

# Understanding the Usage of IT-Security Games in the Industry and Its Mapping to Job Profiles

Tilman Dewes  

Siemens AG, München, Germany

Tiago Gasiba  

Siemens AG, München, Germany

Thomas Schreck  

Hochschule für angewandte Wissenschaften München, Germany

---

## Abstract

Due to the increasing dependency on IT systems in both the private and industrial sectors, IT security training is becoming increasingly important. One way to teach IT security topics is through serious games, which besides being fun to play, impart knowledge on certain topics. As these games are more and more used in the industrial environment, this paper aims to develop a mapping between industrial roles and the games to show which game fits how well for the training of an industrial role. In doing so, an evaluation of the games was established that allows for comparability across the different roles. Thus, the research question which serious games is suitable for which industrial role could be addressed. Further results of the work are an ontology, which contains the essential characteristics of serious games for this work, a collection of industrial roles with their required IT-skills and a collection of serious games with an evaluation of the level of support of IT-skills.

**2012 ACM Subject Classification** Applied computing → Learning management systems; Security and privacy → Software security engineering; Applied computing → Distance learning; Applied computing → E-learning

**Keywords and phrases** Serious Games, IT-Security, Industrial Roles, Mapping, Ontology

**Digital Object Identifier** 10.4230/OASICS.ICPEEC.2022.3

## 1 Introduction

Obtaining practical IT security skills takes much effort. To acquire the required level of skills, it often takes “a long journey of discovery, trial and error, and optimization seeking through a broad range of programming activities that learners must perform themselves.” [12]. In order to ensure secure systems in today’s world, where the dependency of companies on IT systems continues to grow, programmers must be adequately trained. Especially because in the last few years, there has been an increase in IT attacks of all kinds, as the current version of the report on the state of IT security in Germany [2] shows.

One possibility to impart knowledge in the area of IT security offers *Serious Games* [4]. These games with a pedagogical learning background usually impart knowledge in a particular topic through gameplay. As the work of Lui et al. [10] and Švábenský et al. [15] shows, game-based learning offers an effective way of teaching security-related scenarios. However, the field of Serious Games in the IT security is diverse and ranges from the conventional board and card games to Capture the Flag- (CTF) and other Cyber Security Challenges (CSC) [6].

Mainly, these games are produced by many developers, which is why a general disorder of games prevails, also with variations in terms of quality as shown in the work of Caserman et al. [3]. Although the work of Katsantonis et al. [9] shows that frameworks for Serious Games in the field of IT-Security are available, these are only aimed at the development of the games, not at publication or description. Consequently, the games are scattered distributed



© Tilman Dewes, Tiago Gasiba, and Thomas Schreck;  
licensed under Creative Commons License CC-BY 4.0

Third International Computer Programming Education Conference (ICPEEC 2022).

Editors: Alberto Simões and João Carlos Silva; Article No. 3; pp. 3:1–3:12

OpenAccess Series in Informatics



OASICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

## 3:2 Usage of IT-Security Games in the Industry and Its Mapping to Job Profiles

throughout the world wide web, often with inadequate descriptions and unclear educational goals. As a result, it is often unclear which game is suitable for which situation, especially in an industrial environment. In particular, it is unclear which games can be used to promote the know-how needed for specific industrial roles. Considering all these circumstances, it becomes clear that there is a need for a clearer structure in this area, especially since the games are often not focused on the industry and its requirements (Gasiba et al. [5]).

The contribution of this work is to present a framework for the selection of Serious Games for people in industrial environments. It highlights how well a game is suitable for the training of an industrial role compared to other games. Therefore, a mapping process for existing Serious Games to industrial roles is presented in this work. The methodology of this work is adaptable to non-industrial educational activities and students and pupils. By contributing a proposal on the selection of games when using them for education, we believe that this work contributes to a better structure and clearer arrangement of the topic of Serious Games.

The next section provides an overview of relevant related work on this topic. Section 3 describes the methodology that was used to achieve the goals of this work. Section 4 then states the achieved results of the approach. These are then discussed in section 5, put into context, and consequences drawn from them. In the 6th section, all points of the work are briefly summarized, and an outline of further work is given.

## 2 Related Work

In order to gather the necessary information, the topic of serious games, in general, was considered first. The paper of Stephen Tang and Martin Hanneghan [14] served as a first introduction to the topic of serious games. It describes a broad ontology that describes serious games in detail with all their characteristics. However, the level of detail is relatively high, and therefore much information is superfluous for the goal of this work. Furthermore, the ontology presented by the authors does not aim at mapping games to roles. Nevertheless, their work serves as a basis for building our ontology. This work was considered relevant, although it is older than 2016, since the information of the paper is up to date and no comparable more recent work could be found regarding ontology in the field of serious games.

In order to determine relevant industrial roles, the company internally published job descriptions were considered. These roles were derived from the Product Solution Security (PSS) Curriculum. The PSS Curriculum is a pictorial representation of the organization within the company to ensure product security. Eight different job profiles were considered relevant through additional expert interviews and internal research. A distinction was made between two types of product solution officers and six different types of product solution experts. The only difference between the two types of officers is the scope of the systems to be supported. The classic Product Solution Security Officer (PSSO) usually operates on a hierarchically lower level and reports to the Principal Product Solution Security Officer (PPSSO). Even though the scope of their tasks is similar, their skillsets differ, as different skills are required at different hierarchical levels. In addition, six different areas were identified in which the Product Solution Security Experts (PSSE) specialize. The following areas of expertise were considered: Expert in Secure Architecture, Implementation, Testing, Manufacturing, Service, and Project Integration. These job profiles contained information about which skills are in demand at what level in which role and served as an essential basis for mapping the Serious Games to them.

Adam Shostack describes himself on his homepage [13] as one of the leading experts in threat modeling and a consultant, expert witness, author, and game designer. He has designed games such as Elevation of Privilege and researched serious games. He presents a collection of physical board and card games that have an IT security learning objective on his website. This collection serves as the basis for the mapping. However, it had to be expanded with information to guarantee a successful mapping. Furthermore, some games were outdated, are no longer sold, or are so similar to other games that they had to be trimmed from the list.

Hill et al. [8] provide a survey of serious games used in cybersecurity education and training. A categorization of the games was carried out into four types based on the topics they cover and the purposes of the games: security awareness, network, and web security, cryptography, and secure software development. The paper then offers a catalog of serious games for different target audiences. However, their work does not consider industrial roles but mainly targets groups in the school environment. Also, no evaluation was performed, but the games were recommended only on the authors' assessment. Furthermore, the categorization for recommendations in the industrial environment is too superficial and does not sufficiently reflect the required skills of the roles.

Gasiba et al. [5] investigate the requirements for Serious Games geared towards software developers in the industry, with the focus on CTFs. It was found that although there are a lot of games available, they are mainly developed for pen-testers and white hackers. Software developers receive little attention; hence there is little information about the challenge design requirements in the secure coding area, especially in the industry. This paper was already an essential indication for this work that industrial roles are neglected in the development of serious games.


Hendrix et al. [7] investigate whether Serious Games are suitable for cybersecurity training. The authors examined several serious games in the IT security context. It was found that games are effective cyber security training tools. Nevertheless, some quality deficiencies could be identified. For example, some of the games were not evaluated, or the overall topic of the game was not clearly communicated. In the end, they conclude that “there is a clear gap in target audience with almost all products and studies targeting the general public and very little attention given to IT professionals and managers”[7]. This work clarified that the subject area of serious games in IT security needs to be more clearly structured and better aligned with the industry.

### 3 Methodology

In order to develop a suitable mapping process of Serious Games to industrial roles, the procedure was divided into five major steps, which are illustrated by the following graphic:

■ **Table 1** Mapping Methodology and Outcome.

<b>Step:</b>	Literature Review	Expert Interviews	Role Research	Game Research	Mapping
<b>Outcome:</b>	Ontology	Evaluated Ontology	Industrial Roles and Skills Collection	Game Collection	Game/Role Mapping
<b>Duration: (in Weeks)</b>	4	2	2	4	3



## 3:4 Usage of IT-Security Games in the Industry and Its Mapping to Job Profiles

As can be seen, the steps were performed sequentially and produced different results. The results are presented in detail in Chapter 4. In this chapter the methodology is clarified by describing the steps in detail.

### 3.1 Literature Review

A literature review was conducted as an initial introduction to the topic. Primarily the google scholar database, other search engines like researchgate or springer were used. These were searched for the keywords Serious Games, IT security, ontology, and efficiency. In addition, the work of Adam Shostack [13] was considered, who broadly gives information about Serious Games on his homepage. In the literature review, only works no older than 2016 were consulted, with two exceptions. The work of Stephen Tang and Martin Hanneghan [14], and from N. Noy and Deborah Mcguinness [11] are from the year 2011, and 2001. However, it was considered relevant for this work because the characteristics of Serious Games and ontologies have not changed in time, and this work contributed essential insights, especially for ontology development. The most important sources used are described in more detail in the Chapter 2. The literature review gained insights into how Serious Games can be used in the IT security context and what characterizes Serious Games in general. The results of the literature review are presented in detail in Chapter 4.

### 3.2 Expert-Interviews

After the literature review, the collected knowledge was evaluated in several expert interviews. A total of five security experts were interviewed. The interviews were conducted in January 2022 with experts from Germany who work in the company's Product Security Lifecycle. In all cases, an interview lasted between 30 and 60 minutes. In this process, the interviewees were first informed about the work's general aim, and then the knowledge gained through the literature review was presented in the form of an ontology. Based on the feedback from the experts, the ontology was shortened in superfluous places and supplemented in missing places. However, not only was the ontology evaluated, but also knowledge about contact points where know-how about internal/industrial roles, their skillset and Serious Games can be found was collected. Thus, the expert interviews were an essential step for the subsequent role research.

### 3.3 Role Research

The expert discussions described above determined that the focus should be on the Product Solution Security (PSS) Curriculum with its roles and respective skillset. The PSS curriculum represents and details the company's organization established to ensure product security. It maps job roles with their associated training. For the roles mentioned therein, detailed job profiles could be found, describing the roles with their functions and their required skills. Each skill has been assigned a skill level between Basic, Advanced, Expert, or none. Since the role descriptions were too confusing for quick comparison and evaluation, the relevant information was filtered out and transferred to a spreadsheet. The different skill levels were assigned numbers representing the skill level instead of the written word (Basic =1, Advanced =2, Expert =3). These numbers allow for comparing different roles and more easily present the differences and commonalities between them. A total of 40 different skills in four different skill categories were identified with the previously mentioned skill levels.

### 3.4 Game Research

After roles and skills were defined, the next step was to create a detailed collection of Serious Games that target the area of IT security. The collection of Adam Shostack [13] described in the related work chapter was primarily used for this purpose. Since this collection offers only rather superficial descriptions, it had to be supplemented with some information. In addition, a few of the games were no longer available, so they had to be removed from the collection. In order to obtain all the necessary information, all the games were inspected individually, and the relevant data was again recorded in the form of a spreadsheet, with the following information: Game name, overall topic, costs, duration, number of players, availability, further link, and a short game description.

### 3.5 Skillset Mapping

For the mapping process, the first step was to shorten the skillset of the industrial roles to those skills that do not have an IT security background. Thus, only eleven of the 40 skills were considered relevant to IT security. Then, an assessment was performed for each of the games: Each game got a rating between the skill level 1 (Basic), 2 (Advanced), 3 (Expert), or - (none) on the previously defined skill, depending on how strongly the game promotes the respective IT security skill. This resulted in an overview of the games which showed which IT security skill they promote at which level (see Table 4).

In the second step, an assessment was made on how well a game fits a role and its skillset. In each case, the distance ( $d$ ) between the skill level of the role and the skill level of the game was considered. The distance was calculated according to the following formula:

$$d = (\textit{Skill level Role} - \textit{Skill level Game}) \quad (1)$$

Points were then awarded for each of the eleven skills according to the following scheme:

■ **Table 2** Scoring in the Mapping Process.

d	-2	-1	0	1	2
points	-50	-25	100	50	25

As can be seen, a maximum distance between  $-2$  and  $2$  could be reached (Skill level Game 1 – Skill level Role 3 or Skill level Game 3 – Skill level Game 1). For a negative distance, either 25 or 50 negative points were assigned; the higher the distance in the negative range, the higher the negative points. This calculation is based on the fact that if a game promotes a higher skill level on a certain skill than is required in a role, it is not suitable for this role. This is especially true if the game targets a topic not required for an expert role in another area, for example. On the other hand, if the skill level of the role is higher than that of the game, positive points are still awarded. Because even if the required skill level of the role is higher, the required skill is still promoted to a certain extent. The highest points were awarded when the distance was zero. In this case, the game maps the respective skill exactly to the role level and fits the role accordingly. All points awarded for each of the eleven skills were added up, so the maximum score was 1100 points ( $11 \times 100$  points). This score ultimately shows how well the game fits the industrial role. Through Excel, an automated evaluation in the form of formulas was possible. The results of the mapping are listed in the next chapter.

## 4 Results

After the steps of Table 1 were explained in the last chapter, the outcome of the steps will be described in more detail in the following.

### 4.1 Ontology

The general knowledge about Serious Games gathered through the literature review and the expert interviews was captured in the form of an ontology. It is provided in the appendix. The upper left part of the ontology refers to Serious Games. Explaining the characteristics contained therein would go beyond the scope of this paper, which is why only the aspects relevant to this paper will be discussed here. It can be seen that an essential part of Serious Games is the game player. He/she has personal characteristics determined by his role and the resulting skills with their skill level. The second part important for this work is the pedagogic learning factor. This has a specific goal and a specific topic. This topic can be IT security. This work aims to match the IT security topics of the Serious Game with the IT security skills of the game player. In the ontology, the matching is represented by the big arrow.

### 4.2 Industrial Role and IT security Skill Collection

The second achievement of the work was to get a collection of industrial roles with their IT security skillset.

■ **Table 3** Role Collection with Skillset Assessment.

		<b>Role:</b>							
		Principal PSSO	PSSO	PSSE for	Architecture	Implementation	Testing	Manufacturing	Service
<b>Skills:</b>									
<i>Product and Solution Security Skills:</i>									
General		3	3	-	-	-	2	-	-
Architecting and Design	-	-		3	2	1	1	1	1
Implementation	-	-		2	3	2	2	1	1
Testing		1	1	2	2	3	2	2	2
Manufacturing	-	-		1	1	1	3	-	-
Service	-	-		1	1	1	-	3	-
Secure Project Integration	-	-		-	-	-	-	-	3
<i>Further Skills</i>									
Product & Solution Security Technologies		1	1	3	2	3	3	2	3
Incident and Vulnerability Handling		3	2	2	2	2	1	2	2
Security Activities and Practices in Lifecycle		3	2	2	2	2	2	1	2
IT Security Technologies		1	1	2	2	2	2	2	2
<b>Legend:</b>									
1 = Basic Knowledge									
2 = Advanced Knowledge									
3 = Expert Knowledge									

As can be seen, eleven IT security skills were defined. Each of the eight different industrial roles was assigned a skill level between 1 (Basic), 2 (Advanced), 3 (Expert), or – (none). This table was essential for the subsequent mapping of the games to the roles.

### 4.3 Game Collection

Another partial result of the work was a collection of 18 board and card games with IT security references. The collection contains information about game-name, overall topic, costs, duration, number of players, availability, further links, and a short game description. In addition, all games in this collection contain a rating between -, 1, 2, and 3 on each of the skills mentioned in Chapter 4.2, depending on how strongly the game promotes the respective skill.

■ **Table 4** Game Collection with Skillset Assessment.

Game	The Agile App Security Game	Backdoors and Breaches	CIA (Collect It All)	Control-Alt-Hack	Crypto Go	Cryptomania	RPG Cyber Threat Defender	Data Heist	Decisions & Disruptions	d0x3d	Elevation of Privilege	Enter The Spadnet	Hacker	Oh Noes!	OWASP Cornucopia	Pivots and Payloads	Protection Poker	Riskio
<b>Skills:</b>																		
<i>Product and Solution Security Skills</i>																		
General	2	2	1	2	3	2	2	1	2	2	1	1	2	2	3	3	2	1
Architecting and Design	1	2	-	2	3	1	2	-	2	3	-	1	3	2	3	3	2	1
Implementation	2	1	-	-	-	-	2	-	1	-	-	2	3	3	2	2	1	-
Testing	1	1	-	1	-	-	1	1	1	1	1	2	2	2	3	2	2	-
Manufacturing	-	-	-	-	-	-	1	-	3	2	-	1	1	1	2	2	2	-
Service	-	-	-	-	-	-	1	-	2	-	-	1	-	1	2	2	2	-
Secure Project Integration	2	1	-	-	-	1	2	-	-	-	1	2	-	2	1	2	2	-
<i>Further Skills</i>																		
Product & Solution Security Technologies	1	2	-	1	3	2	1	-	1	2	1	1	1	2	2	2	2	1
Incident and Vulnerability Handling	2	3	1	-	-	-	1	-	1	2	1	1	-	3	1	1	1	1
Security Activities and Practices in Lifecycle	3	1	1	2	-	1	1	1	1	2	2	-	3	3	2	3	2	1
IT Security Technologies	1	3	-	2	3	1	1	-	1	1	-	1	1	2	1	2	2	1

**Legend:**  
 1 = Basic Knowledge  
 2 = Advanced Knowledge  
 3 = Expert Knowledge

### 4.4 Game/Role Mapping

The main result of the work is a mapping between the previously described Game Collection and the Role Collection. The data mentioned in Tables 3 and 4 were used to evaluate through the procedure mentioned in Chapter 3. As a result, a table was created to record how well a game fits the respective industrial role. The higher the score, the better the game supports the required skills mentioned in the job profiles. As shown in Table 5, scores between 675 and -100 were achieved. The games in bold show which games achieve the highest score in each role and thus best match it. The accumulated value is the added value of the games across the roles. From this, it can be derived how well a game fits the industrial roles in general. The highest value was achieved by Cyber Threat Defender, followed by OWASP Cornucopia and Protection Poker. So these are particularly well suited to training in the industrial sector. The game Crypto Go is the least suitable, with a score of only 50, mainly because it hardly promotes skills in demand, as shown in Table 4. The highest score for a specific role was achieved by the game OWASP Cornucopia in combination with the PSSE for Implementation. Besides this, only the game Protection Poker and Cyber Threat Defender on the roles PSSE for Implementation and PSSE for Manufacturing could collect points of 600 or more. The Agile App Security Game, Decisions and Disruptions, d0x3d, Hacker, and Oh Noes! were also able to collect a score of over 400 in certain roles and thus achieve comparatively high values. The table also shows that the score achieved in a game can vary

### 3:8 Usage of IT-Security Games in the Industry and Its Mapping to Job Profiles

■ **Table 5** Results of Game Role Mapping.

Role:	Game:																			
	The Agile App Security Game	Backdoors and Breaches	CIA (collect it all)	Control-Alt-Hack	Crypto Go	Cryptomancer RPG	Cyber Threat Defender	Data Heist	Decisions & Disruptions	d0x3d	Elevation of Privilege	Enter The Spudnet	Hacker	Oh Noes!	OWASP Cornucopia	Pivots and Payloads	Protection Poker	Riskio		
Principal PSSO	500	200	75	275	0	150	400	150	400	325	300	250	325	175	225	125	50	275		
PSSO	425	100	125	325	0	175	450	175	450	425	375	275	200	-75	300	25	125	325		
<b>PSSE for</b>																				
Architecture	325	200	100	325	175	175	575	100	225	450	225	150	550	325	625	300	450	200		
Implementation	325	275	100	400	-75	250	600	100	300	350	250	200	400	550	675	175	525	250		
Testing	375	100	100	225	25	250	475	75	125	275	200	225	350	200	425	275	325	275		
Manufacturing	375	200	200	350	0	350	475	150	450	375	325	325	250	325	275	625	375			
Service	275	275	150	150	-100	350	275	150	275	375	125	250	100	150	200	150	450	350		
Project Integration	325	200	100	250	25	275	225	100	200	400	250	225	125	125	300	100	525	275		
Accumulated	2925	1550	950	2300	50	1975	3475	1000	2425	2975	2050	1900	2375	1700	3075	1425	3075	2325		

greatly from role to role, for example in the game Oh Noes! where values between -75 and 550 were achieved. This shows that the different skillsets of the role have a substantial impact on the rating. Other games, such as Crypto go or Data Heist, failed to score 200 or more on any reel. This shows that these games are unsuitable for use in the industrial sector. This table shows how well a game fits one of the defined industrial roles, and the Accumulated Value shows how well it is generally applicable in the industrial environment.

## 5 Discussion

The previously described results are discussed and put into context in this chapter. For all of the results, it should be noted that the majority knowledge come from internal company sources are therefore limited.

### 5.1 Discussion on Literature Review

In the course of the review, it became apparent that a large number of literature on the topic of Serious Games is available, including literature on IT security, which demonstrates a high degree of research in this area. Nevertheless, the quality of the games is mostly not on the expected level. This does not mean the creativity or the structure of the games, but rather that the learning objective and the required and promoted skills are not clearly recognizable. Even if new works like from Zhao et al. [16] or Beckers and Pape [1] show that there is a stronger focus on suitability in the industrial environment, the majority of available games neglect this factor. It would be desirable to establish a procedure in which the developers of the games define the goal of the games and the associated skills. These could then be easily understood with the overall topic as a unified game description. Furthermore, it was noticeable that there are hardly any games specifically designed for use in the industrial sector for professionals in the cybersecurity workforce. Although some of the games covered knowledge areas that are important for specific roles, no game specifically designed for one of the roles could be found.



## 5.2 Discussion on Ontology

In the case of ontology, it is important to note that it has been adapted to the purpose of the work. Especially subcategories of aspects of Serious Games that do not contribute to the mapping or are essential to the understanding of Serious Games have been shortened. For example, there are different types of rules, such as Interaction Rules or Scoring Rules, that determine the events within the game. Also, the game objects were described in much more detail in the initial ontology by attributes such as Vital, Position, or Solidity State, but these did not contribute to the mapping or the general basic understanding of Serious Game. However, changes and additions were also made through the expert discussions and our reflections. Two experts mentioned that it would also be important to map the game's internal role, game master or player, in the ontology. The division into game-specific and personal characteristics were based on the experts' considerations. This way, a good differentiation could occur because the game-specific characteristics serve mainly the basic understanding for Serious Games while the personal characteristics were essential for mapping the games. Also, the wording was adapted in some places to provide a better understanding by the players; for example, the Pedagogic Event Indicator became a pedagogic learning factor, or the Game Scenario became a Level. Overall, the ontology could make the purpose of this work more understandable and can be used for research on similar topics, but it could be that for another goal, the ontology contains too little information, or the added information is superfluous. The ontology aims to support research and help understand what the industrial requirements are for games. Thus, it can support the preparation and selection of games.

## 5.3 Discussion on the Mapping Process

The mapping process must also be considered from a certain point of view. Although the games were examined in as much detail as possible, the evaluation of the games in their respective skill levels was still done from a subjective point of view. In addition, there was simply no time to play each game from start to finish, which is why there could be reasons for distortions in the evaluation. In order to ensure the most accurate rating possible, an evaluation of the required skills directly by the developer or publisher would be desirable. For this purpose, a framework could be developed. For example, the developer or publisher of the game could choose from a pool of skills how strongly they are promoted. This could easily create comparability of the games, and mapping to industrial roles would be much easier, and it would generally contribute to standardization in the field of Serious Games.

Nevertheless, the mapping process created here can also be used for roles and games not covered in this paper. When adding new games, you only have to evaluate how strongly the game promotes the eleven defined skills, according to the principle outlined in the chapter methodology. The same applies to adding new roles, as long as they contain the same IT security skills.

A role with new skills would also be conceivable. But then the new skills would have to be evaluated for the PSSO and PSSE roles as well, or they would have to be deleted, and only the new roles are considered. Practically speaking, one could define what skills children of a certain grade level need to have and thus select the most appropriate game to complement traditional teaching methods.

A finer detailing of the skill levels is also discussable. In this work, a distinction is only made between the Basic, Advanced, Expert, and none levels. This can be extended as desired. Then a new evaluation of all games and roles must take place; thereby, a more exact mapping evaluation could be done. However, the amount of work must be considered because this should be in proportion to the benefits.

## 6 Conclusion

In summary, through research, feedback from experts, and an evaluation system, it was possible to determine which Serious Games are relevant for IT security roles in the industry. In this paper, two different roles for general Product Security (PSSO) and six different types of Expert roles (PSSE) in the industry were considered relevant. A collection of board and card games by Adam Shostack was used to conduct a mapping for these roles. Some useful information was added to this collection, and a few outdated or no longer available games were removed from the list. The mapping result was that the games were given a score that shows how well a game fits an IT security role. The mapping assessment considered how much a game promoted the required skills of one of the PSSO or Expert roles. Eleven IT security skills were taken into account. Thereby comparability could be established based on how well a game represents the required IT security skills of the respective role. The basis for this scoring was that each game received a rating between none, Basic, Advanced, and Expert, which showed how a particular skill was promoted in one of the games. The roles also received a rating, as described, considering what level of skill is required in that role. A score could then be derived based on a rating system, which describes how well a game fits a role.

During the process, an ontology was developed, which only contains the essential aspects of Serious Games and mainly aims at developing the mapping process. The level of detail of the general characteristics of Serious Games is not very high, but the ontology shows which aspects can be used to map the games to the personal characteristics determined by the industrial role and the resulting skills. This knowledge can be used to apply the mapping process to other circumstances, such as companies, schools, or universities with other roles with other skillsets or to the general audience. Also, the created collection of games with skills ratings can be used for other mapping processes, either by adding new games to the games collection with a skills rating or by adding new roles with a rating of the eleven skills.

We will transfer the obtained results into a database for easy querying for future work. The results can also be presented in a graphical user interface. It would be conceivable to expand the interface with additional information about Serious Games so that a platform is established that serves as a central point of contact for Serious Games in the context of IT security. Furthermore, a recommendation process could be created here, which concludes the interests and skills of the user based on specific questions. Based on the answers, extra points can be given to the games, and the ones with the highest score will be recommended. In conclusion a process could be developed to run a mapping between industrial roles and IT security Serious Games. As a result, different games are now available with an evaluation that describes how much the required skills of the industrial roles are mapped. The result of the work also shows that there is an unused potential for Serious Games in IT security. First, the games' content and goals can be better adapted to the industrial roles and skills, and second, the content and the goal could be communicated more transparently, for example, by a standardized description of which skills the respective game promotes.

---

## References

- 1 Kristian Beckers and Sebastian Pape. A Serious Game for Eliciting Social Engineering Security Requirements. In *2016 IEEE 24th International Requirements Engineering Conference (RE)*, pages 16–25, 2016. doi:10.1109/RE.2016.39.
- 2 Bundesamt für Sicherheit in der Informationstechnik. *Die Lage der IT-Sicherheit in Deutschland 2021*. BSI, 2021.

- 3 Polona Caserman, Katrin Hoffmann, Philipp Müller, Marcel Schaub, Katharina Straßburg, Josef Wiemeyer, Regina Bruder, and Stefan Göbel. Quality criteria for serious games: Serious part, game part, and balance. *JMIR Serious Games*, 8(3):e19037, July 2020. doi:10.2196/19037.
- 4 Ralf Dörner, Stefan Göbel, Wolfgang Effelsberg, and Josef Wiemeyer. *Serious Games: Foundations, Concepts and Practice*. Springer International Publishing, 1. Ed, Switzerland, 2016. doi:10.1007/978-3-319-40612-1.
- 5 Tiago Espinha Gasiba, Kristian Beckers, Santiago Suppan, and Filip Rezabek. On the Requirements for Serious Games Geared Towards Software Developers in the Industry. In *2019 IEEE 27th International Requirements Engineering Conference (RE)*, pages 286–296, 2019. doi:10.1109/RE.2019.00038.
- 6 Tiago Gasiba, Ulrike Lechner, and Maria Pinto-Albuquerque. CyberSecurity Challenges for Software Developer Awareness Training in Industrial Environments. In *International Conference on Wirtschaftsinformatik*, pages 370–387. Springer, 2021.
- 7 Maurice Hendrix, Ali Al-Sherbaz, and Victoria Bloom. Game Based Cyber Security Training: are Serious Games suitable for cyber security training? *International Journal of Serious Games*, 3, March 2016. doi:10.17083/ijsg.v3i1.107.
- 8 Hill Jr, Mesafint Fanuel, Xiaohong Yuan, Jinghua Zhang, and Sajad Sajad. A Survey of Serious Games for Cybersecurity Education and Training. *KSU Conference on Cybersecurity Education, Research and Practice*, October 2020.
- 9 Menelaos Katsantonis, Isabella Kotini, Panayotis Fouliras, and Ioannis Mavridis. Conceptual Framework for Developing Cyber Security Serious Games. In *2019 IEEE Global Engineering Education Conference (EDUCON)*, pages 872–881, April 2019. doi:10.1109/EDUCON.2019.8725061.
- 10 Lin Liu, Affan Yasin Chouhan, Tong Li, Rubia Fatima, and Jianmin Wang. Improving Software Security Awareness Using A Serious Game. *IET Software*, 13, July 2018. doi:10.1049/iet-sen.2018.5095.
- 11 Natalia. Noy and Deborah McGuinness. Ontology Development 101: A Guide to Creating Your First Ontology. *Knowledge Systems Laboratory*, 32, January 2001.
- 12 José Carlos Paiva, José Paulo Leal, and Álvaro Figueira. Automated Assessment in Computer Science Education: A State-of-the-Art Review. *ACM Trans. Comput. Educ.*, January 2022. Just Accepted. doi:10.1145/3513140.
- 13 Adam Shostack. Threat Modeling Expertise, Training, Coaching, July 2022. URL: <https://shostack.org/>.
- 14 Stephen Tang and Martin Hanneghan. Game Content Model: An Ontology for Documenting Serious Game Design. In *2011 Developments in E-systems Engineering*, pages 431–436, 2011. doi:10.1109/DeSE.2011.68.
- 15 Valdemar Švábenský, Jan Vykopal, Milan Cermak, and Martin Laštovička. Enhancing Cybersecurity Skills by Creating Serious Games. In *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education, ITiCSE 2018*, pages 194–199, New York, NY, USA, 2018. Association for Computing Machinery. doi:10.1145/3197091.3197123.
- 16 Tiange Zhao, Tiago Espinha Gasiba, Ulrike Lechner, and Maria Pinto-Albuquerque. Exploring a Board Game to Improve Cloud Security Training in Industry (Short Paper). In *ICPEC*, 2021.

**A Appendix**

**Table 6** Ontology of Serious Games regarding Mapping to Industrial Roles.

