The Path to Choosing a SIEM System – A Systematic Literature Review

Seminar paper

Hase, Linus, FH Wedel, Wedel, Germany, winf105407@stud.fh-wedel.de

Abstract

Today, Security Information and Event Management systems are one of the most used security solutions for detecting anomalies and potential threats within an organization's IT infrastructure. Thus, companies get assisted in fulfilling compliance mandates and ensuring overall safety. However, integrating a SIEM in one's IT environment must be a thoughtful process as it contains risks and barriers. This paper systematically reviews the literature on SIEMs and their selection process, including all actions that must be considered. Furthermore, the paper summarizes the challenges that current SIEM systems face, as well as future enhancements. The work aims to provide security managers with a practical guide to ensure the best fitting SIEM solution will be chosen and installed.

Keywords: SIEM, capabilities, selection process, challenges, enhancements

Table of Contents

1 Introduction

Cyber attacks are still one of the most vulnerable threats to firms of all sizes. With 79% of all attacks in 2023 motivated by cybercrime and over 50% of the techniques used assigned to Malware attacks and exploitation of vulnerabilities (Passeri, 2024), organizations still seem to be a welcomed target. One of the most popular countermeasures today is Security Information and Event Management (SIEM). First mentioned and established by security institution Gartner Inc., a SIEM system unites the security fields of Security Information Management (SIM) and Security Event Management (SEM) (Vielberth & Pernul, 2018). Nowadays, SIEM systems deal with such a high volume of complex events, data, and logs that a simple plug-and-play installation is far from reality anymore (Thakur et al., 2016).

Security and risk management (SRM) leaders are made accountable for picking the best SIEM solution for their organization. However, this is a very challenging task. It needs a lot of precision and expertise as there is a broad spectrum of SIEM vendors with partially crucial differences in their occurrence (Davies et al., 2024). Therefore, every company needs to perform a detailed evaluation, as not every SIEM solution might fit one's specific concerns (Nabil et al., 2017). Choosing the wrong SIEM because of an injudicious decision and not considering future challenges or enhancements regarding the SIEM system will outcome in a costly, inoperative miscalculation (Žgela & Penga, 2019).

In this literature review, I systematically work out the actions and considerations that must take place for a successful SIEM integration. Thus, I answer the following research questions: What is the state of the art of literature on the SIEM selection process, and what challenges and possible enhancements do current systems face?

The structure of the literature review looks the following: First, I explain the chosen research methodology for more reproducibility with regard to the results. Afterward, I will review the current literature on SIEM systems and their proper evaluation. Therefore, I outline a guideline of the steps to execute and the difficulties, as well as enhancements to observe during that process. Finally, I discuss the results that were previously constituted and give a brief overview of potential future work.

2 Literature Review

I conducted a systematic review of the literature covering SIEM based on the Grounded Theory framework by Wolfswinkel et al. (2013) for performing a rigorous literature review. Therefore, I arranged my procedure for the review as follows: Define and Search, Select, and Form interrelations. Next, I further elaborated on those steps for transparency reasons.

Define and Search: The literature review was conducted using the following databases: EBSCOHost, SpringerLink, ScienceDirect, IEEE Xplore, and Google Scholar, as well as highly regarded IT consultancies. To perform the search, I started with the search terms *SIEM* and *"security information and event management"*. As SIEM has a vital role in IT security, much of the literature mentions the search terms I used but does not elaborate on them any further. Thus, I limited the search fields to only the title, abstract, and keywords to catch more relevant literature. Furthermore, I expanded the inclusion criteria to only results published within the last ten years, as this paper needs fairly present literature to provide meaningful results. Besides Google Scholar, all databases were additionally limited to only peer-reviewed results. Across all searched databases, this led to a total number of 1.595 results as groundwork.

Select: To develop a carefully selected set of proper literature, I carried out a stepwise selection process. First, I started removing all duplicates from the initial result pool. Secondly, I began scanning the titles of my findings to filter out literature that did not reference IT security, as the acronym "siem" has multiple ranges of applications. With those results out of the scope, I continued reading the keywords, abstracts, and text sections with chapter headings of potential relevance. Thus, only the findings that matched the defined frame of my research questions were considered. With a filtered choice of literature, I undertook forward and backward searches, as Webster and Watson (2002) described, on the most relevant papers from that pool. Only the databases mentioned above were checked for possible citations for the forward search. After finalizing the selection process, I ended up with 23 papers on which the following literature review builds.

Form interrelations: Subsequently, I used the Grounded Theory method proposed by Wolfswinkel et al. (2013) to analyze the final literature pool in relation to the structure of the paper's result part. Therefore, I reread the selected literature to extract all sections that seemed relevant for the final literature review. Afterward, I applied the declared coding steps (Wolfswinkel et al., 2013) for a detailed analysis. Thus, I adopted 'open coding', 'axial coding', and 'selective coding' on the highlighted parts to identify related concepts, then used these concepts to precisely form the final categories for the paper's result section and organize the selected papers into those categories. The final allocation of my findings is constituted in the following concept matrix (Table 1).

References	*definition*	*selection process*			*challenges*	*enhancements*
		prerequisites	*capabilities*	*evaluation*		
Ban et al., 2023						•
Bedwell, 2014		•	•			
Bezas and Filippidou, 2023						•
Bhatt et al., 2014	•	•	•		•	
Cinque et al., 2018					•	
Davies et al., 2024			•			•
Islam, 2023		•				
González-Granadillo et al., 2021		•	•		•	•
Kavanagh et al., 2020			•			
Măcăneață, 2024	•	•	•		•	•
Manzoor et al., 2024	•		•	•		
Miloslavskaya and Tolstoy, 2019						•
Mokalled et al., 2019	•	•		•		
Mokalled et al., 2020			•			
Nabil et al., 2017			•			
Podzins and Romanovs, 2019		•	•		•	
Sadowski et al., 2020		•	•			
Scarfone, 2018			•			
Schneider et al., 2022			•	•		
Sekharan and Kandasamy, 2017			•			
Skendzic et al., 2022	•	•	•			•
Yadav and Mishra, 2021					•	
Žgela and Penga, 2019					•	

Table 1. Concept Matrix.

3 Results

3.1 Definition of Security Information & Event Management

A Security Information and Event Management (SIEM) system is an all-encompassing cybersecurity solution that collects, normalizes, and correlates event data from various sources to provide real-time monitoring and analysis of an organization’s security posture (Manzoor et al., 2024). The architecture of a SIEM comprises: (i) physical components, (ii) collectors and processors of events, (iii) network sensors, (iv) an event collection software, and (v) event databases for storage, as seen in Figure 1 (Skendžic et al., 2022). The collectors, also called agents, are thereby deployed hierarchically in modern-day SIEM systems (Mokalled et al., 2019). Collected logs then get fortified with contextual information about connected users, threats, and vulnerabilities (Mokalled et al., 2019). Finally, detected anomalies are sent to a security management platform, which alerts analysts with the help of terminal-based visualization (Bhatt et al., 2014). All in all, a SIEM solution ensures a robust defense system against all kinds of security threats (Măcăneață, 2024).

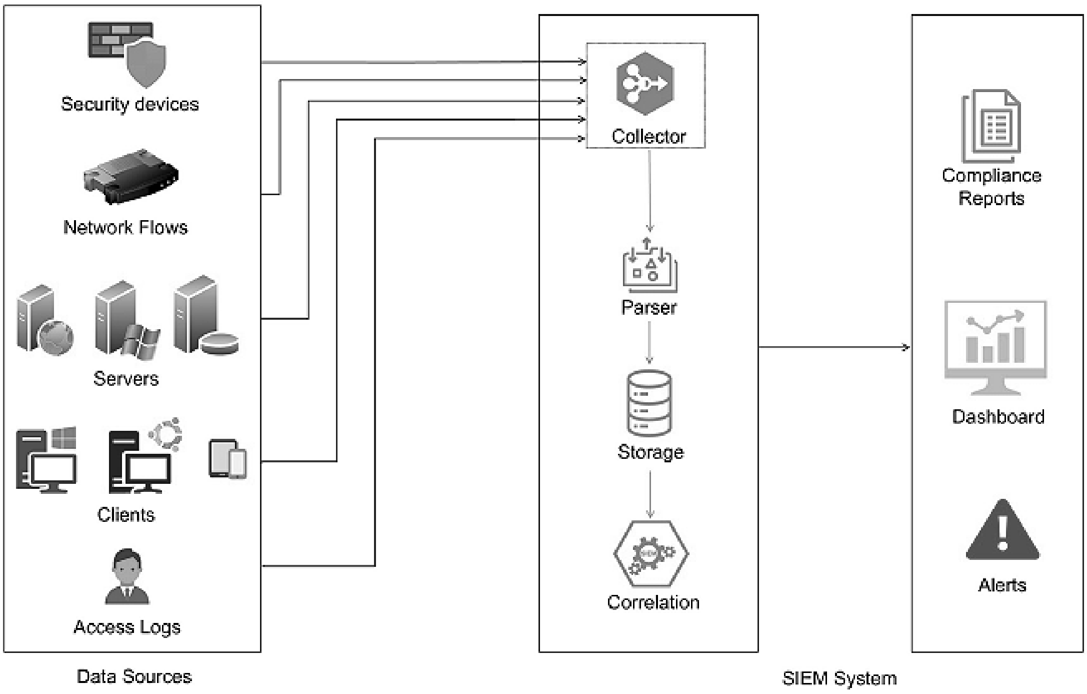

Figure 1. A basic SIEM architecture (Manzoor et al., 2024).

3.2 The SIEM selection process

First and foremost, the most crucial aspect that most of the literature dealing with the selection process of a fitting SIEM points out at the start is that the procedure is highly individual, and every company needs to perform its own evaluation to maximize the resulting value of a SIEM integration (Mokalled et al., 2019; Skendžic et al., 2022; Nabil et al., 2017; Sadowski et al., 2020; Scarfone, 2018). Nevertheless, a fundamental conceptual framework for a structured evaluation approach can be outlined.

Prerequisites: Before going into a detailed evaluation, the following topics should be taken into consideration:

The Company: Critical key figures like size, location, or budget should be determined, as well as a detailed overview of the IT infrastructure that will eventually be part of a SIEM integration, e.g., computers, routers, servers, cloud platforms, firewalls, distribution systems, and other critical software components (Mokalled et al., 2019; Măcăneață, 2024).

Assets/Risks: An analysis of the company's most valuable assets and, therefore, the most vulnerable risks the SIEM should recognize must be performed (Mokalled et al., 2019). In general, but especially for small and medium-sized enterprises (SMEs), this plays a vital part in the upcoming evaluation (Bedwell, 2014).

Compliance and regulations: Analysts must closely examine internal restrictions regarding data privacy, as well as at external regulations (Mokalled et al., 2019). Moreover, the geographical location can impact certain political, legal, and economic factors that need to be noted and documented (Mokalled et al., 2019; González-Granadillo et al., 2021).

Employee/human aspects: Though modern SIEMs try to get more processes to work automatically (Islam, 2023), the human factor still plays a crucial role in SIEM integration (Skendžic et al., 2022). Companies need to be clear about their capabilities regarding employees and their expertise to work with the SIEM (Skendžic et al., 2022). The literature agrees that it is best practice to build a Security Operation Centre (SOC) around the SIEM (Mokalled et al., 2019; Podzins & Romanovs, 2019; Bhatt et al., 2014; Sadowski et al., 2020). This approach requires a large budget, so affordability and usability must be carefully evaluated (Bhatt et al., 2014). Either way, knowing the operating team that will take charge of the SIEM after deployment, and the employee costs arising, e.g., through training, is essential (Mokalled et al., 2019).

Another beneficial step in preparing for an actual SIEM evaluation is building use cases for one's potential SIEM solution. This can be crucial as it visualizes what capabilities will be critical in one's organization (LogRhythm, 2020). The fundamental acts to build a set of well-prepared use cases might look the following: (i) frame the use case as an insight, (ii) get the correct data for the required insight, (iii) apply the right analytics for the required insight, and (iv) organize and prioritize the security use cases (LogRhythm, 2020).

Capabilities: This section will outline the capabilities and criteria for evaluating a SIEM solution. SRM leaders may choose from that listing depending on what they consider to be the most valuable features to integrate within the company's IT infrastructure.

Log collection: A SIEM tool can analyze any type of Log file. However, it is only recommended to consider some types as it can result in an unintended overhead (Podzins & Romanovs, 2019). Therefore, SRM leaders should start by selecting only those log sources that are key components within the IT infrastructure (Bedwell, 2014) and later incrementally adding further logs (Sadowski et al., 2020). Microsoft has categorized just 11 security event types with a "high" criticality (Microsoft, 2022). SIEM solutions use different methods for their log collection. First, there is the Agent-Based Log Collection with benefits like Granular Visibility and Real-time Monitoring, whereas Agentless Log Collection has in advantage in points of Installation or Interoperability (Nabil et al., 2017; Măcăneață, 2024). The Agent-Based approach is mostly used for logs from systems allowing installation, e.g., Windows/Linux; the agentless approach best suits firewalls, hypervisors, routers, switches, vulnerability scanners, web servers, and cloud platforms (Măcăneață, 2024).

Correlation Rules: As one of the main components, SIEMs widely differ when it comes to correlation rules. With most of them providing elementary correlation rules, not all SIEMs can perform complex search queries due to robust search capabilities (González-Granadillo et al., 2021). It is also to examine if SIEM vendors grant the possibility to add specific custom rules to extend individual threat detection (Manzoor et al., 2024). Furthermore, companies should be vigilant about the used correlation type, differentiating between (i) Similarity-based Correlation, (ii) Knowledge-based Correlation, and (iii) Statistical correlation (Sekharan & Kandasamy, 2017). I.e., knowledge-based correlation rules cannot detect new attacks while having a low rate of error. In contrast, Statistical correlation can reveal new anomalies but with a higher risk of false-positive reports (Sekharan & Kandasamy, 2017).

Visualization/UI: This is one of the fundamental capabilities that varies most among SIEM vendors (Podzins & Romanovs, 2019). The UI setup defines the efficiency with which security analysts can process incoming events (González-Granadillo et al., 2021). Thus, interactiveness and customization should be the focus of this capability's evaluation (Manzoor et al., 2024). Depending on one's use case, there often must be a trade-off. First, a UI offers a high level of security monitoring solution but with increased complexity (Schneider et al., 2022). Second, a more user-friendly UI with more guidance but less details and granularity (Schneider et al., 2022). This step needs to consider the level of expertise of the users and administrators.

Price: It is essential to know the costs of integrating and maintaining a SIEM. First, SRM leaders must be aware of the licensing method, as the prices differ substantially depending on the method used (González-Granadillo et al., 2021). Thus, one must be informed of the exact number of users, logs, queries, alerts, correlations, dashboards, etc., that will be part of the integration to choose the right licensing option (González-Granadillo et al., 2021). Therefore, it is recommended to use the incremental approach of adding new log files (see *Log collection*) to keep the initial purchase costs at a minimum. Companies must also check what hardware and workforce are available and what needs to be acquired or hired (Bhatt et al., 2014). Especially the maintenance costs on the employee side can be quickly overlooked as i.e. a SIEM integration within a SOC requires 24/7 support (Podzins & Romanovs, 2019).

Storage: SIEM solutions gather all tracked logs on their own databases (Podzins & Romanovs, 2019). Thus, it is crucial to assess what storage technologies are used, the storage capacity, and the length of storage (González-Granadillo et al., 2021). SRM leaders must also check what storage technologies are currently used within the company to migrate or cut possible redundancies (Podzins & Romanovs, 2019). It is also important to look at the likelihood of only sending the logs marked with high criticality through the SIEM and storing logs with a lower priority at long-term data storage (Patton, 2019).

Deployment: Deploying a multi-context security tool such as a SIEM is complex when aligning all elements (Nabil et al., 2017). Therefore, companies should look for ease of deployment to quickly be able to start operating on the SIEM (Schneider et al., 2022). In addition, it is to assess whether an incremental deployment is possible or if it is supplied in one big step (Sadowski et al., 2020). Most importantly, the deployed SIEM must fit into the current IT environment (Mokalled et al., 2020). Thus, it is to balance whether the SIEM solution runs on-premises, as a SaaS solution, or as a hybrid model (Măcăneață, 2024).

Scalability: This capability needs to be assessed in terms of the system's ability to adjust to increasing numbers of devices, events, users, and supported logs (Manzoor et al., 2024). The modularity of installing new sensors that can be monitored is also to be evaluated (González-Granadillo et al., 2021). Thus, the need and likelihood of scalability should be checked vertically and horizontally (Sadowski et al., 2020).

Interoperability: SIEM solutions often come with a basic architecture (Skendžic et al., 2022). The compatibility of this architecture with the rest of the IT infrastructure, and the logs of all different sources is critical for event normalization (Nabil et al., 2017). Therefore, SRM leaders may even look for vendors of SIEM solutions from which the IT environment already includes other security tools, e.g., SOAR, UEBA, or other cloud security solutions (Schneider et al., 2022). This guarantees a higher interoperability, which might be of interest to one's organization.

Data Sources: As one's IT infrastructure can be highly individualized, it is vital to assess what data sources are provided by the possible SIEM solutions (González-Granadillo et al., 2021). Moreover, it happens that, at times, security analysts need to integrate new custom data sources that also should be part of the SIEMs monitoring cycle (Manzoor et al., 2024). Thus, it should be checked if vendors offer the possibility to individually write plugins for certain cases to manage all kinds of custom sources (Manzoor et al., 2024).

Threat Intelligence: Threat Intelligence covers the most common and newest observed external threats (Sekharan & Kandasamy, 2017). SIEM vendors differ in the depth of their knowledge base provided and in the threat analysis tools used (Manzoor et al., 2024). Thus, the assessment should be based on the quality of the threat intelligence feed, including update frequency, significance, and reliability (Scarfone, 2018).

Performance: This capability mainly focuses on the event processing speed of the SIEM solutions (Manzoor et al., 2024). That is because the speed of SIEMs can differ drastically depending on the used rule correlations, data storage capabilities, the computational conditions, or rather the provided hardware, along with data search and monitoring (González-Granadillo et al., 2021). It is key as most security teams tend to handle occurring events in as little time as possible (Bhatt et al., 2014).

Unique features: As a matter of course, SIEM solutions do have USPs and features that differentiate them from that of their competitors on the market (Davies et al., 2024). That is why it may be worth considering looking at those distinctive characteristics, e.g., Independent Host Forensic, or a unique way of flexible dashboarding, and aligning these with one's own use cases to look for advantageous fits (Sekharan & Kandasamy, 2017).

Support: As already mentioned, SIEMs constitute complex systems and operation can be challenging at times. Thus, vendors that provide a support team, client training, comprehensive documentation, and an active community should be favored over the less supported ones (Manzoor et al., 2024). Support is crucial in the integration and deployment phase of new SIEM implementations (Sadowski et al., 2020). Nevertheless, buyers must keep an eye on prices here, too, as there can be costly support plans that may not be needed.

Evolution of the product: It is necessary to also keep track of the evolution of the assessed SIEM solutions as they are dynamically growing and changing at high speed (Nabil et al., 2017). Therefore, it is a prudent step to look at the SIEM vendors, their financial and practical success, and their plans regarding the future development of their SIEM product (Kavanagh et al., 2020) to make sure buyers will be supplied with patches, updates, or even newer versions (Nabil et al., 2017).

Evaluation: To determine a SIEM solution that is suitable for one's company, there must be a ranking process that evaluates the presented capabilities. Some of the literature provides models to fulfill this action.

Manzoor et al. (2024) provide a simple scoring methodology. Each capability considered gets a certain weight (Manzoor et al., 2024). Capabilities one considers crucial get a greater weighting than less major ones. Following this, every SIEM solution is examined for each capability (Manzoor et al., 2024). Therefore, a value, i.e., 0 for an insufficient feature, 1 for basic fulfillment, and 2 for solutions meeting the expectations at their fullest, is assigned to a capability and multiplied with the defined weighting (Manzoor et al., 2024). The sum of all products forms the final score of one SIEM (1) (Manzoor et al., 2024). Mokalled et al. (2019) describe a relatively similar approach.

$$SIEMScore = \sum_{i=1}^{n} W_i * V_i \ (1)$$

Schneider et al. (2022) came up with a slightly different method. First, when companies have built use cases in the first step, each use case is separately evaluated. Second, the capabilities are equipped with percentage weightings so that all weightings add up to 100 percent (Schneider et al., 2022). Third, a SIEM tool will be assessed for each capability depending on the currently considered SIEM use case (Schneider et al., 2022). Therefore, a value between 1.0 and 5.0 is awarded and multiplied by the percentage weighting (Schneider et al., 2022). Hence, each use case gets its own final score so that a fitting SIEM solution can be picked based on the importance of one's individual case.

3.3 Challenges

Although SIEM systems are widely distributed in today's IT security landscape, they still entail some difficulties. These difficulties must be considered when assessing different SIEM solutions and reviewed in terms of how providers handle them. In the following, the most current challenges the literature covers are examined.

Correlation Rules: False positives, meaning events that are mistaken for security threads, are the most common yet painful problems (Măcăneață, 2024). That is because syntax is prioritized over semantics (González-Granadillo et al., 2021). That means SIEM integrators still focus on getting as much normalized information as possible and only after that on writing effective correlation rules (González-Granadillo et al., 2021). However, writing powerful correlations is in the hands of the analysts (Cinque et al., 2018). Moreover, analysts must know about the asset, user, temporal, and location context (Žgela & Penga, 2019). Otherwise, ineffective rules will be the outcome (Žgela & Penga, 2019).

Human dependency: Though implementing more and more automated processes within a SIEM is a rising trend, most of the analysis and decision-making regarding threat incidents is still executed by humans (González-Granadillo et al., 2021). This is time-consuming and costly from a salary perspective (González-Granadillo et al., 2021; Podzins & Romanovs, 2019). Another difficulty occurring with the reliance on humans is alert fatigue due to the incredibly high number of incoming events (Măcăneață, 2024).

Storage archive: Once the SIEM has handled logs, the archiving process still needs to be done manually in most security environments (González-Granadillo et al., 2021). This has two problems. First, it is very costly to execute and analyze the necessity of each log (Bhatt et al., 2014). Second, manual archiving can quickly lead to mistakes that can result in security or reliability problems (González-Granadillo et al., 2021).

Data loss/theft: Another difficulty regarding the storage of logs is that data filed in cloud storage or on-premises is not secured by appropriate account security (Yadav & Mishra, 2021). Often, critical data moves with the SIEM infrastructure without a proper confidentiality analysis (Žgela & Penga, 2019). Furthermore, it is yet to prevent users from pulling data that the SIEM processes onto other storage media types not in control of the SIEM (Žgela & Penga, 2019).

3.4 Future enhancements

As SIEM systems still evolve at rapid pace, it is necessary to be aware of potential enhancements that will improve future SIEMs. The most auspicious ones will be illustrated next.

AI/ML technologies: As in most IT-related fields, artificial intelligence (AI) and machine learning (ML) influences are on the rise (Davies et al., 2024). The goal is to implement these technologies to the point where significant parts of the monitoring process can be automated (Skendžic et al., 2022). It can especially be helpful in predictive procedures like analyzing user or network traffic anomalies (González-Granadillo et al., 2021). This will help in points of alert fatigue and event detection (Măcăneață, 2024). Ban et al. (2023) created an AI-assisted SIEM Framework that helps to address these difficulties.

Enhanced Storage: To address the problem of log archiving, there should be an interest in developing a SIEM extension or finding a vendor who will approach that challenge (González-Granadillo et al., 2021). This extension aims to provide an automated, elastic solution for archiving processed data, e.g., with the help of S3 buckets (González-Granadillo et al., 2021).

IoT devices: With the growth of the Internet of Things (IoT), there will be a need to monitor the behavior of IoT devices within a SIEM solution (Bezas & Filippidou, 2023). As this leads to yet another enlargement in terms of log volume, possible enhancements will be seen with the new generation of SIEMs getting more domain-specific (González-Granadillo et al., 2021). Nevertheless, they will still provide data interoperability from all new sources and no loss in data integrity (Miloslavskaya & Tolstoy, 2019).

Integration with SOAR: The combination of SIEM and SOAR is one of the most promising security capabilities (Măcăneață, 2024). By covering complementary fields, the symbiosis of SIEM and SOAR tools can help maximize the effectiveness of security monitoring and unlock a proactive threat detection, which is preferable to the reactive one (Măcăneață, 2024). It simultaneously forwards the enhancement of using AI and ML technologies.

4 Discussion

To accumulate the worked-out results of this paper, I summarize my findings by giving an overview of the commonalities and differences spotted within the literature. Furthermore, I give a brief review of the practical benefits of the paper as well as the limitations of my research. Finally, I point out potential future research fields regarding SIEM integration in organizations.

Selecting a SIEM solution for one's company is challenging, with many complex considerations and tricky barriers to overcome. The literature indicates that an organization must conduct its own evaluation process to find the best solution for its environment. All the individual conditions are to be considered to have a successful integration. Moreover, most reviewed papers agree that one of the critical success factors for the next generation of SIEM systems is a deeper understanding of using AI and ML technologies and how to maximize their use. It is necessary as it gains more efficiency within security-related processes to keep up with the massively increasing amount of data. Therefore, every SRM leader must be aware of it. However, there is literature asserting that SIEM systems will never reach a level to replace human analysts fully, and AI/ML technologies are more likely to be seen as assistance tools than substitutions (Bhatt et al., 2014). Thus, watching for a competent security team that runs, maintains, and further develops the SIEM system is essential. For that reason, the literature also points out visualization and UI as the key features and future enhancements because they are the main capabilities that strongly affect the human side of the SIEM effectiveness.

By adopting the results presented in this paper, security managers have great opportunities to execute a successful SIEM integration within their company. It provides a clear handbook with all the necessary steps to consider through that selection process. Moreover, it is easily adaptable and configurable for managers wanting to cover more capabilities or apply their own evaluation method to choose the right SIEM solution. There are no strict boundaries set, which is returnable to the individualism of the procedure itself.

Nevertheless, it is impossible to dismiss the fact that SIEM systems are still predominantly designed to work within large-scale enterprises. Although SIEM vendors also tend to enlarge their commitment to small and medium-sized enterprises (Sadowski et al., 2020), it often is still outside the budget of many companies to apply an applicable system. This review of a SIEM selection ties in with this problem. The provided results are practicable for almost every organization, but going deep into the analysis of some of the capabilities can be very costly and time-consuming. Thus, this paper is limited to the managers having a sufficient budget to integrate a SIEM.

Due to these limitations, some future research fields still need to be dealt with further:

- The literature must cover affordable SIEM solutions in more detail. This refers to commercial SIEMs that aim to cover the SME market as well as promising open-source solutions.
- With other viral security tools on the market, it is always good practice to further examine the possibilities of combining different security systems with a SIEM to maximize the safety of an IT infrastructure.
- Literature reviews like this also need to be updated periodically, as the subject area surrounding SIEM is constantly changing at a rapid pace, occasionally resulting in outdated literature.

5 Conclusion

The paper aimed to review the literature's state of the art on Security Information and Event Management and their evaluation and selection process from a company's perspective. Therefore, I provided a guideline of all the steps to consider when deciding to integrate a SIEM solution into one's IT environment. Furthermore, I call attention to challenges and future enhancements SIEM systems currently face that also should be included in the selection process.

In conclusion, the work contributes to a better understanding of SIEMs as multifaceted technologies. Thus, future organizations have an elaborated access point to quickly start installing an appropriate SIEM solution within their IT infrastructure.

References

Ban, T. *et al.* (2023). 'Breaking Alert fatigue: AI-Assisted SIEM Framework for Effective Incident response', *Applied Sciences*, 13(11), p. 6610. https://doi.org/10.3390/app13116610.

Bedwell, P. (2014). 'Finding a new approach to SIEM to suit the SME environment', *Network Security*, 2014(7), pp. 12–16. https://doi.org/10.1016/s1353-4858(14)70070-4.

Bezas, K. and Filippidou, F. (2023). 'Comparative Analysis of Open Source Security Information & Event Management Systems (SIEMs)', *Indonesian Journal of Computer Science*, 12(2), pp. 443–468. https://doi.org/10.33022/ijcs.v12i2.3182.

Bhatt, S., Manadhata, P.K. and Zomlot, L. (2014). 'The operational role of security information and event management systems', *IEEE Security & Privacy*, 12(5), pp. 35–41. https://doi.org/10.1109/msp.2014.103.

Cinque, M., Cotroneo, D. and Pecchia, A. (2018). 'Challenges and Directions in Security Information and Event Management (SIEM)', *2018 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW),* pp. 95-99. https://doi.org/10.1109/issrew.2018.00-24.

Davies A. *et al.* (2024). 'Gartner Magic Quadrant for Security Information and Event Management', *Gartner Group Research Note*, 8 May, Available at: https://www.gartner.com/en/documents/5415763 (Accessed: 28 May 2024).

Islam, M.A. (2023). 'Application of artificial intelligence and machine learning in Security Operations Center', *Issues in information Systems*, 24(4). Available at: https://comp.mga.edu/static/media/doctoralpapers/2023_Islam_0516152253.pdf (Accessed: 17 May 2024).

González-Granadillo, G., González-Zarzosa, S. and Diaz, R. (2021). 'Security Information and Event Management (SIEM): analysis, trends, and usage in critical infrastructures', *Sensors*, 21(14), p. 4759. https://doi.org/10.3390/s21144759.

Kavanagh, K., Bussa, T., and Sadowski, G. (2020). 'Magic Quadrant for Security Information and Event Management', *Gartner Technical Report*, 18 February, Available at: https://www.gartner.com/en/documents/3981040 (Accessed: 23 May 2024).

LogRhythm (2020). 'How to Build Security Use Cases for Your SIEM', *LogRhythm Security Tips and Tricks*, 9 November. Available at: https://logrhythm.com/blog/how-to-build-security-use-cases-for-your-siem/ (Accessed: 17 May 2024).

Măcăneață, C. (2024). 'Overview of security information and event management systems', *Informatică Economică*, 28(1/2024), pp. 15–24. https://doi.org/10.24818/issn14531305/28.1.2024.02.

Manzoor, J. *et al.* (2024). 'Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs', *PloS One*, 19(3), p. e0301183. https://doi.org/10.1371/journal.pone.0301183.

Microsoft (2022). 'Appendix L: Events to Monitor', *Microsoft official documentation*, 18 June, Available at: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor (Accessed: 19 May 2024).

Miloslavskaya, N. and Tolstoy, A. (2019). 'New SIEM system for the internet of things', *Advances in intelligent systems and computing*, pp. 317–327. https://doi.org/10.1007/978-3-030-16184-2_31.

Mokalled, H. *et al.* (2019). 'The Applicability of a SIEM Solution: Requirements and evaluation', *IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*, pp.132-137. https://doi.org/10.1109/wetice.2019.00036.

Mokalled, H. *et al.* (2020). 'The guidelines to adopt an applicable SIEM solution', *Journal of Information Security*, 11(01), pp. 46–70. https://doi.org/10.4236/jis.2020.111003.

Nabil, M. *et al.* (2017). 'SIEM selection criteria for an efficient contextual security', *2017 International Symposium on Networks, Computers and Communications (ISNCC)*, pp. 1-6. https://doi.org/10.1109/isncc.2017.8072035.

Passeri, Paolo (2024). '2024 Cyber Attacks Statistics', 26 March. Available at: https://www.hackmageddon.com/2024/03/26/2024-cyber-attacks-statistics/ (Accessed: 2 June 2024).

Patton B. (2019). 'SIEM Integration Best Practices: Making the Most of Your Security Event Logs', *Quest Software White Paper*. Available at: https://www.quest.com/whitepaper/siem-integration-best-practices8139415 (Accessed: 19 May 2024).

Podzins, O. and Romanovs, A. (2019). 'Why SIEM is Irreplaceable in a Secure IT Environment?', *2019 Open Conference of Electrical, Electronic and Information Sciences (eStream)*, pp.1-5. https://doi.org/10.1109/estream.2019.8732173.

Sadowski, G., Kavanagh K., and Bussa T. (2020). 'Critical capabilities for security information and event management.', *Gartner Group Research Note*, 24 February. Available at: https://www.gartner.com/en/documents/3981260 (Accessed: 1 June 2024).

Scarfone, K. (2018). '*Seven criteria for evaluating today’s leading SIEM tools*'. Available at: http://searchsecurity.techtarget.com/feature/Comparing-the-best-SIEM-systems-on-the-market (visited on 05/18/2024).

Schneider M., Davies A., and Shoard P. (2022). 'Critical capabilities for security information and event management', *Gartner Group Research Note*, 22 November. Available at: https://www.gartner.com/en/documents/4021424 (Accessed: 23 May 2024).

Sekharan, S.S. and Kandasamy, K. (2017). 'Profiling SIEM tools and correlation engines for security analytics', *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, pp. 717-721. https://doi.org/10.1109/wispnet.2017.8299855.

Skendzic, A., Kovacic, B. and Balon, B. (2022). 'Management and Monitoring Security Events in a Business Organization - SIEM system', *2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO)*, pp. 1203-1208. https://doi.org/10.23919/mipro55190.2022.9803428.

Thakur, K. *et al.* (2016). 'An Analysis of Information Security Event Managers', *2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud)*, pp. 210-215. https://doi.org/10.1109/cscloud.2016.19.

Vielberth, M. and Pernul, G. (2018). 'A security information and event management pattern', *12th Latin American Conference on Pattern Languages of Programs (SugarLoafPLoP 2018)*, pp. 1-12. https://doi.org/10.5283/epub.41139.

Webster, J., and Watson, R.T. (2002). 'Analyzing the Past to Prepare for the Future: Writing a Literature Review', *MIS Quarterly*, 26(3), pp. xiii–xxiii.

Wolfswinkel, J.F., Furtmueller, E., and Wilderom, C.P.M. (2013). 'Using grounded theory as a method for rigorously reviewing literature.', *European Journal of Information Systems*, 22(1), pp. 45–55. https://doi.org/10.1057/ejis.2011.51.

Yadav, M., and Mishra, D. S. (2021). 'Study of challenges faced by Enterprises using Security Information and Event Management (SIEM)', *Journal of University of Shanghai for Science and Technology*, 23(8), pp. 511-522. Available at: https://jusst.org/wp-content/uploads/2021/08/Study-of-challenges-faced-by-Enterprises-using-Security.pdf (Accessed: 25 May 2024).

Žgela, M., and Penga, I. (2019). 'Security Information and Event Management–Capabilities, Challenges and Event Analysis in the Complex IT System', *Central European Conference on Information and Intelligent Systems*, pp. 259-266. Available at: https://www.proquest.com/openview/4d4bac43b7c2bce82f3d54cc1b380f25/1?pq-origsite=gscholar&cbl=1986354 (Accessed: 2 June 2024).