Security Champions Without Support: Results from a Case Study with OWASP SAMM in a Large-Scale E-Commerce Enterprise

Marco Gutfleisch
Ruhr University Bochum, Germany
marco.gutfleisch@rub.de

Markus Schöps
Ruhr University Bochum, Germany
markus.schoeps@rub.de

Stefan Albert Horstmann
Ruhr University Bochum, Germany
stefan-albert.horstmann@rub.de

Daniel Wichmann
Ruhr University Bochum, Germany
daniel.wichmann@mailbox.org

M. Angela Sasse
Ruhr University Bochum, Germany
angela.sasse@rub.de

ABSTRACT

Developer-centered security research has identified a variety of reasons why software developers do not follow recommended security practices: lack of knowledge, outdated information sources, time pressure, and low usability of security mechanisms and tools. Contextual factors play an important role in security, but few studies have investigated security interventions with developers in organizational settings. In this case study, we track the impact of appointing security champions in a large e-commerce company with five software development teams, using the OWASP Security Assurance Maturity Model (OWASP SAMM) to measure the extent to which security practices were adopted. We also elicited the experiences of the security champions and developers in each team in 15 qualitative interviews. The results of the OWASP SAMM assessment show the adoption of secure practices varied widely between the different teams. Results from the interviews revealed different levels of security knowledge and commitment to the role between the security champions - but they agree in their perceived lack of support from company security experts and management. We conclude that secure software development requires more than appointing individuals such as security champions - to transform software development practices requires an organization-wide commitment, including access to resources and support.

KEYWORDS

Security, Software Engineering, Usable Security, Case Study, Security Frameworks, OWASP

ACM Reference Format:
Marco Gutfleisch, Markus Schöps, Stefan Albert Horstmann, Daniel Wichmann, and M. Angela Sasse. 2023. Security Champions Without Support: Results from a Case Study with OWASP SAMM in a Large-Scale E-Commerce Enterprise. In *The 2023 European Symposium on Usable Security (EuroUSEC 2023), October 16–17, 2023, Copenhagen, Denmark.* ACM, New York, NY, USA, 17 pages. https://doi.org/10.1145/3617072.3617115

1 INTRODUCTION

The number of reported security vulnerabilities in software products is constantly increasing [18, 73]. Attackers look for and exploit these vulnerabilities; organizations in the critical infrastructure sector, for instance, are constantly being screened [28, 53]. Outside critical infrastructure, profitable companies are increasingly targeted for financial gain. For an e-commerce company, the financial losses of disruption quickly mount up, as well as long-term reputational damage after a cybersecurity breach. Still, many e-commerce companies do not invest in securing the software they develop and operate - they employ security professionals, but these are rarely present in software development. The burden of security thus rests on the shoulders of the teams or individual developers.

A significant number of studies over the past few years have investigated the security knowledge and practices of developers - or lack thereof [14, 69, 71]. Most of those studies are laboratory studies, or collect data via interviews or surveys (e.g. [4, 20, 50]). Some ask developers about the impact of development frameworks and other organizational factors. The results suggest that challenges that lack support, and fail to adjust organizational structures or processes are the main reasons why attempts to instill secure software development practices fail [6, 36, 71]. Our aim was to gain a deeper understanding of how organizational context factors enable or hinder the transition to secure software development, even when a company has stated this as a clear goal.

To investigate the challenges and problems of making secure development happen, we established a cooperation with a large e-commerce company operating in a German-speaking country, with more than 6000 employees, including 200 software developers. We were given access to five of their agile software teams. Furthermore, the company has a security champion program in place. The company nominated a security champion for each agile development team. Our aim was to evaluate the company's effort to improve the security of the software developed in-house, and collect the experiences and perceptions of that those involved in software development had of security:

- **RQ1:** *Which security practices do developers perform, and what challenges or problems do they encounter in the Software Development Process (SDP)?* Security does not depend exclusively on individuals. We, therefore, want to understand the development process holistically in order to recognize overarching patterns and identify problems and challenges.
- **RQ2:** *How do different roles perceive software security within the organization and their software teams?* Understanding the causes of individual actions in the process requires an understanding of individual perceptions and motivations. These shape how the process is lived, and consequently determine the success of a defined security strategy. We also asked to what extent they consider the usability of the security measures they implement for customers. This is not part of OWASP SAMM or other security frameworks, but academic research over the past 20 years has shown that security needs

to be usable to be effective and that online retailers and platforms with cumbersome security lose customers [25].

We use both the OWASP Security Assurance Maturity Model (SAMM) (a standardized model to measure the extent of security practices performed) [55] and structured qualitative interviews to more closely investigate problems, challenges, perceptions, and opinions about security. We collected and analyzed data from a total of 20 people with different roles (Developers, DevOps, Product Owners, and Scrum Masters).

Key Findings. A common concept in the agile development context is to assign the role of *security champions* to individual team members [29]. These security champions support the team in security matters and are ideally networked with the company's security team(s), as well as other security champions in the company. Although the company had established a security champion in each development team, the software teams did not follow a uniform security strategy. The security champions are generally trusted to fulfill their role, resulting in many team members handing over their security responsibilities to them. The fact that the security champions are not sufficiently supported by management further complicates their day-to-day work, in addition to their main roles as developers. Security requirements must find their way from the security champions to the team leaders and up to higher stakeholder levels. The prioritization of requirements, therefore, does not follow a security strategy or risk analysis but is done at the team owner level and often suffers the pressure of functional requirements arising from different business domains.

Contributions. We are among the first to examine security and security champions in an agile development context [1]. Furthermore, (i) we present how software security is implemented and highlight existing problems and challenges. (ii) We focus on security practices in the software development process, as well as on the security perceptions and opinions of different stakeholders. (iii) Based on our findings, we make recommendations for improving the security in the SDP. Furthermore, we discuss open challenges for academia and industry.

2 RELATED WORK

We divide the related work into four main topics: First, we examine scientific work related to secure software development with a focus on usability (2.1). Secondly, we summarize recent work on security behavior, security routines (2.2), and security champions (2.3), and thirdly, we investigate publicly available security standards, guidelines, and frameworks (2.4). Lastly, we introduce the field of usable security (2.5), as we treat usability as an integral part of secure software development in our interview guide.

2.1 Secure Software Development

With time, the call for usable, secure software and tools has been extended to usable tools and models for software developers to use during the software development process. Software developers can face problems when trying to develop secure software if they are hard to use. Green and Smith [34, 35] have called for usable security APIs to support software developers during the development process, with Acar et al. [2] later developing a scale to measure the usability of cryptographic APIs. As an example, security warnings in cryptographic APIs have been shown by Gorski et al. [32] to have a positive impact on code security when used, showing the benefit of more usable tools. Naiakshina et al. [50–52] as well as Danilova et al. [19] and Geierhaas et al. [30] studied software developers' behavior when trying to store user passwords securely. Commonly, they found that developers often lacked the knowledge to store the password securely, but providing them with tools and information sources could increase their success. However, Acar et al. [3, 4] as well as Fischer et al. [23] noticed that the use of information sources can hurt the security of the software if the used sources are unreliable, which stresses the need for systems and guidelines to support developers during programming. Usability is not only required for tools but also practices and protocols: Krombholz et al. [44] found in an experiment that even knowledgeable participants had difficulties deploying the TLS protocol correctly due to bad usability, resulting in less secure solutions. In a further study, where they examined the mental models of administrators as well as end-users with regard to HTTPS [43], they found that both groups had misconceptions about the benefits and threats to HTTPS and revealed further usability challenges. In addition to software developers, software meant for other related operators must also be usable. Dietrich et al. [21] showed that misconfiguration due to bad usability can lead to security issues.

2.2 Security Behaviour & Security Routines

The security of software does not solely depend on software developers, but on the multiple factors during the software development. Assal and Chiasson [6] studied security practices by interviewing software developers about the security routines of the software development life cycle (SDLC) in place at their workplace. They found that the SDLC practices used in a company context were often different when compared to the best practices found in the literature. Commonly, the reason given for this was a cost-benefit trade-off, as the practice of security was associated with a high workload. The results support the need for usable best practice standards and guidelines. In a second study [7], Assal and Chiasson strengthen this claim by analyzing 123 responses in an online survey. They recognized that software developers do care about security, however, they were often deterred by the systems in place at their companies. When interviewing app developers, Balebako et al. [10] found a connection between company size and the likelihood of positive security and privacy practices. Gutfleisch et al. [36] conducted an interview study examining the software development process in companies. They interviewed software developers, software designers, and software architects regarding usability and security. The interviews showed a strong influence of contextual factors on the usable security of products. Further, they were able to point out gaps and possible remedies. Haney et al. [38] conducted a study specifically on the mindset present in companies developing cryptographic products. They noticed a strong security mindset based on a strong security culture. However, Hallett et al. [37] found that giving developers specifications on password storage showed only a small effect on the security of the password storage, suggesting that only through instructions from the top, security can only be increased by a small factor. In addition, they were able to once again confirm the difficulties of software developers in storing passwords securely.

2.3 Security Champions

In Organizations, security champions serve as local representatives that encourage and monitor security policies, with the task of being an extension of the security management team [29]. Security champions can benefit the security culture of an organization by making communication about security and the explanation of this topic to employees more effective [12]. The concept also helps to decrease the experienced social distance and promotes security as a collaborative activity [47]. Security champions need adequate and coordinated company policies to work [12], which can be difficult if these security policies are not seen as usable by the employees [11]. Furthermore, security champions work best if being seen as "bottom-up" agents, who also question policies and discover solutions to improve the security of the organization [11]. Support by the company, therefore, is crucial to benefit from these roles. Jaatun et al. examined the implementation and maintenance of a security champion program at two Norwegian companies [41]. They highlighted the importance of management support and pointed out differences in the effectiveness of appointed and voluntary security champions. Furthermore, they recommended that the introduction and maintenance of a security champion program should be investigated in more organizations.

2.4 Standards, Guidelines & Frameworks

In the past, several different frameworks and tools have been created with the goal in mind to help software development achieve a secure software development life cycle. While guidelines are introduced by companies, governments, or researchers [15, 17, 31, 48, 54, 55, 57], developers often rely on other sources for help [3, 23, 40].

Software Assurance Maturity Model (SAMM). The framework developed by OWASP [55] aims to assess and improve software security. In its current form, OWASP SAMM defines five business functions, namely Governance, Design, Implementation, Verification, and Operations. Each business function is split into three security practices for a total of 15. With SAMM, OWASP aims to provide an effective tool for companies of all sizes to measure and improve the security within their SDP.

Building Security in Maturity Model (BSIMM). The BSIMM framework [15] was developed to support organizations using software security initiatives and defines Governance, Intelligence, SSDL Touchpoints, and Deployment as its four domains, which are further separated into 12 practices. Overall, they map 122 activities to those practices. Furthermore, Weir et al. [75] analyzed data collected with the BSIMM framework over twelve years.

Other Frameworks. Morrison [49] constructed a security practice evaluation framework and evaluated the framework itself. Such et al. [67] conducted a study analyzing security assurance techniques contained in the ISO/IEC 27001 standard [40]. They were able to identify techniques with high impact and relatively low costs to implement.

2.5 Usable Security

Zurko and Simon [77] promoted the idea of user-centered security and usable security. Adams and Sasse [5] found issues with the usability of password policies in companies, resulting in little effect on the overall security. Similarly, Whitten and Tygar [76] showed that many users had difficulties using PGP 5.0 for email encryption. They concluded that the tool was simply not usable enough for the average user, thus drastically reducing the effectiveness of the tool. As shown by Stransky et al., usability problems with end-to-end encryption persist to this day [66]. Sasse et al. [61] argued that users do not have to be seen as the weakest link, but for designers to create usable security software. Further, Sasse et al. [62, 63] argued against the misconception of the existence of a forced trade-off between security and usability and for a shift away from blaming the users in general [60].

3 METHODOLOGY

Within section 3.2 we describe how we set up and used OWASP SAMM to assess the security practices in the development teams. Furthermore, we created interview guides for various roles in the organization (*Software Developer & DevOps, Scrum Master, Product Owner*) to further extend the data basis and to better understand employees' security perceptions. The process of developing the interview guides, the scientific analysis, as well as the structure of the interview guides are described in section 3.3. The data collection steps were conducted by one researcher, who is involved in the cooperating company. Figure 1 illustrates the assessment activities mentioned above and their order in the research process. All data needed for replication (all interview guides and our codebook) can be found in the Appendix (see A).

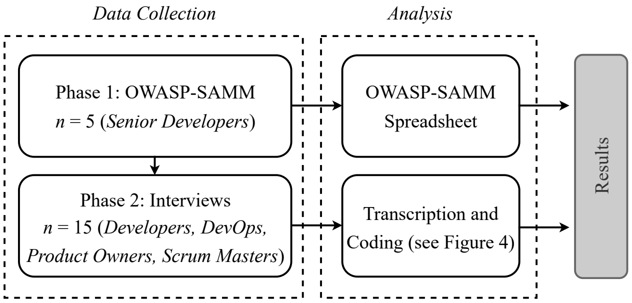
Data Collection
Analysis
Phase 1: OWASP-SAMM
n = 5 (Senior Developers)
Phase 2: Interviews
n = 15 (Developers, DevOps, Product Owners, Scrum Masters)
OWASP-SAMM Spreadsheet
Transcription and Coding (see Figure 4)
Results

Figure 1: Overview of the Methodology

3.1 Company Context

The e-commerce company operates in the German-speaking market, generating over €1 billion in sales annually. It has several thousand employees, and more than 200 are software professionals who develop elements of the e-commerce platform and related services, using Scrum [64] as their main development framework. The web shop is supported on several platforms. We were given access to five of their development teams to conduct the OWASP SAMM, as well as 15 interviews with different roles in the five teams: *product owner, developer, quality assurance expert, scrum master* and sometimes also an expert on *DevOps*. In Scrum, product goals and development tasks are broken down into smaller chunks, so-called user stories. Those stories are primarily maintained and prioritized by the product owner with the help of the other team members. The scrum master serves as a process specialist enhancing the team's processes to achieve their set goals. The company also appointed one security champion for each scrum team. However, the security champions perform their main activities in parallel either as DevOps or as developers.

3.2 OWASP Security Assessment Maturity Model (SAMM)

OWASP SAMM is split into five so-called business functions (*Governance, Design, Implementation, Verification, Operations*). Table 1 describes each business function shortly. Each business function is divided into 3 security best practices, resulting in a total of 15. Every practice is categorized into two streams. This results in 30 different areas, which are further divided into three levels of maturity, totaling in 90 possible security activities for software development. Figure 5 illustrates the OWASP SAMM.

Table 1: Short-description of Business Functions

Business Function	Description
Design	Focuses on activities such as how an organization sets software development goals and how software is developed in general. This includes, for example, requirements, architecture and how to deal with them.
Implementation	Focuses on activities that involve building and deploying of software grouped in this business function.
Verification	Focuses on activities that check and test artifacts created in the SDL.
Operations	Focuses on activities, which aim to ensure confidentiality, integrity, and availability of an application and its related data throughout its operational lifetime.

The activity for the first maturity level of the stream *Secret Management*, for example, belongs to the business function *Implementation*. It recommends "introduce basic protection measures to limit access to production secrets" [55]. The activity assigned to the second level further recommends "inject secrets dynamically during deployment process from hardened storages and audit all human access to them". All activities are described in detail and cover specific quality criteria, as well as questions for assessing the organization's maturity level of specific streams. To answer these questions, it is recommended to do the assessment by interviewing experts who have knowledge about the process that is investigated. OWASP provides a spreadsheet that supports the assessment by serving as a template. The scores of the streams, as well as of the security practices and business functions are calculated within the template.

According to the creators of OWASP SAMM, after conducting the assessment, an organization should set its target and define the plan. For more detailed information about the business functions, their streams, the corresponding security activities, and their assessment, we refer readers to the official documentation of OWASP SAMM [55].

The teams in our study used the second version of OWASP SAMM. At the time of conducting the research, some information had not yet been migrated to SAMM 2.0, so we also used guidelines from the first version. We translated assessment questions and quality criteria within the spreadsheet into German. To further prepare for the study, the lead researcher conducted three pilot assessments with experienced software professionals from other organizations supervised by another researcher. We noticed that some of the questions were unclear or misunderstood by pilot participants; following their suggestions, we added concrete examples for each question.

3.3 Qualitative Interviews

3.3.1 Instrument Development & Piloting. The aim of the interviews was to identify challenges and problems within the current process, and, on the other hand, to better understand employees' security perceptions. To develop the interview guide, two researchers collected an initial set of questions and formed an initial interview guide independently. In multiple collaborative sessions, two researchers further refined the interview guide for development roles within the team (developer, DevOps). We then split questions, which aimed at investigating the current SDL (addressing RQ1) from those who focus more on the individual perception and opinions (addressing RQ2). Using the first draft of the interview guide, the lead researcher conducted five pilot interviews in total, with at least one additional researcher listening in and taking notes to further refine the interview guide. After each pilot session, the interview guide was slightly adapted. After three loops of refining the guide for development roles within the team, we derived versions for the roles of the product owner and the scrum master. We piloted both derived interview guides once.

3.3.2 Interview Guide & Procedure. The final interview guide consisted of four parts (*On-boarding, Problems & Challenges within the SDP, Security Perceptions & Opinions, Off-boarding*). During onboarding, we informed participants about the purpose of the study, as well as how data would be collected, processed, and stored, and by whom. We ensured to answer all participant's questions in advance and afterward asked for explicit consent to record the interview. At the beginning of the interview, we asked participants to think of a concrete user story in which security was a part. We then guided the participants through the phases of the software engineering process (*Communication & Planning, Modeling, Construction, Deployment*) specified by Roger et al. [59]. For each of the phases, we asked questions to help us understand the SDL following the life cycle of the user story. We also tried to determine if something had been done differently in other user stories. At the end of each phase, we explicitly asked whether they could think of any problems that occurred during the current phase in focus. After the last process phase, we focused on the usability aspect of the security feature and how it was handled during feature development. Based on previous research [16, 36] we consider usability an integral part of any security feature, product or process. For the Scrum Masters, the first part of the interview did not follow the phases of the SDP, as their involvement within the SDP differs compared to other team members. The first part of the interview guide was therefore focused on the phases of the scrum model: *Planning I+II, Refinement, Dailies* and *Other Meetings* (e.g. Retrospectives).

The second phase of the interview guide (*Security Perceptions & Opinions*) aimed to capture participants' security perceptions as well as how they think of security within the organization. This section of the interview guide was divided into seven subsections: *Usable Security, Security Breaches, Opinion Security, Importance Security, Security Motivation, Message to Leadership, Wish for Improvement.* At the end of the interview, we asked participants whether they would like to add something that we might not have covered during the interview. Furthermore, we asked if they had any further questions regarding the study and finally stopped the recording. The components of the interview guide are illustrated in Figure 2 and the full interview is listed in the Appendix (see A).

3.3.3 Analysis. We used Kuckartz [45] qualitative analysis with MAXQDA [74] as a guide. Two authors started deductively, creating an initial draft of the codebook independently, based on the interview guide. Then, they agreed on one first version of the codebook and started coding the same interview once. While coding, both coders inductively expanded the codebook with new codes. Afterwards, they again merged the system and agreed on one initial codebook. The remaining 14 interviews were split equally among the two coders. After that, both coders again expanded the codebooks independently and then merged them to create a final one. All 15 interviews were then coded by both authors and finally merged. The coding process consisted of evaluating the transcribed interviews systematically. The data was structured into categories and subcategories by assigning codes to selected content relevant to at least one of the research questions. During each step of the process, memos were written to preserve ideas that appeared. These memos then influenced all subsequent steps of the coding process, generating theories that formed the creation of code categories and vice versa. The use of memos is seen as an important strategy in qualitative research to enhance data exploration and maintain the continuity of the process [13]. The coding process (see figure 3) as well as the (see Table 4) are presented in the appendix.

3.4 Ethics and Data Privacy

Our institution did not have an institutional review board (IRB) nor an ethics review board (ERB) at the time of planning and conducting the study. We adhered to the strict German and EU privacy laws. Furthermore, the information provided to the participants at the beginning of the interview, as well as for participation in the questionnaire, was compliant with the European General Data Protection Regulation (GDPR) and covered the content that would usually be required for a US IRB approval. We specifically did not enforce the request of participation in any parts of the study by supervisory roles, as doing so would potentially put pressure on participants, and voluntary participation may then not be guaranteed. Furthermore, we took special caution to protect the identity of the company and participant by not disclosing product details, specific implementation issues, or detailed demographics. We also removed potentially identifying text from the transcripts or replaced names, services used, or products with pseudonyms.

4 RESULTS

In this section, we present the demographics and our findings of the OWASP SAMM and the qualitative interviews.

4.1 Demographics

For anonymity and data protection reasons, we cannot provide detailed demographic information about our participants. Participant roles, classified into the three assessment methods, can be seen in table 2. The roles are also assigned to the respective participant designations, which are used in the following results. For the OWASP SAMM assessment, five senior developers (with more than five years of experience within the organization) were interviewed and represented each development team. For the qualitative interviews, we interviewed 15 participants, holding different roles in the organization: developers, DevOps, scrum masters, and product owners.

Table 2: Number of participants and their roles (* = security champions) in the qualitative interviews.

	Number of Participants	Description in Text
Developer	6	P1*, P2*, P3, P4, P5, P11
DevOps	2	P6, P7*
Scrum Master	3	P8, P9, P10
Product Owner	4	P12, P13, P14, P15
Total	15	

4.2 OWASP SAMM

The OWASP SAMM assessment was conducted with five employees, one from each development team. As Table 3 illustrates, the business functions differed in their level of maturity. With the maximum level being 3.0, the operations domain had the highest average level of maturity with a score of 0.86, and the design domain had the lowest average level of maturity with 0.50. The five teams also differed in their level of business function maturity. In the governance domain, teams B and D had the highest scores (0.71), and team A the lowest (0.38). In the design domain, Team B had the highest (0.71), and teams A and C had the lowest score (0.38). In the implementation domain, team B achieved the highest score (1.00), and teams C and D the lowest (0.67). The verification domain was led by team D (0.92), with team E having the lowest score (0.21). Lastly, team C had the highest score in the operations domain (1.13), and team A the lowest (0.63). Looking at the scores of the security practices within the domains, we can also see a big difference between the five teams. In the first security practice (Strategy & Metrics), for example, team D had a much higher score (0.75) than the other teams, which all scored below 0.25, with two teams even having the lowest score possible. This sort of scattering of team maturity scores within the different security practices proceeded in the following categories and can be seen in the statistics columns of Table 3. Looking at the coefficient of variation, a statistical measure of the relative dispersion of data points around the mean, we can see that many security practices have a high percentage, showing that scores are distributed very unevenly between teams.

4.3 Qualitative Interviews

In this section, we present the findings of our qualitative analysis of the interview data. We used our codebook (see Table 4) as a guide for structuring this section into nine categories. These categories, therefore, cover problems and challenges (addressing RQ1) as well

Table 3: OWASP-SAMM team maturity scores of business functions and security practices (n = 5). (CV = Coefficient of variation).

	Teams					Statistics	
	A	**B**	**C**	**D**	**E**	***Mean***	***CV***
Governance	0,38	0,71	0,42	0,71	0,50	*0,54*	*28,97*
Strategy & Metrics	0,00	0,13	0,25	0,75	0,00	*0,23*	*137,55*
Policy & Compliance	0,13	1,00	0,00	0,25	0,50	*0,38*	*104,92*
Education & Guidance	1,00	1,00	1,00	1,13	1,00	*1,03*	*5,67*
Design	0,38	0,71	0,38	0,54	0,50	*0,50*	*27,18*
Threat Assessment	0,00	0,75	0,00	0,13	0,13	*0,20*	*155,03*
Security Requirements	0,63	0,50	0,25	0,75	0,13	*0,45*	*57,19*
Secure Architecture	0,50	0,88	0,88	0,75	1,25	*0,85*	*31,84*
Implementation	0,71	1,00	0,67	0,67	0,83	*0,78*	*18,21*
Secure Build	0,75	1,13	0,88	0,63	1,25	*0,93*	*27,86*
Secure Deployment	1,13	1,75	0,88	1,13	1,00	*1,18*	*28,54*
Defect Management	0,25	0,13	0,25	0,25	0,25	*0,23*	*23,76*
Verification	0,29	0,71	0,63	0,92	0,21	*0,55*	*53,74*
Architecture Assessment	0,13	1,13	0,13	0,25	0,00	*0,33*	*139,32*
Requirements Testing	0,13	0,50	1,13	1,75	0,00	*0,70*	*104,25*
Security Testing	0,63	0,50	0,63	0,75	0,63	*0,63*	*14,08*
Operations	0,63	0,83	1,13	0,79	0,92	*0,86*	*21,38*
Incident Management	0,75	1,25	1,25	1,13	1,00	*1,08*	*19,47*
Environment Management	0,13	0,63	1,00	0,50	0,75	*0,60*	*53,46*
Operational Management	1,00	0,63	1,13	0,75	1,00	*0,90*	*22,74*
Mean Total	0,48	0,79	0,65	0,73	0,59	*/*	*/*

as individual security perceptions (addressing RQ2), depending on the focus of the category. The role of the security champion is referred to in the company as the *security lead* or *sec lead*. We refer to the designation of the security champion in the results but have retained quotes from the participants as faithfully as possible within our translation.

4.3.1 *Organizational & Technical Challenges & Problems.*

What stood out in the first part of the interviews was that participants only mentioned few distinct security activities. For example, participant P2 described that they set up a dependency checker, which could potentially be used across teams or migrated with minimal effort. But this is happening rather slowly, if at all. Furthermore, almost no specific security tests are conducted.

4.3.2 *Requirements & Story Refinement.*

Participants explained that the company requires each Scrum team to provide one security champion - they are either developers, DevOps experts, or quality assurance specialists. However, their primary responsibility lies still on their main duty and not on security. All security champions meet at least every two weeks to discuss upcoming problems and challenges. Each security champion takes security topics and requirements into the teams they are part of, but the product owner then decides whether and when to address those requirements. With the exception of some requests from the data protection officer, or occasional regulatory requirements (e.g. for payment services), the product owners reported that stakeholders usually do not raise security requirements. P2 explained how they break down and refine a security requirement, brought by a security champion, for example: *"In Refinement, we talk about the tickets until they are ready. And then in planning, we talk about the tickets again, and then in planning II we have the technical meeting, so to speak, where we talk about the tickets again explicitly with the developers. So theoretically, there were several opportunities to further specify the tickets."* – [P2]. All participants stated that the process for refining stories with security-relevant contexts did not differ from the usual ones: *"Security is basically part of the normal process for us [. . .]"* – [P11]. Nevertheless, in case of an urgent security incident, the process may differ, as the work on an incident starts immediately and other topics fall aside.

4.3.3 *Usable Security.*

Protecting software against skilled attackers is very important - but the usability of security features or products is important, too. If security features are time-consuming or cumbersome, users are likely to circumvent them, or abandon the service and go elsewhere. When asking participants how usability and security relate to each other, 10 participants (P1-P4, P6, P10, P12-P15) mentioned that it's important for security to be usable for their customers: *"One would like to have solutions, where the customers have to perform less cumbersome actions. [. . .]"* – [P1]. Furthermore, they explained that good usability would increase the likeliness of usage: *"So security must always be usable, otherwise it will not be used."* – [P1]. Only participant P3 stated that security would suffer from bad usability. In contrast to perceptions that cover correct aspects of usable security, six participants described the relation between security and usability either as a trade-off (P1, P7, P11, P12), or they did not see any relation (P8, P9) or they blamed the user if something was not performed correctly (P11). Furthermore, participants highlighted the involvement of UX experts if the user would be affected. They also did not mention any specific measures that might be done differently compared to the standard procedure when working on a story that affects both usability and security.

4.3.4 *Communication.*

What stood out among all the statements was that security champions were often referred to for questions about security, or they were described as the main pivot point of security communication. Five participants (P2, P3, P5, P8, P15) described the openness of the security champions to talk about or help with security topics. Nevertheless, eight participants mentioned either examples where security requirements or procedures led to communication issues (P1, P5, P12, P15) or they wished for more, sophisticated, transparent, and/or strengthened security communication (P2, P5, P9, P10, P13): *"[. . .] there should be more transparency. It might be useful to have something proactive like "news from the security team""* – [P9]. Furthermore, we noticed four participants (P4, P10, P6, P13) either directly or indirectly mentioned that security knowledge was only present in a few employees (the security champions). Five participants (P4, P7, P8, P10, P13) said that, apart from the ideas and requirements of the security champions, there is no further exchange about security.

4.3.5 *Security Perceptions of Security Champions.*

The security champions were valued by both the product owners and their team colleagues: *"Because I know our security lead, I can really trust him, he is very accurate. Sometimes more than I would like. He reminds me regularly that certain things have to be done."* – [P15]; *"And we would actually love to clone our [security champion] because he does so much important work* *and is very, very committed and involved in a lot of topics and has a lot of knowledge."* – [P4]. Also, the security champions described their duty as a contact point for security: *"So the role of the security lead is to discuss security-relevant aspects in the sec lead round, to see if anyone else brings topics with them, whether they might be relevant for our team, and if so pushing them to their team, and also to keep an eye on it in general, so that the team doesn't forget to take security into account."* – [P2]. Although the role of the security champions is appreciated and respected, one scrum master described to us that he experienced differences in security skills and motivation among the security champions: *"Saying with my words: this role [Security champion] is lived with different intensity. Some colleagues contribute strongly [in their role as a security champion] [. . .] and others sometimes let sweep security aspects under the table [laughs]."* – [P9]. Furthermore, we found out that security champions did not receive any security training or other security-specific educational support from their employer.

4.3.6 Security Perceptions of Developers & DevOps. The opinions on how security is perceived by non-security champions in the development teams differ. Eight participants (P1, P2, P6, P9, P10, P12-P14) stated directly or indirectly that team members have a sufficient level of security awareness, but the level of awareness described varied: *"So I know that my colleagues take security seriously. And are also happy when we can address security issues and improve our security."* – [P1]; *"So I think they have a basic level of awareness for security."* – [P6]. However, five participants see the potential for improvement in the security mindset and motivation: Team members think *"more pragmatic"* – [P2] about security, are less motivated than security champions (P1) or think that there is *"potential for improvement in terms of the mindset"* – [P6] regarding security. Furthermore, three participants described security as rather annoying and disruptive: *"[. . .] you can immediately hear a certain indifference or annoyance and no interest or enthusiasm."* – [P5]; *"Well, I think that some people see this as a rather annoying topic, as an annoying topic in the background [. . .] So, it has to be done, but probably very few people like to deal with it."* – [P6]. This is also in line with the experience of the researcher who was part of the development department: Awareness is definitely present, but the motivation clearly differs from the security champions' ones.

4.3.7 Security Perceptions of Product Owners. Six participants (P2, P12-P15), including all interviewed product owners, explained that product owners do not have sufficient expertise in the field of security. Product owner P14 explained that he relies on his colleagues: *"I don't know in detail [security user story] because I actually relied on my colleagues as they know how to proceed."* – [P14]. Another product owner (P12) also admits this, and highlights that there is a lack of education regarding security among product owners: *"I think what we do is basically good, but the education of the product owners, I find rather lacking and also the driving of these topics is missing somewhere [. . .] At least as a product owner, I always feel a bit lost."* – [P12]. Both interviewed scrum masters and three interviewed members of the development team (P2, P3, P5, P9, P10) described that, sometimes, employees had to argue for security. Furthermore, participant P2 even described it as a fight: *"The [security] topics are often hypothetical concerns until they occur. And that's why, in discussions with stakeholders or with the PO [. . .] you sometimes have to fight for a topic, because it naturally stands out against other topics that may have a direct impact on revenue, whereas a security topic only has an impact on revenue if you somehow have a loss of revenue."* – [P12] The product owners are also aware of this: Two product owners honestly expressed the desire for key metrics and decision-making aids on the subject of security. Six participants (P6, P7, P11, P13, P15) stated that security is generally a less important topic and it's more important to develop new features: *"Why does it fail? Time, I think. For that, one needs to get time from the PO [. . .] so that one can deal with such things. Mostly it's just about a feature or future feature being developed [. . .]"* – [P7]. However, five participants (P1, P7, P9, P10, P14) stated that product owners have a sufficient level of awareness of security. We also observed that there is a rather good and respectful relationship between the product owners and teams, specifically the security champions, as both parties admire the skills and expertise of each other's roles.

4.3.8 Security Perceptions of the Leadership & Management. We asked participants how important security was for the management, taking into account the provided guidance and resources. Six participants (P2-P5, P7, P8) thought that the leadership sees security as an important topic. We even got descriptions that some participants could not understand why they should not pay attention to security, as that would pose a risk to the company. Furthermore, participants P2 and P3 valued the time the security champions get for spending time on security topics. However, five participants (P1, P6, P11, P14, P15) stated either directly or indirectly that security is not important for leadership. Specifically, two product owners described these perceptions: *"From my point of view and also from the point of view of the business owners who are in the company, none of us are really interested in security. I'm not saying that we don't care, but we just assume that when things are developed, security is automatically taken into account."* – [P15]; *"But the facts speak differently: Feature, feature, feature, revenue."* – [P14]. Participant P11 also stated that security is a less important topic for leadership: *"For them, this is a convenience topic, and as long as it works, no one cares."* – [P11].

4.3.9 Resources. Eleven participants (P1-P4, P6-P8, P10, P12, P13, P15) described to us that the available resources are not sufficient, or that more resources would be needed for security. Participants expressed that there should be more staff, but also more time available for security topics in general. Participant P3 wished for training or workshops so that other people could also acquire at least a basic level of security knowledge. Participants P2 and P4 specifically criticized the multiple role concept and suggested ideas for improvement: *"We have the role of a security lead. But this is actually a normal employee, who only partly spends time dealing with security topics. And I would appreciate making this a full-time role."* – [P2]

4.3.10 Security Incidents. The company suffered from security incidents in the past, which came up often in the interviews. We specifically asked participants to explain the process for solving a (hypothetical) security issue. We noticed that almost everyone felt a high level of urgency and comprehension for acting in case of a (hypothetical) security incident. However, the described incident response process was described rather vaguely: *"Yes, if something came to light, we would take a look at it. Discuss it with the team and then someone would get to work on the solution promptly."* – [P7]. Seven participants (P1, P4, P5, P8, P9-P12, P14, P15) mentioned that the leadership or other colleagues were more aware of security after incidents happened: *"I think the awareness has become a bit bigger again with the Log4J topic for* *sure."* – [P14]; *" [...]I think, some were shaken up and have noticed that it is not as secure as they thought and that one has to put a higher priority on security topics."* – [P12].

4.3.11 Responsibility. During the interview, participants were asked who they thought was responsible for the security or a specific security incident. Almost all answered that the team was responsible. Also, some disliked the responsibility question and argued for a more solution-oriented responsibility framing *"Actually, it is important to ask who is responsible for fixing that [security issue]"* – [P1]. We did not notice anyone blaming others for past security incidents, or pushing the responsibility for security away completely. However, ten participants (P1-P8, P11, P12) mentioned the security champions when talking about responsibility: *"[. . .] ultimately as a security lead I am responsible, but also it is the responsibility of the teams. I am just there, making pressure and pointing to [security] problems"* – [P7].

4.3.12 Message to Organization Leaders. At the end of the interview, we asked our participants what they would like to tell the management about security. Seven participants (P3, P6, P8, P10, P11-P13) either wished for more resources and transparency or warned the management that they should take the topic of security more seriously: *"That's my impression, so I would say "Don't underestimate it". Because I think then you the topic gets the importance that it needs."* – [P13]. Participant P11 furthermore criticized the leadership's behavior from the last cyberattacks: *" [...] We are currently like, "Ah, we've been hacked. Then we must be extremely insecure, that's bad. That's why I'm mad at him and him" - that doesn't help anyone. Instead, we need to look at where our potential dangers actually lie." In order to have a better view of this, to understand that at one point or another, it is also a task for the company as a whole, and not just a technical task."* – [P11]. Another participant mentioned that *"more attention should be paid when decisions are made as to what risks are indicated by the specialist departments."* – [P12]. Participant P10 also appealed to the management: *"I could only recommend to the management that they show more interest, i.e. that they take a more businesslike look at issues that are more sustainable and that affect us all [. . .] and that they perhaps also ask questions in a more interested, not more critical, but more interesting way and enter into dialog [about security topics]."* – [P10]. One participant laughed when we asked the question and answered the question (with respect to security topics) with: *"Sometimes things take longer and it's ok."* – [P15].

5 DISCUSSION

In this section, we summarize and discuss the findings of our case study, and infer a set of recommendations for companies on security champion initiatives (see 5.2) and academia (see 5.3) based on our findings and experience with the methodology.

5.1 Case Analysis

Lack of Security Strategy. The first insight from looking at the OWASP SAMM scores was how much they vary across the teams. The overall score is low (0,65), and the teams perform various activities that contribute to secure software development to varying degrees - even though they are all contributing to the same product. The results of the interview analysis show that different teams described different security activities and problems (see 4.3.1). Together with the results of the OWASP assessment (e.g. a low mean score of 0.54 in the governance area), and a high variance in the extent of the security activities carried out, suggest a lack of guidance and internal regulations for security. Furthermore, the security practice *Strategy & Metrics* place among the lowest ranked practices with a score of 0,23 on average.

Unsupported Security Champions. The company established a security champion initiative, and required each team to nominate a team member for the role. The individuals put forward are meeting regularly, and taking ideas and requirements from the meetings to the teams. Security topics are discussed with the product owner, who then has to decide when - and if at all - to address them. The activities of the champions here are similar to those described in the OWASP SAMM, and the BSIMM as well as in the work from Becker et al. [11] - but the way it is implemented here is fragile. Security requirements almost exclusively come from the security champions to the teams, but whether teams adopt them is finally decided by the product owners - even though they have little security expertise, and without having metrics and key performance indicators to rely upon. Thus, the champions are assigned responsibility, but have no authority. Product owners, as well as team members, told us that they are pushed by the leadership to develop features and that there is little room for aspects that do not bring immediate business value (see 4.3.5). Security topics often involve cross-team aspects that require a certain degree of coordination and commitment from all product owners involved. Security champions do not have the authority to push and coordinate security topics across team borders. This creates a risk that security aspects are only partially implemented, take too long to be implemented, or are not implemented at all - each champion is left to fight for security within their software team. The lack of leadership and coordination means security requirements risk falling by the wayside. We also noticed that the level of expertise and motivation among the security champions varies, and that they were not offered security training or expert support when uncertain or reaching the limits of their expertise. For some, being given the role of security champion was motivating, but for others, being given responsibility without support was another burden added to an already busy job. This might further explain why teams performed differently in the context of security. In order to successfully change behavior, both motivation and ability need to be sufficiently high [27]. Here, the organization tried to motivate the security champions by assigning them a role, but did not ensure they had the ability.

Security Champions as a Bottleneck. Almost all communication about security in the company originates from the security champions or security incidents (see 4.3.4). Security champions here have a lot of responsibility and workload because they have to perform those duties in addition to their main role as developers or DevOps. Participants described that taking multiple roles is challenging for them, and wished for expert security staff they could refer to. Having security as part of the team has benefits, but it also carries the risk of teammates projecting all responsibility for security onto the champions (see 4.3.6) - thus further increasing the load on them.

Security Awareness. Despite the lack of support from leadership for security, awareness for security among stakeholders and in development teams was high - especially among the product owners.

But awareness alone does not necessarily lead to secure behavior [8] - and the low number of security practices reported by participants indicates this is the case here (see 4.2). The security champions have played their part in raising general security acceptance and awareness, and past security incidents have made many employees realize that their own company can be affected (see 4.3.10). Türpe et al. showed within one field study that security awareness and motivation increased after the team received a report from a professional penetration test of their product. But with the number of fixed issues, the pressure decreased, and the motivation declined, too [72]. Poller et al. also showed that without a change in development practices, the security taught to developers slips away [58]. In our case, where a security incident is so prominent and the level of urgency is high, the company should not wait any longer to start implementing new security measures.

No-Blame Culture. Almost all participants said the whole team is responsible for security, or expressed that it is more important to find out how to fix an issue than to blame someone (see 4.3.11. Open communication about security and related mistakes is highly beneficial in terms of security [46]). Also, as Senge points out in his book "The Fifth Discipline" [65], team learning is a central skill in organizations, which can be developed by regularly reflecting on errors and failures.

Customer-Focused Thinking. When asked about usable security, most of our participants expressed very customer-focused thinking (see 4.3.3). They also mentioned that security champions often collaborate with UX experts if a security feature could affect the end user. Collaboration between UX- and security experts seems to benefit usable security [36]. This is a positive finding compared to Caputo et al. [16], where developers described security and usability as a tradeoff, i.e. that more usability would reduce security. The participants in our case study develop B-2-C products, and work with user stories and a product owner - whereas those in Caputo et al. worked on B-2-B software and what little - if any - information they had about end-users came from pre-sales engineers.

5.2 Recommendations for Practitioners

OWASP SAMM for Use in Industry. One of the most common security activities companies invest in are penetration tests [58, 75]. Relying on annual penetration tests alone is risky because it only captures a snapshot of security in an organization at a particular time. Increasingly, security maturity is about how well an organization is able to manage a security incident, and whether it is capable of learning from one to improve its security. Keeping track of security activities being performed on an ongoing basis is a valuable Key Performance Indicator (KPI) in addition to penetration tests or security defect tracking. OWASP SAMM is a measurement approach that companies can apply to assess themselves on a regular basis. There is an initial investment required to understand the maturity model, but it only took about six hours to complete the assessment for all five teams with the tools provided. The explanations and ideas provided for each security activity foster a better understanding of security in software engineering. Also, we recommend having examples at hand when conducting the assessment (see 3.2). However, setting the overall direction or prioritizing the future implementation of certain security activities, might require an in-depth understanding of the context and the employees' security perception. In our investigation, it was only through the interviews that we discovered the value of security champions and their challenging role within the company. Furthermore, it is unclear whether employees would even have sufficient skills to perform any kind of security tests, threat assessments, architecture verification, or other security practices. Additionally, it is not uncommon that corporate structures are often a major factor influencing the adoption and rejection of security-enhancing activities [58, 72]. Hence, understanding and addressing those might accelerate the implementation of a set security strategy.

Empower Strategic Change Management. Changing behavior and routines in organizations is a very challenging task. Trying to manage behavior by pronouncing rules and trying to enforce them is futile [33]. That is why increasingly, organizations are adopting change management frameworks and tools, Kotter [42] being one of the pioneers. Other concepts like nudging [9, 24, 68, 70], Fogg's BMAT model [26, 27], intentional forgetting [22, 39] or related concepts might also help setting up a strategy to smooth the path for the adoption of secure behaviors. In almost every project, there are supporters as well as detractors (e.g. in our case the security champions were the most powerful supporters at the time of investigation). Empowering supporters and convincing detractors, as well as undecided involved parties, is essential for pushing change forward and should be the responsibility of organizational leaders. Data from an initial measurement could well be used for escalation to create a sense of urgency, and to create the desired amount of motivation that people are willing to leave their comfort zone. Data and graphs from the OWASP SAMM, quotes, statements, ideas, and insights from the interviews can be powerful sources for this.

Support your Security Champions. Assigning the role of security champions to intrinsically motivated team members is not enough to transform existing development practices. In our study, some champions were passionate about security and took their role seriously, but they still struggled because of a lack of resources and support from leadership. Security champions who have expertise have a mountain to climb when faced with a team that has no security expertise. Thus, the role of a security champion was formally filled, but not lived. This is not the fault of the individuals, but the organization. The security champions need access to expertise and training programs in which the relevant knowledge is imparted. It would also make sense to promote the community of security champions more strongly. Networking can lead to better access to knowledge that is distributed among the security champions. Especially in the introductory phase of the security champions, there will be large differences in the existing knowledge. In addition, security champions should also have the freedom to pursue the topic of security so as not to be completely subject to the stress of day-to-day business. Of course, this must be taken into account in the planning of the respective team leads or product owners and requires corresponding commitment on their part. For industry, therefore, it makes sense to pay attention to previous research (see

2.3) to avoid key pitfalls. Furthermore, OWASP's Security Champion Playbook can help to get started [56]. We will address this more in detail in section 5.3.

5.3 Recommendations for Researchers

Contextual Factors. Research on developer-centered security has focused on better tools and interfaces, or instructions for developers on how to build secure software. Security tools and knowledge can help development teams - if they are adopted by developers in practice and become a routine - but most current interventions do not achieve this [58]. Change is hard when professional lives are busy - and developers constantly battle deadlines. Secure software development is way more than the writing of secure code or individual decisions by developers. Today's software systems are becoming more and more complex and often depend on many components from third parties. Additionally, company structures can block enabling real change towards more security. We argue that in the course of new and innovative approaches, more thought should be given to how this can be used in a real-world context. Even a small user study as a first approach to validate a new tool or project can facilitate the adaptation of an idea. Furthermore, we need more studies investigating resource-saving approaches that might help software teams achieve more security in their products.

The Role of Security Champions. The number of risks and threats against which organizations must protect themselves is constantly increasing. It is not sustainable for many companies to buy in a large number of security experts, which take responsibility for all security concerns. Building expertise within the development teams and organizing it holistically, therefore, makes sense in order to distribute the burdens and responsibilities related to security. The concept is seductively simple, but the implementation in practice can be challenging (see 5.1). In today's world, where more complex products require more and more third-party components, the distribution of security risks is no longer the sole responsibility of the development team but lies often outside their remit. We need research to understand the challenges and problems organizations face when it comes to security and develop and evaluate solutions. It remains to be seen which responsibilities a security champion should actually address and to what extent, in the context of modern and complex agile software development. There are no published studies that specifically examine the process of introducing security champions in an organization for the first time - for example, using the OWASP Security Champion playbook from [56], that supplements the model with further practice-relevant recommendations based on the insights gained. The creation of the role description and the building of knowledge on the part of the security champions need to be investigated in the context of different industries and types of development teams. Usable security is currently not addressed by the OWASP approach but is important in many contexts - so ways of providing usable security knowledge and skills to security champions is a key challenge.

Usable Security. Security research over the past two decades has established the importance of making security usable. Otherwise, security features are likely to be misused, circumvented, or just rejected. As a result, one might build a product with high-security technology components which are lastly bypassed by their users. As usability is not considered in most security standards and regulations, we from academia need to create a basis for promoting the importance of the interplay between usability and security, which is also spilling over into the industry. One approach could be to investigate the collaboration between designers or UX-Experts and security experts in more detail, as this might seem a key factor for achieving more usable security in software products [36]. Conceptually, it would be conceivable to investigate the approach of linking security champions not only with internal security departments but also to build the bridge design and UX department. Furthermore, the topic of usability and its impact on the effectiveness of security applications or features should be part of any security training.

5.4 Limitations

The specified counts in the qualitative results section are intended to lend weight to the statements, but generalization across all teams (including the remaining software teams of the company) is difficult due to the qualitative nature of the data. Furthermore, participation was voluntary, which might have led to biased sampling, as we might have gotten people with more interest in security and with a closer relationship to our executing researcher. Because the interviews were not conducted by someone external, this could have also had the effect of people withholding or falsifying information to please the interviewer. Still, we experienced people being very open in the interviews, which might be traced back to the fact that they were talking with someone from their community. We made sure to address different stakeholders from multiple teams of the development department, but we might have missed relevant stakeholders. Our overall approach worked well in our case, but it may not be adaptable for every case. For example, a development framework other than Scrum could be used, so the first part of the interview guide would have to be adapted slightly. Our findings or recommendations may not be transferable for every case, as company contexts with their structures and different individuals may differ from case to case. However, we conclude that understanding a context and its underlying problems in-depth is essential before setting up a strategy for change.

6 CONCLUSION

Within our study, security is almost exclusively driven by the security champions, but they receive only moderate to no support from the leadership. It is obvious from both the OWASP SAMM results (see 4.2) and the qualitative interviews (see 4.3) that there is no unified security strategy. Structural changes are necessary so that the topic of security is not only implicitly expected from development teams, but addressed strategically and thoroughly. Security champions are on their own, they do not have a specific contact person for security and they do not receive any kind of security training from the company. Although they are trusted by their colleagues and product owners, the entire burden for security matters lies solely with them. Security requirements of the products, as well as the development environment, are created at the level of the software teams. Whether resources are released for this is the decision of the respective product owner. As a result, each team pursues its own security strategy, but this has fatal consequences because all teams work on the same product. Due to past security incidents, there is currently still a high level of awareness of security within the development teams. However, as our case and others show, a high level of awareness does not necessarily lead to the adaption of secure behavior. Security champions cannot bear the entire burden of the issue of security alone. They need support in the form of training and education, as well as backing from leadership.

ACKNOWLEDGMENTS

Funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – EXC 2092 CaSa – 390781972.

REFERENCES

[1] Hege Aalvik, Anh Nguyen-Duc, Daniela Soares Cruzes, and Monica Iovan. 2023. Establishing a Security Champion in Agile Software Teams: A Systematic Literature Review. In *Future of Information and Communication Conference*. Springer, San Francisco, USA, 796–810.

[2] Yasemin Acar, Michael Backes, Sascha Fahl, Simson Garfinkel, Doowon Kim, Michelle L Mazurek, and Christian Stransky. 2017. Comparing the usability of cryptographic apis. In *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Jose, CA, USA, 154–171.

[3] Yasemin Acar, Michael Backes, Sascha Fahl, Doowon Kim, Michelle L Mazurek, and Christian Stransky. 2016. You get where you're looking for: The impact of information sources on code security. In *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Jose, CA, USA, 289–305.

[4] Yasemin Acar, Christian Stransky, Dominik Wermke, Charles Weir, Michelle L Mazurek, and Sascha Fahl. 2017. Developers need support, too: A survey of security advice for software developers. In *2017 IEEE Cybersecurity Development (SecDev)*. IEEE, Cambridge, USA, 22–26.

[5] Anne Adams and Martina Angela Sasse. 1999. Users are not the enemy. *Commun. ACM* 42, 12 (1999), 40–46.

[6] Hala Assal and Sonia Chiasson. 2018. Security in the software development lifecycle. In *Fourteenth symposium on usable privacy and security (SOUPS 2018)*. USENIX Association, Boston,USA, 281–296.

[7] Hala Assal and Sonia Chiasson. 2019. 'Think secure from the beginning' A Survey with Software Developers. In *Proceedings of the 2019 CHI conference on human factors in computing systems*. Association for Computing Machinery, New York, NY, USA, 1–13.

[8] Maria Bada, Angela M Sasse, and Jason RC Nurse. 2019. Cyber security awareness campaigns: Why do they fail to change behaviour? https://doi.org/10.48550/arXiv.1901.02672

[9] Rebecca Balebako and Lorrie Cranor. 2014. Improving app privacy: Nudging app developers to protect user privacy. *IEEE Security & Privacy* 12, 4 (2014), 55–58.

[10] Rebecca Balebako, Abigail Marsh, Jialiu Lin, Jason I Hong, and Lorrie Faith Cranor. 2014. The privacy and security behaviors of smartphone app developers. *Workshop on Usable Security (USEC 2014)* February (2014), 1–10.

[11] Ingolf Becker, Simon Parkin, and M Angela Sasse. 2017. Finding security champions in blends of organisational culture. *Proc. USEC* 11 (2017), 124.

[12] Odette Beris, Adam Beautement, and M Angela Sasse. 2015. Employee rule breakers, excuse makers and security champions: Mapping the risk perceptions and emotions that drive security behaviors. In *Proceedings of the 2015 New Security Paradigms Workshop*. Association for Computing Machinery, New York, NY, USA, 73–84.

[13] Melanie Birks, Ysanne Chapman, and Karen Francis. 2008. Memoing in qualitative research: Probing data and processes. *Journal of research in nursing* 13, 1 (2008), 68–75.

[14] David Botta, Rodrigo Werlinger, André Gagné, Konstantin Beznosov, Lee Iverson, Sidney Fels, and Brian Fisher. 2007. Towards understanding IT security professionals and their tools. In *Proceedings of the 3rd symposium on Usable privacy and security*. Association for Computing Machinery, New York, NY, USA, 100–111.

[15] BSIMM. 2022. Building Security In Maturity Models. https://www.bsimm.com/ Accessed: August 2022.

[16] Deanna D Caputo, Shari Lawrence Pfleeger, M Angela Sasse, Paul Ammann, Jeff Offutt, and Lin Deng. 2016. Barriers to usable security? Three organizational case studies. *IEEE Security & Privacy* 14, 5 (2016), 22–32.

[17] Ann Cavoukian et al. 2009. Privacy by design: The 7 foundational principles. *Information and privacy commissioner of Ontario, Canada* 5 (2009), 2009.

[18] Council of the European Union. 2022. Cybersecurity: how the EU tackles cyber threats. https://www.consilium.europa.eu/en/policies/cybersecurity/ Accessed: August 2022.

[19] Anastasia Danilova, Alena Naiakshina, Johanna Deuter, and Matthew Smith. 2020. Replication: On the Ecological Validity of Online Security Developer Studies: Exploring Deception in a {Password-Storage} Study with Freelancers. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, Boston,USA, 165–183.

[20] Anastasia Danilova, Alena Naiakshina, Anna Rasgauski, and Matthew Smith. 2021. Code Reviewing as Methodology for Online Security Studies with Developers - A Case Study with Freelancers on Password Storage. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. USENIX Association, Virtual Event, 397–416. https://www.usenix.org/conference/soups2021/presentation/danilova

[21] Constanze Dietrich, Katharina Krombholz, Kevin Borgolte, and Tobias Fiebig. 2018. Investigating system operators' perspective on security misconfigurations. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. Association for Computing Machinery, New York, NY, USA, 1272–1289.

[22] Thomas Ellwart and Annette Kluge. 2019. Psychological Perspectives on Intentional Forgetting: An Overview of Concepts and Literature. In *KI - Künstliche Intelligenz: Vol. 33, No. 1*. Springer Nature, Berlin Heidelberg, 79–84. https://doi.org/10.1007/s13218-018-00571-0

[23] Felix Fischer, Konstantin Böttinger, Huang Xiao, Christian Stransky, Yasemin Acar, Michael Backes, and Sascha Fahl. 2017. Stack overflow considered harmful? the impact of copy&paste on android application security. In *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Jose, CA, USA, 121–136.

[24] Felix Fischer and Jens Grossklags. 2022. Nudging Software Developers Toward Secure Code. *IEEE Security & Privacy* 20, 02 (2022), 76–79.

[25] Dinei Florêncio, Cormac Herley, and Baris Coskun. 2007. Do strong web passwords accomplish anything? *HotSec* 7, 6 (2007), 159.

[26] B.J. Fogg. 2020. *Tiny Habits: The Small Changes that Change Everything*. Houghton Mifflin Harcourt, Boston, USA.

[27] Brian J Fogg. 2009. A behavior model for persuasive design. In *Proceedings of the 4th international Conference on Persuasive Technology*. Association for Computing Machinery, New York, NY, USA, 1–7.

[28] Center for Strategic and International Studies. 2023. Significant Cyber Incidents. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents Accessed: June 2023.

[29] Trevor Gabriel and Steven Furnell. 2011. Selecting security champions. *Computer Fraud & Security* 2011, 8 (2011), 8–12.

[30] Lisa Geierhaas, Anna-Marie Ortloff, Matthew Smith, and Alena Naiakshina. 2022. {Let's} Hash: Helping Developers with Password Security. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. USENIX Association, Boston,USA, 503–522.

[31] Google. 2021. Supply-chain Levels for Software Artifacts (SLSA). https://cloud.google.com/blog/products/application-development/google-introduces-slsa-framework Accessed: August 2022.

[32] Peter Leo Gorski, Luigi Lo Iacono, Dominik Wermke, Christian Stransky, Sebastian Möller, Yasemin Acar, and Sascha Fahl. 2018. Developers deserve security warnings, too: On the effect of integrated security advice on cryptographic {API} misuse. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association, Boston, USA, 265–281.

[33] David Graeber. 2016. *Bürokratie: die Utopie der Regeln*. Klett-Cotta, Stuttgart, Germany.

[34] Matthew Green and Matthew Smith. 2015. Developers Are Users Too: Designing Crypto and Security APIs That Busy Engineers and Sysadmins Can Use Securely. https://www.usenix.org/comment/536

[35] Matthew Green and Matthew Smith. 2016. Developers are not the enemy!: The need for usable security apis. *IEEE Security & Privacy* 14, 5 (2016), 40–46.

[36] Marco Gutfleisch, Jan H. Klemmer, Niklas Busch, Yasemin Acar, M. Angela Sasse, and Sascha Fahl. 2022. How Does Usable Security (Not) End Up in Software Products? Results From a Qualitative Interview Study. In *43rd IEEE Symposium on Security and Privacy, IEEE S&P 2022, May 22-26, 2022*. IEEE Computer Society, San Francisco, CA, USA, 893–910.

[37] Joseph Hallett, Nikhil Patnaik, Benjamin Shreeve, and Awais Rashid. 2021. "Do this! Do that!, And nothing will happen" Do specifications lead to securely stored passwords?. In *2021 IEEE/ACM 43rd International Conference on Software Engineering (ICSE)*. IEEE, Madrid, ES, 486–498.

[38] Julie M Haney, Mary Theofanos, Yasemin Acar, and Sandra Spickard Prettyman. 2018. " we make it a big deal in the company": Security mindsets in organizations that develop cryptographic products. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association, Boston, USA, 357–373.

[39] Jonas Hielscher, Annette Kluge, Uta Menges, and M. Angela Sasse. 2021. "Taking out the Trash": Why Security Behavior Change Requires Intentional Forgetting. In *New Security Paradigms Workshop (NSPW '21)*. Association for Computing Machinery, Virtual Event, USA, 108–122.

[40] ISO/IEC. 2013. ISO/IEC 27001: Information Security Management Report. https://www.iso.org/isoiec-27001-information-security.html Accessed: August 2022.

[41] Martin Gilje Jaatun and Daniela Soares Cruzes. 2021. Care and Feeding of Your Security Champion. In *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*. IEEE, Dublin, Ireland, 1–7. https://doi.org/10.1109/CyberSA52016.2021.9478254

[42] John P Kotter. 2012. *Leading change*. Harvard business press, MA, USA.

[43] Katharina Krombholz, Karoline Busse, Katharina Pfeffer, Matthew Smith, and Emanuel Von Zezschwitz. 2019. " If HTTPS Were Secure, I Wouldn't Need 2FA"-End User and Administrator Mental Models of HTTPS. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Francisco, USA, 246–263.

[44] Katharina Krombholz, Wilfried Mayer, Martin Schmiedecker, and Edgar Weippl. 2017. " I Have No Idea What I'm Doing"-On the Usability of Deploying {HTTPS}. In *26th USENIX Security Symposium (USENIX Security 17)*. USENIX Association, Vancouver, Canada, 1339–1356.

[45] Udo Kuckartz. 2014. *Qualitative text analysis: A guide to methods, practice & using software.* SAGE, Los Angeles and London and New Delhi and Singapore and Washington, DC.

[46] Uta Menges, Jonas Hielscher, Annalina Buckmann, Annette Kluge, M Angela Sasse, and Imogen Verret. 2021. Why IT Security Needs Therapy. In *European Symposium on Research in Computer Security*. Springer, Darmstadt, Germany, 335–356.

[47] Uta Menges, Jonas Hielscher, Annalina Buckmann, Annette Kluge, M Angela Sasse, and Imogen Verret. 2022. Why IT Security Needs Therapy. In *Computer Security. ESORICS 2021 International Workshops: CyberICPS, SECPRE, ADIoT, SPOSE, CPS4CIP, and CDT&SECOMANE, Darmstadt, Germany, October 4–8, 2021, Revised Selected Papers*. Springer, Darmstadt, Germany, 335–356.

[48] Micorsoft. 2022. Microsoft Security Development Lifecycle. https://www.microsoft.com/en-us/securityengineering/sdl Accessed: August 2022.

[49] Patrick Morrison. 2015. A security practices evaluation framework. In *2015 IEEE/ACM 37th IEEE International Conference on Software Engineering*, Vol. 2. IEEE, Florence, Italy, 935–938.

[50] Alena Naiakshina, Anastasia Danilova, Eva Gerlitz, Emanuel Von Zezschwitz, and Matthew Smith. 2019. " If you want, I can store the encrypted password" A Password-Storage Field Study with Freelance Developers. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ssociation for Computing Machinery, Scotland, UK, 1–12.

[51] Alena Naiakshina, Anastasia Danilova, Christian Tiefenau, Marco Herzog, Sergej Dechand, and Matthew Smith. 2017. Why do developers get password storage wrong? A qualitative usability study. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. Association for Computing Machinery, New York, NY, USA, 311–328.

[52] Alena Naiakshina, Anastasia Danilova, Christian Tiefenau, and Matthew Smith. 2018. Deception task design in developer password studies: Exploring a student sample. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association, Baltimore, USA, 297–313.

[53] National Cyber Security Centre (NCSC). 2021. Semi-annual report 2021/2. , 21-22 pages. https://www.ncsc.admin.ch/dam/ncsc/en/dokumente/dokumentation/lageberichte/NCSC_2021-2_HJB_EN.pdf.download.pdf/NCSC_2021-2_HJB_EN.pdf Accessed: June 2023.

[54] NIST. 2022. National Institute of Standards and Technology Cybersecurity Framework. https://www.nist.gov/cyberframework Accessed: August 2022.

[55] Open Web Application Security Project. 2022. Open Web Application Security Project Software Assurance Maturity Model. https://owaspsamm.org/ Accessed: August 2022.

[56] Open Web Application Security Project. 2023. Security Champions Playbook. https://owasp.org/www-project-security-culture/v10/4-Security_Champions/ Accessed: February 2023.

[57] OWASP. 2021. Application Security Verification Standard (ASVS). https://owasp.org/www-project-application-security-verification-standard/ Accessed: August 2022.

[58] Andreas Poller, Laura Kocksch, Sven Türpe, Felix Anand Epp, and Katharina Kinder-Kurlanda. 2017. Can security become a routine? A study of organizational change in an agile software development group. In *Proceedings of the 2017 ACM conference on computer supported cooperative work and social computing*. Association for Computing Machinery, New York, NY, USA, 2489–2503.

[59] S Pressman Roger and R Maxin Bruce. 2015. *Software engineering: a practitioner's approach.* McGraw-Hill Education, London, UK.

[60] Angela Sasse. 2015. Scaring and bullying people into security won't work. *IEEE Security & Privacy* 13, 3 (2015), 80–83.

[61] Martina Angela Sasse, Sacha Brostoff, and Dirk Weirich. 2001. Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT technology journal* 19, 3 (2001), 122–131.

[62] M Angela Sasse and Matthew Smith. 2016. The Security-Usability Tradeoff Myth [Guest editors' introduction]. *IEEE Security and Privacy* 14, 5 (2016), 11–13.

[63] M Angela Sasse, Matthew Smith, Cormac Herley, Heather Lipford, and Kami Vaniea. 2016. Debunking security-usability tradeoff myths. *IEEE Security & Privacy* 14, 5 (2016), 33–39.

[64] Ken Schwaber and Jeff Sutherland. 2020. The Scrum Guide.

[65] PM Senge. 1990. The Fifth Discipline. *Currency, Sydney* 1, 3 (1990), 104–17.

[66] Christian Stransky, Oliver Wiese, Volker Roth, Yasemin Acar, and Sascha Fahl. 2022. 27 Years and 81 Million Opportunities Later: Investigating the Use of Email Encryption for an Entire University. In *43rd IEEE Symposium on Security and Privacy, IEEE S&P 2022, May 22-26, 2022*. IEEE Computer Society, San Francisco, CA, USA, 860–875.

[67] Jose M Such, Antonios Gouglidis, William Knowles, Gaurav Misra, and Awais Rashid. 2016. Information assurance techniques: Perceived cost effectiveness. *Computers & Security* 60 (2016), 117–133.

[68] Mohammad Tahaei, Alisa Frik, and Kami Vaniea. 2021. Deciding on Personalized Ads: Nudging Developers About User Privacy. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. USENIX Association, Virtual Event, USA, 573–596.

[69] Mohammad Tahaei and Kami Vaniea. 2019. A survey on developer-centred security. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, Stockholm, Sweden, 129–138.

[70] Richard H. Thaler and Cass R. Sunstein. 2022. *Nudge.* Econ, Berlin, Germany.

[71] Tyler W Thomas, Madiha Tabassum, Bill Chu, and Heather Lipford. 2018. Security during application development: An application security expert perspective, In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. *arXiv preprint arXiv:2205.02544* 1, 1–12. https://doi.org/10.1145/3173574.3173836

[72] S Türpe, L Kocksch, and A Poller. 2016. Penetration Tests a Turning Point in Security Practices? Organizational Challenges and Implications in a Software Development {Team}. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, Denver, USA, 197850.

[73] United Kingdom Department for Digital, Culture, Media & Sport. 2022. Businesses urged to boost cyber standards as new data reveals nearly a third of firms suffering cyber attacks hit every week. https://www.gov.uk/government/news/businesses-urged-to-boost-cyber-standards-as-new-data-reveals-nearly-a-third-of-firms-suffering-cyber-attacks-hit-every-week Accessed: August 2022.

[74] VERBI Software. 2022. MAXQDA. https://www.maxqda.com/ Accessed: August 2022.

[75] Charles Weir, Sammy Migues, Mike Ware, and Laurie Williams. 2021. Infiltrating security into development: exploring the world's largest software security study. In *Proceedings of the 29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*. Association for Computing Machinery, New York, NY, USA, 1326–1336.

[76] Alma Whitten and J Doug Tygar. 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0.. In *USENIX security symposium*, Vol. 348. USENIX Association, Monterey, USA, 169–184.

[77] Mary Ellen Zurko and Richard T Simon. 1996. User-centered security. In *Proceedings of the 1996 workshop on New security paradigms*. Association for Computing Machinery, Arrowhead, USA, 27–33.

A APPENDICES

In this section, we present the artifacts needed for replication. This includes the interview guides for Software Developers and Development Operations A.1, Scrum Master A.2, and Product Owner A.3, as well as the codebook Table 4 used for analysis.

A.1 Interview Guide - Software Developers & Development Operations

Onboarding.

Problems & Challenges. Tell me about a case where you developed something related to security.

(1) Communication & Planning
- How specific were the requirements?
  - Did you specify concrete security goals?
  - How did you approach estimating the user story?
    - ∗ Was there someone who took the lead in the process?
    - ∗ Were there any uncertainties?
  - Was the approach different from other user stories that did not include security features?
- If we now look at the first phase up to the end of the assessment - what did not go so well or where were problems?
  - Were there any similar problems in other projects?

(2) Modeling
- How was the first architectural design created?
  - Who was involved?
  - Which resources did you access? (Google? Official documentation? ...)

- If we now look at this phase again - what did not go so well or where were problems?
  - Were there any similar problems in other projects?

(3) Construction
- How was the implementation proceeded?
  - Who was involved?
  - Who is usually involved?
  - What resources did you access when implementing? (Google? Official documentation? ...)
    - ∗ Was anything done differently than usual?
  - How was your code tested?
- What did not work so well or where were problems?
  - Were there any similar problems in other projects?

(4) Deployment
- Could you describe to me the process of how the security feature reached the customer?
  - What exactly did the deployment process look like?
- What didn't go so well or where were problems?
  - Were there any similar problems in other projects?

(5) Usable Security
- How important is the usability of a security feature? (e.g. login)
- Who is responsible for it?
- Is anything done differently when usability of a security feature is concerned?
  - Are more resources invested?
  - Are any other tests conducted?

Security Perceptions & Opinions.

(1) How do you think usability and security are connected?
- Are they connected at all?

(2) Imagine that a major security vulnerability is found in a feature that your team has developed.
- How likely do you think this is?
- What could have led to this?
  - Who would you blame for this?
- How would this problem be dealt with / what would the solution process look like?

(3) Is enough being done for security in your opinion?
- Why?/Why not?
- What are the reasons?
- What should be improved?
- Are you getting enough resources for this?
- How do your colleagues see it?
- Do you talk about security enough within the team?
- Who do you think is responsible for security?
  - How do you see your role in relation to security?

(4) If you look again at the measures for security in development and the resources you get for it, how important would you say is the topic of security to the management?
- How important is the topic for your product owner?

(5) What motivates you or other colleagues to develop secure software?

(6) In conclusion to your interview, what would you like to tell the management about security?

(7) Is there anything you would like to have on the topic of security?

Offboarding.

(1) Is there anything else that you would like to tell?

(2) Do you have any questions?

A.2 Interview Guide - Scrum Master

Onboarding.

Problems & Challenges. I want to take a look at some of the meetings with you and hear your impression of how the team and the product owner dealt with the issue of security.

(1) Planning I + II
- What role does the topic of security play in Planning I and II?
- How do we deal with stories where security plays a role?
  - Do discussions take place more often?
- Did you notice anything else in these meetings that went well or not so well in relation to security?

(2) Refinement
- What role does security play in Refinement?
- What is the assessment process when it concerns the topic of security?
- Were there specific requirements for the security of certain features?
  - How specific were the requirements?
  - Did the team have any problems with them?
- Did you notice anything else about these meetings that went well or not so well related to security?

(3) Daily
- What role does security play in the Dailies?

(4) Other meetings
- Has the team ever addressed the issue of security in any other way?
  - What were the problems?
  - How were the problems dealt with?
- How does it look like in other meetings outside the team? Was there ever anything related to security?

(5) Usable Security
- How important is the usability of a security feature? (e.g. login)
- Who is responsible for it?
- Is anything done differently when usability of a security feature is concerned?
  - Are more resources invested?
  - Are any other tests conducted?

Security Perceptions & Opinions.

(1) How do you think usability and security are connected?
- Are they connected at all?

(2) Imagine that a major security vulnerability is found in a feature that your team has developed.
- How likely do you think this is?
- What could have led to this?
  - Who would you blame for this?
- How would this problem be dealt with / what would the solution process look like?

(3) Is enough being done for security in your opinion?
- Why?/Why not?

- What are the reasons?
- What should be improved?
- Are you getting enough resources for this?
- How do your colleagues see it?
- Do you talk about security enough within the team?
- Who do you think is responsible for security?
  - How do you see your role in relation to security?

(4) If you look again at the measures for security in development and the resources you get for it, how important would you say is the topic of security to the management?
  - How important is the topic to the product owner?
  - How important is the topic to the developers?

(5) What motivates you to get involved in security? What do you think motivates your colleagues to develop secure software?

(6) In conclusion to your interview, what would you like to tell the management about security?

(7) Is there anything you would like to have on the topic of security?

Offboarding.

(1) Is there anything else that you would like to tell?
(2) Do you have any questions?

A.3 Interview Guide - Product Owner

Onboarding.

Problems & Challenges. Tell me about a case where the team has developed something related to security.

(1) Communication & Planning
  - How specific were the requirements?
    - Did you specify concrete security goals?
    - How was the issue of security discussed with you in the specific case?
      * How specific were the security requirements?
      * How was it with other stories?
  - Were there any disagreements or uncertainties related to security?
  - How did you communicate the specific feature to the team?
  - Did you specify security goals?
  - How did you approach the estimation?
    - Was there someone who took the lead in the process?
    - Were there any uncertainties?
  - Was the approach different from other user stories that did not include security features?
  - If we now look at the first phase up to the end of the assessment - what did not go so well or where were problems?
    - Were there any similar problems in other projects?
  - Do you usually have a specific contact person when it concerns security?
  - How does the team split up?

(2) Modeling
  - How was the first architectural design created?
    - Who was involved?
    - What resources did you access? (Google? Official documentation? ...)
  - If we now look at this phase again - What did not go so well or where were problems?
  - Were there any similar problems in other projects?

(3) Construction
  - Were there any problems in the implementation phase in the particular case?
  - Did the team get back to you?
    - How did it compare to other stories with security content?

(4) Deployment
  - Could you describe to me the process of how the security feature reached the customer?
    - How exactly did your deployment process look like?
  - What didn't go so well or where were problems?
    - Were there any similar problems in other projects?

(5) Usable Security
  - How important is the usability of a security feature? (e.g. login)
  - Who is responsible for it?
  - Is anything done differently when usability of a security feature is concerned?
    - Are more resources invested?
    - Are any other tests conducted?

Security Perceptions & Opinions.

(1) How do you think usability and security are connected?
  - Are they connected at all?

(2) Imagine that a major security vulnerability is found in a feature that your team has developed.
  - How likely do you think this is?
  - What could have led to this?
    - Who would you blame for this?
  - How would this problem be dealt with / what would the solution process look like?

(3) Is enough being done for security in your opinion?
  - Why?/Why not?
  - What are the reasons?
  - What should be improved?
  - Are you getting enough resources for this?
  - How do your colleagues see it?
  - Do you talk enough about security within the team?
  - Who do you think is responsible for security?
    - How do you see your role in relation to security?

(4) If you look again at the measures for security in development and the resources you get for it, how important would you say is the topic of security to the management?
  - How important is the topic to your product owner?

(5) What does motivate you or other colleagues to develop secure software?

(6) In conclusion to your interview, what would you like to tell the management about security?

(7) Is there anything you would like to have on the topic of security?

Offboarding.

(1) Is there anything else that you would like to tell?
(2) Do you have any questions?

B TABLES & FIGURES

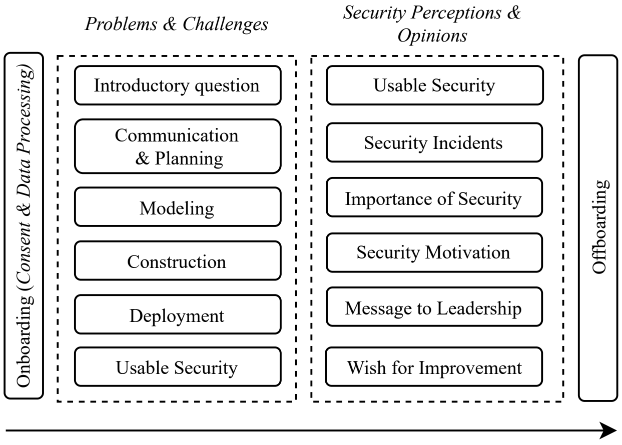

Figure 2: Interview Guide

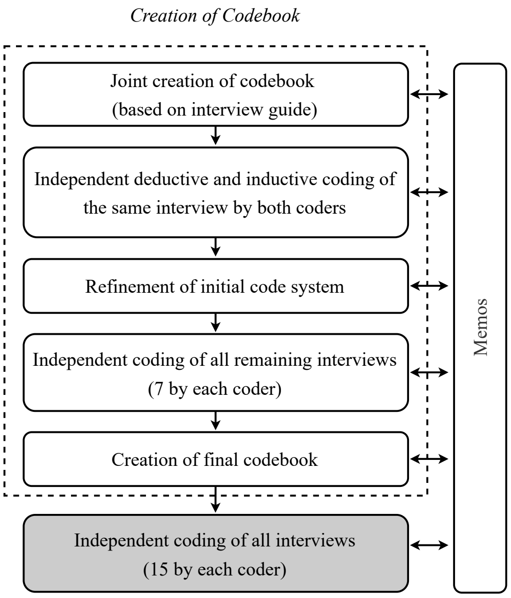
Creation of Codebook
Joint creation of codebook (based on interview guide)
Independent deductive and inductive coding of the same interview by both coders
Refinement of initial code system
Independent coding of all remaining interviews (7 by each coder)
Creation of final codebook
Independent coding of all interviews (15 by each coder)
Memos

Figure 3: Coding Process

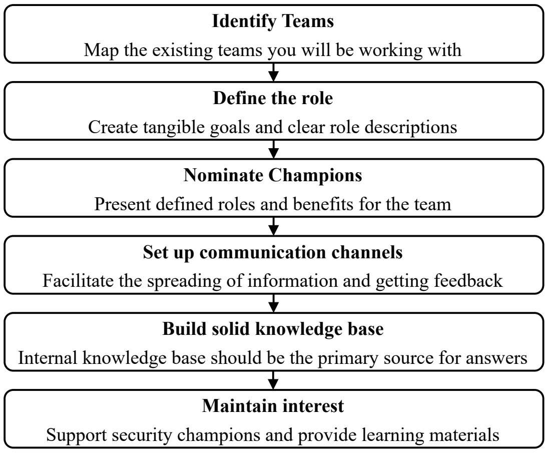
Identify Teams
Map the existing teams you will be working with
Define the role
Create tangible goals and clear role descriptions
Nominate Champions
Present defined roles and benefits for the team
Set up communication channels
Facilitate the spreading of information and getting feedback
Build solid knowledge base
Internal knowledge base should be the primary source for answers
Maintain interest
Support security champions and provide learning materials

Figure 4: Illustration of Phases from the OWASP's Security Champions Playbook [56]

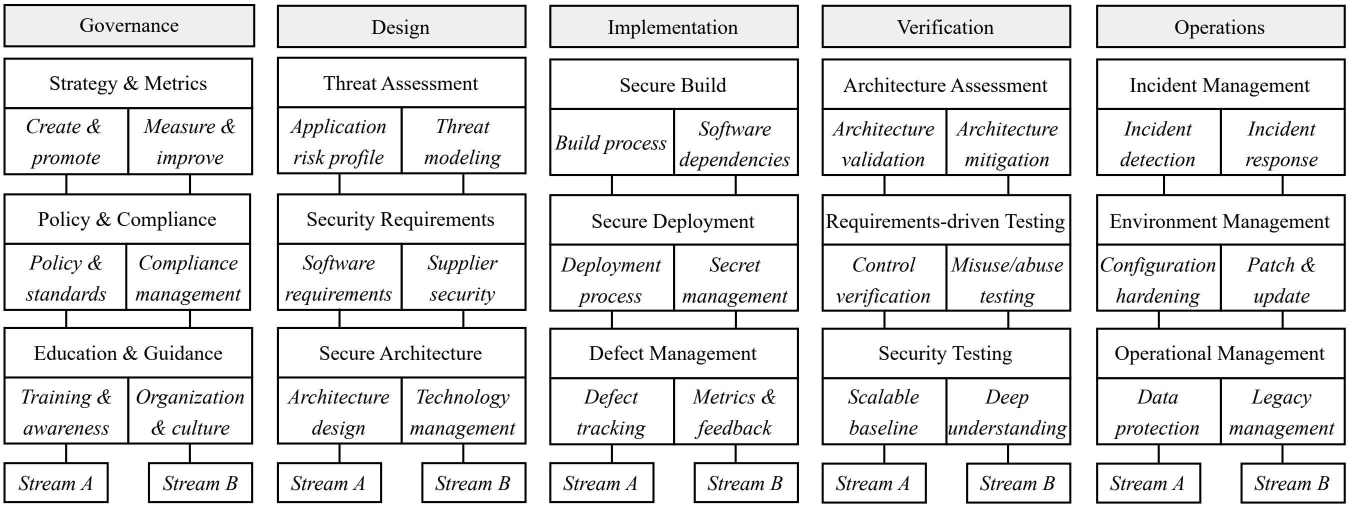

Figure 5: OWASP SAMM Model

B.1 Codebook

Table 4: Codebook

Code	Description	***Example Quote***
Usable Security	–	–
Usec. Perception	Participants described a scientifically correct (meaning that usability can enhance security) or a scientifically wrong perception about the interaction of security & usability (meaning that there is a trade-off between them)	*So security must always be usable, otherwise it will not be used. (P5)*
Usec. in Software Development	Participants described how usable security is handled in the software development process	*[..]]but also yes in that case the UX designers, if you say now related to the UI, of course, the UX is also included, but the developer should also develop that so that that it runs without problems. (P3)*
Security Incident	–	–
Mitigation Strategy	Participants described specific mitigation strategies on how they or the organization would react to a security incident	*[...]We would discuss it in the team and then someone would get to work on the solution in a timely manner and, as I said, we basically have two, uh, four-eyes principle, one fixes it, the other reviews it and then we would just try to clear it up as quickly as possible. (P7)*
Incident Likeliness	Statements that implicate that participants did think or didn't think that security incidents were likely to happen	*I think that is quite unlikely. (P14)*
Effects on Security Perceptions	Participants described how the occurrence of one or more security incidents affected their or other's perception of security processes or security in general	*[...]the topic that has to do with the customer is then of course particularly sensitized, that customer data is really treated according to all the regulations and legal requirements. (P9)*
Communication	Participants described cases in which the communication in the organization was good or lacking/bad and/or the reasons why	*[...] it's not that we regularly talk about it in the team meeting or something, have we actually checked it or something, but rather, as I said, on an occasion-related basis. (P7)*
Processes	–	–
Technical & Organizational Challenges & Problems	Participants described technical or organizational processes in the organization that had a negative impact on security	*[...] it's also possible that there is simply no patch for a security vulnerability. And then you can't deploy until there is a patch. That's a state that you can't accept. (P2)*
Requirements & Story Refinement	Participants described the role and/or challenges of security in the requirements and refinement process	*Well, we do it together. In Refinement, we talk about the tickets until they are ready. And then in planning, we talk about the tickets again, and then in planning II we have the technical meeting, so to speak, where we talk about the tickets again explicitly with the developers. (P2)*
Security Perceptions	–	–
Developers & DevOps	Participants described their own (if developer or DevOps) or other developer's or DevOps' perceptions about security and their role in the organization	*I think security is important to most people, but I also think there is room for improvement in terms of mindset. (P6)*
Security Leads	Participants described their own (if security lead) or other security lead's perceptions about security and their role in the organization	*I actually have a good feeling about this, but that's also due to the fact that I have a lot of trust in our DevOps and the sec leads, so I simply trust them. (P4)*
Product Owners	Participants described their own (if product owner) or other product owner's perceptions about security and their role in the organization	*For this, you would have to get time from the PO, from the product owner, so that you can deal with exactly such things. Most of the time, a feature has been developed and the new feature is to be developed. (P7)*
Management & Leadership	Participants described management and leadership's perceptions about security and their role in the organization	*As long as nothing happens, I'm convinced that the issue of safety doesn't really play a role, and I don't even mean that in a bad way. They simply assume that this is naturally part of our work and is taken into account accordingly. (P15)*
Responsibility	Participants described who they thought was responsible for security in the organization and what implication this had	*Well, with the whole team. So, we are all responsible for making sure that everything runs smoothly. (P3)*
Message to Leadership	Participants answered a specific question about what they would like to tell leadership about security in the organization	*I could only recommend to the management that they show more interest, i.e. that they take a more businesslike look at issues that are more sustainable and that affect us all, that affect them as people, as individuals, as private persons, as well as business people in their function as management, and that they perhaps also ask questions in a more interested, not more critical, but more interested way and enter into the dialog. (P10)*