Scientific Research Publishing

Journal of Information Security, 2020, 11, 46-70
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

The Guidelines to Adopt an Applicable SIEM Solution

Hassan Mokalled[1,2,3], Rosario Catelli[4,5], Valentina Casola[5], Daniele Debertol[1], Ermete Meda[1], Rodolfo Zunino[2]

[1]Cyber Security Assurance and Control Department, Hitachi Rail STS, Genoa, Italy
[2]Dipartimento di ingeneria navale, elettrica, elettronica e delle telecomunicazioni, University of Genoa, Genoa, Italy
[3]MECRL Lab, EDST, Lebanese University, Beirut, Lebanon
[4]Cyber Security Assurance and Control Department, Hitachi Rail STS, Napoli, Italy
[5]Dipartimento di ingeneria elettrica e delle tecnologie dell'informazione, University of Naples, Naples, Italy
Email: hassan.mok7@gmail.com

How to cite this paper: Mokalled, H., Catelli, R., Casola, V., Debertol, D., Meda, E. and Zunino, R. (2020) The Guidelines to Adopt an Applicable SIEM Solution. *Journal of Information Security*, **11**, 46-70.
https://doi.org/10.4236/jis.2020.111003

Received: October 7, 2019
Accepted: December 10, 2019
Published: December 13, 2019

Abstract

The need for SIEM (Security Information and even Management) systems increased in the last years. 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. 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 an applicable SIEM. It starts by suggesting the requirements that should be addressed in a SIEM using a systematic way, and then proposes a methodology for evaluating SIEM solutions that measures the compliance and applicability of any SIEM solution. This approach aims 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 an SIEM system should have; and to suggest criteria to judge SIEM systems using an evaluation process composed of quantitative and qualitative methods. This approach, unlike others, is customer driven which means that customer needs are taken into account when following the whole approach, specifically when defining the requirements and then evaluating the suppliers' solutions.

Keywords

SIEM, Security Information and Event Management, Requirements, Evaluation, Cybersecurity

1. Introduction

Information and communication technology (ICT) has made a remarkable impact on the society. Companies nowadays rely on information and communication technology which 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 [2] [3]. They need to protect their clients and employees both inside and outside the organization [4]. 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 [5]. On the other hand, 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 in 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 [6]. 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 of 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 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 [7].

From an organization perspective, the challenge is not just about selecting any SIEM 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 [8].

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 place and effective monitoring of performance to keep on track and avoid unexpected outcomes. Therefore, 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. This approach proposes the requirements 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 quantitative and qualitative methods. The goal is to select the appropriate SIEM that fits best in company's environment. However, and because of the complexity, precision and thoroughness required to apply our whole approach, 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 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 work 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 2 will briefly report a background about main high-level features of SIEM systems and related works. In Section 3, we present our proposed approach. Section 4 demonstrates how this approach is applied to select one solution among a set of SIEMs proposed and received by different suppliers, through defining both technological and organizational requirements that the customer seeks to have in the SIEM and evaluating the received SIEMs using the proposed quantitative and qualitative evaluation methods. After that, Section 5 compares this approach with similar existing work. Finally, Section 6 presents the conclusions.

2. Backgrounds and Related Works

2.1. 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 [9] [10], 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 by deploying multiple collection agents (collectors) in a hierarchical manner. Log collectors forward events to a centralized management console, which performs inspections and flags anomalies [4]. 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 center, 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 [11]. According to Gartner, by 2020, 75% of all SIEMs will use big data technologies at their core, along with machine learning, to improve threat detection and response capabilities [8]. In short, there are so many SIEM systems in the market created by skilled and expert security vendors with their own features; however, 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.

2.2. 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 [8] [11] [12]. In [11], authors 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. According to authors in [8], a list is defined containing the critical capabilities that a SIEM should include, and they suggested three different and general use cases to use in the evaluation: 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 suggested scenarios. [13] provided an 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 databases, and the ability to store and analyse these events, in order to evaluate and even design a SIEM system. [14] 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.

The common point between the above-defined related-work is that all of them are product driven, where the evaluation of the solution is for the product as a technical solution. However, our approach is customer driven, where the selection phase is not only based on the technical features of the product but also subject to pre-defined customer's needs.

3. 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, 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. This approach, unlike others, is customer driven which means that customer needs are taken into account when following the approach, specifically when defining the requirements and then evaluating the suppliers' solutions. 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 quantitative and qualitative methods. This evaluation methodology is divided into two phases:

1) Quantifying each requirement of the received SIEM solution using a quantitative based method;

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 fits best in company's environment and resources; however, we stress that a final installation-testing phase must be accomplished with the suppliers to make sure about the compliance of the selected solution to the needs addressed. The time complexity of such an approach depends on more than one factor: First, since this approach is customer driven, it depends on the specification that the customer includes while setting the requirements, as larger enterprises might require in-depth specification of requirements. In addition, the evaluation phase of the received SIEM solutions affects the time complexity of this approach also. It is recommended to adopt a cost-benefit analysis to select a set of the relevant and optimal (or even sub-optimal) solutions among the received solutions as some solutions might be absolutely complex and hard to implement in the customer's environment or they could cost more than the limit available, so there would be no need to waste time on the evaluation phase for those proposals. And this is taken into account in this approach when using both a qualitative and quantitative methodologies to evaluate.

3.1. Technical and Organizational SIEM Requirements:

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. 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 [8]. This section groups the requirements needed to adopt a SIEM platform covering in detail the "*mandatory*" and "*nice-to-have*" requirements. Those requirements represent the needs of the customer, they cover all the features and services that the supplier should include when proposing a SIEM, they are divided into 5 sections: platform, operations, integration, advanced features and licensing-support services, as listed in **Table 1**.

3.2. 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 [15]. 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 [16], 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: 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 (**Figure 1**).

On the other hand, the second method "*Applicability Evaluation*" represents the qualitative side of this evaluation process, it focuses on the observations,

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 prioritize response and analysis
		14) Customizable and compliance reports
		15) Alerting capabilities
		16) Technical documentation and online help
		17) Ability of Monitoring the platform
		18) Secure Software
		19) Context enrichment based on collected logs
		20) Support for collection of real-time and deferred logs
	Nice to have	1) Multi-tenant capabilities (views)
		2) Anonymization of logs
		3) Support MITRE ATT&CK correlation matrix
Operations	***Mandatory***	1) Role-based access control
		2) Accounting: log events done by operators
		3) Web interface for day-by-day operation
	Nice to have	1) Customizable time-zones for the GUI
Integration	***Mandatory***	1) Active Directory integration for administrative management
	Nice to have	1) Integration with asset management tools
		2) Case Management and trouble-ticketing activities tracking
		3) Trouble ticketing module
		4) 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) Licensing restrictions
		3) Specification of the project Roadmap
		4) Delayed license activation
		5) Technical assistance support and professional services
		6) Training provided

Platform: Describes the technical requirements needed in the platform; **Operations:** Groups the requirements needed to manage the solution; **Integration:** Groups the requirements needed to integrate the SIEM solution into the Company's information system; **Advanced features:** Describes the advanced features, they could be considered as nice-to-have requirements; **Licensing and support:** Describes the licensing and support services requirement.

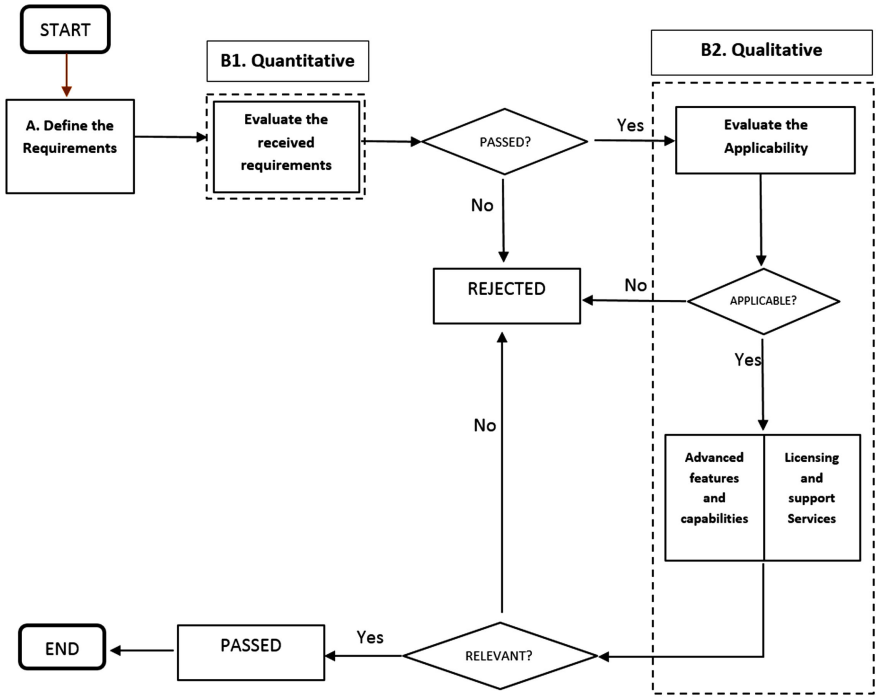

Figure 1. How to apply the overall approach.

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.

3.3. 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, SRM leaders evaluate each SIEM solution separately, where each requirement is evaluated to get a total score for the whole solution. Two different parameters are assigned to each and they are the requirement *value* (V) and the *weight* (W). 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 require-

ments, for example, a mandatory requirement has a high value compared to nice-to-have ones. Then, a *score* (S) is calculated for each requirement ($S = V * W$), and after that a total for each requirements section is computed. Finally, the total score is obtained by adding all the totals corresponding the requirements family sections. Table 2 is an example used in applying this evaluation method.

For a better evaluation, a scale is suggested to represent the requirement value (V). This scale is used to differentiate between an insufficient, good, very good, and excellent 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 a set of accepted SIEM solutions which all complied the defined requirements, but at the end one solution should be adopted, and this is the role of the second evaluation method, which examines the applicability.

Applicability Evaluation: A Qualitative Method

SRM leaders increasingly seek SIEMs 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 [11]. 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

Table 2. Requirement-based evaluation.

SIEM X	Requirement	Requirement Value (V)	Weight (W)	Score (s)	Total
Platform	a_1 a_{23}	$V(a_1)$ $V(a_{23})$	$W(a_1)$ $W(a_{23})$	$V(a_1) * W(a_1)$ $Va_{23} * Wa_{23}$	$\sum_{i=1}^{23} V(a_i) * W(a_i)$
Operations	b_1 b_4	$V(b_1)$ $V(b_4)$	$W(b_1)$ $W(b_4)$	$V(b_1) * W(b_1)$ $V(b_4) * W(b_4)$	$\sum_{i=1}^{4} V(b_i) * W(b_i)$
Integrations	c_1 c_5	$V(c_1)$ $V(c_5)$	$W(c_1)$ $W(c_5)$	$V(c_1) * W(c_1)$ $V(c_5) * W(c_5)$	$\sum_{i=1}^{5} V(c_i) * W(c_i)$
Advanced features	d_1 d_4	Vd_1 Vd_4	Wd_1 Wd_4		$\sum_{i=1}^{4} Vd_i * Wd_i$
Licensing and support	e_1 e_6	Ve_1 Ve_6			$\sum_{i=1}^{6} Ve_i * We_i$
		TOTAL SCORE			Σ: *Total*

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.

➢ **Indicators:**

Indicators are grouped into families, and might be assigned different weights (high, medium, and low), where some are key factors in the selection process more than others are. They help adequately evaluate qualitatively the solution and then decide which solution fits better.

The PLATFORM

The "platform" family-of-indicators assess the applicability of the proposed solution:

- **Compliance:** represents to what extent is the solution compliant. In other words, it evaluates the compliance of the mandatory requirements or the existence of non-compliant requirements, taking 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:** evaluates the level of complexity in terms of: ease of deployment, number of nodes, platform kind, integration, relevance, etc.
- **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 and roadmap**: Evaluation of the planned duration by the supplier to install the solution, and if it has a clear road map.
- **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 24 h/24 h).
- **Training**: evaluates the training level provided.

Advanced features:

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

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

Other Indicators

- **Skill of the supplier/vendor**: Examines if the supplier or vendor has the expertise in this field, and the services that it offers.
- **The price:** Represents an important indicator in the selection process and a cost-effective option should be selected.

➢ **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.

➢ **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, and excellent.

➢ **Notes:**

Notes could be the team's general conclusion drawn up based on the described solution in each tender (Table 3).

Table 3. Applicability evaluation for each SIEM solution.

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

4. Applying the Approach

The approach presented in this work was applied at Hitachi Rail STS Company. Hitachi Rail STS is a leading Company operating in the sector of high technology for Railway and Urban Transport [17]. To select a SIEM solution, the Company believes that a structured and systematic procedure should be followed, in an organized manner, which is the way Hitachi Rail STS tends to manage its challenges, *i.e.* ensuring that there are agreed objectives, good management controls in place to keep on track and avoid unexpected outcomes. Another main reason for selecting and adopting such an approach is to provide enhanced compliance and requirements coverage in bids.

4.1. Creating a Request-for-Proposal (RFP): Specifying SIEM Requirements

Specifying requirements is the first step while applying this approach. Therefore, a request-for-proposal (RFP) document (containing all the requirements that are believed to be *mandatory* or *nice-to-have* in the SIEM quest) was prepared and inspired by the SIEM requirement section of this approach, extending and describing briefly each requirement, to make the suppliers aware of the features that their solution should have to fit the customer needs. Following the approach, requirements are divided into 5 sections: platform, operations, integration, advanced features and licensing-support services, below is the requirements' part defined in the RFP document sent to the suppliers:

1) Platform:

a) Log Management System capability: The technical solution must address the collection, hashing, normalization, indexing, compression plus archiving, retention, (and all usual Log Management Systems' features) of events and log files along with aggregation, correlation, analysis, reporting and alerting.

b) SIEM platform kind: The supplier should provide details about the kind of SIEM platform available (for example hardware appliances or virtual appliances, or software only), where hardware is preferred in our case.

c) Supporting an extended set of log sources: The platform must be able to parse with native support the most widespread log sources, and a list of the mandatory ones must be listed by the supplier.

d) Customization of parsers/connectors: The platform should be able to support the creation of a library of customized parsers/connectors.

e) Method for retrieving events/flows/logs: The supplier should specify the method used for retrieving events/flows/logs (by agent/agentless support): and the customer must be aware about the relevant method that fits the case.

f) Hierarchical and modular/scalable architecture: The architecture should be scalable featured by unlocking license or adding modules, without the need of replacement and reconfiguration. Additional value if regional-based hierarchy is supported, with local collection and caching at main nodes and intelligent correlation at a central post.

g) Time-zones management: The SIEM architecture must support many different time-zone management capabilities, even up to providing time-zones when capturing log files which have none.

h) Platform computing capacity: The calculation to determine the appropriate number of sustained EPS and the EPS peak value proposed, should all be stated.

i) Platform storage capacity: The platform must be able to store the events/logs for an agreed period of time (e.g. in months) for a quick indexed access and for a long-term storage.

j) Installation model: The supplier should specify what installation model is available (e.g. on premise, private cloud or managed option).

k) High Availability/caching options: The redundancy/caching options should be available to avoid event/log file transfer losses in case of the distributed installation. Additional value if load balancing is possible among remote nodes while sustaining the same number of EPS.

l) Availability of both default and customizable correlation rules: The platform should include a set of standard correlation rules scenarios, and must be able to design further correlations rules.

m) Dashboard features: The dashboard should be able to quickly prioritize response and analysis.

n) Customizable and compliance reports: The supplier should provide details about the availability out of the box of compliance reports and the generation of customizable ones.

o) Alerting capabilities: Capability of triggering alerts, e.g. sending a notification message or email, and so to respond to incidents.

p) Technical documentation and online help: Availability of technical documentation, both with offline and online help.

q) Monitoring*:* The SIEM platform should be monitored using any standard protocol (e.g.: SNMP) so it can be added in the company's monitoring platform.

r) Secure Software: The supplier should state the SIEM platform operating system and version along with the "secure by design" techniques adopted.

s) Context enrichment based on collected logs: Availability of correlation rules to gather and merge information from the different log sources, to be able to provide all the info of the array [Mac, IP, hostname, username] whenever available somewhere in the logs.

t) Support for collection of real-time and deferred logs: The supplier should provide details about the support, normalization and indexing of logs retrieved in real-time and deferred way (e.g. sent by batch jobs).

u) Multi-tenant capabilities (views): The supplier should provide details about the SIEM solution capability to display some views based on connector grouping (e.g., connectors associated to different geographical entities or based upon management responsibilities like systems, DBs, network or security devices).

v) Anonymization of logs, e.g. for GDPR compliance: Provide details about

anonymization of logs (e.g., by at least masquerading privacy-related info to some profiles of users).

w) Support MITRE ATT&CK correlation matrix: Provide details about the support of TTP use detection of MITRE ATT & CK matrix.

2) Operations:

a) Role-based access control: The platform has to implement a role based access control mechanism suitable by the configuration of multiple user profiles owning different privileges to implement the accountability and separation of duties principles.

b) Accounting: The SIEM platform must have an audit log facility in order to track the activity relevant from the security perspective performed by operators.

c) Web interface for day-by-day operation: The SIEM platform interface used by users for daily analysis has to be web-based.

d) Customizable time-zones for the GUI: The interface must allow the user to choose in which time zone all the data must be displayed.

3) Integration. This section groups the requirements needed to integrate the SIEM solution into the Company's information system.

a) Active Directory integration for administrative management: The platform access must be granted only to qualified users authenticated and authorized via the Company's Active Directory database.

b) Integration with asset management tools: The ability to integrate the solution with asset management standard tools (e.g. Configuration Management Data Base).

c) Case Management and trouble-ticketing activities tracking: The ability to manage incident handling issues and the conditional support of standard IT trouble ticketing systems (workflows, prioritization, KB email exchange).

d) Trouble ticketing module*:* The supplier should provide details in case of the availability of a trouble ticketing system with the SIEM.

e) Integration with vulnerability management tools: A nice feature is the ability to integrate with vulnerability management tools.

4) Advanced features. This section describes the advanced features, they could be considered as *nice-to-have* requirements.

a) Threat Intelligence analysis tools support: Availability of threat analysis tools is a plus if already available by the vendor and by using standard formats for exchange such as: STIX, TAXII, IoC, other standard formats.

b) Support for forensics analysis activities: Additional value if forensics analysis activities are available (file integrity monitoring, pcaps, NetFlow, evidence acquisition).

c) Analytics support: Additional value if there is a support for anomaly detection, use and entity behavioral profiling.

d) Automatic response capabilities: Additional value if there is a support for automatic response capabilities (e.g. SOAR: security orchestration automatic response).

5) Licensing and support: This section lists and describes the licensing and

support services requirement.

a) Preferred License type: The supplier should specify if the SIEM solution would be available only by license or also in other purchase option, e.g. such as leasing.

b) Licensing restrictions: State any license limitations, for example what happens in case of exceeding the limits mentioned in license.

c) Project Roadmap: Describe the tasks involved with the project of the SIEM platform installation and configuration and the corresponding timeframes.

d) Delayed license activation: The license activation should start only after the end of the acceptance tests in which all the project requirements will be met. The customer must ask for an acceptance-testing period to verify that the solution complies with the received description.

e) Technical assistance support and professional services: The supplier should include a description of the including technical support and professional services provided/available by vendor/system integrator.

f) Training provided: A description of training package should be provided.

4.2. Evaluating the Received SIEM Solutions

Different solutions were proposed by a set of suppliers according to their expertise in the field and using the most powerful SIEM products available in the market nowadays. In this case study, only three solutions are selected to apply the proposed approach, which are believed to be enough to show and verify the efficiency and effectiveness of our approach. However, for the purpose of not being subjective or promoting a solution, the study will not mention any supplier or SIEM product name, and instead it will anonymize their names and use the following notation for them:

1) Supplier 1 using Product X
2) Supplier 2 using Product Y
3) Supplier 3 using Product Z

Where the "supplier" is the one who provided the whole SIEM solution (product, architecture, installation, licenses, training, etc.) and the "product" is the name of the innovator who created the SIEM product.

After receiving the tenders from the suppliers, describing their overall solutions, the next step in the approach is to apply the evaluation phase. Evaluation is divided into two methods, *requirements-based* (quantitative) and *applicability-based* (qualitative), where the first aims to qualify a set of the best in terms of matching and complying the requirements specified by the customer, and the latter aims to select only one solution that best fits the company. And so, the evaluation done next is based on the whole solution offered, which includes the proposed architecture (topology for installation and deployment), kind of the platform, complexity, technical features, licensing, etc…, and it is not only an evaluation for the tool or the vendor that develops it. Again, the evaluation applied using this approach is from a customer point of view, ensuring the selec-

tion of the most appropriate and applicable solution based on the needs and context.

4.2.1. Requirement-Based Evaluation: Using a Quantitative Method

According to the received tenders, only three solutions were selected to demonstrate the evaluation of our approach, which we believe are enough to show the effectiveness of such an approach, knowing that they used the most powerful SIEMs existing in the market nowadays that are developed by well-known, skilful and expert vendors.

The approach assigns each requirement two different parameters, which are the *weight* (W) and the *requirement value* (V):

- The *weight* (W) 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.
- The *requirement value* (V) is the grade assigned to evaluate the answer of the supplier to the current requirement in the under-evaluation SIEM solution.

Then, a *score* (S) is calculated for each requirement ($S = W * V$), and after that a total for each requirement section is computed, and finally a total score is computed for the whole solution.

The approach suggested to use a non-linear growth scale because of its ability to differentiate between the values using the high growth rate, and so requirement value will get a non-linear value as suggested in the approach and will vary between 0, 1, 2 *and* 4 corresponding a zero, low, medium and high requirement evaluation. On the other hand, the weight will vary between zero and one, where one represents a critical requirement.

Therefore, to evaluate those solutions, a quantitative evaluation is used to show the *requirement-based* evaluation. Tables 4-6, present the quantitative evaluation of the received SIEM solutions.

➢ ***Supplier* 1, *product X*:**

Supplier 1 offered a solution based on a product X, the solution composed of two layers:

1) Collection layer that uses collection nodes to collect the logs, and to parse and normalize.

2) Processing layer for data storage and correlations based on specific rules.

In addition, the supplier offered a solution that can be deployed using two alternative architecture for deployment:

1) All-in-One deployment, where all layers are within a single node.

2) Distributed deployment, that consists of multiple nodes, composed of multiple nodes.

The solution covers most of the requirements, e.g. indexing, normalization, compression, and hashing for tamper proof, and it is able to parse a lot of sources and supports also custom parsing. Moreover, it is able to store events/logs locally for a long period. In addition, based on the proposed architecture of deployment, high availability is preserved.

Table 4. Evaluation of the SIEM solution by supplier 1.

SIEM Product X Supplier 1	Requirement	Weight (W)	Value (V)	Score (s)	Total
PLATFORM	a_1	**1.0**	4	4	
	a_2	**1.0**	2	2	
	a_3	**0.9**	2	1.8	
	a_4	**0.8**	2	1.6	
	a_5	**1.0**	4	4	
	a_6	**1.0**	2	2	
	a_7	**1.0**	2	2	
	a_8	**1.0**	2	2	
	a_9	**1.0**	2	2	
	a_{10}	**1.0**	4	4	43.8
	a_{11}	**1.0**	2	2	
	a_{12}	**0.8**	2	1.6	
	a_{13}	**0.8**	1	0.8	
	a_{14}	**0.8**	1	0.8	
	a_{15}	**1.0**	1	1	
	a_{16}	**0.8**	2	1.6	
	a_{17}	**0.8**	1	0.8	
	a_{18}	**1.0**	2	2	
	a_{19}	**1.0**	4	4	
	a_{20}	**0.9**	2	1.8	
	a_{21}	**0.6**	1	0.6	
	a_{22}	**0.7**	2	1.4	
	a_{23}	**0.5**	0	0	
OPERATIONS	b_1	**1.0**	1	1	
	b_2	**1.0**	1	1	3.8
	b_3	**0.9**	2	1.8	
	b_4	**0.8**	0	0	
INTERGRATIONS	c_1	**0.8**	1	0.8	
	c_2	**0.5**	0	0	
	c_3	**0.8**	0	0	2.1
	c_4	**0.8**	1	0.8	
	c_5	**0.5**	1	0.5	
ADVANCED FEATURES	d_1	**0.7**	2	1.4	
	d_2	**0.6**	1	0.6	
	d_3	**0.6**	2	1.2	3.7
	d_4	**0.5**	1	0.5	
LICENSING AND SUPPORT	e_1	**1.0**	2	2	
	e_2	**1.0**	1	1	
	e_3	**1.0**	2	2	
	e_4	**0.8**	2	1.6	12.6
	e_5	**1.0**	2	2	
	e_6	**1.0**	4	4	
				SCORE	**66**

Table 5. Evaluation of the SIEM solution by supplier 2.

SIEM Supplier 2 Product Y	Requirement	Weight (W)	Value (V)	Score (s)	Total
PLATFORM	a_1	**1.0**	1	1	
	a_2	**1.0**	4	4	
	a_3	**0.9**	1	0.9	
	a_4	**0.8**	1	0.8	
	a_5	**1.0**	4	4	
	a_6	**1.0**	0	0	
	a_7	**1.0**	2	2	
	a_8	**1.0**	4	4	
	a_9	**1.0**	1	1	
	a_{10}	**1.0**	4	4	31.4
	a_{11}	**1.0**	0	0	
	a_{12}	**0.8**	2	1.6	
	a_{13}	**0.8**	1	0.8	
	a_{14}	**0.8**	1	0.8	
	a_{15}	**1.0**	1	1	
	a_{16}	**0.8**	2	1.6	
	a_{17}	**0.8**	1	0.8	
	a_{18}	**1.0**	0	0	
	a_{19}	**1.0**	0	0	
	a_{20}	**0.9**	2	1.8	
	a_{21}	**0.6**	1	0.6	
	a_{22}	**0.7**	1	0.7	
	a_{23}	**0.5**	0	0	
OPERATIONS	b_1	**1.0**	1	1	
	b_2	**1.0**	1	1	2.9
	b_3	**0.9**	1	0.9	
	b_4	**0.8**	0	0	
INTERGRATIONS	c_1	**0.8**	1	0.8	
	c_2	**0.5**	0	0	
	c_3	**0.8**	0	0	1.6
	c_4	**0.8**	1	0.8	
	c_5	**0.5**	0	0	
ADVANCED FEATURES	d_1	**0.7**	0	0	
	d_2	**0.6**	0	0	
	d_3	**0.6**	0	0	0
	d_4	**0.5**	0	0	

Continued

LICENSING AND SUPPORT	e_1	**1.0**	2	2	
	e_2	**1.0**	2	2	
	e_3	**1.0**	1	1	
	e_4	**0.8**	2	1.6	9.6
	e_5	**1.0**	2	2	
	e_6	**1.0**	1	1	
				TOTAL SCORE	**45.5**

Table 6. Evaluation of the SIEM solution by supplier 3.

SIEM Supplier 3 Product Z	Requirement	Weight (W)	Value (V)	Score (s)	Total
PLATFORM	a_1	**1.0**	4	4	
	a_2	**1.0**	2	2	
	a_3	**0.9**	2	1.8	
	a_4	**0.8**	2	1.6	
	a_5	**1.0**	4	4	
	a_6	**1.0**	4	4	
	a_7	**1.0**	4	4	
	a_8	**1.0**	2	2	
	a_9	**1.0**	1	1	
	a_{10}	**1.0**	4	4	47.3
	a_{11}	**1.0**	2	2	
	a_{12}	**0.8**	2	1.6	
	a_{13}	**0.8**	1	0.8	
	a_{14}	**0.8**	1	0.8	
	a_{15}	**1.0**	1	1	
	a_{16}	**0.8**	2	1.6	
	a_{17}	**0.8**	1	0.8	
	a_{18}	**1.0**	2	2	
	a_{19}	**1.0**	4	4	
	a_{20}	**0.9**	2	1.8	
	a_{21}	**0.6**	1	0.6	
	a_{22}	**0.7**	2	1.4	
	a_{23}	**0.5**	1	0.5	
OPERATIONS	b_1	**1.0**	2	2	
	b_2	**1.0**	1	1	4.8
	b_3	**0.9**	2	1.8	
	b_4	**0.8**	0	0	

Continued

INTERGRATIONS	c_1	**0.8**	1	0.8	
	c_2	**0.5**	1	0.5	
	c_3	**0.8**	1	0.8	6.3
	c_4	**0.8**	4	3.2	
	c_5	**0.5**	2	1	
ADVANCED FEATURES	d_1	**0.7**	2	1.4	
	d_2	**0.6**	1	0.6	
	d_3	**0.6**	2	1.2	4.2
	d_4	**0.5**	2	1	
LICENSING AND SUPPORT	e_1	**1.0**	1	1	
	e_2	**1.0**	2	2	
	e_3	**1.0**	2	2	
	e_4	**0.8**	0	0	8
	e_5	**1.0**	2	2	
	e_6	**1.0**	1	1	
				TOTAL SCORE	**70.6**

➢ ***Supplier* 2, *Product X*:**

The solution proposed by supplier two uses product Y. It has a modular and distributed architecture, and is composed of two layers:

1) A layer that groups collection and standardization, it can receive logs of any type of data source within the network without the need to install agent designed for each specific platform.

2) A layer for correlation on the main appliance.

The solution uses a hardware-based appliance (on premise or in cloud) that is able to support continuous traffic.

However, the solution lacks a lot of the main requirements such as indexing, hashing, normalization, customizable dashboard per user, and for compliance reports, etc…

➢ ***Supplier 3, product Z*:**

This solution is divided into two layers: collection and correlation.

1) Collection layer: composed of software instances (agents) where each agent works on a source.

2) Correlation layer: a copy of the collected logs is sent to this layer to be processed; it consists of one hardware and is able to handle fair number of EPS.

The solution ensures high availability through deploying redundant appliances. Other main requirements that this solution covers are indexing, hashing and normalization. However the license is activated at the beginning of the deployment process and there is no delayed license.

Therefore, applying the quantitative evaluation on the received SIEMs will

output an evaluation (total score) for each solution. At the end two solutions are selected as qualified SIEM solutions, where only one of them will be adopted finally. In the next section, *applicability* evaluation is applied to select one of the two qualified SIEM solutions.

4.2.2. Applicability Evaluation: Using a Qualitative Method

As said before, not always the solution that got the highest score in the requirement-based evaluation will be adopted; however, as explained, there are other factors and indicators that should be considered, and they are represented in the *applicability* evaluation.

After evaluating the SIEM solutions quantitatively, the next step is to apply the qualitative evaluation (*applicability* evaluation). In our case, the applicability evaluation is applied to choose between the two qualified solutions (by supplier 1 and supplier 3). Table 7 and Table 8 show the applied qualitative evaluation:

- ***Supplier* 1, *Product X***
- ***Supplier* 3, *product Z***

Both the two SIEM solutions (by supplier 1 and 3) got the highest value. However, the first solution matched more the customer's needs and the defined indicators. Even if the solution proposed by supplier 3 got a higher value, it was not selected. The first solution offered two architectures to choose from, which helps in the ease of deployment, better licensing, support, and it matched

Table 7. Qualitative evaluation for the first SIEM solution by supplier 1.

Supplier 1 Product X	Indicators	Importance or weight	Evaluation	NOTES
Applicability	Level of Compliance	*High*	*Excellent*	High compliance
	Complexity	*High*	*Very Good*	Very Flexible
	Quality of services	*High*	*Very Good*	
	Robust Architecture	*High*	*Very Good*	High availability is guaranteed
	Scalability	*Medium*	*Good*	
Licensing and support services	Complete description	*High*	*Excellent*	
	Installation duration/ clearness of road map	*High*	*Very Good*	Clear roadmap including all steps
	Licensing	*High*	*Very Good*	Clear dimensioning including user acceptance test period
	Support	*Medium*	*Good*	24 × 7
	Training	*Medium*	*Good*	
Advanced Features	Additional features	*Low*	*Good*	
	Integration with third parties	*Medium*	*Good*	
Other indicators	Expertise/Skill of Vendor/Supplier	*Medium*	*Excellent*	One major player
	Price	*Medium*	*Excellent*	
	RESULT			ACCEPTED

Table 8. Qualitative evaluation for the third SIEM solution by supplier 3.

Supplier 3 Product Z	Indicators	Importance or weight	Evaluation	NOTES
Applicability	Level of Compliance	*High*	*Very Good*	Mostly compliant
	Complexity	*High*	*Good*	Non trivial deployment
	Quality of services	*High*	*Very Good*	
	Robust Architecture	*High*	*Very Good*	High redundancy is guaranteed
	Scalability	*Medium*	*Good*	
Licensing and support services	Complete description	*High*	*Excellent*	
	Installation duration/clearness of road map	*High*	*Very Good*	
	Licensing	*High*	*Insufficient*	Use-acceptance-testing period was not included and low dimensioning of EPS
	Support	*Medium*	*Good*	
	Training	*Medium*	*Good*	
Advanced Features	Additional features	*Low*	*Good*	
	Integration with third parties	*Medium*	*Good*	
Other indicators	Expertise/Skill of Vendor/Supplier	*Medium*	*Very Good*	Major player but adopting less know system integrator
	Price	*Medium*	*Insufficient*	A bit high if compared to proposed number of licenses
	RESULT			REJECTED

another relevant indicator, which is the price, offering a solution that is consistent to the budget.

5. Comparison

To prove the eligibility of using our approach we select Gartner's work to compare with. Gartner Inc. is one of the leading information technology research and advisory company that deliver the technology-related insight necessary for clients to make the right decisions, research, analyze and interpret the business of IT within the context of their individual role.

Gartner published its 2018 Critical Capabilities for Security Information and Event Management report [8] to evaluate and rank different SIEM vendors (products). First, they started by specifying the critical capabilities that a SIEM should have. Critical capabilities are architecture, deployment, operations and support, log and data management, real-time monitoring, analytics, data and application monitoring, threat and environmental context, user context and monitoring, incident management and threat detection tools.

After that, they defined three use cases: basic security monitoring, complex security monitoring, and advanced threat defense, where the SIEM vendors are evaluated in each use case. These use cases used represent three "operational" levels in which the SIEM will be deployed.

Critical capabilities are then weighted, where each capability is given a weight in terms of its relative importance in each use case. In addition, for each SIEM product, the critical capabilities are rated on a scale of 1 to 5, where 1 represents a poor requirement, whereas 5 is an outstanding (significantly exceeds requirements). Finally, an overall score is carried out for each SIEM on the three different use cases. To determine an overall score for each product in the use cases, the ratings (evaluations) are multiplied by the weightings to come up with the product score in use cases. Different SIEM products developed by the most expertise and skilled vendors are used in the evaluation applied by [8], where each vendor's product or service is evaluated in terms of how well it delivers each of the capabilities defined. This kind of evaluation can be defined as a product driven evaluation, where the capabilities of the product are evaluated without differentiating the customer's needs factor.

However, our approach suggests the customer to create a more detailing list of requirements that reflects their needs, which is a subjective and detailed list representing the SIEM seeking for, therefore, to receive an overall solution and not just a product, and so the evaluation will be influenced by these specific requirements.

Moreover, we defined a second level of evaluation, which is a qualitative evaluation method (applicability based) that selects from the qualified solution evaluated previously by the quantitative evaluation method (requirement based) (Table 9).

6. 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

Table 9. A comparison between the proposed SIEM evaluation approach and Gartner's report.

Product-driven SIEM evaluation	Customer-driven: Our SIEM Evaluation Approach
Suggests a list of the main requirements (capabilities) that a powerful SIEM should have	Suggests a list of requirements with some specifications from a customer point of view
Has a flat approach when weighting the requirements	Can adopt weights to reflect more significant requirements
Uses quantitative evaluation	Uses both quantitative and qualitative evaluation
Evaluation is applied for general use cases	Evaluation is applied based on customer needs and context
Evaluates a product	Evaluate an overall solution: product, architecture, deployment, price, etc…

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.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Mokalled, H., Pragliola, C., Debertol, D., Meda, E. and Zunino, R. (2019) A Comprehensive Framework for the Security Risk Management of Cyber-Physical System. In: Flammini, F., Ed., *Resilience of Cyber-Physical Systems, Advanced Sciences and Technologies for Security Applications*, Springer, Cham, 49-68. https://doi.org/10.1007/978-3-319-95597-1_3

[2] Casola, V., Fasolino, A.R., Mazzocca, N. and Tramontana, P. (2009) An AHP-Based Framework for Quality and Security Evaluation. 12*th IEEE International Conference on Computational Science and Engineering*, Vancouver, 29-31 August 2009, 405-411. https://doi.org/10.1109/CSE.2009.391

[3] Casola, V., Fasolino, A.R., Mazzocca, N. and Tramontana, P. (2007) A Policy-Based Evaluation Framework for Quality and Security in Service Oriented Architectures. *IEEE International Conference on Web Services*, Salt Lake City, 9-13 July 2007, 1181-1182. https://doi.org/10.1109/ICWS.2007.11

[4] Miloslavskaya, N. (2018) Analysis of SIEM Systems and Their Usage in Security Operations and Security Intelligence Centers. In: Samsonovich, A. and Klimov, V., Eds., *Biologically Inspired Cognitive Architectures* (*BICA*) *for Young Scientists*, Advances in Intelligent Systems and Computing, Vol. 636, Springer, Cham, 282-288. https://doi.org/10.1007/978-3-319-63940-6_40

[5] Widup, S., Rudis, B., Hylender, D., Spitler, M., Thompson, K., Baker, W., Bassett, G., Karambelkar, B., Brannon, S., Kennedy, D. and Jacobs, J. (2015) Verizon in the Data Breach Investigations Report.

[6] IBM Corporation (2010) IT Security Compliance Management Design Guide with IBM Tivoli Security Information and Event Manager. 2nd Edition. http://www.redbooks.ibm.com/abstracts/sg247530.html

[7] Sadowski, G., Kavanagh, K. and Bussa, T. (2018) Technology Insight for the Modern SIEM. Resource Document. Gartner Inc., Stamford.

[8] Bussa, T., Kavanagh, K. and Sadowski, G. (2018) Critical Capabilities for Security Information and Event Management. Resource Document. Gartner Inc., Stamford.

[9] Tech Target: Security Information and Event Management (SIEM) (2014). http://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM

[10] Scarfone, K. (2015) Introduction to SIEM Services and Products. http://searchsecurity.techtarget.com/feature/Introduction-to-SIEM-services-and-products

[11] Kavanagh, K., Bussa, T. and Sadowski, G. (2018) Magic Quadrant for Security Information and Event Management. Gartner MQ for Security Information and Event Management. Resource Document. Gartner Inc., Stamford.

[12] Rochford, O., Kavanagh, K.M. and Bussa, T. (2016) Critical Capabilities for Security Information and Event Management. Resource Document. Gartner Inc., Stamford.

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

[14] Nabil, M., Soukainat, S., Lakbabi, A. and Ghizlane, O. (2017) SIEM Selection Criteria for an Efficient Contextual Security. *International Symposium on Networks, Computers and Communications,* Marrakech, 16-18 May 2017, 1-6. https://doi.org/10.1109/ISNCC.2017.8072035

[15] Scriven, M. (1967) The Methodology of Evaluation. In: Stake, R.E., Ed., *Curriculum Evaluation*, Rand McNally, American Educational Research Association, Chicago, 39-83.

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

[17] (2019) Hitachi Rail Signaling and Transportation Systems (Hitachi Rail STS). http://sts.hitachirail.com/en/about-us