IADIS International Journal on Computer Science and Information Systems
Vol. 19, No. 1, pp. 31-47
ISSN: 1646-3692

EDO4SIEM – A PROCEDURE MODEL FOR THE IMPLEMENTATION OF SECURITY INFORMATION AND EVENT MANAGEMENT SYSTEMS IN ORGANISATIONS

Maximilian Rosenberg, Bettina Schneider, Christopher Scherb and Petra Maria Asprion
University of Applied Sciences and Arts Northwestern Switzerland FHNW, Peter Merian Str. 86, 4002 Basel, Switzerland

ABSTRACT

The topic of cybersecurity is becoming increasingly important as the number of cyberattacks continues to grow; it is no longer just a matter of protecting, but rather of detecting cyberattacks at an early stage and responding accordingly. Detecting cyberattacks in organisations is an increasingly difficult task, since the ability of malware to hide from Anti-Virus systems has massively improved. Therefore, more sophisticated security measures are required, to protect complex information systems from cyberthreats. One of the state-of-the-art solutions is a ´Security Information and Event Management´ (SIEM) system, which collects all security related information and events on a central location. Thus, it is possible to correlate and better analyse security-related events, detect, and defend sophisticated threats. The deployment of a SIEM system (SIEMS) is a process where all devices in the network need to be registered and integrated. There is no generic model for the evaluation, deployment, and operation of a sufficient SIEMS that can be applied independently of the dedicated vendor. Usually, vendors provide deployment guides for their SIEMS; however, these are product-specific and not scientifically evaluated. Applying Design Science as methodological approach, the goal of this research was to develop and scientifically validate a generic model called ´EDO4SIEM´ for the vendor-neutral evaluation, deployment, and operation of a SIEMS in organisations. As desire for future research, the model should be applied in various organisations to confirm its applicability and to further develop it.

KEYWORDS

Cybersecurity, Frameworks, EDO4SIEM, Security Information and Event Management, SIEM

1. INTRODUCTION

Cybersecurity is a major concern for organisations (Eurostat, 2023; IBM Security, 2023; Bygrave, 2022; Morgan, 2020). One accepted way to track security-related activities of an organisation is with the help of a ´Security Information and Event Management´ system (SIEMS). A SIEMS collects, stores, and analyses security-related logs that provide information related to information, network, data security, and regulatory compliance (Chuvakin, 2010). Only when sufficient implemented, a SIEMS unfolds its value. The implementation is a resource-intense and demanding procedure. Insufficient implementation may lead to having an expensive SIEMS in place without realizing the anticipated benefits (Mokalled et al., 2019), potentially rendering the system unused. Selecting the appropriate system, ensuring adequate customization and deployment are essential.

Literature research across the platforms ´Google Scholar´, ´IEEE Xplore´, ´ResearchGate´, ´Scopus´ and ´Swisscovery` has shown that there are some models available, but all dependent on the specific vendor of the SIEM product. An analysis of existing models showed the following research gaps: (1) No SIEM model/procedure could be found that comprehensively covers the phases ´evaluation´, ´deployment´ and ´operation´. (2) Some models from SIEM product vendors provide inputs for the evaluation phase dedicated to the vendor´s product. (3) No model/procedure for the operations phase could be found. In response, this research introduces a prototype model named EDO4SIEM, outlining how to evaluate, deploy, and operate a SIEMS in any organisation. This contribution aims to fill the identified gaps and provide a comprehensive framework for organisations seeking effective SIEMS implementation.

The following representations are structured as follows: in section 2, the methodology is elaborated; section 3 explains the core of the given problem and defines the requirements. In section 4, existing models and relevant security related frameworks are analysed. Section 5 explains how the prototypical model was systematically developed, whereas section 6 explains the validation and the final model. Finally, section 7 concludes the main elements and offers an outlook for further research.

2. METHODOLOGY

To ensure a systematic approach, Design Science Research (DSR) as outlined by Hevner et al. (2008) was applied. DSR starts with the identification of a problem, which in this research is the lack of a sufficient model for the implementation of a SIEM in organisations. Figure 1 shows five process steps performed to develop the EDO4SIEM based on Kuechler and Vaishnavi´s (2008) process steps rooted in the principles of DSR.

Figure 1. DSR process adopted from Kuechler & Vaishnavi (2008)

The first step - Problem Awareness - derived why a new model is needed for the implementation of a SIEMS. Awareness of the problem was raised by conducting a literature review on log management, log analysis and the current state of different SIEMS. In the second step - Analysis - existing models for the implementation of a SIEMS were searched and

analysed. In this context, security frameworks were examined to derive recommendations. In addition, a case study was conducted at a Swiss retail organisation which was in the process to evaluate and establish a SIEMS. Due to this case study, practical experience could be investigated. The third step - Development - was used to combine the previously acquired knowledge and findings in a new model – the EDO4SIEM. In the fourth step - Validation - interviews were conducted with subject matter experts to test and improve the newly developed EDO4SIEM. Based on the interviews, further insights could be gained, which could iteratively be incorporated. During the last step - Conclusion - EDO4SIEM was revised and finalized based on the inputs of step 4. Overall, the research resulted in a practitioner-oriented, generic model for the establishment of any SIEMS in organisations.

3. PROBLEM AWARENESS

SIEMS are relatively new products and should be distinguished from traditional logs. Logs are records of events that occur in systems, networks, or applications. While originally logs were used for troubleshooting, nowadays they serve e.g., recordings to user interactions, performance, or malicious activities. As threats to corporate networks and systems continue to grow, the need to analyse logs has emerged (Sahoo et al., 2012; Kent & Souppaya, 2006). Organisations use mostly centralized Log Management Systems (LMS) that receive, retrieve, and store logs from various hosts; the logs should be analysed, kept for a defined period, and deleted afterwards. LMS offer various basic functionalities such as ´Log Collection´, ´Log Filtering´, ´Log Archival´, or ´Event Correlation´.

While a LMS collects and stores all types of logs, a SIEMS focuses on security-relevant logs. Consequently, the most obvious difference between a SIEMS and a LMS is the focus of a SIEMS on security events and their analysis (Chuvakin, 2010). The concept and functionality of a SIEMS is the combination of Security Information Management (SIM) and Security Event Management (SEM). SIM collects security-related logs for report generation whereas SIEMS analyse these security-related logs. SIEMS are mainly used by Security Operations Centers (SOC), which aim to maintain and improve the security of an organisation (Vielberth, 2021; Miloslavskaya, 2018; Kent & Souppaya, 2006). Most SIEMS have the previously mentioned functionalities of LMS. In addition, SIEMS offer further functionalities such as the integration of user and entity behaviour analysis (UEBA) or machine learning-based data analysis[1] (Yelevin & Batami, 2022; González-Granadillo, González-Zarzosa, & Diaz, 2021; Salitin & Zolait, 2018; Chuvakin, 2010).

There are different solutions of SIEMS from different vendors, but their basic functionalities are similar. Incoming events are analysed using various rules or data models and compared with past events. Alerts can be triggered, which inform about events, or a multitude of them (Shahid & Shah, 2021; Salitin & Zolait, 2018; Kent & Souppaya, 2006). Establishing a SIEMS can provide organisations benefits, but these are cancelled by incorrect configuration or maintenance. One essential benefit is that a SIEMS allows to analyse security-related logs in real time. Based on the analysis, security teams can immediately initiate countermeasures.

The evaluation of a SIEMS can be resource consuming for both – the deployment and operation phase. If the alerts of a SIEMS are not analysed and processed, the introduction of a SIEMS is worthless. A SIEMS is usually established for mapping use cases; for example, for reporting regulatory compliance, insider threats or threat hunting. Consequently, the

[1] https://community.exabeam.com/s/article/Exabeam-Use-Case-Series-Contextualization

EDO4SIEM to be developed should include as first an evaluation phase. Kavanagh, Rochford, & Bussa (2021) revealed that the SIEMS market grew from 3.55 billion in 2019 to 3.58 billion in 2020; the study indicates further that organisations are re-evaluating their current SIEMS vendors because of incomplete and failed deployments. Consequently, the new EDO4SIEM should include a deployment as well as an operation phase.

The first search for models/procedures, which can be used for the evaluation of SIEM products, delivered few results which could partly be adopted; all the analysed contributions provided some criteria for evaluating a SIEMS. But they were mostly contributions/guides from SIEMS vendors (AlienVault, 2021). An assessment method for SIEM products was provided by Safarzadeh, Gharaee and Panahi (2019). A second search for the deployment phase resulted in one best practice manual for the deployment of Microsoft Sentinel (Yelevin & Batamig, 2021) and a contribution describing the deployment of a SIEMS in a cloud infrastructure (Holik et al., 2015). The third search - focused on how to operate a SIEM or any operational application after deployment - did not yield any results.

In summary, our research identified an absence of a model or procedure for implementing a SIEMS that is universally applicable, irrespective of specific products, and encompasses one or more of the three identified phases as relevant. Based on these results, additional literature analysis, and results from a qualitative oriented case study, requirements were defined (Table 1) for the new EDO4SIEM to be developed which includes all three phases - evaluation, deployment, and operation.

Table 1. EDO4SIEM Requirements (R1 to R5)

#	Requirements Description	Justification
R1	The model is based on elements of existing (project management) methods.	To ensure that the model can be applied in an intuitive and practical manner, it should be based on elements of widely recognized (project management) methods.
R2	The model covers the three phases ´evaluation´, ´deployment´ and ´operation´.	Prior to deployment, an organisation needs to select a specific SIEMS. The new model should, therefore, incorporate an evaluation phase. After the decision and deployment of the chosen SIEMS, the system is transitioned to operations. Hence, EDO4SIEM should include a phase where the system is handed over to the operational organisation for further development.
R3	The model can be applied regardless of manufacturer/vendor or product.	While SIEMS vendors offer guidance on how to assess a SIEMS, it is essential to enable vendor-independent evaluation of different SIEMS. EDO4SIEM should offer universal applicability for SIEMS projects.
R4	The model is based on agile methods and approaches.	Traditional project management follows a sequential approach, making it challenging to adapt to changing requirements. Agile project management, with its iterative process, enables the incorporation of new requirements as the project advances. For example, in a SIEMS implementation project, a new requirement could involve setting up and transferring logs from a new firewall during deployment.
R5	The model includes references to other methods and/or security frameworks.	The model should include references to security frameworks to provide a customized reference to security use cases and challenges.

4. ANALYSIS

To develop the first prototype of EDO4SIEM, an analysis of relevant elements to be considered was performed: first, minimum criteria were established; these were expanded, especially for the deployment phase, with (agile) project management methods. Second, security frameworks were studied, and three accepted ones were selected, from which relevant elements derived that were then considered.

4.1 Relevant Criteria for EDO4SIEM

One derived requirement for EDO4SIEM is that it should be based (on elements) of existing models that are usually used (R1 in Table 1) for the establishment or deployment of a software. Consequently, literature research was conducted to find models which could be adopted. The models investigated (Broy & Kuhrmann, 2021; Schatten, et al., 2010), were divided into three categories: (1) sequential (waterfall model or V-Model XT), (2) iterative (spiral model, rational unified process, openUP model, prototyping), and (3) agile (scrum, incremental approach, extreme programming, kanban, DevOps). Based on the analysed models, minimum criteria for the evaluation phase were derived (Table 2) and the three models were compared regarding the criteria surveyed. In the following, the three selected models are presented and weighed against each other in terms of their suitability for the evaluation phase.

Waterfall or V-Model: Royce (1987) first described the model by mapping software development processes. At the initialization of a project, different phases are defined, which are passed through. The phases are run through sequentially from top to bottom during the project. Feedback makes it possible to ´jump back´. In terms of design, the model offers flexibility, as the phases can be freely defined. By milestones, control and decision points can be established that facilitate the decision of whether a phase is complete. The completion of one phase is necessary to move to the next. According to Schatten, et al. (2010), the waterfall model should mainly be used for projects where the requirements can be clearly defined.

Table 2. Required Criteria for the Evaluation Phase

#	Minimum Criteria for the New EDO4SIEM
C1	The model includes phases and/or activities.
C2	The model can be applied to two of the three phases (evaluation, deployment, operation).
C3	The model has agile characteristics or can be combined with agile methods.
C4	The model has return options or control mechanisms.
C5	The model is generic.

V-Model XT: The previous V-Model contains various procedure modules that can be individually combined to tailor the model to the specific project. The activities, which can be seen before the ´V´, are processed and run through sequentially, as in the waterfall model. Also, after the ´V´ elements can be shown, which are run through in a sequential form after all iterations have been completed (Broy & Kuhrmann, 2021). The V-Model XT can be seen as a combination of a sequential and iterative approach (Kneuper, 2018). An advantage of V-Modell XT is the exact description of how and in which form the model can be applied in practice.

Scrum: Scrum is a collaborative project management approach (Takeuchi & Nonaka, 1986); the model can deal dynamically with changing requirements. Scrum defines a general framework of how the activities in the project should be carried out. The team organises itself during the several ´Sprints´; this allows the team to fully concentrate on the current tasks, which were selected at the ´Sprint Planning Meeting´. By prioritizing the requirements, which are carried out by the ´Product Owner´ in collaboration with the business, the requirements that are most important for the business can be implemented first. The use of Scrum is efficient for smaller teams, as communication during a Sprint and at the various meetings can be well coordinated. Scrum proves to be useful when results should be delivered within the shortest possible time. For example, Scrum could also be used for the development of a concept, whereby partial results are delivered again and again until finally the complete concept has been developed (Lucht, 2019; Schatten, et al., 2010).

4.2 Security Frameworks

Another requirement for the EDO4SIEM is that it should include references to recognized cybersecurity frameworks (R5 in Table 1). These references should help to reference and apply accepted methods in well-known/established frameworks. Based on literature analysis, three widely accepted cybersecurity related frameworks were selected: (1) the NIST Cybersecurity Framework (CSF)[2], (2) the ISO/IEC 27001/2[3] (Humphreys, 2016) standard, and (3) the MITRE Att&ck framework[4]. In the following paragraphs, the selected frameworks are briefly presented.

4.2.1 NIST CSF

The NIST CSF helps organisations to manage cybersecurity. This CSF supports organisations in the process of identifying, assessing, and responding to risks. With the help of the framework, organisations can specify their risk tolerance. By knowing the risk tolerance, an organisation can prioritize cybersecurity events and make decisions based on this information to faster fight critical threats (NIST, 2018). In the context of a SIEMs, it makes sense to take a closer look at the ´Detect´ function: the function contains various categories, for example ´Anomalies and Events´. This category is about detecting anomalous activities and understanding the potential impact. Within this category, there are sub-categories that provide more specific aspects and address different areas, e.g., event detection and analysis (DE.AE-2), or event collection and correlation (DE.AE-3). If the NIST CSF is already in use, the introduction of a SIEMS can help to cover recommended categories or various sub-categories. However, the NIST CSF can also be a support for organisations that do not currently use the framework because it provides many references in the individual (sub-)categories to other frameworks and standards that could be considered when establishing a SIEMS.

4.2.2 ISO/IEC 27001/2

The ISO/IEC 27001/2 defines requirements for an Information Security Management System (ISMS), e.g., for the establishment, maintenance, and improvement of an ISMS. Along with these requirements, it provides information on how information security risks could be assessed

[2] https://www.nist.gov/cyberframework
[3] https://www.iso.org/isoiec-27001-information-security.html
[4] https://attack.mitre.org

and addressed. The annex of ISO/IEC 27001:2013 describes (recommended) control objectives and controls, e.g., on information on logging and monitoring (A.12.4). Further, the following four points are described about logging and monitoring[5]: (1) Event Logging (A.12.4.1), (2) Protection of Log Information (A.12.4.2), (3) Administrator and Operator Logs (A.12.4.3), and (4) Clock Synchronization (A.12.4.4). In addition to the requirements from ISO/IEC 27001:2013, the ISO/IEC 27000 series also provides further information relating to ISMS.

4.2.3 MITRE Att&ck FRAMEWORK

The MITRE Att&ck Framework is a knowledge base that contains tactics and techniques used by attackers. The framework contains 14 tactics, 191 techniques and 386 sub-techniques. Organisations can use it to learn which techniques are used by hackers when attacking organisations. As an example, the tactic ´Reconnaissance´ describes techniques that are used to gather information, which in turn could be used to plan attacks. Further techniques such as ´active scanning´ and ´phishing for information´ are described. However, the framework does not describe which solutions and tools should be used to detect an attack. The MITRE Att&ck framework can be used as a source of information for defining use cases because of the tactics, techniques, and sub-techniques described. An obvious use case could be detecting phishing emails without relying on the user. The framework provides examples of such attacks for the techniques (’Procedure Example’) and how they can be mitigated (’Mitigations’) and detected (’Detection’). Furthermore, data sources and related data components are mentioned, which should support the recognition of that kind of an attack. Overall, the MITRE Att&ck Framework can be used by organisations for the definition of use cases.

4.3 Derived Elements of EDO4SIEM

By analysing existing models, methods and frameworks, relevant elements could be collected that should be considered and used in the new EDO4SIEM (Table 3, 4 and 5).

Table 2. Adoptable Criteria Project Management

Approach	Application Conditions
Sequential	Requirements can be clearly defined from the beginning.
Agile	Requirements cannot be clearly defined; they could change during the project.

Table 3. Adoptable Tools and Methods

Phase	Tools and Methods Relevant for the New EDO4SIEM
Evaluation	Analysis of stakeholders, requirements, utilities, preference matrix, documentation.
Deployment & Operation	Documentation, Review, Burn- Down-Chart, Scrum Board.

[5] https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/45/54534.html

Table 4. Adoptable Security Framework Elements

Phase	Section in a Dedicated Framework Relevant for the New EDO4SIEM
Evaluation	NIST CSF: requirements (detection phase). ISO/IEC 27001: requirements (logging and monitoring). MITRE Att&ck: use cases and required log sources.
Deployment	NIST CSF: procedures and processes to be followed after an incident. ISO/IEC 27001: requirements (protection of log information, clock synchronization).
Operation	NIST CSF: continuous monitoring of the security of the organisation. ISO/IEC 27001: regular review of the collected information. MITRE Att&ck: use cases and sources.

5. DEVELOPMENT

To structure the first prototype of EDO4SIEM, four levels and six main design elements were created (Figure 2 – the validated prototype):

Level 1: Phases (1),
Level 2: Activities (2),
Level 3: Delivery Objects (3) and Tasks (4),
Level 4: Method References (5) and Security Framework Reference (6).

Moreover, it is imperative to recognize project management as an intrinsic component within the project paradigm. Consequently, the magic triangle of project management has added to the model as an overarching principle. Accordingly, the project management should monitor time, scope, and budget of the project across all phases. In the following sub-sections, the development of the three phases (evaluation, deployment, and operation) as defined (R2 in Table 1).

5.1 Evaluation

The evaluation phase should help to assess appropriate SIEMS that meets an organisation's requirements. However, before these can be defined, the project team needs to understand which roles/people are authorized to define the requirements for the new SIEMS and which roles/people will be affected by the deployment and operation of the SIEMS.

A stakeholder analysis should be performed to identify these roles/people (e.g., CISO, CTO, DPO) in the organization. By analysing the organization´s system landscape, it is possible to identify the core systems that are of primary importance for the initial deployment. Furthermore, it should be analysed which logs should be transmitted to the SIEMS obligatory. The results of the system landscape analysis can be supportive at a later stage for example for the definition of relevant use cases (e.g., detection of phishing emails). Consequently, the evaluation phase should start with an analysis of the initial situation, whereby both a stakeholder and a system landscape analysis should be performed.

Upon analysing the initial situation, the requirements, which need to be fulfilled by a SIEMS must be defined. During the stakeholder analysis, it should have become clear which roles/people define the requirements for the SIEMS. Therefore, these roles/people should subsequently be surveyed using an appropriate method, such as questionnaires or interviews. The functional and non-functional requirements are needed in the subsequent step for the

evaluation and selection of the SIEMS. Once the requirements and the most relevant use cases have been defined, various SIEMS should be evaluated. For this purpose, it is recommended to create a preference matrix that ranks and weights the requirements for the SIEMS. During this task, stakeholders can exchange information with each other as well as discuss and decide together which requirements are most important for the organisation. The SIEM product with the highest score is the most suitable system for the organisation based on the criteria previously defined and approved by the stakeholders. For the evaluation of the system requirements, the product websites of SIEMS can be visited and analysed. Likewise, the developers or partners of the SIEMS in question can be asked directly to obtain more information. Since, in addition to the functional and non-functional requirements, the use cases also play a role in the evaluation, research should be conducted to determine which SIEMs are capable to address which use cases.

5.2 Deployment

The establishment of a selected SIEMS is the overarching goal of the deployment phase. Before a SIEMS can be installed and put into operation, the contracts for obtaining the licenses must be concluded. Kavanagh, Rochford, & Bussa (2021) report that vendors outside their region often offer their product through partners or subsidiaries; these partners assist new customers in deploying the SIEMS. In addition to the purchase, license and service contracts, local data protection laws should be considered, since personal data is transmitted, stored, and analysed in a SIEMS.

Since the new EDO4SIEM should be able to be used independently of manufacturer or product (R4 in Table 1), the focus of the deployment phase is on the connection of the log sources. Even SaaS deployments require installations in the organisation's data center, depending on which logs should be transferred to the SIEMS. In Azure Sentinel (Sahay, 2020), for example, agents are installed on the servers that send the logs to a gateway server, which forwards the logs received to the cloud-SIEMS. Exabeam[6] and Splunk (Mehta, 2021) use collectors that forward the on-premises logs to the cloud. Therefore, EDO4SIEM includes the task ´Installation´. The activities ´Contract signing´ and ´Installations and preparations´ should be carried out sequentially. The integration of the log sources should take place in iterations, whereby an iteration contains four tasks (Table 6), which must be executed until a log source can be marked as implemented. In addition to the various activities, deliverables, and tasks in the deployment phase, EDO4SIEM includes references to security frameworks and methods as defined in the requirements.

[6] https://docs.exabeam.com/collectors/

Table 6. Necessary Iterations

#	Tasks
1	Configuration firewall / proxy rules: Before the logs are sent to the SIEMS from on-premises applications, servers, systems, or appliances, it is necessary to open/enable the communication channels required for this purpose
2	Configuration Log Forwarding: After the ports are opened on the firewall, log forwarding can be configured. Unnecessary logs should be filtered and not transferred to the SIEMS. The configuration of log forwarding must be documented and available to all authorized roles/people
3	Parsing the logs: As soon as the logs arrive in the SIEMS, the parsing of the logs can be started. If the SIEMS vendor already offers the appropriate parser, e.g., known and standardized logs, there is no need to create your own. Nevertheless, it is necessary to control how the logs are parsed and whether the required information is extracted.
4	Review: When the previous three steps are complete and the logs are parsed correctly, a review should take place. The goal of the review is to verify that all relevant logs are sent from a system to the SIEMS and that the logs are parsed correctly. In addition, a completeness and quality check of the documentation should be performed

5.3 Operation

In the first step of the operating phase, the handover should be prepared. User documentation should be created, responsibilities defined, and operational processes documented. User documentation supports the project team in training the defined operators of any system (Scherb et al., 2023). In addition, the users can refer to the documentation at a later point in time and train new users in the same way. By defining and recording responsibilities, it is clearly agreed which roles/people are responsible for which task.

Furthermore, the processes for handling the SIEMS should be clarified and recorded. When defining responsibilities and operational processes, the NIST CSF should consider the respond categories. Once the documentation has been prepared, responsibilities and processes defined, the SIEMS can be handed over. This should involve introducing and training the users who will be working with the system in the future before the system is effectively used by these individuals in their day-to-day work. The activity also includes the task of handing over all artifacts and documents that were developed during the project. This ensures that the people working with the SIEMS have access to all required information and documents. When the first two activities of the operational phase are completed, the SIEMS can be handed over to operations.

The SIEMS must be further developed by the operations team from this point on. The reason for this is that new applications and systems are constantly being introduced and old ones replaced in an organisation. As a result, every time applications or systems change new log sources must be added. In addition, new use cases may need to be implemented due to new attack techniques, user needs, or changed and new corporate security policies. Consequently, the operational activities include the operation, maintenance, and further development of the SIEMS. The operation of a SIEMS should therefore take place in an agile form, as visualized in the framework for agile management in cybersecurity (Asprion et al., 2023). With the help of an agile operational organisation, incidents can be processed, new log sources can be integrated, and additional use cases can be implemented within a reasonable period.

6. VALIDATION

The DSR approach demands a validation of the prototypical EDO4SIEM. The validation approach used the results from two qualitative interviews with subject matter experts and the case study experience; the aim was to determine whether the model is applicable and what can still be improved. We structured the interviews along to (1) relevant requirements, (2) the applied approach, and (3) the three phases (evaluation, deployment, operation)

6.1 Interview Results

Relevant requirements: The interviews showed that the developed model fulfils all five requirements (Table 1). It includes all three defined phases, and the elements are based on existing project management methods used in practice (R1 and R2). Both experts mentioned that the model shows a high-level perspective, thus fulfilling the requirement that the model can be applied independently of any manufacturer/vendor or product (R3). Despite the high-level perspective, relevant activities which must be performed in a SIEMS project are included in EDO4SIEM. One reason for this feedback is that the activities in EDO4SIEM contain various results and tasks providing users with information about which artefacts could be created. Likewise, the references to various methods and frameworks are helpful to understand how a result can be achieved or a task can be performed (R5). Since EDO4SIEM reflects the three phases of a SIEMS project from a high-level perspective, organisations may incorporate additional activities, tasks and results that are specific to the product and/or organisation. For project management, agility is maintained in EDO4SIEM in that way that deliverables and tasks can be performed within the activities. Furthermore, the connection of the log sources and the operation must be iterative, which is why the requirements regarding agility are also met (R4).

Applied approach: The experts are convinced that a purely sequential or agile model is generally not suitable for the introduction of software. The activities themselves are often carried out in projects through agile methods or an iterative process. The case study also showed that a sequential approach to evaluating the SIEMS was beneficial. The agile/iterative approach to deployment and operations also proved suitable. Furthermore, it was confirmed that the operation of a SIEMS must be carried out by an agile team. Otherwise, according to the experts, the system cannot be further developed on an ongoing basis, which in turn means that the effectively possible added value of a SIEMS is reduced.

Evaluation phase: The interviews revealed that the most important components of an evaluation of a SIEMS are present in the evaluation phase depicted. Nevertheless, there were a few suggestions for improvement from the experts. When analysing the system landscape, in addition to the interviews, a document analysis would be very helpful if high-quality documentation is available. Many organisations use a Configuration Management Database (CMDB) in which the documentation of the various components of an organisation is stored. Both experts mentioned that systems should already be prioritized during the analysis of the system landscape. They said that the systems should be prioritized during this analysis based on their relevance for the organisation. The background to this prioritization is that initial use cases can already be derived from such an analysis. In the case study, the organisation's systems were also prioritized for the subsequent definition of the use cases and log sources to be considered during the initial deployment. In addition, such prioritization can be used to determine which logs from which systems must be sent to a SIEMS. Within the analysis of the initial situation,

the IT strategy of the organisation would still have to be examined and aligned, according to one expert. This should already take place before the stakeholder analysis and analysis of the system landscape. The IT strategy of an organisation can already be used to gather initial findings. The analysis of the IT strategy makes it possible to find out what goals the IT organisation wants to achieve by introducing a SIEMS. Additionally, arguments for an investment in a SIEMS can be gathered, which have a direct impact on the achievement of the corporate strategy goals. Apart from that, one expert said that by analysing the IT strategy, high level use cases and requirements can already be derived, which in turn could be considered as a basis for the next activity. About the security frameworks, the interviews showed that the process model contains references to the internationally known frameworks at the necessary points that are relevant in the SIEM context. In addition to the MITRE Att&ck Framework, one expert mentioned the SPEED SIEM Use Case Framework by Jurgen Visser for defining relevant use cases. The mentioned framework should support an organisation in structuring, categorizing, defining, and describing use cases. The case study showed that a Proof of Concept (PoC) after a system was selected would have been beneficial to show the people who will later work with the system what the system can do and how their current workflow will be enriched by a SIEMS.

Deployment phase: Both subject matter experts said that the deployment phase can be carried out in the manner described and includes the elements that must be present in a SIEMS project from a high-level perspective. Nevertheless, there were two suggestions for improvement: In the contract signing activity, one expert found the topic of service level agreement (SLA) missing, which is particularly essential for cloud-based SIEMS. The other expert noted that the architecture was not considered in the installation and preparation activity. According to the expert, the architecture should be a concept that includes the structure, the defined use cases and the log sources required for them and the roles and authorization management. For the creation of this concept, the artifacts created so far can be used and combined into one document. Based on this concept, the iterations for the log sources and the use cases integration could be used in the further course of the deployment phase. The log sources and use cases could then be transferred from the concept to a Scrum Board, which the project team should use in the iterative process of deployment phase. Regarding the references to methods and security frameworks, the experts said that no important framework was missing or that further references to methods should be added to the model.

Operation phase: According to the subject matter experts, the operation phase includes all activities, results and tasks that are required for the handover of the SIEMS. In addition, it was mentioned that the activity 'Operation, Maintenance and Further Development' shows that a SIEMS is not only introduced once through an initial deployment but must iteratively be further developed and adapted from the organisation. In this context, it was criticized that the same element for the agile way of working should be used for the deployment phase as for the modelling in the operation phase. This would show more clearly that the iterations which are carried out during the connections of the log sources should be carried out again in the operational phase. Regarding the Security Framework references, there were no comments from the experts that further requirements must be fulfilled to operate a SIEMS. Instead, the creation of a RACI matrix (Responsible, Accountable, Consulted, and Informed) was suggested, which would be beneficial for defining at least the responsibilities and accountabilities. The expert justified this statement by emphasizing that such a matrix clearly and transparently defines related tasks, responsibilities, accountabilities and communication flows for decisions and changes in the organisation.

6.2 Practical Case Study

As outlined in section 2, as methodological approach a case study was conducted in a Swiss retail organisation to challenge the development of EDO4SIEM. The retail organisation was actively assessing and implementing a SIEMS, whereas the operations phase was yet to come. With the active participation of one of our researchers in the case study, valuable firsthand experience was acquired and leveraged for our research process. In more detail, the decision to implement a SIEMS by the Swiss retail organisation in 2021 stemmed from the lack of centralized management for its system logs. The introduction of the SIEMS facilitated centralized log management, simultaneously enhancing visibility in terms of information security and cybersecurity. Real-time log analysis and anomaly-triggered alerts were key features of this improvement.

Initiating the process, an evaluation phase was conducted to identify a suitable SIEMS aligning with the organisation's requirements. In collaboration with us as scientific advice board, a research team comprising four junior and one senior academic personnel undertook the evaluation process in several sequentially processed phases. This sequential approach was chosen for its pre-planned feasibility in organising the phases and activities. Various methods and tools were employed across different phases and activities to yield specific results, such as an early-stage stakeholder analysis. What worked well was the structuring and documentation of stakeholder requirements according to the KANO model. The latter involves defining functional and non-functional requirements as well as that all evaluated requirements are divided into basic, performance and excitement features (Hicking & Völkel, 2022).

For the definition of use cases the MITRE Att&ck Framework were consulted and tactics, techniques, and sub-techniques were used. An obvious use case could be the detection of phishing emails without having to rely on any user. In the MITRE Att&ck Framework, phishing is one technique (ID T1566) within the tactic 'Initial Access'. The framework provides procedure examples for the techniques and how these can be detected and mitigated. In this case, the framework also provides information on five measures that can be used to prevent phishing attacks: 1) Antivirus software (M1049): Suspicious files are quarantined; 2) Network Intrusion Prevention Systems (M1031): Scanning of emails to detect malicious attachments or links, which are automatically removed; 3) Restrict Web-Based Content (M1021): Blocking certain websites or attachment types that could be used for phishing; 4) Software Configuration (M1054): Use of anti-spoofing and email mechanisms that can be used to check the validity of the sender domain and the integrity of the message; 5) User Training (M1017): Educate and train users to recognise phishing emails themselves.

The MITRE Att&ck Framework can be used to define which log sources could be used to detect phishing attacks. Furthermore, data sources and their data components are named, which should support the detection like network traffic and application logs and file creation events on the computers from the employees of the company.

Following the completion of the evaluation, the Swiss retail organisation, based on a preference matrix, selected the most suitable product, marking the commencement of the deployment phase. The system implementation was undertaken in partnership with a service provider experienced in deploying the chosen SIEM product. Due to necessary data accessibility during implementation by both the retailer's staff and the service provider's cybersecurity engineers, signing confidentiality and data processing agreements was imperative. As next activities, the deployment and integration of log sources were planned, defining the logs to be

integrated based on the earlier evaluation. This involved installing on-premises servers for linking log sources, collecting logs from internal systems, and forwarding them to the cloud-based SIEMS. The iterative connection of logs, achieved through an agile approach, proved effective. Filters were developed and applied to selectively send relevant logs to the SIEMS, and each log source underwent scrutiny to ensure complete and accurate transmission and processing. The agile log connection, executed through iterative processes, demonstrated success in planning and executing activities for each log source within a designated one-week timeframe per iteration. This structured, sequential approach, previously employed during the evaluation, facilitated adherence to a stringent schedule, ensuring timely delivery of various required results.

An early definition of the use cases which needs to be mapped with the selected system was identified as particularly important in the reflection on the case study. In addition, the MITRE Att&ck Framework could be used to define the use cases. Furthermore, referencing the ISO/IEC 27001:2013 standard and the NIST CSF helped the Swiss retail organisation to appropriately prioritize relevant security features, such as access management, when deploying the SIEMS.

6.3 The Final EDO4SIEM

Based on the validation results, the first EDO4SIEM (https://bit.ly/3C9UHaIL) was iteratively revised and newly visualized (Figure 2). As outlined above (section 5) EDO4SIEM consists of three phases:

Phase 1: The evaluation phase includes four activities (blue boxes) that support an organisation in evaluating SIEMs that meets defined requirements. These activities must be completed sequentially, as in each case the results of the previous activity are assumed for the next activity. In this phase, there is the possibility to jump back from one activity to the previous one if results or task were not completed correctly or completely. For each activity there are various tasks and corresponding results.

Phase 2: In the subsequent deployment phase, it is assumed that the evaluated SIEMS is (now) implemented based on the two activities assigned.

Phase 3: The final operation phase deals with the handover of the SIEMS to operations. Like in the previous phase, the first two activities support the transfer of the transition of the SIEMS to operations. The first activity ensures that user documentation is created, and responsibilities and operational processes are defined and documented. After the users have been trained and have received all documentation and information, the SIEMS can be handed over for continuous operational use, maintenance, and further development.

As indicated in Table 1, the procedure model should incorporate references to diverse methods and cybersecurity frameworks applicable across different phases and activities (R5). Informed by literature research and a comprehensive analysis of the practical case study, several references were integrated into the first prototyping EDO4SIEM model, visually represented besides the tasks in Figure 2. Even though more security frameworks have been aligned with our model during the research process, the focus was set on the ISO/IEC 27001:2013, NIST CSF, and MITRE Att&ck Framework.

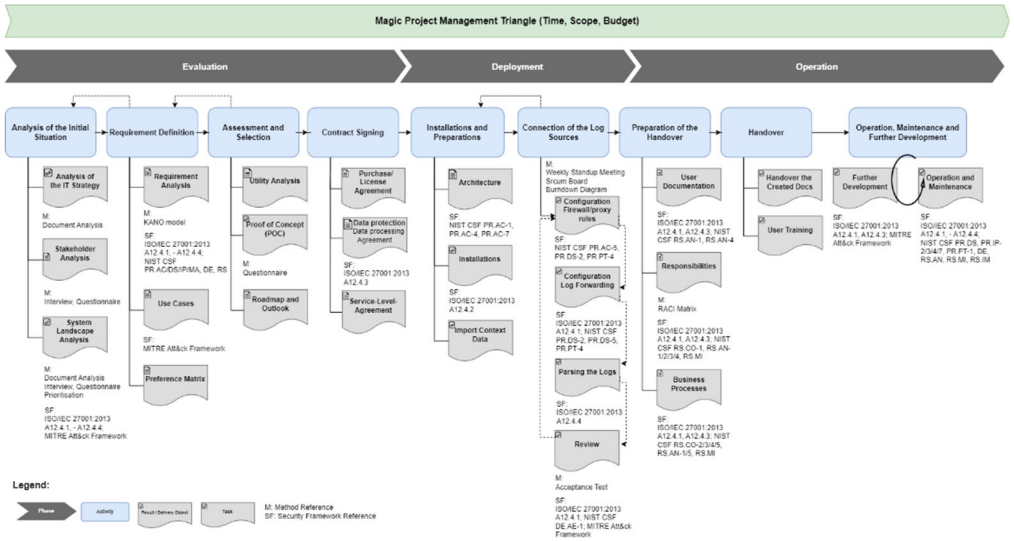

Figure 2. EDO4SIEM – Validated Prototype

7. CONCLUSION AND OUTLOOK

With our research, we exposed the research gap, that there is no model nor generic guide available to evaluate, deploy, and operate a SIEMS. By conducting a literature review, fundamental disparities of log management and a SIEMS were outlined. To develop a new prototypical model for the establishment of a SIEMS, traditional models and cybersecurity frameworks were investigated. It was researched whether the waterfall model, the V-Model XT and the Scrum approach can be used for SIEM projects. Furthermore, three highly recognized frameworks/standards – the NIST CSF, the ISO/IEC 27001/2 and the MITRE Att&ck were examined regarding suitable elements for our first prototype; the result was a newly developed and validated model – the EDO4SIEM.

Furthermore, EDO4SIEM was reflected by means of a practical case study at a Swiss retail organisation. The development of the artifact and the practical case study took place at the same time in many parts. The following further measure is desired for the future: EDO4SIEM should be applied in organisations to prove its general use in practice. Through systematic supervision and evaluation, the model could be further improved and, if necessary, expanded. Currently, the model contains a manageable number of references to three cybersecurity frameworks. It would be conceivable that in a next stage further frameworks, standards, or best practices could be identified, which could be enhance the theoretical background in a SIEMS project. To keep the model clear and simple, an additional diagram could be created in which the various references could be categorized and catalogued.

But even in the first prototype version, EDO4SIEM offers many significant advantages that can be used in a SIEM project in any organization: 1) it is based on existing and well-recognized project management methods and can therefore be applied in a straightforward manner, 2) it holistically covers the phases ’Evaluation’, ’Deployment’ and ’Operation’ of a SIEM project, 3) it is generic and can be used independently of any vendor or product, 4) it is based on agile

methods and approaches, which makes it flexible and adaptable, 5) as a special feature, it contains references to further methods based on cybersecurity frameworks and standards.

This research contributes to solving the problem that so far there is no model for the establishment of a SIEMS. Using Kuechler and Vaishnavi´s (Figure 1) approach, we created a methodologically grounded artifact that is publicly available. Our research is intended to produce a benefit for practitioners who are responsible for a SIEMS establishment in their organisation. Likewise, the model is at disposal for critical appraisals, further developments, and adaptations of the research and practitioner community.

REFERENCES

AlienVault, 2021. *The SIEM Evaluator's Guide*. At&t. Retrieved from https://cdn-cybersecurity.att.com/docs/guides/The-SIEM-Evaluators-Guide.pdf

Asprion, P. M. et al., 2023. Agile Management in Cybersecurity. *Proceedings of Society 5.0 Conference, Vol. 93.* University of Pretoria, South Africa, pp. 21-32.

Broy, M. and Kuhrmann, M., 2021. Vorgehensmodelle in der Softwareentwicklung. In M. Broy, & M. Kurhmann (Eds.), *Einführung in die Softwaretechnik* (pp. 83-124). Springer: Heidelberg.

Bygrave, L. A., 2022. Cyber Resilience versus Cybersecurity as Legal Aspiration. *14th International Conference on Cyber Conflict: Keep Moving! (CyCon)*. Tallin, Estonia, pp. 27-43.

Chuvakin, A., 2010. *The complete guide to log and event management*. White Paper. Retrieved from https://www.netiq.com/en-gb/docrep/documents/m47h82fbmy/the_complete_guide_to_log_and_event_management_wp_ee.pdf

Eurostat, 2023. *22% of EU enterprises had ICT security incidents*. News Article. Retrieved from https://ec.europa.eu/eurostat/web/products-eurostat-news/w/edn-20230214-1

González-Granadillo, G., González-Zarzosa, S. and Diaz, R., 2021. Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures. *Sensors,* Vol. 21, No. 14, 4759.

Hevner, A. R. et al., 2008. Design science in information systems research. *Management Information Systems Quarterly*, Vol. 28, No. 1, pp. 75-105.

Hicking, J. and Völkel, A., 2022. Anforderungsmanagement. In G. Schuh, V. Zeller, & V. Stich (Eds.), *Digitalisierungs- und Informationsmanagement Handbuch Produktion und Management 9* (pp. 249-296). Springer: Berlin, Heidelberg.

Holik, F. et al., 2015. The deployment of security information and event management in cloud infrastructure. *25th International Conference Radioelektronika (RADIOELEKTRONIKA)*. Pardubice, Czech Republic, pp. 399-404.

Humphreys, E., 2016. *Implementing the ISO/IEC 27001: 2013 ISMS Standard*. Artech house.

IBM Security, 2023. *Cost of a Data Breach Report 2023*. Retrieved from https://www.ibm.com/reports/data-breach

Kavanagh, K. M., Rochford, O. and Bussa, T., 2021. *Magic quadrant for security information and event management*. Gartner Group Research Note. Retrieved from https://www.gartner.com/en/documents/4003080

Kent, K. A. and Souppaya, M., 2006. *Guide to Computer Security Log Management. Recommendations of the National Institute of Standards and Technology*. Special Publication 800-92. Retrieved from https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-92.pdf

Kneuper, R., 2018. *Software processes and life cycle models*. Springer: Cham.

Kuechler, B. and Vaishnavi, V., 2008. On theory development in design science research: anatomy of a research project. *European Journal of Information Systems*, Vol. 17, pp. 489-504.

Lucht, D., 2019. *Theorie und Management komplexer Projekte*. Springer: Wiesbaden.

Mehta, D., 2021. Setting up a Splunk Environment with AWS. In D. Metha (Ed.), *Splunk Certified Study Guide: Prepare for the User, Power User, and Enterprise Admin Certifications* (pp. 395-419). Berkeley, CA: Apress.

Miloslavskaya, N., 2018. Analysis of SIEM systems and their usage in security operations and security intelligence centers. *Biologically Inspired Cognitive Architectures (BICA) for Young Scientists: Proceedings of the First International Early Research Career Enhancement School on BICA and Cybersecurity (FIERCES 2017)*. Moscow, Russia, pp. 282-288.

Mokalled, H. et al., 2019. The guidelines to adopt an applicable SIEM solution. *Journal of Information Security*, Vol. 11, No.1, pp. 46-70.

NIST, 2018. *Framework for improving critical infrastructure cybersecurity*. Retrieved from https://nvlpubs. nist. gov/nistpubs/CSWP/NIST. CSWP, 4162018.

Royce, W. W., 1987. Managing the development of large software systems: concepts and techniques. *Proceedings of the 9th international conference on Software Engineering*. Monterey, CA, USA, pp. 328-338.

Safarzadeh, M., Gharaee, H. and Panahi, A. H., 2019. A novel and comprehensive evaluation methodology for SIEM. *Information Security Practice and Experience: 15th International Conference (ISPEC 2019)*. Kuala Lumpur, Malaysia, pp. 476-488.

Sahay, R., 2020. Azure Monitoring. In *Microsoft Azure Architect Technologies Study Companion: Hands-on Preparation and Practice for Exam AZ-300 and AZ-303*, pp. 139-167. Apress.

Sahoo, P. K. et al., 2012. Syslog a Promising Solution to Log Management. *International Journal of Advanced Research in Computer Science*, Vol. 3, No. 3, pp. 584-588.

Salitin, M. A. and Zolait, A. H., 2018. The role of User Entity Behavior Analytics to detect network attacks in real time. *2018 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*. Sakhier, Bahrain, pp. 1-5.

Schatten, A. et al., 2010. *Best practice software-engineering: Eine praxiserprobte Zusammenstellung von komponentenorientierten Konzepten, Methoden und Werkzeugen*. Springer-Verlag: Heidelberg.

Scherb, C. et al., 2023. A Cyber Attack Simulation for Teaching Cybersecurity. *Proceedings of Society 5.0 Conference 2023, Vol. 93*. University of Pretoria, South Africa pp. 129-140.

Shahid, N. and Shah, M. A., 2021. Anomaly Detection in System Logs in the Sphere of Digital Economy. *Competitive Advantage in the Digital Economy (CADE 2021).* Online Conference, pp. 185-190.

Takeuchi, H. and Nonaka, I., 1986. The new new product development game. *Harvard business review*, Vol. 64, pp. 137-146.

Vielberth, M., 2021. Security information and event management (SIEM). In S. Jajodia, P. Samarati, M. Yung (Eds.) *Encyclopedia of Cryptography, Security and Privacy* (pp. 1-3). Springer: Heidelberg, Berlin.

Yelevin, L. and Batami, G., 2022. *Classify and analyze data using entities in Microsoft Sentinel*. Retrieved from https://docs.microsoft.com/en-us/azure/sentinel/entities