



Applying onboarding theory on the security champion program

Matti Paavilainen

Master's thesis

May 2022

Information and Communications Technology

Master's Degree Programme in Information Technology

Cyber Security

Paavilainen, Matti

Applying onboarding theory on the security champion program

Jyväskylä: JAMK University of Applied Sciences, May 2022, 104 pages

Master's Degree Programme in Information Technology, Cyber Security, Master's thesis

Permission for open access publication: Yes

Language of publication: English

Abstract

As the technology evolves and societies are more and more using different cloud SaaS (Software as a Service) through the Internet. At the same time cyber domain has evolved too and the amount of malicious activity has risen and brought more cyber threats that are targeting the services found on the Internet.

This has effects on the SaaS service development where we have seen different Secure Software Development Life Cycle (S-SDLC) frameworks that are used to implement built-in security in the services instead of reactively add security on top of the services. At the same time, we have seen the emergence of the so-called security champions which are key players when thinking the implementation of the security in the development life cycle phases. As all new employees or employees who change their roles in their organization, also the security champions need to be onboarded to that role to give them enough confidence and knowledge related to their new role as usually they do not have a strong cyber security background.

The onboarding process of new employees and the things that affect how successful the onboarding is or what kind of results the onboarding produces has been researched for a long time. One onboarding process theory was used to research the onboarding of new security champions in a large European SaaS service provider. The company uses a S-SDLC and one part of that program is the assignment of a security champion for each service that is onboarded to the S-SDLC program. The research included a survey and semi-structured interviews, and the results provide more information about what things are functioning in the onboarding process and what could be done better. Based on the results there are suggestions that might be helpful for other organizations that are running a security champion program.

Keywords/tags (subjects)

security champion, onboarding process, security program

Miscellaneous (Confidential information)

The transcriptions of interviews and the detailed survey results are confidential material that will not be published with the thesis.

Paavilainen, Matti

Perehdyttämisprosessin hyödyntäminen security champion -ohjelmassa

Jyväskylä: Jyväskylän ammattikorkeakoulu, toukokuu 2022, 104 sivua

Tietojenkäsittely ja tietoliikenne, tekniikan ylempi ammattikorkeakoulututkinto, YAMK-opinnäytetyö

Verkkojulkaisulupa myönnetty: Kyllä

Julkaisun kieli: Englanti

Tiivistelmä

Teknologian kehittyessä yhteiskunnat käyttävät yhä enemmän erilaisia pilvi SaaS-palveluita (Software as a Service) Internetin kautta. Samaan aikaan myös kyberdomain on kehittynyt ja haitallisen toiminnan määrä on kasvanut ja tuonut lisää kyberuhkia, jotka kohdistuvat Internetistä löytyviin palveluihin.

Tämä vaikuttaa SaaS-palvelukehitykseen, jossa olemme nähneet erilaisia tietoturvallisen sovelluskehityksen (Secure Software Development Life Cycle) -viitekehyksiä, joita käytetään sisäänrakennetun tietoturvan toteuttamiseen ohjelmistoihin ja palveluihin sen sijaan, että tietoturvaa lisätään reaktiivisesti palveluihin jälkikäteen. Samalla olemme nähneet ns. security championien esiinmarssin. Security championit ovat keskeisiä toimijoita, kun ajatellaan tietoturvan toteutusta sovellusten kehityksen elinkaaren eri vaiheissa. Kuten kaikki uudet työntekijät tai työntekijät, jotka vaihtavat roolejaan organisaatiossaan, myös uudet security championit on ajettava sisään uusiin tehtäviinsä perehdytysprosessin kautta, jotta heille luodaan riittävät edellytykset toimia uudessa roolissaan. Security championit eivät myöskään usein omaa vahvaa kyberturvallisuustuntemusta aloittaessaan kyseisessä roolissa.

Yleisesti voidaan sanoa, että uusien työntekijöiden perehdytysprosessia ja niitä asioita, jotka vaikuttavat perehdyttämisen onnistumiseen tai millaisia tuloksia perehdytys tuottaa, on tutkittu pitkään. Yhtä perehdytysprosessin teoriaa käytettiin tutkittaessa uusien security championien käyttöönottoa suuressa eurooppalaisessa SaaS palveluita tarjoavassa yrityksessä. Yritys hyödyntää tietoturvallista sovelluskehityksen viitekehystä ja yksi sen osa-alue on security championin nimeäminen ja perehdyttäminen jokaiselle ohjelmaan kuuluvalla palvelulle tai ohjelmistolle. Tutkimus toteutettiin kyselyn ja teemahaastatteluiden kautta ja tulokset antavat enemmän tietoa siitä, mitkä asiat perehdytysprosessissa toimivat ja mitä voisi tehdä paremmin. Tulosten perusteella tehdään suosituksia perehdytysohjelman kehittämiseksi. Suositukset voivat olla hyödyllisiä myös muille organisaatioille, jotka hyödyntävät security championia omassa toiminnassaan.

Avainsanat (asiasanat)

security champion, onboarding process, security program

Muut tiedot

Teemahaastattelujen litteroinnit ja kyselytutkimuksen yksityiskohtaiset vastaukset ovat salassa pidettävää tietoa, eikä niitä julkaista tämän opinnäytetyön julkaisun yhteydessä.

Contents

1	Introduction	5
1.1	About Visma group.....	6
1.2	Research questions in this thesis	7
1.3	Used research methodologies	8
2	Previous studies of onboarding	10
3	Theoretical background	12
3.1	Security champions	12
3.1.1	Security champions in Visma	14
3.2	Onboarding process theories	15
3.2.1	Theory on organizational socialization tactics.....	16
3.2.2	The research-based theory made by Bauer	17
3.3	Software development life cycle, SDLC.....	20
3.3.1	Software engineering and the “software crisis”	20
3.3.2	Software development life cycle models	23
3.3.3	Waterfall	24
3.3.4	Spiral	25
3.3.5	Agile development process	27
3.4	Secure Software Development Life Cycle, S-SDLC	28
3.5	Secure SDLC framework used in Visma group	30
3.5.1	Product security catalog	32
3.5.2	Security engineer	33
3.5.3	Security Self-Assessment	33
3.5.4	Static Application Security Testing service, SAST	36
3.5.5	Automated Third-party Vulnerability Service, ATVS	37
3.5.6	Dynamic Application Security Testing, DAST	37
3.5.7	Penetration Testing	38
3.5.8	Cyber Threat Intelligence Service	39
3.5.9	Security Log Management	39
3.5.10	Bug Bounty Program.....	40
3.5.11	Measuring security maturity	41
4	Survey analysis	43
4.1	Survey population	43
4.2	Survey instrumentation.....	43
4.3	Reliability of the research	47

4.4	Data analysis.....	49
4.4.1	Selection of the security engineers	50
4.4.2	Self-efficacy of the security engineers.....	53
4.4.3	Role clarity analysis.....	57
4.4.4	Social Integration	64
4.4.5	Knowledge of the culture	67
4.4.6	Analysis of the general improvement questions.....	70
4.4.7	Summary of the survey results	73
5	Interview results analysis.....	74
5.1	Results concerning orientation	75
5.2	Thoughts on training	76
5.3	General improvement of the onboarding process	78
5.4	Other findings.....	78
6	Successful onboarding or not?	79
6.1	Selection	79
6.2	Self-efficacy	79
6.3	Role clarity.....	80
6.4	Social integration.....	81
6.5	Knowledge of culture	82
7	Discussion.....	83
7.1	Research questions	86
7.2	Reflections with previous studies	87
7.3	Ideas for further investigation	88
8	Conclusion.....	88
	References.....	90
	Appendices	93
	Appendix 1. Security engineer survey structure and questions	93
	Appendix 2. Interview guide	98
	Appendix 3. Consent form for processing personal data	100

Figures

Figure 1. Functions and attributes based on the Bauer (2010) model.....	20
Figure 2. The software development phases as Winston Royce (1970) presented them.....	22
Figure 3. SDLC phases and life cycle	24
Figure 4. The original diagram of the spiral development model (Boehm, 1988)	26
Figure 5. The definition of the Scrum framework (Scrum Alliance, 2020).	28
Figure 6. Product details of the Wintime product from Visma Trust Centre	32
Figure 7. Cyber security topics included in the SSA.....	34
Figure 8. SSA questions related to the access controls of the service	35
Figure 9. Visma group bug bounty program details at Initigrity	41
Figure 10. A view on the security maturity index product page	42
Figure 11. Multiple choice question type settings.....	44
Figure 12. Multiple-choice grid question type settings.	44
Figure 13. Checkboxes question type settings.....	45
Figure 14. The initial message from 1st of Feb about the survey.....	46
Figure 15. A reminder with some information of responses this far (17th of Feb).....	47
Figure 16. Sample size formula (Creative Research Systems, 2012)	48
Figure 17 . Confidence Interval calculation.	49
Figure 18. Levers that affect how successful the onboarding process is.	49
Figure 19. How long security engineers had been working in the role.....	50
Figure 20. Previous security competence of the security engineers.....	51
Figure 21. Correlation of how person was assigned to security engineer and how motivated they feel working as security engineers.....	53
Figure 22. Results of the self-efficacy related questions.....	54
Figure 23. Correlation between mentoring and how onboarding process affected to the confidence and efficiency of the security engineers.	56
Figure 24. Correlation of previous security experience and how satisfied security engineers are with the training that they have received during the onboarding process.....	57
Figure 25. How pre-allocated hours affected to having role conflicts between security engineer role and other roles.	58
Figure 26. Results from Likert scale questions related to the role clarity.....	59
Figure 27. Does the length of the SE career affect how realistic the given view of security engineer role is being considered?	60
Figure 28. Correlation of previous experience and how realistic view of security engineer role was given during onboarding.....	61

Figure 29. How satisfied the security engineers were to orientation if they had received formal orientation about the role.	62
Figure 30. How satisfied the security engineers were to orientation if they had received formal orientation about the Visma Application Security Program.....	63
Figure 31 Security engineers' satisfaction to received feedback	64
Figure 32. How well the security engineers know the different coaching & support activities.	65
Figure 33. How security engineers communicate with others.	66
Figure 34 Social integrarion related propositions with Likert scale	67
Figure 35. Did the onboarding help to understand why security engineers are needed in Visma?	68
Figure 36. Correlation between mentoring and do the security engineers understand why they are needed in Visma.....	68
Figure 37 Do security engineers know where they can share their opinions on the security engineer program	69
Figure 38 Are security engineers asked for their opinions on the security engineer program..	70
Figure 39. Security engineers would like to improve the following onboarding process functions.	71
Figure 40. Is the onboarding process for new security engineers clear in Visma.	73
Figure 41. Overall onboarding process status.	79

Tables

Table 1. Response types and dimensions and tactics.....	17
Table 2. How Jones grouped the socialization tactics under institutionalized and individual tactics	17
Table 3. The frequencies of the main roles of the respondents.....	52
Table 4 Crosstab of satisfaction to feedback and how long person had been a security engineer	64
Table 5. Crosstabulation between the onboarding function that needs improvement vs. security engineer experience.	71
Table 6. Crosstabulation between the onboarding function that needs improvement vs. previous security experience before starring as a security engineer.	72

1 Introduction

Throughout human history there have been legends and fairytales about champions who, e.g., single-handedly defeated an overwhelming enemy or did some other miraculous things. Today this is also seen in the current tense geopolitical situation where there have been stories of war heroes like the “Ghost of Kyiv” who was rumored to take down over 40 Russian jet fighters. The Ukrainian government released later official information about the identity of the person behind the myth as just war propaganda to boost the morale of the people waging war. So, it seems that there is a need for heroes or champions, and we like to hear stories about them.

In the same time information systems and technology like mobile and cloud computing have developed fast in the 20th century and the playfield of the enterprises and organizations that are players in the information technology sector has been under constant change. We could even call this as the era of cloud computing as more and more organizations as well individuals utilize cloud services over the internet instead of producing the services with their own IT infrastructure and platforms.

As a result, the malicious activity in the cyber domain has been increasing as in that domain there is a lot of attack surface for those parties who want to benefit from it. We see more and more ransomware and supply chain attacks and even attacks that have effects in the physical world. We see more activity from state sector supported Advanced Persistent Groups or APTs as well not so sophisticated threat actors like Lapsus\$, which one leader was just a 16-year-old kid but still managed to gather about 14 million dollars with extortion and hacking. So as the threat landscape has evolved there is a need to have heroes in the blue teams too, and to fill that gap, we are now seeing the emergence of so-called security champions.

As even champions or at least newly hired champions might need assistance and guidance to get themselves efficient and confident in what they are supposed to do, an onboarding process for new security champions is needed. This thesis was assigned by the Visma Group, which is one of the leading cloud service providers in Europe. Thesis is examining how the security champions are onboarded to the Visma security champion program and could existing new employee onboarding theories bring ideas or suggestions to the onboarding process of the new security champions used

in Visma to make them even more confident and efficient in their new role. In general, well-functioning onboarding process can have various positive short-term and long-term effects e.g., on the motivation and commitment of the newcomers.

1.1 About Visma group

Visma group was founded in 1996 in Norway. In the 1990s Visma even had a Marine Division. Øystein Moan was named as Visma CEO in 1997 and Visma group had 400 employees at the end of 1999. The Marine division was sold in the year 2000 which proved Visma a solid economic basis for the company. In the 2000s Visma's growth was substantial as it acquired more companies under its wings, and it also invested in organic growth. At the end of 2000s Visma had 10 000 SaaS users and had already almost ten times more employees than at the end of 1990s. Visma has also become a one of the key software companies in the Nordics and Visma also has a foothold in the Netherlands with an acquisition. (Visma group a.)

In the 2010s Visma put more effort into the cloud business and grew both organically and with acquisitions. As an example, Visma bought Huldt & Lillevik, Aditro Public Sweden, Bluegarden and Raet as well as many other companies. At the end of 2010s Visma group had 11 175 employees and it had a very firm grip in the European market as a provider of SaaS services to companies and public organizations. Visma group had expanded its operations to also Hungary, Latvia, and Poland. (Visma group a.)

Visma offers a wide range of software mainly as SaaS services to its customers. In their offerings Visma group emphasizes automation, security, and user experience. The following presents the different segments for which Visma group offers its services:

- Accounting and ERP
- Financial Management
- HR and payroll
- Procurement
- Invoicing and debt collection
- Welfare technology. (Visma group, b.)

As the vision of Visma group (Visma group c) is

“Our vision is to shape the future of society through technology.”

and they try to fulfill the following mission:

“Our mission is to empower people by simplifying and automating complex processes.”

Based on the vision and mission one could describe that Visma group is technology driven and wants to produce added value to its customers with the use of technology but to do it in such a way that it would not be too complicated for the users of Visma group services and would prove an elevated level of automation of tasks.

1.2 Research questions in this thesis

The idea for the research was formed based on the thesis writer’s experiences from the Visma security champion and the secure software development life cycle programs. Hypothesis related to the security champion program onboarding was that the current onboarding process of the new security champions needs improvement in helping the security champions to gain more confidence and competence so that they would be able to produce a good and regular results in improving the security of the various services that Visma group and its legal units produce to external customers. Visma has given a lot of thought and conducted earlier research on how those programs could be implemented successfully but there might always be room for improvement. The research in this thesis concentrates on how well the new security champions are onboarded the security engineer program in Visma and could the current onboarding process be evolved more by using an onboarding process theory.

The main research question in this thesis is

- R1 How to improve the onboarding process of security champions using existing onboarding theories?

There are three supportive research questions to the main research question. The supportive research questions are the following

- R1.1 What onboarding process theories exist for onboarding?
- R1.2 What are the parts of the onboarding of the new security champions that need the most attention?
- R1.3 What improvements can an onboarding theory bring to the current security champion onboarding process in use?

1.3 Used research methodologies

After the research problem is defined, it needs to be solved. This is achieved by utilizing research methods. Research methods can be then grouped for methods that are used for data gathering and methods that are used for analyzing the gathered data (Kananen, 2015). Data can be collected in many ways e.g., with surveys or observations and analysis of the data can be done, for example with cross tabulation and correlations or content analysis. (Kananen, 2015).

The chosen methods of collecting the data and analyzing it are related to what kind of approach for the research of the phenomenon is chosen, quantitative or qualitative or the combination of both methods. Quantitative research method is used when there is a need to produce a common and measurable view of the phenomenon that is being researched and the quantitative approach is objective as the research is being made in a structured manner and there is no possibility for the researcher to influence the results of the research (Vilkka, 2007). According to Vilkka (2007) Objectivity in the interpretation of the research results is achieved by applying theoretical frameworks to the results. Quantitative research will usually find causality between different measured variables or confirming or invalidating hypotheses (Vilkka, 2007).

Qualitative research instead tries to help to understand the phenomenon, how it is experienced amongst the persons that are being studied in the research (Merriam & Tisdell, 2016). Merriam and Tisdell (2016) mention three other main aspects of qualitative research which are

- the researcher is the driving force behind the data collection and analysis of the data
- qualitative research is an inductive process which means that there might not be an existing theory, or they cannot be used to describe the phenomenon, which is researched, and new theories and hypotheses can rise through the research observations for interpreting the phenomenon
- qualitative research describes the results of the research by words instead of numbers that are used in quantitative research.

In this thesis the research question was approached by using both qualitative and quantitative approaches. The data gathering methods used were a survey targeted to all known security champions in Visma as well as semi-structured interviews with security champions. The survey was structured based on the Bauer (2010) theory of the onboarding process to pinpoint parts of the onboarding process that might need improvement by measuring the results based on the success factors of the onboarding process. Survey data was also used to find suggestions for improving the onboarding process through cross tabulations. As the target population of the research was the security champions in Visma the survey was conducted for them. Visma calls security champions as security engineers so that name is used later in this thesis. The amount of existing security engineers was calculated based on the security engineer information on the Product Security Catalog of the Visma Application Security Program. Visma Application Security program is the Secure Software Development Lifecycle framework that Visma uses, and Product security Catalog is an asset inventory for the different services that Visma develops. They will be explained more in the chapter 3.5 Secure SDLC framework used in Visma group. The number of security engineers was found to be 247. The survey was based on a sample of 73 security engineers.

After the survey analysis identification of the pain points in the onboarding process was done, semi-structured interviews were conducted to further analyze the problematic parts of the onboarding process of the new security champions that were identified through the survey. The interviews were done for 11 security engineers that were randomly selected from the whole security engineer population.

The research methods (survey and semi-structured interviews) used for data gathering are very commonly used when doing research on different phenomena. Survey contents should be planned in detail so that the actual survey and its questions would be as unambiguous as possible so that the respondents and the creator of the survey will understand the questions in the same way (Valli & Aaltola, 2018a). Earlier surveys have been conducted e.g., with mail surveys, but today there are a lot of tools that make it possible to create survey forms in ease, making the actual process of conducting the survey very easy as well as cost effective. Valli & Aaltola (2018b) mention also that pitfalls of the survey-based data gathering are usually related to the questions and how they are presented as there is often the risk of misinterpretation if the questions are not clear or the questions are made as such that they lead the respondent to some distinct direction and thus the results of the survey can be misleading.

Different types of interviews on the other hand are an efficient way of getting the hang of what the interviewee thinks of the phenomenon. Semi-structured interviews are one type of interview where it follows loose structure based on themes that should be processed during the interview, but it is possible to have still open discussion and the interview flow does not need to follow an exact plan or order of questions like in a structured interview (Valli & Aaltola, 2018b). As the security engineers in Visma might have quite different situations and background semi-structured interviews were chosen as the data gathering method as it provides freedom of changing the interview flow and the possibility to discuss on other issues as well as the ones defined in the interview guide.

2 Previous studies of onboarding

Even though the onboarding theory used in this thesis is a research-based theory there is quite many other previous onboarding process studies available. Some of them are researching software developers, but no other study was seen that would have been researching the onboarding of the security champions. However, as the security champions in Visma are usually developers or working in other roles in development teams they might be used to help with the onboarding of security champions. Usually, the software developer onboarding studies seem to be quite new thing and probably because of that they are not very commonly cited in other research papers. Here are few examples of other studies concerning onboarding process amongst organizations that develop software.

Onboarding software developers and teams in three globally distributed legacy projects: A multi-case study

The study done by Britto et al. (2018) utilized the same Bauer theory what was used in this thesis. The study was done as three different case studies and it studied the new employee onboarding of three legacy software projects. Britto et al. (2018) have for example the following suggestions

- telling accurately to the newcomers what they are expected to do
- formal and generic orientation helps when there are multiple development teams in many places
- they recommend getting the new employees start working with real tasks as soon as possible.

Overall Britto et al. (2018) recommend thinking the onboarding process as a comprehensive process and that the process is typically not the same in different organizations or it might be different even in one organization based on the needs of the onboarding taking place. So, the onboarding might vary between different roles etc.

A Case Study of Onboarding in Software Teams: Tasks and Strategies

This study was done as a case study for Microsoft US division, and it was aimed to study how developers were onboarded to different teams (Herzig et al., 2021). It included interviews and survey. The study builds upon using three different themes which are learning, confidence building, and socialization and the study presents clear recommendations for actual activities that improve the three themes (Herzig et al, 2021). For example, the study recommends using different social events to improve the feeling that the newcomer is working in safe environment and having dedicated time to learn the needed things in the new role or position

Please Turn Your Cameras on: Remote Onboarding of Software Developers During a Pandemic

As the COVID-pandemic hit the world the organizations had a new challenge when onboarding new employees as the social integration happened mainly on-line instead of face-to-face meetings. This study researched what kind of challenges there were when software developers were onboarded. The study was conducted by Microsoft, and it had a survey that done to 267 new employees who started working in development teams (Ford et al., 2021). Study recommends creating an agile onboarding process that can be changed according to needs. In detail Ford et al. (2021) emphasizes the that the newcomers would be bonded better to development teams e.g., by having more virtual events, those events could be relaxed events too. The study also recommends mentoring in a couple of ways they call the other one as “onboarding buddy” and its responsibility is to help in general things like helping to find needed resources and to see that the onboarding goes well. They also recommend of also having a technical mentor. Documentation should also be kept up-to-date and having easy tasks at hand at first. (Ford et al., 2021.)

3 Theoretical background

The theoretical background of this thesis is divided into chapters that describe more about the security champions in general as well as what kind of onboarding process theories were investigated during making this thesis. As in Visma the security engineers are a key part of securing the whole software development life cycle, they are also covered shortly. Visma Application Security Program or VASP is also described in detail as security engineers will be involved in running the program within the various products and services that Visma and its legal units develop and provide to its customers.

3.1 Security champions

In today's modern application development security aspects need to be considered in every step of the development life cycle as well as raising the security awareness throughout the organization as the cyber threat landscape is crowded with different threats and threat actors. Security Champions can be key players for achieving enough security. But what is a security champion? The Open Web Application Security Project, OWASP, describes security champions as follows: "Security Champions are active members of a team that may help to make decisions about when to engage the Security Team" (OWASP a). The same Security Champion Playbook (OWASP a) also emphasizes the fact that security champions are needed to assure the proper level of security within the product that is being developed.

OWASP Security Champion Playbook (OWASP a) describes the following six different steps when implementing a security champion program

1. Identify teams
 - This phase considers getting facts about the development teams that are working with development of a software product or service. To get proper idea about the teams and what they are dealing with there should be intelligence on e.g., what kind of technologies are in use, what is the automation level of the team, are codes and the related documentation where what kind of release cycle the product or service has.
2. Define the role
 - The security champion role needs to be clearly defined and have objectives that are easy to understand. The role description should include, for example, the participation in the product development tasks, identification of risks and making or reviewing security reviews in the team. These are just examples so there are a lot more things to be considered when defining the role.

3. Nominate the champions
 - When nominating the security champions, it is essential to have support from the top of the organization so the management should be involved in the process. There should be managers involved from the top to the team level managers otherwise there is a risk that the security champion does not have the proper authorization to promote the security related activities in the team. OWASP suggests that at least a day in a work week is dedicated to security tasks in the beginning. It is crucial that expectations and targets and also what kind of benefits like there might be for the security champions. The onboarding of the new security champions is part of this step.
4. Set up communication channels
 - The collaboration aspect is important for the security champions, and it is necessary to think how the security champions communicate with each other and the actual security organization. Nowadays there are many collaboration tools like Slack available, so it is up to the organization to decide what tools to use. In general, it just should be possible to raise awareness and share information as well as be able to get feedback easily.
5. Build solid knowledge base
 - Organizations should make available some kind of knowledge base where different aspects of security starting from the strategy to the different guidelines and best practices are available when a security related question pops out. There should also be training available for the security champions, especially when the security champion has little or no previous experience related to cyber security. So, the security champion training should be thought through. If the organization wants a security champion could have e.g., different competence tiers based on what kind of training they have had in the organization training program and what kind of results they are able to produce.
6. Maintain interest
 - To keep the security champions motivated and efficient they should have constant activities, which can be e.g., tournaments or workshops and some constant security-related news or meetings. The security champions can also have some dedicated pages or forums etc. Main thing is that the security champions will have enough stimulus to keep going on with their role.

So, the security champion program needs a top-down approach to ensure that the whole organization is involved in it. That is the key element to be successful with the program. The security engineers also need constant attention and possibilities to evolve and improve. Security champion programs are not yet studied much. One research by Jaatun & Soares Cruzes (2021) suggested that the security champion can be also based on the concept of champions of innovation in addition to champions of security. Their research resulted in the conclusion that both models should be used in conjunction as they will both bring something useful to the security champion programs. As for other conclusions, they emphasize the importance of management involvement and the fact that the security champions need time and the possibility to constantly be involved in security related tasks. They suggest that it is better to have many security champions with less

weight on the security champion tasks instead of for example having one full-time champion as it might be impossible for a single champion to help multiple teams at a satisfactory level. (Jaatun & Soares Cruzes, 2021.)

3.1.1 Security champions in Visma

Visma has a security champion program in place, and it is tightly related to the secure software development life cycle of Visma that is called the Visma Application Security Program, VASP. For managing the security in the whole Visma, it has a common security organization that is called the Visma security team. The Visma security team is responsible for managing the security champion program and VASP. Both programs have taken their characteristics from the OWASP security engineer playbook and the OWASP Software Assurance Maturity Model (SAMM).

The security champions are called security engineers in Visma. The security engineers are named for each product or service that the different Visma companies produce for their customers. There can be one or several security engineers in one product though. The security engineer's role is described in the internal team workspace and the same team workspace has also other company-wide security guidelines. Security engineers are recommended to have experience of software development as well as an interest in security. Security engineers are the main responsible for running the VASP in their product or service. It includes the annual reassessment of the Security Self-Assessment, SSA, as well organizing the Visma internal penetration test goes with the name Manual Application Vulnerability Assessment in Visma before the previous test run has expired. Security engineers should make sure that all the security services (DAST, SAST, SCA) that are included in the program are also up & running correctly. Fortunately, most of the services are maintained by the Visma security team but there is still much to do for the security engineers when thinking about how to configure the services and how to interpret and act based on the results of the services.

In addition to running the Visma Application Security Program the security engineers are supposed to be actively involved in the whole development process and in the secure development lifecycle. The responsibilities include, for example

- gathering and documenting all security and privacy related requirements that should be considered later in the development process
- proactively suggesting security and privacy related enhancements in the design phase
- constant contribution to improve security and privacy in development and support processes
- contribution in making guidelines & best practices related to secure software development
- responsibility of creating and monitoring the security issues found during security testing
- making sure that that service pipeline is adequate security and privacy wise
- Having the responsibility that the proper monitoring tools are in use and that they have the needed thresholds and alerts in place
- taking care of the security and privacy documentation
- reporting on security and privacy incidents
- assisting in incident management.

These are just examples so we can see that the expectations for what security engineers should do include a lot of activities.

Security engineers form their own community inside Visma which is led by the Visma security team. The community has frequent meetings with the whole community and there is a dedicated slack channel for the security engineers to ease the communication concerning the activities of the security engineer and the Visma Application Security Program as well information sharing. Security engineers are also encouraged to participate in other common security related activities like the monthly security awareness meeting facilitated by the Visma security team.

3.2 Onboarding process theories

The onboarding process of newcomers has been studied for a long period of time and there are theories on the subject available. Successful onboarding is a key element which can help the newcomers to conform to their new job or role and blend into the other employees. Successful onboarding will benefit the newcomer as well as the organization too. There are different theories to the subject but in most studies the theory of different organizational socialization tactics made by Van Maanen & Schein is the most cited of the theories. As time has passed there is more and more research-based information available and because of that fact this thesis will be based on Bauer's theory which is based on multiple research projects on the subject. In the following chapters Bauer's theory as well as the basic organizational socialization theory will be described in more detail.

3.2.1 Theory on organizational socialization tactics

In 1979 Van Maanen and Schein released their theory of the socialization tactics that organizations can use with newcomers or role changers. Their theory is based on six different dimensions which each have two different tactics that can be applied in the onboarding process. The different dimensions are

- Collective vs. individual socialization process
- Formal vs. informal socialization process
- Sequential vs. random steps in the socialization process
- Fixed vs. variable socialization processes
- Serial vs. disjunctive socialization processes
- Investiture vs. divestiture socialization processes (Van Maanen & Schein 1979).

The different tactics mentioned on these dimensions will produce different results. Van Maanen & Schein (1979) have in their theory predictions on what effect the chosen or used tactic has in the end. For example, when thinking of formal vs informal tactics, they have four different suggestions:

1. Formal socialization tends to happen in organizations that have more specific roles and positions with predetermined values and attitudes related to the roles and positions.
2. Informal socialization on the other hand is related more in situations where newcomers need to study new abilities, working methods or practical skills
If the new role or position has high risk for the newcomer, co-workers, organization, or clients of the organization then formal socialization tactics are also usually used (e.g., firefighters, doctors)
3. Formal socialization tactics will usually produce more general results amongst newcomers
4. Informal tactics may produce even more generalized results than formal tactics or it can also produce innovative results from newcomers. That is because a more individual approach will have the newcomer have more freedom to take the new position or role into control (Van Maanen & Schein 1979).

Van Maanen & Schein (1979) raise the following result types for the onboarding in their theory; custodial response, content innovation and role innovation. Custodial response is a result that is common and expected and the content innovation and role innovation results describe more unexpected and innovative results for how the newcomers can handle the situations thrown at them in their new job or role. The different response types with used tactics in the dimensions are presented in Table 1.

Table 1. Response types and dimensions and tactics.

Response type	Dimension & tactic					
	1	2	3	4	5	6
Custodial response			Sequential	Variable	Serial	Divestiture
Content innovation	Collective	Formal	Random	Fixed	Disjunctive	
Role innovation	Individual	Informal	Random		Disjunctive	Investiture

Later Jones (1986) added the individual and organizational characteristics to the dimensions that Van Maanen & Schein presented in their theory and grouped them under them as shown in Table 2. The study made by Jones (1986) hypothesized also that the self-efficacy of the newcomers can have an effect on the results of different socialization tactics when role orientations are considered. Study results showed that the amount of self-efficacy did affect the results (Jones, 1986).

Table 2. How Jones grouped the socialization tactics under institutionalized and individual tactics

Dimension	Tactic	
	Institutionalized	Individual
1	Collective	Individual
2	Formal	Informal
3	Sequential	Random
4	Fixed	Variable
5	Serial	Disjunctive
6	Investiture	Divestiture

3.2.2 The research-based theory made by Bauer

Bauer's theory (2010) is based on various studies of the onboarding process and other theories from the subject. Bauer theory adds the results of different studies into a research-based model of the onboarding process which will result in both short and long-term effects. Van Maanen's & Schein's (1979) organizational socialization tactics theory is also present in Bauer's model. The studies that were conducted was done for large organizations but the best practices that it presents can be used with medium and small organizations too but there might be need avoid some of the best practices as they might become too expensive for them (Bauer, 2010).

Bauer's (2010,2) model identifies four key dimensions that correlate with a good onboarding process. Those are Compliance, Clarification, Culture and Connection (Bauer 2010, 2). Bauer (2010) commonly talks about them as the "Four C's". Compliance presents the fact of how newcomers are introduced to the legal and regulatory aspects of the organization. Clarification concerns how accurately the newcomers know the objectives and responsibilities of the job or role and what is expected from them. Culture means how well the newcomers feel that they fit into the organization's values, objectives and work community. The connection is more about how well the newcomers are able to communicate with the important stakeholders or colleagues that are related to their new job or role.

According to Bauer (2010) there can be three different levels of onboarding based on the organization's decisions on how the onboarding process is done. The levels are

1. Level one - Passive onboarding
 - Only the compliance aspect is fully involved in the onboarding process and the Clarification is partly present. Culture and Connection are not at all thought of
2. Level two - High Potential
 - In addition to the Passive onboarding there are some aspects of the Culture and Connection present
3. Level three – Proactive
 - All the dimensions (Compliance, Clarification, Culture and Connection) are fully present in this type of onboarding (Bauer, 2010).

For the actual onboarding process Bauer (2010) has identified six different functions which will all have their own effects on various aspects of the onboarding. The functions are

- recruiting process
- orientation Forums
- support tools & processes
- Feedback tools
- Training
- coaching & support.

How well the whole onboarding goes based on the functions will result in some general results for both the organization and the newcomers. Newcomers will adjust to their new job or role better and fit better into the other personnel of the organization and they will aim for the same objectives that the organization has if the onboarding goes well. Thus, newcomers will have better

chances of being an efficient employee for the organization as their motivation can be at a higher level as well, they might be productive faster in the new job or role. On the other hand, a not so well-handled onboarding process might result, e.g., in a lack of motivation and dissatisfaction with the job or role. In this scenario new employees are probably not so efficient for the organization and there is a larger possibility that the newcomer will not stay long in the organization.

After the newcomers have been selected through the recruitment function, Bauer (2010) represents four different attributes which are key variables when considering how successful the onboarding will be. The same attributes are also the short-term effects of the onboarding process. The implementation of the six onboarding functions has an effect on what level the different attributes will be amongst the newcomers. The four attributes are the following

1. Self-efficacy
2. role clarity
3. social integration
4. knowledge of culture (Bauer, 2010).

In addition to the attributes mentioned, the selection of newcomers also plays a part in how successful the onboarding of newcomers is. If the selection for the best candidates succeeds there are better results overall when considering the whole onboarding process (Bauer, 2010). Figure 1 elaborates the relationship between the different onboarding functions and attributes.

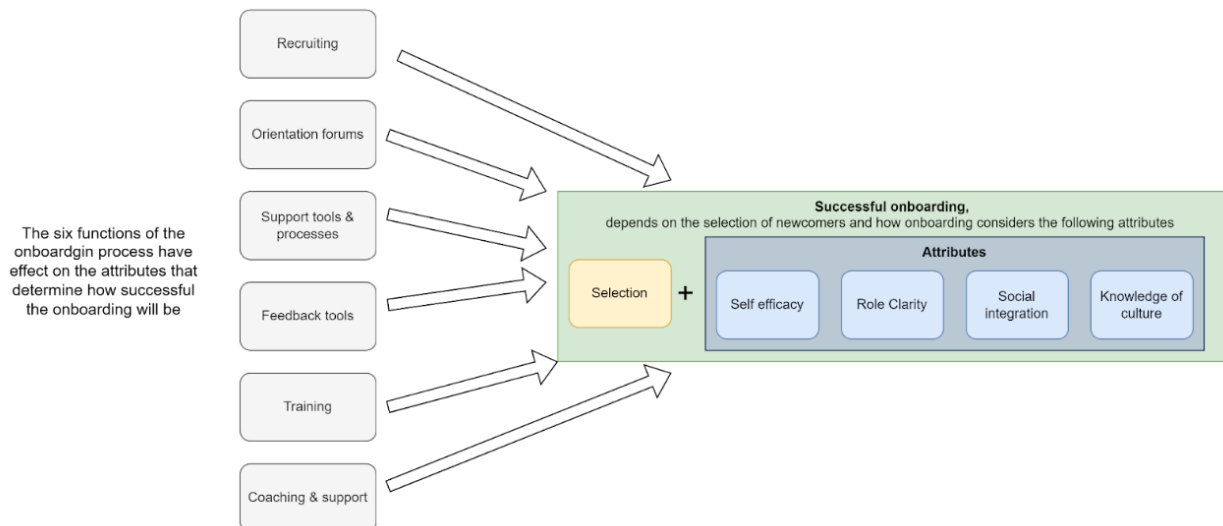


Figure 1. Functions and attributes based on the Bauer (2010) model.

There are also long-term effects that will be visible after a longer period of time. Bauer (2010) makes a conclusion that the longer-term effects of a good onboarding include e.g., more committed organization, high job or role satisfaction and employees that are more efficient and at the same time have lower stress levels than employees that have had an onboarding that has not been so good. Employee retention is also at a higher level if a good onboarding process is practiced (Bauer 2010). With those results in mind the onboarding process can be thought of as a crucial part of the organizations and their management of human capital.

3.3 Software development life cycle, SDLC

The introduction and development of information systems has emerged a process which defines a set of activities that are related to the different phases like design, development and maintenance of the information system or software life cycle. That process is called software development life cycle (SDLC). In this chapter software development and some examples of software development methodologies and the secure SDLC common practices are discussed.

3.3.1 Software engineering and the “software crisis”

In 1964 software engineering made a major breakthrough as IBM released its System/360 main-frame family publicly. The whole development process took as long as two years and cost 5 billion dollars which would be today about 30 billion dollars and required a few million lines of code for

the mainframe to be working (IBM, 2008). The purpose of the System/360 was to produce a device that would make it possible to migrate software and data without big effort to new computers which would have more processing power (IBM, 2008).

The System/360 was a success but it had its own drawbacks as the development of software for such large and monolithic computer systems usually produced software systems that were also big and cumbersome to develop and maintain. The results of that combination resulted in big costs for maintenance of the mainframe as well as the software. This eventually led to the “Software crisis” in which the main source of costs of an information system can be seen coming from the software development and maintenance instead of the hardware costs as the machine-based software based was not easy or fast. It was also seen that there were a lot of issues concerning software like poor quality, rising costs of development vs. budget, no defined development process thus the activities of the developers were not clear. (Mohapatra, 2010.)

As there seemed to be demand for how software systems life cycle is managed a first description of the phases of the software development phases were introduced by Winston Walker Royce in 1970 (Mohapatra, 2010). The model that Royce suggested for software development described in the Figure 2 is a waterfall model which is one method of software development, but Royce (1970) never presented that term in his technical paper.

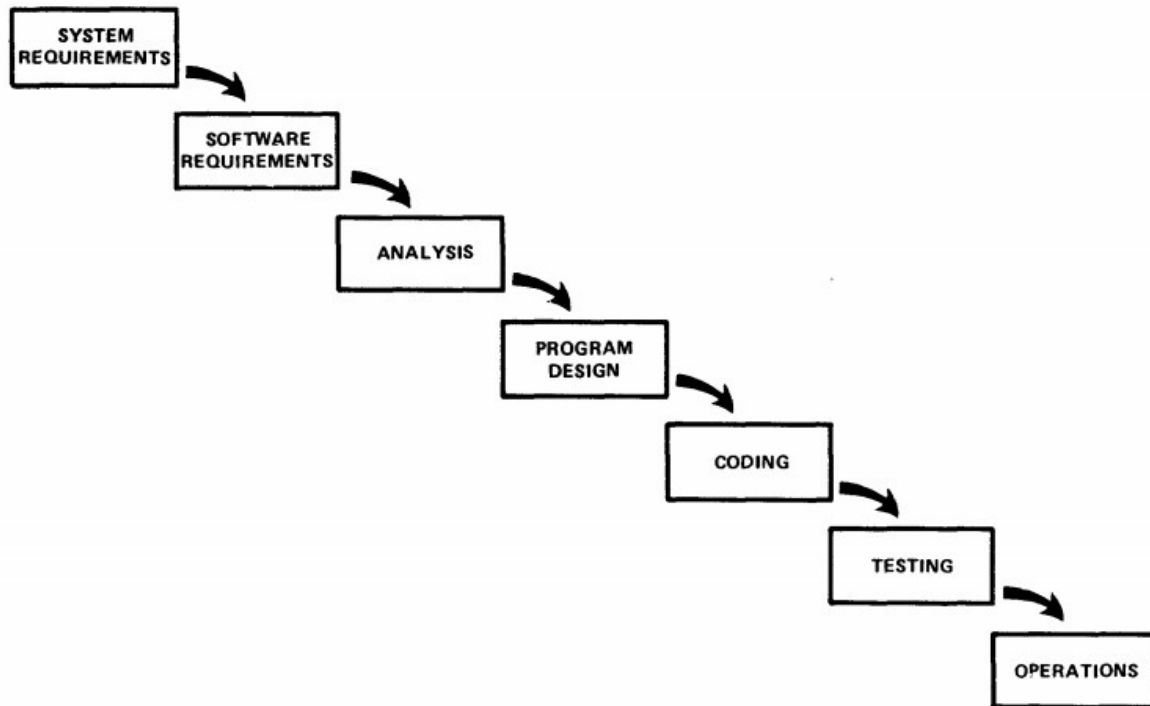


Figure 2. The software development phases as Winston Royce (1970) presented them

Since the mainframe-based systems and applications a lot have changed in the previous decades and new software development methodologies like the Agile development process have been developed after the waterfall model as it has its own weaknesses that cannot mitigate all the findings of the “Software crisis”. The technical platforms have also drastically changed as cloud computing takes a bigger role all the time when it comes to the fact where the infrastructure and platform of an information system is running. Even though the changes the elements of the crisis are still around though there are a lot more tools or methods available to mitigate those issues.

3.3.2 Software development life cycle models

When a software is developed it should always have similar phases in its development life cycle.

The development starts from some idea or concept and ends finally when the software is retired.

Dooley (2011) presents the development life cycle phases as the following

- 1 Idea/concept/planning
- 2 requirement specification
- 3 designing the software
- 4 Development
- 5 Testing
- 6 Release/deployment
- 7 Maintenance
- 8 Retirement.

The phases can be also combined so the phase amount can be smaller depending on the software being developed and the SDLC methodology in use can also affect how the phases are implemented and is there how many iterations in some phases (Dooley, 2011). The Figure 3 presents a visual view of the SDLC phases. The maintenance and retirement phases are not always presented in the visual view.

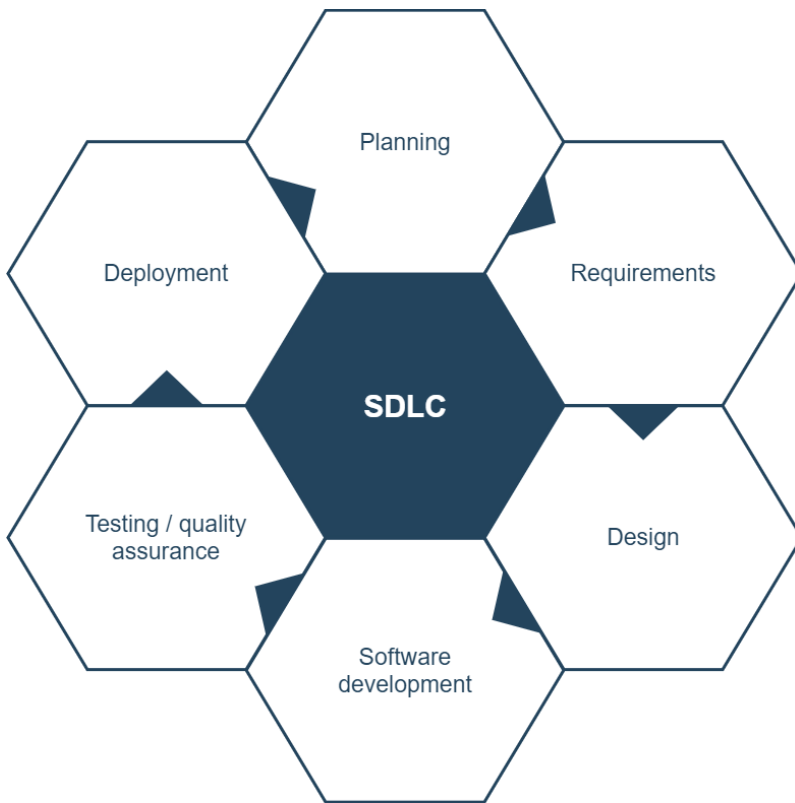


Figure 3. SDLC phases and life cycle

The approaches of the SDLC process models are different but they all are aiming for fixing the caveats that have not gone anywhere since the original “software crisis”. So, we could say that they try at least to remedy that the software being developed would correspond to the customer requirements, increase the quality of the solution, and add transparency to the whole development process.

3.3.3 Waterfall

As mentioned earlier, the waterfall was the first SDLC process model that Winston Royce developed in 1970. Dooley (2011) says that the weakness of that model is that it requires that the phase is finalized before moving to the next phase of the development process. If we look at the phases of the model in figure x that means that all the requirements must be gathered and analyzed before the design of the solution can begin. That would mean that before moving on to the design the development team should now be 100 % sure that they have all the requirements that the customer is expecting from the software written down. This is not a situation that usually happens. (Dooley, 2011.)

The second weakness of the model according to Dooley (2011) is that the model does not present any option to move backwards in the model. And usually in the software development process there is the need to think and maybe redesign some aspects of the software differently than what the initial design was. Because of these issues Waterfall is not the most practical model, but it might be a useful development model for some teams. (Dooley, 2011.)

3.3.4 Spiral

Barry Boehm released the spiral development model when he wrote the paper “A Spiral Model of Software Development and Enchantment” in 1988. The spiral model is quite comprehensive, it takes into consideration the high-level design e.g., the different options how the software or functionality can be implemented, and it has a risk-driven approach which enables the possibility of doing the actual development with other development process models like waterfall or prototyping. The spiral model described in the Figure 4 describes prototyping development where each cycle of the spiral will present another prototype. A risk analysis is always done in conjunction with each of the prototypes to see whether the remaining risk is acceptable or not and another cycle is needed before the software can be developed into a production version (Boehm, 1998). Overall, during the spiral model, the software is getting better in each cycle of the spiral.

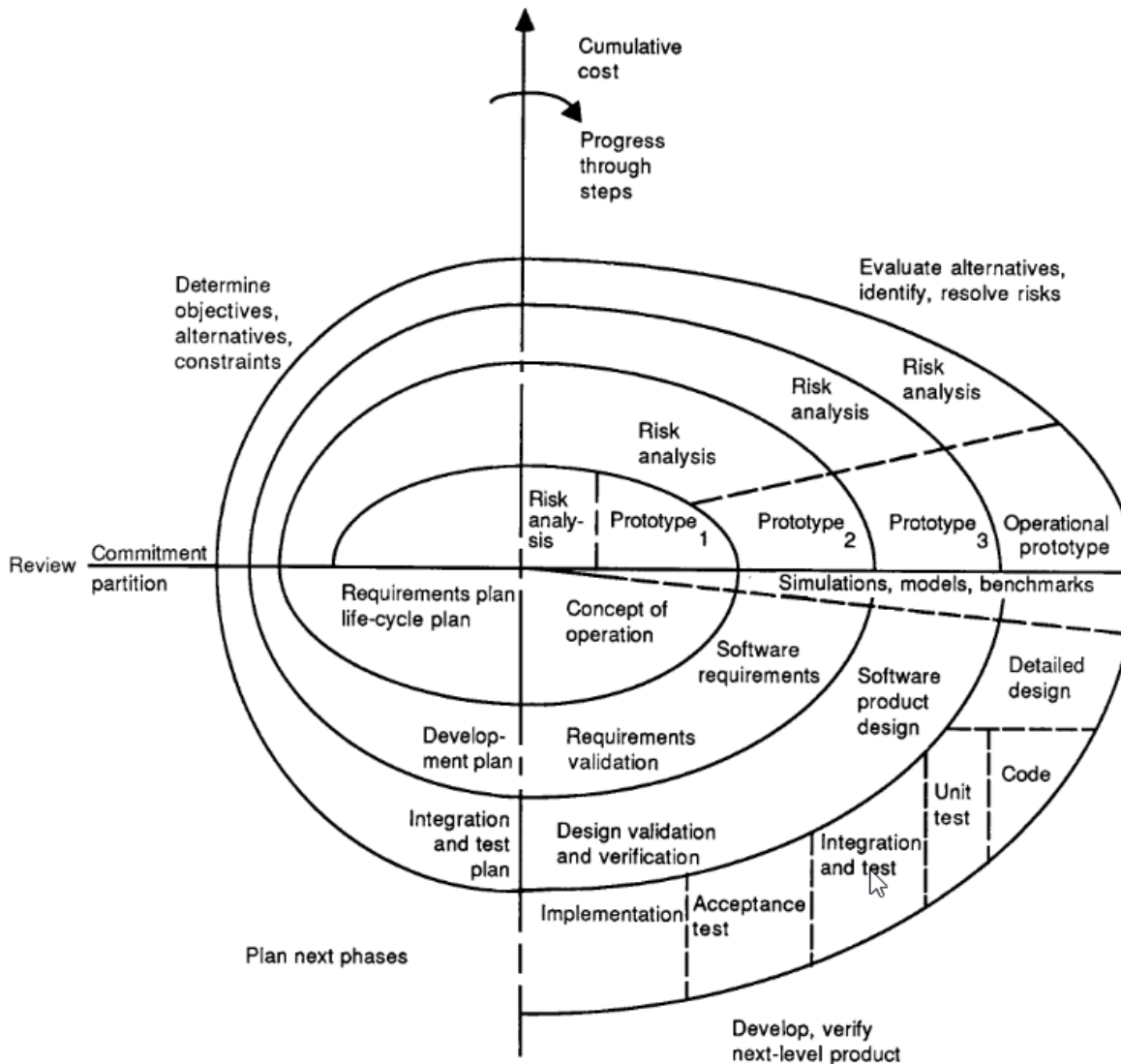


Figure 4. The original diagram of the spiral development model (Boehm, 1988)

The benefits of the spiral model are that it allows the use of already developed software development process models and the risk-based approach that can mitigate the risks associated with the previously mentioned models. On the other hand, it also has its disadvantages like the risk-driven approach requires more competence when considering the risk assessment capabilities and the continuous development of the spiral model cycles. (Boehm, 1998.)

3.3.5 Agile development process

As the traditional development models were quite time-consuming and laborious there was a need for a lighter-weight development model in the software development industry. In the year 2001 seventeen software developers released a manifesto for an agile software development model. That manifesto made by Beck et al (2001a) is called “Manifesto for Agile Software Development” and it presents the views on the software development process of the writers of the manifesto. The content of the manifesto is

“Individuals and interactions over processes and tools

Working software over comprehensive documentation

Customer collaboration over contract negotiation

Responding to change over following a plan”

So that group of developers had a clear view of how the software development process can be made nimbler and more efficient and to make sure that resulting software would serve the customers better and to get working software ready faster. The manifesto was backed up by several principles and the following list has a few examples from those principles

- customer satisfaction is achieved by releasing working software fast and frequently instead of producing just documentation
- frequency of deliveries should be kept minimum, preferably there should be a release every few weeks or a maximum in a couple of months
- changes are always imminent, and the Agile model welcomes changes in every phase of the software development process
- development teams should have control of adjusting their own work independently and the team should reflect their doings continuously and change their working methods if there is a need for it to get even better results. (Beck et al., 2001b)

It is typical for an agile development model that during the development process the planning phase is not so detailed and more effort is put into how to get the customer more satisfied. That is usually possible via involving the customer more in the whole development process. And to support the agile development process model many frameworks, processes and guidelines have been developed such as Scrum, Test Driven Development (TDD) and Extreme Programming (XP). (Stober & Hansmann, 2010.)

The Scrum framework is one of the most used agile frameworks, which is based on iterations, sprints, that usually last from two weeks to one month. The process includes several roles like the scrum master who is responsible for keeping the daily scrum meetings where the development situation is shortly gone through. Other roles can be for example, product owner and developer. The product backlog is a list of requirements that should be done. The product owner prioritizes the product backlog items and, in a sprint, planning meeting the goal of a sprint is defined and the needed backlog items will be assigned to the sprint. Figure 5 presents the idea of the scrum framework defined by the Scrum Alliance. (Scrum Alliance, 2020.)

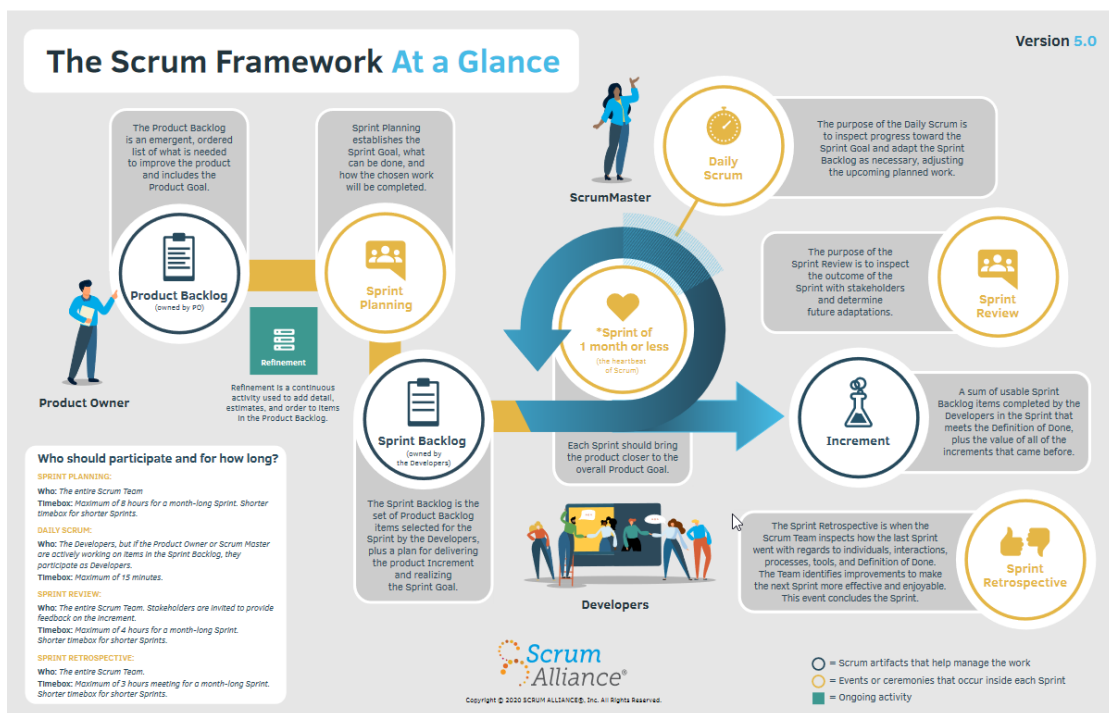


Figure 5. The definition of the Scrum framework (Scrum Alliance, 2020).

3.4 Secure Software Development Life Cycle, S-SDLC

As there are more and more threats and threat actors of various capabilities around today and the meaning of software has all the time become more crucial as the societies are heavily dependent on different services the need of ensuring the security of the software during the development life cycle is becoming also more important. In the recent months we have seen for example the SolarWinds/Sunburst attack, a very sophisticated supply chain attack, that is suspected to be done by a state actor APT29 aka “Cozy Bear” (Corfield, 2021), Dependency Confusion attacks that related to

different package management tools and their logic getting the needed private packages when building a software project (Birsan, 2021) and the Microsoft Exchange Vulnerability that based on several zero-day vulnerabilities that was also originally exploited by a group called Hafnium which is also analyzed as a state-based actor (Burt, 2021). Those all show that during the life cycle of the software there might be several different places where vulnerability can cause big problems. And that is why Secure Software Development Life Cycle (S-SDLC) has been added to the toolbox when the security issues in software development are concerned.

There are various types of S-SDLCs and capability maturity models (CMM) which have different approaches to improve the security of a software project during its development phases. For example, Microsoft has its own approach Security Development Lifecycle (SDL), OWASP foundation has OWASP Software Assurance Maturity Model (OWASP SAMM) and BSIMM framework presents one other approach to mention some of those models. Noopur (2005) has found that secure software development should be focusing on the following four key areas:

- security engineering activities
- security assurance activities
- security organizational and project management activities
- Security risk identification and management activities.

Security engineering activities should consist of activities concerning the secure design of the software as well utilizing different tools like static code analysis as well as doing code reviews to ensure that the developed software code is also secure. This phase should also take into consideration that the testing methods are safe. Different verifications and validations of the built software as well external reviews like penetration tests made by external parties should be the activities of the security assurance area. (Noopur, 2005.)

In the governance area that is related to organizational and project management security there should be defined policies for the organization and management should be involved and committed to the security aspects. The roles concerning the various aspects of the development process should be defined and if there are some other things that need to be in place in the organization to increase security. (Noopur, 2005.)

Noopur (2005) also found that the finding and managing the risks concerning security should be one of the key aspects of a S-SDLC as the risks will usually generate other tasks. If security related risks are found, they usually also can affect how the secure development activities are done and how much effort is put into assuring security. Security risks can have effects on project management too. (Noopur, 2005.)

As there are many models around, they all have a slightly different approach to what kind of activities are included in each model for those key areas of security. They are still all good guidelines on how to secure the whole life cycle of software but there might be still needed to do something differently. In the following chapter the Visma approach, Visma Application Security Program, is described in more detail.

3.5 Secure SDLC framework used in Visma group

Visma has produced its own Secure Software Development Life Cycle framework called Visma Application Security Program (VASP). Constantly changing threat landscape was one driver for creating the framework and maturity models like BSIMM and OWASP SAMM have been one of the references when the framework was developed (Cruzes & Johansen, 2021). The security activities in the common security framework ensure that the needed security controls of secure development are in place in all life cycle phases across all the Visma development teams. It also increases the security self-awareness of the development teams as well as the transparency of the security situation of the teams and products. The framework also allows Visma to measure the security maturity of the development teams and the software products that they develop in a common way.

Cruzes and Johansen (2021, 167) describe this framework as “Ambidextrous Software Security Initiative” as it allows both top-down and bottom-up approaches to improve security. As Visma is a large enterprise that has acquired many smaller companies in many countries this kind of versatility has been found effective as the development teams work differently and the cultural differences can affect negatively on the secure development when implementing just a top-down approach (Cruzes & Johansen 2021). Cruzes and Johansen (2021) also find other things that can go wrong with just a top-down approach such as

- security related issues are not treated as equal to functional requirements and management does not fully support security improvements. Organizations should put enough effort and resources to get security involved in every step of the development life cycle.
- If the security activities are pushed too hard to the teams the results are not very good and the impact of them tends not to be continuous. It would be best to get people excited about the things at hand and enable teams to easily implement and use the needed security controls within the VASP framework.

But not only the top-down approach has its problems as there are also some things that should be considered bottom-up approach. For example, the communication aspect might give a headache to the security engineers as the communication with managers is totally different thing compared to talking with more technical person and convincing management to do required security fixes or bigger tasks instead of business requirements can be challenging. It is also imperative to have the management support and commitment to this kind of approach.

VASP framework has many actions and Cruzes & Johansen (2021) mention the following examples of them

- Making a security self-assessment (SSA) to get the team an overview of their current security posture.
- Different security testing activities that include e.g., testing tools and manual application penetration testing
- Cyber Threat Intelligence Service (CTI)
- Bug bounty program
- Possibility to utilize a Red Teaming Service
- And Trust Centre (found from <https://www.visma.com/trust-centre/>), which is a service available to Visma customers on the Internet that provides details about Visma Security Program and the products that Visma offers. For example, the Figure 6 has a screenshot of the data that Visma Trust Centre shows about the Wintime products that Visma Public Oy FMS unit offers to its customers.

The screenshot shows the Visma website's 'Products' page. At the top is a blue navigation bar with the Visma logo and links for Organisation, Investors, Products, Insights, Responsibility, Careers, Media, and Log in. Below this is a secondary navigation bar with links for Trust centre, Security, Privacy, Products, and SMB Software Products. The main heading is 'Products'. A paragraph explains that transparency is key for customer trust and that the site provides information on data centres, locations, sub-processors, and certifications. A 'Product Search' section follows, with a search bar containing 'wintime'. Below the search bar are two product cards: 'Wintime' and 'Wintime Classic'. Each card lists the Data Center (location of data) as Valtti Kumppanit Oy, Finland; Data Center Certifications as ISO/IEC 27001:2013 and ISO/IEC 20000-1:2011; and Sub-processor (purpose) as AdvancelIT (Database operations).

Figure 6. Product details of the Wintime product from Visma Trust Centre

There are also other actions that are part of the framework. In the following chapters the security activities will be gone through in more detail.

3.5.1 Product security catalog

First step when starting the implementation of the VASP framework the services or applications that the Visma company needs to be listed in the security product catalog. That could be also called a registry of assets for the services that Visma owns and develops. The catalog, as the name implies is concentrating on security and how data is protected. The catalog entry information will be later utilized in the Visma Security Maturity Index (SMI).

3.5.2 Security engineer

As a one task each service or product team should name one or more security engineers whose role should be the facilitator of the security activities in the team. Cruzes & Johansen (2021) call the security engineers as "champions" in the security framework according to. According to Cruzes & Johansen (2021) security engineers should take care of the following activities

- improve security knowledge in their own teams and organizations
- share information about the VASP program and guide others on how to use it
- think of the means how to implement security related tasks in a proofed and working way inside their own teams and organizations
- communication between the team and the Visma product security team.

If we look at the listed tasks and as the VASP framework is an ambidextrous S-SDLC model, we can conclude that the security engineers are key players when it comes to ensuring each service security and sharing security related information across the several Visma companies. Cruzes & Johansen (2021) want still to remind that as all the appointed security engineers do not have similar characteristics, nor the knowledge from the field of cyber security or the enthusiasm towards the subject it is recommended that in these situations the security engineers should be assisted in their efforts to improve the security in their own teams and organizations.

3.5.3 Security Self-Assessment

The Security Self-Assessment (SSA) is one part of the whole secure system development life cycle framework in Visma group. The SSA describes the main cyber security topics that each team and the service they provide should take into consideration. The Figure 7 shows the different topics that are built into the SSA, and Figure 8 has an example from the SSA concerning the questions related to the access controls of the service.

- RM01: Risk Profile
- SEC01: System Diagram
- DP01: Data List
- DP02: Data Classification
- DP03: Privacy and Data Protection by Design
- DP04: Formal requirements and standards
- DP05: Customer contract and supported version
- SEC02: Attack Surfaces
- SEC03: Access Control Quality
- SEC04: Password storage
- SEC05: Crypto/hash algorithms
- SEC06: Application misuse
- SEC07: Software Dependencies
- SEC08: File upload validation
- SEC09: Secrets in source code
- SEC10: Secret Management
- SEC11: Phishing
- SEC12: Testing and Quality Assurance
- SEC13: Secure Deployment
- SEC14: Infrastructure permissions (databases, storage, queues, service bus etc)
- SEC15: Host and Network Security basics
- SEC16: Security Logging
- SEC17: Threat Intelligence
- RM02: Risk Review
- RM03: Risk Assessment
- RM04: Risk Register

Figure 7. Cyber security topics included in the SSA

SEC03: Access Control Quality

Use your System Diagram and verify that all endpoints, that needs Access Control have it implemented and properly.

Control
<p>Can a user only access the data that the user is intended to access?</p> <p><i>Do a smaller review of code. Make sure that you always check that a user has the necessary permissions BEFORE fulfilling the request. Do not rely on easily guessed ids or even GUIDs. OWASP IDOR cheatsheet.</i></p>
<p>Are tenants/customers isolated from each other?</p> <p>Database level: each tenant/customer has a separate database and the application ensures that the correct database is accessed for each request.</p> <p>Application level: tenants/customers share database and application ensures that the correct tenant/customer id is included in each database request.</p>
<p>Where are Access Control checks done?</p> <p><i>Client side controls can easily be bypassed but useful from a user experience view.</i></p>
<p>If a developer forgets to configure Access Control rules for a new resource, will it fail securely (access denied)?</p> <p><i>Secure by default.</i></p>
<p>Are procedures or features in place to review if access granted exceed the normal access levels for a given user?</p> <p><i>For example, regularly review old or inactive users, and to verify correct access level (ex users who shouldn't be admin anymore).</i></p>

Figure 8. SSA questions related to the access controls of the service

The development teams will fill the SSA in the best way they can with the help of the security engineer and if needed the team can consult the Visma security team. After the team has fulfilled the SSA it will be reviewed by the security team. With the SSA organizations will have an idea of the cyber security situation of their own and they will also generate some documentation about the controls that they have already in their services. (Cruzes & Johansen 2021.)

The SSA was found to be the best option to increase cyber security knowledge and the situation of it in Visma companies as the teams work independently and decide their own approaches to security in their own services. The other option would be more traditional learning and teaching, but Visma security team wanted to approach the teams with a solution that would be more like tutoring the teams and the inquiry based SSA was created for that purpose. (Cruzes & Johansen 2021.)

The following are the targets that the SSA is aimed at

- having a common checklist for the teams that can be used for getting a view of the security posture of the service that the team is providing for its customers
- having findings about the possible lack of security controls that there is in the service during its life cycle and help in prioritizing the found flaws
- giving the teams a generic way to implement proactive security related controls
- having responsibility about security in the teams as well increasing the knowledge and competence related to the cyber security in them. (Cruzes & Johansen, 2021.)

3.5.4 Static Application Security Testing service, SAST

If we look more closely at the Static Application Security Testing (SAST) and what that is, we can say that it is usually a tool that is made for analyzing security vulnerabilities in source code or even from compiled code. These tools can be integrated to developers IDEs or build pipelines so that the possible defects are found early in the development process as it is much easier to fix them early compared to that they are found in the later development process phases. (OWASP a.)

SAST tools have their own positive and negative points and there are also many aspects that should be considered when choosing the right tool for the organization like what programming languages does it support and how well it can detect different types of vulnerabilities. And of course, the possible cost of such a tool might be a key factor. (OWASP a.) As an example, Synopsys Coverity is one commonly used SAST tool.

Static Application Security Testing service (SAST) service was found as the second critical thing when the Visma security team first thought about the activities and controls that should be included in the VASP framework as it is easy to have security flaws in source code when developing services as the team might be utilizing e.g., insecure coding practices. Also, the security team wanted the teams to have more capability to find the possible defects as soon as possible in the development phases. Because of those facts Visma security team decided that it would provide the SAST as a service in the VASP framework to the development teams of the Visma companies. (Cruzes & Johansen 2021.)

Visma has chosen the tools based on their capabilities for the official SAST tools used in the VASP framework. But even though they are carefully selected they have their own restrictions. Because of that the security team also hosts other similar tools that provide code quality analysis for situations where, for example, the programming language is not supported by the VASP SAST service.

And in Visma there is a need for variety in the SAST tools as Visma organizations utilize about 80 different program languages in the products that they provide to their customers.

3.5.5 Automated Third-party Vulnerability Service, ATVS

Software Composition Analysis (SCA) is a tool which provides information about the third-party components that are used to produce a software product. SCA tools provide information about the vulnerabilities in these components and can also help to maintain a Bill of Materials which is a list of the third-party components in use. If the SCA tools leave gaps in the list of third-party components the list should be updated manually. The list should also be reviewed at least when there is a change in the components that are used in the software product so that the list will be kept up to date. It would also be good to have guidelines on how to act when the third-party component has vulnerabilities or is it at the end of its life cycle. That way the development team has a clear understanding of how they should react to the situation when a third-party component needs to be updated or replaced with another similar component or the team's own code.

Visma security team provides SCA as a service to teams through the VASP framework. In the framework the SCA service is known as the Automated Third-party Vulnerability Service (ATVS). The teams can decide whether they want to use the ATVS service in an automated way or will they have manual scans from time to time.

3.5.6 Dynamic Application Security Testing, DAST

Dynamic Application Security Testing or DAST is a testing tool that can be used for checking what kind of known vulnerabilities can be found from the functional application. The testing method that the DAST tools do when scanning an application is black box testing as the tools do not know how the application is built nor do they get access to source code (SAST is for that) or have information about the infrastructure of the application before the application is being tested. DAST tools can find multiple vulnerabilities that, for example, are related to OWASP top10 threats and thus they can give a view of how vulnerable the application shows to the possible evil actor that would try to access and hack it. (Walker, 2019.)

DAST tools should be used in late phases of the development life cycle as the application should be in that state that it is when running in the production environment. As of that fact the findings of the tool are usually vulnerabilities that will need a new deployment of the application that fixes that vulnerability. DAST tool's basic principle is to mimic realistic attack scenarios and they can be used to ensure the security of different size applications. (Walker, 2019.) There are many DAST tools available for the organizations that need that kind of service. Some examples of DAST tools are Nikto which is an open-source command line tool, Nessus and Netsparker.

Visma security team is offering one DAST tool as a service to the development teams within Visma group. The security team can also produce the DAST service as such that it will make the initial triage of the DAST tool findings for the team, or the team can self-manage the DAST service. The teams can also utilize some DAST tool other than the Visma Group specified one, but the team must then take care of how the findings are managed and the security team should be informed about the findings that the tool will find.

3.5.7 Penetration Testing

Manual vulnerability testing or penetration testing is also one important aspect of the VASP framework. Penetration testing can be described as one of the main tools when application or service security is being tested. During the penetration testing the testers are trying to break the security of the system with similar attacks that malicious actors would do in real life (NCSC, 2017). Penetration testing is usually done by an external partner, but Visma has a dedicated team that is doing the penetration testing for Visma companies.

Penetration testing should confirm that the security controls and processes of the system being tested are valid and working so the main thing should be getting confirmation about that. NCSC (2017) recommends that before penetration testing it is good to have gathered all the other facts and knowledge of possible weaknesses about the system via other controls. In the VASP framework they relate to the SSA and the different vulnerability scanners that the framework has.

Penetration testing can be done as black box testing where the testing party does not have any detailed information about the system that is to be tested. This is the method that simulates the real-world scenario where the attacker just sees the system as a box but does not know what is

inside the box. As in black-box testing scenarios the organization that is doing the testing has only a little information about the system, the testing results are not so comprehensive as in white-box testing. If we talk about the white box testing, there “the box” is open, and the tester can access even the source code of the system being tested which enables the tester also to analyze how well the code is written. (NCSC, 2017.) There is also a third testing option, gray-box testing, where both previously mentioned techniques are used at the same time (Cody et al., 2008).

3.5.8 Cyber Threat Intelligence Service

The VASP framework also includes a Cyber Threat Intelligence Service that the Visma companies can use to proactively gather intelligence from the Internet and the dark web about threats that are concerning their services or the companies themselves. The Service is part of the security framework that Visma security team offers to Visma companies. The service is provided to Visma companies in co-operation with an external partner.

This kind of service tries to find out if there are any actors that might have intent to harm the service or organization that is gathering intelligence about themselves. These kinds of services are also used for gathering more detailed information about the possible adversary capabilities. For example, the gathered intelligence information might have hints of what kind of techniques they might be using and how the adversary might be accessing the targeted service or organization. (Intel & Analysis Working Group.)

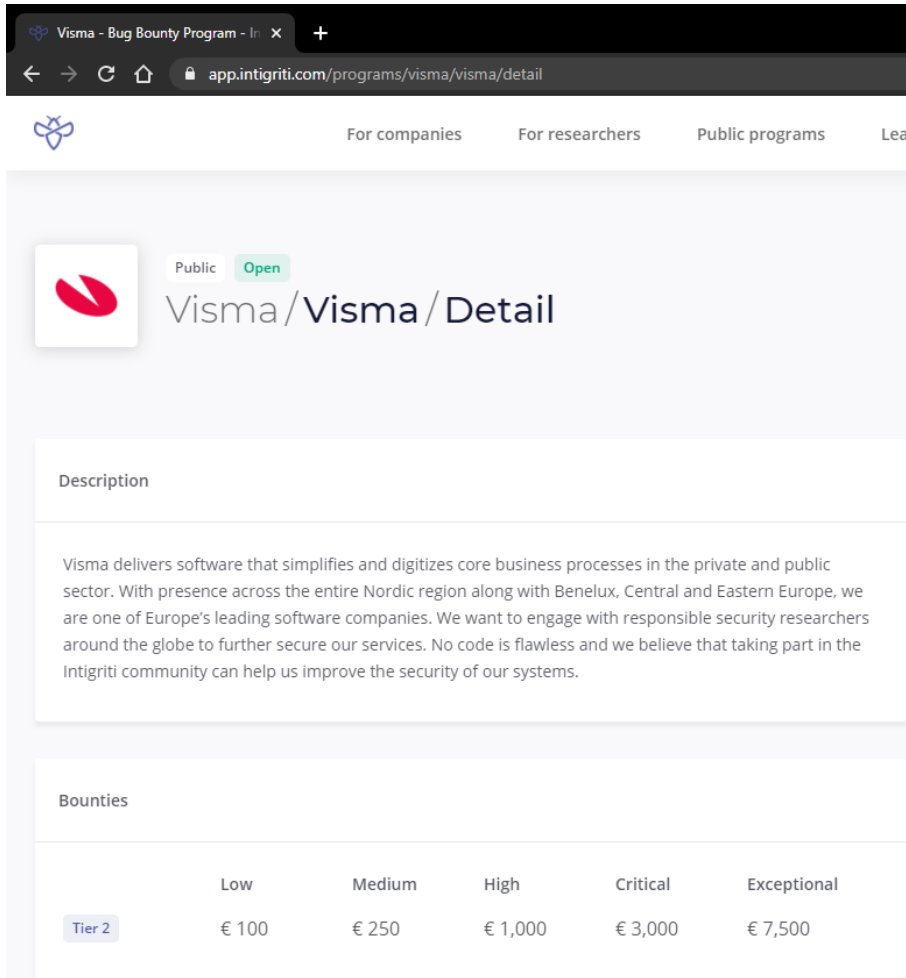
3.5.9 Security Log Management

Visma has been implementing a solution for Centralized Log Management for the services that utilize IaaS and PaaS from the key players of the Public Cloud business such as Microsoft Azure or Amazon AWS. The solution is called Visma Security Log Management (SLM). As not all services that Visma provides to its customers are not implemented and running in the required public cloud IaaS and PaaS providers the Security Log Management activity is not a required part of the VASP. SLM was designed to provide a common framework for the services to have similar logging and log management capabilities for infrastructure security logging and application security audit logging.

3.5.10 Bug Bounty Program

A bug bounty program is a program where the white hat hacker community can help organizations to find vulnerabilities in their services. The ethical hackers might get rewards for their findings in the bug bounty programs. Usually, this kind of community driven testing can expose critical vulnerabilities faster than other methods. There are different types of bug bounty programs like public programs where all can participate in finding the vulnerabilities and private programs where only invited hackers can participate in the program. (HackerOne, 2017)

Visma has had a bug bounty program for several years and this kind of activity has been considered as a complimentary service to the other services and controls that the VASP framework provides to the Visma companies to ensure the security of the services that develop and maintain. Each of the product teams can by themselves consider joining the bug bounty program. It is not a necessity in the VASP framework. Currently Visma is having co-operation with Intigriti that provides the bug bounty platform to connect Visma and ethical hackers that try to find vulnerabilities from Visma services. The Figure 9 describes the general information and the bounty tiers of the public Visma group bug bounty program in Intigriti.



The screenshot shows a web browser window with the URL `app.intigriti.com/programs/visma/visma/detail`. The page header includes navigation links: 'For companies', 'For researchers', 'Public programs', and 'Lea'. The main content area features the Visma logo, a 'Public' status indicator, and an 'Open' button. The title is 'Visma / Visma / Detail'. Below this is a 'Description' section with the following text: 'Visma delivers software that simplifies and digitizes core business processes in the private and public sector. With presence across the entire Nordic region along with Benelux, Central and Eastern Europe, we are one of Europe's leading software companies. We want to engage with responsible security researchers around the globe to further secure our services. No code is flawless and we believe that taking part in the Intigriti community can help us improve the security of our systems.'

Below the description is a 'Bounties' section containing a table with the following data:

	Low	Medium	High	Critical	Exceptional
Tier 2	€ 100	€ 250	€ 1,000	€ 3,000	€ 7,500

Figure 9. Visma group bug bounty program details at Intigriti

3.5.11 Measuring security maturity

The Visma security team has built a model to measure the maturity of the security based on the other activities of the VASP program. This model is called the Visma Security Maturity Index (SMI) and it was taken into use in the year 2018 (Cruzes & Johansen 2021). Maturity is measured with a dashboard which data is taken from various systems and is based on the activities of the VASP program (Cruzes & Johansen 2021). Each product that is listed in the security product catalog will have an entry in the SMI.

So, the SMI presents a gamified view that will take into account how well the service being measured is adopting controls and handling the other VASP activities and their findings. If there is a lack of compliance the service will have penalty points and they will affect negatively when concerning

the maturity of the service. Each service is reviewed before they are added to the SMI and the services are classified into different categories or tiers according to the fact of how important they are strategically to the Visma business. The results of the SMI are available through the whole Visma group to provide transparency. (Cruzes & Johansen 2021.) Figure 10 shows an example of the view provided by the SMI.

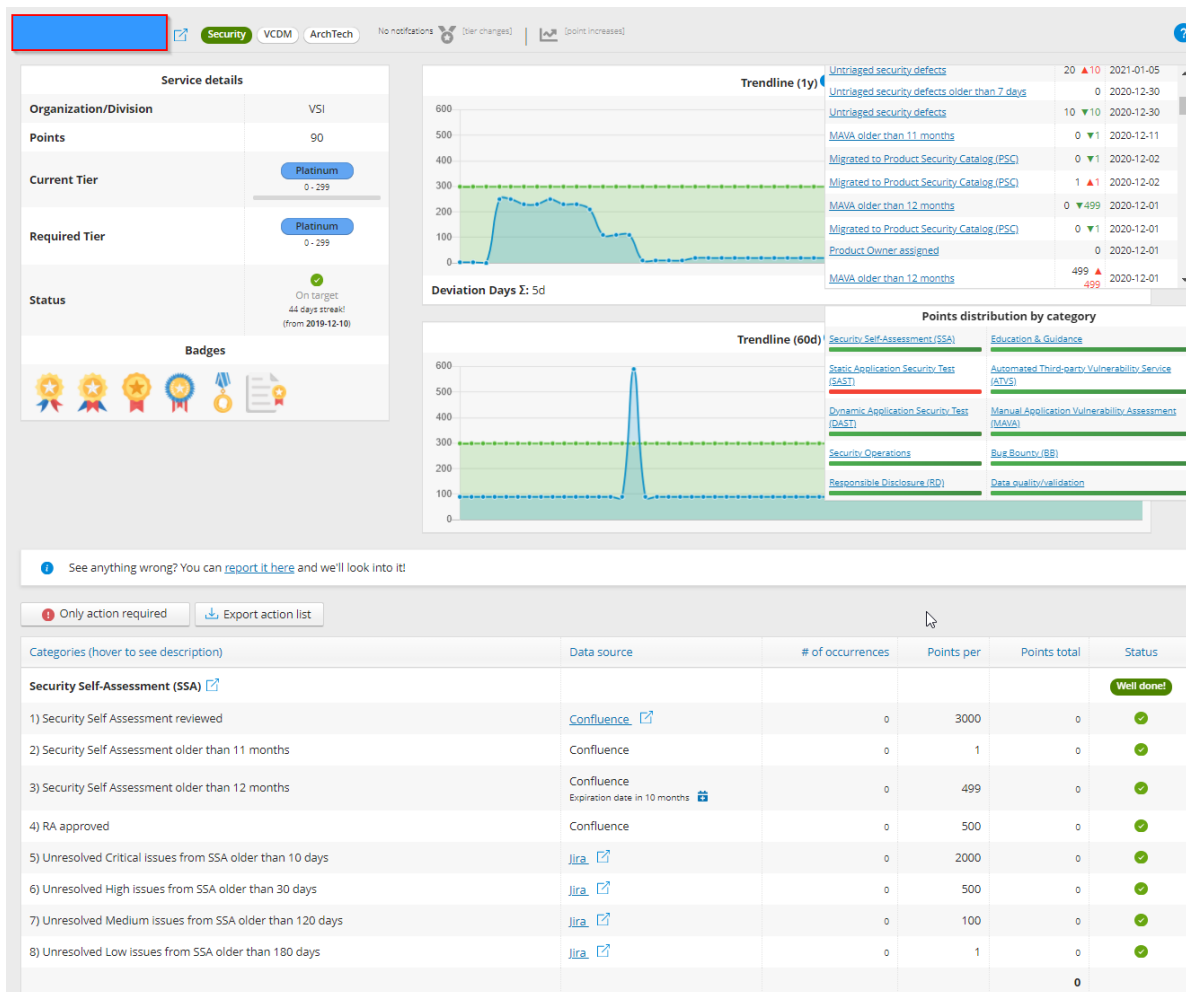


Figure 10. A view on the security maturity index product page

The SMI sole purpose is to provide a tool that will help the teams to improve the security posture by showing the security situation and the direction where the team is going with it. The transparency and gamified experience are useful as the whole organization can see the situation and can work together towards the target tier. If the team and service stay a long time in the same tier and the tier upgrades do not seem possible it might negatively affect the motivation of the teams. And

quite often the reason for slow advance is found within how the team or service owners prioritize the VASP activities and security findings in its backlog. (Cruzes & Johansen 2021.)

4 Survey analysis

A quantitative analysis was made for the Visma Security engineer to have an idea of how the current onboarding for the security engineers work and is there some general points of interest in the onboarding process that need to be adjusted and looked more closely. To be able to do such an analysis a survey was conducted, and it was targeted at the security engineers of Visma and its legal units. The survey was made in collaboration with another student from the Norwegian University of Science and Technology, NTNU, as the student was doing at the same time another master's thesis that was related to the whole Visma engineer program. A common survey was then conducted to serve the purposes of both theses.

4.1 Survey population

A population can be described as a group of people and in this survey the security engineers in Visma were targeted at, so they represent the whole targeted population. The amount of existing security engineers was calculated based on the security engineer information on the Product Security Catalog of the Visma Application Security Program. The number of security engineers was found to be 247 when the survey was on-going. All the security engineers did not answer to the survey, so the survey was based on a sample of 73 security engineers.

4.2 Survey instrumentation

The survey was conducted with Google Forms. The survey included questions related to the onboarding process as well as the whole security engineer program in Visma. The idea with a combined survey was that the security engineers would not be overloaded with several surveys running at the same time. Several surveys running at the same respondents might have also negative effects on the number of responses for each survey. The survey had five different sections which all concerned the various parts of the security engineer program. The survey had three different question types

- multiple choice (Figure 11). Used usually for nominal type variables.
- multiple-choice grid (Figure 12). This was usually used when asking about propositions and using a Likert scale-based answers to them
- checkboxes. Some questions of this type did have limits on how many options could be answered (Figure 13).

I have been a Security Engineer for

Multiple choice

less than 1 year

1-2 years

more than 2 years

Add option or [Add "Other"](#)

Required

Figure 11. Multiple choice question type settings.

Please answer to the following propositions.

Multiple-choice grid

Rows		Columns
1. I was given a realistic view what was expe...	<input type="checkbox"/>	<input type="radio"/> Strongly agree
2. I do not have role conflicts with the Securi...	<input type="checkbox"/>	<input type="radio"/> Agree
3. I am satisfied with the orientation that I h...	<input type="checkbox"/>	<input type="radio"/> Neutral
4. I am satisfied with my performance as Se...	<input type="checkbox"/>	<input type="radio"/> Disagree
5. Add row		<input type="radio"/> Strongly disagree
		<input type="radio"/> N/A
		<input type="radio"/> Add column

Require a response in each row

Figure 12. Multiple-choice grid question type settings.

The screenshot shows the configuration for a 'Checkboxes' question type. The question text is 'I would improve the following onboarding process functions (max two options)'. The question is set to 'Required' and 'Select at most 2' options. The available options are: Recruitment, Orientation, Training, Support Tools and processes, Coaching and support, Feedback, and an 'Add option or Add "Other"' button. Each option has a checkbox and a close button (X). At the bottom, there are icons for copy, trash, and a 'Required' toggle switch which is currently turned on.

Figure 13. Checkboxes question type settings.

In the survey the questions where respondents could not always answer to, had the value N/A or Not Applicable as one selectable option. Neutral option was also available for the different propositions that used the Likert scale. All the questions of the survey and the different sections can be found in appendix 1.

The main channel where the survey information was sent to the security engineers was Slack and within it, mainly the security engineer guild channel was used for sharing information about the survey. In addition to the messaging via Slack, the survey was presented also in the security engineer guild meeting on the same day the survey was launched and there was a brief reminder about it in the next guild meeting two weeks later. The security engineer guild meeting is a meetup of the security engineer in all Visma legal units and during the meeting current news on the cyber security front is presented to the security engineers or some insights concerning Visma security will be gone through. So, the meetings are for raising awareness and sharing information from the Visma security team to the security engineers. The survey was launched 1st of February

2022, and the survey was closed on 24th of February 2022 so it was open for responses for 24 days. During that time, the following events were published in Slack

- 1st of Feb – Initial message and link to the survey in Slack and presentation about the survey in the security engineer guild meeting.
- 8th of Feb – 1st reminder about the survey was sent
- 15th of Feb – 2nd reminder and a quick reminder in another security engineer guild meeting
- 17th of Feb – 3rd reminder
- 18th of Feb – 4th reminder
- 21st of Feb – 5th reminder. This reminder was different than the previous ones as a notification to all security guild slack channel was sent about the reminder.
- 24th of Feb – Message about the closing of the survey was sent via Slack.

Originally the survey was planned to be open for only two weeks but as there was a problem getting enough responses to the survey, it needed to be open longer. With the Slack messages sent different approaches were tried (Figure 14, Figure 15) to activate the security engineers. In the end the more frequent reminders as well as the message that notified the security engineers were the most effective ways to get more responses.

matti.paavilainen 10:51 AM

As presented in the Security Guild meeting there is ongoing master's theses research concerning the Security Engineer program and the onboarding process of the new Security Engineers. So You now have the chance to have an effect on what kind of improvements there might be in the program by answering a short survey here:

<https://forms.gle/> 

Survey results will be anonymous and the survey will be open for approximately two weeks from now. If You have any questions about the survey, feel free to contact me via Slack or send me an email.

Your answers will be really appreciated so 🙏 in advance!

Figure 14. The initial message from 1st of Feb about the survey.

matti.paavilainen 3:17 PM

Are You happy with the feedback that you receive as a security engineer? The others think this way about it. You can give your own opinion about the security engineer program and onboarding to it through the survey 🖱️ <https://forms.gle/...>

image.png ▾

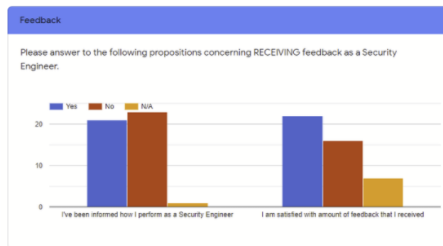


Figure 15. A reminder with some information of responses this far (17th of Feb).

In addition to the Slack messages the survey was presented to the Benelux area Chief Security officer who promoted the survey within the security engineers working in the Benelux area. The Finnish Security officers was also contacted directly so that they could also promote survey in their own legal units.

4.3 Reliability of the research

As the entire population of security engineers was out of reach for the survey a sample of the population was needed to conduct the survey. Sampling from the population can be done in a few different ways. Alternatives for sampling are random, representative and convenience sampling (Urdan, 2005). As a clearly defined population (only security engineers) was found and we could say that the respondents presented a representative sample. When using a representative sample, the results of the survey will reflect more accurately the targeted population (Urdan, 2005).

Based on the security engineer list that was gotten from the Product Security Catalog and having unique persons based on the catalog the exact maximum population of security engineers was found to be 247. And from that population 73 responded to the survey. The confidence level for the survey was targeted at 95 %. With that confidence level the confidence interval or margin of error was 9,6 %. It can then be interpreted that the results would be 95 % accurate if the entire population had answered the survey questions and the results would have a margin of error of 9,65 %. The margin of error means for example that if 50 % of the survey respondents would have answered Yes to one question, then in the whole population the same answer would have been between 59,65 % ($50 + 9,65$) and 40,35 % ($50 - 9,65$).

The confidence level and confidence interval were calculated with Creative Research Systems Sample Size Calculator (Creative Research Systems, 2012). The calculation is based on the formula shown in Figure 16 and it has the finite population correction in place.

Sample Size

$$SS = \frac{Z^2 * (p) * (1-p)}{C^2}$$

Where:

Z = Z value (e.g. 1.96 for 95% confidence level)

p = percentage picking a choice, expressed as decimal
(.5 used for sample size needed)

c = confidence interval, expressed as decimal
(e.g., .04 = ±4)

Correction for Finite Population

$$\text{new SS} = \frac{SS}{1 + \frac{SS-1}{\text{pop}}}$$

Where: pop = population

Figure 16. Sample size formula (Creative Research Systems, 2012)

The Confidence Interval calculation parameters were calculated for the worst-case scenario where the percentage of the survey sample answers would be 50. The results for the calculation are found from Figure 17.

Find Confidence Interval

Confidence Level: 95% 99%

Sample Size:

Population:

Percentage:

Confidence Interval:

Figure 17 . Confidence Interval calculation.

4.4 Data analysis

The survey results were analyzed based on Bauer's (2010) theory and the levers which by the theory influence how successful onboarding process is. Also, the selection part of the onboarding was analyzed. Figure 18 shows the various parts considered in the analysis.

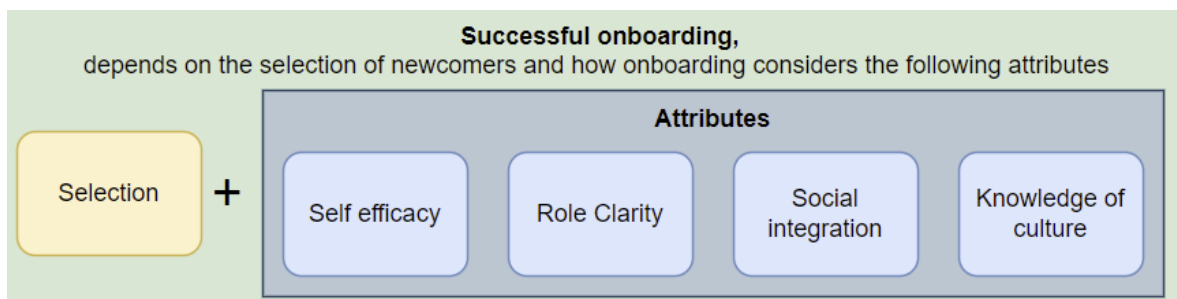


Figure 18. Levers that affect how successful the onboarding process is.

Survey results were imported to MaxQDA 2022 application where they were analyzed further. Also, Microsoft Excel was used for the analysis to produce more detailed charts based on the analysis. The not applicable values were present in frequencies, but they were not used when correlation was made. For some analysis based on the Likert scale questions, the agree-type (strongly agree and agree) were in some analysis combined to one value (agree) and similar combination of values was done the strongly disagree and disagree which were combined to value disagree.

4.4.1 Selection of the security engineers

When analyzing the selection part of the onboarding process the background information and the way respondents (volunteered vs. appointed) became security engineers was looked at in detail. From Figure 19 we can see that the respondents were quite evenly divided into the different values available. Only security engineers that had one to two years' experience in the role were a small minority.

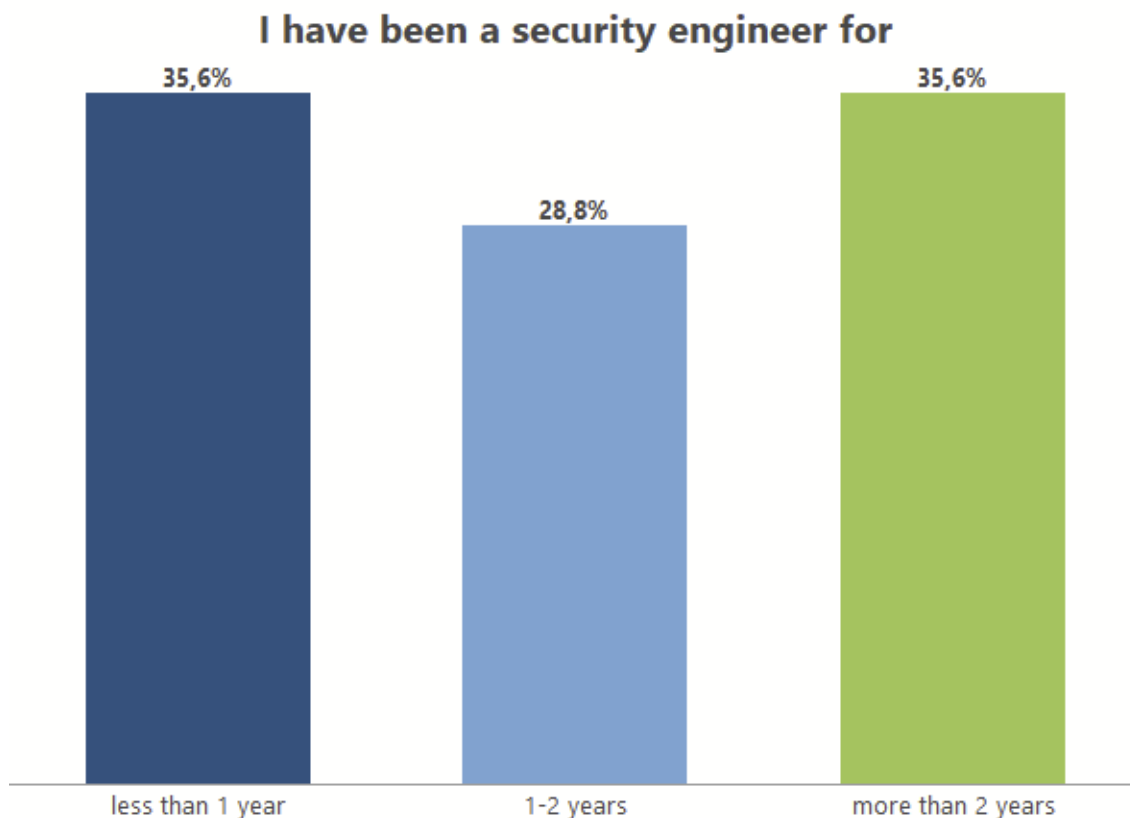


Figure 19. How long security engineers had been working in the role.

Survey results (Figure 20) show that more than half of the respondents had just beginner level competence or no competence at all on security before starting as a security engineer. 41,1 % thought that their competence was at intermediate level. 4,1 % (frequency=3) thought that they were already security professionals already before they started to work as security engineers.

Security competence before starting as a security engineer

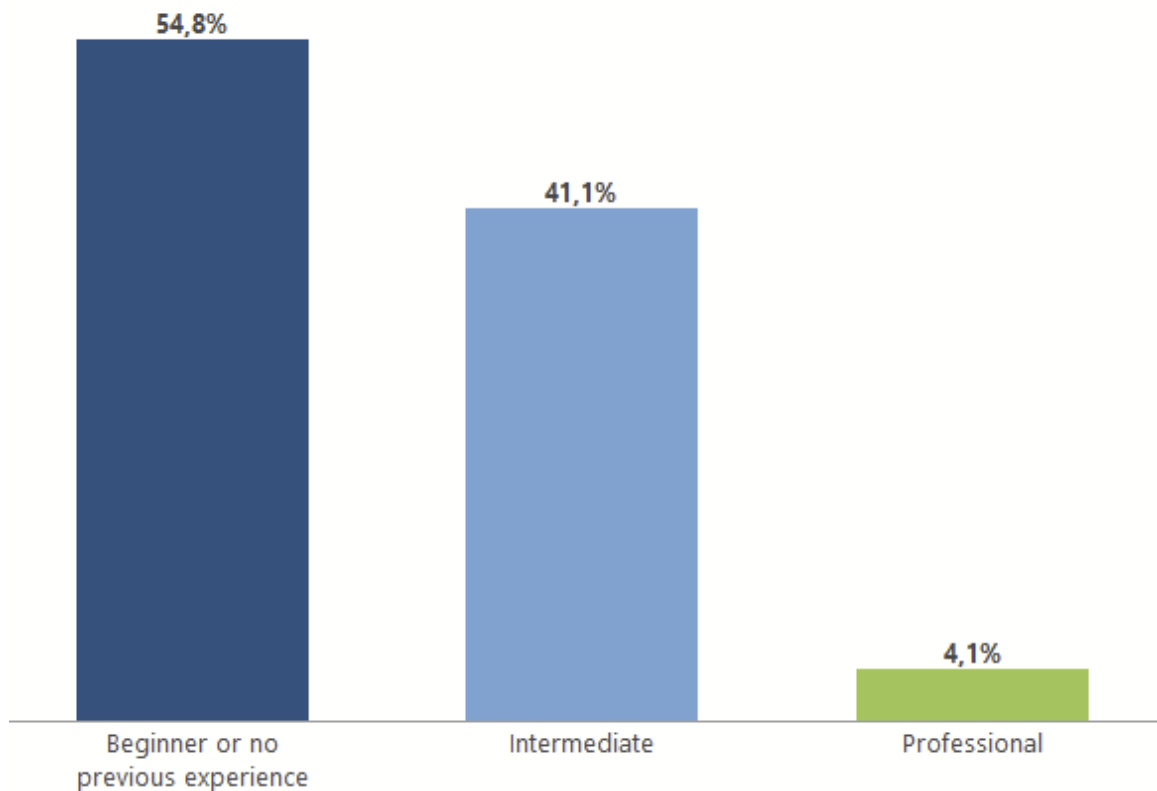


Figure 20. Previous security competence of the security engineers.

As the security engineer is usually a secondary role in Visma the main role of the security engineer was also asked. The majority (86,3 %) of the respondents had their main role in development team (developer, architect, and tester / quality assurance specialist) and the rest were working in other functions e.g., management or operations. As security engineers are intended to be from the development teams, that objective is realizing quite well. It was surprising that there were also quite a lot of respondents that worked in a management position, one even as a Business Unit Director. The distinct roles and their frequencies can be seen from Table 3.

Table 3. The frequencies of the main roles of the respondents.

Main role in Visma

	Frequency	Percent	Percent (valid)	Percent (cum.)
Developer	49	67,1	67,1	67,1
Architect	11	15,1	15,1	82,2
Tester / Quality Assurance Specialist	3	4,1	4,1	86,3
Business Unit Director	1	1,4	1,4	87,7
DevOps and Team Leader	1	1,4	1,4	89,0
DevSecOps Manager	1	1,4	1,4	90,4
Infrastructure	1	1,4	1,4	91,8
Infrastructure engineer	1	1,4	1,4	93,2
Manager	1	1,4	1,4	94,5
Operation Specialist	1	1,4	1,4	95,9
Security Champion/Intern auditor	1	1,4	1,4	97,3
Security officer	1	1,4	1,4	98,6
Service Owner / Infrastructure Engineer	1	1,4	1,4	100,0
TOTAL (valid)	73	100,0	100,0	
MISSING: System	0	0,0		
TOTAL	73	100,0		

In the survey security engineers were asked how they were assigned to the security engineer role. About six out of ten (61,6 %) of the respondents did volunteer for the role by themselves and the rest (38,4 %) were appointed to the role by someone else. The correlation between the fact how person was assigned to the role and how motivated was researched. The volunteered security engineers were more motivated as almost 91 % of them agreed on being motivated and only 4,7 % disagreed and 4,7 % had neutral stand. In comparison from appointed security engineers 57,1 % was motivated and 17,9 % was not and 25 % responded neutrally on feeling motivated working as a security engineer. The Figure 21 shows the correlation with a bar chart.

How the the way person was recruited to the SE role affected the motivation to work as SE.

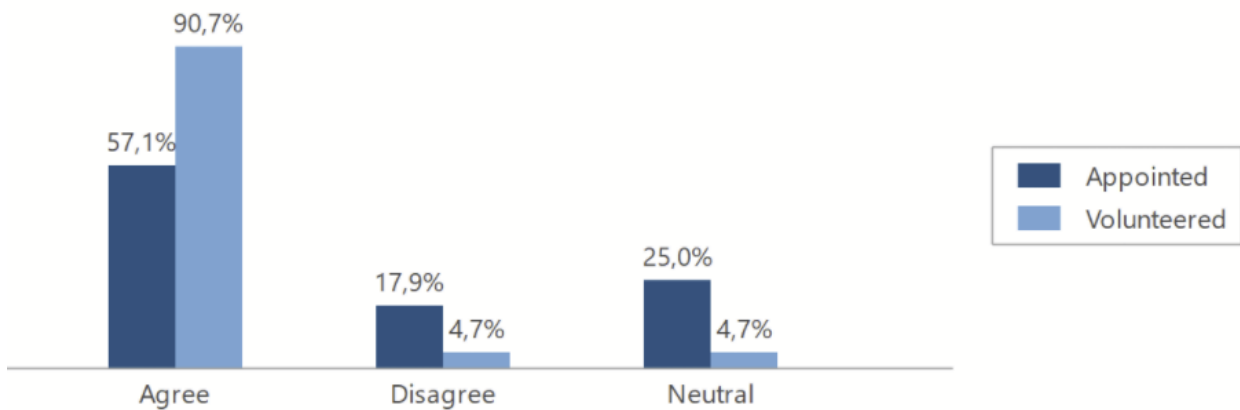


Figure 21. Correlation of how person was assigned to security engineer and how motivated they feel working as security engineers.

4.4.2 Self-efficacy of the security engineers

In the survey Self-efficacy of the security engineers was researched by several questions. The questions included the motivation of the security engineers and what they thought of their performance as one of the security engineers. The efficiency and confidence and satisfaction of the training that they have had was also thought to influence their self-efficacy in the role. The happiness towards the resources that security engineers need in their role was also on part of measuring the self-efficacy. Figure 22 presents details of the results to the questions mentioned.



Figure 22. Results of the self-efficacy related questions.

The respondents were quite well motivated as we concluded in the security engineer selection too. Half of the respondents were also satisfied with the performance that they have had as security engineers. The onboarding process thus seems to divide opinions concerning how it improved the confidence and efficiency levels in the security engineer role as the number of respondents that agreed or disagreed to these propositions were almost the same. And there were also a lot of neutrally thinking respondents.

The training received as security engineer did turn more to the negative side as about half of the respondents were not at all satisfied with it. This was seen for both the security-related training and the softer skills training like, for example, communications skills training. The resources that the security engineers are provided needed in the role were found to be enough by over half of the respondents.

To have more information about what could enhance how efficient and confident the security engineers felt, an analysis of the possible correlation between them and mentoring was made. Of all respondents 12 of them (16,4 %) had a mentor during the onboarding process, 58 (79,5 %) answered that they did not have a mentor and three were not sure (4,1 %). Based on these results it can be said that only a minority of the current security engineers have a chance of having a more senior security engineer or some other security engineer guiding them in their first steps as a security engineer.

As seen from Figure 23 there seems to be a correlation between whether the newcomer had a mentor and whether the onboarding process to the role makes them more confident and efficient working as a security engineer. If a person had a mentor during the onboarding process half of the respondents thought that the onboarding process makes them more efficient and 40 % thought that they are more confident in the role after the onboarding. If we compare the same results to the respondents that did not have a mentor, the percentages were 25,6 % (efficiency) and 17,50 % (confidence) respectively. It is however notable that when there was no mentor available the respondents that could not say whether the onboarding process affected positively or negatively to the efficiency or confidence were the most chosen option. The non-applicable responses of both questions were removed from the correlation results.

How mentoring during onboarding affected to the confidence and efficiency of SE

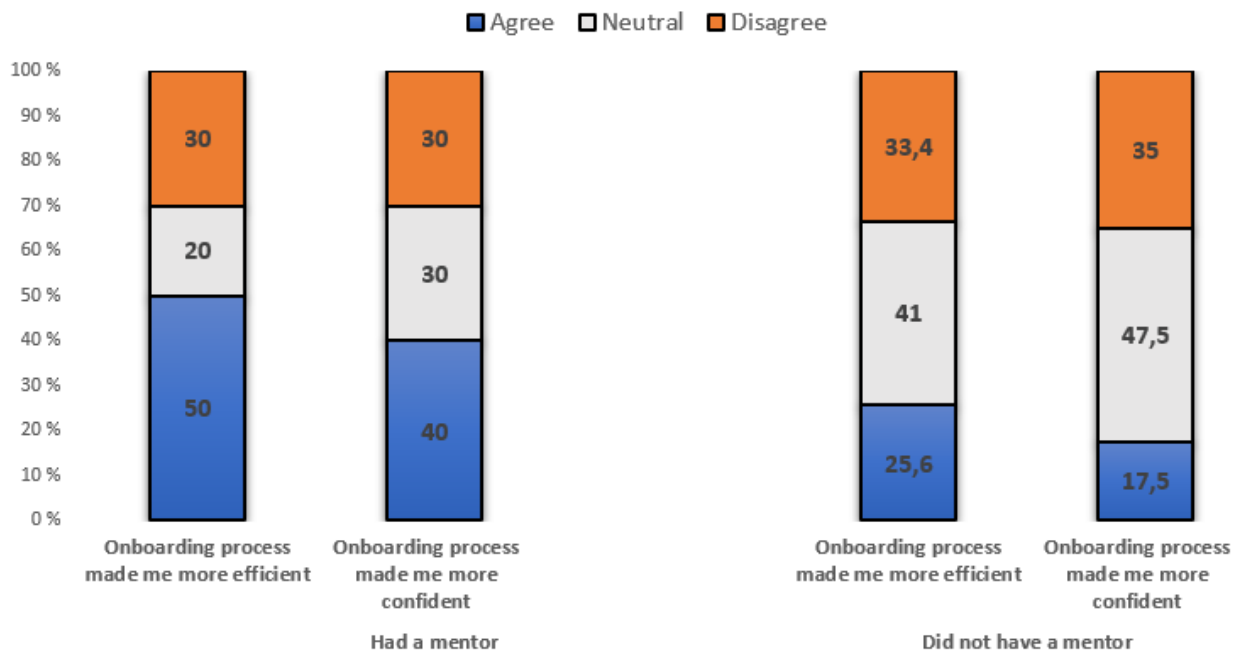


Figure 23. Correlation between mentoring and how onboarding process affected to the confidence and efficiency of the security engineers.

As the new security engineers are not usually security experts when they begin their security engineer career the training given to them affects their thinking of how they think of their self-efficacy. In general, satisfaction with giving training was found to be at a low level but to see whether the previous experience of security affected the satisfaction with the training, a correlation between the two was made. From the correlation analysis (Figure 24) it could be seen that if the security engineers were already security experts before starting as one, they were all not satisfied at all with the training that they had received. This was the situation with both security and softer skills training. With the security engineers who had beginner or no previous experience or intermediate experience with security there is not similar situation as there was 10,5 % to 18,4% satisfied respondents seen and a sizeable portion of the respondents thought neutrally on the subject

How the previous experience on security affected to satisfaction of the trainings, % of responses

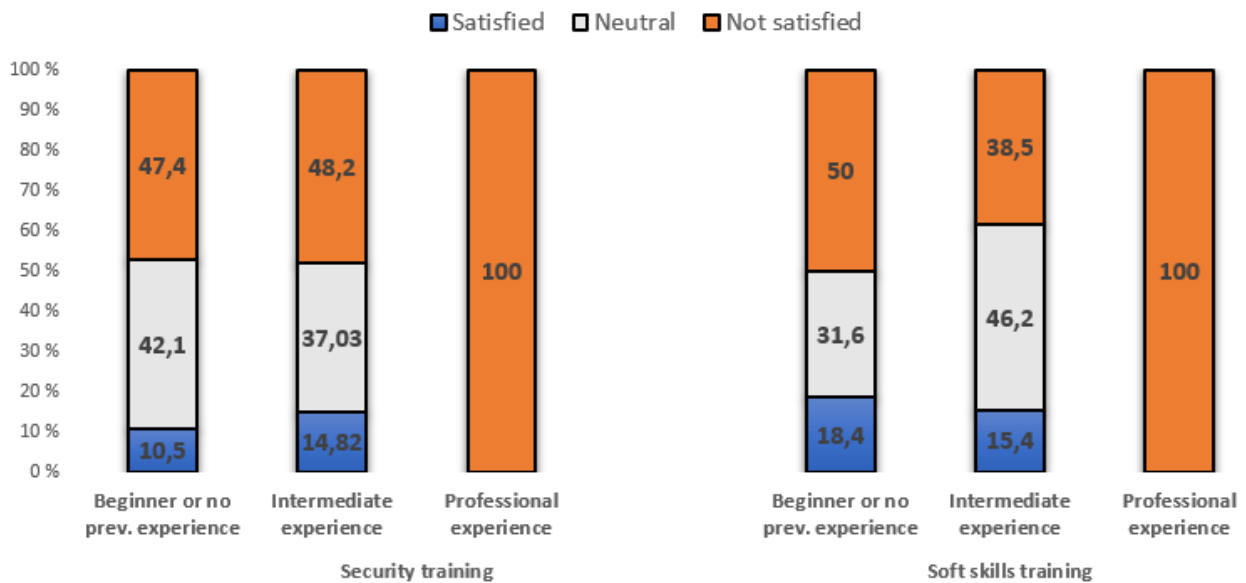


Figure 24. Correlation of previous security experience and how satisfied security engineers are with the training that they have received during the onboarding process.

4.4.3 Role clarity analysis

As role clarity is also one of the key aspects of the onboarding according to Bauer (2010) it was also one of thing that was analyzed with the survey. The following facts were considered in the analysis

- were they given a realistic view of what is expected of them in the role
- do the security engineers have pre-allocated hours and are there any role conflicts
- are there enough written guidelines for the security engineer role and Visma Application Security Program that the security engineer can follow and
- are they satisfied with the orientation that they received?

Likert scale questions results are described in Figure 26. Based on the results almost half of the respondents thought that they were given a realistic description of the role during recruitment.

About ¼ of the respondents thought that the given view was not realistic, and 28,6 percent had

neutral stand on this issue. Amongst the respondents only a minority answered having role conflicts between the security engineer role and with the other roles they have and about three out four respondents thought that they did not have such conflicts. There were some neutral answers too. 44,8 % of the respondents had an arrangement of using pre-allocated hours to security engineer tasks and accordingly 55,2 % did not have such agreement on the time usage. If pre-allocated hours for security engineer tasks were used it just marginally improved the situation about possible role conflicts between security engineer role and the other roles as shown in Figure 25.

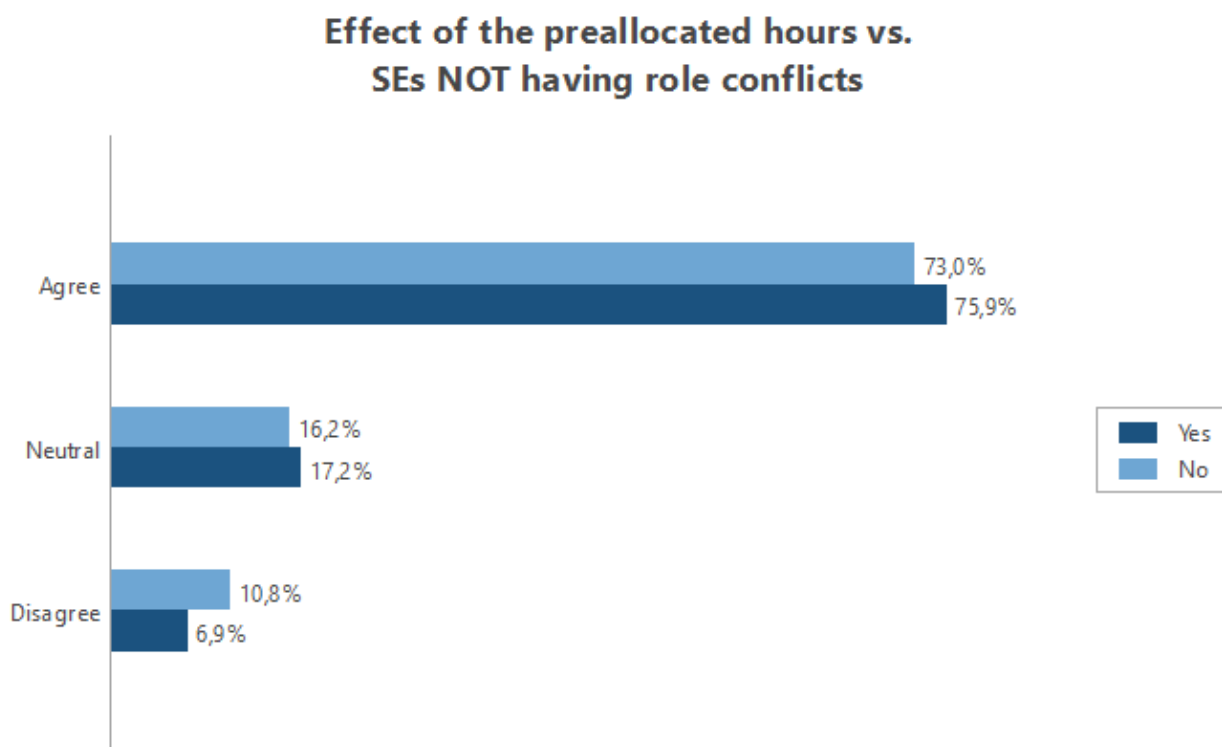


Figure 25. How pre-allocated hours affected to having role conflicts between security engineer role and other roles.

When asked about the are there enough written guidelines about the role and Visma Application Security Program, 45,5 % thought that there are enough guidelines. 18,2 % disagreed on that and 36,3 % could not agree or disagree. 44,4 % are satisfied with the orientation that they are given as new security engineers. However, one out of three security engineers are not happy with the orientation and about 22 % cannot tell if they are satisfied or dissatisfied with the orientation.

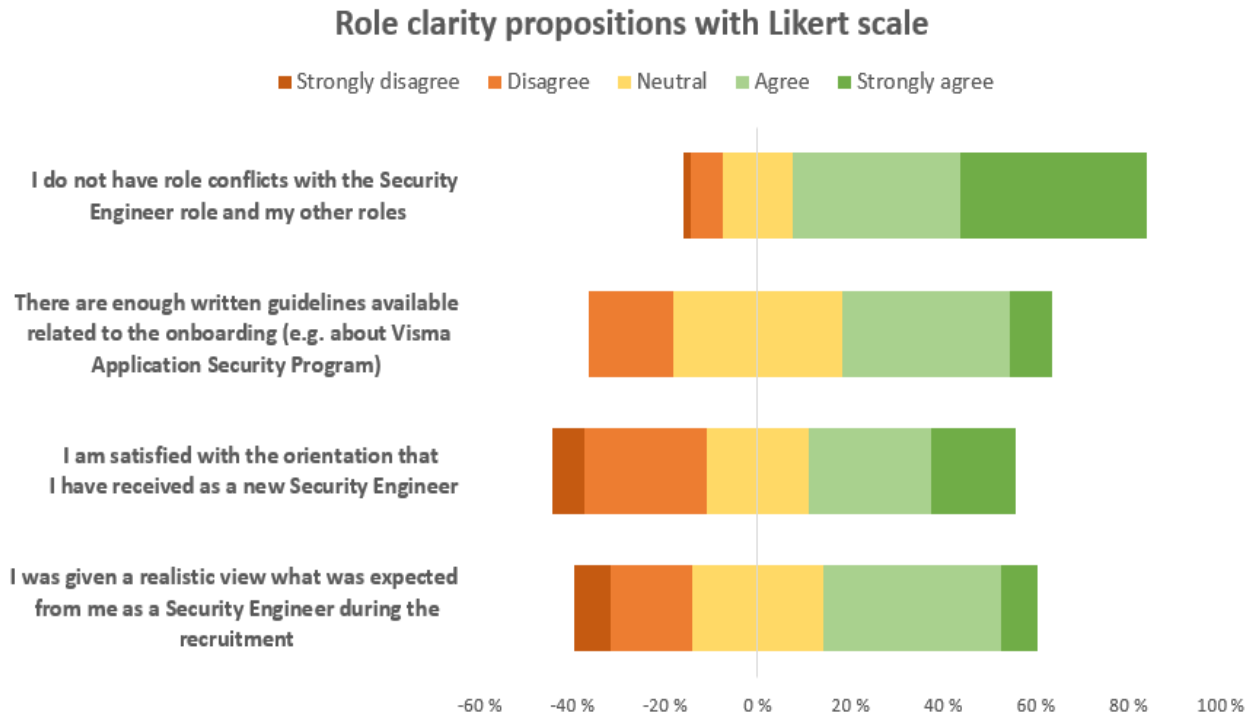


Figure 26. Results from Likert scale questions related to the role clarity.

When finding out how previous experience or how long security engineer had been working as a security affected to the way that security engineers thought on how realistic the role description was during recruitment it was seen that it did not really change the situation if the security engineer was a freshman or if he or she had been working already longer period as a security engineer. This is shown in Figure 27.

Are the told expectations for SEs accurate based on how long the SE has been a SE

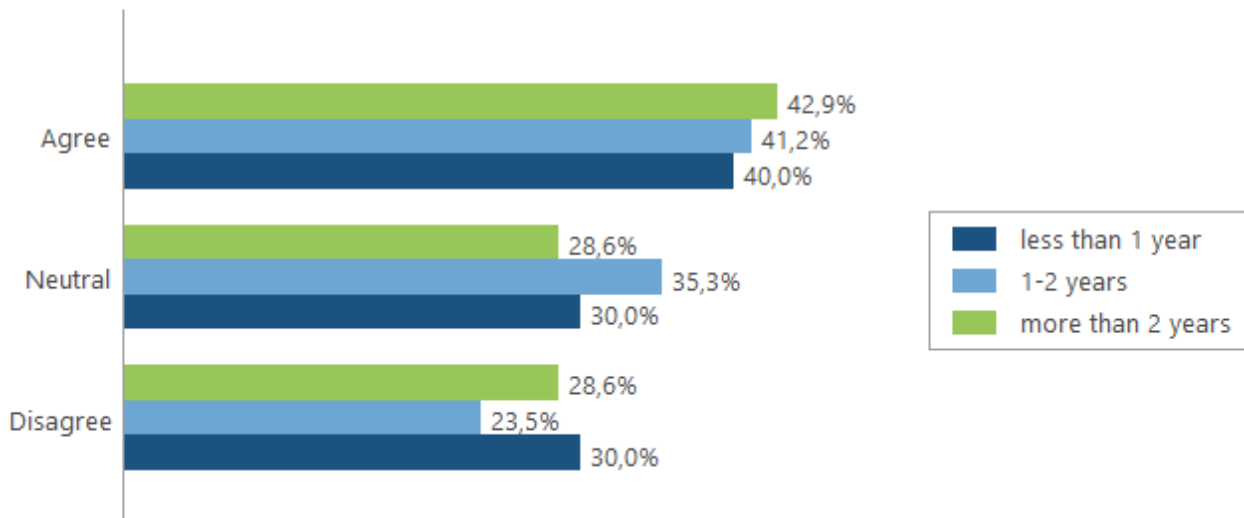


Figure 27. Does the length of the SE career affect how realistic the given view of security engineer role is being considered?

Previous security experience however seemed to have an effect as the security engineers with intermediate security experience thought that the view was not as realistic as 34,6 % both agreed and disagreed when within the security engineers with beginner or no experience almost half thought that the view given to them was realistic and only roughly 22 % disagreed on that. Security engineers with professional security background were left out of the correlation results as they had answered Not applicable to the realistic view of the role question. Figure 28 shows the statistics of this correlation.

Are the told expectations for SEs accurate based on the previous security experience of the SEs

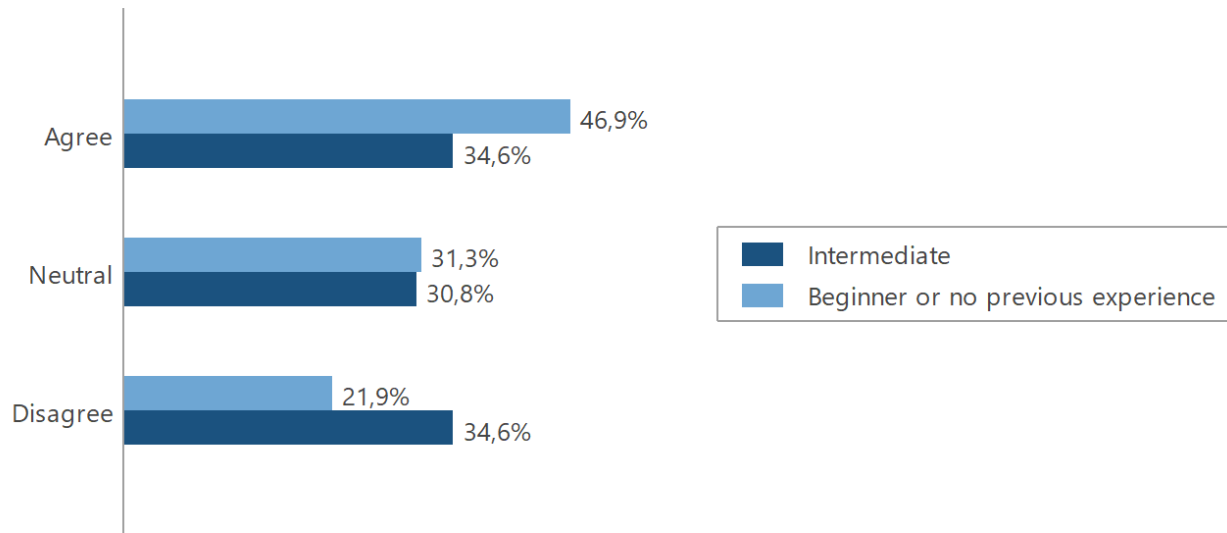


Figure 28. Correlation of previous experience and how realistic view of security engineer role was given during onboarding.

As some of the respondents had formal orientation about the role or/and about the Visma Application Security Program the correlation between formal orientation and how satisfied the security engineers were in orientation was done. Based on the valid results of the survey 37,1 % of respondents had formal orientation about the role and 40 % about the VASP. If we look then how those results correlated to the satisfaction to the orientation it was seen that if formal orientation is given to new security engineers more of them will be more satisfied to orientation in general and that increases the role clarity too. This was seen more clearly when the formal orientation to the security engineer role was considered. Correlations are described more in Figure 29 and Figure 30.

How received orientation about SE role affected to the satisfaction to the orientation.

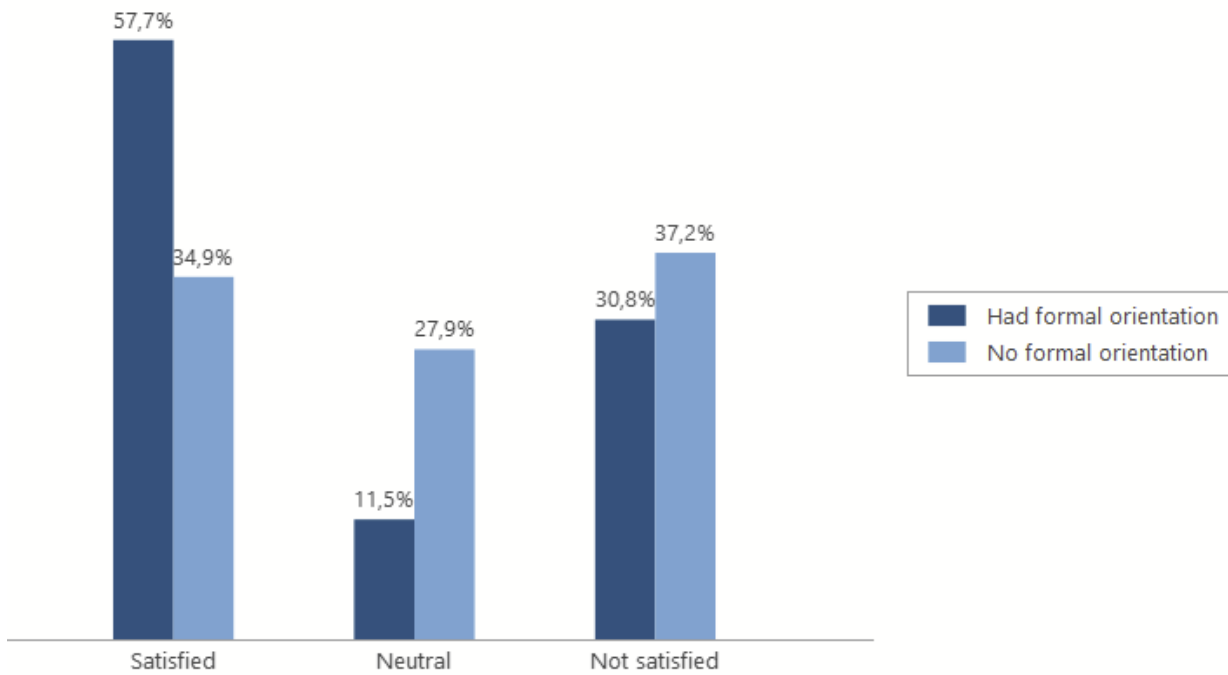


Figure 29. How satisfied the security engineers were to orientation if they had received formal orientation about the role.

How received formal orientation about VASP affected to the satisfaction to the orientation.

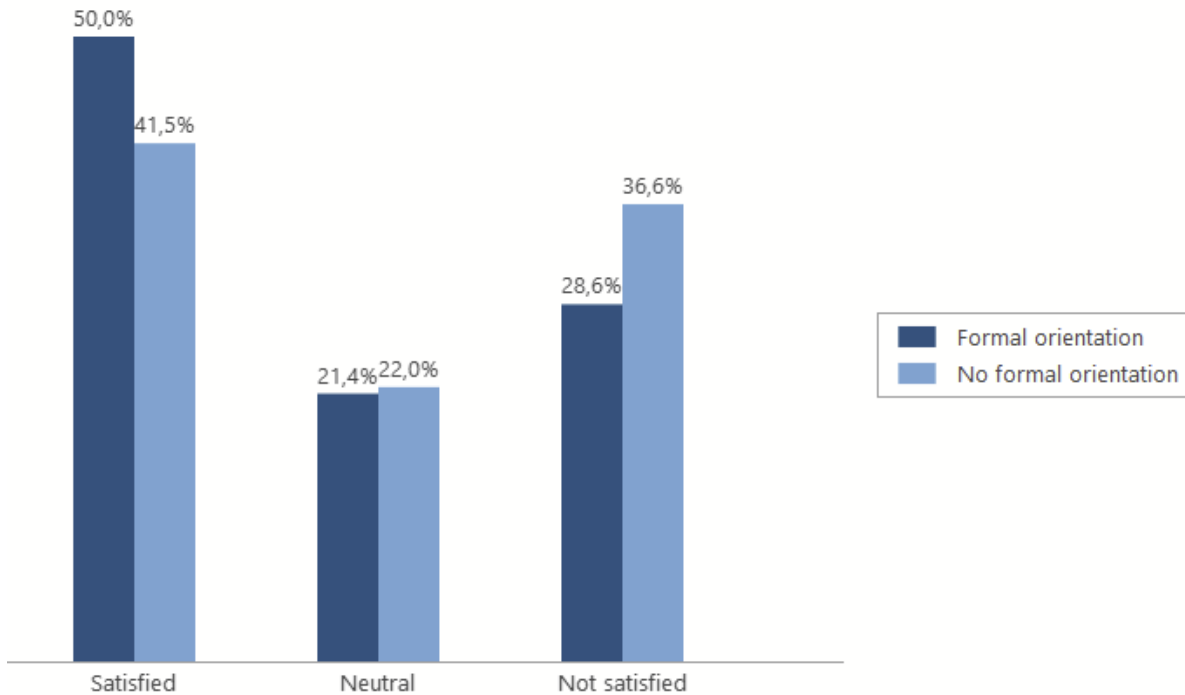


Figure 30. How satisfied the security engineers were to orientation if they had received formal orientation about the Visma Application Security Program.

Little over half of the Security engineers were satisfied with the feedback that they have received as seen in Figure 31. There is cross tabulation with the fact how long the security engineer had been working as a security engineer. The results were quite similar but more senior security engineers seem to a bit more satisfied with the feedback than the newcomers as 42,1 percent of security engineers that had been working in the role under a year in the role were satisfied with the amount of feedback that they had received. Cross tabulation results can be seen from Table 4.

Satisfied with amount of feedback received

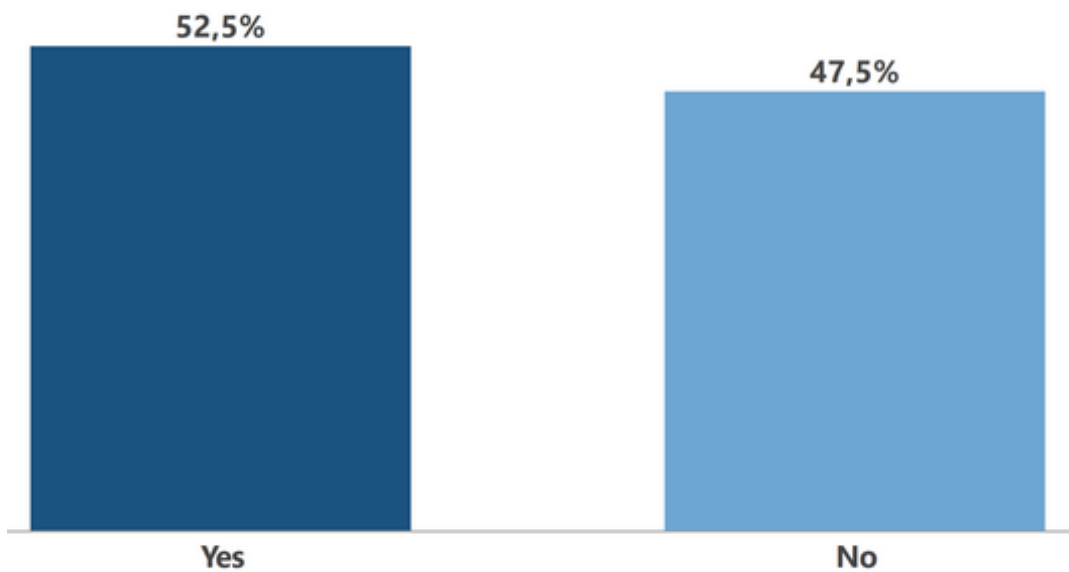


Figure 31 Security engineers' satisfaction to received feedback

Table 4 Crosstab of satisfaction to feedback and how long person had been a security engineer

Satisfied with amount of feedback received	less than 1 year	1-2 years	more than 2 years	Total
Yes	8 (42,1)	11 (61,1)	12 (54,5)	31 (52,5)
No	11 (57,9)	7 (38,9)	10 (45,5)	28 (47,5)
Total	19 (100,0)	18 (100,0)	22 (100,0)	59 (100,0)

Valid cases: 59; Missing cases: 14 (19,2%)

4.4.4 Social Integration

As the security engineer community in Visma is quite large and the Visma group driven function security team is also helping the security engineers actively, security engineers were also asked do they know the available coaching and support activities that are provided to them. By knowing and using those activities the security engineers need to also socialize with others and thus it affects how well they integrate into the security community of Visma. The tools were very well known as shown in Figure 32. Almost nine of ten security engineers were familiar with the security

engineer Slack channel and security engineer guild and the guild meetings. About $\frac{3}{4}$ had directly contacted security team and been also at security awareness meetings. The training platform, Secure Code warrior, was familiar for 68,5 % of the respondents. Through that training platform it is possible to arrange e.g., Capture the Flag (CTF) events, which could also improve the social integration of the rest of the group.

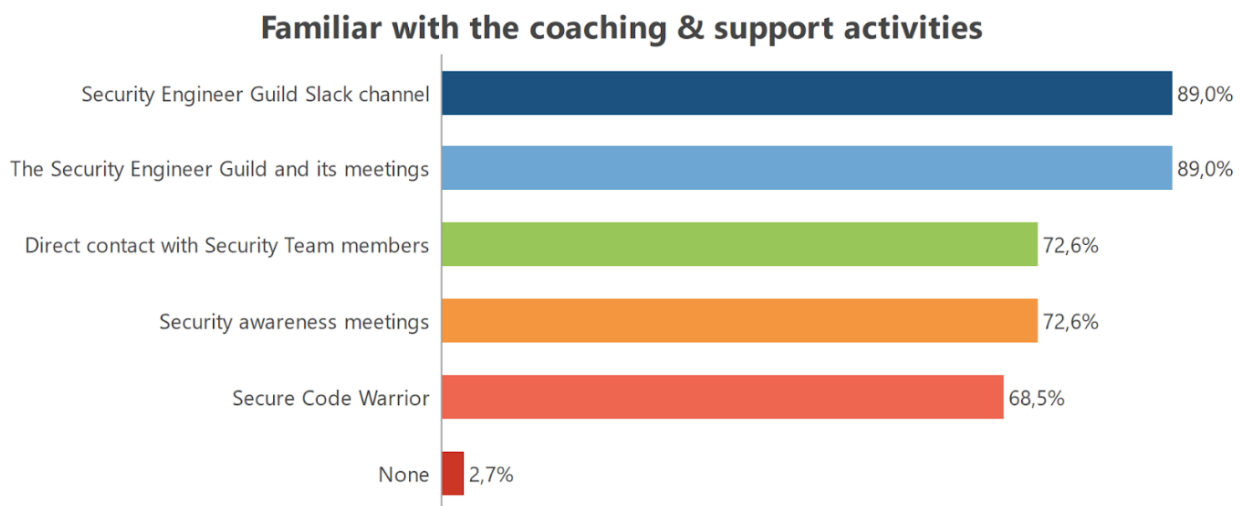


Figure 32. How well the security engineers know the different coaching & support activities.

For communication between the security engineers the most used tool is Slack which is used by 83,1 %. Email and talking at the office were the second and third most used communication channels. Little more than one out ten (12,7 %) do not communicate with other security engineers. More details about the communication channels used are found in Figure 33.

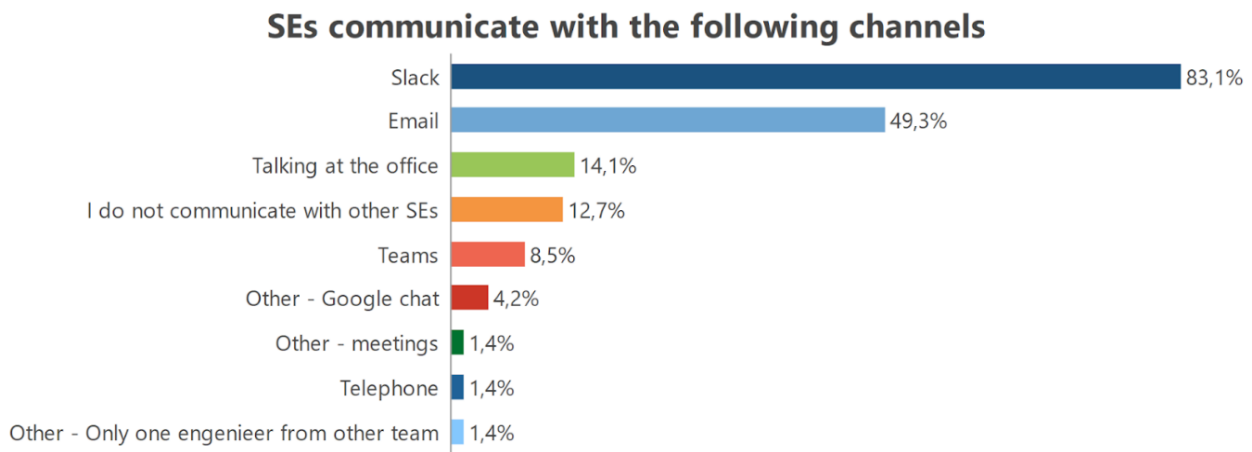


Figure 33. How security engineers communicate with others.

Other individual questions related to social integration are presented in Figure 34. As security engineers know well the support and coaching tools, they also think that they are useful ways to share information and raise awareness. Over half of the security engineers also feel like they belong in a special community working as security engineers, so they seem to have blended quite well into the security engineer community. The Visma security team is also able to promptly help the security engineers if they need help from the security team. Security engineer guild meetings are also thought to be useful. Overall, it seems that the different activities and tools that are now available are working quite well and even though the pandemic is forced to have most of the communication on-line via different services and communication tools.

Social integration related propositions with Likert scale

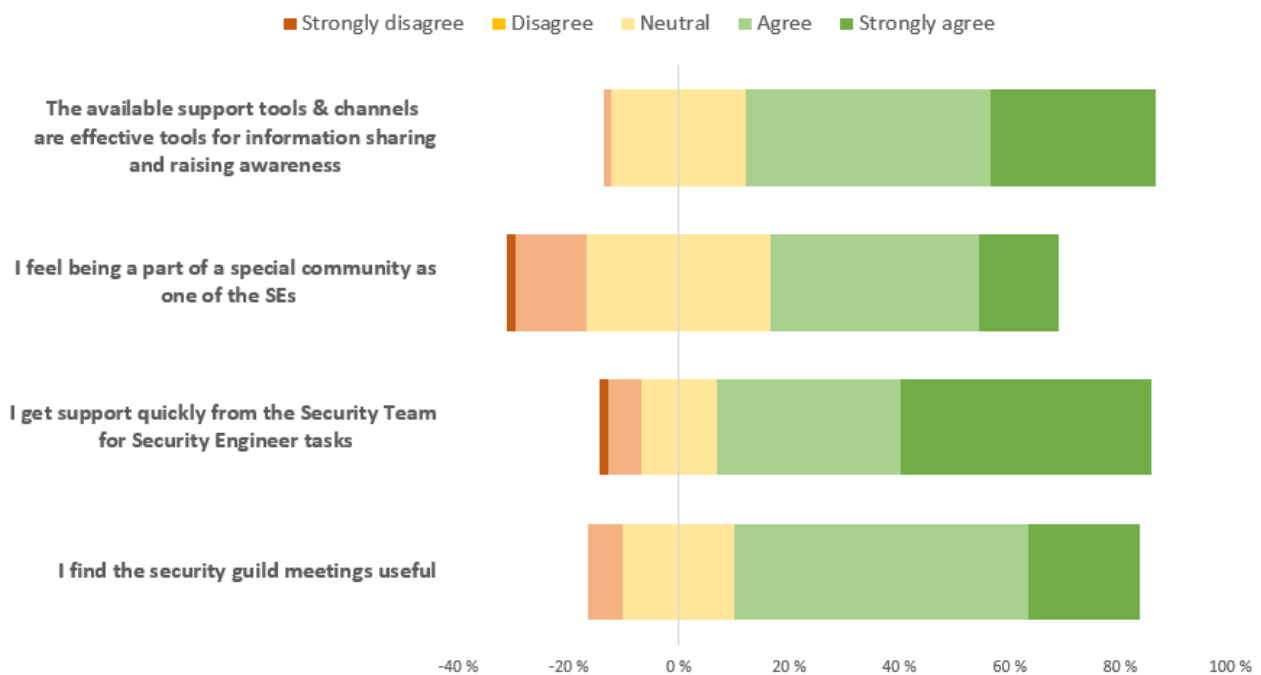


Figure 34 Social integration related propositions with Likert scale

4.4.5 Knowledge of the culture

For this part of the analysis the issues related to whether the security engineers know where to share their opinions or are they asked about them related to the security engineer program were studied in detail. Security engineers were also asked about do they know why they are needed in Visma, what is their purpose?

Three out of four security engineers do know about where to share their opinions about the security engineer program and 52 % of security engineers were asked about their opinions concerning the program. So, there seems to be some room for improvement at least when thinking the how security engineers could be activated more.

General understanding of the need for security engineers was not at such a good level as only about 40 % thought so. Over 22 % disagreed and little less than 38 % could not say did they understand the need or not as shown in the Figure 35. As mentoring seemed to have an effect in the other parts of the successful onboarding, its correlation to this question was analyzed. The results

showed that the security engineers having mentoring does help to understand the meaning of security engineers in Visma (Figure 36).

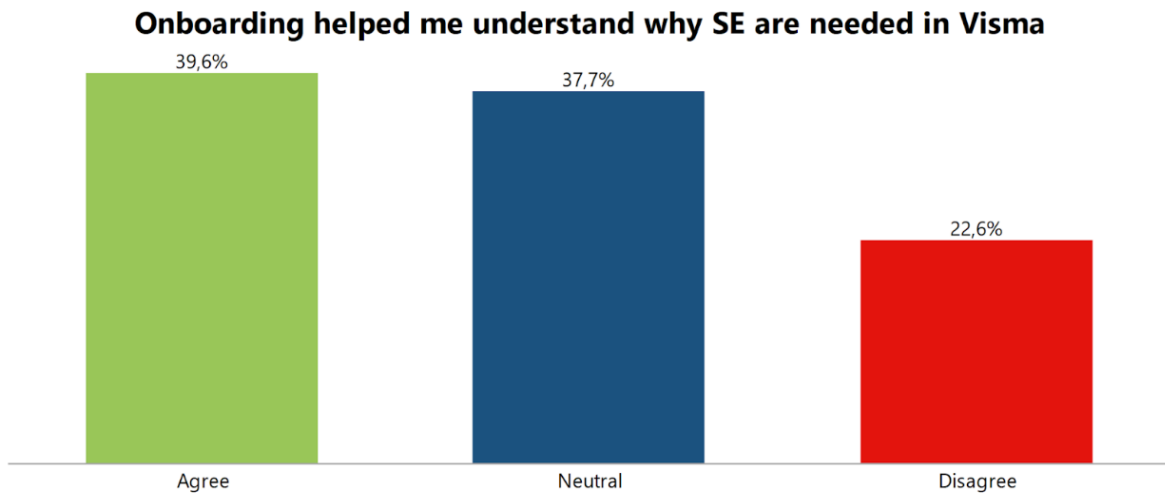


Figure 35. Did the onboarding help to understand why security engineers are needed in Visma?

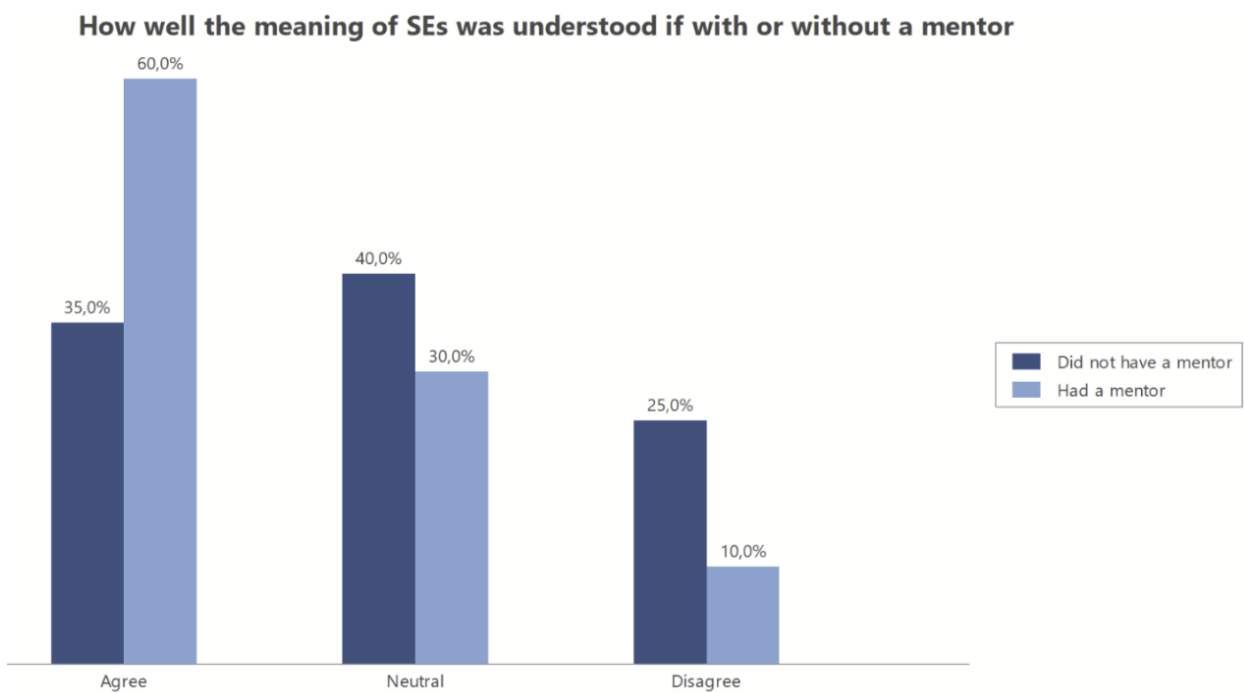


Figure 36. Correlation between mentoring and do the security engineers understand why they are needed in Visma.

The security engineers are quite aware where they can share their thought and ideas on the security champion program in Visma as three out of four security engineers thought so. This is seen in Figure 37. However, over half of the security engineers did think that they are not asked about their opinions on the program so this might be a point of improvement as seen in Figure 38.

I know where to turn to share opinions on the security engineer program, i.e., suggestions for improvement

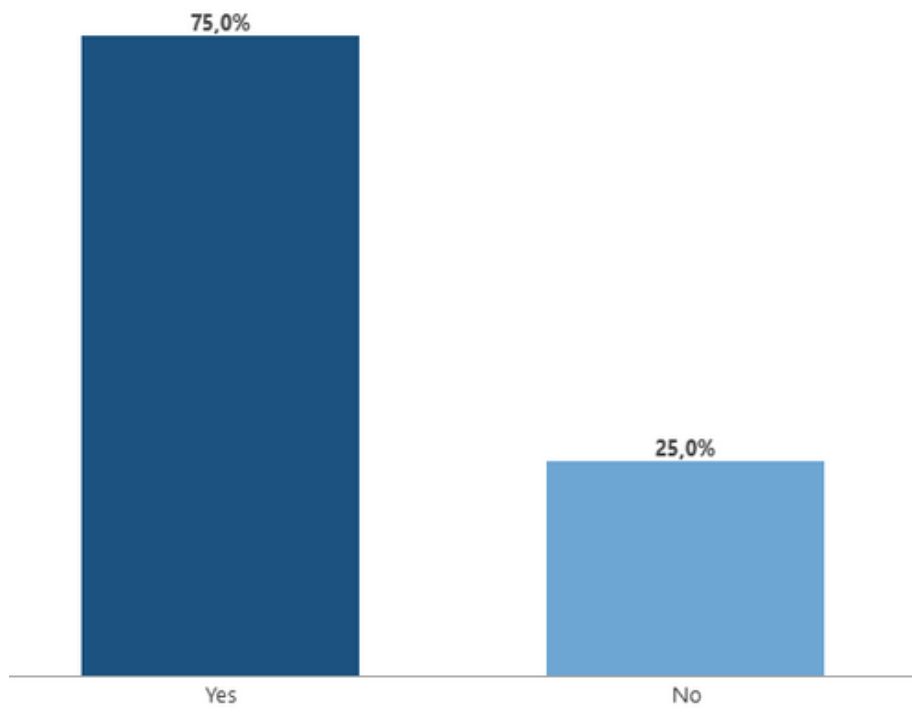


Figure 37 Do security engineers know where they can share their opinions on the security engineer program

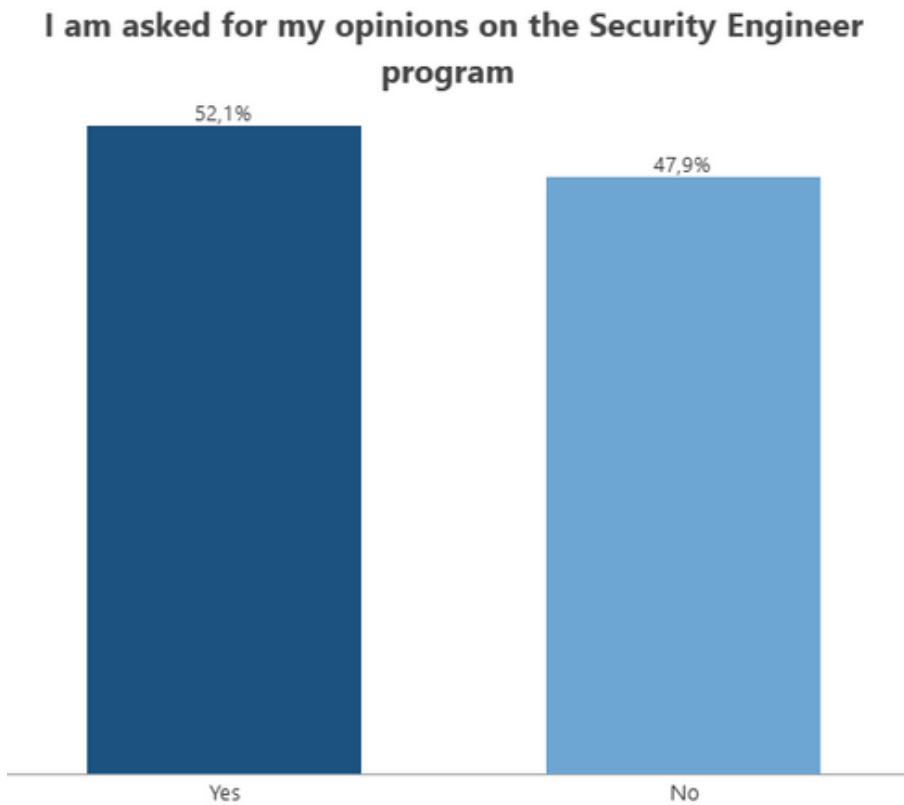


Figure 38 Are security engineers asked for their opinions on the security engineer program.

4.4.6 Analysis of the general improvement questions

The last part of the survey analysis related directly to what kind of thoughts the security engineers have about what should be improved in the onboarding and in the whole security program. Security engineers were also asked about do they think that the onboarding process is clear to them. The most wanted part for improvement was training (67,1 %) and orientation was the second in list (43,8). Coaching & support was in the third place with 38,4 %. Feedback was chosen as the part to be improved by only 5,5 % of the security engineers. Concerning this question, security engineers had the chance to select only two most important parts of the onboarding process. Details about the result of this question can be found in Figure 39

What onboarding functions the SEs want to improve?

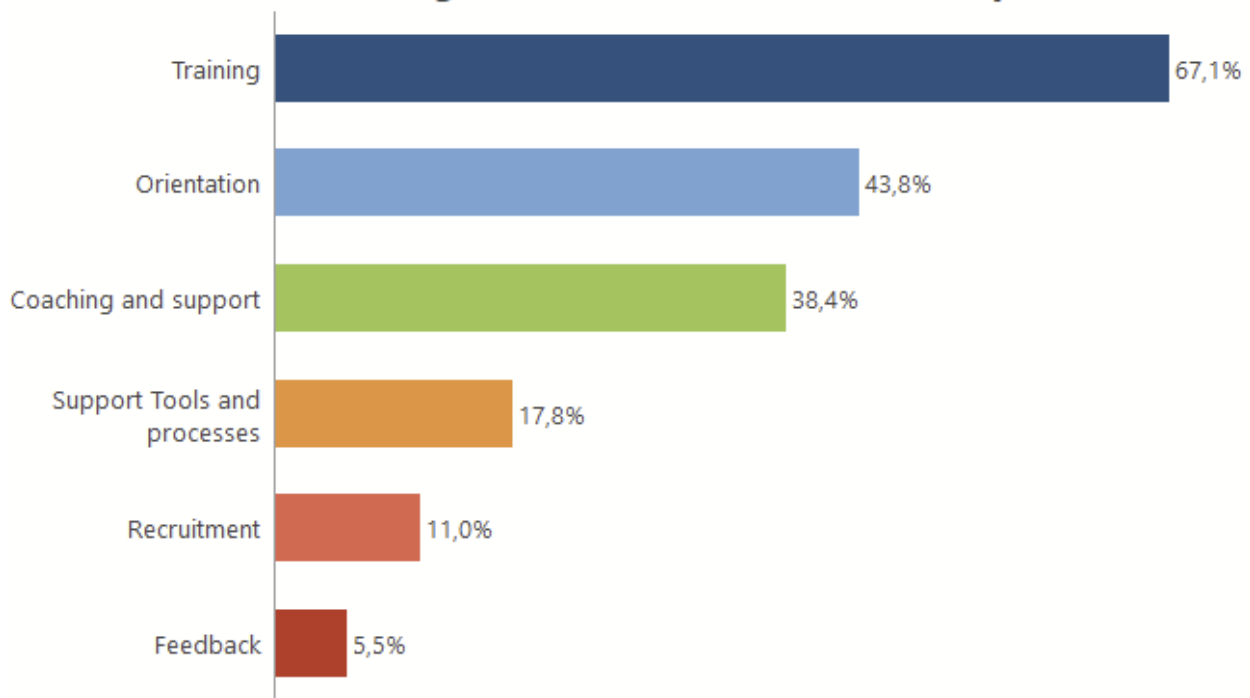


Figure 39. Security engineers would like to improve the following onboarding process functions.

When having crosstabulation with the security engineer experience there was slight difference in the results. Security engineers that had been security engineer for maximum of two years thought that training and orientation are still the two most wanted functions for improvement. More experienced security engineers wanted to improve training and coaching and support. This is seen from Table 5.

Table 5. Crosstabulation between the onboarding function that needs improvement vs. security engineer experience.

Onboarding function	I have been a SE for		
	less than 1 year	1-2 years	more than 2 years
Recruitment	10,6 %	5,0 %	2,1 %
Orientation	27,7 %	27,5 %	17,0 %
Training	38,3 %	40,0 %	31,9 %
Coaching and support	12,8 %	22,5 %	27,7 %
Support Tools and processes	10,6 %	5,0 %	12,8 %
Feedback	0,0 %	0,0 %	8,5 %

When considering the security competence before starting as a security engineer, things change little more. Training was still the first thing to improve when security engineers had less security experience but the security engineers that had already professional security skills wanted improvements to support tools and process the most. The ones with already good security skills did not see that orientation needs improvement at all. Not so competent security engineers see orientation still as the second part that should be improved. For the beginners coaching and support is in shared second place with the orientation as seen in Table 6.

Table 6. Crosstabulation between the onboarding function that needs improvement vs. previous security experience before starting as a security engineer.

Onboarding function	Security competence before starting as a SE		
	Beginner or no previous experience	Intermediate	Professional
Recruitment	5,3 %	7,3 %	0,0 %
Orientation	22,7 %	27,3 %	0,0 %
Training	40,0 %	32,7 %	25,0 %
Coaching and support	22,7 %	18,2 %	25,0 %
Support Tools and processes	5,3 %	12,7 %	50,0 %
Feedback	4,0 %	1,8 %	0,0 %

Most of the security engineers disagreed that the onboarding process is clear as almost half of the security engineers thought so and only 15,2 percent thought that the process was clear. Little less than 40 percent answered neutrally to this question. Figure 40 shows details about this question.

Is the onboarding process for SE role clear?

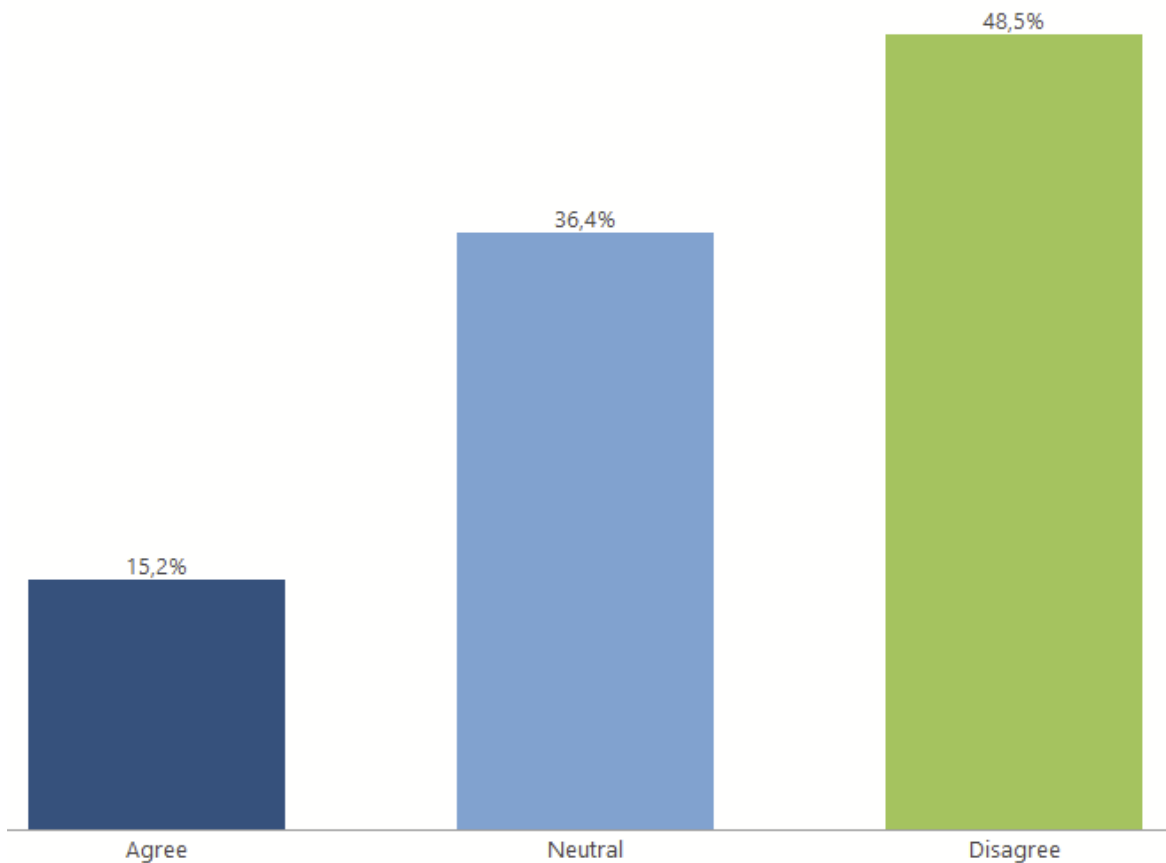


Figure 40. Is the onboarding process for new security engineers clear in Visma.

4.4.7 Summary of the survey results

Basis on the survey results it can be said that most of the security engineers come from development roles and roughly six out of ten security engineers are starting in the role voluntarily. That is good as it seems to be increasing the motivation for the security engineer's tasks. The appointed security engineers were though mostly motivated too so in general lack of motivation of the security engineers is not a big problem.

Concerning self-efficacy, the security engineers are quite satisfied with the resources that they get for SE tasks and for their own performance and they feel motivated too. However, when we look in detail how the onboarding effects to the confidence and the efficiency things are little bit different as there are more security engineers who think that the current onboarding process does not have positive effect on those things. Training (security & softer skills) is the biggest pain point and

probably if there was more training during onboarding it would have a positive effect on confidence and efficiency as well. Security engineers themselves think similarly as training was the most wanted part of the onboarding process to improve when asking about their opinions of what should be improved in the onboarding process. Security engineers that are the most experienced are the unhappiest with the training. Some of the security engineers had a mentor too and that increased the feeling of confidence and efficiency within the security engineers during the onboarding.

The security engineers do not seem to usually have role conflicts with the main role and most of the security engineers are happy with the current written guidelines that are available. The orientation for the role seems to have some flaws as about one out of three security engineers are not satisfied with the orientation that they are given, and it was in second place when security engineers were asked about the parts that need improvement in the onboarding process. It seems that if formal orientation were given, the security engineers would be happier with the orientation. As not all was given a formal orientation there seems to be diversion in how the orientation is arranged for the security engineers.

5 Interview results analysis

Semi-structured interviews were organized after the surveys which were targeted at the whole security engineer population as well. The used interview guide can be found from appendix 2. The purpose of the interviews was to have comments from the security engineers about the pitfalls of the current onboarding process as well the whole security engineer program. This thesis is though concentrating on the onboarding process.

Interviews were done with Microsoft Teams meetings. The interview was recorded and the meeting transcript functionality in Microsoft Teams was used to get the initial transcript of the interview. The interviewees were asked for their consent to process their personal data. Consent was asked during the interviews, and it was based on the consent form found from appendix 3. The initial transcripts were anonymized and then they were imported to MaxQDA software which is a data analysis tool. In MaxQDA the transcripts were corrected as the automatic meeting transcripts that the Microsoft Teams made had typically errors in them. The corrected transcripts were sent

to the interviewees, and they could fix the transcript if they found out that there were errors that needed correction.

Interviewees were selected partly based on the recommendations of the Visma security team and just randomly picking up possible candidates for the interviews by selecting them from two different security engineer lists that the Visma security team provided. In the end the number of people interviewed was 11. The interviewees were all working with different Visma applications, and they were geographically from seven different countries and both men and women were interviewed. Most of the interviewed security engineers were working as part-time security engineers in addition to their main roles, some were full-time security engineers and two of the interviewees have been security engineers but were now working as full-time security team members.

As the survey results pointed out the parts of the onboarding process that needed to be examined more, the interview concentrated more on orientation, training, and the whole onboarding process. Interviews were conducted in collaboration with the NTNU student who researched the whole security champion program so the interview questions included questions concerning the other research too. During the interviews security engineers were also asked about their background information related to their career in Visma and as a security engineer to have more perspective on the onboarding process and its phases.

5.1 Results concerning orientation

During the interviews it was found that the security engineers did not usually receive formal orientation and they would want more information about the role, its objectives, tasks, and responsibilities. They were not certain what they should do and how they should do things. It was seen that security engineers were missing a formal orientation, as well there was uncertainty where to start and where are the needed guidelines. However there seem to be plenty of guidelines and information available for self-studying them but there were problems finding them. Here are few comments from interviewees when asked about the orientation that they had received

Almost none, I think. I was given the link to the Confluence page where You can read about security engineer. And I had on shorter meeting with the former security engineer where we mostly discussed the SSA, since that was the most relevant thing to do at the time. But other than that, not much educational orientation, or onboarding.

Well, a clarity in the role, and expectations of the role. It's always good to have. I always like to know the boundaries of things and what's expected of me. So, I think that's the most important part. So, when You take the role, You know what You're getting yourself into.

I think there's a lot of information if You look for it.

In addition to the details about the role interviewees were also yearning for fundamental training of security or hands-on sessions to get more familiar with the aspects of security. The offensive testing (hacking into some vulnerable example application) workshops that were organized by the Visma security team before the COVID hit the globe, were found very useful. The following quote tell little more about the feelings of the interviewees.

I mean, I know it's not practical because of the corona virus, but 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.

So, in general the interviews proved the similar results as the survey. The security experience before starting as security engineer did seem to have an effect to the satisfaction towards the orientation.

5.2 Thoughts on training

As the training was the most wanted part of the onboarding process for improvement it was gone through in the interviews too. Concerning security related training, the interviewees had had those offensive testing workshops mentioned already in the previous chapter and some had had data protection training, and some had been at security conferences. There were also some internal trainings that was arranged in some legal unit. It seems that there is no common organized training program for the new security engineers, and quite many of the interviewed security engineers did not get any trainings from the Visma security team or their legal unit. However, security engineers seem to do a lot of self-studies. Services like Hack the Box or Tryhackme were mentioned for that.

Security engineers think that it is best to have practical trainings as it was seen that they are the best method of learn new things. Offensive security trainings were thought to increase interest in the security domain as well as it was seen that it will help in convincing others in the development teams to see that they might have real security issues in their applications.

Many interviewees also thought that group training would be a good way to learn. That kind of training is seen increasing the socialization of the security engineers as well it would be beneficial for learning as more experienced persons can team up with beginners and share their knowledge thus it might lower the learning curve for the more inexperienced security engineers. The following quotes present some of the things that the interviewees brought up in concerning the security trainings.

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.

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.

When asked about the softer skills training that the interviewees had not many had had those, just one project management training was mentioned. During the interviews it was seen that the communication aspect as well delegation of tasks to other team members was seen problematic. The challenges with the communication were related to how to speak and present security related issues to different audiences so that they can be understood correctly. Security engineers might need to speak to audiences from top to bottom so they need to know when and how they should express themselves in more technical way and in the other hand in more general way. Correct and appropriate communication of security issues was seen in general as an important thing as it will help convincing others instead of having others think negatively with the message that is communicated. The following quotes present some opinions of the interviewees.

I would need more help with how to convince my team that we need to fix some things.

So being very blunt about things can make the person you're talking to that you're trying to inform, go to defensive stand. And that is not a good thing.

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.

5.3 General improvement of the onboarding process

The things that the security engineers rise in the interviews were mostly related to the onboarding plan or the lack of it. Interviewees talked about that there was not enough information about the role given, there was some problems concerning the VASP program onboarding, fundamental security and VASP training would have been wanted to clarify the tasks the security engineers need to do. There were also mentions that mentors would be good to have during the onboarding process. The following few quotes describe more the situation.

Well, you need to give something at the beginning, so you need to have a dedicated program in mind with some initial steps, maybe some documentation, some videos. So, you should have a plan.

I think I mentioned a little extra training. Yes, I did not get any. No training in tools. No advanced pen testing methods. No Project management, communication, or delegation training.

Sometimes we didn't fully understand the picture because of the lack of knowledge.

To have a person delegated for me like a mentor, that would have been really nice.

5.4 Other findings

During the interviews it was generally seen that the security engineers thought that the VASP program is the security champion program even though it is the used S-SDLC. As the security engineers are typically assigned when a Visma product is enrolled to the VASP program it seems natural as the security engineers will then start to do tasks related to the VASP program.

Security engineer personality and the lack of security competence seemed to have an effect to the socialization factor. Some said that they are very shy, and others said that are just passive participants in the discussions on the slack or the meetings that security team organizes.

6 Successful onboarding or not?

When putting things together based on the survey and the interviews the overall situation based on the Bauer's theory looks like presented in the Figure 41. The color scales go from green (good) to red (not so good). The most problematic attributes of the onboarding process seem to be the self-efficacy and role clarity.

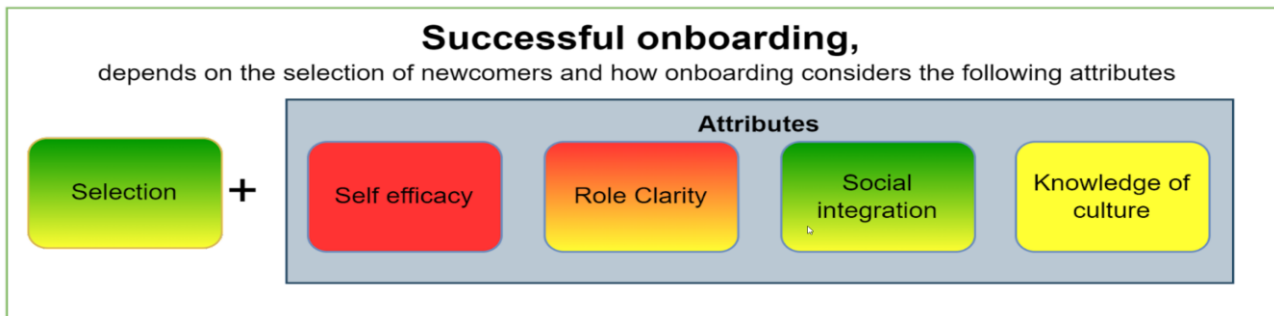


Figure 41. Overall onboarding process status.

6.1 Selection

We can see that the selection seems to be in quite good order. The selected security engineers are mostly from development teams, and they are motivated. It seems that security engineers usually volunteer as they find security interesting. There could however be still more volunteers and the role could be promoted more. As Visma grows a lot by acquiring a lot of companies there could e.g., be some presentation or similar during that process to raise knowledge of the role during that process. There could be more information to the management as well the development teams.

Security engineers tend to grow into the role and want to take more responsibility so a raise in salary with the role might also increase interest to become a security engineer.

6.2 Self-efficacy

Maybe the single most important aspect that was found in the research when thinking the efficiency of the security engineers was that they were lacking in trainings. Most of the security engineers did not have any organized trainings. When thinking that over half of the security engineers

do not have any or just little security experience before starting as a security engineer the combination is not very well functioning. Before COVID Visma security team organized security events for security engineers, but similar events are not organized anymore.

To fix this it is recommended to have some security fundamentals training that could be included in the orientation function as well as some hands-on training to the new security engineers during the orientation or little later during the onboarding. Security fundamentals learning could be an automated course too. The hand-on training could be e.g., basic offensive security based as that will probably motivate and interest people. It would also be good to keep that session as a group training so that the socialization factor would be noted too.

Security team could also gather the recommendations for self-learning (subjects, e-learning platforms) to help the new security engineers on what to study by themselves as some security engineers are struggling with that. Visma Learning Zone could be emphasized as the location as it is already having some information about development paths.

Mentoring was also one thing that improved the confidence and efficiency of the security engineers in their role, and it was also mentioned as very positive thing during the interviews. Mentoring though can be a very expensive solution so there is need to think a plausible solution for that. If legal unit has a more senior security engineer those could help, security team could also arrange maybe virtual Questions & Answers sessions and utilize maybe breakout rooms to have discussions in smaller groups. Or there could be group mentoring where one security team member would mentor a group of security engineers for some time to get them started.

6.3 Role clarity

In Visma a named person must be chosen as security engineer when an application is onboarded to the VASP program and added to the Product Security Catalog. So typically, security engineers are selected then. They then start to onboard to different VASP services and start filling the security self-assessment, SSA. There are written guidelines how to do the onboarding and SSA guides the security engineer forward with the steps in the SSA. Visma security team is also there and help the new security engineers to onboard to the VASP program.

When we look the current recruitment process and how it affects to the role clarity just less than half of the security engineers think that they are given realistic view on the expectations of the role. During the interviews it was seen that the security engineers are struggling with what they should do as security engineers. As discussed earlier the recruitment part could have changes and to clarify things the orientation of the new security engineers should be improved. As survey results show, security engineers with formal orientation are in general happier with the orientation, it is recommended to implement that. There could be e.g., common virtual or physical meetup with new security engineers where the role (objectives, responsibilities) and VASP program could be gone through. In addition to detailed description of the role and VASP there should be information about where different documentation can be found, where You can ask for support etc. And maybe the fundamental security training could be part of the orientation that was mentioned in the chapter 5.2 Self-efficacy. A formal orientation program is also one of the best practices that Bauer (2010, 16) suggest being implemented.

6.4 Social integration

Most of the social integration happens through the security engineer guild channel and the security team organized meetings (security engineer guild meeting and security awareness meeting) and they are very well known. The meetings are mostly informative as their audience might be even few hundred persons. Security team is also highly appreciated, and support can be gotten from them fast with the different communication channels available in Visma. Some legal units have internal meetings with their own security organization and there are also some meetings with different legal team security engineers or developers. Minority of the security engineers have had mentors from their own organizations during the onboarding and that can help to blend in with other security engineers as well the security organization provided by the Visma security team.

Security engineer community was brought up as one strength of the whole security champion program. But there are challenges as security engineers brought up their shyness, or lack of competence in security as well as there were few comments that some security engineers that are appointed do just the minimum that is expected from them and nothing more and thus, they probably are not the most active members of the security engineer guild. It was also brought up that it is easier to discuss with native language.

To ease up the socialization there could be few possible treatments. Mentoring could help here too as mentors would provide an easily approached contact that would be there to help and discuss with. Mentoring though has its own problems that have been already discussed. Security team could also organize those security events or workshops that were found interesting and very useful. Especially teaming and doing challenges with others was found a good way to socialize as you can work as a team and support each other. That can also be a very good learning experience as the team members might be in very different level when considering e.g., the security competence. This kind of teaming or meeting with others would be good in the orientation function of the onboarding process. And of course, there could be more relaxed events. These might not be so easy to arrange as there are so many different legal units and people are working from different countries

One simple treatment could also be to do separate channels for “newbie” security engineers where you could ask even the most basic questions related to the security and the Visma provided development frameworks and then another for the more experienced security engineers. That might encourage the new security engineers to discuss more with others. And the formal orientation program could help here too as it would give more confidence to the newcomers.

Internal meetings could also be a good way to gather people interested in security and discuss e.g., what kind of issues there has been on-going with VASP or some else concerning security. It could be also a place where mentoring happens. However, this probably needs to be done in the legal units. Security team could however help if legal unit has only single security engineers so that there could be a meeting with more than one legal unit.

6.5 Knowledge of culture

As Visma as a big SaaS provider takes the security of its services seriously. The security organization and the VASP program as well other development frameworks support the high targets for security. During the onboarding process, the aspects of security in Visma culture are brought up when onboarding to the VASP program. Security engineer learns by taking the necessary steps with the VASP program. But still there seemed to be problems to understand why the security engineers are needed in Visma. As a positive observation the security engineers know very well where they can tell opinions about the security champion program.

Visma security team organizes yearly surveys for security engineers about the security engineers, but it might be so that these do not reach security engineers during the onboarding as the survey is sent annually. The survey might be missed anyway as the information about the survey as it is not directly sent to security engineers but information about it is posted to security engineer guild slack channel or Visma Space. Security team conducts more thorough interview-based research in every second or third year about how security engineer program should be improved.

These might be the reasons why almost half of the security engineers are not getting any feedback from their doings as security engineers, or they are not satisfied with the amount of feedback they get. If the feedback could be improved that would probably improve the knowledge of culture too.

One way of improving the feedback during the onboarding process Bauer's (2010, 16) theory suggests using milestones so that the progress and needs of newcomers would be considered more. This could also be done as survey and arrange a virtual or physical meeting depending on where the security team member and security engineer are located.

Other thing that could be thought of is to have those steps that the new security engineer should take in the development discussions of an employee where the annual targets and objectives as things related for competence growing are gone through. This way security team could communicate the needs and objectives of the security engineers to their managers thus it would improve the collaboration between the security team and different Visma legal units.

As for the yearly surveys it is suggested to send information about the survey directly to the security engineer (email, direct message in some other communication channel) to ensure that the information about the survey reaches its targets. Another thing that can improve the situation too based on the survey is mentoring.

7 Discussion

Visma as a company proved to be a fruitful target for the research that was conducted. Visma has a very comprehensive S-SDLC with the VASP program and means for measuring the security which will improve the security situation in applications that onboard to that. And as Visma organization

structure includes a lot of partly independent legal units this kind of approach ensures that security and data protection is done in a homogenous way with the applications that Visma develops.

In addition to the VASP program, Visma has another development framework, Visma Cloud Delivery Model or VCDM, for applications that utilize public cloud infrastructure like Microsoft Azure or Amazon Web Services. VCDM is ISO27001 certified and has ISA3402 type 2 assurance statement. Only the security engineers that are assigned to an application running the VCDM program have official role description. As only about 15 % of the Visma applications are in the VCDM program the majority of the security engineers might be confused about their role as they do not have their role described. VCDM applications need to also be enrolled in the VASP program, and they have stricter requirements on the target tier in it. In general security engineers are not supposed to be security engineers but they are rather thought of being “spy” or “infiltrator” that will eventually change the way the development teams think and act with security requirements and issues.

Visma security team has the responsibility on the VASP program as well as the security champion program in Visma. Security team works as a matrix organization across the different Visma legal units and provides the necessary security services used within VASP to the legal units. Security team is also responsible to for arranging guidelines, discussion forums (e.g., Slack channels), feedback gathering and support for legal units’ security champions through the security champion program. Legal units can have in addition more support for their security engineers e.g., it is possible to have more senior security engineer as a mentor or the legal unit arrange trainings for their own security engineers. But in the end Visma security team a key role in Visma when the security of the Visma applications is considered as the development frameworks, security tools and the security champion program are all owned by the it.

When thinking how applicable of the research results are to other organizations it is good to bear in mind that Visma has very detailed and thought secure development frameworks and tools and guidelines which helps a lot when the frameworks are being implemented in applications. The security team is also very capable and ensures that the development teams mostly need to consider how to deal with the findings the services related to the frameworks instead of maintaining them or investigating how they work. Security team is also very capable and helps the development

teams when necessary and provides general guidelines to all different Visma legal units. These aspects may affect how well the results of this research can be generalized in other organizations as there the security champions might need to do such tasks as their tasks in other organizations where there are yet not such comprehensive frameworks implemented and security team is not so capable.

As for conducting the research in collaboration with another student was fruitful as it made possible to change ideas and there was also another person's perspective available. Collaboration made it possible to divide the workload conducting both the survey and the interviews and interpreting the results even though both students had their own topics for the research. When concerning the ethical issues related to this thesis and the research conducted, the Ethical Principles for JAMK University of Applied Sciences Approved by the Student Affairs Board on 11 December 2018 were followed. When thinking the privacy issues during making of the thesis, the of the survey respondents was guaranteed by not gathering any personal data that could be linked to a single person in the survey results. For the interviews automatic transcripts were used in Microsoft teams. The produced transcripts were anonymized when the transcripts were saved to MaxQDA for further analysis. In the end the data being processed in the MaxQDA was anonymized. Only the writer of this thesis and the student of the NTNU and their supervisors were granted access to the transcripts. Interviewees were also asked about their consent for processing their personal data. During that their rights e.g., having copy of the transcript were gone through. More information about the consent is found from Appendix 3. The survey and interview data will be deleted latest in the end of July 2022.

During the study, it was actively discussed with the host organization how to do the surveys or the interviews so that it was ensured that the research was made by the book. It was also discussed with the host organization that the thesis will be publicly available after its publication and the thesis was reviewed by the host organization. During the writing of this thesis the referencing guidelines of JAMK have been followed.

When doing a self-reflection of the thesis and thinking what could be improved in it, the review part of different onboarding process theories is quite narrow, and it could have been wider to have better view on them. There is a lot of information about Software Development Life Cycle

and the Visma secure implementation of that and that might be not so relevant. On the other hand, the Visma Application Security Program is the first thing that the security champions will be doing after they start in their role, and it is then an important part of the onboarding. Another negative thing is that the thesis does not have very much information about previous studies although the used theory is based on many studies from the subject. The structure of the thesis might not be optimal either so that is one aspect to consider when doing similar studies later. When considering the research itself it was not found that similar study that concentrates on security champions was not conducted before. So, in that light the study might provide some advice what should be considered when security champions are being onboarded to ensure their capabilities in their new role.

7.1 Research questions

R1 How to improve the onboarding process of security champions using existing onboarding theories?

The Bauer's research-based theory provides a solid and easy to understand framework for developing an onboarding process. It points out clear functions that should be addressed in the onboarding process and presents the parts that affects to the overall success of the onboarding process. The theory presents the short- and long-term effects that can be seen during and after the onboarding. When thinking the onboarding of the security engineers using the best practices and concerning all the functions defined in the theory can be seen beneficial. For example, it was seen that the security champions would want to have more structured way (onboarding plan) of the onboarding with clear steps how to move forward with the onboarding and the tasks and responsibilities concerning their new role. This is a fact that should be emphasized more as the security champions are typically not security experts when beginning in their role and as security domain is large and complicated a push to the right direction will become really handy for them. This recommendation fits in all the organizations that are running a security champion program.

R1.1 What onboarding process theories exist for onboarding?

During the research it was found that onboarding theories exists and that is a subject that has been researched already for a long time. For the research Bauer's research-based theory was chosen to be the basis as the research. There are a lot of other theories as well and within this re-

search Van Maanen's & Schein's (1979) "Toward a theory of organizational socialization" was examined a bit as it is very commonly used and cited in very many later studies related to onboarding process of new employees.

R1.2 What are the parts of the onboarding of the new security champions that need the most attention?

As this research was conducted only in the Visma group the results are more specific for that organization and situation might be different in other organizations. During the research it was found that the orientation and training were the key points that need improvement in the Visma implementation. Coaching & support was not very far at third place and that is also one thing that could be improved.

R1.3 What improvements can an onboarding theory bring to the current security champion onboarding process in use?

Maybe the most important thing to consider is to think the onboarding process as a bigger thing and have clear steps for it. It was seen that the current implementation of the onboarding to the security champion role is not clear and security champions want to have more defined steps to follow. They want to know what they should do next within the onboarding, when and what kind of orientation they will have, what training they shall have or what they should self-study, where they can find guidelines and who they can contact etc. Responsible organization or the owner of the security champion program is recommended to think all the functions described in the process and have a rational implementation of them. Used onboarding theory also suggests some best practices or other advice that can be followed e.g., formal orientation and mentoring. During the conducted research mentoring was found to have positive effect in the confidence and efficiency and in the interviews, it was discussed often as a thing that could improve the onboarding

7.2 Reflections with previous studies

The results of this thesis reflect in a similar way with the other onboarding studies. Even though the previous studies were done for software developers the situation is somewhat similar in this thesis as most of the security champions have their main role in a development team. Well defined onboarding plan with exact steps for newcomers was also seen as good thing in the study made by Britto et al. (2018). At same time there should be enough (Britto et al., 2018) and up to

date information available for new employees or role changers (Herzig et al., 2021). Herzig et al. (2021) recommends for example, that there would some initial meetings where newcomers are given a general view of the expectations and their new role and that the newcomers would get feedback on their progress continuously during the onboarding. Ford et al. (2021) have more ideas on the socialization side they encourage to have e.g., mentoring in a couple of ways and in making communication simple and frequent with others as when working remotely so that it can be done at a low threshold. So, they present also quite similar recommendations compared to this thesis. The studies can provide other recommendations that could also be utilized and it could be beneficial to look them through when thinking other improvements to onboarding process.

7.3 Ideas for further investigation

As the research was conducted for only the security engineers and the different responsibilities between Visma security team and the different legal units was not really examined thoroughly it might be good to somehow investigate more how well the management of the legal units are aware of the current onboarding process of the new security engineers. There might be some points where the responsibilities are not clear getting more information on that situation might also prove useful. When thinking well maintained cyber security, committed management is one key aspects of it and it would be interesting to know how well that achieved when the onboarding of new security champions is considered.

8 Conclusion

As typically security champions do not have security background and information and cyber security as a domain is wide and not the easiest one to understand, it seems to be a good practice to have carefully thought and comprehensive onboarding process for them. This was seen by the research conducted in this thesis as most of the security champions were just beginners on cyber security when they started as security champions. Well-functioning onboarding can increase the confidence and efficiency of the security champions in their role. The used onboarding process theory used in this research has many good best practices which help in planning the whole onboarding process and seem to fit also when thinking of the onboarding of new security champions. It however depends on the organization and how thoroughly the cyber security is already

thought what means or best practices are wise to be implemented to improve the onboarding process.

References

- Bauer, T.N. (2010). Onboarding new employees: Maximizing success. Alexandria, VA: SHRM Foundation
- Beck, K., Beedle, M., van Bennekum, A., Cockburn, A., Cunningham, W., Fowler, M., Grenning, J., Highsmith, J., Hunt, A., Jeffries, R., Kern, J., Marick, B., Martin, R. C., Mellor, S., Schwaber, K., Sutherland, J., Thomas, D. (2001a). Manifesto for Agile Software Development. Retrieved from <https://agilemanifesto.org/>
- Beck, K., Beedle, M., van Bennekum, A., Cockburn, A., Cunningham, W., Fowler, M., Grenning, J., Highsmith, J., Hunt, A., Jeffries, R., Kern, J., Marick, B., Martin, R. C., Mellor, S., Schwaber, K., Sutherland, J., Thomas, D. (2001b). Principles behind the Agile Manifesto. Retrieved from <https://agilemanifesto.org/principles.html>
- Birsan, A. (2021). Dependency Confusion: How I Hacked Into Apple, Microsoft and Dozens of Other Companies. Medium. Retrieved from <https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610>
- Boehm, B. (1988). A Spiral Model of Software Development and Enhancement. Retrieved from <http://www-scf.usc.edu/~csci201/lectures/Lecture11/boehm1988.pdf>
- Britto, R. , Cruzes DS, Smite, D. & Sablis, A. (2018). A. Onboarding software developers and teams in three globally distributed legacy projects: A multi-case study. *J Softw Evol Proc.* 2018; 30:e1921. <https://doi.org/10.1002/smr.1921>
- Burt, T. (2021, March 2). New nation-state cyberattacks. Microsoft Corp. Retrieved from <https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/>
- Cody A., Orebaugh, A., Scarfone, K., Souppaya, M. (2008) SP 800-115 - Technical Guide to Information Security Testing and Assessment. 2008. National Insitute of Standards and Technology, NIST. Retrieved from <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf>
- Corfield, G. (2021, April 15). It was Russia wot did it: SolarWinds hack was done by Kremlin's APT29 crew, say UK and US. *The Register*. Retrieved from https://www.theregister.com/2021/04/15/solarwinds_hack_russia_apt29_positive_technologies_sanctions/
- Creative Research Systems. (2012). Sample Size Calculator. Retrieved from <https://www.surveysystem.com/sscalc.htm>
- Cruzes, D. S., & Johansen, E. A. (2021). Building an Ambidextrous Software Security Initiative. In M. Mora, J. Gómez, R. O'Connor, & A. Buchalceková (Ed.), *Balancing Agile and Disciplined Engineering and Management Approaches for IT Services and Software Products* (pp. 167-188). IGI Global. <https://doi.org/10.4018/978-1-7998-4165-4.ch009>
- Dooley, J. (2011). *Software Development and Professional Practice* (1st ed. 2011.). Apress.
- HackerOne. (2017). The Hacker-powered security report 2017. HackerOne. Retrieved from <https://ma.hacker.one/rs/168-NAU-732/images/hacker-powered-security-report-2017.pdf>

Herzig, K., Ju, A., Kelly, S. & Sajjani, H. (2021). A Case Study of Onboarding in Software Teams: Tasks and Strategies. 2021 IEEE/ACM 43rd International Conference on Software Engineering (ICSE), 2021, pp. 613-623, doi: 10.1109/ICSE43902.2021.00063.

IBM. (2008). A history of progress - 1890s to 2001. Retrieved from https://www.ibm.com/ibm/history/interactive/ibm_history.pdf

Intel & Analysis Working Group. What is Cyber Threat Intelligence? CIS, Center for Internet Security. Retrieved from <https://www.cisecurity.org/blog/what-is-cyber-threat-intelligence/>

Jaatun, M. G., & Soares Cruzes D. (2021). Care and Feeding of Your Security Champion, 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2021, pp. 1-7. <https://doi.org/10.1109/CyberSA52016.2021.9478254>

Jones, R. (1986). Socialization Tactics, Self-Efficacy, and Newcomers' Adjustments to Organizations. *AMJ* 29(2), 262–279. <https://doi.org/10.5465/256188>

Kananen, J. (2015). Online research for preparing your thesis: A guide for conducting qualitative and quantitative research online. JAMK University of Applied Sciences.

Merriam, S. B. & Tisdell, E. J. (2016). *Qualitative research: A guide to design and implementation* (Fourth edition.). Jossey-Bass.

Mohapatra, P. K. J. (2010). *Software engineering: (a lifecycle approach)*. New Age International.

Noopur, D. (2005). *Secure Software Development Life Cycle Processes: A Technology Scouting Report*. Carnegie Mellon University. <https://apps.dtic.mil/sti/pdfs/ADA447047.pdf>

NCSC, National Cyber Security Centre. (2017, August 8). *Penetration Testing*. National Cyber Security Centre. Retrieved from <https://www.ncsc.gov.uk/guidance/penetration-testing>

OWASP a. *Source Code Analysis Tools*. OWASP Foundation. Retrieved from https://owasp.org/www-community/Source_Code_Analysis_Tools

OWASP b (Alexander Antukh). *Security Champions Playbook v 2.1*. <https://github.com/cOrdis/security-champions-playbook>

Ford, D., Houck, B., Rodeghero, P. & Zimmermann, T. (2021). Please Turn Your Cameras on: Remote Onboarding of Software Developers During a Pandemic. 2021 IEEE/ACM 43rd International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP), 2021, pp. 41-50, doi: 10.1109/ICSE-SEIP52600.2021.00013

Royce, Winston W. (1970). *Managing the development of large software systems*. University of Southern California. Retrieved from <http://www-scf.usc.edu/~csci201/lectures/Lecture11/royce1970.pdf>

Scrum Alliance. (2020). *The Scrum Framework At a Glance (Version 5.0)*. Retrieved from https://www.scrumalliance.org/ScrumRedesignDEVSite/media/ScrumAllianceMedia/Files%20and%20PDFs/VER5-scrum-framework_2020.pdf

Stober, T. & Hansmann, U. (2010). *Agile Software Development: Best Practices for Large Software Development Projects* (1st ed. 2010.). <https://doi.org/10.1007/978-3-540-70832-2>

Urduan, T. C. (2005). Statistics in plain english. Lawrence Erlbaum Associates, Incorporated.

Valli, R. & Aarnos, E. (2018a). Ikkunoita tutkimusmetodeihin: 1, Metodien valinta ja aineistonkeruu : virikkeitä aloittelevalla tutkijalle (5., uudistettu painos.). PS-kustannus.

Valli, R. & Aaltola, J. (2018b). Ikkunoita tutkimusmetodeihin: 2, Näkökulmia aloittelevalla tutkijalle tutkimuksen teoreettisiin lähtökohtiin ja analyysimenetelmiin (5., uudistettu painos.). PS-kustannus.

Van Maanen, J., & Schein, E. (1979). Toward a theory of organizational socialization. In B. Staw (Ed.), Research in organizational behavior (Vol. 1, pp. 209-264). Greenwich, CT: JAI Press

Vilka, H. (2007). Tutki ja mittaa: Määrällisen tutkimuksen perusteet. Tammi.

Visma group a. Over two decades of software innovation. Retrieved from <https://www.visma.com/organisation/history/>

Visma group b. Work smarter with innovative software. Retrieved from <https://www.visma.com/software-solutions/>

Visma group c. Visma brand – Vision & Mission. Retrieved from <https://brand.visma.com/vision/>

Walker A. (2019, August 14). SAST vs. DAST: Application Security Testing Explained. G2 Research Hub. Accessed 23 March 2021. Retrieved from <https://research.g2.com/insights/sast-vs-dast>

Appendices

Appendix 1. Security engineer survey structure and questions

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 at the end of 2022. If you have any questions about the survey, please contact me by email (xxxx.xxxx@xxxx.xxxx)

Please submit your response before 15/02/2022.

Background information

1. I have been a Security Engineer for *

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

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

- Beginner or no previous experience
- Intermediate
- Professional

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

- Developer
- Tester / Quality Assurance Specialist
- Architect

- Other:

Becoming a Security Engineer

4. I became a Security Engineer because *

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

5. Please answer the following propositions. *

Options for each proposition: Strongly agree | Agree | Neutral | Disagree | Strongly disagree |

N/A

- I was given a realistic view of 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

6. Please answer 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

7. 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)

8. 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:

9. Please answer 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 resources provided to help me in my role as a Security Engineer

Feedback

10. Please answer 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

11. Please answer 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

12. Please answer 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

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

- Recruitment
- Orientation
- Training
- Support Tools and processes
- Coaching and support
- Feedback

14. 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:

15. 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 2. Interview guide

ID	Question
Q1 General information	
Q1.1	What is your main role in Visma?
Q1.2	For how long you have been a SE?
Q1.3	What was your security competence before starting as a SE?
	How were you recruited to the SE role? Volunteered or appointed?
Q1.3	If volunteered: What made you volunteer for the SE role?
Q1.4	How much time do you usually (weekly) spend on SE tasks?
Q1.5	Can you describe what kind of tasks you do as a SE?
Q1.6	How do you fit your SE role into your daily activities?
	How do you prioritize your tasks?
	Do you prioritize working on your everyday tasks before your SE tasks?
Q1.7	Do you procrastinate your SE tasks more than your other tasks?
Q2 Orientation	
	Did You receive any orientation on how to do Your work as a Security Engineer?
Q2	Follow-up: Was it enough? What would You do otherwise?
Q3 Training	
	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?
Q3.1	Follow up: What do you think would be useful to learn instead?
	And now that you have worked as SE for a while, have you received any additional training?
Q3.2	What do you think about it?
Q4 Coaching and Support tools	
Q4.1	Coaching and support tools (Guild and its meetings, Guild slack channel, Security team support, Security awareness meetings) were the third functions that Security engineers would want to improve. Are you satisfied with them?
Q4.2	Is there something you would want to change in the current activities or add something else to improve the situation?
Q5 Communication	
Q5.1	While continuing to work as a SE, do you have much communication with other SEs? About what?

	<p>Do you ever reach out to more experienced SEs for advice?</p> <p>Do other SE reach out to you for advice?</p>
	<p>Do you participate in internal SE meetings (not security guild meetings, but internal for your legal unit/department) and do you find these meetings useful?</p> <p>Why do You find them useful?</p>
Q5.2	If not: Is this something that you would like to have?
Q6 Summary	
	<p>What do you think is the key to success for the SE program in Visma? What is the best thing about the program?</p> <p>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.</p>
Q6.2	Is there anything you do not like about the program?
Q6.3	Is there something that You would like change to make the whole onboarding process more efficient?

Appendix 3. Consent form for processing personal data

Consent for processing your personal data

The purpose for the data processing

The purpose of the processing is to research the current security engineer program and the onboarding of new security engineers. Research results will be used in two master's theses which will be published later this year.

We process the following personal information

- Name (First name & Last name)
- Work Email address
- And the answers to the interview questions concerning different aspects related to your security engineer role

Storing and using the data

- Recording of the interview
- Recording of the transcript
- The MaxQDA program will be used to transcribe the recordings. The results are used for analyzing the interview data. Actual personal data will not be stored in MaxQDA. MaxQDA thus stores only anonymized data.
- Microsoft Teams is used to keep the interviews
- Both students and their supervisors can access the MaxQDA data.
- No personal information will be included in the final publications.

When data will be deleted

- The personal data stored for processing will be deleted at the end of July 2022.

Your rights as a data subject

- The recording of the interview and the transcript based on the interview will be shared with You

- You have the right to correct the personal data based on the recording and the transcript.
- You have the right to have your personal data deleted

You can send a complaint about the processing activities to [contact person in NTNU],
nnnn.nnnn@ntnu.no