio-technical aspects of security.
  - **Trends and Challenges:** Trends include the increasing use of NLP to extract insights from unstructured qualitative data (e.g., threat intelligence reports and user feedback). Qualitative methods are also central to usability studies for security tools and understanding human factors in cybersecurity. Challenges involve the difficulty of scaling qualitative analysis, integrating its findings with quantitative data systems in a meaningful way, and ensuring rigor in qualitative data collection and interpretation.

- **Mixed-Methods Analysis in Security Analytics:**
  - **Elaboration and Evidence:** A mixed-methods approach strategically combines quantitative and qualitative techniques to leverage the strengths of both, aiming for a more comprehensive and nuanced understanding. The reviewed literature explicitly highlighted several studies adopting this integrated methodology (see Table 4) to gain a more holistic perspective on their research questions.
  - **Analysis:** Mixed-methods research can provide stronger validation of findings through triangulation, offer deeper insights by explaining quantitative results with qualitative data (or vice-versa), and lead to more robust and actionable conclusions. The relatively limited explicit mention of mixed-methods studies in the enterprise security analytics literature could indicate a methodological gap or an area wherein research practices could be more explicitly articulated. Encouraging more mixed-methods research could significantly enhance the depth, relevance, and practical applicability of security analytics studies. For enterprises, this translates to the ability to combine 'what' is happening (from quantitative data) with 'why' it's happening (from qualitative insights) for more effective security strategies.
  - **Trends and Challenges:** The increasing complexity of cybersecurity problems inherently calls for multifaceted analytical approaches. The development of XAI can be seen as a move towards bridging quantitative model outputs with qualitative human-understandable explanations, embodying a mixed-methods spirit. The primary challenge is the increased complexity in research design, data collection, analysis, and interpretation, requiring researchers proficient in both paradigms.

In conclusion, Observation 6 highlights that while both quantitative and qualitative analyses provide distinct and valuable perspectives in enterprise security analytics, a more deliberate and widespread adoption of mixed-methods approaches could foster deeper insights and more comprehensive solutions. Enterprises stand to benefit most when they can leverage the precision of quantitative data alongside the contextual depth of qualitative understanding to inform their security posture management and decision-making processes.

Observation 7 (Ob7): Enterprise Security Analytics Strategies are Evolving Towards Proactive and Predictive Postures

Our systematic review reveals a clear evolution in strategic approaches to enterprise security analytics. While all identified strategies—detective, reactive, proactive, and predictive—serve distinct purposes, the literature indicates a significant trend moving beyond primarily reactive tactics towards more forward-thinking, anticipatory measures. This shift is underscored by the prevalence of studies focusing on proactive (40 studies) and predictive (22 studies) strategies, although detective approaches (27 studies) remain a cornerstone. Reactive strategies (5 studies) are recognized as necessary but are less emphasized in current research on analytics-driven security.

- **Elaboration and Evidence of Strategic Approaches:**
  - **Reactive Strategy:** This traditional strategy involves responding to security incidents after they have occurred, with the primary goals of damage mitigation and rapid recovery. Activities include closing exploited vulnerabilities, eradicating malware, and restoring systems. While essential for incident management, this strategy's inherent nature signifies a prior failure in prevention or detection. In our reviewed literature, the number of studies that concentrated primarily on developing or applying analytical techniques specifically for this reactive phase was comparatively low (five studies—[41,53,66,68,74]). This observation suggests that while analytics for reactive measures are explored, the main thrust of research in security analytics tends to favor earlier intervention points—such as proactive, predictive, and detective capabilities—aligning with the broader cybersecurity goal of minimizing threat impact before extensive reaction is needed.
  - **Detective Strategy:** This strategy is critically focused on the timely identification of security incidents either as they are actively unfolding or very shortly after their occurrence. The primary objective is to minimize the dwelling time of threats within the enterprise environment. It relies on a foundation of robust systems for continuous monitoring, comprehensive logging from diverse sources (such as network devices, servers, endpoints, and applications) and sophisticated alerting mechanisms. These components work in concert to flag anomalous patterns, suspicious activities, or known indicators of compromise (IoCs) that could signal an ongoing or imminent attack [45,60,63,73,78]. Key technologies often underpinning this strategy include SIEM platforms, Intrusion Detection/Prevention Systems (IDS/IPS), and EDR solutions. Security analytics plays a pivotal role here by automating the analysis of vast data volumes, correlating disparate events to uncover complex attack chains, and employing techniques ranging from signature-based detection and rule-based correlation to advanced statistical anomaly detection and machine learning models for identifying novel or evasive threats. With 27 studies in our review emphasizing this approach, its importance in providing crucial, timely awareness for immediate and effective incident response is well established, forming an indispensable layer in a defense-in-depth security structure.

    - **Proactive Strategy:** This strategy embodies a forward-looking security philosophy focused on taking preemptive measures to prevent cyber threats from materializing, thereby reducing the overall attack surface and strengthening defenses before an attack is attempted. It moves beyond merely reacting to incidents by systematically identifying and mitigating vulnerabilities and fortifying security postures. Core activities include comprehensive and continuous risk assessments, including threat modeling to anticipate potential attack vectors; regular security audits to ensure compliance and identify weaknesses; diligent system hardening (e.g., removing unnecessary services, configuring secure baselines, implementing robust access controls); timely and prioritized patch management to address known vulnerabilities; and engaging security awareness training, often incorporating phishing simulations, to mitigate human error. Furthermore, developing and testing robust incident response plans is a key proactive step, ensuring preparedness to minimize damage should an incident occur despite preventative efforts [46,48,80,86,92]. Analytics can support proactive strategies by, for instance, prioritizing vulnerability remediation based on exploit likelihood and asset criticality, or by identifying anomalous configurations that deviate from security best practices. As the most frequently emphasized strategy in the reviewed literature (40 studies), it highlights a clear strategic preference within the field for preventing incidents, an approach that is demonstrably more cost-effective and less disruptive to enterprise operations than reacting to successful breaches.
    - **Predictive Strategy:** Representing the most advanced and aspirational security posture, this strategy aims to forecast potential future threats and anticipate attack campaigns, often before they are widely known or actively launched. It leverages sophisticated analytical techniques, primarily ML and AI, to analyze vast datasets comprising observed patterns from historical incidents, real-time security telemetry, global threat intelligence feeds, dark web monitoring, and even geopolitical or sector-specific risk factors. Unlike proactive strategies that harden defenses against known vulnerability classes or general threats, predictive analytics seeks to identify the likelihood of specific future attack types, emerging malicious tools, or targeted campaigns, enabling organizations to adapt their defenses preemptively and in a highly targeted manner [37,67,75,79,84]. The goal is to neutralize threats before they can cause harm by providing early warnings and actionable intelligence. While immensely powerful in concept, this approach faces challenges such as the need for high-quality, voluminous data, the risk of false positives/negatives in predictions, ensuring the explainability of AI-driven insights, and staying ahead in an adversarial landscape where attackers also evolve their tactics. Nevertheless, the significant research attention given to predictive strategies (22 studies) underscores a strong industry-wide aspiration to achieve this forward-looking capability, striving to shift from a reactive or merely preventative stance to one of true cyber foresight.
- **Analysis of the Strategic Shift:** The observed strategic evolution is driven by several factors, including the increasing volume, sophistication, and business impact of cyber threats. Purely reactive approaches are no longer sustainable or cost-effective in the face of advanced persistent threats and rapid exploit development.

  - **Value Proposition:** Proactive and predictive strategies offer the potential to significantly reduce the likelihood and impact of security incidents, thereby enhancing business resilience and trust. Detective capabilities remain critical as a bridge, providing the necessary alerts when preventative measures are bypassed.
  - **Interdependencies:** Effective security relies on a balanced combination of these strategies. For instance, detective mechanisms provide data that can refine proactive controls and train predictive models. A robust proactive posture reduces the burden on detective and reactive systems.
  - **Enterprise Impact:** This strategic shift necessitates changes in organizational culture, processes, and technology adoption. It requires investment in advanced analytical tools (as mentioned in the Ob5 on techniques like MLCI), skilled personnel, and comprehensive threat intelligence. The emphasis on proactive strategies also implies a greater need for thorough risk assessments and preventative maintenance.
  - **Challenges:** While proactive and predictive strategies are aspirational, their implementation faces hurdles. Predictive analytics, for example, demands high-quality data, sophisticated modeling (which can be a "black box"), and carries the risk of false positives or negatives. Measuring the ROI of proactive measures can also be more challenging than quantifying the cost of a prevented incident.

- **Trends and Challenges:**
  - **Enabling Technologies:** The rise of Big Data platforms, advanced AI/ML algorithms (especially deep learning), and cloud computing power are key enablers of more effective detective, proactive, and particularly predictive strategies. SOAR platforms are enhancing detective and reactive capabilities by automating responses. Threat Intelligence Platforms (TIPs) are crucial for informing proactive defenses and predictive models.
  - **Emerging Paradigms:** Concepts like zero-trust architecture embody a proactive stance by default. The push for "security by design" also aligns with proactive thinking.
  - **Persistent Hurdles:** Challenges include managing the vast amounts of data required, addressing the cybersecurity skills gap (especially for data scientists and AI specialists in security), integrating diverse security tools and data sources, ensuring the explainability and trustworthiness of predictive models, and keeping pace with the adversarial use of AI. The cost of implementing and maintaining advanced analytics solutions also remains a significant barrier for some organizations.

In summary, Observation 7 underscores a significant maturation in cybersecurity strategy within enterprises, characterized by a decisive shift from reactive responses towards proactive prevention and predictive foresight. While detective capabilities are indispensable and reactive measures remain a necessary fallback, the clear momentum is towards leveraging advanced analytics to anticipate and neutralize threats earlier in the attack lifecycle. An optimal defense posture for the evolving threat landscape involves an intelligent, adaptive, and balanced integration of all these strategic elements.

The following table (Table 5) summarizes the evaluation methods employed for the security analytic approaches discussed in the reviewed literature, along with the potential security risks these approaches aim to address. It is important to note that some studies were not included in this table if their evaluation methods were not explicitly detailed or were insufficiently clear for categorization. This table provides insights into how the effectiveness and applicability of various security analytics solutions are being assessed in research.

Table 5. Enterprise security analytic evaluation methods.

Study	Evaluation Method				Potential Security Risks
	Experiment /Simulation	Case Study	Real-World Scenario	Comparison with Others	
S1 [41]	✓				–
S2 [42]		✓			–
S3 [43]					Multi-step network intrusions
S4 [31]	✓				Illegal intrusions
S5 [32]	✓	✓			–
S6 [34]		✓	✓	✓	–
S7 [33]					APTs
S8 [35]		✓			–
S9 [36]		✓			Insider attacks; unauthorized access; data leakage
S10 [91]		✓			STRIDE: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Priviledge
S11 [98]	✓	✓			Gaining root access
S12 [87]		✓			–
S13 [53]	✓				Distributed Denial-of-Service
S14 [83]			✓		Administrator password theft; insider attack
S15 [61]					Multistage attacks & APTs
S16 [82]		✓			Unauthorized activity
S18 [71]			✓		Jail-breaking; malicious carrier ID; unusual location
S19 [88]		✓			Internal, external, and accidental threats
S20 [99]		✓	✓		Illegal intrusions
S21 [62]	✓	✓			SQL injection; XSS; DoS attacks
S22 [90]	✓		✓		Port scanning; network scanning; brute-force attacks
S24 [100]		✓	✓	✓	–
S26 [94]	✓		✓		Malware
S29 [95]	✓	✓			Stuxnet worm & phishing campaign
S30 [47]	✓		✓		Brute force; replay attacks; authentication failures; shared access abuse
S31 [55]			✓		Users' abnormal behaviours
S33 [104]				✓	–
S34 [56]	✓			✓	Malware; DDoS
S35 [102]	✓				Multistage & Multihost attack scenarios
S36 [63]		✓			Abnormal access
S37 [73]	✓		✓		XSS; SQLi; CSRF; DDoS
S38 [60]	✓		✓		Service-denial and scan/flood attacks (NULL, SYN, X-MAS)
S39 [72]	✓				DDoS
S40 [52]	✓		✓		Malicious co-resident VMs
S41 [77]	✓	✓			Known APTs & CVEs
S42 [57]	✓				Anomalies
S43 [93]	✓			✓	CVE vulnerabilities
S44 [84]			✓		–
S45 [78]	✓	✓			–
S46 [64]	✓			✓	Sensitive-file interactions; process executions; suspicious traffic
S47 [65]	✓				–
S48 [92]	✓				Multi-step attacks; known CVEs
S49 [79]		✓			Various

Table 5. *Cont.*

Study	Evaluation Method				Potential Security Risks
	Experiment /Simulation	Case Study	Real-World Scenario	Comparison with Others	
S50 [58]					Spoofing; tampering; DoS; privilege elevation
S51 [86]		✓			APTs
S52 [46]		✓			Various
S53 [74]		✓			Spyware; baiting; DDoS; vishing; smishing; hijacking; spam; scareware; rogue ATM infection
S56 [75]	✓		✓	✓	Various
S57 [97]		✓			Known CVEs
S58 [48]		✓			Evasion; poisoning; exploratory & Software attacks
S59 [76]	✓				RTCIA; RSCA; DIA
S60 [59]	✓				Unauthorized intrusions
A1 [67]		✓			Intellectual property theft
A2 [37]			✓		APTs; contextual anomalies
A3 [38]	✓		✓		Malware; APTs; enterprise breaches
A4 [49]			✓		–
A5 [68]	✓				–

4.4. Key Data Sources and Types in Enterprise Security Analytics (RQ4)

Observation 8 (Ob8): Critical Reliance on Diverse and Heterogeneous Data Sources for Comprehensive Security Insight

Enterprise security analytics fundamentally depends on the collection, integration, and analysis of data from a wide spectrum of sources and types, as detailed in the studies summarized in Table 6. This diversity is not incidental but essential for achieving a holistic understanding of an enterprise's security posture, enabling effective threat detection, contextualizing alerts, and supporting informed incident response. The selection and prioritization of these data sources are critical, often dictated by the specific security objectives, operational environment, regulatory landscape, and threat model of a given enterprise. Our analysis categorizes these vital data inputs as follows

- *System Monitoring and Log Data:* This foundational category remains paramount in security analytics, encompassing real-time information and historical logs generated by various IT assets. Examples include application logs, firewall and proxy logs, Intrusion Detection/Prevention System (IDS/IPS) alerts, operating system event data, endpoint activity logs, and server log files (e.g., [37,41,59,64,83,84]). Analyzing these logs provides a granular audit trail crucial for detecting anomalous behaviors, reconstructing attack timelines, conducting forensic investigations, and demonstrating compliance. The sheer volume, velocity, and variety of this data, however, present significant challenges in terms of collection, storage, normalization, and processing, necessitating robust data management and analytics platforms.
- *Network Configuration and Traffic Data:* Data derived from network elements, including traffic logs (e.g., NetFlow, sFlow, PCAPs) and device configuration information, are central to understanding network-based threats (e.g., [49,59,65,75,102]). These sources offer a granular view of the network's architecture, communication patterns, and operational status. Analyzing this data helps to reveal potential vulnerabilities in network design, detect unauthorized access attempts, identify malware propagation, and monitor for unusual data exfiltration. Changes in configuration or anomalous network traffic patterns (like unexpected spikes or communication with known mali-

cious IPs) can serve as early indicators of a security breach. The integrated analysis of network configuration and traffic data significantly enhances an enterprise's capability to anticipate, identify, and react to network-borne threats, though the increasing use of encryption can sometimes limit deep packet inspection capabilities.

- *User and Application Behavior Data:* Understanding user and application activities is increasingly critical, with data collected from identity and access management systems, application interaction logs, mobile application usage, and even physical access systems (e.g., [33,54,55,71,73]). This data provides significant insights into behavior patterns, allowing security analytics, particularly UEBA solutions, to establish baselines of normal activity and identify deviations that could indicate compromised credentials, insider threats, or malicious application behavior. While powerful, the collection and analysis of such data must carefully navigate privacy considerations and the complexity of accurately distinguishing malicious from benign behavioral anomalies.
- *Business and Transactional Data:* Integrating data from core business processes and systems, such as query logs, financial transaction records, and customer relationship management (CRM) data, provides crucial context to security events (e.g., [34,67,74,91]). This category allows security analytics to correlate technical indicators of compromise with potential business impact, aiding in the prioritization of alerts and response efforts. For instance, anomalous access to sensitive customer databases or unusual transaction patterns can be flagged as high-priority security events. The challenge often lies in effectively integrating disparate business systems with security analytics platforms and defining clear correlations between business processes and security telemetry.
- *External Threat Intelligence and Public Datasets:* Leveraging external information sources is vital for enriching internal security data and enhancing proactive and predictive capabilities. This includes curated threat intelligence feeds (providing indicators of compromise, information on threat actors, and attack methodologies), publicly available breach datasets, vulnerability databases, and security scan reports from reputable sources (e.g., [52,60,72,77]). These external inputs are invaluable for benchmarking internal security posture, training machine learning models to recognize emerging threats, and providing early warnings about new attack techniques or campaigns. The effective use of such data depends on its timeliness, reliability, and the ability to operationalize it within the enterprise's security analytics framework.
- *Compliance and Policy Data:* Information related to regulatory compliance mandates, internal security policies, security rules, and configuration standards plays an essential role in governance-focused security analytics (e.g., [38,85,86]). Compliance reports help to identify deviations from required security baselines, informing corrective actions and shaping strategic security investments. Security rules and policy definitions provide a benchmark against which system configurations and user behaviors can be evaluated, enabling the detection of policy violations that could introduce vulnerabilities or elevate risk. Analyzing this data helps enterprises maintain an informed, adaptive, and demonstrable approach to meeting their security and regulatory obligations.

In conclusion, the efficacy of enterprise security analytics is profoundly influenced by the strategic selection, integration, and contextualization of diverse data sources. While individual data types offer specific insights, the trend and recognized best practice involve fusing these heterogeneous datasets to create a richer, more comprehensive understanding of the threat landscape. This holistic approach enables more accurate detection, reduces false positives, and facilitates more effective incident response. However, managing the complexity of data integration, ensuring data quality, and addressing the sheer scale of data remain significant operational challenges for many enterprises.

Table 6. Common sources and types of data for security analytics.

Study	Data Source	Data Type
S1 [41]	System Monitoring Data	Application logs; IDS alerts; firewall logs
S6 [34]	Business Operation Data	Plan number; digital data; plan validation
S7 [33]	User Activity Logs	Data logs; audit trails; data transfers; network usage
S9 [36]	Process Monitoring Data	Running-process events
S10 [91]	Transactional Data	Query logs; login, payment and transfer records
S13 [53]	Honeypot-Collected Data	Network traffic; logs; attack signatures
S14 [83]	System Behavior Data	Behaviour of networked systems; events
S15 [61]	System and User Documents	Configuration files; documents; manuals; e-mail inboxes/outboxes; contact lists
S16 [82]	System Architecture and User Activity	Ordinary user activity; enterprise-architecture repository
S17 [85]	Compliance and Configuration Data	Rule results: pass, fail, error, unknown, not applicable, not checked, not selected, informational, fixed
S18 [71]	Mobile-Application Usage Data	System calls; network traffic; user interactions
S19 [88]	Incident-Response Data	Probability; mean and standard deviation of time to breach
S21 [62]	Security Event Data	Manual input; sensors; network-scanning tools; SIEM system
S22 [90]	Windows System Logs and Dataset	Windows-firewall, event, application, and web logs
S23 [54]	User-Experience Data	Login logs; application logs; program errors; hardware interrupts
S24 [100]	Security-Incident Data	IDS alerts; audit logs
S25 [89]	Interview Findings	Qualitative interview results
S26 [94]	Windows Module Data	Black-listed and white-listed modules
S30 [47]	Security Event Data	Logs from hosts, domain controllers, other log-management systems
S31 [55]	User Behaviour Data	Software, hardware, and system logs
S32 [45]	Unstructured System Data	Standard syslogs; legacy-application logs
S34 [56]	Virtual-Machine Monitoring Data	Network and application logs
S35 [102]	Network Configuration Data	Topology; configurations; vulnerability information
S36 [63]	Web-Usage Data	Access information; registration days; login time; permission level; client browser; source IP; login mailbox; continuous-login days
S37 [73]	Web-Usage Data	URL sequences
S38 [60]	Public Dataset	Application, event, firewall, and other security logs
S39 [72]	Public Dataset	PCAP-format files
S40 [52]	Scan-Report Data	VMs, hosts, connectivity, per-VM vulnerabilities
S41 [77]	Scan-Report Data	Logs; vulnerabilities; host configuration and network topology
S42 [57]	Unstructured System Data	Open-source Hadoop log dataset
S44 [84]	SIEM / ICS / SCADA Data	Network traffic; configuration information
S45 [78]	IAM Event Data	Event logs
S46 [64]	System Monitoring Data	Network, process and file events
S47 [65]	Network-Traffic Data	IP address; port; protocol; log file
S48 [92]	Device and Scan-Report Data	Relationship; type; service and vulnerability info
S49 [79]	Event and Scan-Report Data	Network traffic; logs
S51 [86]	Security Policy Data	Network elements; security policy definitions
S53 [74]	Operation and Transaction Data	Network traffic; click-stream; event logs; transaction records
S55 [66]	Attack Event Data	Persistent attack records; logs
S56 [75]	IDS Alert Data	Threat alert logs
S60 [59]	Network and System Monitoring Data	Captured packets; log files; alerts
A1 [67]	Business and IT Infrastructure Data	Device inventory; log data; ERP-system data
A2 [37]	SIEM Data	Logs; network and device events
A3 [38]	Security Control Data	Logs from web proxies; domain controllers; anti-virus software
A4 [49]	Network Traffic Data	PCAP log files
A5 [68]	Syslog and SNMP Data	Server, anti-viruses, system and network events/logs

4.5. Barriers to Implementing Security Analytics in Enterprises (RQ5)

Observation 9 (Ob9): Overcoming Significant and Interconnected Barriers to Effective Enterprise Security Analytics

The successful implementation and operationalization of security analytics in enterprise environments are impeded by a range of significant and often interconnected challenges. These barriers span technological, human, financial, legal, ethical, and contextual dimensions, demanding a holistic understanding and strategic mitigation efforts. Failure to address these can severely limit the efficacy of security analytics initiatives, leaving organizations vulnerable despite investments. Based on the literature and the broader operational context, these challenges can be synthesized into the following overarching categories:

- *Data-Related Challenges:* The foundation of security analytics is data, yet its collection, management, utility, and protection present substantial hurdles. Enterprises grapple with the sheer volume, variety, and velocity of security data, particularly log data emanating from diverse event sources [63,68]. This is exacerbated by the lack of standardized data formats and retrieval protocols, especially in specialized environments like SCADA systems [84], complicating data integration and interoperability. Furthermore, the inherent security risks of big data systems themselves, often not designed with security as a primary concern, can introduce new vulnerabilities [46]. A critical and increasingly prominent data-related challenge is ensuring data privacy. Practically, enterprises must navigate complex and stringent data protection regulations (e.g., GDPR, CCPA, HIPAA), which impose significant obligations regarding the collection, processing, storage, and retention of personal or sensitive data used in security analytics. This includes implementing robust data minimization strategies, anonymization or pseudonymization techniques where feasible, managing user consent appropriately, and ensuring the privacy of data processed by third-party analytics tools or cloud services [59]. The limitation here is that overly aggressive data anonymization can sometimes reduce the utility of data for certain types of security analysis, creating a difficult trade-off. Consequently, the collected data is frequently noisy, containing redundancies, lacking crucial context, or posing privacy risks if not handled correctly, all of which can hamper efficient and compliant analysis, particularly for concurrent event tracking and user behavior analytics [64]. Addressing these multifaceted data issues requires robust data governance frameworks (incorporating privacy-by-design), advanced data-processing techniques, and the development of centralized data correlation platforms capable of providing a unified, reliable, and compliant view of security events [67].
- *Technological and Methodological Limitations:* Beyond data, the tools and underlying methodologies for security analytics face limitations. Current security assessment techniques often involve a cumbersome mix of automated scanning and manual exploitation, demanding significant expertise and up-to-date information on system topologies and vulnerabilities to interpret complex outputs like attack graphs [77,97]. Many traditional security tools struggle to effectively address modern, sophisticated threats [72] or to analyze the security of increasingly prevalent machine learning systems themselves [48]. A critical and persistent challenge is the difficulty in adapting to dynamic network security threats and accurately identifying unknown or novel attacks in real-time [65]. These technological gaps are compounded by methodological shortcomings, such as the lack of clear definitions or standardized approaches for applying emerging techniques like process mining in cybersecurity [78]. A significant methodological limitation impacting the entire field is the dearth of standardized evaluation metrics and benchmarks for security analytics solutions. Practically, this makes it exceedingly difficult for enterprises to objectively compare the effectiveness, effi-

ciency, and ROI of different tools and approaches, to benchmark their own capabilities against industry peers, or for researchers to reliably compare outcomes across studies. This lack of standardization hinders mature adoption and slows evidence-based advancements. Moreover, the relatively slow maturation of theoretical foundations for core cybersecurity concepts (e.g., logical vulnerability, comprehensive threat modeling, quantifiable risk assessment) and the absence of a common, expressive language for security policies impede the development of more robust, adaptable, interoperable, and scientifically grounded analytics solutions [74].

- *Resource and Organizational Constraints:* Effective security analytics is not solely a technological problem; it is significantly constrained by available resources and various organizational factors, including ethical considerations. Financial constraints are a major barrier, particularly for SMEs that often lack the capital to invest in advanced security analytics tools, technologies, and specialized personnel [58,86,92]. These costs can be further inflated by the absence of a comprehensive, overarching security strategy, leading to fragmented investments and reduced cost-effectiveness [52]. A critical human factor is the pervasive shortage of skilled cybersecurity professionals capable of managing analytics systems, interpreting complex data, and translating insights into actionable security measures [52,86,92]. This includes a common lack of dedicated data scientist roles within security teams who could unlock deeper insights from business security data [67]. Compounding this is often a general lack of cybersecurity awareness and understanding among general employees [66,92], who can be unwitting sources of risk. It is also crucial to engage users appropriately, avoiding overwhelming them with security tasks to prevent security fatigue, which can undermine compliance and vigilance [49,105]. Furthermore, ethical considerations in the deployment of security analytics, particularly those involving extensive data monitoring (e.g., user behavior analytics) or AI-driven decision making, present significant organizational challenges. Practically, organizations must establish clear ethical guidelines, governance structures, and oversight mechanisms to prevent algorithmic bias, ensure fairness, maintain employee trust, and address the societal implications of surveillance technologies [94]. The limitation is that navigating these ethical dimensions requires careful deliberation and may constrain the types of data collected or the manner in which analytics are applied, demanding a balance between security objectives and ethical responsibilities.
- *Systemic Complexity and the Evolving Threat Landscape:* The inherent complexity of modern IT environments and the continuously evolving nature of cyber threats present formidable challenges. The intricate and heterogeneous nature of enterprise systems, including sprawling cloud infrastructures, creates significant integration and interoperability problems for security analytics solutions [52,68]. Enterprises often struggle with effectively translating high-level cybersecurity objectives into concrete design choices and accurately assessing risks within these complex architectures [101]. Existing security approaches may not be well-suited for analyzing the emergent behaviors and vulnerabilities in such multifaceted systems [48]. Specific complexities also arise in managing security in public cloud environments due to shared responsibility models and, as noted earlier, heightened concerns over data privacy, security, and operational efficiency [59]. Simultaneously, organizations face an increasingly dynamic and sophisticated threat landscape, ranging from financially motivated malware campaigns to highly targeted attacks by organized crime and nation-state actors [38]. Traditional signature-based security mechanisms are often inadequate for detecting these advanced threats in real time [56], and the detection of unknown or zero-day threats remains a persistent and critical difficulty across the field [65,66].

In summary, the challenges confronting the implementation and effective operationalization of enterprise security analytics are multifaceted, deeply interconnected—spanning data management and privacy, technological and methodological maturity, resource availability, organizational culture, ethical responsibilities, and the complexity of both enterprise systems and the threat landscape—and demand comprehensive, adaptive strategies for mitigation. Overcoming these hurdles necessitates a concerted effort involving technological innovation, substantial investment in talent development and retention, the cultivation of a strong and ethically-informed security culture, robust governance including privacy-by-design principles, and the adoption of adaptive, integrated security architectures. Addressing these diverse barriers is paramount for enterprises to fully leverage the potential of security analytics in safeguarding their critical assets against an ever-evolving array of cyber threats.

4.6. Research Gaps and Future Opportunities in Enterprise Security Analytics (RQ6)

Observation 10 (Ob10): Charting the Course for Future Advancements in Enterprise Security Analytics

The rapidly evolving landscape of enterprise security analytics, while demonstrating significant progress, presents numerous research gaps and compelling opportunities for future investigation. Addressing these areas is crucial not only for advancing the theoretical underpinnings of the field but also for enhancing the practical efficacy of security analytics solutions in combating increasingly sophisticated cyber threats. Our analysis of the reviewed literature identifies several pivotal domains where focused research efforts can yield substantial impact:

- *Innovations in Methodological Approaches:* There is a persistent call for the exploration and refinement of advanced analytical techniques, particularly deep learning and ensemble learning methods, to achieve higher accuracy and robustness in threat detection and prevention [47,67,72]. Future research should move beyond simply applying these models to investigating their explainability (XAI) in a security context, their resilience against adversarial AI attacks, and their optimal application to specific threat types. Critical foundational gaps also exist in data-preprocessing stages, including more intelligent and automated feature selection, effective data-labeling strategies (especially for unsupervised or semi-supervised learning in dynamic environments), and efficient data-encoding techniques capable of handling vast, real-time data streams without prohibitive computational overhead [75]. A significant opportunity lies in designing adaptive, context-aware, and human-centric security analytics solutions. Current approaches often inadequately account for the dynamic nature of enterprise systems, the evolving behavior of attackers, and critical human factors in security operations [92]. Future work should aim to develop systems that can learn from and adapt to these changing conditions, potentially incorporating behavioral economics or cognitive science principles to better support human analysts and mitigate security fatigue [66]. Furthermore, the field would benefit from increased methodological rigor and standardization. This includes establishing clearer definitions and frameworks for applying techniques like process mining to cybersecurity incident response and analysis [78], and developing a common, expressive language for security policies to facilitate interoperability and automated reasoning [74].
- *Holistic Data Integration and Cross-Functional Contextualization:* A recurring challenge, and thus a research opportunity, is the effective integration and semantic correlation of heterogeneous data sources. Beyond merely aggregating logs, future research needs to focus on developing sophisticated frameworks for fusing diverse internal data (e.g., system, network, application logs) with external sources (e.g., threat intelli-

gence, vulnerability databases) to construct a unified, comprehensive, and real-time understanding of an enterprise's security position [74,90]. This includes research into scalable data fusion techniques and knowledge representation for complex security events. Crucially, there is a significant gap in integrating security analytics outputs with broader business functions, such as enterprise risk management, compliance reporting, and internal audit processes [67]. Future studies should explore methodologies and platforms that can translate technical security findings into quantifiable business risk metrics, enabling better strategic decision making and demonstrating the value of security investments. This involves bridging the communication gap between technical security teams and executive leadership.

- *Enhanced Human–Computer Interaction and Actionable Insights:* While the power of analytics grows, ensuring that human analysts can effectively interpret and act upon the generated insights remains a challenge. Future research is needed in advanced data visualization techniques tailored for complex, high-dimensional security data, moving beyond static dashboards to interactive exploration tools that can help analysts identify subtle patterns, anomalies, and causal relationships quickly [38,47]. Closely related is the need for explainable AI in security analytics. As models become more complex, their "black-box" nature can hinder trust and adoption. Research into XAI methods that can articulate the reasoning behind alerts or predictions in a human-understandable manner is vital for empowering analysts and enabling more confident response actions.
- *Achieving True Real-Time, Proactive, and Predictive Capabilities:* The demand for real-time detection and response continues to outpace the capabilities of many existing systems. Periodic log collection and batch processing are often insufficient for countering advanced, fast-moving attacks [56]. Future research should focus on developing ultra-low latency stream processing architectures, edge analytics for immediate threat detection in distributed environments (e.g., IoT/OT), and robust frameworks for automated or semi-automated incident response based on real-time analytical triggers [76]. Beyond real-time detection, there is a significant opportunity to enhance predictive security analytics. This involves improving the accuracy, lead time, and actionability of threat prediction models, exploring novel indicators of future attacks (e.g., precursor activities, geopolitical shifts) and developing methodologies to translate these predictions into concrete, prioritized proactive defense measures.
- *Ensuring Scalability, Performance, and Operational Efficiency:* As data volumes continue to explode, the scalability and performance of security analytics frameworks remain paramount concerns, especially in large-scale enterprise and big data environments [37]. Continuous research is required into more efficient distributed processing algorithms, optimized data storage and retrieval mechanisms, hardware acceleration techniques, and automated resource management for analytics pipelines to ensure that solutions can cope with increasing demands without prohibitive costs or performance degradation [59,75]. This also includes research into automated security assessment tools that can scale across large, dynamic infrastructures.
- *Democratizing Security Analytics for SMEs:* A notable and critical research gap is the limited focus on the unique security analytics needs of SMEs [106]. SMEs often face similar threat landscapes as larger enterprises but typically operate with significant resource constraints (in terms of finances, technical expertise, and dedicated personnel). Future research should prioritize the development and adaptation of scalable, cost-effective, and user-friendly security analytics solutions specifically tailored to SME environments. This includes exploring lightweight deployment models, managed security analytics service offerings suitable for SMEs, and practical guidance

on implementing foundational analytics capabilities within their operational context. Addressing this gap is essential for fostering a more inclusive and resilient digital economy.

In conclusion, while enterprise security analytics has achieved considerable advancements, the field is rich with unresolved questions and promising research avenues. Progress in these areas—spanning methodological innovation, data intelligence, human–machine synergy, real-time capabilities, performance engineering, and SME accessibility—is essential for the continued evolution of security analytics. Successfully addressing these gaps will not only enhance our ability to counter sophisticated cyber threats but also contribute to building a safer and more secure digital future for all organizations.

5. Limitations of the Review and Observations on the Primary Literature

5.1. Limitations of This Systematic Literature Review Process

Firstly, the temporal scope of our review was intentionally set from January 2013 to December 2023. This decade was chosen to capture the most relevant period reflecting the maturation of key technologies (such as Big Data analytics, cloud computing, machine learning, and artificial intelligence) that have fundamentally reshaped enterprise security analytics, as highlighted in our findings (Observation 2). While this focus ensures the review concentrates on contemporary approaches, it necessarily excludes earlier foundational work. More significantly, with our search concluding at the end of December 2023, developments and publications from 2024 and early 2025 were not included. Given the rapid pace of evolution in cybersecurity, this means the very latest advancements were outside the purview of this analysis. This is an inherent constraint of systematic reviews with fixed search completion dates, which is compounded by typical delays in database indexing for the most recent literature.

Secondly, our review adhered to specific inclusion criteria regarding publication language and type. We focused exclusively on peer-reviewed journal articles and full conference papers published in English. This approach ensures a baseline of academic rigor but means that potentially valuable research published in other languages or disseminated through other channels such as preprints, theses, dissertations, industry white papers (those without clear peer-review), or books was not included. This could have limited the geographical diversity of perspectives and might have excluded some very recent or niche findings not yet available in the selected peer-reviewed formats.

Thirdly, the search process itself, while systematic and based on a comprehensive tripartite keyword strategy across six major academic databases, has inherent limitations. The effectiveness of keyword-based searches is contingent on the consistency of terminology used by authors and the indexing practices of the databases. It is, therefore, possible that some relevant studies employing different terminologies or indexed in a way that did not precisely match our search query may not have been retrieved, despite our efforts to ensure broad coverage, including snowballing techniques.

Finally, this review provides a broad overview and thematic synthesis of enterprise security analytics. While we have highlighted differences where the literature permitted (e.g., concerning SMEs), the level of granular detail for every specific enterprise sub-context (e.g., varying sizes beyond SME/large, or highly specialized industry sub-sectors) may be limited by the general focus of many primary studies.

5.2. Reflections on the Reviewed Primary Literature

Beyond the limitations of our review methodology, the process of synthesizing the 65 included studies has highlighted certain characteristics and potential limitations within the primary literature itself, which are important for contextualizing our findings:

- **Potential for Publication Bias in the Field:** While our own review process is susceptible to publication bias, it is also important to consider that this bias may be present in the broader field of enterprise security analytics. The body of reviewed literature appeared to predominantly feature studies reporting successful implementations or positive outcomes of proposed techniques. Research studies that find a particular data analysis method or security strategy to be ineffective (producing null or negative results), or where the results are not clear-cut (producing inconclusive findings), are likely not published as often as studies that show positive or successful results.
- **Extent of Real-World Validation and Methodological Rigor:** A notable observation from our review of the included studies is the variation in the extent of real-world validation for the proposed methodologies and technologies. While some studies presented evaluations in operational or near-operational settings, many appeared to rely on simulations, lab-based experiments, or proof-of-concept demonstrations. The direct applicability and scalability of findings from studies lacking robust validation in diverse, real-world enterprise environments can be limited. Furthermore, while our quality appraisal focused on relevance and clarity for this review's mapping objectives, a formal critical appraisal of the intrinsic methodological soundness of each primary study (e.g., using tools like CASP or AMSTAR) was not utilized as an exclusion criterion, which means the included studies themselves may have varied in their methodological rigor.
- **Standardization of Evaluation Metrics and Benchmarks:** Our review of the primary literature indicated a potential challenge related to the lack of standardized evaluation metrics and benchmarks within the enterprise security analytics field. Different studies often employed varied, and sometimes bespoke, metrics to evaluate the performance of their proposed techniques or systems. This heterogeneity makes direct comparison of results across studies difficult and can hinder efforts to establish widely accepted benchmarks for efficacy and efficiency in enterprise security analytics. This lack of standardization was also noted as a broader challenge in the field (Observation 9).
- **Depth of Discussion of Practical Long-Term Considerations:** While many studies proposed novel techniques or frameworks, the depth of discussion of long-term practical considerations for enterprise adoption—such as maintainability, the total cost of ownership beyond initial deployment, the evolution of models in response to concept drift, or integration with existing complex legacy systems—was not consistently extensive across all reviewed papers.

6. Conclusions

This systematic literature review, conducted in accordance with the PRISMA protocol, analyzed 65 peer-reviewed studies published between 2013 and 2023. Our objective was to consolidate the current state of cybersecurity analytics within enterprise environments, synthesizing key trends, prevalent methodologies, significant challenges, and emergent future research directions based on ten thematic observations derived from the selected literature.

The synthesis reveals a cybersecurity analytics field undergoing a significant technological and strategic transformation over the past decade. Driven by the escalating complexity of cyber threats and evolving business imperatives (**Ob1**), enterprises have markedly shifted from traditional, often signature-based, security tools towards more sophisticated, data-intensive, and AI-powered analytical approaches (**Ob2**). This era has been characterized by the pronounced adoption of Big Data infrastructure, cloud computing platforms, and, critically, machine learning and artificial intelligence as foundational enablers. Consequently, there is a clear pivot in security strategies from predominantly reactive postures towards more proactive and predictive paradigms (**Ob7**). This shift leverages diverse and heterogeneous data sources—primarily system logs and network traffic (**Ob8**)—to anticipate, detect, and mitigate threats more effectively. Our findings indicate that large organizations, particularly those in high-risk sectors such as finance and ICT, are at the forefront of this adoption curve (**Ob4**), frequently employing a sophisticated blend of quantitative and qualitative analytical techniques (**Ob5, Ob6**) to navigate the intricate modern security landscape.

Despite strong advocacy in the literature for a *holistic approach* (**Ob3**)—one that integrates technical security measures with a comprehensive understanding of broader business processes and objectives—our review suggests this largely remains an acknowledged ideal rather than a universally or systematically implemented reality. The journey towards truly holistic security analytics is impeded by significant and persistent challenges. These include the technical difficulties of integrating diverse and voluminous data sources, the substantial financial costs of implementation, the complexities of managing sophisticated interconnected systems, and a critical shortage of skilled cybersecurity professionals capable of harnessing these advanced analytics (**Ob9**). These multifaceted hurdles also likely contribute to a notable gap identified in our analysis: the underrepresentation of research specifically addressing the unique security analytics needs and constraints of SMEs.

Our review has several limitations as mentioned above. However, notwithstanding these limitations, this review offers valuable, actionable insights. The clear trajectory towards ML/AI-driven, predictive analytics (**Ob2, Ob7**) signals a critical imperative for practitioners: the strategic need to invest in the requisite advanced infrastructure and to cultivate or acquire the specialized skills to manage these systems effectively (**Ob9**). For the research community, the persistent challenges (**Ob9**) coupled with the clearly delineated research gaps (**Ob10**) chart a compelling course for future investigation. Key priorities for advancing the field include the development of more scalable real-time analytics, the establishment of unified policy languages for better interoperability, innovations in data integration methodologies, the robust validation of holistic security frameworks, and, crucially, the creation of tailored, accessible, and effective security analytics solutions for SMEs. Addressing these gaps, particularly for the underserved SME sector, is paramount for enhancing cybersecurity resilience across the entire spectrum of enterprise. Ultimately, the maturation of enterprise security analytics hinges on continued innovation not only in algorithms and technologies but also in devising practical strategies to overcome the significant barriers to their widespread and effective implementation and adoption, as identified herein.

Supplementary Materials: The following supporting information can be downloaded at: https://www.mdpi.com/article/10.3390/electronics14112252/s1, Table S1: Extracted data from the selected studies.

Author Contributions: Conceptualization, T.D.L.; methodology, T.D.L.; investigation, T.D.L., T.L.-D. and S.U.; data curation, T.D.L., T.L.-D. and S.U.; writing—original draft preparation, T.D.L.; writing—review and editing, T.L.-D. and S.U.; validation and final approval of the manuscript, T.D.L., T.L.-D. and S.U. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: During the preparation of this manuscript, the authors used Grammarly (Premium), Quillbot (Premium), and Google Gemini 2.5 Pro solely for grammar checking and refining sentences to an academic tone. We did not use AI to generate new content, figures, or data. All suggestions were reviewed and edited by the authors, who take full responsibility for the final text.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A

This section shows the selected studies and their contributions to the review.

Table A1. Selected studies and their contributions to the review.

Study	Authors	Title	RQ1	RQ2	RQ3	RQ4	RQ5	RQ6
S1 [41]	Cheng, F., Azodi, A., Jaeger, D., & Meinel, C.	Multi-Core Supported High Performance Security Analytics	✓	✓	✓	✓	✓	✓
S2 [42]	Holm, H., Sommestad, T., Ekstedt, M., & Nordström, L.	CySeMoL: A Tool for Cyber Security Analysis of Enterprises	✓	✓	✓		✓	✓
S3 [43]	Purboyo, T. W.	Methods for Strengthening a Computer Network Security	✓		✓		✓	
S4 [31]	Wang, Y., Li, J., Meng, K., Lin, C., & Cheng, X.	Modeling and Security Analysis of Enterprise Network Using Attack-Defense Stochastic Game Petri Nets	✓		✓	✓	✓	✓
S5 [32]	Abraham, S., & Nair, S.	Cyber Security Analytics: A Stochastic Model for Security Quantification Using Absorbing Markov Chains	✓		✓			✓
S6 [34]	Ahmed, N., & Matulevičius, R.	Presentation and Validation of Method for Security Requirements Elicitation from Business Processes	✓	✓	✓	✓	✓	✓
S7 [33]	Brewer, R.	Advanced Persistent Threats: Minimising the Damage	✓		✓	✓	✓	✓
S8 [35]	Li, T., & Horkoff, J.	Dealing with Security Requirements for Socio-Technical Systems: A Holistic Approach	✓	✓	✓		✓	✓
S9 [36]	Rieke, R., Repp, J., Zhdanova, M., & Eichler, J.	Monitoring Security Compliance of Critical Processes	✓	✓	✓	✓	✓	
S10 [91]	Xin, T., & Xiaofang, B.	Online Banking Security Analysis Based on STRIDE Threat Model		✓	✓	✓		
S11 [98]	Abraham, S., & Nair, S.	Exploitability Analysis Using Predictive Cybersecurity Framework			✓			✓
S12 [87]	Cai, Z. Q., Zhao, J. B., Li, Y., Si, S. B., & Ni, M. N.	Information Security Evaluation of System Based on Bayesian Network		✓	✓			
S13 [53]	Hussein, M. K., Zainal, N. B., & Jaber, A. N.	Data Security Analysis for DDoS Defense of Cloud-Based Networks	✓		✓	✓		
S14 [83]	Rieke, R., Zhdanova, M., & Repp, J.	Security Compliance Tracking of Processes in Networked Cooperating Systems	✓	✓	✓	✓	✓	
S15 [61]	Stepanova, T., Pechenkin, A., & Lavrova, D.	Ontology-Based Big-Data Approach to Automated Penetration Testing of Large-Scale Heterogeneous Systems	✓	✓	✓	✓		✓
S16 [82]	Välja, M., Korman, M., Shahzad, K., & Johnson, P.	Integrated Metamodel for Security Analysis	✓		✓	✓		
S17 [85]	Alsaleh, M. N., Husari, G., & Al-Shaer, E.	Optimizing the ROI of Cyber Risk Mitigation	✓		✓	✓	✓	
S18 [71]	Baluda, M., Pistoia, M., Castro, P., & Tripp, O.	A Framework for Automatic Anomaly Detection in Mobile Applications	✓	✓	✓	✓	✓	
S19 [88]	Jenab, K., Khoury, S., & LaFevor, K.	Flow-Graph and Markovian Methods for Cyber Security Analysis	✓	✓	✓	✓		
S20 [99]	Kim, B. J., & Lee, S. W.	Analytical Study of Cognitive Layered Approach for Understanding Security Requirements Using Problem Domain Ontology		✓	✓		✓	✓
S21 [62]	Kotenko, I., & Doynikova, E.	Dynamical Calculation of Security Metrics for Countermeasure Selection in Computer Networks	✓		✓	✓		✓
S22 [90]	Naik, N., Jenkins, P., Savage, N., & Katos, V.	Big-Data Security Analysis Approach Using Computational Intelligence Techniques in R for Desktop Users		✓	✓	✓	✓	✓

Table A1. *Cont.*

Study	Authors	Title	RQ1	RQ2	RQ3	RQ4	RQ5	RQ6
S23 [54]	Niu, D. D., Liu, L., Zhang, X., Lü, S., & Li, Z.	Security Analysis Model, System Architecture and Relational Model of Enterprise Cloud Services	✓		✓	✓	✓	✓
S24 [100]	Ou, X.	A Bottom-Up Approach to Applying Graphical Models in Security Analysis	✓		✓	✓	✓	
S25 [89]	Välja, M., Lagerström, R., Korman, M., & Franke, U.	Bridging the Gap Between Business and Technology in Strategic Decision-Making for Cyber Security Management	✓	✓	✓	✓	✓	✓
S26 [94]	Buyukkayhan, A. S., Oprea, A., Li, Z., & Robertson, W.	Lens on the Endpoint: Hunting for Malicious Software Through Endpoint Data Analysis		✓	✓	✓		
S27 [96]	Kato, Y., Kanai, A., Tanimoto, S., & Hatashima, T.	Dynamic Security Level Analysis Method Using Attack Tree	✓		✓			✓
S28 [70]	Lagerström, R., Johnson, P., & Ekstedt, M.	Automatic Design of Secure Enterprise Architecture	✓	✓	✓			
S29 [95]	Nguyen, H. H., Palani, K., & Nicol, D. M.	An Approach to Incorporating Uncertainty in Network Security Analysis	✓	✓	✓			✓
S30 [47]	Sapegin, A., Jaeger, D., Cheng, F., & Meinel, C.	Towards a System for Complex Analysis of Security Events in Large-Scale Networks	✓	✓	✓	✓	✓	✓
S31 [55]	Zhu, G., Zeng, Y., & Guo, M.	A Security Analysis Method for Supercomputing Users' Behaviour	✓	✓	✓	✓	✓	
S32 [45]	Cinque, M., Cotroneo, D., & Pecchia, A.	Challenges and Directions in Security Information and Event Management (SIEM)	✓	✓	✓	✓	✓	✓
S33 [104]	Sion, L., Yskout, K., Van Landuyt, D., & Joosen, W.	Poster: Knowledge-Enriched Security and Privacy Threat Modeling	✓		✓		✓	✓
S34 [56]	Win, T. Y., Tianfield, H., & Mair, Q.	Big-Data-Based Security Analytics for Protecting Virtualized Infrastructures in Cloud Computing	✓	✓	✓	✓	✓	✓
S35 [102]	Wu, S., Zhang, Y., & Chen, X.	Security Assessment of Dynamic Networks via Integrating Semantic Reasoning and Attack Graphs	✓		✓	✓	✓	
S36 [63]	Lai, J.	Analysis and Visualization of Website Log Data from the Perspective of Big Data	✓		✓	✓	✓	✓
S37 [73]	Padmanaban, R., Thirumaran, M., Sanjana, V., & Moshika, A.	Security Analytics for Heterogeneous Web	✓		✓	✓		✓
S38 [60]	Sharma, S., Sharma, A., & Saini, H.	Advanced Network Security Analysis (ANSA) in Big-Data Technology	✓		✓	✓	✓	✓
S39 [72]	Ahmed, A., Hameed, S., Rafi, M., & Mirza, Q. K. A.	An Intelligent and Time-Efficient DDoS Identification Framework for Real-time Enterprise Networks: SAD-F: Spark based Anomaly Detection Framework	✓		✓	✓	✓	✓
S40 [52]	Alavizadeh, H., Alavizadeh, H., & Jang-Jaccard, J.	Cyber Situation Awareness Monitoring and Proactive Response for Enterprises on the Cloud	✓		✓	✓	✓	✓
S41 [77]	Chowdhary, A., Huang, D., Mahendran, J. S., Romo, D., Deng, Y., & Sabur, A.	Autonomous Security Analysis and Penetration Testing	✓	✓	✓	✓	✓	✓
S42 [57]	Elsayed, M. A., & Zulkernine, M.	PredictDeep: Security Analytics as a Service for Anomaly Detection and Prediction	✓	✓	✓	✓		✓
S43 [93]	Ivanov, D., Kalinin, M., Krundyshev, V., & Orel, E.	Automatic Security Management of Smart Infrastructures Using Attack Graph and Risk Analysis		✓	✓			
S44 [84]	Nashivochnikov, N. V., Bolshakov, A. A., Lukashin, A. A., & Popov, M.	The System for Operational Monitoring and Analytics of Industry Cyber-physical Systems Security in Fuel and Energy Domains Based on Anomaly Detection and Prediction Methods	✓	✓	✓	✓	✓	✓
S45 [78]	Sundararaj, A., Knittl, S., & Grossklags, J.	Challenges in IT Security Processes and Solution Approaches with Process Mining	✓	✓	✓	✓	✓	✓
S46 [64]	Taylor, T., Araujo, F., & Shu, X.	Towards an Open Format for Scalable System Telemetry	✓	✓	✓	✓	✓	✓

Table A1. *Cont.*

Study	Authors	Title	RQ1	RQ2	RQ3	RQ4	RQ5	RQ6
S47 [65]	Wu, L., & Deng, T.	Computer Network Security Analysis Modeling Based on Spatio-Temporal Characteristics and Deep-Learning Algorithm	✓		✓	✓	✓	✓
S48 [92]	Zhang, Y., Wang, B., Wu, C., Wei, X., Wang, Z., & Yin, G.	Attack-Graph-Based Quantitative Assessment for Industrial Control System Security	✓	✓	✓	✓	✓	✓
S49 [79]	Aquino, M. F. M., & Noroña, M. I.	Enhancing Cyber Security in the Philippine Academe: A Risk-Based IT Project Assessment Approach	✓		✓	✓		
S50 [58]	Empl, P., & Pernul, G.	A Flexible Security Analytics Service for the Industrial IoT	✓	✓	✓		✓	
S51 [86]	Kumar, R., Singh, S., & Kela, R.	A Quantitative Security Risk Analysis Framework For Modelling and Analyzing Advanced Persistent Threats	✓		✓	✓	✓	✓
S52 [46]	Rosado, D. G., Moreno, J., Sánchez, L. E., Santos-Olmo, A., Serrano, M. A., & Fernández-Medina, E.	MARISMA-BiDa Pattern: Integrated Risk Analysis for Big Data	✓		✓		✓	
S53 [74]	Vassilev, V., Sowinski-Mydlarz, V., Gasiorowski, P., Ouazzane, K., & Phipps, A.	Intelligence Graphs for Threat Intelligence and Security Policy Validation of Cyber Systems	✓	✓	✓	✓	✓	✓
S54 [80]	Chen, G., & Mazin, T.	Computer Network Security Analysis Based on Deep-Learning Algorithm	✓		✓			
S55 [66]	Chun, Y. H., & Cho, M. K.	An Empirical Study of Intelligent Security Analysis Methods Utilizing Big Data	✓	✓	✓	✓	✓	✓
S56 [75]	Ndichu, S., Ban, T., Takahashi, T., & Inoue, D.	Critical-Threat-Alert Detection Using Online Machine Learning	✓	✓	✓	✓	✓	✓
S57 [97]	Hankin, C., & Malacaria, P.	Attack Dynamics: An Automatic Attack-Graph Generation Framework Based on System Topology, CAPEC, CWE, and CVE Databases			✓		✓	✓
S58 [48]	Zou, Q., Zhang, L., Singhal, A., Sun, X., & Liu, P.	Attacks on ML Systems: From Security Analysis to Attack Mitigation	✓		✓		✓	
S59 [76]	Efiong, J. E., Akinyemi, B. O., Olajubu, E. A., Aderounmu, G. A., & Degila, J.	CyberSCADA Network Security Analysis Model for Intrusion Detection Systems in the Smart Grid	✓	✓	✓			✓
S60 [59]	Vassilev, V., Ouazzane, K., Sowinski-Mydlarz, V., Maosa, H., Nakarmi, S., Hristev, M., & Radu, S.	Network Security Analytics on the Cloud: Public vs. Private Case	✓		✓	✓	✓	✓
A1 [67]	Early, G., & Stott III, W.	Preemptive Security Through Information Analytics	✓		✓	✓	✓	✓
A2 [37]	Puri, C., & Dukatz, C.	Analyzing and Predicting Security-Event Anomalies: Lessons from a Large-Enterprise Big-Data Streaming-Analytics Deployment	✓	✓	✓	✓		✓
A3 [38]	Li, Z., & Oprea, A.	Operational Security Log Analytics for Enterprise Breach Detection	✓	✓	✓	✓	✓	✓
A4 [49]	Ulmer, A., Schufrin, M., Lücke-Tieke, H., Kannanayikkal, C. D., & Kohlhammer, J.	Towards Visual Cyber-Security Analytics for the Masses	✓	✓	✓	✓	✓	
A5 [68]	Chernova, E. V., Polezhaev, P. N., Shukhman, A. E., Ushakov, Y. A., Bolodurina, I. P., & Bakhareva, N. F.	Security-Event Data Collection and Analysis in Large Corporate Networks	✓	✓	✓	✓	✓	

References

1. Kaur, J.; Ramkumar, K. The recent trends in cyber security: A review. *J. King Saud Univ.-Comput. Inf. Sci.* **2022**, *34*, 5766–5781. [CrossRef]
2. Shajan, A.; Rangaswamy, S. Survey of security threats and countermeasures in cloud computing. *United Int. J. Res. Technol.* **2021**, *2*, 201–207.
3. Zhao, T.; Zhang, G.; Zhang, L. An Overview of Mobile Devices Security Issues and Countermeasures. In Proceedings of the 2014 International Conference on Wireless Communication and Sensor Network, Wuhan, China, 13–14 December 2014; pp. 439–443. [CrossRef]
4. Lu, Y.; Xu, L.D. Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics. *IEEE Internet Things J.* **2019**, *6*, 2103–2115. [CrossRef]
5. Xiong, W.; Legrand, E.; Åberg, O.; Lagerström, R. Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. *Softw. Syst. Model.* **2021**, *21*, 157–177. [CrossRef]
6. Saleem, J.; Adebisi, B.; Ande, R.; Hammoudeh, M. A state of the art survey—Impact of cyber attacks on SME's. In Proceedings of the International Conference on Future Networks and Distributed Systems, ICFNDS '17, Cambridge, UK, 19–20 July 2017. [CrossRef]
7. Corallo, A.; Lazoi, M.; Lezzi, M. Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. *Comput. Ind.* **2020**, *114*, 103165. [CrossRef]
8. Klein, D. Relying on firewalls? Here's why you'll be hacked. *Netw. Secur.* **2021**, *2021*, 9–12. [CrossRef]
9. Khraisat, A.; Gondal, I.; Vamplew, P.; Kamruzzaman, J. Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity* **2019**, *2*, 20. [CrossRef]
10. Tounsi, W.; Rais, H. A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Comput. Secur.* **2018**, *72*, 212–233. [CrossRef]
11. Narang, S. The reality of zero-day vulnerabilities. *Comput. Fraud Secur.* **2021**, *2021*, 20. [CrossRef]
12. Salahdine, F.; Kaabouch, N. Social Engineering Attacks: A Survey. *Future Internet* **2019**, *11*, 89. [CrossRef]
13. Rajasekar, V.; Premalatha, J.; Dhanaraj, R.K. Security analytics. In *System Assurances*; Elsevier: Amsterdam, The Netherlands, 2022; pp. 333–354. [CrossRef]
14. Nallaperumal, K. CyberSecurity Analytics to Combat Cyber Crimes. In Proceedings of the 2018 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Madurai, India, 13–15 December 2018; pp. 1–4. [CrossRef]
15. Khan, S.; Olivia, T.S.L.; Khan, N.; Why, N.K.; Wei, T.S. Data Analytic for Cyber Security: A Review of Current Framework Solutions, Challenges and Trends. *Eurasia Proc. Sci. Technol. Eng. Math.* **2022**, *18*, 1–6. [CrossRef]
16. Verma, R. Security Analytics: Adapting Data Science for Security Challenges. In Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics, CODASPY '18, Tempe, AZ, USA, 19–21 March 2018; pp. 40–41. [CrossRef]
17. Sharma, G.; Tyagi, B. Security Analytics: Challenges and Future Directions. *IITM J. Manag. IT* **2017**, *8*, 37–41.
18. Jing, X.; Yan, Z.; Pedrycz, W. Security Data Collection and Data Analytics in the Internet: A Survey. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 586–618. [CrossRef]
19. Rassam, M.A.; Maarof, M.; Zainal, A. Big Data Analytics Adoption for Cybersecurity: A Review of Current Solutions, Requirements, Challenges and Trends. *J. Inf. Assur. Secur.* **2017**, *11*, 124–145.
20. Perumal, P.R.; Roy, G.G.R.; Kumar, B.R. Security Analysis of Future Enterprise Business Intelligence. In Proceedings of the 2014 World Congress on Computing and Communication Technologies, Tiruchirappalli, India, 27 February–1 March 2014; pp. 191–194. [CrossRef]
21. Birzniece, I. Security Analytics: Dispelling the Fog. In Proceedings of the BIR 2018 Short Papers, Workshops and Doctoral Consortium Co-Located with 17th International Conference Perspectives in Business Informatics Research (BIR 2018), Stockholm, Sweden, 24–26 September 2018; Volume 2218, pp. 160–169.
22. Grahn, K.; Westerlund, M.; Pulkkis, G., Analytics for Network Security: A Survey and Taxonomy. In *Information Fusion for Cyber-Security Analytics*; Springer International Publishing: Cham, Switzerland, 2016; pp. 175–193. [CrossRef]
23. Mahmood, T.; Afzal, U. Security Analytics: Big Data Analytics for cybersecurity: A review of trends, techniques and tools. In Proceedings of the 2013 2nd National Conference on Information Assurance (NCIA), Rawalpindi, Pakistan, 11–12 December 2013; pp. 129–134. [CrossRef]
24. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *Int. J. Surg.* **2021**, *88*, 105906. [CrossRef]
25. Rohan, R.; Pal, D.; Hautamäki, J.; Funilkul, S.; Chutimaskul, W.; Thapliyal, H. A systematic literature review of cybersecurity scales assessing information security awareness. *Heliyon* **2023**, *9*, e14234. [CrossRef]
26. Cremer, F.; Sheehan, B.; Fortmann, M.; Kia, A.N.; Mullins, M.; Murphy, F.; Materne, S. Cyber risk and cybersecurity: A systematic review of data availability. *Geneva Pap. Risk Insur.-Issues Pract.* **2022**, *47*, 698–736. [CrossRef] [PubMed]

27. Marican, M.N.Y.; Razak, S.A.; Selamat, A.; Othman, S.H. Cyber Security Maturity Assessment Framework for Technology Startups: A Systematic Literature Review. *IEEE Access* **2023**, *11*, 5442–5452. [CrossRef]
28. Ratchford, M.; El-Gayar, O.; Noteboom, C.; Wang, Y. BYOD security issues: A systematic literature review. *Inf. Secur. J. Glob. Perspect.* **2021**, *31*, 253–273. [CrossRef]
29. Garg, M.; Goel, A. A systematic literature review on online assessment security: Current challenges and integrity strategies. *Comput. Secur.* **2022**, *113*, 102544. [CrossRef]
30. Webster, J.; Watson, R.T. Analyzing the past to prepare for the future: Writing a literature review. *MIS Q.* **2002**, *26*, xiii–xxiii.
31. Wang, Y.; Li, J.; Meng, K.; Lin, C.; Cheng, X. Modeling and security analysis of enterprise network using attack–defense stochastic game Petri nets. *Secur. Commun. Netw.* **2012**, *6*, 89–99. [CrossRef]
32. Abraham, S.; Nair, S. Cyber Security Analytics: A Stochastic Model for Security Quantification Using Absorbing Markov Chains. *J. Commun.* **2014**, *9*, 899–907. [CrossRef]
33. Brewer, R. Advanced persistent threats: Minimising the damage. *Netw. Secur.* **2014**, *2014*, 5–9. [CrossRef]
34. Ahmed, N.; Matulevičius, R. Presentation and Validation of Method for Security Requirements Elicitation from Business Processes. In *Information Systems Engineering in Complex Environments*; Springer International Publishing: Cham, Switzerland, 2015; pp. 20–35. [CrossRef]
35. Li, T.; Horkoff, J. Dealing with Security Requirements for Socio-Technical Systems: A Holistic Approach. In *Advanced Information Systems Engineering*; Springer International Publishing: Cham, Switzerland, 2014; pp. 285–300. [CrossRef]
36. Rieke, R.; Repp, J.; Zhdanova, M.; Eichler, J. Monitoring Security Compliance of Critical Processes. In Proceedings of the 2014 22nd Euromicro International Conference on Parallel, Distributed, and Network-Based Processing, Torino, Italy, 12–14 February 2014; pp. 552–560. [CrossRef]
37. Puri, C.; Dukatz, C. Analyzing and Predicting Security Event Anomalies: Lessons Learned from a Large Enterprise Big Data Streaming Analytics Deployment. In Proceedings of the 2015 26th International Workshop on Database and Expert Systems Applications (DEXA), Valencia, Spain, 1–4 September 2015; pp. 152–158. [CrossRef]
38. Li, Z.; Oprea, A. Operational Security Log Analytics for Enterprise Breach Detection. In Proceedings of the 2016 IEEE Cybersecurity Development (SecDev), Boston, MA, USA, 3–4 November 2016; pp. 15–22. [CrossRef]
39. González-Granadillo, G.; González-Zarzosa, S.; Diaz, R. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors* **2021**, *21*, 4759. [CrossRef]
40. Bahrami, P.N.; Dehghantanha, A.; Dargahi, T.; Parizi, R.M.; Choo, K.K.R.; Javadi, H.H. Cyber kill chain-based taxonomy of advanced persistent threat actors: Analogy of tactics, techniques, and procedures. *J. Inf. Process. Syst.* **2019**, *15*, 865–889. [CrossRef]
41. Cheng, F.; Azodi, A.; Jaeger, D.; Meinel, C. Multi-core Supported High Performance Security Analytics. In Proceedings of the 2013 IEEE 11th International Conference on Dependable, Autonomic and Secure Computing, Chengdu, China, 21–22 December 2013; pp. 621–626. [CrossRef]
42. Holm, H.; Ekstedt, M.; Sommestad, T.; NordstrM, L. CySeMoL: A tool for cyber security analysis of enterprises. In Proceedings of the 22nd International Conference and Exhibition on Electricity Distribution (CIRED 2013), Stockholm, Sweden, 10–13 June 2013; p. 1109. [CrossRef]
43. Purboyo, T.W.; Kuspriyanto. Methods for strengthening a Computer network security. In Proceedings of the 2013 Joint International Conference on Rural Information & Communication Technology and Electric-Vehicle Technology (rICT & ICeV-T), Bandung-Bali, Indonesia, 26–28 November 2013; pp. 1–4. [CrossRef]
44. Reddy Pulyala, S.; Gupta Desetty, A.; Dutt Jangampet, V. The Impact of Security Orchestration, Automation, and Response (SOAR) on Security Operations Center (SOC) Efficiency: A Comprehensive Analysis. *Turk. J. Comput. Math. Educ. (TURCOMAT)* **2019**, *10*, 1545–1549. [CrossRef]
45. Cinque, M.; Cotroneo, D.; Pecchia, A. Challenges and Directions in Security Information and Event Management (SIEM). In Proceedings of the 2018 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), Memphis, TN, USA, 15–18 October 2018; pp. 95–99. [CrossRef]
46. Rosado, D.G.; Moreno, J.; Sánchez, L.E.; Santos-Olmo, A.; Serrano, M.A.; Fernández-Medina, E. MARISMA-BiDa pattern: Integrated risk analysis for big data. *Comput. Secur.* **2021**, *102*, 102155. [CrossRef]
47. Sapegin, A.; Jaeger, D.; Cheng, F.; Meinel, C. Towards a system for complex analysis of security events in large-scale networks. *Comput. Secur.* **2017**, *67*, 16–34. [CrossRef]
48. Zou, Q.; Zhang, L.; Singhal, A.; Sun, X.; Liu, P. Attacks on ML Systems: From Security Analysis to Attack Mitigation. In *Information Systems Security*; Springer Nature: Cham, Switzerland, 2022; pp. 119–138. [CrossRef]
49. Ulmer, A.; Schufrin, M.; Lücke-Tieke, H.; Kannanayikkal, C.D.; Kohlhammer, J. Towards Visual Cyber Security Analytics for the Masses. In Proceedings of the EuroVis Workshop on Visual Analytics 2018, Brno, Czech Republic, 4 June 2018. [CrossRef]
50. Geluvaraj, B.; Satwik, P.M.; Ashok Kumar, T.A. The Future of Cybersecurity: Major Role of Artificial Intelligence, Machine Learning, and Deep Learning in Cyberspace. In *International Conference on Computer Networks and Communication Technologies*; Springer: Singapore, 2018; pp. 739–747. [CrossRef]

51. Alani, M.M. Big data in cybersecurity: A survey of applications and future trends. *J. Reliab. Intell. Environ.* **2021**, *7*, 85–114. [CrossRef]
52. Alavizadeh, H.; Alavizadeh, H.; Jang-Jaccard, J. Cyber Situation Awareness Monitoring and Proactive Response for Enterprises on the Cloud. In Proceedings of the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 29 December 2020–1 January 2021; pp. 1276–1284. [CrossRef]
53. Hussein, M.K.; Bin Zainal, N.; Jaber, A.N. Data security analysis for DDoS defense of cloud-based networks. In Proceedings of the 2015 IEEE Student Conference on Research and Development (SCOReD), Kuala Lumpur, Malaysia, 13–14 December 2015; pp. 305–310. [CrossRef]
54. Niu, D.D.; Liu, L.; Zhang, X.; Lü, S.; Li, Z. Security analysis model, system architecture and relational model of enterprise cloud services. *Int. J. Autom. Comput.* **2016**, *13*, 574–584. [CrossRef]
55. Zhu, G.; Zeng, Y.; Guo, M. A Security Analysis Method for Supercomputing Users' Behavior. In Proceedings of the 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), New York, NY, USA, 26–28 June 2017; pp. 287–293. [CrossRef]
56. Win, T.Y.; Tianfield, H.; Mair, Q. Big Data Based Security Analytics for Protecting Virtualized Infrastructures in Cloud Computing. *IEEE Trans. Big Data* **2018**, *4*, 11–25. [CrossRef]
57. Elsayed, M.A.; Zulkernine, M. PredictDeep: Security Analytics as a Service for Anomaly Detection and Prediction. *IEEE Access* **2020**, *8*, 45184–45197. [CrossRef]
58. Empl, P.; Pernul, G. A Flexible Security Analytics Service for the Industrial IoT. In Proceedings of the 2021 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems, CODASPY '21, Virtual, 28 April 2021; pp. 23–32. [CrossRef]
59. Vassilev, V.; Ouazzane, K.; Sowinski-Mydlarz, V.; Maosa, H.; Nakarmi, S.; Hristev, M.; Radu, S. Network Security Analytics on the Cloud: Public vs. Private Case. In Proceedings of the 2023 13th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 19–20 January 2023; pp. 151–156. [CrossRef]
60. Sharma, S.; Sharma, A.; Saini, H. Advanced Network Security Analysis (ANSA) in Big Data Technology. *Int. J. Innov. Technol. Explor. Eng.* **2019**, *8*, 2634–2639. [CrossRef]
61. Stepanova, T.; Pechenkin, A.; Lavrova, D. Ontology-based big data approach to automated penetration testing of large-scale heterogeneous systems. In Proceedings of the 8th International Conference on Security of Information and Networks, SIN '15, Sochi, Russia, 8–10 September 2015; pp. 142–149. [CrossRef]
62. Kotenko, I.; Doynikova, E. Dynamical Calculation of Security Metrics for Countermeasure Selection in Computer Networks. In Proceedings of the 2016 24th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing (PDP), Heraklion, Greece, 17–19 February 2016; pp. 558–565. [CrossRef]
63. Lai, J. Analysis and Visualization of Website Log Data from the Perspective of Big Data. In Proceedings of the 2019 International Conference on Computer Network, Electronic and Automation (ICCNEA), Xi'an, China, 27–29 September 2019; pp. 26–30. [CrossRef]
64. Taylor, T.; Araujo, F.; Shu, X. Towards an Open Format for Scalable System Telemetry. In Proceedings of the 2020 IEEE International Conference on Big Data (Big Data), Atlanta, GA, USA, 10–13 December 2020; pp. 1031–1040. [CrossRef]
65. Wu, L.; Deng, T. Computer Network Security Analysis Modeling Based on Spatio-temporal Characteristics and Deep Learning Algorithm. *J. Phys. Conf. Ser.* **2020**, *1648*, 042111. [CrossRef]
66. An empirical study of intelligent security analysis methods utilizing big data. *J. Logist. Inform. Serv. Sci.* **2022**, *9*, 26–35. [CrossRef]
67. Early, G.; Stott, W., III. Preemptive Security Through Information Analytics. *Inf. Secur. J. Glob. Perspect.* **2015**, *24*, 48–56. [CrossRef]
68. Chernova, E.; Polezhaev, P.; Shukhman, A.; Ushakov, Y.; Bolodurina, I.; Bakhareva, N. Security event data collection and analysis in large corporate networks. In Proceedings of the V International Conference Information Technology and Nanotechnology 2019, ITNT-2019, Samara, Russia, 21–24 May 2019; pp. 233–241. [CrossRef]
69. Moshika, A.; Thirumaran, M.; Natarajan, B.; Andal, K.; Sambasivam, G.; Manoharan, R. Vulnerability Assessment in Heterogeneous Web Environment Using Probabilistic Arithmetic Automata. *IEEE Access* **2021**, *9*, 74659–74673. [CrossRef]
70. Lagerstrom, R.; Johnson, P.; Ekstedt, M. Automatic Design of Secure Enterprise Architecture: Work in Progress Paper. In Proceedings of the 2017 IEEE 21st International Enterprise Distributed Object Computing Workshop (EDOCW), Quebec, QC, Canada, 10–13 October 2017; pp. 65–70. [CrossRef]
71. Baluda, M.; Pistoia, M.; Castro, P.; Tripp, O. A framework for automatic anomaly detection in mobile applications. In Proceedings of the International Conference on Mobile Software Engineering and Systems, ICSE '16, Austin, TX, USA, 16–17 May 2016; pp. 297–298. [CrossRef]
72. Ahmed, A.; Hameed, S.; Rafi, M.; Mirza, Q.K.A. An Intelligent and Time-Efficient DDoS Identification Framework for Real-Time Enterprise Networks: SAD-F: Spark Based Anomaly Detection Framework. *IEEE Access* **2020**, *8*, 219483–219502. [CrossRef]
73. Padmanaban, R.; Thirumaran, M.; Sanjana, V.; Moshika, A. Security Analytics for Heterogeneous Web. In Proceedings of the 2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN), Pondicherry, India, 29–30 March 2019; pp. 1–6. [CrossRef]

74. Vassilev, V.; Sowinski-Mydlarz, V.; Gasiorowski, P.; Ouazzane, K.; Phipps, A. Intelligence Graphs for Threat Intelligence and Security Policy Validation of Cyber Systems. In *Proceedings of International Conference on Artificial Intelligence and Applications, Proceedings of the ICAIA 2020, Hong Kong, China, 21–23 October 2020*; Springer: Singapore, 2020; pp. 125–139. [CrossRef]
75. Ndichu, S.; Ban, T.; Takahashi, T.; Inoue, D. Critical-Threat-Alert Detection using Online Machine Learning. In Proceedings of the 2022 IEEE International Conference on Big Data (Big Data), Osaka, Japan, 17–20 December 2022; pp. 3007–3014. [CrossRef]
76. Efiong, J.E.; Akinyemi, B.O.; Olajubu, E.A.; Aderounmu, G.A.; Degila, J. CyberSCADA Network Security Analysis Model for Intrusion Detection Systems in the Smart Grid. In *Advances in Intelligent Systems, Computer Science and Digital Economics IV*; Springer Nature: Cham, Switzerland, 2023; pp. 481–499. [CrossRef]
77. Chowdhary, A.; Huang, D.; Mahendran, J.S.; Romo, D.; Deng, Y.; Sabur, A. Autonomous Security Analysis and Penetration Testing. In Proceedings of the 2020 16th International Conference on Mobility, Sensing and Networking (MSN), Tokyo, Japan, 17–19 December 2020; pp. 508–515. [CrossRef]
78. Sundararaj, A.; Knittl, S.; Grossklags, J. Challenges in IT Security Processes and Solution Approaches with Process Mining. In *Security and Trust Management*; Springer International Publishing: Cham, Switzerland, 2020; pp. 123–138. [CrossRef]
79. Aquino, M.F.M.; Noroña, M.I. Enhancing cyber security in the Philippine academe: A risk-based it project assessment approach. In Proceedings of the 11th Annual International Conference on Industrial Engineering and Operations Management, Singapore, 7–11 March 2021; pp. 5166–5179.
80. Chen, G.; Mazin, T. Computer Network Security Analysis Based on Deep Learning Algorithm. In *Application of Intelligent Systems in Multi-Modal Information Analytics*; Springer International Publishing: Cham, Switzerland, 2022; pp. 993–998. [CrossRef]
81. Ilieva, R.; Stoilova, G. Challenges of AI-Driven Cybersecurity. In Proceedings of the 2024 XXXIII International Scientific Conference Electronics (ET), Sozopol, Bulgaria, 17–19 September 2024; pp. 1–4. [CrossRef]
82. Valja, M.; Korman, M.; Shahzad, K.; Johnson, P. Integrated Metamodel for Security Analysis. In Proceedings of the 2015 48th Hawaii International Conference on System Sciences, Kauai, HI, USA, 5–8 January 2015; pp. 5192–5200. [CrossRef]
83. Rieke, R.; Zhdanova, M.; Repp, J. Security Compliance Tracking of Processes in Networked Cooperating Systems. *J. Wirel. Mob. Netw. Ubiquitous Comput. Dependable Appl.* **2015**, *6*, 21–40.
84. Nashivochnikov, N.V.; Bolshakov, A.A.; Lukashin, A.A.; Popov, M. The System for Operational Monitoring and Analytics of Industry Cyber-Physical Systems Security in Fuel and Energy Domains Based on Anomaly Detection and Prediction Methods. In *Cyber-Physical Systems: Industry 4.0 Challenges*; Springer International Publishing: Cham, Switzerland, 2019; pp. 261–273. [CrossRef]
85. Alsaleh, M.N.; Husari, G.; Al-Shaer, E. Optimizing the RoI of cyber risk mitigation. In Proceedings of the 2016 12th International Conference on Network and Service Management (CNSM), Montreal, QC, Canada, 31 October–4 November 2016; pp. 223–227. [CrossRef]
86. Kumar, R.; Singh, S.; Kela, R. A Quantitative Security Risk Analysis Framework for Modelling and Analyzing Advanced Persistent Threats. In *Foundations and Practice of Security*; Springer International Publishing: Cham, Switzerland, 2021; pp. 29–46. [CrossRef]
87. Cai, Z.Q.; Zhao, J.B.; Li, Y.; Si, S.B.; Ni, M.N. Information security evaluation of system based on Bayesian network. In Proceedings of the 2015 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Singapore, 6–9 December 2015; pp. 315–319. [CrossRef]
88. Jenab, K.; Khoury, S.; LaFevor, K. Flow-Graph and Markovian Methods for Cyber Security Analysis. *Int. J. Enterp. Inf. Syst.* **2016**, *12*, 59–84. [CrossRef]
89. Valja, M.; Lagerstrom, R.; Korman, M.; Franke, U. Bridging the gap between business and technology in strategic decision-making for cyber security management. In Proceedings of the 2016 Portland International Conference on Management of Engineering and Technology (PICMET), Honolulu, HI, USA, 4–8 September 2016; pp. 32–42. [CrossRef]
90. Naik, N.; Jenkins, P.; Savage, N.; Katos, V. Big data security analysis approach using Computational Intelligence techniques in R for desktop users. In Proceedings of the 2016 IEEE Symposium Series on Computational Intelligence (SSCI), Athens, Greece, 6–9 December 2016; pp. 1–8. [CrossRef]
91. Xin, T.; Ban, X. Online Banking Security Analysis based on STRIDE Threat Model. *Int. J. Secur. Its Appl.* **2014**, *8*, 271–282. [CrossRef]
92. Zhang, Y.; Wang, B.; Wu, C.; Wei, X.; Wang, Z.; Yin, G. Attack Graph-Based Quantitative Assessment for Industrial Control System Security. In Proceedings of the 2020 Chinese Automation Congress (CAC), Shanghai, China, 6–8 November 2020. [CrossRef]
93. Ivanov, D.; Kalinin, M.; Krundyshev, V.; Orel, E. Automatic security management of smart infrastructures using attack graph and risk analysis. In Proceedings of the 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, UK, 27–28 July 2020; pp. 295–300. [CrossRef]
94. Buyukkayhan, A.S.; Oprea, A.; Li, Z.; Robertson, W. Lens on the Endpoint: Hunting for Malicious Software Through Endpoint Data Analysis. In *Research in Attacks, Intrusions, and Defenses*; Springer International Publishing: Cham, Switzerland, 2017; pp. 73–97. [CrossRef]

95. Nguyen, H.H.; Palani, K.; Nicol, D.M. An Approach to Incorporating Uncertainty in Network Security Analysis. In Proceedings of the Hot Topics in Science of Security: Symposium and Bootcamp, HoTSoS '17, Hanover, MD, USA, 4–5 April 2017; pp. 74–84. [CrossRef]
96. Kato, Y.; Kanai, A.; Tanimoto, S.; Hatashima, T. Dynamic security level analysis method using attack tree. In Proceedings of the 2017 IEEE 6th Global Conference on Consumer Electronics (GCCE), Nagoya, Japan, 24–27 October 2017; pp. 1–3. [CrossRef]
97. Sonmez, F.O.; Hankin, C.; Malacaria, P. Attack Dynamics: An Automatic Attack Graph Generation Framework Based on System Topology, CAPEC, CWE, and CVE Databases. *Comput. Secur.* **2022**, *123*, 102938. [CrossRef]
98. Abraham, S.; Nair, S. Exploitability analysis using predictive cybersecurity framework. In Proceedings of the 2015 IEEE 2nd International Conference on Cybernetics (CYBCONF), Gdynia, Poland, 24–26 June 2015; pp. 317–323. [CrossRef]
99. Kim, B.J.; Lee, S.W. Analytical Study of Cognitive Layered Approach for Understanding Security Requirements Using Problem Domain Ontology. In Proceedings of the 2016 23rd Asia-Pacific Software Engineering Conference (APSEC), Hamilton, New Zealand, 6–9 December 2016; pp. 97–104. [CrossRef]
100. Ou, X. A Bottom-Up Approach to Applying Graphical Models in Security Analysis. In *Graphical Models for Security*; Springer International Publishing: Cham, Switzerland, 2016; pp. 1–24. [CrossRef]
101. Sion, L.; Yskout, K.; Van Landuyt, D.; Joosen, W. Knowledge-enriched security and privacy threat modeling. In Proceedings of the 2018 IEEE/ACM 40th International Conference on Software Engineering: Companion (ICSE-Companion), Gothenburg, Sweden, 27 May–3 June 2018.
102. Wu, S.; Zhang, Y.; Chen, X. Security Assessment of Dynamic Networks with an Approach of Integrating Semantic Reasoning and Attack Graphs. In Proceedings of the 2018 IEEE 4th International Conference on Computer and Communications (ICCC), Chengdu, China, 7–10 December 2018; pp. 1166–1174. [CrossRef]
103. Evrin, V.; CISA; CRISC; COBIT 2019 Foundation; CDPSE; CEHv9; ISO 27001-22301-20000 LA. Risk assessment and analysis methods: Qualitative and quantitative. *ISACA J.* **2021**, *2*, 1–6.
104. Sekharan, S.S.; Kandasamy, K. Profiling SIEM tools and correlation engines for security analytics. In Proceedings of the 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 22–24 March 2017; pp. 717–721. [CrossRef]
105. Cram, W.A.; Proudfoot, J.G.; D'Arcy, J. When enough is enough: Investigating the antecedents and consequences of information security fatigue. *Inf. Syst. J.* **2020**, *31*, 521–549. [CrossRef]
106. Alahmari, A.; Duncan, B. Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. In Proceedings of the 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland, 15–19 June 2020; pp. 1–5. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.