2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)

The applicability of a SIEM solution: Requirements and Evaluation

Hassan Mokalled
Dipartimento di ingeneria navale, elettrica, elettronica e delle telecomunicazioni
University of Genoa, Italy
Cyber security assurance and control department
Hitachi Rail STS Company
Genoa, Italy
hassan.mokalled.ext@hitachirail.com

Rosario Catelli
Dipartimento di ingegneria elettrica e delle tecnologie dell'informazione,
University of Naples, Italy
Cyber security assurance and control department
Hitachi Rail STS Company
Naples, Italy
rosario.catelli@unina.it

Valentina Casola
Dipartimento di ingegneria elettrica e delle tecnologie dell'informazione,
University of Naples, Italy
Naples, Italy
valentina.casola@unina.it

Daniele Debertol
Cyber security assurance and control department
Hitachi Rail STS Company
Genoa, Italy
daniele.debertol@hitachirail.com

Ermete Meda
Cyber security assurance and control department
Hitachi Rail STS Company
Genoa, Italy
ermete.meda@hitachirail.com

Rodolfo Zunino
Dipartimento di ingeneria navale, elettrica, elettronica e delle telecomunicazioni
University of Genoa
Genoa, Italy
rodolfo.zunino@unige.it

***Abstract* — The need for SIEM systems increased in the last few years, especially as cyber-attacks are evolving and targeting enterprises, which may cause discontinuity of their services, leakage of their data, and affect their reputation. Cybersecurity breaches can range from no or limited impact to stealing or manipulation of data, or even taking control of systems. Many companies seek to reinforce their security capabilities to better safeguard against cybersecurity threats, so they adopt multi-layered security strategies that include using a SIEM solution. A significant factor for the increasing adoption of SIEMs is the capabilities that such systems offer, being able to provide near-real time analysis of security alerts and logs generated from various set of sources within an organization IT infrastructure. However, implementing a SIEM solution is not just an installation phase that fits any scenario within any organization; the best SIEM system for an organization may not be suitable at all for another one. An organization should consider other factors along with the technical side when evaluating a SIEM solution. This paper proposes an approach to aid enterprises, in selecting the most suitable SIEM solution; it suggests technical and organizational requirements that should be addressed and examines the SIEM applicability using quantitative and qualitative evaluation criteria.**

Keywords — SIEM, Security Information and Event Management, requirements, evaluation, cybersecurity, SOC, Security Operation Centre

I. INTRODUCTION

Information and communication technology (ICT) has made a remarkable impact on the society. Nowadays most of the companies rely on information and communication technology, this puts their assets under certain risks especially cyber ones, hence they must be kept under control by means of security countermeasures that generate confidence in the use of these assets [1]. Companies all over the world need to ensure valuable assets, uninterrupted business operation (processes), reliable data and quality of service (QoS) to various groups of users [10][16]. They need to protect their clients and employees both inside and outside organization [2]. According to Gartner by 2020, 30% of global enterprises will have been directly compromised by an independent group of cybercriminals or cyber activists. Moreover, in 60% of network breaches, hackers compromise the network within minutes [3]. On the other hand, the companies' IT environment is getting more complex, involving many security appliances that may contribute to security strategy in business processes. Therefore, organizations started to invest on integrating SIEMs (Security Information and Event Management) to improve their security.

The term SIEM was introduced by Gartner in 2005. The SIEM system has replaced two types of systems before separated – Security Information Management (SIM) and Security Event Management (SEM) systems [4]. The former provided long-term storage, analysis and reporting, while the latter collected events in real time. Their combination yearned for near real-time analysis, to send notifications and represent information at an operator's console in charge for taking defensive actions. Overall, SIEM system combines SIM and SEM functionalities into one security management system, which collects and correlates relevant data from multiple sources, outputs reports, identifies deviations and takes appropriate actions. For example, when a potential issue is detected, SIEM might log it as a new information, generate an alert and instruct other security controls to stop any activity progress. Gartner estimates the SIEM market will grow at a compound annual growth rate (CAGR) of 9.5% between 2016 and 2022, and the worldwide spending on SIEM will reach 3.72 billion dollars [13].

From an organization perspective, the challenge is not just about selecting any SIEM solution but implementing the right solution that fits better within company structure and is aligned with the existing threats landscape. In addition, it must be flexible enough to be easily adapted to meet any changes thereafter. Security and risk management (SRM) leaders evaluating SIEM solutions must understand their use cases and then define specific requirements in conjunction with applicable stakeholders and company strategy in general [12].

On the other hand, organizations must require a structured approach for managing their challenges. This will ensure that there are agreed objectives, good management controls in

978-1-7281-0676-2/19/$31.00 ©2019 IEEE
DOI 10.1109/WETICE.2019.00036

place and effective monitoring of performance to keep on track and avoid unexpected outcomes. So, this paper proposes not just technological but pragmatic approach to support companies that are seeking to adopt SIEM systems into their environments, suggesting suitable answers to preferred requirements that are believed to be valuable prerequisites a SIEM system should have. The aim of the proposed approach is to advice a pre-installation strategy, a way to evaluate functional components that a SIEM should comprise in terms of both technical and organizational requirements, and to suggest criteria to judge SIEM systems using an evaluation process composed of quantitative and qualitative methods.

However, and because of the complexity, precision, thoroughness of this work, it is mainly dedicated to large enterprises, which include wide variety of broad and specific skills and several specialists to manage certain applications or parts of the IT infrastructure, and most of them comprise a dedicated department to manage the information security. Therefore, this approach can be followed by those bigger enterprises that in general tend to manage their work in a very structured manner, and they need to assert successful management and performance, and this is our goal, to aid in following a thorough approach for the issue. This approach represents the first and primary phase in the procedure of choosing a SIEM or a set of qualified SIEMs, however, it has to be followed by a testing phase that enable the customer to check the solution directly after the installation. The remainder of this paper is structured as follows: After this introduction, section II will briefly report a background about main high-level features of SIEM systems and related works. In section III we describe the main aspects that should be addressed before adopting a SIEM solution. In section IV we present our proposed approach. Finally, section V presents the conclusion.

II. Backgrounds and related works

A. *SIEM system: Definitions*

There is a plethora of features regarding SIEM systems, which are developed differently by each vendor. In general, SIEM collects, normalizes and aggregates event data produced by security devices, network infrastructure, systems, and applications. Event data is combined with contextual information about users, assets, threats and vulnerabilities. SIEM systems could be agentless and agent based [5, 6], or even hybrid (using both agent and agentless) and may adopt new technologies such as HEC (Http Event Collection). Agentless means that the log-source transmits its logs to the SIEM, or an intermediate logging server involved, such as a syslog server; while agent-based means that an agent is installed on a source-log to gather security events from the endpoint itself. Today, most SIEM systems work deploying multiple collection agents (collectors) in a hierarchical manner. Log collectors forward events to a centralized management console, which performs inspections and flags anomalies [2]. Then after collection, the data should be normalized so it can be correlated and analysed. Another feature is the pre-filtering that is related to processing centre, some systems use a pre-processing mechanism at the edge collectors, with only certain events being passed through to a centralized management node. In this way, the volume of information being communicated and stored can be reduced.

SIEM technology provides near real-time correlation of events for security monitoring, query and analytics for historical analysis and other support for incident investigation, compliance reporting, and alerting [7]. According to Gartner in [12], by 2020, 75% of all security information and event management (SIEM) solutions will use big data technologies at their core, along with machine learning, to improve threat detection and response capabilities. In short, there are so many SIEM systems in the market created by skilled and expert security vendors with their own features that selecting the suitable SIEM is not a trivial task anymore: it is not simply about installing the most powerful one, for instance, a very powerful SIEM may be too complex to apply in some cases.

B. *Related works*

Several studies were conducted in the field of “How to select a SIEM system”. Gartner reports are an excellent example where they present a detailed evaluation of the current SIEM products based on many characteristics such as sales execution, pricing, costumer experience, marketing message evaluation against the understanding of customer needs [7][8][12]. [7] examined different SIEM products that are the leaders of SIEM technology, they focused on technical requirements and showed strengths and cautions for each vendor and at the end they defined evaluation criteria from an Ability-to-execute point of view. In [12] analysts defined a list of critical capabilities that a SIEM should include and suggested 3 general different use cases: Basic Security Monitoring, Complex Security Monitoring, Advanced Threat Defence. They used an evaluation criterion to evaluate the most powerful SIEM products available, which is based on the defined critical capabilities and the three different scenarios. [9] provided environment-specific criteria to benchmark SIEM solutions, where organizations should consider factors like events-per-second (EPS), considering the number of employees in each sub-net, number of data-bases, and the ability to store and analyse these events, in order to evaluate and even design a SIEM system. In [11] Nabil et al. proposed an after-installation evaluation approach: such an approach may be time-consuming for companies, and it should be preceded by a PRE-installation evaluation approach that qualifies and select the applicable SIEMs from the plethora of solutions available before installing them.

III. Aspects to be addressed before adopting a SIEM solution

Before starting the procedure of choosing a SIEM and following the proposed approach, it is essential to consider some general aspects that could influence the technical and the organizational evaluation of the solution. Companies must understand completely the problems they are trying to solve, considering aspects such as company type, its assets, what to secure, internal policies and external regulations. This task could seem easy, but it worth noting that assessing business and technical requirements a SIEM should have it is a lot more than a basic exercise.

To select an appropriate SIEM, the customer should prepare a list of requirements to describe the needs sought in the SIEM, usually described in a request-for-proposal (RFP) documents. However, before defining those requirements (section 4.A), some general aspects that affect the SIEM selection should be examined, and the Security and risk management (SRM) leaders must include at least the following considerations as a first step:

- **The company**

Companies may differ by vertical, size, location, and other factors that may affect their decisions. Each company has its own information system and architecture, some companies could be geographical distributed, and require high availability services, and may generate enormous logs with different formats.

- **Prioritizing assets and risks**

It is necessary to conduct an overall study to identify and evaluate the most critical assets and their corresponding risks in order to specify the most important targets of the monitoring and defensive activities of the SIEM system. The goal is to identify odds and costs if something wretched happened. Prioritizing risks helps in selecting what logs are more important, to give them high priority when installing the SIEM for more efficient correlation and reporting.

- **Compliance, regulations and forensics capability**

The company might be impacted by internal or external regulations. Compliance could be like conforming to international standards, or internal policies. For example, in some cases, it may be necessary to keep collectors on site to secure data in the place of origin, based on a specific state or country regulation, hence the entire deployment will be affected with such regulations, and so they should be considered. On the other hand, forensics should be addressed from two sides, the first is about ensuring, once collected, the logs were not altered and their integrity were preserved, the other side of forensics is that the SIEM should support incident management and investigation activities.

- **Security Operation Centre**

One essential aspect is about who will own, maintain and operate this new technology. SOC is a centralized unit that deals with security issues on an organizational level made up of a team primarily composed of security analysts (and operators) organized to detect, analyse, respond to, report on, and prevent security incidents in order to minimize risks [6]. This choice is part of a more general view oriented to the integration into company IT environment and effort needed to maintain such a system during license lifetime. And so, in the selection of a SIEM, the responsible should be aware of who will operate the SIEM, and if they can operate the selected SIEM platform or by considering the training costs.

- **Human and technological aspects**

Finally, an important aspect that should be also considered is to gather feedback from inside the organization about the IT resources and capabilities to support a specific SIEM product and potentially overlapping technologies in order to release IT means and personnel and skills to be allocated in this activity. Moreover, the organization should be aware about how the selected platform must be easily integrated in the technology environment of the company.

IV. A SIEM SELECTION APPROACH: REQUIREMENTS AND EVALUATION

What characterizes our work is that it proposes an overall approach for the problem of selecting the applicable SIEM solution, and searching the previous work will show how few, if no similar comprehensive approaches were proposed. Some of the work done focused just on the technical requirements without addressing the organizational ones, and other aspects. Others did not consider the problem of applicability or integration in the environment.

Saving time, using a systematic-organized strategy for decision-making and balancing costs to needs are the main advantages of adopting such an approach. This approach starts by suggesting the requirements (technical and organizational) that should be addressed in a SIEM solution in a systematic way, and then proposes a methodology for evaluating SIEM solutions that measures the compliance and applicability of any SIEM solution using a quantitative and qualitative methods. This evaluation methodology is split into two phases, 1) Quantifying each requirement of the SIEM solution using a quantitative based method and 2) Measuring the applicability of the solution using a qualitative based method after defining a list of indicators that enables the evaluation of this applicability. The goal is to select the appropriate SIEM that matches a company's environment and resources, however we stress that at the end an installation-testing phase must be accomplished with the suppliers to make sure about the compliance of the selected solution to the needs addressed.

A. Technical and Organizational SIEM Requirements:

Information security and risk management leaders responsible for security operations should focus their evaluation on the critical capabilities that align with their use cases, requirements, and current and future IT environments (e.g., on-premises versus cloud-based services) [12].

This section groups the technical requirements needed in order to adopt a SIEM platform covering in detail the mandatory and advanced or nice-to-have requirements, as listed in Table 1.

Table 1 SIEM requirements

Section	Type	Requirement
Platform	**Mandatory**	*1. Log Management System capability* *2. Supporting an extended set of log sources* *3. Customization of parsers/connectors* *4. Method for retrieving events/flows/logs* *5. Specification of the method for retrieving events/flows/logs* *6. Hierarchical and modular/scalable architecture* *7. Time-zones management* *8. Platform computing capacity* *9. Platform storage capacity* *10. Installation model* *11. High Availability/caching options* *12. Availability of both default and customizable correlation rules* *13. Dashboard features: ability to quickly prioritize response and analysis.* *14. Customizable and compliance reports* *15. Alerting capabilities* *16. Technical documentation and online help* *17. Ability of Monitoring the platform*
	Nice to have	*18. Multi-tenant capabilities (views)* *19. Anonymization of logs*
Operations	**Mandatory**	*1. Role-based access control* *2. Accounting: log events done by operators*

	Nice to have	*3. Customizable time-zones for the GUI*
Integration	**Mandatory**	*1. Active Directory integration for administrative management*
	Nice to have	*2. Integration with asset management tools* *3. Case Management and trouble-ticketing activities tracking* *4. Trouble ticketing module* *5. Integration with vulnerability management tools*
Advanced features	**Nice to have**	*1. Threat Intelligence analysis tools support* *2. Support for forensics analysis activities* *3. Analytics support* *4. Automatic response capabilities*
Licensing and support	**Mandatory**	*1. Specification of the preferred License type* *2. Specification of the project Roadmap* *3. Delayed license activation* *4. Technical assistance support and professional services*
	Nice to have	*5. Technical assistance support and professional services* *6. Training provided*

Those requirements represent the needs of the customer, they cover all the features and services that the supplier should include when proposing a SIEM solution. Defining requirements is an important task; it helps the companies to define their needs, be aware of any shortage, and aids them in the evaluation phase. Requirements are divided into 5 sections: platform, operations, Integration, advanced features and licensing-support services. Each section includes a set of mandatory and nice-to-have requirements listed in table 1.

a. **Platform:** Describes the technical requirements needed in the platform.
b. **Operations:** Groups the requirements needed to manage the solution.
c. **Integration:** This section groups the requirements needed to integrate the SIEM solution into the Company's information system.
d. **Advanced features:** This section describes the advanced features, they could be considered as nice-to-have requirements.
e. **Licensing and support:** This section lists and describes the licensing and support services requirement.

B. Measuring the compliance and applicability of a SIEM: An evaluation process

Evaluation is the structured interpretation and giving of meaning to predicted or actual impacts of proposals or results. It looks at original objectives, and at what is either predicted or what was accomplished and how it was accomplished [14]. It can assist an organization to assess and help in decision-making; or to ascertain the degree of achievement or value about the aim and objectives and results of any action. Evaluation is methodologically diverse; two types of methods may be qualitative or quantitative. Quantitative methods are distinguished by emphasis on numbers, measurement, experimental design, and statistical analysis [15], and hopes the numbers will yield an unbiased result that can be generalized to some larger population. However, qualitative methods evaluate other parameters such the success and the eligibility of a product in a specific environment using non-numerical (textual forms) data to assess the eligibility and reliability of adopting the solution, such as the use of internal discussions, interviews, comparisons to provide feedbacks, etc. Both quantitative and qualitative evaluation methods have their benefits, quantitative evaluation can help remove human bias, thus more accurate. However, qualitative evaluations may also involve truths, but these truths are harder to get at, and evaluators may not always agree. In our approach, an evaluation process is proposed; it is applied after receiving the description of the SIEM solution from suppliers. It is divided into two methods of type quantitative and qualitative. The first method "Requirements-based Evaluation" is the quantitative side of the evaluation process; it evaluates the degree of compliance for each requirement of the received SIEM solution using numerical values and mathematical operations. This method is applied to the SIEM solutions that might be adopted and used to obtain a list of qualified ones as an output. After that, the output of this method is then provided as input to the second method (see the flowchart in figure 1).

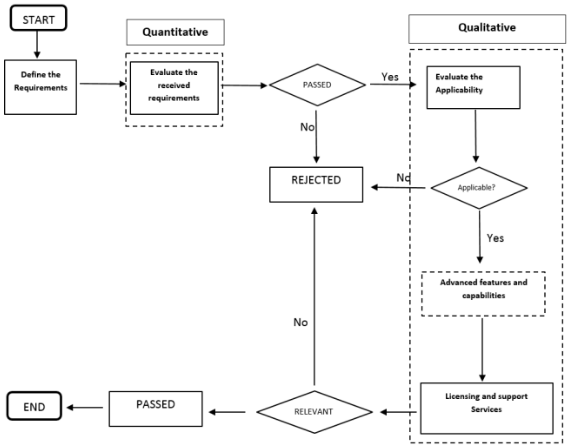
START
Quantitative
Qualitative
Define the Requirements
Evaluate the received requirements
PASSED
Yes
Evaluate the Applicability
No
REJECTED
No
Applicable?
Yes
Advanced features and capabilities
No
END
PASSED
RELEVANT
Licensing and support Services

Figure 1. How to apply the overall approach

On the other hand, the second method "Applicability Evaluation" represents the qualitative side of this evaluation process, it focuses on the observations, interpretation and the opinion of the concerned parties, rather than going into measuring the value of each requirement of the received SIEM solution. Both methods are complementary in the evaluation process, using both helps in getting a deeper understanding and obtaining a precise and flexible evaluation. The quantitative side represents the accuracy that evaluates and qualify a set of SIEMs, however the qualitative side represents the flexibility, where the evaluators add their analysis, opinion and understanding to compare the qualified solutions and finally to select the most applicable one. Figure 1 shows how to apply the approach starting by defining the requirements that the customer seeks in their SIEM product, then evaluating the received ones using the proposed evaluation process described in the next section.

1) Compliance measurement: A Quantitative Requirement-Based Evaluation Method

The first evaluation method measures the degree of compliance of each requirement in the SIEM solution that might be adopted, it is a first step evaluation. After receiving the tenders from diverse suppliers proposing a SIEM solution, security and risk management (SRM) leaders evaluate each SIEM solution separately, where each requirement is evaluated to get a total score for the whole solution. Each requirement is assigned two different parameters which are the requirement value (V) and the weight (W). The requirement value is the grade assigned to evaluate the answer-to-requirement in the under-evaluation SIEM solution, while the weight represents the importance of current requirement in the solution from the user point of view, and is assigned initially when the customer defines his requirements, for example, a mandatory requirement has a high value compared to nice-to-have ones. And then, a score(S) is calculated for each requirement ($S= V*W$), and after that a total for each requirement section is computed. Finally, the total score is obtained by adding all the totals corresponding the requirements family sections. Table 2 is suggests an example to use in applying this evaluation method.

For a better evaluation, a scale is suggested, it represents the requirement value (V). This scale is used to be able to differentiate between an insufficient, good, very good, and perfect requirement proposed by the supplier, by translating the level of compliance of the under-evaluation requirement into a numerical value. A non-linear growth scale is suggested to be used because of its ability to differentiate between the values using the high growth rate.

At the end, evaluators may define a passing grade to use to select the qualified "under-evaluation SIEM solutions, so they can directly reject a solution with lower total score. The output of this method should be several succeeded SIEM solutions which all complied the defined requirements, but the end one solution should be adopted, and this is the role of the second evaluation method, which examines the applicability.

Table 2. Requirement-based Evaluation

SIEM X	Requirement	Requirement Value(V)	Weight(W)	Score(s)	Total
PLATFORM	a_1 . . A_{19}	$V(a_1)$ . . $V(a_{19})$	$W(a_1)$ $W(a_{19})$	$V(a_1)*W(a_1)$ $Va_{19}*Wa_{19}$	$\sum_{i=1}^{19} V(ai) * W(ai)$
OPERATIONS	b_1 . b_3	$V(b_1)$. $V(b_3)$	$W(b_1)$. $W(b_3)$	$V(b_1)*W(b_1)$. $V(b_3)*W(b_3)$	$\sum_{i=1}^{3} V(bi) * W(bi)$
INTERGRATIONS	c_1 . . c_5	$V(c_1)$ . . $V(c_5)$	$W(c_1)$ . . $W(c_5)$	$V(c_1)* W(c_1)$ . . $V(c_5)*W(c_5)$	$\sum_{i=1}^{5} V(ci) * W(ci)$
ADVANCED FEATRES	d_1 . . . d_4	Vd_1 . . . Vd_4	Wd_1 . . . Wd_4	. . .	$\sum_{i=1}^{4} Vdi * Wdi$
LICENSING AND SUPPORT	e_1 . . e_6	Ve_1 . . Ve_6	. . .	. . .	$\sum_{i=1}^{6} vei * wei$
			TOTAL SCORE		∑: Total

2) *Applicability Evaluation: A Qualitative method*

Security and risk management leaders increasingly seek SIEM solutions with capabilities that support early targeted attack detection and response. Users must balance advanced SIEM capabilities with the resources needed to run and tune the solution [7]. The best SIEM system for an organization may not be suitable at all for another. Other variations should be considered along with the technical side when evaluating a SIEM solution. Therefore, the qualitative side of the approach takes place; it is about examining the whole solution in terms of applicability rather than measuring mathematically the value of each requirement. The highest-grade solution is not always the choice, it may have powerful features, but too complex to install, or even too expensive. This method aims to evaluate the qualified SIEM solutions in a high-level manner. It does not aim to evaluate technically each solution, however, to examine the applicability of them. In such method, a unified scale is followed, and a set of INDICATORS is used to evaluate and compare, without going deeply into technical details as in the requirement-based evaluation. Weight, evaluation, notes are other parameters used, and described below.

a) Indicators:

INDICATORS are grouped into families, and have different weights (High, medium, and low), where some are key factors in the selection process more than others are. They help adequately evaluate technology solution vendors and then decide which solution is the best fit.

THE PLATFORM

The "platform" family-of-indicators is an answer for the following question: Is the proposed solution applicable in our case? This section encompasses the following list of indicators and should be considered important.

- **Compliance:** the compliance indicator represents to what extent is the proposed solution compliant. In other words, it evaluates the compliance of the mandatory requirements or the existence of non-compliant requirements. Take into account the restrictions, constraints, regulations or policies that prevent the implementation of such solution: e.g., kind of the solution proposed: software/hardware.

- **Quality of services:** a general evaluation for the Quality of the services, capabilities that the solution offers?

- **Robust Architecture:** evaluates the proposed architecture of the solution, the deployment, and if this architecture preserves a high availability.

- **Scalability:** evaluates the ease and the ability of the solution to grow, in terms of adding additional features in the future, e.g.: adding additional licenses, etc.

- **Complexity of the solution:** this indicator evaluates the Applicability of the platform (platform kind, number of nodes, etc.), ease of deployment, level of integration, relevance: E.g. The user does not need to modify or develop something hard to integrate the solution.

- **Clearness:** evaluates the clearness of description of the SIEM solution (e.g. Does the received RFP include a complete description or is there something ambiguous?).

LICENSING AND SUPPORT SERVICES

- **Duration**: evaluation of the planned duration by the supplier to install the solution: Does it have a clear roadmap.

- **Licensing**: evaluates the type of the licensing offered by the supplier (license or other purchase options, e.g. leasing), and evaluates if the activation starts after the end of the acceptance tests in which all the project requirements will be met.

- **The support**: evaluation for the availability of the technical support (e.g. 7 days/ week and 24h/24h)

- **Training**: evaluates the training level provided.

ADVANCED FEATURES:

- **Support additional features:** Evaluation of the available advanced features or additional ones.

- **Integration with third parties:** How much the solution can be integrated with 3rd-party tools, or just restricted or limited.

Other Indicators

- **Skill of the supplier/ vendor**: Does the supplier or vendor has the expertise in this field, their popularity, the services they offer.

- **The price:** Represents an important indicator in the selection process; and a cost-effective option should be selected.

b) Weight

It corresponds to the weight of the indicator that will be evaluated; the weight in terms of its relative importance in the whole solution, weight could take different values such as high, medium or low. It is up to the evaluator to assign those values based on their own needs and addressing related aspects.

c) Evaluation

An evaluation is defined for each indicator. The evaluation is carried out based on the eligibility and reliability. Values could be insufficient, good, very good, perfect.

d) Notes

Any additional note, which the evaluator considers and should be highlighted. It could be the team's general conclusion drawn up based on the described solution in each tender.

Table 3. Applicability Evaluation for each SIEM solution

SIEM X	*Indicators*	*Importance or weight*	*Evaluation*	NOTES
Applicability	Level of Compliance			
	Complexity and Relevance			
	Quality of services/ capabilities			
	Robust Architecture			
	Scalability			
	Clearness/ complete description/ vision			
Licensing and support services	Installation duration/ clearness of road map			
	Licensing			
	Support			
	Training			
Advanced Features	Additional features			
	Intergradation with third parties			
Other indicators	Expertise/Skill of Vendor/ Supplier			
	Price			
		OVERALL	RESULT	ACCEPTED REJECTED

Table 3 shows a model (table-form) to use in applying this proposed method in an easy way.

At the end, the suggested indicators may intersect or overlap, so the evaluators may merge some together or even split others. On the other hand, each organization may assign a different weight for those indicators based on the requirements they need, policies, regulations, etc.

V. Conclusion

In conclusion, organizations tend to ensure good management controls are in place to avoid unexpected outcomes and to keep on track, so they require a structured approach for managing their tasks. This paper proposed a thorough approach to support companies that are seeking to adopt SIEM systems into their environments, it suggests suitable technological and business requirements that are believed to be valuable in a SIEM system and proposes a two-phase evaluation process to measure the compliance and applicability of a SIEM. At the end, as said before, this approach must be completed by a testing phase of the selected SIEM to confirm that the received requirements are as described by the suppliers.

VI. References

[1] Mokalled H., Pragliola C., Debertol D., Meda E., Zunino R. (2019) A Comprehensive Framework for the Security Risk Management of Cyber-Physical Systems. In: Flammini F. (eds) Resilience of Cyber-Physical Systems. Advanced Sciences and Technologies for Security Applications. Springer, Cham

[2] Natalia Miloslavskaya, Analysis of SIEM Systems and Their Usage in Security Operations and Security Intelligence Centers, 2017.

[3] Verizon in the Data Breach Investigations Report, 2015

[4] IBM Corporation: IT Security Compliance Management Design Guide with IBM Tivoli Security Information and Event Manager. 2nd edn. (2010) http://www.redbooks.ibm.com/abstracts/sg247530.html?Open. Accessed March 1st 2019.

[5] Techtarget: Security information and event management (SIEM) (2014). http://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM. Accessed March 1st 2019

[6] Scarfone, K.: Introduction to SIEM services and products (2015). http://searchsecurity.techtarget.com/feature/Introduction-to-SIEM-services-and-products. Accessed March 1st 2019

[7] Kelly Kavanagh, Toby Bussa, Gorka Sadowski, Magic Quadrant for Security Information and Event Management. Gartner MQ for Security Information and Event Management, December 2018.

[8] O. Rochford, K.M. Kavanagh, T. Bussa, Critical Capabilities for Security Information and Event Management, 2016.

[9] SANS Institute InfoSec Reading Room, Benchmarking Security Information Event Management (SIEM), 2009.

[10] An AHP-based framework for quality and security evaluation Casola, V., Fasolino, A.R., Mazzocca, N., Tramontana, P. 2009 Proceedings - 12th IEEE International Conference on Computational Science and Engineering, CSE 2009 3,5283262, pp. 405-411.

[11] M. Nabil, S. Soukainat, A. Lakbabi and O. Ghizlane, "SIEM selection criteria for an efficient contextual security," *2017 International Symposium on Networks, Computers and Communications (ISNCC)*, Marrakech, 2017, pp. 1-6.

[12] Toby Bussa, Kelly Kavanagh, Gorka Sadowski, Critical Capabilites for security Information and Event management: Gartner, Decemeber 2018.

[13] Gorka Sadowski, kelly kavanagh, Toby Bussa, Technology Insight for the modern SIEM, Gartnet Inc, October 2018.

[14] Michael Scriven, "The methodology of evaluation". In Stake, R. E. Curriculum evaluation. Chicago: Rand McNally. American Educational Research Association (monograph series on evaluation, no. 1. (1967).

[15] Palomba, C. and Banta, T.W. (1999) Assessment Essentials: Planning, Implementing, and Improving Assessment in Higher Education. Jossey-Bass, Inc., San Francisco.

[16] A policy-based evaluation framework for quality and security in service oriented architectures Casola, V., Fasolino, A.R., Mazzocca, N., Tramontana, P. 2007 Proceedings - 2007 IEEE International Conference on Web Services, ICWS 2007 4279735, pp. 1181-1182.