Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Computer Science

Hege Aalvik

Towards an Effective Security Champions Program

Master's thesis in Computer Science
Supervisor: Daniela Soares Cruzes
June 2022

NTNU
Kunnskap for en bedre verden

Hege Aalvik

Towards an Effective Security Champions Program

Master's thesis in Computer Science
Supervisor: Daniela Soares Cruzes
June 2022

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Computer Science

NTNU
Norwegian University of
Science and Technology

Abstract

Over the past few decades, malicious attacks have become a major concern for the software industry. The software industry struggles to create secure software due to a lack of security experts and developers who perceive security as something "mysterious." A security champion is a developer who has taken on the role of advocating for security in their team and could be an effective way of creating more security awareness in the development teams. However, there is currently little research on the subject. This master's thesis aims to investigate security champions and look into how companies are establishing security champions programs, the challenges, and what is an effective approach.

A systematic literature review was performed as a part of a pre-study for this thesis, and the findings were used to create a suggested approach to how a security champions program can be established and maintained in a company. The approach is further investigated in this study, using a case study with a questionnaire and interviews as data generation methods to verify whether the approach found in the pre-study is, in fact, effective.

The study contributes to research by being one of the first studies to investigate security champions programs further. The findings are important for the industry because they offer companies a credible strategy for establishing a security champion program by providing an academic framework. The research provides companies with insight into the thoughts and opinions of security champions, allowing them to better identify the areas that require focus and the needs of the security champions. The main contribution of the research is a set of validated steps on how to establish and maintain a security champion program.

Key-words: *security champions, software security, secure software engineering, security culture, security awareness*

Sammendrag

I løpet av de siste tiårene har ondsinnede dataangrep blitt en betydelig bekymring i programvareindustrien. Bransjen sliter med å lage sikker programvare grunnet mangel på sikkerhetseksperter og utviklere som oppfatter sikkerhet som noe mystisk. En security champion er en utvikler som har tatt på seg rollen som forkjemper for sikkerhet i teamet sitt og kan være en effektiv strategi for å gjøre utviklingsteam mer sikkerhetsbevisste. Likevel er det foreløpig svært lite forskning på temaet. Denne masteroppgaven tar sikte på å undersøke security champions og ser på hvordan selskaper etablerer security champions programmer, utfordringene de møter, og hva som er en effektiv tilnærming.

Et systematisk litteratursøk ble utført som en del av en forstudie til dette prosjektet, og funnene derfra ble brukt til å lage et forslag til hvordan et security champions program kan etableres og vedlikeholdes i et selskap. Tilnærmingen fra forstudiet ble videre undersøkt i dette prosjektet, ved å utføre en casestudie med et spørreskjema og intervjuer som datagenereringsmetoder.

Studien bidrar til forskning ved å være en av de første studiene som videre undersøker security champions programmer. Funnene er viktige for industrien fordi de tilbyr bedriftene en troverdig strategi for å etablere et security champions program ved hjelp av et akademisk rammeverk. Forskningen gir bedriftene innsikt i tankene og meningene til security champions, slik at de bedre kan identifisere områdene som krever fokus og hva security champions trenger. Hovedbidraget fra denne studien er et sett med validerte steg for hvordan man etablerer og vedlikeholder et security champions program.

Nøkkelord: *secuirty champions, programvaresikkerhet, sikker programvareutvikling, sikkerhetskultur*

Acknowledgements

First and foremost, I would like to show my gratitude and appreciation to my supervisor, Professor Daniela Soares Cruzes, for her exceptional guidance and engagement throughout this year. Without her assistance and expertise in the field, this project would not have been possible. Further, I want to thank Anh Nguyen Duc for using his knowledge in the domain to provide valuable recommendations and feedback.

I would also like to give a great thanks to Matti Paavilainen for the collaboration. The close cooperation has been a great experience, and his contribution and participation have been much appreciated.

This master's thesis was done in cooperation with Visma. I would like to thank everyone who made that possible, especially Monica Iovan, who provided insight and expertise that greatly assisted the research. In addition, I would like to thank all the participants in the case study who voluntarily agreed to use their time to share their opinions and experiences.

Lastly, I would like to thank the Norwegian University of Science and Technology (NTNU) and the Department of Computer Science (IDI) for their excellent services and facilitation of a great learning experience.

Table of Contents

List of Figures

List of Tables

Acronyms

EU European Union. 5, 14

GDPR General Data Protection Regulation. 5

IDI Department of Computer Science. iii

NSD Norwegian Centre for Research Data. 5

NTNU Norwegian University of Science and Technology. iii, 4, 5

SE Security Engineer. 14–16, 19–22, 24–31, 33–40, 42–49, 51, 57, 58, 68

SMI Security Maturity Index. 15, 20, 23

SSA Security Self-Assessment. 15, 39, 46

VASP Visma Application Security Program. 14, 15, 45, 68

Chapter 1

Introduction

A security champion is a developer with a particular interest in security who has agreed to take on the role of advocating for security in their team [1]. The security champion is not responsible for the security of their team's project but rather serves as a resource for guidance and support on security issues [2]. The champion's job is to promote security best practices and introduce security in the early development life-cycle [3]. Because the security champion is personally invested in the project, she can communicate security concerns to the development team in a way that will be understood and appreciated [4]. The security champion will ensure that the team focuses on security throughout the product's development phase, even though the developers often perceive security as inconvenient, unimportant, expensive, or even mysterious, leading to low adoption [5]. The goal is to increase security awareness, security functions, and software security in general [2].

1.1 Motivation

Software security is the idea of engineering software so that it continues to function correctly under malicious attacks [6]. During the last decades, malicious attacks have grown to become a major concern in the software industry. Attacking software systems has gotten easier as a result of the Internet's popularity [7], and by exploiting flaws in the source code, hackers can obtain access to sensitive information and software systems. The consequences can be severe, especially for companies that might suffer considerable financial losses. In 2020, the cost of cyber-crime was estimated to be around 945 billion US dollars [7]. Preventative measures were predicted to cost roughly 145 billion dollars, bringing the total cost to around 1 trillion dollars, or somewhat more than 1% of the global gross domestic product [7].

Despite the numerous studies offering new approaches, strategies, guidelines, and tools to improve software security, the number of security faults and vulnerabilities reported each year continues to rise [8][7]. The threats are constantly evolving, and in 2019, 144,91 million new forms of malware were discovered [7]. There are multiple reasons why

companies struggle to withstand attacks. However, one factor that has been mentioned in several studies is the lack of security focus throughout the software development process [9][10], often due to developers' lack of security expertise and interest [11]. Most developers are not security experts but still have to develop systems that require security features [11]. In addition, they find it challenging to use static analysis tools to detect security vulnerabilities due to large numbers of false positives, lack of collaboration support, and complicated tool output [1].

Another reason is the prevalence of the bolt-on approach. The bolt-on approach's philosophy is to "make it work, and then make it right," and is one of the most common approaches to security in software teams [10][11]. The strategy results in a development process that ignores security until the very end and then tries to fix mistakes made earlier in the process [10]. There is a presumption that just enough security can be applied to get the job done [10]. Meier [10] claims that this approach always results in failure or at least inefficiency.

Most businesses have a security team to assist with software security. However, this is usually a restricted resource. Every organization has a budget and a security team that is of limited size [12]. The security professionals have their hands full with a constantly evolving set of threats, and the reality is that there is never enough money or qualified employees to fulfill all of the security responsibilities that are required [12]. Increasing the involvement of the developers in the security processes could relieve the security team of some of their workload and allow them to focus on more advanced cases. Despite this, research reveals that developers are rarely involved in the security processes [1]. Many developers believe that security is the responsibility of others, and as a result, they avoid engaging [1][13].

Providing employees with information and basic security training has proven insufficient to ensure better and consistent security behaviors [14]. Individuals adjust their behavior to fit with the group they identify with [14], and often will a person joining a group quickly, and maybe unwillingly, adopt the mindsets and practices of the group [15]. Therefore is developing a solid security culture inside development teams an effective strategy to improve software security. Companies must foster a culture where security is everyone's responsibility and doing the right thing is the norm [16]. However, creating a security culture can be challenging. Employees' habits are more likely to be influenced by their bosses and colleagues than security managers, according to research [17]. Because of this, Guo et al. [17] recommend that organizations train a "power user" who can act as a role model and a resource for other employees in the same team when they deal with security issues. Establishing a security champion network will be an efficient technique for building a security culture.

Existing research on security champions is limited. It is a new field of study, and very few papers are available. Even so, software companies seem curious and are asking for more research. Security champions are a new role and not widely spread, and as a result, not many companies have evidence of the best practices and how to implement the role. Having more companies adopt a security champions program will make it easier to conduct more research and gain deeper insight. Therefore, this thesis aims to take a deep dive into security champions and figure out how a security champions program is best established

and maintained in a company and what challenges the companies are facing.

1.2 Research Questions

The objective of this thesis is to investigate further how to establish a security champions program in a company with agile teams and understand what challenges the companies are facing.

The following research questions are examined in this thesis:

RQ1: How are security champions programs implemented in agile software projects?

RQ2: What are the challenges and improvements for implementing a security champions program?

RQ3: What is an effective way to establish and maintain a security champions program in an agile context?

1.3 Research Process

The research process is depicted in Figure 1.1, and the chosen research methods are marked in red.

The initial step of the research process was to conduct a literature review. The literature review was undertaken to learn more about the topic and better understand existing research and the gaps in the field. The three research questions and a conceptual framework were formed based on this. More information about the pre-study can be seen in Chapter 2.

A case study in two phases was then undertaken to answer the research questions. Phase 1 consisted of an electronic questionnaire, and Phase 2 consisted of semi-structured interviews. A case study was applicable because the goal was to test an existing theory using rich descriptive data from the phenomenon's real-life context [18]. A survey was not chosen as the research strategy because I wanted comprehensive and descriptive data from the research, and according to Oates [18], surveys only provide a general overview of the studied phenomenon and tend to focus on breadth of coverage instead of details.

Finally, the data was examined. Both quantitative and qualitative data analysis methods were used. An expert interview was conducted to validate the findings.

More details about the research methodology are presented in Chapter 3.

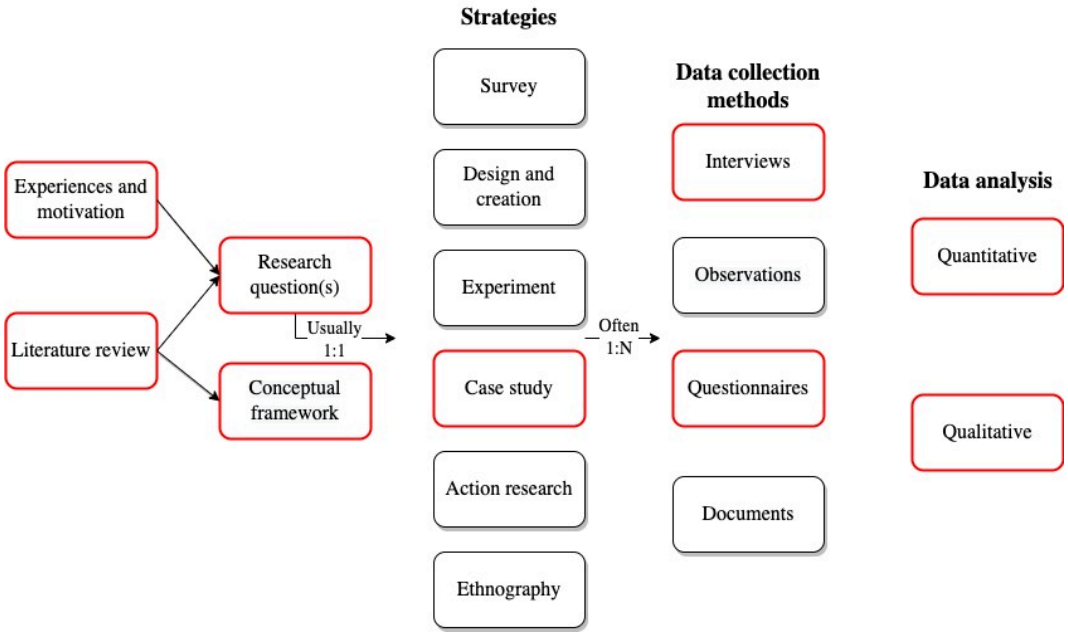


Figure 1.1: Overview of the research process, adapted from Oates [18].

1.3.1 Research Paradigm

As the research aims to identify a set of steps that companies can use to establish a security champions program, it is reasonable to assume that researchers working during different periods and locations will reach the same conclusions about the phenomenon under study. Further, the researchers will act as objective observers, observing events that exist independently of them and will not impact or disturb what they observe. Therefore, it is fair to conclude that the study will fall within the philosophical research paradigm of positivism.

1.3.2 Research Scope

Research questions RQ1 and RQ2 are limited to the companies within Visma. Research question RQ3 is focused on investigating the steps found in the pre-study. The thesis will essentially focus on confirming or refuting whether these are effective and investigate how the steps are best carried out.

1.3.3 Ethics

According to Oates [18], it is crucial to be ethical when doing research, and the researchers have to pay close attention to the rights and responsibilities of those involved. This study collected personal data via a questionnaire and interviews, and the researchers had to be careful not to violate any of the participants' rights. All data were collected according to the guidelines for data collection provided by NTNU [19]. The participants

were informed of their rights, and it was highlighted that all data were anonymized. Because the interviews were recorded, it was essential to ensure that the handling of these was according to the Norwegian General Data Protection Regulation (GDPR) law and guidelines for research. A data management plan was submitted to Norwegian Centre for Research Data (NSD) to ensure that the data collection and management would be in line with the requirements of the Research Council of Norway and the European Union (EU). The data management plan was approved on 28.01.22 and can be seen in totality in Appendix A.

Completing the questionnaire was voluntary, and rights and contact information for questions and complaints were provided at the beginning of the questionnaire. All the participants in this study work within Visma. Because Visma has a data processing agreement with Google, we used Google Forms to collect data from the questionnaire.

For the interviews, we used Microsoft Teams, and all the collected data were stored in SharePoint because NTNU has a data processing agreement with Microsoft. Consents for processing the personal info obtained through the interviews were collected at the beginning of each interview. Rights were readout, and the participants were asked whether they consented to the researchers processing the data. Transcripts of the interviews, including the consent, were sent to participants after the interviews. As a result, the interviewees also received their rights in writing. The oral consent form was created according to the guidelines created by Oates [18] and can be seen in Appendix B.

The data in this project was collected in collaboration with a student from the JAMK University of Applied Sciences. All the respondents were informed that the collected data would be used by both the researchers in two different theses. The collected data will be deleted after the submission of both the theses around the end of June 2022.

1.4 Contribution

There exists little research on security champions. This study is one of the first studies to further investigate security champions and see how a security champions program is best established in a software company. There is a gap in the knowledge about security champions, and only seven papers were found in the structured literature review. This thesis takes basis in former research, trying to fill the gaps and facilitate further research, as well as helping the companies by proving a method for establishing and maintaining a security champions program.

1.5 Outline of the Thesis

The rest of the thesis is organized as follows: Chapter 2 covers relevant background and subjects related to the research. The background chapter also presents a pre-study, including a literature review conducted prior to this project. Chapter 3 describes how the research has been planned and conducted and the reasoning behind important choices.

Chapter 4 presents the findings from the research. The results are then discussed in Chapter 5, which includes implications for research, implications for practice, limitations, and further work. The conclusion of the thesis can be read in Chapter 6.

Chapter 2

Background

This section provides an introduction to the main concepts concerning security champions and other relevant backgrounds for the research.

2.1 Software Security in Agile Teams

Agile software development is an umbrella term for a set of frameworks and practices based on the values expressed in the Manifesto for Agile Software Development and the 12 Principles behind it [20]. Examples are Scrum and Extreme programming (XP). Agile methods are associated with better productivity, higher quality, and customer satisfaction [21]. The methods have rapidly grown in popularity [2] and are expected to grow until most software is produced in an agile way [12].

However, agile methods make creating secure software challenging. Because the iterations are short, it is difficult to fit in time-consuming security activities. Due to the high development speed, developers will often prioritize their implementation tasks over security [1]. It is also common for the customer to lack security knowledge and cannot state security requirements for their product [21]. Few agile teams have a good grasp of the threats that face their system; they do not know what risks they are taking, they do not track or do anything to mitigate those risks, and they often do not know who is attacking their software [12]. As a result, current studies show that agile teams frequently neglect security [2][12][22][23][24].

This thesis is written in the context of agile development teams.

2.2 Security Champions

As mentioned in the introduction, a security champion is a developer with a particular interest in security who has agreed to take on the role of advocating for security in their

team [1]. In addition to assisting in creating security awareness within the team, one of the security champion's key responsibilities is to ensure communication between the security team and the developer team [1]. The security champion serves as an important liaison between the teams and helps extend the efforts of the security experts, which is often of limited quantity [1][25].

To better understand the security champion's work, typical tasks found in case studies are listed in Table 2.1.

Table 2.1: Typical security champion tasks found in research papers.

Typical security champion tasks	**Source**
Motivate developers to write safe code and fix the security problems founds	[1]
Contribute to security awareness	[2][16][14]
Help developers follow the security policies given by their company	[14]
Organise security briefings in their teams	[14]
Ensure that security is not a blocker on active development or reviews	[2]
Help integrate security into the software development life cycle	[2]
Show developers how to use cryptographic libraries, authentication functions, and key management	[2]
Help team report phishing emails and scam phone calls	[16][14]
Participate in peer reviews	[1][2]
Help with quality assurance and testing	[2]
Assist in making security decisions for their team	[2]
Get the opinion from the security team about upcoming changes or questions to the company's Security Program	[2]
Report back valuable insights to the security team	[16][14]
Engage and introduce "non-security" people into security	[2]

As seen in the table, the security champions' job is to help the security team with straightforward but essential tasks and create a better security culture within the team.

Usually, no formal security training is needed to become a security champion [1]. During their role, the champion will gain security knowledge on a basic level. In addition to security knowledge, a successful champion needs a set of soft skills. Because the primary function of the champion is to advocate and motivate, the champion must be good at communicating. Positive and genuine disposition in interactions with others and the ability to build relationships are mentioned as important personal characteristics for a champion [26].

2.3 Pre-study

A pre-study for this thesis was conducted in the fall of 2021. The objective was to do a literature review to investigate approaches to establishing and maintaining a security champions program in an organization. Because security champions are a relatively new

phenomenon, the thesis also investigated if theories from other research fields existed that could be applied to security champions.

The research questions of the pre-study were as follows:

RQ1: What is an effective way to establish and maintain a security champions program in an organization with agile software development teams?

RQ2: What other theories can be applied to security champions?

2.3.1 Pre-study Research Design

Firstly, a broad search on the internet was conducted. The search was done to investigate if there was any information about the security champions outside published research papers. The search resulted in 23 different activities to establish and maintain a security champions program. However, most of the guidelines were proposed by companies offering consulting, creating bias in the results. The OWASP Playbook stood out as a more reliable source as it is a nonprofit foundation that works to improve software security.

Then a systematic literature review was conducted. The review resulted in seven papers regarding security champions. As mentioned, security champions are a relatively new field. This claim was proven by looking at the publishing year of the found papers. Four of the seven papers were published in 2021, the year the literature review was conducted. However, this also indicates that the subject is currently being researched. The results from the structured literature review proved that the grey literature and the research literature propose similar approaches.

Due to not finding many papers, a non-systematic literature review was also conducted. The objective was to find other theories that could be related to the security champions. Four papers were found.

Both the literature reviews were conducted according to the guidelines proposed by Kitchenham [27]. The papers found in the pre-study can be seen in Appendix C.

2.3.2 Pre-study Results

A categorization system containing 14 categories was created to summarize the actions found. The created categories are presented in Table 2.2.

Table 2.2: Description of the categories adapted from the prestudy.

ID	Category	Explanation
Ct1	Management and stakeholders	Actions regarding how the management and stakeholders are involved.
Ct2	Define the role	How the security champions role and responsibilities is defined.
Ct3	Assessment	Assessing the security of the security champion's project.
Ct4	Recruitment	The recruitment process of the security champion.
Ct5	Training	Training and skill development for the security champion.
Ct6	Communication	Communication between security champions and other relevant people.
Ct7	Meetings	Regular meetings between the security champions.
Ct8	Resources	Resources to support the security champion.
Ct9	Feedback	Collecting feedback to improve security champion program.
Ct10	Automation	Automation of security champion activities.
Ct11	Time	Allocation of time for security champion tasks.
Ct12	Motivation	Actions to keep the security champions motivated.
Ct13	Support from the security team	Support from and services the security champion can request from the security team in the organization.
Ct14	Measure results	Measure success and milestones.

All the actions found were then sorted into the categories. This is presented in Table 2.3.

Table 2.3: Categorization of actions found in research papers, adapted from the prestudy. The sources can be found in Appendix C.

ID	Activity	Source
Ct1 Management and stakeholders		
A1	Software security person as driving force	S1.1
A2	Create briefing document for the managers	S2
A3	Have stakeholders support the program within the company	S3
A4	Attain top management commitment	S8, S9
A5	Get requisite decision making authority	S11
Ct2 Define the role		
A6	Define role, responsibility and main skills	S2, S3
A7	Provide clear expectations about what the champion role involves	S11
Ct3 Assessment		
A8	Assess current state, define ideal future, analyze the gap, and determine the steps needed	S9
A9	Define the specific business problem and develop strategic action plan	S8
Ct4 Recruitment		
A10	Let champions volunteer	S1.1, S1.2, S3, S11
A11	If not enough volunteers, appoint people for the role	S1.2, S11
A12	Identify person with interest	S1.1, S1.2, S3
A13	Select potential champions	S8, S10
Ct5 Training		
A14	Individual skill development	S1.1
A15	Skill development performed on demand	S1.2
A16	Training in groups of max 10 employees	S2
A17	Educate employees, train to perform the champion role	S8, S9, S10, S11
A18	Training with reward system	S8
Ct6 Communication		
A19	Set up communication channels: Email, Slack	S1.1, S1.2, S10
A20	Set up communication channels: Monthly newsletter, internal website, Yammer, Facebook.	S2
Ct7 Meetings		
A21	Bi-weekly meeting with the security champions to discuss and share information	S1.1, S1.2
Ct8 Resources		
A22	Page with links for learning materials and list of courses and conferences	S1.1
A23	Cyber-security hub with support and materials	S2
Ct9 Feedback		
A24	Retroperspective after 6 months	S1.1
A25	Collect feedback from the employees	S3, S8
A26	Provide feedback to the employees	S9
Ct10 Automation		
A27	Automate activities like onboarding and training to make the program more scalable	S3
Ct11 Time		
A28	Pre-allocate time for working on security	S1.1, S11
Ct12 Motivation		
A29	Create small wins	S8
A30	Recognition and rewards in form of career development (pay increase or promotion)	S10, S11
Ct13 Support from the security team		
A31	Request services like briefing on latest threats, phishing drills, or tour of the security department	S3
Ct14 Measure results		
A32	Identify metrics, measures and milestones	S8, S9

The pre-study concludes with a proposed approach for establishing and maintaining a security champions program. The steps are presented in Table 2.4. Furthermore, the study confirmed that the approaches proposed by the industry corresponds to the approach found in the research literature. The proposed approach from the pre-study was used as the basis for this thesis, where I investigated whether the steps in the suggested approach is effective and go more into detail on how the steps should be carried out.

Table 2.4: Proposed approach for establishing a security champion program, adapted from the prestudy.

ID	Step	Reasoning
St1	Involve management and stakeholders	It is evident that support and funding are necessary for successfully establishing a program. Assigning a person to run the program could also be beneficial.
St2	Define the role	There is a consensus that champions should volunteer for the role [2][14][28]. Our assumption is that it will be easier to recruit when the role and responsibilities are clearly defined. It will also be clearer to the champions what is expected from them.
St3	Assess security status	Assessing the security status can help convince management and stakeholders and help identify goals and define the roles.
St4	Recruit champions	The program needs to recruit champions. There is consensus among the papers that the best approach is for champions to volunteer for the role [2][14][28].
St5	Training	Champions should be trained in security and soft skills to be able to successfully fulfill the responsibilities of the role
St6	Set up communication channels	It is important that the champions can easily communicate with each other and other relevant people to help, discuss and share information.
St7	Ensure regular meetings	Regular meetings could help the champions share knowledge and solve problems. It could also be a helpful resource for building a tighter community of champions.
St8	Ensure necessary resources	The champions should have available resources to help them with their security champion tasks. A buddy program could help with the onboarding of the champion.
St9	Collect feedback	To continuously improve the program, the company should collect feedback. This can be done, i.e., via a questionnaire or a retro perspective.
St10	Automate activities to make the program more scalable	Especially in larger companies, it can be beneficial that some parts of the process go automatically. This can include activities like onboarding and training.
St11	Pre-allocate time for champion tasks	Research shows that it is difficult for the champion to juggle day-to-day tasks and champions responsibilities [2][28]. This could be solved with pre-allocated hours to work on the champion tasks.
St12	Motivate the champion	To best maintain the champion, the company should do measures to ensure that the champion is motivated for the role. This could also help with the recruitment of the champions.
St13	Support from the security team	The security team is a useful source for the champion and can help with both training and motivation.
St14	Measure results	Research has found that concrete results can help motivate the champion and the team [29][30].

The pre-study can be read in its entirety by accessing the file in SharePoint. The link to access the file is found in reference [31].

2.4 Visma

The research is carried out within the Visma Group. Visma is one of the top five software companies in the EU, providing software and services that help businesses in both the private and public sectors simplify and digitalize their processes [32]. Their customers range from small businesses to large corporations and municipalities and include all sectors from plumbing to banking. The Visma Group consists of more than 200 companies and operates in 20 countries worldwide [32]. In Europe, they specifically operate in the Nordic region, Benelux, and central and Eastern Europe. According to recent numbers, the company has more than 14000 employees, including 6500 developers [32].

2.4.1 Visma Application Security Program

In order to provide appropriate security and data protection across their products and services, Visma has created a program called the Visma Application Security Program (VASP) as a part of their security program.

VASP is a Visma-specific Secure Software Development Life Cycle (SSDLC) framework based on industry standards, and best practices [33]. The program aims to improve the security and privacy of services as well as raise the security awareness in the teams. This includes ensuring that the product is managed, developed, and operated in a secure and compliant manner in terms of application security, data protection, and privacy. VASP aims to give the teams the tools they need to provide the best possible security, and as a part of this, every team gets a dedicated "Security Engineer." A Security Engineer (SE) in Visma is the same as a Security Champion, as defined in section 2.2.

2.4.2 Security Engineers

Each publicly offered service at Visma has at least one SE [33]. The SE receive additional security and data protection training and act as the teams' specialist and primary point of contact on security and data protection issues while maintaining their original role, typically as a Developer or System Architect [33]. There were approximately 247 SEs scattered across Visma's over 200 companies at the time of this study. Because the SEs are working in different companies, the experience of working as a SE might vary, even though they all officially work within the Visma Group.

As defined by Visma, typical tasks for a SE include improving security, following up on issues found during testing, assessing the priority and severity of security issues, and translating them into team context [33]. Tools and resources available to help the SEs at Visma include a Security Awareness Program, Slack channels, a Secure coding training platform, self-studies, Visma internal security event, internal guidelines, security conferences, and Security Engineer Guild meetings [33].

The Security Engineer Guild meetings are held biweekly for all the SEs in Visma. The meetings are typically used to present current security news and other relevant inform-

ation. Because SEs from all locations are invited to the meetings, they are always held online. The main purpose of the meetings is to motivate the SEs and enhance security awareness.

2.4.3 Visma Security Self-Assessment

The Visma Security Self-Assessment (SSA) is a detailed document containing a set of questions that the development team has to answer to document the security of their product/service. The document is annually reviewed by a member of the security team and a representative from the data protection program [33], and the output of the assessment consists of tickets describing actions that must or should be taken to improve the product's security [33]. The SSA is usually the SEs first interaction with the VASP, and introduces and familiarize the SEs with some of the main security areas.

The purpose of the SSA is [34]:

- Provide teams with a documented way to assess the security of their service/product according to a common checklist;
- Identify improvements regarding the security of the service and decide how to prioritize them;
- Have a common approach on how to work with proactive security measures;
- Educate and increase awareness of security topics for team members;
- Place responsibility of security inside the teams.

2.4.4 Visma Security Maturity Index

The Security Maturity Index (SMI) is an internal tool used to measure the security status of a product/service in Visma [33]. It identifies strengths and weaknesses over time and helps prioritize development that improves security and data protection [33]. The products are put in different tiers depending on how they perform, and the results are transparent and shared across the company [34]. The index is based on penalty points, which vary depending on the severity of the non-compliance [34]. For example, failing to complete the SSA could result in 3000 penalty points. Teams can celebrate advances when they move up tiers (for example, from Silver to Gold), which has shown to be a good motivator to keep focusing on security over time [34]. The SEs also uses the SMI to decide the order of security activities because they can see which activities the security experts consider most important.

Chapter 3

Research Methodology

This chapter discusses the research strategy and data collection methods used in this study, as well as the data analysis procedures.

3.1 Collaboration

The study was created and conducted in collaboration with a student from JAMK University of Applied Sciences [35]. He is writing a master's thesis concerning the onboarding part of the security champions program, and we were thus able to use much of the same data. Some of the data gathered are not analyzed and presented in this thesis because it is outside the thesis' scope. In addition to writing the master thesis, he is working as a Security Officer in Visma Public Oy. Due to this, he has been a valuable resource for recruiting SEs for the case study and getting a thorough understanding of Visma. However, it is emphasized that I created all the content of this thesis and that the collaboration was strictly limited to data collection.

3.2 Research Design

The objective of this study is to further investigate the steps found in the pre-study, described in Section 2.3, to determine whether they are effective in establishing a security champions program. Additionally, we wanted to investigate how software companies currently maintain security champions programs and what challenges and improvements exist. We debated between a case study and a survey but ultimately chose a case study. A survey will most likely take a broad but superficial look at several instances of the topic under inquiry [18], and because we wanted to look at the steps thoroughly, we did not choose this strategy. As shortly mentioned in Section 1.3, a case study was chosen because it makes it possible to study a single factor in isolation, which in this case is the set of proposed steps. In addition, a case study is suitable for theory testing and produces data close to people's experiences. The study had to focus on depth rather than breadth

because rich, detailed data makes it possible to further investigate the set of steps and understand how they should be carried out.

Visma was selected as the subject of the case study due to convenience and because Visma consists of multiple companies, making it possible to get a broader look. Even though the companies are under Visma, they are still semi-independent. Because of this, we believe that the population provided a typical instance of the case, making it possible to generalize the findings. Case studies are sometimes criticized for producing knowledge that only relates to the case under examination. However, it is possible to generate broader conclusions that are relevant beyond the case itself, known as generalization [18]. Even though some factors are unique to a particular case, other factors will be similar in many cases. We believe that it is possible to generalize in this case because the case contains security champions from different companies, which gives us different perspectives. Also, the security engineer program in Visma is regarded as a typical security champions program, and does not, to my knowledge, contain any extreme cases. Generalizing the data from the case study makes it possible to test the existing theory and make conclusions that will apply to all similar situations. One of the disadvantages of case studies mentioned by Oates [18] is that it is time-consuming to access the necessary resources and people. However, this was not a problem as my collaborator had access to internal communication resources in Visma and contacts within the organization.

The case study was conducted in two phases: The first phase consisted of an electric questionnaire, and the second phase consisted of semi-structured interviews. The research process can be seen in Figure 3.1.

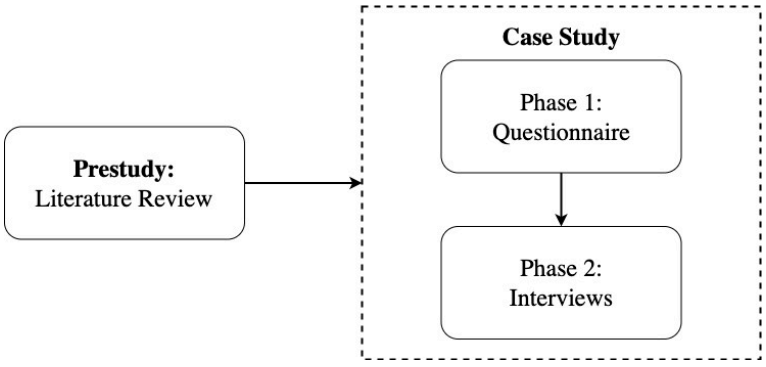


Figure 3.1: The case study research process.

The reason for choosing a self-administrated electronic questionnaire for the data generation method is that it makes it possible to obtain standardized data from many people, making the generalization of the case study more valid. Given that the respondents are a group of people who work with technology, it is reasonable to assume that they will be able to read and understand the questions and possible replies, justifying the questionnaire being self-administered. An electronic questionnaire was chosen as the most convenient technique for collecting the data because the respondents lived all over Europe and were assumed to have a high degree of computer skills.

Interviews were selected as the second method of gathering data. Interviews were chosen because they allowed for an in-depth discussion of the issue and were used to obtain more

details about some of the questionnaire responses. In addition, little equipment is needed. The disadvantage of conducting interviews is that they are time-consuming. Another downside is that the interview results may lack reliability because the interviewees are less anonymous and may be hesitant to express their true feelings. Oates [18] also notes that interviews are not suitable for making generalizations about a whole population, as you would need many interviewees. However, in combination with the participants in the questionnaire, we believed that the two data generation methods have a big enough population to make generalizations about the topic.

Before we started collecting data, we got feedback from other researchers on the research plan, which is known to reduce the risk of missing relevant data sources and questions [36].

Both a questionnaire and interviews were used as a part of the case study, which forms a triangulation by creating different angles towards the studied objects and thus a broader picture [36]. The type of triangulation applied in this case study is methodological triangulation, as we combined different types of data collection methods: Qualitative and quantitative methods. A combination of qualitative and quantitative data often provides a better understanding of the studied phenomenon [36].

3.3 Phase 1: Electronic Questionnaire

The first phase of the case study was to collect primary data on Visma's security engineers through an electronic self-administered questionnaire. The questionnaire provided an efficient way of collecting brief data from a large number of people.

3.3.1 Developing the Questionnaire

The questions were created according to the guidelines in B. Oates's book *Researching Information Systems and Computing* [18] and consisted of a set of fixed questions in a pre-established order with standardized wording. The responses to most of the questions had to be selected from a small list of alternatives.

The questions were identified using the results from the literature review and the research questions. To ensure that the wanted data was generated, I created a mapping between the steps in the pre-study and the questions. The mapping can be seen in Figure 3.2. Some of the steps were left out of the questionnaire because we thought they were better explored through interviews. Because the potential respondents originated from all over Europe, the questionnaire was in English.

The questionnaire was distributed using Google Forms. The final questionnaire can be seen in Appendix E.

3.3.2 Subject Selection and Recruitment

The subject group for the questionnaire was anyone who works at Visma as a SE. Because the questionnaire had few geographical limits to where it could be used, we sent it out to SEs in all of Visma's companies via the SE's common Slack channel.

A low response rate is a serious and common problem with self-completion questionnaires [37], and we made efforts to ensure we got the wished number of respondents.

The questionnaire was first presented at the bi-weekly Security Guild Meeting, described in subsection 2.4.2, to introduce it to all the SEs. Around 75 SEs were present at the meeting when the questionnaire was presented. After the meeting, the presentation was followed up by posting reminders on the Security Guild Slack Channel. The Slack channel is common for all the SEs and has over 600 members. The number of members in the Security Guild Slack channel is higher than the number of SEs because all employees interested in security can join. We emphasized the importance of the questionnaire and the value of the SEs' participation in the reminders. We sent four reminders, and the Visma Security Team sent one. In the third reminder, we included some results from the questionnaire, hoping to engage more SEs.

In addition to this, we contacted the Chief Information Security Officer in the Benelux countries. She agreed to promote the questionnaire in a more intimate meeting with the Benelux area's SEs.

Because my collaborator is working at Visma Public in Finland, we sent two direct reminders to Visma Public. We also contacted the Finnish Security Officer so they could promote the questionnaire within their legal unit.

The questionnaire ended up getting 73 respondents.

3.3.3 Confidence

We used a confidence interval and confidence level to guarantee that the target population was accurately portrayed. For the target group, which consisted of 247 persons, we decided to accept a confidence interval (also known as a margin of error) of 10. We also agreed that a level of confidence of 95% would suffice. Using these values, we needed at least 69 responses. The number of respondents required was calculated using an online sample size calculator [38]. Since our questionnaire received 73 responses, we have high confidence in the results.

3.3.4 Data Analysis

The data collected from the questionnaire was subjected to quantitative data analysis. Because we used Google Form, we did not have to modify the data set to use it. The data were analyzed in an exploratory manner, using the software Microsoft PowerBI. Mind maps were created to cover all important aspects and correlations. We conducted de-

scriptive and correlation analyses and analyzed the data separately to prevent bias. The results were then presented and discussed with two additional researchers. No contradictions were found between the two analyses.

In several of the questions, the respondents were asked to answer using the Likert scale [39]. When analyzing the data, responses were in some cases reduced to disagree, neutral, and agree, rather than including all five steps on the scale. Agree included Strongly Agree and Agree, and disagree included Strongly Disagree and Disagree. The neutral results remained the same. This was done to make the graphs more understandable and less overwhelming.

T-tests were conducted to increase the validity of the results. The t-tests were performed using Graphpad T-test Calculator [40]. Because a t-test only include two cases, the neutral responses were not included in cases where the Likert scale was used.

The results from the analysis can be seen in Subsection 4.2.

3.4 Phase 2: Interviews

To gain more detailed information about the SE program, we conducted semi-structured interviews using the interview guide seen in Appendix F. Each interview lasted from 30 minutes to one hour.

3.4.1 Identification of Interview Questions

The interview guide was developed based on the pre-study and the questionnaire results. The mapping in Table 3.2 gave us confidence that there were no gaps in the results and that all steps were investigated. The purpose of the interviews was to explore further the steps that did not get enough attention in the questionnaire and collect more detailed information. The interview guide consisted of six categories containing, in total, 17 questions. Semi-structured interviews were chosen because they allow for improvisation and exploration of the studied objects [36].

3.4.2 Subject Selection and Recruitment

Visma has a list of all the SEs in the company and an additional list of the SEs responsible for products with a lower security level than desired according to the SMI, described in Section 2.4.4. We selected people randomly from these two lists and sent them a Slack direct message asking if they would like to participate in an interview. Three interviewees were obtained using this method. Then we asked a person in the security team if she could suggest some possible candidates. Through this method, we were able to get three more interviews. We also asked the security officers in Finland if they could recommend any potential candidates, which gave us two more interviewees. My collaborator asked a person in the same legal unit as him who was willing to do an interview. Lastly, we asked

some of the more active members of the Security Engineer Slack channel if they would like to participate. One person agreed.

My collaborator asked the SEs via a direct message in Slack, as he has access to the internal Visma Slack workspace. Some did not respond; some said no, and some agreed. In total, we ended up interviewing 11 people.

We believe we were able to get a diverse population of SEs. Some general data about the interviewees are presented in Table 3.1

Table 3.1: Data about the interviewees.

Main roles	Software developer (6), full-time SE (3), architect (2)
Prior security competence	None/low (5), medium (4), high (2)
Time in the role	$<$ 1 year (3), 1-2 years (2), 3-4 years (4), $>$ 4 years (2)
Locations	Finland (4), Sweden (2), Lithuania, Latvia, Netherlands, Norway, Romania
Gender	Female (5), Male (6)

3.4.3 Data Collection Procedure

All the interviews were conducted online using Microsoft Teams because the interviewees were located all over Europe. We saved video recordings and a generated transcription from each interview. Each transcript was then manually checked and cleaned up to ensure correct data. The data was also anonymized. We collected the consent for data processing orally at the beginning of each interview, where we also clarified the purpose of the research and ensured confidentiality and anonymity. The consent form can be seen in Appendix B. After we had checked the transcripts, they were sent back to the participants to enable correction of the raw data.

3.4.4 Data Analysis

The information was analyzed qualitatively using the software MaxQDA [41]. The data was divided into 11 different codes, with, in total, 45 sub-codes, which also contained sub-sub-codes. The codes were developed to categorize the data to make it possible to answer the research question and thus verify the steps. We used the technique open coding.

3.5 Mapping of the Questions

A mapping was created to ensure that the questions covered all the steps and to verify that the desired data was generated. The mapping is displayed in Table 3.2. All of the steps were covered except for St1, St3, and St14, which are administrative processes that an ordinary SE typically would not be able to provide significant knowledge about.

Table 3.2: Mapping of step to questionnaire (Q) and interview (I) questions.

ID	Step	Question
St1	Management and stakeholders	Not covered
St2	Define role	Q5, I4, I5
St3	Asses security status	Not covered
St4	Recruitment	Q4, I3
St5	Training	Q9, I9, I10, I11
St6	Communication	Q8, I14
St7	Meetings	Q9, I15
St8	Resources	Q7, Q9, I12, I13
St9	Feedback	Q10, Q11
St10	Automation	Q15
St11	Time	Q5, Q6
St12	Motivation	Q12
St13	Support from security team	Q7, Q9
St14	Measure results	Not covered

3.6 Analysis of Slack Data

Slack [42] is a communication platform and is used for internal communication in Visma. Because Slack is an important tool for the SEs, some basic data from the Security Guild Slack Channel was analyzed to better understand how the tool is used. The data was downloaded from the Slack Analytics Dashboard [43], which provides monthly stats from the Slack channels. The data were combined and used to analyze further the communication in the channel. The data was analyzed quantitatively, and the results can be seen in Section 4.5.

3.7 Expert interview

To validate our findings and recommendations so far, we had a meeting with a member of the Security Awareness and Training team, which is closely engaged with the SE program in Visma. During the meeting, we presented our results and recommendations for improvements and got feedback on whether they were realistic.

Chapter 4

Results

The findings from the research are presented in this section. First, Visma's current implementation of the steps from the literature is explained to provide some context. Then follows the results from the questionnaire and the findings from the interviews. Following that, the results of the Slack data analysis are presented. Lastly, contradictions in the results are presented.

4.1 Visma Context

To better understand the results, Table 4.1 explains how the steps from the pre-study are carried out in Visma.

Table 4.1: How Visma carries out the steps found in the prestudy.

ID	Step	Execution of step
St1	Involve management and stakeholders	The security team are responsible for the SE program, but it is up to management to make requested features happen.
St2	Define the role	Visma has no clear role definition for a regular SE. Only SEs in the VCDM (a more strict development framework certified with ISO27001 and ISAE3402) have a defined role description.
St3	Assess security status	A product's security is assessed in the security program, VASP, as described in Section 2.4.1. The SSA, described in Section 2.4.3 assesses if the design is secure. The SMI described in Section 2.4.4 is the end-results of the assessments.
St4	Recruit champions	Visma's business unit managers are responsible for ensuring that every team has a SE. Visma culture encourages volunteers, but there are some appointed SEs.

St5	Training	Visma did not offer any organized training from top management at the time of the study, but they did to some degree before Covid-19. Classroom training has not been prioritized because the program struggles to keep up with the scale and growth of Visma, but they have tried to focus on e-learning platforms and other resources for self-learning.
St6	Set up communication channels	The SEs in Visma can contact each other using the Visma Security Guild Slack Channel, a common slack channel for all SEs and other people interested in security.
St7	Ensure regular meetings	Visma's security team arranges a bi-weekly online meeting for all SEs where they present the latest security news. The meeting is briefly described in Section 2.4.2. There is also a security awareness meeting once a month.
St8	Ensure necessary resources	Visma ensures many different resources to help the SEs in their role, including online resources for training, communication channels, meetings, and support from the security team.
St9	Collect feedback	SEs receive annual surveys, and they can give continuous feedback using Slack and Jira. Visma conducts an interview session with members of the security program, including SEs, every other year. The interviews gather information on their preferences, dislikes, and desired changes.
St10	Automate activities to make the program more scalable	No specific activities are currently automatic. However, "self-service" is in place; the SEs do not need to contact someone to be added to bi-weekly meetings, the slack channel, or access other learning programs.
St11	pre-allocate time for champion tasks	There is no standard policy for giving the SEs pre-allocated hours to work on SE tasks. However, Visma recommends that standard SEs spend 20% of their work hours on SE tasks.
St12	Motivate the champion	Motivating measures are the Guild meeting and the Security Guild Slack Channel. Visma also sends out merchandise like t-shirts and stickers and arranges hacking events.
St13	Support from the security team	The security team can be contacted on Slack, Google Chat, email, and other internal tools and communities for help and support. It is also possible to order different tests and checks.
St14	Measure results	The results of the security work are measured using the Visma Security Maturity Index, as described in Section 2.4.4.

4.2 Results Phase 1: Questionnaire

This section presents the results from analyzing the data collected using the questionnaire.

4.2.1 Defining the Role

According to the literature review, it is recommended that the security champion role and its responsibilities are clearly defined. The questionnaire was used to investigate further the consequences of having a clear role definition or not. Figure 4.1 shows the number of SEs that think they were given a realistic view of what was expected from them as a SE during recruitment.

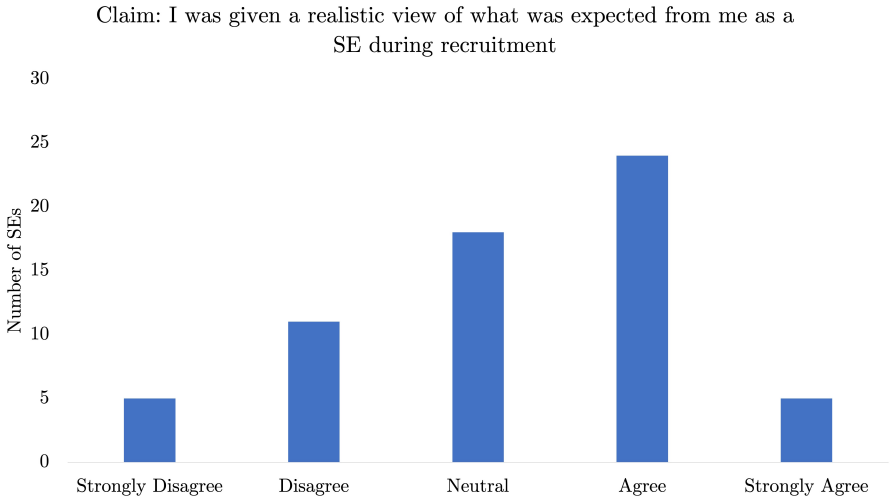


Figure 4.1: Number of SEs who say they were given realistic expectations for the role.

Table 4.2 presents the correlation between role expectation and reported satisfaction in percentages. SEs who said they were given a realistic picture of what was expected of them as a SE throughout the recruitment process responded to the statements less negatively.

Table 4.2: Percentages of SEs who disagree (D), are neutral (N), or agree (A) with various claims based on their perceived role expectations. The full claims can be seen in Appendix D

		Not Realstic Exp.			Neutral			Realistic Exp.		
ID	%	D	N	A	D	N	A	D	N	A
R1	C1: There is a clear onboarding process (...)	80	13	7	50	39	11	23	58	19
R2	C2: I am satisfied with the orientation (...)	69	6	25	22	28	50	17	31	52
R3	C3: I am satisfied with the security training (...)	74	13	13	47	47	6	30	59	11
R4	C4: I am satisfied with the soft skills training (...)	86	7	7	59	41	0	19	54	27
R5	C5: I am satisfied with my performance (...)	19	44	37	33	17	50	6	35	59

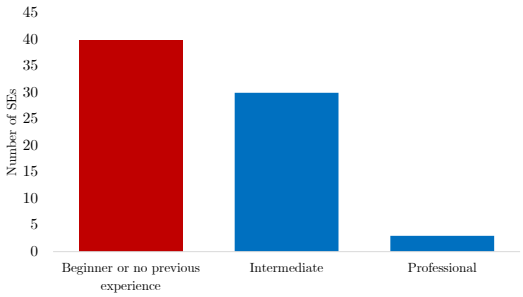
To conclude, the results indicate that defining the role and giving the employee realistic expectations of the role is beneficial and has a positive effect on the SE's perceived satisfaction. T-tests were conducted to validate the results. The t-test shown in Table 4.3 indicates that the role expectations have an impact on whether the onboarding process is clear and the satisfaction with the orientation and training. The SEs' satisfaction with their own performance in the role was not affected.

Table 4.3: Results from performing t-tests on the data used in Table 4.2

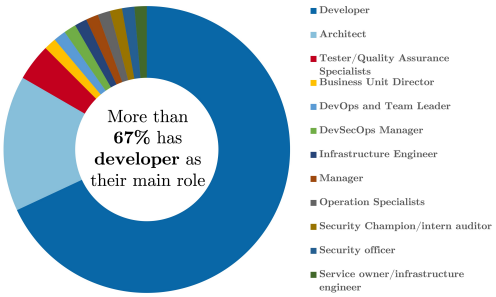
Correlation	Statistically significant?	P-Value	Confidence Interval	SD
R1	Extremely	0.0003	-1.00	0.25
R2	Extremely	0.0003	-1.37	0.35
R3	Yes	0.0187	-0.72	0.29
R4	Very	0.0016	-0.97	0.28
R5	No	0.1781	-0.38	0.28

4.2.2 Recruitment

According to the findings shown in Figure 4.2a, most SE have little to intermediate security competence when they first start in the position, which is usual for a security champion. The most common main roles are developer or architect, shown in Figure 4.2b.



(a) SEs' security competence before starting in the role.



(b) SEs' main role.

Figure 4.2: The SEs' background.

The pre-study recommends that the security champions volunteer for the role. Figure 4.3 displays the number of appointed SEs compared to the number SEs who volunteered in Visma.

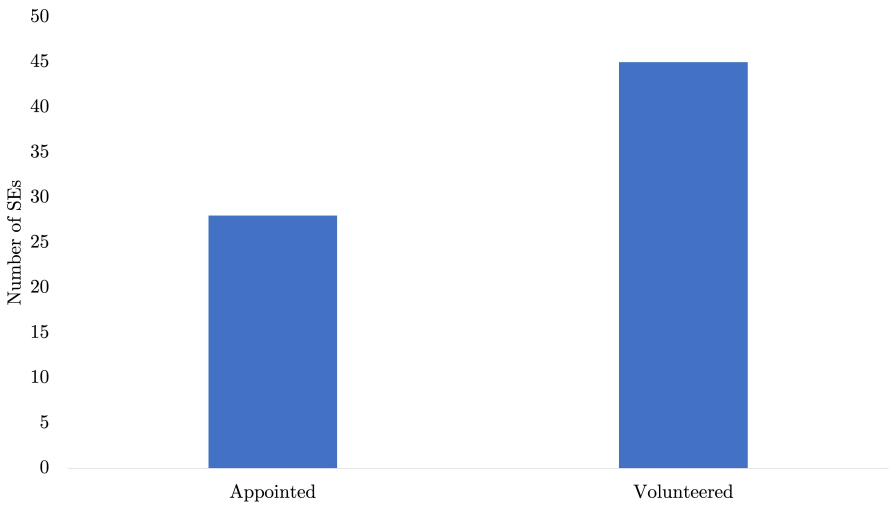


Figure 4.3: Number of SEs who was appointed compared to the number of SEs who volunteered.

The two groups answered similarly on most statements, except one. The motivation for the role is considerably different. Almost 91% of those who volunteered state that they are motivated for their role as a SE, compared to 57% for appointed ones.

Table 4.4: Percentages of SEs who disagree (D) are neutral (N) or agree (A) with various claims, based on whether they volunteered or were appointed. The full claims can be seen in Appendix D

		Volunteered			Appointed		
ID	%	D	N	A	D	N	A
R6	C1: There is a clear onboarding process(...)	45	42	13	52	30	18
R7	C2: I am satisfied with the orientation(...)	39	20	41	25	25	50
R8	C3: I am satisfied with the security training(...)	53	35	12	44	45	11
R9	C4: I am satisfied with the soft skills training(...)	53	32	15	45	35	19
R10	C5: I am satisfied with my performance(...)	20	24	56	18	43	39
R11	C6: I feel motivated(...)	5	4	91	18	25	57
R12	C7: I do not have role conflicts(...)	9	14	77	7	18	75

However, when looking at the answers regarding what the SEs want to improve with the SE program, only one appointed SE answered recruitment, as seen in Figure 4.4. This implies that people do not resent getting appointed, which might be necessary if the company cannot find enough volunteers.

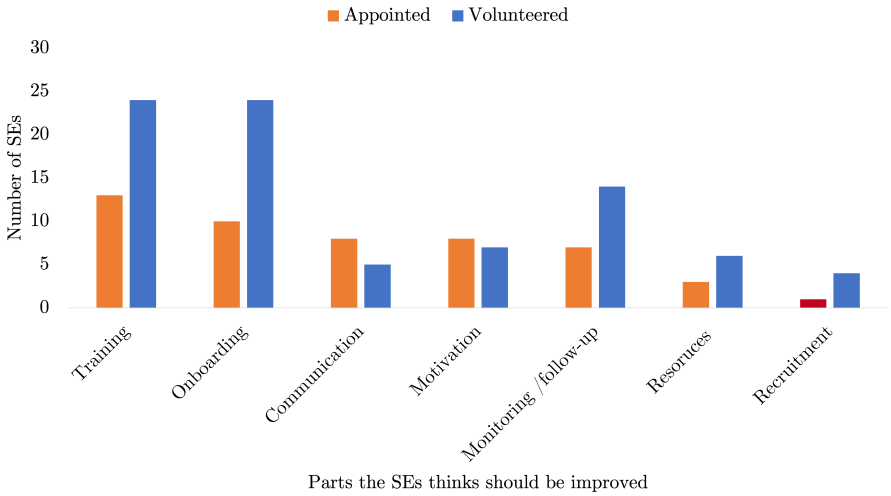


Figure 4.4: Parts of the SE program that the SEs think could be improved.pdf

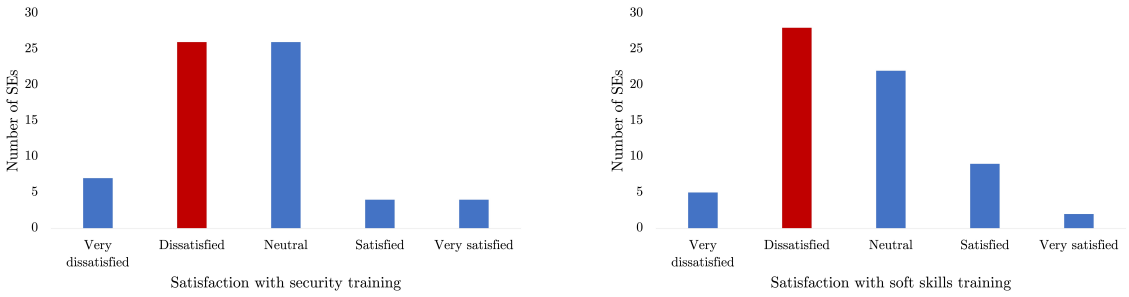
T-tests were performed to validate the results. The results regarding motivation are extremely statistically significant, while the other results are not statistically significant at all.

Table 4.5: Results from performing t-tests on the data used in Table 4.4

Correlation	**Statistically significant?**	**P-Value**	**Confidence Interval**	**SD**
R6	No	0.9264	-0.02	0.25
R7	No	0.3491	0.28	0.30
R8	No	0.9427	-0.02	0.24
R9	No	0.8192	-0.05	0.24
R10	No	0.4622	-0.18	0.24
R11	Extremely	0.0005	-0.78	0.22
R12	No	0.7522	-0.08	0.24

4.2.3 Training

Training is the part of the SE program where the highest dissatisfaction was recorded. Figure 4.5a depicts what the SEs think about the received security training. A majority of SEs answer that they are dissatisfied. Many are neutral, but very few answer that they are satisfied. The same thing applies to the soft skills training, as illustrated in Figure 4.5b. The vast majority are dissatisfied or neutral, with only a handful SEs expressing satisfaction.

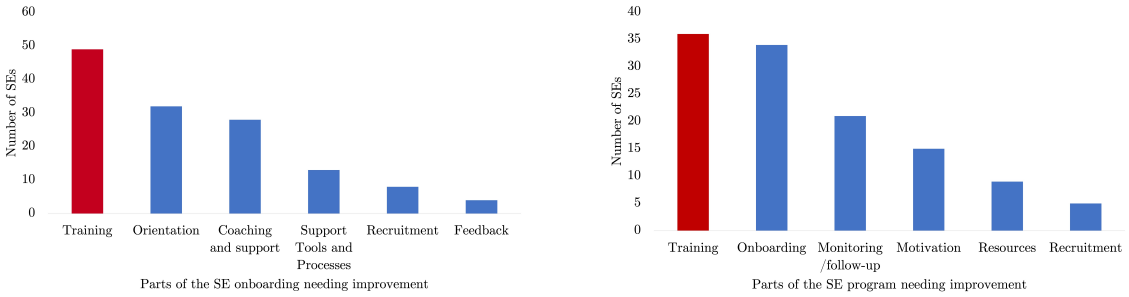


(a) SEs' satisfaction with received security training.

(b) SEs' satisfaction with received soft skills training.

Figure 4.5: SEs' training satisfaction.

The SEs were also asked what aspects of the SE program, both in terms of onboarding and the overall program, they think should be improved. As seen in Figure 4.6, it was yet again confirmed that training is something that the SEs are unhappy with.



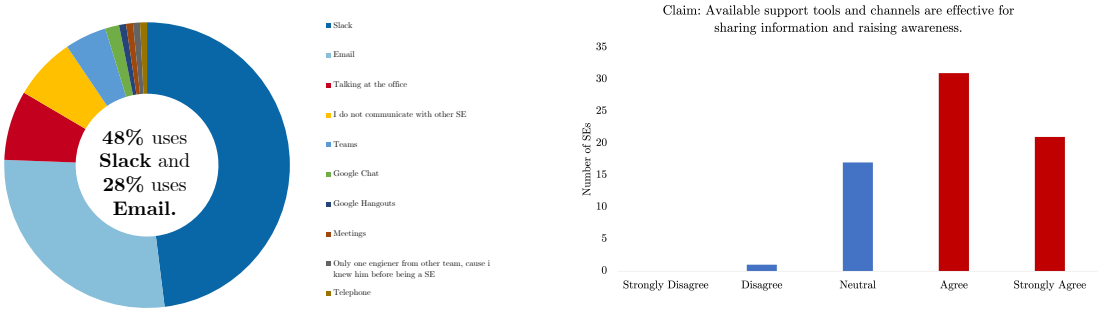
(a) Parts of the onboarding SEs wants to improve.

(b) Parts of the whole program that SEs wants to improve.

Figure 4.6: Parts of the program that needs improvement according to the SEs.

4.2.4 Communication

As illustrated in Figure 4.7a, Slack and Email are the most used communication tools. When asked if the available support tools and channels are effective for sharing information and raising awareness, more than 74% answered agree or strongly agree, as illustrated in Figure 4.7b.

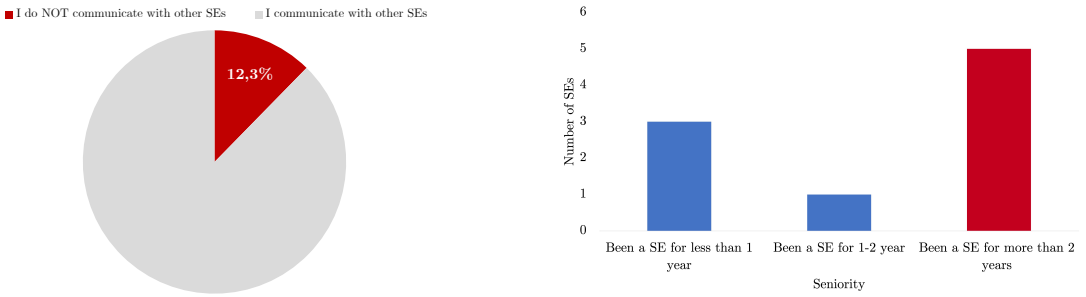


(a) Tools used to communicate with other SEs.

(b) Opinions on the effectiveness of available tools.

Figure 4.7: The most used communication tools, and the SEs' satisfaction with them.

Figure 4.8a shows that around 12% of the SEs answer that they do not communicate with other SEs. Looking into this, it appears that the majority of people who do not communicate with other SEs have had the role for more than two years, as illustrated in Figure 4.8b.



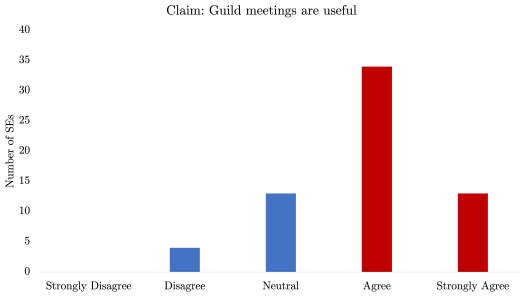
(a) Percentage of SEs who do not communicate with other SEs.

(b) SEs who do not communicate with other SEs based on their seniority.

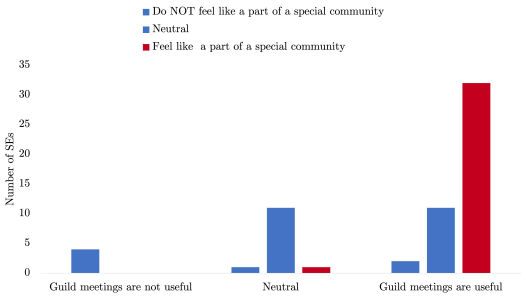
Figure 4.8: SEs who do not communicate with other SEs.

4.2.5 Regular Meetings

In the literature review, some studies recommended regular meetings for the security champions. In Visma, they have something called the Guild Meeting, which is described in Subsection 2.4.2. The results from the questionnaire prove that 73% of the SEs find the Guild Meeting useful, illustrated in Figure 4.9a. As illustrated in Figure 4.9b, those who find the meetings useful also feel more like they are a part of a special SE community than those who do not find the meetings useful.



(a) Number of SEs that thinks Guild meetings are useful.

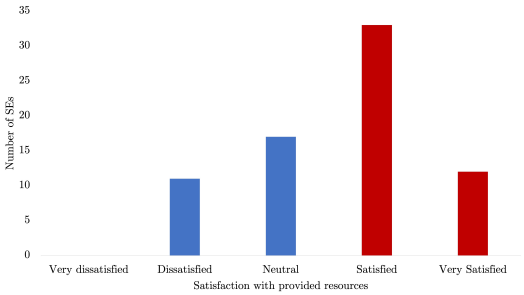


(b) Number of SEs that feel like a part of a special SE community based whether they find the Guild meeting useful.

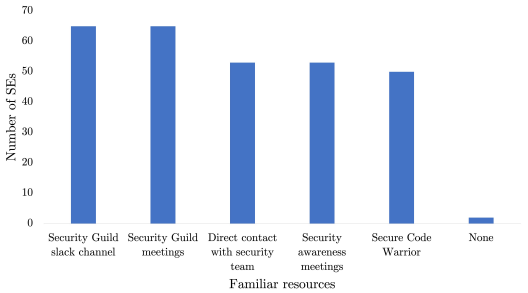
Figure 4.9: Guild meeting usefulness and its impact on community feeling.

4.2.6 Resources

Figure 4.10a illustrates the SEs' satisfaction with provided resources and suggests that most SEs are generally satisfied with the resources provided to help them in their role as a SE. Figure 4.10b illustrates what resources the SEs are familiar with.



(a) Number of SEs that are satisfied with resources provided to help in the role as a SE.



(b) Number of SEs that are familiar with various coaching and support provided by Visma.

Figure 4.10: Satisfaction and familiarity with resources.

During their onboarding to the SE role, some SEs were assigned a mentor. The number of SEs who had a mentor can be seen in Figure 4.11.

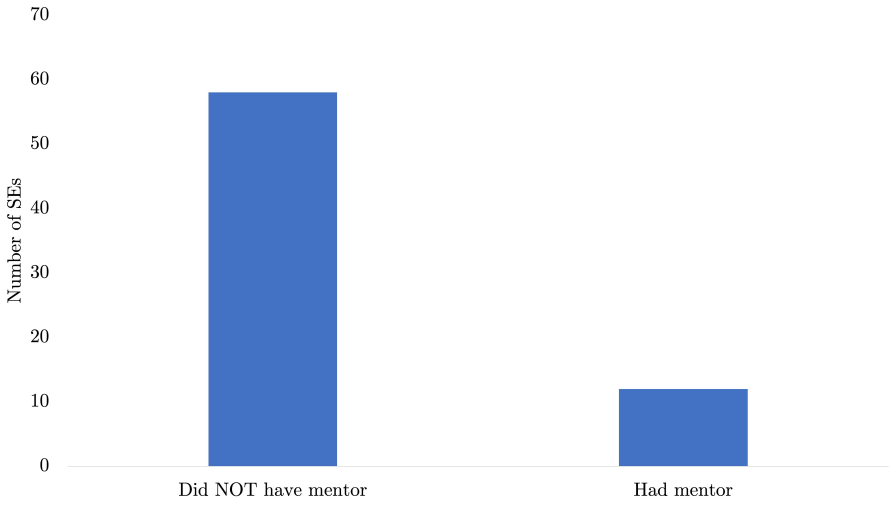
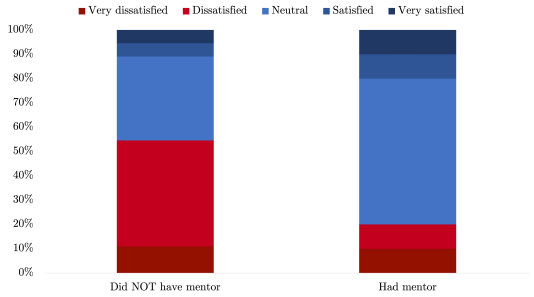
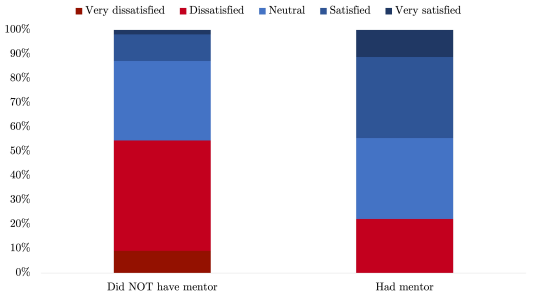


Figure 4.11: Number of SEs who had a mentor during onboarding to the SE role.

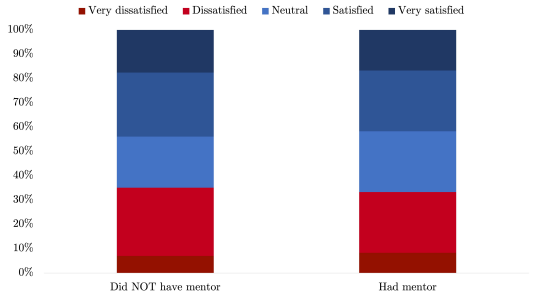
As shown in Figures 4.12a and 4.12b, having a mentor had favorable impacts, particularly on reported satisfaction with the received training. However, having a mentor did not appear to have a substantial impact on satisfaction with the orientation received, as shown in Figure 4.12c, even though it did appear to make onboarding clearer, as shown in Figure 4.12d.



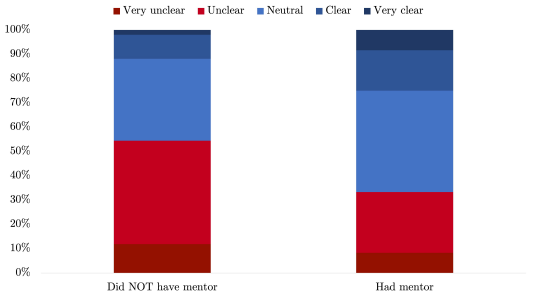
(a) Satisfaction with received security training based on whether the SE had a mentor or not.



(b) Satisfaction with received soft skills training based on whether the SE had a mentor or not.



(c) Satisfaction with received orientation based on whether the SE had a mentor or not.



(d) If the onboarding was perceived as clear based on whether the SE had a mentor or not.

Figure 4.12: The effects of having a mentor during the onboarding to the SE role.

T-tests were conducted to validate the results in Figure 4.12. Although the t-tests show

that the results are not statistically significant, they still give an indication of the situation.

Table 4.6: Results from performing t-tests on the data used in Table 4.12

Correlation	Statistically significant?	P-Value	Confidence Interval	SD
4.12a	No	0.1475	0.49	0.34
4.12b	Yes	0.0129	0.82	0.32
4.12c	No	0.9468	-0.03	0.39
4.12d	No	0.1433	0.45	0.30

4.2.7 Feedback

Results regarding feedback are displayed in Figure 4.13. Most SEs know where to share opinions on the SE program, but not that many can do it anonymously. Around 50% are specifically asked for opinions on the SE program. Around half of the SEs are satisfied with the amount of feedback they receive, and just under half are informed about how they perform as a SE.

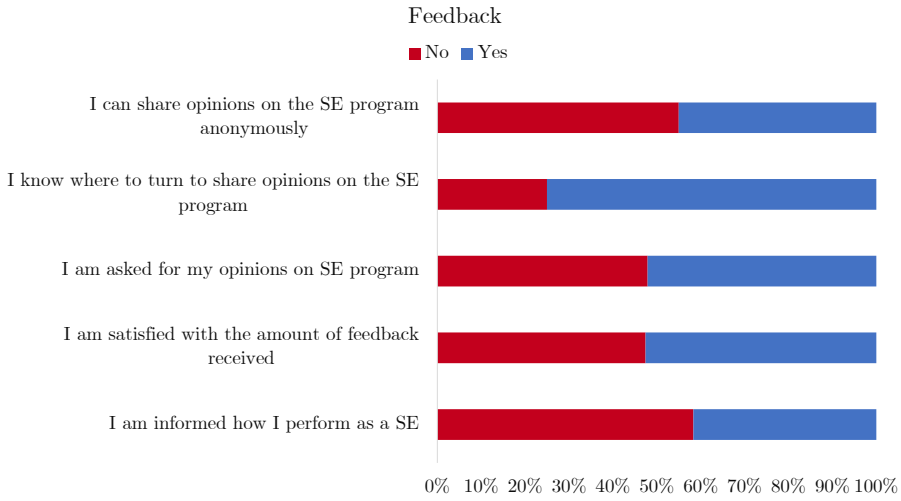
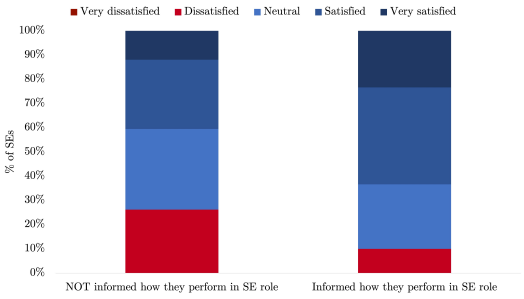
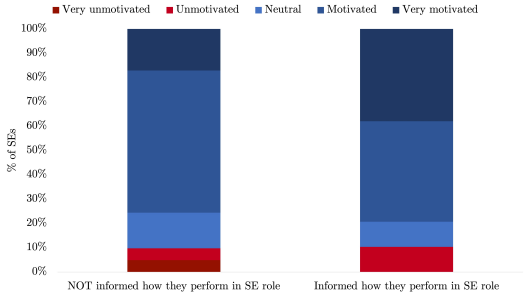


Figure 4.13: Number of SEs that have given and received feedback.

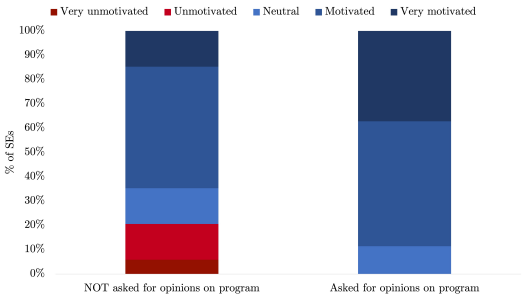
The studies from the pre-study stated that feedback is meaningful for the security champions program. Figure 4.14 shows some of the impact giving and receiving feedback had on the SEs. In Figure 4.14a we see that being informed about how they perform makes the SEs more satisfied with their own performance. However, as seen in Figure 4.14b it does not affect the motivation. Figure 4.14c shows that being asked for their opinions on the SE program can be motivating.



(a) Satisfaction with own performance based on whether the SE was informed how they perform or not.



(b) Motivation to work as a SE based on whether the SE was informed how they perform or not.



(c) Motivation to work as a SE based on whether the SE was asked for opinions of the program or not.

Figure 4.14: The effects of receiving and giving feedback in the SE role.

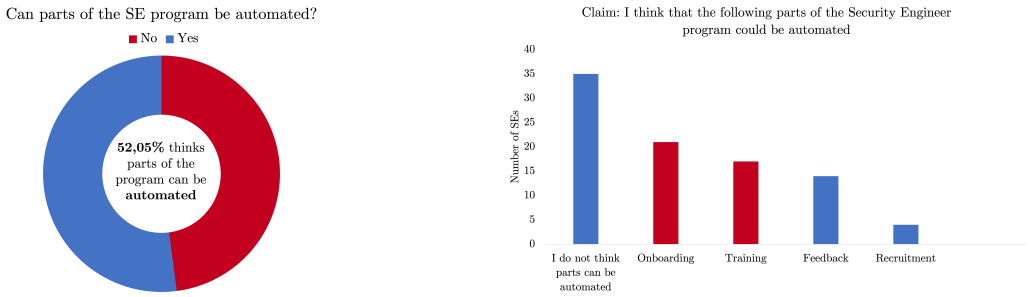
To verify if the results in Figure 4.14 are statistically significant, t-tests have been performed. The t-test are displayed in Table 4.7, and show that the results of Figure 4.14a and 4.14c are significant, while Figure 4.14b is not.

Correlation	**Statistically significant?**	**P-Value**	**Confidence Interval**	**SD**
Figure 4.14a	Yes	0.0324	-0.5	0.23
Figure 4.14b	No	0.2206	-0.29	0.23
Figure 4.14c	Very	0.0014	-0.73	0.22

Table 4.7: Results from performing t-tests on the data in Figure 4.14.

4.2.8 Automation

One of the studies from the literature review in the pre-study claimed that parts of the SE program could be automated to make the program more scalable. The questionnaire asked the SEs in Visma if they thought it was possible and, if so, what parts. As shown in Figure 4.15a, more than 50% thought it was possible. When asked what parts could be automated, onboarding and training was the most frequently selected choice, seen in Figure 4.15b.



(a) Percentages of SEs that thinks parts of the SE program can be automated.

(b) What parts of the SE program SEs think can be automated.

Figure 4.15: SEs' opinions on automating parts of the SE program.

4.2.9 Pre-allocated Time

Figure 4.16 shows the number of SEs with pre-allocated hours to work on SE tasks.

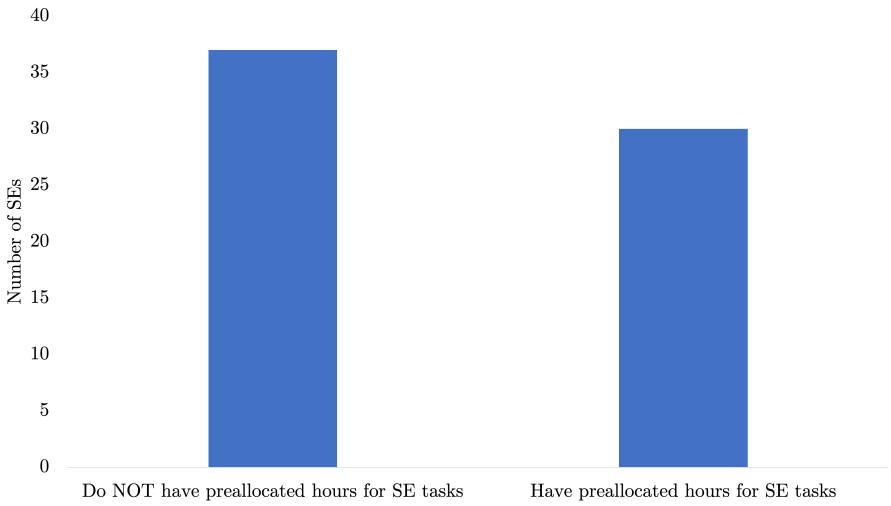


Figure 4.16: Number of SEs who have pre-allocated hours to work on SE tasks.

However, the results displayed in Table 4.8 show no particular evidence that having pre-allocated hours gives any particular effect. SEs who were given pre-allocated hours to work on SE tasks answered to the claims similarly to those not given pre-allocated hours. Having pre-allocated hours to work on SE tasks did not help with either satisfaction with security training, motivation, or role conflicts.

Table 4.8: Percentages of SEs who disagree (D), are neutral (N) or agree (A) with various claims, based on whether they have pre-allocated hours to work on SE tasks or not. The full claims can be seen in Appendix D.

	Pre-allocated hours?	No			Yes		
ID	%	D	N	A	D	N	A
R13	C3: I am satisfied with the security training(...)	44	44	12	57	29	14
R14	C6: I feel motivated(...)	8	11	81	10	17	73
R15	C7: I do not have role conflicts(...)	11	16	73	7	17	76

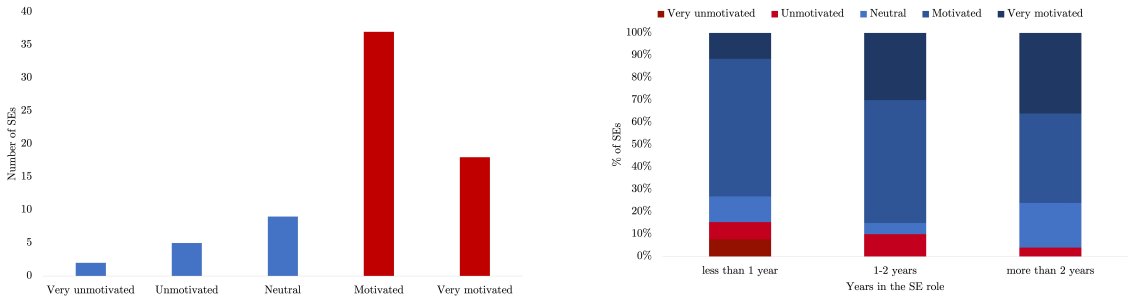
After conducting t-tests on the results, the conclusion is that the results are of no statistical significance, which verifies that having pre-allocated hours to work on SE tasks does not have any particular effect. The results from the t-tests are displayed in Figure 4.9.

Table 4.9: Results from performing t-tests on the data used in Table 4.8.

Correlation	**Statistically significant?**	**P-Value**	**Confidence Interval**	**SD**
R13	No	0.1013	0.52	0.31
R14	No	0.8446	-0.04	0.23
R15	No	0.9339	0.02	0.25

4.2.10 Motivation

As seen in Figure 4.17a, the SEs at Visma are generally motivated for their role. The motivation is also maintained for the SE that has been in the role for multiple years, shown in Figure 4.17b.



(a) Number of SEs that reports being motivated for their role as a SE.

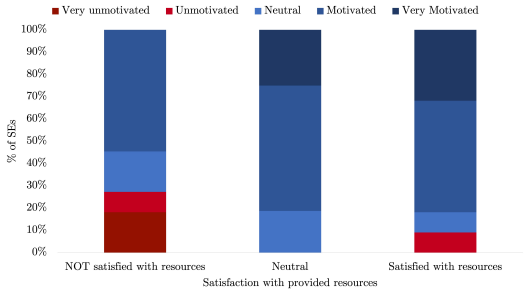
(b) Number of SEs that reports being motivated for the SE role based on years in the role.

Figure 4.17: SEs' motivation for the SE role.

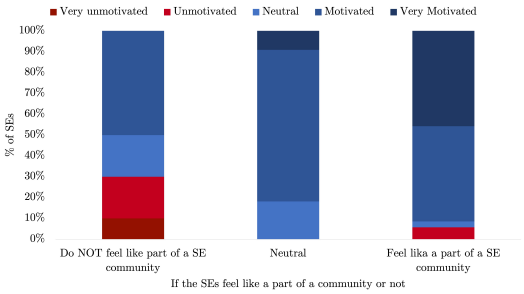
Multiple factors seem to be motivating for the SEs. As mentioned in Subsection 4.2.2, those who volunteered for the role are more motivated than those who were appointed. Another source of motivation that has already been discussed is getting and receiving feedback, as discussed in Subsection 4.2.7. In addition, those who are satisfied with the

received security training are more motivated, as depicted in Figure 4.18a. Also, being satisfied with provided resources and the feeling of being a part of a community had positive effects on the motivation, as shown in Figures 4.18b and 4.18c.

(a) How motivated the SEs are based on whether they are satisfied with the security training or not.



(b) How motivated the SEs are based on whether they are satisfied with the proivded resources or not.



(c) How motivated the SEs are based on whether they feel like a part of a SE community or not.

Figure 4.18: Motivating factors for the SE role.

From the t-tests presented in Table 4.10, we see that Graphs 4.18a and 4.18c are considered statistically significant. The neutral cases (the middle bar of the graphs) were not included to be able to conduct the t-tests.

Table 4.10: Results from performing t-tests on the data used in Table 4.18

Correlation	**Statistically significant?**	**P-Value**	**Confidence Interval**	**SD**
4.18a	Yes	0.0231	-0.96	0.41
4.18b	No	0.1064	-0.38	0.23
4.18c	Extremely	0.0003	-1.21	0.31

4.2.11 Support From the Security Team

Getting support from the company's security team is important for the SE since they have a high level of expertise and can assist with problems that the SE cannot solve independently. Figure 4.19 displays how quickly the SEs experience getting support from the security team.

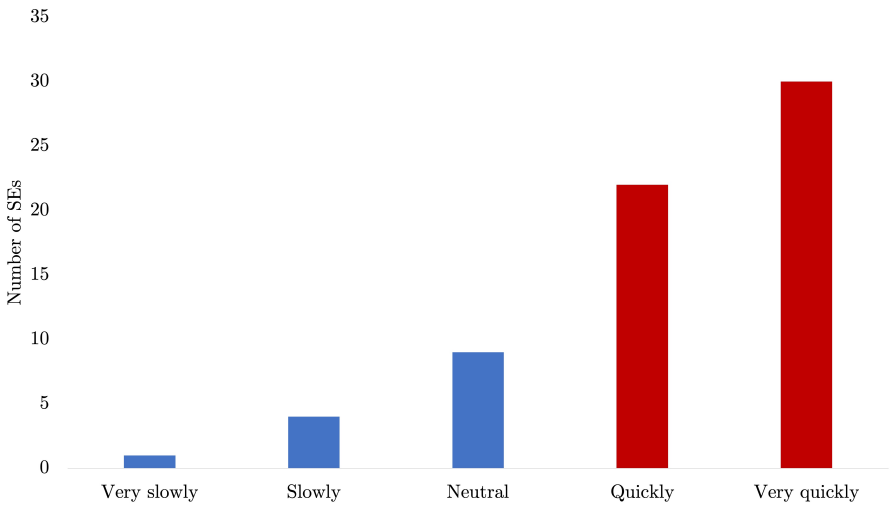


Figure 4.19: Number of SEs who experience getting support from the security team quickly.

There is a big difference when comparing how quickly the SEs get support from the security team to how satisfied they are with the available resources. Figure 4.20 displays that the SEs who get support quickly are happier with the provided resources than those who do not get support quickly. The results verify that the security team is an essential resource for the SEs.

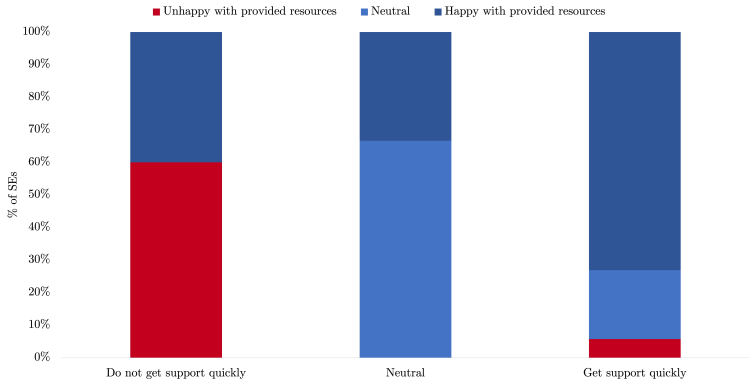


Figure 4.20: The SEs' satisfaction with resources based on how quickly they get support from the security team.

4.3 Results Phase 2: Interviews

The results and findings from the interviews are presented in this section. Not all the steps found in the pre-study are included in these results, as they were found to be adequately covered in the questionnaire. However, a few results regarding St13 Management and Stakeholder involvement are included. In addition, the results include some general facts and opinions on orientation and onboarding, which is initially outside the scope.

4.3.1 The Security Engineer Role

To better understand the SE role, we collected data about typical tasks and time usage. Typical tasks are presented in Table 4.11.

Table 4.11: Typical SE tasks discovered through interviews.

ID	Task
T1	Filling out security assessments (SSA)
T2	Working with security risks and data protection issues
T3	Using and checking code scanners
T4	Using Coverity [44] (static code analysis tool)
T5	Triage vulnerabilities
T6	Checking new libraries and packages
T7	Testing and finding new vulnerabilities
T8	Keeping track of the security issues in the backlog and making sure they are properly labeled
T9	Making sure there are security related cases in the Sprint
T10	Ordering tests from the security team
T11	Assisting the rest of the team in security matters
T12	Showing and explaining found vulnerabilities to the team
T13	Delegating security tasks
T14	Developing knowledge, self learning
T15	Be up to date with security

There was a great variety in the time spent on SE tasks. The average seemed to be one or two days per week, but several SEs said that time spent varied from week to week. Filling out the SSA, for example, was recorded as something that required additional time. Some SEs also found it difficult to respond because the tasks overlapped with their regular responsibilities. One SE stated: "I feel like it is a way of working aligned with the development role." Another said: "I think most things we do are highly related to security."

When asked whether they found it challenging to fit the SE tasks into daily tasks, most answered no. A majority of the interviewees highlighted prioritizing urgent security tasks and the need to be flexible about it. Known security issues take precedence over other tasks, and they considered themselves SE first and developer second. Having an understanding product owner and team leader was also emphasized.

4.3.2 Defining the Role

Visma has a role description, but only for SEs working on projects with particular security standards. In addition, we received feedback that the role description is difficult to find and has complex wording. One of the interviewees also noted that they felt like the role description did not fit their company: "When we read it, we did not think it fit us very

well because Visma is a large company with many products. So what we did, we just started with the roles that Visma has provided and made our own based on those."

The responsibilities and tasks that belong to the role also seemed unclear to many: "There are some things that came as a surprise because I did not have a list or anything I could follow." Another SE stated: "I have no deep understanding about what I should do, what are my main tasks?" Several SEs mentioned a list of tasks or responsibilities to improve this issue: "It would be nice to have a formal list of responsibilities that I had to do because sometimes there was something that I thought, 'OK, wait, I have to do this as well? I did not know that'".

A common theme among interviewees was a lack of comprehension of the whole picture: "I could have had more like the big picture view." Another interviewee noted: "Also to understand what it is really about. I think that is one of the sections that maybe could be improved."

4.3.3 Recruitment

The survey results showed that several SEs volunteered for the role. Because of this, we wanted to use the interviews to learn more about what makes a SE volunteer.

All of the SEs who said they volunteered for the position in the interviews indicated they did so because they were interested in security. Security was identified as a trending direction, and people were curious about the field. Trying something new and getting a variation from everyday work tasks was also a motivation: "I felt that having that role and making a difference in security would be cool and not as grinding as just the normal development work." Another interviewee voiced: "I do not have any security-related background, so it was a chance to try something new."

The SEs were given the role in one of two ways: They were either explicitly offered the role, or the role was advertised to the entire team. There was also one incident where the SE was recruited as a student: "When picking up this role, it gave me a good opportunity to write my [master's] thesis around this topic, and it seemed like a good opportunity to combine my studies, the job, and my interests."

4.3.4 Security Training

The survey results revealed that the SEs are highly dissatisfied with their security training. Therefore, the interviews were used to investigate the problem further.

Organized Training

Most SEs did not have a lot of organized security training, which seemed to be the main problem. Some had a previous SE they could consult, but otherwise, not anything specific.

One of the interviewees stated: "It would be nice to have some structure to organize some courses to, at least, get some basics."

The organized training we recorded is presented in Table 4.12.

Table 4.12: Organised training recorded in the interviews.

ID	Training	SE specific?
Tr1	Application security training organized by Visma as a part of a bigger security event	No
Tr2	Other security engineers held cyber security training within the company	No
Tr3	Small workshop with other SEs	Yes
Tr4	Instant courses on how to detected and hack a server set up for the course	No
Tr5	Theoretical presentation on data protection and information related to that	No
Tr6	Presentation with real examples from the OWASP Top Ten [45]	No
Tr7	Security Conferences	No

Self-study

However, many interviewees talk about self-studying as their primary form of training. "I think it was mostly off to ourselves how we wanted to work with the security things." Multiple resources for self-studying were recorded. They are presented in Table 4.13.

Table 4.13: Resources for self-study discovered in the interviews.

Practical learning	
L1	Secure Code Warrior [46]
L2	Pluralsight [47]
L3	TryHackMe [48]
L4	HackTheBox [49]
L5	Cybersecurity course offered by a private company
Theoretical learning	
L6	Different security Slack channels
L7	Googling
L8	Security news
L9	Conferences
L10	Visma Career Website
L11	OWASP [45]
L12	Articles received from the security team

Numerous interviewees had used online tools to learn about security and hacking. The tools appeared to be something with which they were very satisfied. Many preferred to learn practically: "In my experience, getting your hands dirty is the best way to learn. So getting an example application and having to try to hack it works best." Self-study is beneficial because it is something you can log in and do from time to time. Also, you can do things at your own pace and look things up while you are going.

Topics for security training

The SEs seemed to be missing more guidance on how to acquire security knowledge. Even though they have time to do self-studies, they struggle to find information and where to start: "I can imagine that it can be cumbersome for new Security Engineers that get appointed to figure out where to start and what to focus on." Another statement suggests that the field is too broad and hard to navigate:

"Developing security skills and gaining more knowledge has been a goal for the past two years. (...) it [the field] is so wide, and I am lost. I do not know what to do or where to start. This failure to gain more knowledge in this field is mostly because I do not know where to look or what to do."

Some suggestions for topics that the SEs think could be suitable for basic security training were recorded. The suggestions are presented in Table 4.14.

Table 4.14: Topics for basic security training mentioned in the interviews.

ID	Topic
Tp1	OWASP cheat sheet series
Tp2	Defensive training
Tp3	Offensive training
Tp4	How to deal with an issue; how to look into it, how to prioritize it
Tp5	Threat modelling
Tp6	Penetration testing
Tp7	How to teach their teams to always think of security
Tp8	How to delegate tasks efficiently

Offensive security is a point mentioned by multiple: "To be able to do a proper defense, you need to understand a little bit of how the enemy thinks." Another one stated: "I cannot understand the risks if I do not know how to hack."

Getting a certification is also mentioned. "(...) it would be nice to get some kind of certification. It would like, feel better."

Training in Groups

The interviewees mentioned multiple aspects of why they would like to develop their knowledge together in groups. Working in groups is beneficial because you can get help from each other and collaborate: "Two people think differently. So even though you are stuck on this task, the other person might not, which makes you understand a little bit more, and you can move on to the next one instead of being stuck on one task."

Another thing mentioned is that it is easier to carry out the training when it is scheduled: "I think it should be done in classrooms because if you have a document, you will just do it later." Another interviewee stated: "When you are on a scheduled training, you have

the whole day for that, and it is booked in your calendar. You know you will do it; you will not miss it."

It was also mentioned that justifying the training to your superior is easier when something is scheduled: "If Visma says, 'On this date, all our security engineers in Oslo need to take this time', then I can go to my manager and say 'OK, this day I need to set aside because I have a course' and that is much easier than to say 'OK, I need to read this 20-page document and I need to take time for it.'"

One SE also mentioned that working in groups is more fun: "(...) It was very fun. And that is also very important for training. If you are having fun, you are learning better. At least that is my experience."

Those who already have some experience with workshops or other group training seemed to be satisfied: "It would be really nice to have those hacking workshops for the developers again. We have a lot of new people who could really benefit from that kind of experience. Just getting a little hands-on experience seeing for themselves that this is how a service gets hacked."

Convince team

There are multiple reasons why the security training should get more attention. One problem we recorded is that the SEs struggle to convince their teams to take threats seriously: "If I do not have a proof of concept on how things are used against us, then I cannot tell my team to do something about it." Another interviewee noted: "Last summer, I spent a whole day trying to figure out how to convince my team to fix something. Maybe if I knew more about hacking, I could do it more easily."

Also, struggling to help the team due to a lack of knowledge is an issue: "(...) sometimes I feel that I cannot help someone, and I feel bad about it. It is a bit stressful."

4.3.5 Soft Skills Training

None of the SEs we interviewed had received any soft skills training. However, when asked if soft skills training is something they would have found useful, the interviewees were a bit hesitant but mostly positive. "An introduction to that, not too big course or something, but an introduction maybe." Another one answered: "Well, yeah. If it helps achieve results faster, make people listen to me, understand me better, or explain myself better."

There are four issues that the SEs struggle with regarding soft skills.

Firstly, they find it hard to talk to the management: "I have to speak to the manager, which is something different because you have to talk to them on a different level, more high scoped. However, I need to speak to them so that they understand that these issues need to be fixed." Another interviewee stated: "This quarter I have to create some kind of security status talk to all the managers in our company. (...) And for that, I am

completely below the water level. That is a completely different thing that I do not know how to do."

The second thing is making the team listen to what they say: "I would need more help with how to convince my team that we need to fix some things." Another interviewee said: "I feel that it is my weak side because I am not sure that I am persuasive. Sometimes, when I tell the team about things that we need to follow up on, they are postponed or skipped. I probably should be tougher."

Then there is explaining security issues to less technical persons: "That is at least my flaw. I am a really technical person, so I dive into things. Knowing how to make things simpler to understand for somebody who does not have a technical background could be beneficial."

The last issue is how to deliver the message of vulnerabilities kindly. One SE talks about people being too blunt: "So being very blunt about things can make the person you are talking to, that you are trying to inform, go to a defensive stand. And that is not a good thing." Another one mentioned pointing fingers:

"How do you handle the different teams in the review meetings because sometimes you need to present a better alternative of doing something but not like pointing fingers. (...) Because if you are in the team, doing this role, then people might not like you because you are telling them that they have done something wrong or implemented something wrong."

However, one interviewee noted that these skills could be difficult to improve: "So being able to speak to others in a good way is definitely a good thing. It can also be very hard to learn because we are set in our ways."

4.3.6 Communication

We used the interviews to further explore communication in the SE program in order to figure out why so many people said they do not communicate with other SEs at all. By doing so, it became clear that the communication mostly takes place between SEs in the same company. Those who do not have any SEs in their company communicate less frequently, if at all. It was also noted that much of the communication was restricted to asking for help or advice.

Over half of the people interviewed said they usually do not communicate with other SEs. Some of them communicated a bit, in the beginning, to ask for help: "On the first stage I did. I asked for some advice from other security engineers". This confirms the findings from the survey: Communication decreases after the SEs have been in the role for a while.

A reason for the lacking communication is that each team is dealing with different things: "At the moment, I think that each team is mainly concentrated on dealing with their own problems. So for some time, there is no frequent communication". The SEs responsible for projects of different sizes also have different responsibilities. One of the interviewees works in a small team and can focus on making small improvements and details. However,

another SE in the company has a product with more than 100 people in the development team and is, therefore, more focused on delegating and having control over the project. "For him, he does not have that much time to deal with those small improvements. I would say he is more focused on delegating stuff (...)". In conclusion, they would not have that much in common to discuss. It is also a problem that the SEs in the same company are not aware of each other. When asked if there were many SEs in the company, one of the interviewees responded that they did not know.

Asking for help

For many, the communication in the SE role is restricted to asking for help: "It seems to me that the communication is mostly like, if someone asks for something, then the help is provided." Asking for help in the Slack channels is talked about as very effective: "Yeah. I personally feel that if there were something that I needed, I could always post it on the Guild channel, and I would be surprised if it took more than five minutes for someone to respond with a helping hand. So those are pretty effective." The Slack channel is also where the SEs find people to contact directly: "Yeah, I have had a few people contacting me about different things. I think that might be because I am so active [in the Slack channel]."

Some interviewees find it hard to reach out for help due to personal characteristics. "I am a shy person, so I do not ask people to help or recommend something. Only if it is a very close person."Another obstacle is not knowing who is a SE: "No, I did not reach out that much because I did not know who is a security engineer."

Increase Communication and Collaboration

According to the interviewees, communication and collaboration could be improved. One interviewee talked about failed attempts to improve the situation.

"I think the collaboration between the engineers is lacking. I would like to see more of that, but we have had multiple initiatives in the past, and they have all ended without any results. We have tried initiatives where we group them by country, but because of how the product unit was made up, that did not work."

The interviewees seemed to be a bit split about whether there is a special SE community: "Sometimes it feels like it is not really a closed community. You can reach out, but discussions in Slack channels are not so often. There is not that much communication between security engineers, at least in the chat. I do not know about private and between teams." However, another one states the opposite:

"I would say that it is the community aspect because, as I already mentioned, if you have a problem with virtually any part of the VASP or any product or anything, you can just hit up via Slack, and there will be someone responsible of that area and telling you how it should work. Or in most cases, there is someone from another Visma company saying that 'hey, yeah, we had the same problem and we just did it like this and this' and it is

a big thing."

There is another interviewee that had similar opinions: "I think I like the fact that, If you have a problem and you ask, there will be someone that will answer it and try to give you some ideas on how to go forward." The contradicting feedback could indicate that there are a few SEs that feel left out of the community.

Information Sharing

Another point with contradicting answers is whether the information flow between the SEs is good. One interviewee stated: "It would be nice to see some more sharing being done, like to learn from." However, one interviewee mentioned sharing as one of the key successes of the SE program: "There are quite a bit of people who are really passionate about what they do and really passionate about sharing news and ideas about security. I think that is the key part." Other statements regarding this were: "I think the fact that we are open with findings and these are shared" and: "Large problems that are found are communicated and shared."

Internal Communication

Having other SEs in the company seemed to be very helpful: "(...) a lot of those things I just deal with my coworkers in the company. We have a few products, and each product has its own security engineer. There are like five of us or something. So we have this kind of internal support network." Another interviewee stated: "I always have a lot of people that I can ask, that already knows a lot about our environment and infrastructure and things like that. Not only the security personnel but also the infrastructure engineer and other people like this. I have already worked in the software developer role for two and a half years, so of course, I know all of them."

When asked what the reason for not communicating with SEs outside the company is, one interviewee answered: "It is easy to discuss in your native language, and we are so interlinked with our products. We have shared environments and shared resources, and teams. So it is effortless because we already know the context. Solving these things is easier with someone who already knows what you are talking about."

Topics discussed in the internal groups extend a bit further than just asking for help, which was the case for those who did not have a close internal community of SEs:

"And the things we talk about are basically anything because, whenever we get some, any kind of thing that requires attention, maybe a vulnerability or anything alarming, or something that just came up, we usually discuss it with each other to kind of, find out if it concerns all of us or only some products, and how we can mitigate this and things like that."

Another interviewee said: "We talk about the situation of our products and the numbers and what we should do next. Security, SSA, what the situation is in every product, and other things. And the problems that we have in general."

Communication With the Security Team

Even though communication between SEs is limited, multiple interviewees mentioned communication with the security team: "I do not remember reaching out to other security engineers. Only to the security group on different subjects, but not the peers." Another interviewee stated: "(...)the communication is quite good with the security team."

4.3.7 Regular Meetings

It is already established from the questionnaire results that the Guild Meeting is something the SEs appreciate. However, we used the interviews to investigate if the SEs also had internal meetings only with the SEs in their company. Only a couple of the people we interviewed reported having some sort of internal meetings. However, when asked, several recognized it as something they would like to have: "I think so, yeah. Maybe you could bring up some more local security issues and stuff." According to another interviewee: "Yes, that is very useful because we can discuss concrete things. It is useful to know that other people and other products have the same problems, and maybe someday we can fix those together, have some solutions together, and help each other if we know each other better."

Topics for meetings

Different topics are discussed in the internal meetings. Developing knowledge together is mentioned by multiple interviewees. Topic currently at or suggested for an internal SE meeting is presented in Table 4.15.

Table 4.15: Topics discussed at or suggested for internal meetings.

ID	Topic
M1	Local security issues
M2	Coordination
M3	Information and knowledge sharing
M4	Pick a topic that somebody is struggling with, and take a deep dive
M5	Investigate topics where competence is missing

Internal Meetings With Other Attendees

There are also some mentions of internal meetings with the SEs, including other people:

"Bigger project meetings and common planning sessions for all of the development teams, where we will also discuss the security improvements and things like this, so everybody is on the same page, not only the security engineers, but everyone working with the development. They know what has happened; we are communicating, dealing the tasks to them rather effectively."

Another interviewee talks about meetings to make it more evident to the customer what the SEs are doing: "When improving the security of a product, you can easily spend countless hours, but it is rarely visible to the customer until it is on the headlines. (...) It is easier to bring this kind of visibility to the process, so everybody knows what we are doing."

Guild meeting

The guild meeting, as described in Subsection 2.4.2, is something many of the interviewees spoke highly about: "I enjoyed the fact that there were bi-weekly meetings where security news was presented in an approachable way. So that is something that I loved, like sharing enthusiasm and knowledge. That is quite important." Another interviewee stated: "I find those meetings interesting. I do not think I get a lot for my daily work, but it is the current situation in security. That is interesting." Another one said: "I think they are useful for staying up to date on the threat landscape, staying aware of whom You can contact if I have this and this problem."

One negative thing that was mentioned about the guild meetings is that there is little variation in the speakers: "It would have been good if it could contain more stuff from other people. (...) more talks from other people, what other companies are doing or experiencing and stuff like that."

4.3.8 Resources and Support

Most of the interviewees seemed satisfied with the provided support and tools: "I think those [the tools] are great because they help us in the real world. And it's also more documented now how you get onboarded on all of these." Another interviewee mentioned: "I think we have very good services for testing and surveillance."

Overview of tools

However, one SE mentioned that it can be a bit overwhelming with all the tools available: "Basically, there are a lot of tools, but the problem is when there are too many of them, it gets quite tedious to follow every single channel and participate in every meeting." There is also some confusion about what tools are available, what they are used for, and who has access to them: "(...) that is something I do not have access to, and I do not know if I can have access to it [the tool] or not." Another interviewee stated: "I am not aware of all the available tools for us as a team in the company."

Documentation hard to find

One of the resources the SEs are not that happy with is the documentation. Multiple SEs mentioned that the information is spread over multiple sites and that it is hard to find

what you are looking for:

"I think there were times when we were not sure if there were any recommendations. We were questioning some third-party application that was used, thinking, 'OK did anyone do a security scanning of these? Where is the stored data?' We ended up finding the answers we needed, but it was not a straight line, knowing that OK, now I go there and I find information about this tool that I am using."

Another interviewee stated: "In some rare cases, it has been kind of difficult to find the document describing how to onboard; in some cases, you have to do a little digging, but you eventually find them." A combined place for all the information is suggested as an improvement: "(...) structuring it [the information] better, even though all the information is available from within the company. (...) There are different parts where this information is available, and maybe a way of combining these, you know, like a learning platform."

Slack channel

As mentioned, the Slack channels have helped the communication between the SEs a lot. One interviewee mentioned it as the best thing about the whole SE program: "I think the part that might actually be the best part of the security engineer program is that we have one place in Slack where we can raise questions and get answers to them." The Slack channel is also helpful for learning reasons: "The Slack channel, I personally have not asked any questions, but I read quite a lot of questions. So I think at least a few a day, and when I read the answers, they are very informative and good."

Mentoring

Almost all of the interviewees mentioned mentoring unsolicited. The interviewees who had a mentor spoke positively about it, while those who did not have it said it was something they were missing: "To have a person delegated for me to ask, like a mentor, that would have been really nice." When asked if there is any tool or document that could have replaced a mentor, the answer was no: "I do not think so, just a dedicated person." A mentor could be helpful because some of the problems the new SEs run into are very specific and hard to solve. "You can read all the technical papers you want. But if you have specific questions, it is hard to find the answer in the documentation." Another interviewee remarked: "I would spend much less time and resources if someone could guide me. It would be much more productive."

One interviewee stated that while he did not have a dedicated mentor, he did have certain colleagues to whom he could turn for advice. However, this was not a good solution as he felt he was taking up too much of his colleague's time: "I had someone I could ask, but at some point, I felt like I was taking too much of their time because it was not part of their work responsibilities."

One interviewee also talked about alternatives to individual mentoring. However, they

were hostile to having mentored in groups because they were not comfortable asking questions in big groups of unknowns. "I think the security Engineer Guild meetings show that people are not keen on asking questions in big groups. (...) If I do not know anyone in a big group of people, I would not ask questions most of the time."

One of the interviewees talked a bit about who could be a mentor: "It is easier if they are in the same company and I can meet him or her in person. But yeah, in our company, we do not have, at least I do not know of anyone who could be a mentor. So it could also be not someone who is not on the premises."

4.3.9 Support From the Security Team

The security team also gets a lot of praise: "I think the entire security team is great. They are very helpful and always there if you have any questions." Another interviewee stated: "I think the security team at Visma is very strong and diverse. They did a great job creating the documentation and holding these weekly meetings about new security-related findings. I have never seen such as security dedicated team before. It is great."

4.3.10 Extra: Management and Stakeholder Involvement

Management and stakeholder involvement was not specifically investigated in the interviews. However, there were a few mentions about it.

Support from the top was mentioned as a key success: "Security as a priority. If you buy into that all the way from the top, you know it will get done. The thing that gets done is the one that the boss cares about. And if they care about security, it has to be done. It always comes down to, you know, priorities and resources."

It was also highlighted that the approach should be holistic: "I think they should look at different levels of applying security because it is not only about the application but also about the infrastructure as assets like building security and deployment of cloud services. They need a holistic approach (...). I think we need to look at it as a whole."

4.3.11 Extra: Orientation and Onboarding

Orientation and onboarding were not a part of the initial steps. However, because it was investigated as a part of my collaborator's thesis and frequently mentioned, this section discusses the results regarding orientation and onboarding to decide whether this is something that should be included in the steps. To make a clear distinguish between the two, *orientation* is defined as "an introduction, as to guide one in adjusting to new surroundings, employment, activity, or the like" [50], and *onboarding* is defined as "the process in which new employees gain the knowledge and skills they need to become effective members of an organization" [51].

Orientation

Most of the interviewees said they did not get any form of orientation, but several said that it is something they would have liked. The main problem seems to be that when they started, they did not know what they were supposed to do or the big picture of their role. When asked if they received any orientation to get started in the role, one interviewee said: "Almost none. I think I was given the link to the confluence page where you can read about SEs."

Onboarding

In combination with training, orientation is the point of the role where SEs have the most complaints. The majority of the interviewees got little to no onboarding, and they were left to figure things out on their own: "I did not get any formal training. I pretty much tried to wing it, and if I had any problem, I could consult a previous SE since we were on good terms." Another SE stated: "There was not really an onboarding at the time. Basically, I got the role assigned, and I had to start figuring out what to do and how to enroll in the program." However, some SEs indicated that they had received some sort of onboarding. The actions is summarized in Table 4.16.

Table 4.16: Actions recorded as received onboarding to the SE role.

ID	Self Study
O1	Received link to confluence page with SE information and steps to do
O2	Security team provided resources for web application security training (i.e., OWASP [45])
O3	Encouraged to watch videos some videos explaining important aspects
O4	Courses in Pluralsight [47]
O5	Received some documentation, security pages of Visma
	Mentoring
O6	Mentored by more experienced SE
O7	Mentored for a whole year
O8	Discussed risk assessment and SSA with former SE
O9	Short meeting with former SE
O10	Consulted former SE/friend

Two of the interviewees reported being satisfied with the onboarding. However, the common feature is that they both had a background in security: "Yeah, I do not think that any of my responsibilities were really difficult. I did not have much trouble."

Onboarding plan

A more systematic onboarding is something that nearly all interviewees mentioned: "For sure, you need a more structured way of doing this introduction." Another one stated:

"You need to give something in the beginning; you need to have a dedicated program in mind with some initial steps, maybe some documentation, some videos. You should have a plan".

Missing information on the onboarding was also a common problem. "There might be some confluence page somewhere, but I do not know where it is.", "Knowing what the onboarding actually is, because right now I do not know.", "I have tried to find something on confluence that we have, but I have read the responsibilities of a security engineer, but that is it. I do not know where to continue."

A starting document is also mentioned as a possible improvement. The document should contain some examples of articles, videos, and different training, but organized and gathered in one place. The problem with the existing documentation is that it is spread out and hard to find. "Now, we have a lot of documentation in a lot of places, but I do not see that there is a central place from which you can start."

There is also a wish for a more specific onboarding. "It [the onboarding] could have been Visma specific. Like all new security, engineers should have this onboarding course or similar." Receiving a diploma after finishing orientation was also mentioned: "Having a proper onboarding with an inauguration or diploma or whatever that said 'OK, now we are starting the onboarding process, and these are the steps you are going to go through to be able to be considered a security engineer of this level.' That might be something."

Other improvements that are mentioned are more guidance and training. Specifically mentioned are more guidance on the tools, advanced pen-testing methods, project management communication, and delegation.

4.4 Summary of the Case Study Results

The results from both the questionnaire and the interviews are summarized and presented in Table 4.4 to create a better overview.

Table 4.17: Summary of case study results.

ID	Step	Questionnaire	Interviews
	General		The SEs spent varying time on SE tasks. The SEs do not have troubles fitting SE tasks into their daily tasks.
St1	**Management**		Management involvement and having a holistic approach were mentioned as essential.

St2	**Define the role**	Having clear role expectations had a positive impact on satisfaction with orientation, onboarding and training.	The SEs want a role description so that they know what to expect. The role description should include responsibilities and important tasks. The SEs are also lacking a view of the whole picture.
St4	**Recruitment**	Most SEs are developers with no to little previous security experience. Those who volunteered for the role are more motivated than those appointed.	SEs volunteered because of security interests.
St5	**Training**	The SEs are dissatisfied with both security and soft skills training. Training is the part of the program where most SEs want to see improvements.	The problem seems to be that the SEs have received little to no training. Self-study is much used. However, they are unsure what they should study and would like some guidance. Many SEs mentions offensive (hacking) training as something they would find useful. Multiple benefits of group training are mentioned. Security training is needed to help convince the team to focus on security. Soft-skills training would help manage the team.

St6	**Communication**	Slack and email are the most used communication tools. The communication tools are effective. Communication decreases with seniority.	The communication between SEs are primarily internal in a company. For those who do not have a network of SEs within their company, the communication is restricted to asking for help. Many SEs would like to increase communication and collaboration. The communication with the security team is good. The Slack channel works well for communicating.
St7	**Regular meetings**	Around 73% of the SEs find the Guild meeting useful. The meeting makes the SEs feel more like a part of a community.	Regular meetings would be useful for discussing local security issues, sharing knowledge, and coordination with stakeholders outside the team. The guild meeting are talked about as interesting and motivating.
St8	**Resources**	Most SEs are satisfied with provided resources.	Most SEs are satisfied with the tools. However, documentation is hard to find. They are missing an overview of the available tools. The Slack channel and the Guild Meeting are especially mentioned as good tools.
St9	**Feedback**	Being asked for feedback improves motivation. Being told how they perform makes the SEs more satisfied with their own performance. However, it did not impact motivation.	
St10	**Automation**	Around 50% of the SEs think parts of the program can be automated. Onboarding and training are the parts most think can be automated.	

St11	**Pre-allocate time**	Preallocating time to work on SE tasks does not seem to have an significant impact on SE satisfaction.	Many SEs say that they work on SE tasks when needed.
St12	**Motivation**	Motivation depends on whether the SE volunteered, training, and community feeling. The motivation does not decrease with seniority.	
St13	**Security team**	Support from the security team is essential for satisfaction with the resources.	The security team gets plenty of positive feedback: Helpful, strong, and diverse. Very dedicated.

4.5 Results from the Slack Data Analysis

The results from the quantitative analysis of the Slack data are presented in this section.

As briefly mentioned in the interview results, the threshold for asking questions in the Slack channel is high. As seen in Figure 4.21, the number of members in the channel is much higher than the number of members that have posted something.

Figure 4.21: Number of members in the Slack channel compared to how many posted something.

As seen in Figure 4.22, there is a big difference between the number of posts and the number of people posting. The results indicate that the members that actually post are highly active. The graph also shows that there are, on average, 247 posts each month, which equals around 12 messages each working day. The result includes the vacation month of July, where the number of posts is lower than for the rest of the year. This means that the actual average of posts each day probably is higher.

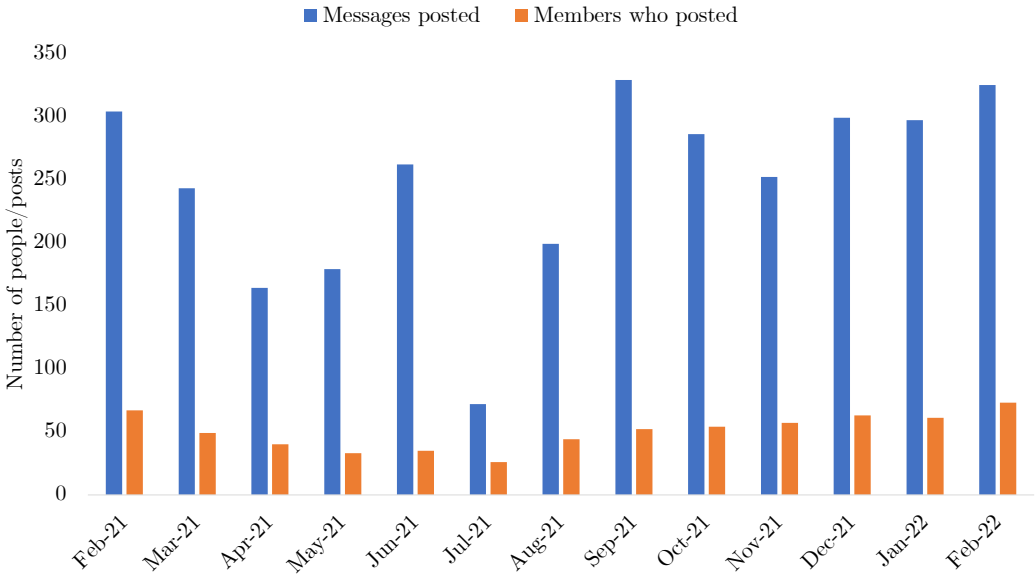


Figure 4.22: Number of messages posted in the Slack channel compared to the number of people who posted something.

Figure 4.23 shows the difference between the number of members who posted and the number of members who read the posts. We see that there are a lot more people who read the posts than people who actually post something. However, the high number of members who reads the posts supports the statement from the interviews, where several interviewees said that they found the questions and answers in the Slack channel useful for learning purposes.

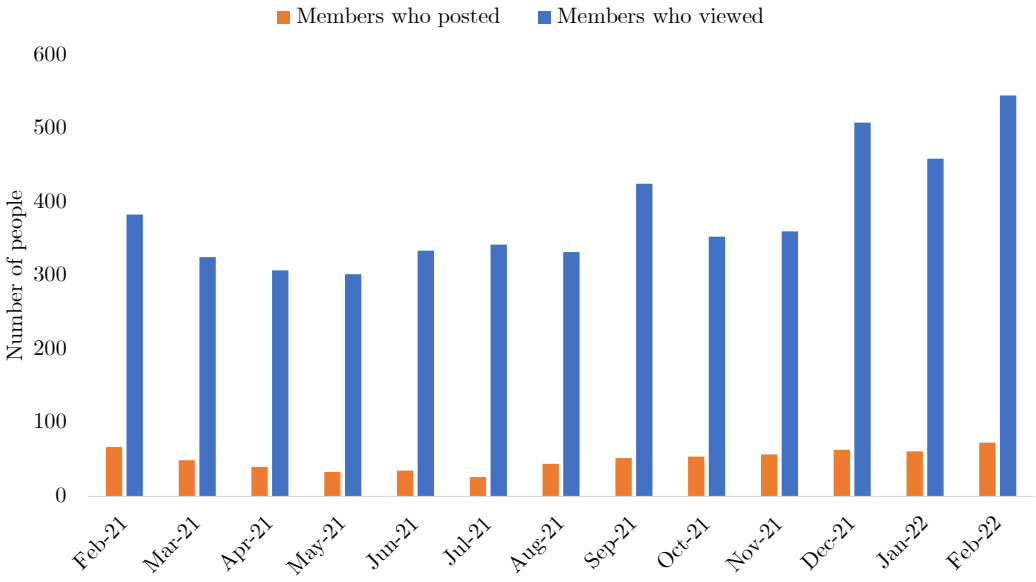


Figure 4.23: Number of people who posted something in the Slack channel compared to number of people who read the posts.

Figure 4.24 shows that the number of people who are reading the posts is not that far from the total number of members in the Slack channel. This indicates that the members follow the posts in the channel even though they are not posting themselves. The average number of members in the channel is 499. However, the number of current SEs is only 247. The big difference might explain why there are also some inactive members.

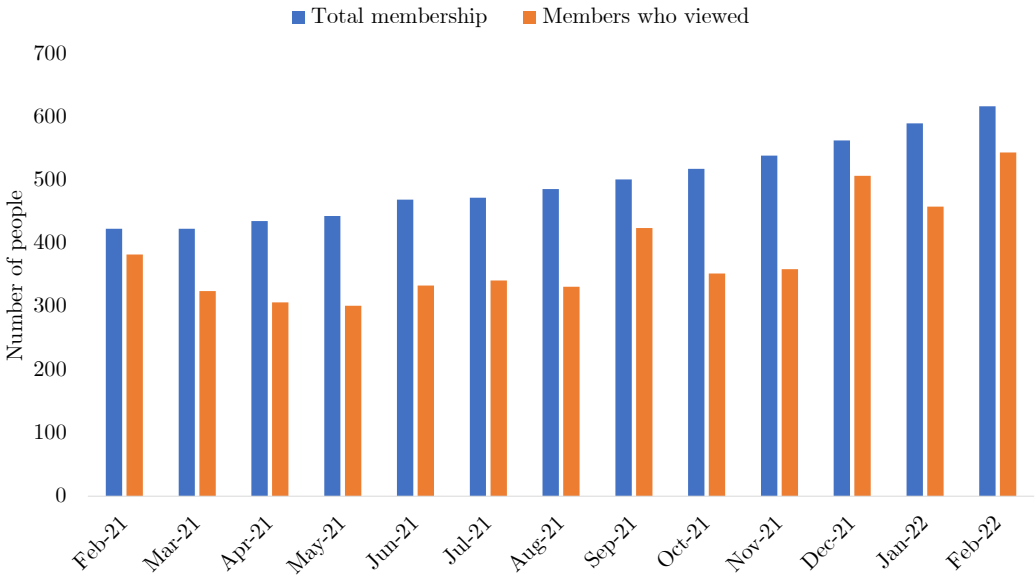


Figure 4.24: Number of members of the Slack channel compared to how many read the posts.

4.6 Contradicting Results

The results did not contain many inconsistencies or surprises. However, in the questionnaire results, we discovered that 75% of SEs report being given a realistic view of what was expected of them in the SE role. In contrast, in the interviews, we were given the impression that most SEs were not given much information when they started in the role and mostly had to figure things out themselves. In addition, they did not have a clear understanding of the whole picture and were unsure about their tasks and responsibilities.

Chapter 5

Discussion

The research findings and their implications for practice and research are discussed in this section. The sections also discuss the research's limitations and further work.

5.1 Implications for Practice

This study has expanded the knowledge base of what we know about security champions and has helped distinguish between effective and non-effective actions. The main contribution of the research is a set of validated steps on how to establish and maintain a security champion program. The research contributes to the industry by allowing the companies to get an insight into the thoughts and opinions of security champions, allowing them to better identify the areas that require attention and what security champions need to accomplish their work effectively. The research could make implementing a security champions program less costly as the companies will be able to do the process themselves and do not need to hire external help or consulting. In addition, the research gives academic proof and can help convince management and other stakeholders about the actions and resources needed to establish the program successfully. For the security champions, the study will hopefully improve their working environment and make it easier to fulfill the role of a security champion.

The research was conducted in a big organization consisting of more than 200 companies. Due to this, the results are foremost relevant for bigger companies. However, some of the findings might be extended to smaller businesses as well. Smaller companies naturally have fewer resources and should therefore focus on the most critical steps of the program, as prioritized in Table 5.2.

5.1.1 Challenges and Areas of Improvement in Visma

The case study identified several challenges and potential areas for improvement for the companies in Visma. These results are important for practice because it helps the com-

panies see what challenges they might run into and how they can be improved. The found challenges and improvements are presented in the following subsections.

Challenges

The companies face several challenges when implementing a security champions program. One of the main challenges is to get enough volunteers. We found that over 40% of the security champions were appointed, even though the companies' culture clearly says "not to force people into a role." One possible explanation for the lack of volunteers is that the role is not adequately defined. Even the security champions themselves were unsure about their role and what they were supposed to do. People are naturally hesitant to volunteer for a role they are unfamiliar with.

Another challenge is creating a security champion community and ensuring communication between the security champions. The results show that providing communication channels is not enough to ensure communication between the security champions. The existence of a security champion community is disputed, which implies that companies find it challenging to create a community where all security champions feel included. Some companies have internal communities, or "internal support networks," as one interviewee described them, while others do not even know if there are other security champions in their company. A part of the problem appears to be that the security champions are never introduced and are thus not aware of each other. There is no arena where the security champions in a company can meet, and the security champions do therefore not know each other. Another issue is that communication decrease with seniority. It appears that this is because the communication ceases when the security champion no longer needs to ask for help.

A consequence of the non-existing community is that the threshold for asking questions and using the Slack channels is high. There are some highly active members, and the rest only reads the discussion without participating. This issue is also briefly touched upon in the interviews, where we got feedback that some people find it uncomfortable to ask questions in big groups of unknowns. The reason for this might be that they feel like they are asking "stupid" questions, especially when they know that there are a lot of security champions with higher competence in the Slack channel.

Lastly, it is a challenge to make the security champion program scale with the company's growth. The results show that essential parts of the security champion program have been down-prioritized. According to the expert interviewee, there are not enough resources to keep up with the company's growth. Currently, no specific actions are automated, which is an important reason why the program struggles to scale.

Improvements

The companies investigated in this case study offer some security training, but it should be improved. Currently, it is primarily up to the champions to acquire the needed security knowledge by doing self-studies. Despite the effectiveness of self-studies, the security

champions are unsure of what aspects of security they should concentrate on. Many also mentioned that they would like to have scheduled group training to make it easier to justify the time spent to their manager. In some cases, it seems to be a challenge that the managers do not see the value of the security champion gaining knowledge. The training needs to be improved because multiple interviewees talk about how they struggle to convince their team to take threats seriously because they do not have enough security knowledge.

A general improvement that can be made is to collect all the documentation regarding security champions in one place. Currently, the documentation is spread all over the place, making it hard for the champions to find the information they are searching for. Creating a common hub with all the information a security champion needs would improve the program.

Visma has no official standard for neither orientation nor onboarding. There is no general orientation about the role when the security champion starts, and the security champions seem insecure about what to do. Giving an introduction together with the defined role would help the security champion understand what they are supposed to do and why the role is important. The orientation could be as easy as a short video introducing information about where to find essential sources and welcoming the security champion to the program. Neither onboarding is offered. The interviews reveal a great deal of ambiguity about the role, with many people unsure of what they should do and how to gain knowledge. Implementing a short orientation and onboarding would improve the program.

5.2 Implications for Research

As established in Chapter 2, there is little former research on security champions, and only seven papers concerning security champions were found in the structured literature review. There is also some grey literature on establishing a security champion program, but the reasoning behind the steps or proof that they are effective is not provided. This study contributes to research by verifying the existing research and providing a starting point for further research. The research could spark curiosity about the field and initiate more researchers to be interested in the subject. The findings are significant for theory because they provide an academic framework that gives the companies a starting point and a credible strategy to establish a security champion program. The approach is confirmed using theoretical methods, and as a result, the risks are lowered, making it more secure for the industry to follow the proposed method.

According to the results, some things are missing from the set of steps to establish a security champions program. The following subsection presents new steps that should be added and the total evaluation of the steps.

5.2.1 New steps

In addition to the steps found in the literature, the program could be improved by adding some additional steps. Steps believed to improve the security champions program are presented and discussed in the following subsections.

Orientation

The security champions we have talked to never got an introduction to the role, which seems to confuse them. They say that they do not have a clear view of the whole program and are unsure of what they are supposed to do and what their tasks are. Giving a short introduction to the role combined with creating a clear definition of the role and what is expected is beneficial. In addition, it should not require too many resources and is an easy fix that will provide much value.

Onboarding

Onboarding onto the role is something that is not mentioned in the literature. However, we see from the results that this could benefit the security champion. The security champions we interviewed struggled to navigate the security field and seemed a bit insecure in their role. They were unaware of tasks and were afraid to ask questions. Additionally, it took a long time for them to figure out things because they had to do it independently. Creating an onboarding plan for the role would provide value by making security champions more confident and efficient in their roles, as well as allowing them to get up to speed more quickly. Looking at what the security champions want to improve in the program, onboarding is most selected right after training. Therefore this should be added as a step. The defined role and the initial training might be enough to onboard the security champion. However, giving the security champion some extra follow-up and perhaps a mentor could ensure that the security champion gets onboarded adequately to the role. We also found that the security champions are missing a more structured way to get onboarded, i.e., a starting document. They also mentioned that it would be beneficial if the onboarding was Visma-specific. As a result, in addition to defining the role and providing basic training, onboarding should include information on how to use the specific technologies. Receiving a diploma when the onboarding is finished could be motivating. Onboarding is also mentioned as something that could be automated.

Mentoring

Mentoring is something many of the security champions are requesting. They seem to be struggling with very specific issues and use a lot of time to figure them out themselves. Those who did have a mentor talked about it positively. Asking colleagues without having anyone dedicated is a possibility, but some security champions found it uncomfortable to ask many questions because it takes a lot of the colleagues' time when it is not really their responsibility. However, assigning a mentor to each security champion will require a

lot of resources and be expensive for the companies. Therefore the solution should be to find a way where one person can mentor multiple people. One solution could be to create online or physical question hours where the security champion can sign in and get help for their security-related issues. We also recorded that it is a problem that some people do not want to ask questions in big groups, which could be solved by creating breakout rooms where the security champions can ask their questions in private. Hopefully, the mentor would save the new security champions a lot of time by helping them with issues that are hard to find the answers to in documentation.

Flexible Hours

Preallocating hours to work on security tasks was found ineffective. Consulting the interview results, the reason for this is because the security champions have to be very flexible about their tasks and jump on security-related tasks when they appear. Several mentioned that when a security issue emerges, it takes precedence over their everyday tasks. Therefore, instead of providing a fixed time where the security champion can work on their tasks, it is beneficial to try instead to be flexible and allow the security champion to work on the tasks when necessary.

Create Community Feeling

One of the challenges we found is that some of the security champions do not feel like they are a part of a security champions community and do not have anyone to communicate with regarding security champion-related issues and thoughts. In the questionnaire results, we saw that feeling like a part of a special community increased the motivation for the role. It would be beneficial if the companies facilitated for creating a community feeling, i.e., by arranging local social events for the security champions. Part of the problem seems to be that the security champions are not aware of each other and therefore do not communicate. If they are introduced and socialize regularly, the threshold for reaching out for help will most likely be lowered. We saw from the interviews that having an internal network allowed the security champions to discuss vulnerabilities they found that could be relevant to the other security champions in the company and discuss the best way to mitigate them. In addition, the motivation for the role will increase if the role is perceived as social and fun, instead of being a role where you get much responsibility and has to figure everything out alone.

Share Findings

Something mentioned as a key success of the security champions program in Visma is that findings are shared. Significant problems found have a high possibility of being relevant to the other security champions, and it is advantageous that those are shared. Creating a Slack channel for sharing significant problems and security news would be beneficial for the program and should be added as an extra step. This will not require any new

resources either. Possibly, findings could be announced over email too, but it is more organized to have it in a Slack channel.

Security Champion Information Hub

There are multiple mentions about documentation being hard to find and spread all over. It would be beneficial to create a hub where all the information relevant to the security champion could be gathered. Hopefully, this would also make it possible to automate parts of the program. Examples of things that could be collected in the hub are a list of all the available tools, recommendations, and assessments that have already been conducted (i.e., whether a third party application is safe to use), whom you can contact, and about what, training, resources, and Slack channels.

5.2.2 Evaluation of the Effectiveness of the Steps

The evaluation of the steps from the pre-study and the new steps are summarized in Table 5.1. Only one of the steps was unnecessary, namely preallocating time for security champion tasks.

Table 5.1: Summary of whether the steps have been proven to be effective and why.

ID	Step	Effective?	Why?
St1	Involve management and stakeholders	Yes	Need funding and support from the management to make the program happen.
St2	Define the role	Yes	Improves satisfaction with and understanding of the role.
St3	Assess security status	Unknown	Did not investigate.
St4	Recruit champions	Yes	Volunteers are more motivated and usually volunteer due to security interests.
St5	Training	Yes	Needed to better perform in the role and help to convince the team to focus on security.
St6	Set up communication channels	Yes	Effective for asking for help and learning from others.
St7	Ensure regular meetings	Yes	Motivating and helps create a community.
St8	Ensure necessary resources	Yes	Need tools to accomplish the work.

St9	Collect feedback	Yes	Motivating, effective for improving the program.
St10	Automate activities	Yes	Help the program scale when the companies grow.
St11	Pre-allocate time for champion tasks	No	No evident effects.
St12	Motivate the champion	Yes	Motivated by the other steps, but still relevant to have additional activities to increase motivation.
St13	Support from the security team	Yes	Important for getting help and increasing resource satisfaction.
St14	Measure results	Unknown	Did not investigate.
St15	Orientation	New	Need to introduce the role and relevant tasks and responsibilities.
St16	Onboarding	New	The security champions need some assistance to get started in the role.
St17	Mentoring	New	The security champions are missing someone they can ask specific question.
St18	Soft skills training	New	Soft skills training could be useful to learn how to communicate security issues to others and make them take it seriously.
St19	Flexible hours	New	The security champion needs to respond to security issues when they emerge.
St20	Create community feeling	New	Having a strong security champions community is beneficial for sharing knowledge and motivation.
St21	Share findings	New	Sharing findings is something that is spoken about as very useful.
St22	Security champion info hub	New	The security champions are missing a place where all relevant information is collected.

The complete suggestion for how to effectively establish and maintain a security champions program is presented in Table 5.2. The steps have been prioritized according to what are the most important steps and include recommendations for how the steps should be carried out.

Table 5.2: The final proposed approach for establishing a security champions program.

Steps	**Recommendations**
First Priority	
Involve management & stakeholders	Management and stakeholders need to ensure that the security champions and the rest of the team get enough time to work on security and that security is prioritized.
Define the role	Provide a clear role description, including responsibilities and main tasks.
Recruit champions	Make an effort to recruit as many volunteers as possible. Define the role clearly, and organize events to raise security interest.
Orientation	Provide a short introduction to the role, presenting role description, responsibilities, tasks, and resources for tools and support. It could, for example, be a short video or a web page.
Onboarding	Help the security champions onboard to the role by providing support to set up tools, basic security training, and an introduction to the community.
Mentoring	Ensure that the security champions can ask for help regarding specific issues. Does not need to be a mentor for each individual but, for example, Q&A sessions with the possibility to ask questions in private.
Flexible hours	Allow the security champions to work on security-related tasks when it is necessary.
Ensure community feeling	Help the champions meet and communicate to create a community feeling. It could be done by, i.e., arranging a local socializing event like a lunch.
Share findings	Ensure that significant findings are shared with all security champions.
Security training	The company should provide a plan for training. Self-study is efficient, but the company should assist on what topics are relevant. Occasionally arranging group training is also recommended because it facilitates socialization and learning from others.

Set up communication channels	Slack and email are recommended communication channels. Create a channel where security champions can ask and read questions and answers. Allow the champions to ask questions anonymously to lower the threshold for asking questions.
Ensure necessary resources	Provide resources but also tools and support for knowledge development. Be careful that the resources are well enough documented.
Support from the security team	The security team should be available for the champion to provide support and perform tests (i.e., pen-testing) on demand from the security champion.
Second Priority	
Ensure regular meetings	Regular meetings have been proven to increase motivation and community feeling. The meetings could be large meetings where security news is presented or internal meetings where the SEs can discuss local issues and develop knowledge together.
Security champion info hub	Gather all relevant information in one place.
Collect feedback	Collect feedback on the program occasionally to ensure improvements.
Automate activities	Orientation, and training could be automated if enough documentation is given. “Self-service” is also efficient.
Useful, not required	
Motivate the champion	It seems like the other steps are already motivating. However, it is never a bad thing to increase motivation even more. Socialization and increasing security interest are factors that could help increase motivation.
Soft skills training	Soft skills training should be available but in smaller quantities. If the company already offers project management courses, the champion could be offered to participate in these.
Need more research	
Assess security status	
Measure results	

5.3 Limitations

A common limitation with case studies is that they are perceived as lacking rigor and leading to generalization with poor credibility [18]. The case study in this project used a questionnaire and interviews as data collection methods. Because the questionnaire's answers are pre-defined, the respondent may not be able to express precisely what they mean, which is a limitation of the questionnaire. In addition, it is hard to check the truthfulness of the answers. Interviews are often unreliable because they only reflect what interviewees say, not necessarily what is true. Interviewees are aware they are being recorded, which may affect how they respond. Although neither of the researchers had conducted interviews before, we were able to obtain the information we needed and do not consider this a significant constraint. Our generalizations might be viewed as inaccurate because we only interviewed 11 people. However, we believe this is not a considerable limitation because the questionnaire results complement the results from the interviews.

As the questionnaire respondents and interviewees all volunteered to participate, the results might be biased. It is possible that those who volunteered are either extremely enthusiastic about the initiative or dislike it intensely, as those who do not have strong opinions might be indifferent to sharing their views. However, due to the number of respondents to our questionnaire and that the results do not have large discrepancies, we do not find this to be a big limitation for results. Another thing that could prevent the results from reflecting reality is that there seems to be some confusion between what activities belong to the VASP program and the actual SE role. When we created the questionnaire, we were unaware that the SEs did not have a clear understanding of the differences between the two. Therefore, the questionnaire results may be affected by this. In the interviews, we began the sessions by specifying the SE role and the scope that we were researching so this misunderstanding would not propagate in the second part of the results.

Some of the interviewees had a lot of security competence, and some even worked as a security engineer full-time. This does not fall within what is regarded as a standard security champion. This might have contributed to affecting the results towards a more positive view, as the more experienced security engineers seemed to meet fewer challenges. We also saw that some of the respondents of the questionnaire answered that they had "professional" security competence before starting in the role. However, this only applied to a couple of participants and should not significantly affect the results.

Even though we have participants from different companies, all the companies are within the Visma group. Because Visma has some standards, it is limited how differently the companies can carry out the security champions program. Furthermore, some research has already been done on security champions in Visma, which might affect the results.

Lastly, many of the questionnaire's findings are based on correlations between responses, which is a drawback because it is difficult to determine whether the associations are due to chance. However, t-tests were conducted to increase the confidence in these results.

5.4 Further Work

Even though this thesis creates a starting point for establishing a security champions program, there are still some challenges and uncertainties. Therefore further work is necessary.

Some of the things that should get more focus in further work are:

- Further work should investigate how the steps perform in other companies. Even though the research was carried out in different subsidiaries, they were still all under the command of Visma. It would be interesting to see if different companies perform the steps in the same way and if there are large discrepancies in how companies implement the security champions program. Visma is a big company, and it would also be interesting to see how the smaller companies implement the program and what challenges they face.
- There should be some more research on the details of the steps and how they are best carried out. Currently, the steps are on an overall level, and there are multiple ways each step could be carried out. For example, more attention should be paid to how to train champions and the most relevant topics, how to define the role, and how mentoring should be conducted.
- One thing that has not been investigated in this study is how the management and stakeholders are involved. It should be looked into what responsibilities the management and stakeholder should have, especially in bigger companies. It should be clarified which things should be organized at an organizational level and what should be organized at a local level.
- Due to time constraints, assessing security status and measuring results are two steps found in the literature review that this study has not investigated. In the companies we have investigated, we see that these steps are typically monitored by the security team, not the security champion. Therefore, it is unclear what role these steps should have in a security champions program. This needs further investigation.
- Lastly, the new steps should be further investigated to see if they have the desired effect.

Chapter 6

Conclusion

In this study, I have taken a deeper look at security champions and tried to fill some of the gaps in the literature.

Firstly, a pre-study was conducted to look into existing research. The pre-study concluded with a suggested approach for establishing a security champion program, further investigated in this thesis. By using a case study including a questionnaire and interviews, this study evaluated the steps formed in the pre-study and concluded whether they are, in fact, effective or not. In addition, challenges and areas of improvement were identified.

One limitation of the research is that all the companies under investigation underlay the same organization, Visma. In addition, case studies are known to produce generalizations with poor credibility. However, due to triangulation using both quantitative and qualitative methods, this is not a significant limitation to the results. Additionally, we got a satisfactory picture of the population. The primary limitation of the population is that some participants had higher security competence than what is typical for a standard security champion and therefore contributed to giving a more positive view of the situation. In addition, all the participants volunteered, which increases the possibility of receiving very positive or very negative views, as those who do not have strong opinions might be indifferent to sharing their views.

There was very little previous research on security champions. This study contributes to research by being one of the first studies to further investigate an approach for establishing and maintaining a security champions program. Further work should be conducted to gain more confidence in the results and develop the method further. The further work should include additional organizations and create a more detailed approach, in addition to looking into the steps from the pre-study that was not investigated in this thesis.

References

[1] Tyler W Thomas et al. 'Security during application development: An application security expert perspective'. In: *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 2018, pp. 1–12.

[2] Martin Gilje Jaatun and Daniela Soares Cruzes. 'Care and Feeding of Your Security Champion'. In: *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*. IEEE. 2021, pp. 1–7.

[3] Gunar Peterson. 'Collaboration in a secure development process part 1'. In: *Information security bull* 9 (2004), pp. 165–172.

[4] *How to Turn Developers Into Security Champions*. URL: https://www.veracode.com/sites/default/files/pdf/resources/ipapers/how-to-turn-developers-into-security-champions/index.html. (accessed: 06.05.2022).

[5] Julie Haney, Wayne Lutters and Jody Jacobs. 'Cybersecurity Advocates: Force Multipliers in Security Behavior Change'. In: *IEEE Security & Privacy* 19.4 (2021), pp. 54–59.

[6] Gary McGraw. 'Software security'. In: *IEEE Security & Privacy* 2.2 (2004), pp. 80–83.

[7] Olena V Sviatun et al. 'Combating cybercrime: economic and legal aspects'. In: *WSEAS Transactions on Business and Economics* 18 (2021), pp. 751–762.

[8] Hossein Keramati and Seyed-Hassan Mirian-Hosseinabadi. 'Integrating software development security activities with agile methodologies'. In: *2008 IEEE/ACS International Conference on Computer Systems and Applications*. IEEE. 2008, pp. 749–754.

[9] Steve Lipner. 'The trustworthy computing security development lifecycle'. In: *20th Annual Computer Security Applications Conference*. IEEE. 2004, pp. 2–13.

[10] JD Meier. 'Web application security engineering'. In: *IEEE Security & Privacy* 4.4 (2006), pp. 16–24.

[11] Haralambos Mouratidis, Paolo Giorgini and Gordon Manson. 'When security meets software engineering: a case of modelling secure information systems'. In: *Information Systems* 30.8 (2005), pp. 609–629.

[12] Laura Bell et al. *Agile Application Security: Enabling Security in a Continuous Delivery Pipeline.* " O'Reilly Media, Inc.", 2017.

[13] Jing Xie, Heather Richter Lipford and Bill Chu. 'Why do programmers make security errors?' In: *2011 IEEE symposium on visual languages and human-centric computing (VL/HCC).* IEEE. 2011, pp. 161–164.

[14] Moneer Alshaikh and Blair Adamson. 'From awareness to influence: Toward a model for improving employees' security behaviour'. In: *Personal and Ubiquitous Computing* 25.5 (2021), pp. 829–841.

[15] Trevor Gabriel and Steven Furnell. 'Selecting security champions'. In: *Computer Fraud & Security* 2011.8 (2011), pp. 8–12.

[16] Moneer Alshaikh. 'Developing cybersecurity culture to influence employee behavior: A practice perspective'. In: *Computers & Security* 98 (2020), p. 102003.

[17] Ken H Guo et al. 'Understanding nonmalicious security violations in the workplace: A composite behavior model'. In: *Journal of management information systems* 28.2 (2011), pp. 203–236.

[18] Briony J Oates, Marie Griffiths and Rachel McLean. *Researching information systems and computing.* Sage, 2022.

[19] *Collection of personal data for research projects.* URL: https://i.ntnu.no/wiki/-/wiki/English/Collection+of+personal+data+for+research+projects. (accessed: 14.01.2022).

[20] *History: The Agile Manifesto.* URL: https://www.agilealliance.org/agile101/.

[21] Hela Oueslati, Mohammad Masudur Rahman and Lotfi ben Othmane. 'Literature review of the challenges of developing secure software using the agile approach'. In: *2015 10th International Conference on Availability, Reliability and Security.* IEEE. 2015, pp. 540–547.

[22] Andreas Poller et al. 'Can security become a routine? A study of organizational change in an agile software development group'. In: *Proceedings of the 2017 ACM conference on computer supported cooperative work and social computing.* 2017, pp. 2489–2503.

[23] Amber van der Heijden, Cosmin Broasca and Alexander Serebrenik. 'An empirical perspective on security challenges in large-scale agile software development'. In: *Proceedings of the 12th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement.* 2018, pp. 1–4.

[24] Imran Ghani, Zulkarnain Azham and Seung Ryul Jeong. 'Integrating software security into agile-Scrum method'. In: *KSII Transactions on Internet and Information Systems (TIIS)* 8.2 (2014), pp. 646–663.

[25] Ita Ryan, Utz Roedig and Klaas-Jan Stol. 'Understanding developer security archetypes'. In: *2021 IEEE/ACM 2nd International Workshop on Engineering and Cybersecurity of Critical Systems (EnCyCriS).* IEEE. 2021, pp. 37–40.

[26] Julie M Haney and Wayne G Lutters. 'The work of cybersecurity advocates'. In: *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems.* 2017, pp. 1663–1670.

[27] Barbara Kitchenham. 'Procedures for performing systematic reviews'. In: *Keele, UK, Keele University* 33.2004 (2004), pp. 1–26.

[28] Christopher M Shea. 'A conceptual model to guide research on the activities and effects of innovation champions'. In: *Implementation Research and Practice* 2 (2021).

[29] Irene Okere, Johan Van Niekerk and Mariana Carroll. 'Assessing information security culture: A critical analysis of current approaches'. In: *2012 Information Security for South Africa*. IEEE. 2012, pp. 1–8.

[30] Johan Van Niekerk and Rossouw Von Solms. 'A holistic framework for the fostering of an information security sub-culture in organizations.' In: *Issa*. Vol. 1. 13. 2005.

[31] Hege Aalvik. 'Establishing a Security Champions Program: A Literature Review'. Dec. 2021. URL: https://studntnu-my.sharepoint.com/:b:/g/personal/hegeaal_ntnu_no/ERF-PeqpJj1AIPXUqwiECm0BP9WN-OeGqdHpov-pmvYHow?e=3ywbqE.

[32] *Who We Are*. URL: https://www.visma.com/organisation/. (accessed: 17.03.2022).

[33] *VASP VCDM*. URL: https://www.visma.com/trust-centre/security/vasp-vcdm/. (accessed: 17.03.2022).

[34] Daniela Soares Cruzes and Espen Agnalt Johansen. 'Building an ambidextrous software security initiative'. In: *Balancing Agile and Disciplined Engineering and Management Approaches for IT Services and Software Products*. IGI Global, 2021, pp. 167–188.

[35] *Jamk University of Applied Sciences*. URL: https://www.jamk.fi/en. (accessed: 04.05.2022).

[36] Per Runeson and Martin Höst. 'Guidelines for conducting and reporting case study research in software engineering'. In: *Empirical software engineering* 14.2 (2009), pp. 131–164.

[37] Colin Robson and Kieran McCartan. *Real world research: a resource for users of social research methods in applied settings*. Wiley, 2016.

[38] *Sample Size Calculator*. URL: https://www.surveysystem.com/sscalc.htm. (accessed: 14.01.2022).

[39] Rensis Likert. 'A technique for the measurement of attitudes.' In: *Archives of psychology* (1932).

[40] *Graphpad T test calculator*. URL: https://www.graphpad.com/quickcalcs/ttest1/?format=C. (accessed: 14.01.2022).

[41] *MaxQDA*. URL: https://www.maxqda.com. (accessed: 30.04.2022).

[42] *Slack*. URL: https://slack.com. (accessed: 03.05.2022).

[43] *Slack Analytics Dashboard*. URL: https://slack.com/help/articles/218407447-View-your-Slack-analytics-dashboard. (accessed: 03.05.2022).

[44] *Coverity Scan - Static Analysis*. URL: https://scan.coverity.com. (accessed: 27.04.2022).

[45] *OWASP Top Ten*. URL: https://owasp.org/www-project-top-ten/. (accessed: 29.04.2022).

[46] *Secure Code Warrior*. URL: https://www.securecodewarrior.com. (accessed: 29.04.2022).

[47] *Pluralsight*. URL: https://www.pluralsight.com. (accessed: 27.04.2022).

[48] *TryHackMe*. URL: https://tryhackme.com. (accessed: 29.04.2022).

[49] *HackTheBox*. URL: https://www.hackthebox.com. (accessed: 29.04.2022).

[50] *Orientation*. URL: https://www.dictionary.com/browse/orientation. (accessed: 18.05.2022).

[51] *Onboarding*. URL: https://dictionary.cambridge.org/dictionary/english/onboarding. (accessed: 18.05.2022).

[52] Jane M Howell. 'The right stuff: Identifying and developing effective champions of innovation'. In: *Academy of Management Perspectives* 19.2 (2005), pp. 108–119.

Appendix A

Data Management Plan

Effektive Security Champions i Smidige Teams

Programvaresikkerhet er viktigere enn noen gang, og samtidig tar smidige utviklingsmetoder over som den foretrukne måten å utvikle programvare på. På grunn av omfavnende kravendring og hyppige leveranser under utvikling, gjør de smidige metodene det utfordrende å lage sikker programvare . I tillegg mangler utviklere ofte sikkerhetsopplæring og -forståelse, noe som resulterer i at utviklere ikke tar de nødvendige skritt for å forhindre sårbarheter i kildekoden. En security champion er et medlem av utviklingsteamet som tar til orde for sikkerhet. Å ha en security champion i et utviklingsteam har vist seg å være en effektiv strategi for å skape en bedre sikkerhetskultur i teamet og dermed sikrere programvare. Målet med dette forskningsprosjektet er å finne den mest effektive måten å etablere og vedlikeholde et security champions program i en bedrift med smidige teams.

Fagområder

Teknologi

Forskningsansvarlig institusjon

Norges teknisk-naturvitenskapelige universitet / Fakultet for informasjonsteknologi og elektroteknikk (IE) / Institutt for datateknologi og informatikk

Prosjektvarighet

14.01.2022 — 31.12.2022

Formål

Forskningsspørsmål: RQ1: Hvordan er secuirty champions programmer implementert i agile programvare prosjekt? RQ2: Hva er utfordringene og forbedringene som kan bli gjort når man implementerer et secuirty champions program? RQ3: Hva er en effektiv måte å etablere og vedlikeholde et secuirty champions program i en smidig kontekst?

Nytteverdi

Programvaresikkerhet i agile teams.

Etiske retningslinjer

- Generelle forskningsetiske retningslinjer
- Naturvitenskap og teknologi

Opphavs- og eiendomsrett

Norges teknisk-naturvitenskaplige universitet

Intervju

Beskrivelse

Lydfiler og transkripsjoner av intervju

Datatype

Lyd, Tekst

Språk

Engelsk

Nøkkelord

Security Champions

Data om personer

Ja

Er det noen andre grunner til at dataene dine trenger ekstra beskyttelse?

Nei

Kategorier av personopplysninger

Alminnelige

Utvalgets størrelse

80

Konfidensialitetsklassifisering

Intern

Innsamlingsperiode

15.02.2022 — 27.05.2022

Innsamlingsenheter

- 1. NTNU Zoom
- 2. NTNU Microsoft Teams
- 6. Annen innsamlingsmåte

Datakvalitet

Standarisert intervjuprotokoll og kvalitetsikre utstyr som bruker til lydopptak og transkribering

Metode

Intervju, Transkripsjon

Beskrivelse

Intervju som vil bli transkribert.

Størrelse

10000 MB

Format

txt, mp4

Programvare

MaxQDA

Navnekonvensjoner

Filene vil bli lagret med dato og et nummer tilsvarende kronologisk rekkefølge på når intervjuene ble gjennomført. Formatet vil se slik ut: #x - dd.mm.yy

Lagring

- 05. NTNU Office 365 (SharePoint, Teams, Onedrive)

Overføring

- 2. Office 365 (SharePoint, Teams, Onedrive)

Arkivering

Nei

Spørreundersøkelse

Datatype

Datasett

Språk

Engelsk

Nøkkelord

Security Champion

Data om personer

Ja

Er det noen andre grunner til at dataene dine trenger ekstra beskyttelse?

Nei

Kategorier av personopplysninger

Anonyme

Utvalgets størrelse

73

Konfidensialitetsklassifisering

Intern

Innsamlingsperiode

01.02.2022 — 20.02.2022

Innsamlingsenheter

- 6. Annen innsamlingsmåte

Datakvalitet

Google forms vil bli brukt som elektronisk spørreskjema. Skjemaene vil bli brukt via Visma der intervju-objektene jobber. Dette sikrer ekstra sikkerhet. Systemene vil dog være interne. Standariserte metoder.

Metode

Selvadministrerende spørreskjema

Størrelse

1000 MB

Format

csv

Programvare

Excel, PowerBI

Navnekonvensjoner

Data fra spørreundersøkelser vil bli lagret i en felles fil. Denne vil bli plassert i mappe, og lagret med filnavn på formatet dd.mm.yy - versjon x

Lagring

- 05. NTNU Office 365 (SharePoint, Teams, Onedrive)

Overføring

- 2. Office 365 (SharePoint, Teams, Onedrive)

Arkivering

Nei

Appendix B

Oral Consent Form for the Interviews

Before beginning the interviews, the participants were informed of their rights and asked if they consented to the use of their personal data. Transcripts of the interviews, including the consent, were sent to participants after the interviews. As a result, they also received their rights in writing. The oral consent form read as follows:

The purpose of the data processing, in this case, is to research the current security engineer program and the onboarding of the new security engineers. The results will be used in two master theses which will be published later this year. We process your personal information like name and work email address and the questions related to your security engineer career and role. We will store the data, the recording, and the interview transcript. We will use a program called MaxQDA to analyze the transcript and will not be saving any personal data in that tool. Furthermore, evidently, we use Microsoft Teams for the interview, so this also processed the data. Both our supervisors can access the data. Concerning the final publications, they will not contain any personal data. We will delete the data at the end of June 2022. You will have access to the recording of this interview and the transcript that is made based on it. The transcript will be shared with you when we have corrected the automatically generated transcript from Microsoft Teams, and you have the right to make adjustments. You also have the right to delete the data earlier. If you have some complaints about how we process your data, you can send complaints to Thomas Helgesen, the privacy representative at the Norwegian University of Technology and Science. I will put his email in the chat. You also have the right to withdraw your consent. Based on these things, will you give us your consent to process your data?

Appendix C

Papers Found in the Pre-study

Table C.1: Papers found during the literature review in the pre-study.

Study	Authors	Title	SLR	Security	Actions
S1	M. Jaatun and D. Cruzes (2021) [2]	Care and Feeding for Your Secuirty Champion	Yes	Yes	Yes
S2	M. Alshaikh (2020) [16]	Developing cybersecurity culture to influence employee behavior: A practice perspective	Yes	Yes	Yes
S3	M. Alshaikh and B. Adamson (2021) [14]	From awareness to influence: toward a model for improving employees' security behaviour	Yes	Yes	Yes
S4	J. Haney and W. Lutters (2017) [26]	The Work of Cybersecurity Advocates	Yes	Yes	No
S5	J. Haney, W. Lutters and J. Jacobs (2021) [5]	Cybersecurity Advocates: Force Multipliers in Security Behavior Change	Yes	Yes	No
S6	T. W. Thomas, M. Tabassum, B. Chu and H. Lipford (2018) [1]	Security During Application Development: an Application Security Expert Perspective	Yes	Yes	No
S7	I. Ryan, U. Roedig and K. J. Stol (2021) [25]	Understanding Developer Security Archetypes	Yes	Yes	No
S8	I. Okere, J. van Niekerk and M. Carroll (2012) [29]	Assessing Information Security Culture: A Critical Analysis of Current Approaches	No	Yes	Yes
S9	J. van Niekerk, R. von Solms (2005) [30]	An holistic framework for the fostering of an information security sub-culture in organizations	No	Yes	Yes
S10	J.M. Howell (2005) [52]	The right stuff: Identifying and developing effective champions of innovation	No	No	Yes
S11	C.M. Shea (2021) [28]	A conceptual model to guide research on the activities and effects of innovation champions	No	No	Yes

Appendix D

Summary of the Claims Used in the Questionnaire

Table D.1: Some of the claims used in the questionnaire.

ID	Claim
C1	There is a clear onboarding process for new Security Engineers in Visma.
C2	I am satisfied with the orientation that I have received as a new Security Engineer.
C3	I am satisfied with the security training I have received as a new Security Engineer.
C4	I am satisfied with the soft skills training (e.g. Communication).
C5	I am satisfied with my performance as a Security Engineer.
C6	I feel motivated to work as a Security Engineer.
C7	I do not have role conflicts with the Security Engineer role and my other roles.

Appendix E

Electronic Questionnaire

The questionnaire is here presented in text format rather than the original Google-form version to make it more compact.

Security Engineer program improvement

We are seeking to improve the current Security Engineer program and Your contribution is important. The survey has five sections with questions regarding your role as a Security Engineer. All answers are completely anonymous. Survey data will be removed in the end of 2022. If you have any questions about the survey, please contact me (xxxx.xxxx@xxxx.xxxx).
Please submit your response before 15/02/2022.

Background information

Q1. I have been a Security Engineer for *

- less than 1 year
- 1-2 years
- more than 2 years

Q2. I would describe my cyber security competence before starting as Security Engineer as *

- Beginner or no previous experience
- Intermediate
- Professional

Q3. My main role in Visma in addition to the Security Engineer role is *

- Developer
- Tester / Quality Assurance Specialist
- Architect
- Other:

Becoming a Security Engineer

Q4. I became a Security Engineer because *

- Someone appointed me to the role
- I volunteered to the role myself

Q5. Please answer to the following propositions. *
Options for each proposition:
Strongly agree — Agree — Neutral — Disagree — Strongly disagree — N/A

- I was given a realistic view what was expected from me as a Security Engineer during the recruitment
- I do not have role conflicts with the Security Engineer role and my other roles
- I am satisfied with the orientation that I have received as a new Security Engineer
- I am satisfied with my performance as a Security Engineer

Q6. Please answer to the following propositions. *
Options for answers: Yes — No — N/A

- I have pre-allocated hours to work on Security Engineer tasks
- I was given formal orientation about the Security Engineer role
- I was given formal orientation about the Visma Application Security Program
- I have had a mentor during the onboarding to the Security Engineer role

Collaboration and training

Q7. I am familiar with the following coaching support activities that the Visma Security Team provides to Security Engineers *

- The Security Engineer Guild and its meetings
- Security awareness meetings

- Security Engineer Guild Slack channel
- Direct contact with Security Team members
- Secure Code Warrior
- None (If this is selected be sure not to select other options)

Q8. I communicate with other Security Engineers via *

- Email
- Slack
- Teams
- Telephone
- Talking at the office
- I do not communicate with other Security Engineers (If this is selected be sure not to select other options)
- Other:

Q9. Please answer to the following propositions concerning the coaching and support available for the new Security Engineers. *
Options for each proposition:
Strongly agree — Agree — Neutral — Disagree — Strongly disagree — N/A

- There are enough written guidelines available related to the onboarding (e.g. about Visma Application Security Program)
- I am satisfied with the security training I have received as a new Security Engineer
- I am satisfied with the soft skills training (e.g. Communication)
- I have received as a new Security Engineer
- I find the security guild meetings useful
- The available support tools channels are effective tools for information sharing and raising awareness
- I get support quickly from the Security Team for Security Engineer tasks
- I feel being a part of a special community as a member of the Security Engineer guild
- I am, in general, happy with the provided resources to help me in my role as a Security Engineer

Feedback

Q10. Please answer to the following propositions concerning RECEIVING feedback as a Security Engineer. *
Options for answers: Yes — No — N/A

- I've been informed how I perform as a Security Engineer
- I am satisfied with the amount of feedback that I received

Q11. Please answer to the following propositions concerning GIVING feedback as a Security Engineer. * Options for answers: Yes — No — N/A

- I am asked for my opinions on the Security Engineer program
- I know where to turn to share opinions on the security engineer program, i.e., suggestions for improvement
- I can share my opinions on the security program anonymously

Conclusions and improvements

Q12.Please answer to the following propositions concerning working in the Security Engineer role. *
Options for each proposition:
Strongly agree — Agree — Neutral — Disagree — Strongly disagree — N/A

- There is a clear onboarding process for new Security Engineers in Visma
- The onboarding process has made me feel more efficient in the Security Engineer role
- The onboarding process has made me feel more confident in the Security Engineer role
- Onboarding has helped me understand why Security Engineers are needed in Visma
- I feel motivated to work as a Security Engineer

Q13. I would improve the following onboarding process functions (max two options) *

- Recruitment
- Orientation
- Training
- Support Tools and processes

- Coaching and support
- Feedback

Q14. I would improve the following functions of the whole Security Engineer program (max two options) *

- Recruitment
- Onboarding
- Communication
- Resources
- Training
- Monitoring/follow-up
- Motivation
- Other:

Q15. I think that the following parts of the Security Engineer program could be automated *

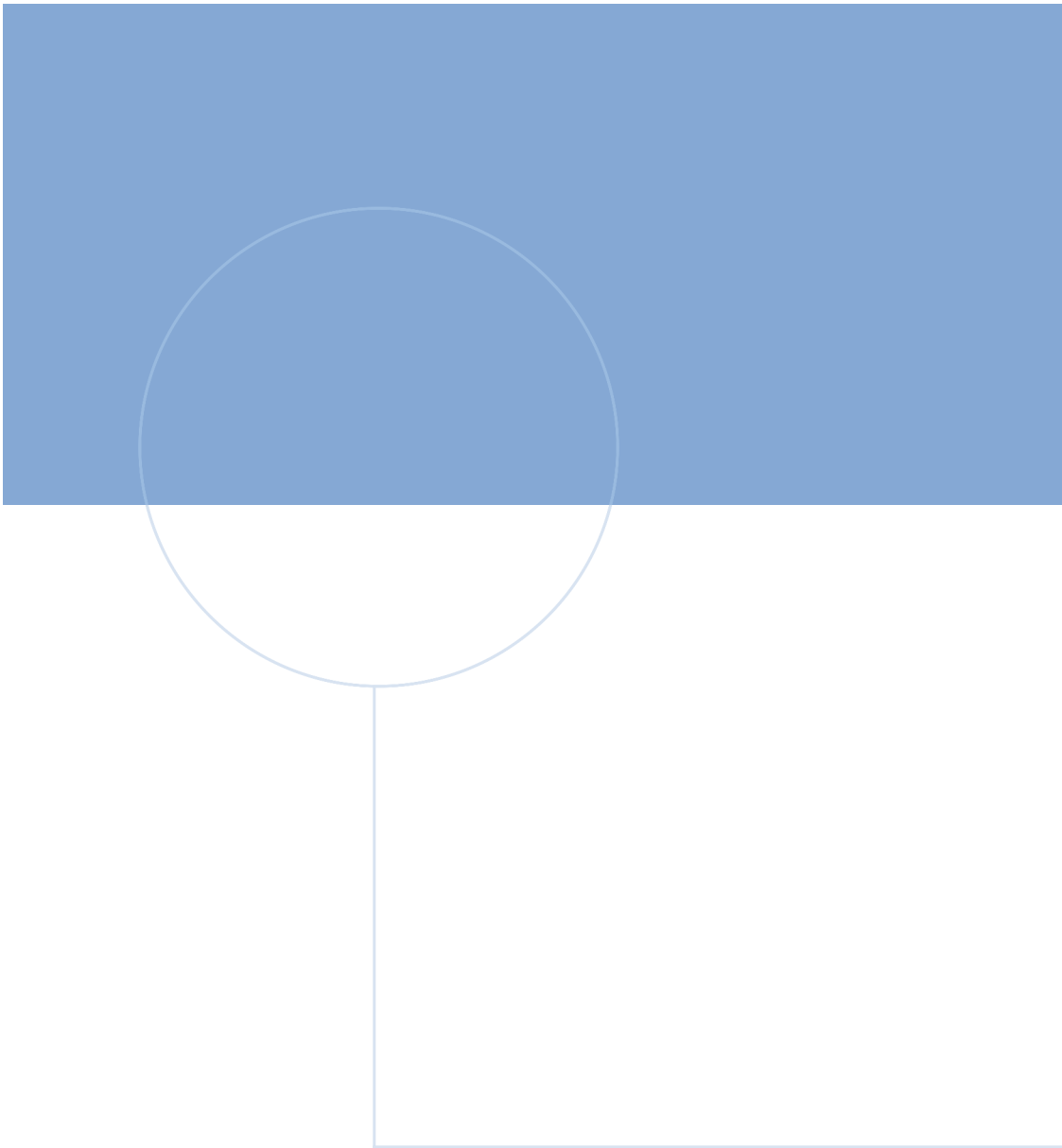
- Recruitment
- Onboarding
- Training
- Feedback
- I don't think that the parts can be automated (If this is selected be sure not to select other options)
- Other:

Appendix F

Interview Guide

ID	Question	Reason
General questions		
I1	What is your main role in Visma?	
I2	For how long have you been a SE?	
I3	How were you recruited to the SE role? Volunteered or appointed? If volunteered: What made you volunteer to the SE role?	Background info on the SE.
I4	How much time do you usually spend on SE tasks (weekly)?	
I5	Can you describe what kind of tasks you do as a SE?	
I6	How do you fit your SE role into your daily activities?	
I7	How to you prioritize your tasks? Do you prioritize working on your everyday tasks before your SE tasks? Do you procrastinate your SE tasks more than your other tasks?	There is a slight difference in satisfaction with own performance between volunteers and appointed. Does this indicate that volunteers do a better job?
Orientation		
I8	Did You receive any orientation on how to do your work as a Security Engineer? Follow-up: Was it enough? What would you do otherwise?	
Training		
I9	What was your security competence before starting as a SE?	
I10	When you started as a security engineer, did you receive any training to prepare you for the role? Was it good or bad? Why was it good or bad? Did you receive any soft-skills training? Follow up: What do you think would be useful to learn instead?	Results from the survey show that people are unhappy with the training. What is the problem?

I11	And now that you have worked as SE for a while, have you received any additional training? What do you think about it?	Survey results show that the more experience and seniority, the more unhappy with the training.
Coaching and Support Tools		
I12	What do you think about the coaching and support tools (Guild and its meetings, Guild slack channel, Security team support, Security awareness meetings)?	Coaching and support tool were the the third functions that Security engineers would want to improve. What is missing?
I13	Is there something you would want to change in the current activities or add something else to improve the situation?	
Communication		
I14	While continuing to work as a SE, do you have much communication with other SEs? About what? Do you ever reach out to more experienced SEs for advice? Do other SE reach out to you for advice?	12,3% of SE does not communicate with other SEs. It is primarily those who have been a SE for more than two years that do not communicate. Why not? It would be beneficial if they could offer guidance and advice to the SEs with less experience.
I15	Do you participate in internal SE meetings (not security guild meetings, but internal for your legal unit/company). Do you find these meetings useful? Why? If not: Is this something you would like to have?	Is it beneficial to have more intimate meetings between the SEs in one legal unit?
Summary		
I16	What do you think is the key to success for the SE program in Visma? What is the best thing about the program? Are there any parts of the program you would recommend to another company starting a program like this? I.e. the guild meetings, some resource, something that has been essential/important for you in your role. Is there anything you do not like about the program?	Check if there are other useful steps that I did not find in the literature review. In the end: What would you improve? What do you think? What would you do differently.
I17	Is there something that You would like change to make the whole onboarding process more efficient?	



NTNU

Kunnskap for en bedre verden