information

Article

Raising Awareness about Cloud Security in Industry through a Board Game

Tiange Zhao [1,*], Tiago Gasiba [1], Ulrike Lechner [2] and Maria Pinto-Albuquerque [3]

[1] Siemens AG, 81739 Munich, Germany; tiago.gasiba@siemens.com
[2] Computer Science, Universität der Bundeswehr München, 85579 Munich, Germany; ulrike.lechner@unibw.de
[3] Instituto Universitário de Lisboa (ISCTE-IUL), ISTAR, 1649-026 Lisbon, Portugal; maria.albuquerque@iscte-iul.pt
* Correspondence: tiange.zhao@siemens.com

Abstract: Today, many products and solutions are provided on the cloud; however, the amount and financial losses due to cloud security incidents illustrate the critical need to do more to protect cloud assets adequately. A gap lies in transferring what cloud and security standards recommend and require to industry practitioners working in the front line. It is of paramount importance to raise awareness about cloud security of these industrial practitioners. Under the guidance of design science paradigm, we introduce a serious game to help participants understand the inherent risks, understand the different roles, and encourage proactive defensive thinking in defending cloud assets. In our game, we designed and implemented an automated evaluator as a novel element. We invite the players to build defense plans and attack plans for which the evaluator calculates success likelihoods. The primary target group is industry practitioners, whereas people with limited background knowledge about cloud security can also participate in and benefit from the game. We design the game and organize several trial runs in an industrial setting. Observations of the trial runs and collected feedback indicate that the game ideas and logic are useful and provide help in raising awareness of cloud security in industry. Our preliminary results share insight into the design of the serious game and are discussed in this paper.

Keywords: cloud security; cloud control matrix; shared-responsibility model; industry; awareness; training; serious game

Citation: Zhao, T.; Gasiba, T.; Lechner, U.; Pinto-Albuquerque, M Raising Awareness about Cloud Security in Industry through a Board Game. *Information* **2021**, *12*, 482. https://doi.org/10.3390/info12110482

Academic Editors: Ricardo Queirós, Mário Pinto, Carlos Filipe Portela, Alberto Simões and Pedro Rangel Henriques

Received: 24 October 2021
Accepted: 12 November 2021
Published: 19 November 2021

1. Introduction

Cloud computing provides a relevant and essential architecture to deploy IT infrastructure and services. The promised value of cloud service providers (CSP) is to deliver high levels of service and security and save business costs. Significant players have dedicated themselves to providing cloud-based solutions to the customer. Customers rely on CSPs with more and more critical applications in the cloud. In particular, this cloud deployment is gaining traction with critical infrastructures due to the high resilience of the deployed environments. Companies in the industry are providing cloud-based products and solutions, such as MindSphere [1] and Teamplay [2], to the customer.

Due to the nature of cloud-based systems, they are facing various security threats listed in [3]. These threats include the nefarious use of cloud services and the lack of cloud security architecture and strategy. Poor management of cloud cybersecurity can lead to severe consequences. In 2017 [4], the United States Department of Defense disclosed login credentials to their cloud environment, which led to the disclosure of secret government intelligence data hosted in their cloud-deployed infrastructure. Also, misconfigurations of S3 buckets in Amazons' cloud environment have allowed several high-profile information to be leaked, resulting in severe monetary consequences due to the data breaches [5]. In [6], Scheffler provides details on the Man-in-the-cloud attack. In this type of attack, the goal of the malicious party is to gain control of the victims' cloud account by capturing credentials

such as those present in OAuth tokens. One of the ways that the author proposes to address this problem is through regular security training to raise awareness on cloud cybersecurity.

The origin of cloud vulnerabilities is often two-fold. On the one hand, there are technical vulnerabilities, e.g., the poor configuration of cloud environments (either manual or automated). On the other hand, there is a lack of cloud security awareness among managers, cloud asset operators, and customers of cloud services. In this work, we address cloud security awareness issues considering particular roles and responsibilities in cloud service provisioning.

There are numerous standards that regulate cloud security, such as [7–9] and security guidelines [10,11] that describe the roles and responsibilities in cloud computing. Security training is the primary method to communicate these standards and guidelines to developers and managers. Enterprises are obligated to help their developers and managers to understand the importance of cloud security and, more precisely, how cloud security standards relate to daily work. Otherwise, the continuity of business is put in danger.

To address this challenge, we propose a serious game in this work—raising awareness on roles and responsibilities related to cloud security. In this research, we are interested in the design of a serious game that facilitates the training of developers and managers about cloud security, especially the roles and responsibilities and the collaboration between cloud service providers and customers. This work presents a tabletop game prototype designed to introduce fundamental concepts in cloud security and the first results on the validation of this game.

The research contribution of this work is to propose a serious game, in the form of a board game, to increase the game participants' awareness of cloud security in an industrial setting. We also provide the results of three trial runs in the industry and discuss our preliminary results.

This article is organized as follows. Section 2 acquaints the related serious game designs, and especially games that target information security. Section 3 reviews the method we employ in our research. Section 4 illustrates the design of our game; and explains details about the evaluator as a novel element in the prototype. Section 5 presents the feedback we collected from our trial runs and discusses our thinking upon it. Section 6 summarizes this work and gives an outlook into possible future research directions.

2. Related Work

There are many standards for information security in the industry, and cloud security is a critical subset of cyber-security. Best known are ISO/IEC27001 [12] and MITRE ATT&CK [13]. The standard ISO/IEC27001 [12] describes how to provide their customers with certified products and services. The standard specify how cloud assets should be protected, e.g., by monitoring and data encryption, and mandate secure deployment and maintenance. MITRE ATT&CK [13] categorizes attack action and defense mechanisms in a cloud matrix based on industry standards and real-world observationSecure mechanisms are highly required in the cloud. Muñoz et al. provides in [14] an overview of the importance of the monitoring of security properties in cloud computing scenarios. Without necessary monitoring, cloud asset are easy victims of hackers. Popović et al. argued in [15] it is very important to take security and privacy into account when designing and using cloud services. That requires people working at the front line realize the importance of cloud security and comply with the standard in their daily work. Our work helps to transfer the requirement of industry standards to industry practitioners by assisting the understanding of cloud security concepts in the format of a serious game.

Dörner et al. establish a baseline for developing serious games [16]. In their seminal work, they define serious games as games that are designed with a goal other than pure entertainment. One such type of serious game is a game that has the goal of raising the cybersecurity awareness of the game participants. We use this work in the design and in the instantiation of our game. Previous work has shown that serious games are an appropriate method to address industry's cybersecurity training requirements. In fact, serious games

are discussed in the IT Baseline Protection (BSI Grundschutzkatalog) of the German Federal Office for Information Security [17] as a possible means to raise cybersecurity awareness. However, Alotaibi et al. in [18] have shown that, while many studies claim the effectiveness of serious games in raising cybersecurity awareness, the game design should be properly addressed in addition to the participants' needs.

The review of various serious games in cybersecurity by Shostack [19] demonstrates the number and amount of serious games in the domain of cybersecurity. However, none of the listed games specifically addresses the topic of cloud security. In particular, Shostack presented in [20] a card game *Elevation of Privilege* that draws developers into threat modeling, whose importance used to be underestimated. It shares similarities with this work in that it aims to utilize a tabletop board game to teach software developers the basic terms of threat modeling.

By designing a cyber-physical systems game, Frey et al. [21] studied the information security field's decision-making process. This is different from *Elevation of Privilege*, because the purpose of the game is to understand the decision-making process, not to train the participants on cyber-physical system security.

Romand-Latapie pointed out in [22] that a role-playing game similar to *Dungeons and Dragons* was helpful in training neophyte audience to the basic principles of computer security. They included cloud computing as a single element in the game design. Beckers et al. designed a serious game to elicit social engineering threats, and subsequent security requirements [23]. It is tested to be effective and efficient in teaching employees on different facets of social engineering attacks.

In [24–27], Gasiba et al. present and discuss a serious game, inspired on the capture-the-flag genre, successfully developed to raise awareness of secure coding of software developers in the industry. In particular, Gasiba el al. discuss the necessary requirements to design a serious game to address software developers in an industrial environment. Their work hints at possible differences in the design of serious games in general and serious games that are developed and geared towards usage in the industry. However, their game, which was evaluated and validated with more than 200 industry participants, focuses on secure software development rather than addressing secure deployment of cloud environments.

Nevertheless, this presented previous work served as a source of inspiration while designing our game to address cloud computing's specific security topics, such as the shared responsibility model, cloud-specific threats, and mitigation.

This article extends our previous work [9] by providing more trial runs results and deeper discussions on these. We also discuss possible variations of our gaming mode and briefly introduce a digital platform to design the game.

3. Method

The design science paradigm guides our research approach according to Hevner et al. [28]. The method literature on design science defines the design of a useful artifact as a creative search process for a useful solution. Gleasure has pointed when the prescriptive aspect of a research problem is less mature than its descriptive or normative dimensions, the information system (IS) research problem is 'wicked' [29]. The above-mentioned theory provides valuable theoretical support to our work since design science research can handle the changing and varying requirements we encounter in practice and industry.

This paper presents a beginning step in the creative design process towards a serious game, aiming to raise awareness of cloud security among industrial cloud services users. In the design process, we conducted multiple brainstorming sessions, in which we stipulated the topic of cloud security. We gathered the first ideas of a game and developed the design principles of a game (cf. Section 4). The topic was selected from professional experiences and game design and security expertise from this paper's various authors because of its relevance in industrial settings.

We designed and implemented the game prototype in early 2021. The first game run was organized in February 2021 with three participants and two observers with research interest and knowledge in security-related cloud service provision topics. Later trial runs had four participants. All the participants agreed to take part in our study, and we collected the data anonymously. The data was collected using the recording material on the game session and participatory observation and then analyzed in a discussion. This paper represents the state of the result and the reflection on the next steps in the design process.

4. Game Design

We introduce the initial design elements and the game prototype in this section. This section starts with the initial design elements, and then the game process is introduced. The is a novel element for the game. Design details of the are also included in this section. In the last part of this section, various gaming modes and the implementation of the digital platform are explained.

4.1. Initial Design Elements

In the first brainstorming sessions, we identified the topic "Cloud Security" and the game framework: it should be a board game that can be played face-to-face or online in a virtual session to cope with the restrictions imposed by the COVID-19 situation. It was also determined that the insider perspective of non-compliance with security policies should be taken into consideration.

By its nature, there are several fundamental facts about cloud security that could be transformed into a board game: (1) Cloud security can be described as a constant fight between attackers and defenders. (2) Both defenders and attackers are facing resource constraints. (3) Defenders might play different roles and thus take different responsibilities determined by their role in cloud security. (4) Attackers take attack actions to compromise cloud assets. Those elements above can be built into a board game prototype geared to help trainees better understand the basic concepts of cloud security.

In the design phase, the following core design elements for the serious game are identified. The game prototype aims to address these design elements:

- Feature 1: Cloud Security Kill Chain.
- Feature 2: 100 percent security does not exist.
- Feature 3: Defense-in-depth helps.

Our previous work [9] includes a description in detail for each of the features.

4.2. Game Process

The classic game prototype needs a Game Master (GM) to organize and host the game. Before the game begins, GM explains the game flow and rules to the participants and handles the questions raised by the participants during the game.

During the game, the defender team should develop a defense plan and the attacker team an attack plan. Each team uses a game board to place different sets of cards to model attack and defense plans. Attackers and defenders can only place a limited number of cards. This constraint reflects the reality that neither attacker nor defender has unlimited resources, and both of them need to prioritize accordingly. This drafting of attack and defense plans is done in teamwork. Teams use breakout rooms virtually to discuss and develop plans in an online game. If the game is played face-to-face, different teams should sit apart and work on their defense or attack plan separately.

In total, there are 40 cards, of which 24 cards are available to the defender team and 16 to the attacker team, as Table 1 shows. On each card for defender team states one countermeasure to secure cloud assets, for example, "Information Encryption" or "Network Segmentation" (see Figure 1). On each card for the attacker team states one attack action to cloud assets, for example, "Monitoring Escaping" or "Network Service Discovery" (see Figure 2).

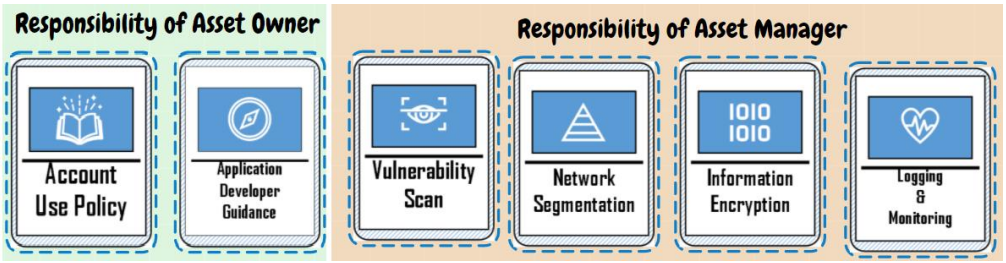

Figure 1. Trial run: a screenshot of the game board on the defender side.

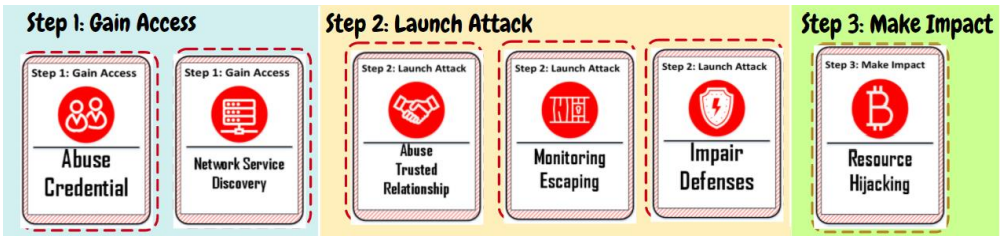

Figure 2. Trial run: a screenshot of the game board on the attacker side.

Table 1. No. of cards for defender team and attacker team.

Defender Team	Total No. of defense cards	24
	No. of defense cards belong to Asset Owner	8
	No. of defense cards to Asset Owner on Defense Plan	2
	No. of defense cards belong to Asset Manager	18
	No. of defense cards to Asset Manager on Defense Plan	4
Attacker Team	Total No. of attack cards	16
	No. of attack cards to chose from for Initial Access	5
	No. of attack cards for Initial Access on Attack Plan	2
	No. of attack cards to chose from for Launch Attack	8
	No. of attack cards for Launch Attack on Attack Plan	3
	No. of attack cards to chose from for Make Impact	3
	No. of attack cards for Make Impact	1

Figure 3 presents the phases of the game as a flow chart.

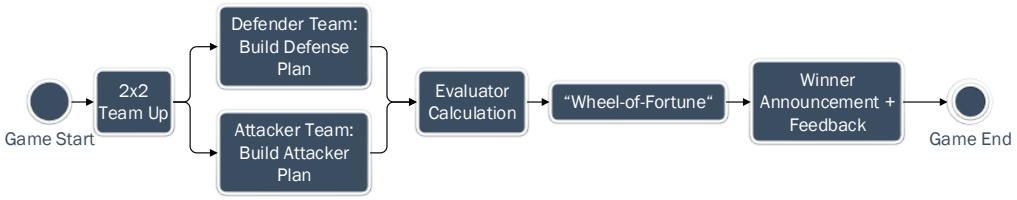

Figure 3. Game Process in Flowchart.

When the game starts, the GM randomly assigns players to the two teams: *defender* and *attacker*. During the game, the task of the *defender* team is to build a defense plan from scratch by selecting defense cards and assigning them to one of the roles: cloud asset owner and cloud asset manager. They should discuss and decide together with their teammates to assign two cards to Asset Owner and four cards to Asset Manager. The defender team needs to determine which ones of the 24 cards are the responsibility of the Cloud Asset Owner and which ones should be taken care of by the Cloud Asset Manager based on their

understanding and knowledge. If a card is assigned to the wrong role, it will be sorted out from the defense plan and not contribute to a successful defense. Table 1 illustrates the number of cards of each category. Two cards could be assigned either to Asset Owner or Asset Manager. That is the reason why the sum of the second and fourth row of Table 1 is two more than the total number of defense cards. On the other hand, the *attacker* should build a three-step attack plan: Gain Access, Launch Attack and Make Impact. In total, 16 attack cards categorized into the three steps are made available to them, and they should discuss and decide with their teammates to assign 2, 3, and 1 card(s) to each step. Both teams have 20 minutes to build their defense plan or attack plan.

We derived the attack cards, defense cards, and the mapping relation between them from MITRE ATT&CK [13] primarily and the CSA cloud control matrix [10] for additional information. The cloud matrix demonstrates the typical attack and defense actions in a cloud environment based on real-world incidents. In case that the players are not so familiar with cloud security defenses and attacks, cheat sheets with the key information are made available to them for their assistance throughout the game process.

Both the defender team and attacker team submit their defense plan and attack plan to an evaluator. The evaluator runs an algorithm to simulate the attack and defense steps and compute the probability of the defense plan withstanding the attack plan.

The GM shows the results of the evaluator to participants and explains to them when necessary. For instance, how an attack action is blocked by a single or multiple defense action card(s) and which attack action is left undefended if there is any. The evaluator finally outputs a percentage number of the probability for the Defender Team to survive the attack in the end.

In the next step, we designed a "Wheel-of-Fortune". This step involves a virtual spinning wheel with different slices marked as "Attacker wins" or "Defender wins." The size of each area is determined by the probability calculated by the evaluator in the previous step. For instance, if the evaluator calculates that the defense plan has 80% of chance withstanding the attack plan, the marked "Defender wins" area will take up 80% of the wheel. The areas are distributed evenly on the surface of the wheel. At the end of the game, GM will spin the "Wheel-of-Fortune", and the winner will be announced.

According to the best of our knowledge, there is no similar design of such an evaluator that is tailored to the requirements of a serious game for cloud security. The key parameter of the evaluator will be introduced in the following sub-section. The evaluator algorithm itself is only introduced briefly in this paper.

4.3. Evaluator

An evaluator suns an algorithm to analyze the defense plan against the attack plan and calculates the probability of the input attack plan to tear down the defense plan. Along with the attack steps, it shows the reasoning also step-by-step. The ultimate output of the evaluator is the calculated probability in percentage number. The evaluator has some adjustable parameters, such as the number of hints and the single success rate.

- Number of Hints

The hint is only available for the defender team to help them assign one card to the correct role in advance of the next game step. When the team assigns a valid defense card to the correct role, as the hint suggests, this guarantees that the card will enter the and contribute to the overall success of the defense plan. Based on the GM's observation of the game and the players, they can decide whether to give the defender team a maximum of two hints. We don't provide any hint for the attacker team to improve their attack plan.

- Single Success Rate

The single success rate (SSR) describes the likelihood of a single defense card successfully blocking a mapped attack card. It is the same for all defense-attack mapping pairs. It reflects the important fact that there is no 100% security (Feature 2 in Section 4). For instance, if we consider Multi-factor Authentication (MFA) as effective mitigation

against account manipulation and the SSR is set to 80%, it means MFA has 80% chance of successfully stopping an account manipulation attack. MFA reduces the chance of account manipulation, but it does not remove the danger completely-the attacker could intercept the authentication traffic or steal the additional credentials too. In general, as the SSR is set higher, the Defender Team would be more likely to win if they select the effective defense action card. In the trial run, we set the SSR to 80%.

- Evaluator Algorithm

The evaluator algorithm is described briefly here. The evaluator takes the defense plan and attack plan as input. It first sorts out all the defense action cards in the defense plan that are assigned to an incorrect role then discards the card. Secondly, it analyzes the attack plan step by step. For each attack action card, it counts the number of mapped defense action cards in the defense plan. The higher the number, the more likely this attack action card will be blocked. The attack action cards in the same step are considered in parallel. It means as long as one attack action in an attack step is successful, this attack step is successful. The three attack steps are considered sequentially, which means the attack plan is successful if and only if all the attack steps are successful.

After design and implementation, the evaluator algorithm was presented to an expert from industry and academia. Two rounds of one-hour feedback and improvement sessions took place in May and June of 2021. The feedback provided by the expert was taken into consideration when designing the evaluator algorithm.

4.4. Gaming Mode and Platform

In the beginning, the game is designed to be played by two teams and optimally more than one player in each team, which is a multiple-player mode. With the help of an evaluator, it is possible to replace the attacking team with a non-player character (NPC). In that case, the game could also be played in a single-player mode, independent of the availability of other players, allowing the game organization more flexibility. In the single-player mode, the attacker's action is simulated by a computer program based on an analysis of the defense attack matrix and the statistic in the previous trial runs.

A digital platform for the game is developed as shown in Figure 4. It consists of a front end and a back end. The front-end application is built on Konva library [30]. It provides a game board for both of the teams with cards that can be dragged around. The page is implemented with a magnetic effect so that the cards can fit into the correct area. The attacker team can only access the Attack Page, and the defender team can only access the Defend Page. Both the Attack Page and the Defend page send a request to the evaluator in the back-end. Both submissions are recorded in the logger anonymously. When time is up, the game master (GM) will share the dashboard, where the output of the evaluator is displayed, as well as a visualization of the chosen defense and attack actions.

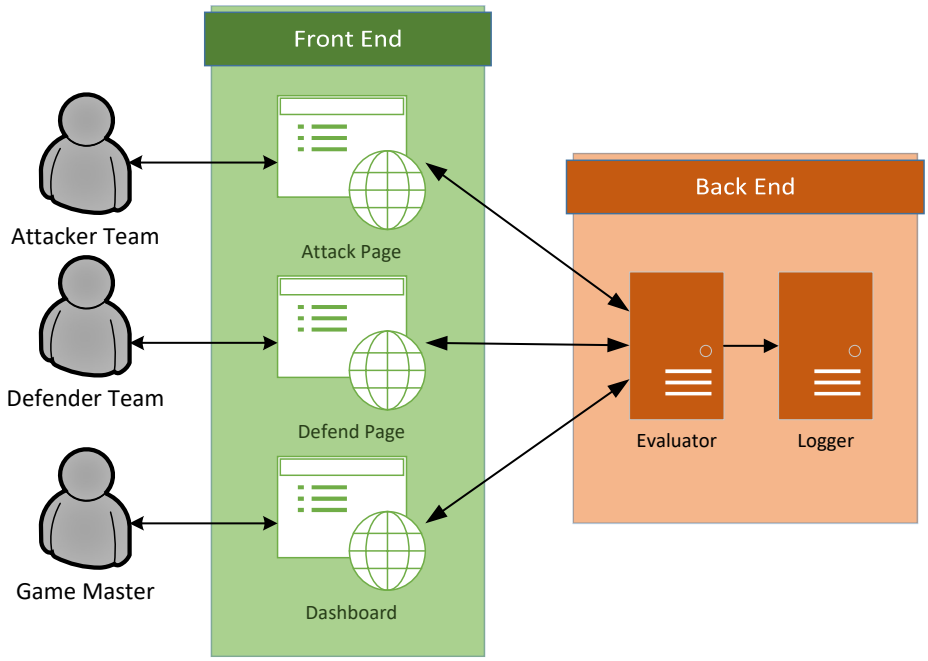

Figure 4. Digital Platform.

5. Evaluation of the Game

For evaluation of the game, we have organized three trial runs in an industry setting. In this section, the first trial run (TR 1) will be described in detail as an example, and we will compare the second and third trial run (TR 2 and 3). The result of all the trial runs will be presented and discussed.

5.1. Trial Runs in Industry

The first three trial runs in industry are presented in this section. Details are summarized in Table 2. Each trial run has three to four players participating. They come from different backgrounds; some were security experts in the industry, some were students from the university. In TR 1, we have also invited two observers to provide objective opinions and give feedback. The players were distributed into two teams: defender and attacker. All the trial runs were hosted online and took 30 minutes for each game. After the game, open discussions were held for 15 minutes with the participants to gather feedback from their experience and the game's design. The first trial run also included two observers. These two observers are cybersecurity experts and also in the development of serious games. They observed the game without interfering. One of them joined the defender breakout room; the other joined the attacker breakout room. They did not participate directly in the game play but were included to gather additional feedback on the game design.

Table 2. Details of each trial runs: TR 1, 2 and 3. ind. = Industry; uni. = University

	TR 1	TR 2	TR 3
Participants in total	3	4	4
Participants (ind.)	2	2	2
Participants (uni.)	1	2	2
Observer	2	0	0
Players in defender team	2 (ind. + uni.)	2 (ind. + ind.)	2 (ind. + ind.)
Players in attacker team	1 (ind.)	2 (uni. + uni.)	2 (uni. + uni.)
Date	4 February 2021	23 April 2021	23 April 2021
Duration	30 mins	30 mins	30 mins
Online/Onsite	Online	Online	Online

As an example, we present the details of TR 1. There were three players who participated in the game. One of them is a university student with an elementary level of cybersecurity knowledge required by the game. Two of them are security experts with years of experience in the field.

Participants were separated into two teams. Each team built their defense or attack plan on an online whiteboard application prepared with the cards and game board in advance. Figures 1 and 2 are the screenshots of the final defense and attacker plan in our game environment.

The defender team assigned the card "Account Use Policy" to the asset owner. So meaningful account use policy is established and enforced. They also assigned the card "Application Developer Guidance" to the asset owner to reduce the number of security weaknesses in the early development phase. The defenders agreed to select "Vulnerability Scan" to track potentially vulnerable software; use "Network Segmentation" to separate critical systems in subnets and avoid lateral movement; apply "Information Encryption" to put protection on confidential data and enable "Logging & Monitoring" to keep an eye on the cloud system performance to detect anomaly behavior. These cards are assigned to the Asset Manager. The defender team made no mistake on the assignment to the correct roles, so all the defense cards chosen could contribute to the defense's success. On the attacker side, several decisions were made: in the first step, Gain Access, the attacker team chose the card "Abuse Credential" to extract credentials and opened up their attack plan. The selected attack action card "Network Service Discovery" helped list all those vulnerable services that were not yet shut down on remote hosts. In the second step, Launch Attack, they played "Abuse Trusted Relationship" to find their way of compromising through third-party provider; "Monitoring Escaping" techniques were selected to bypass detection, and "Impair Defenses" helped them to maliciously manipulate components of a victim environment. In the last step, Make Impact, the attacker team did a "Resource Hijacking", which meant they would like to take advantage of the resources of co-opted systems in the cloud and earn virtual currency by means such as bitcoin mining.

At the end of the game, both attack and defense plans were transmitted to the evaluator. The evaluator simulated the defenses and attacks step-by-step and displayed the intermediate result during the calculation. Finally, the overall probability of the defense plan against the attack plan was computed 96%. This meant the defender had 96% of the chance to stop the attacker. This probability was then configured to the Wheel-of-Fortune. To everyone's surprise, even though the attacker team had only a 4% chance of winning the game, the Wheel-of-Fortune finally stopped at the slice of "Attacker wins". However, it reflects Feature 2 in Section 4 in a way that no defense is 100% secure.

5.2. Trial-Runs Results and Feedback

The chosen cards in each trial run are summarized in Table 3. Surprisingly, in all the trial runs, the attacker team won the game.

Table 3. Chosen cards in previous trail runs.

			TR 1	TR 2	TR 3
Attack Plan	Step 1	Exploit Public-Facing Application		x	
		Abuse Credential	x	x	x
		Cloud Infrastructure Discovery			x
		Network Service Discovery	x		
	Step 2	Abuse Trusted Relationship	x	x	x
		Impair Defenses	x		x
		Infrastructure Manipulation		x	
		Monitoring Escaping	x	x	x
	Step 3	Defacement		x	
		Resource Hijacking	x		x
Defense Plan	Asset Owner	Application Developer Guidance	x	x	x
		Audit		x	x
		Account Use Policy	x	x	
	Asset Manager	Network Segmentation	x	x	x
		Application Isolation and Sandboxing			x
		Vulnerability Scan	x		x
		Logging & Monitoring	x		
		MFA		x	x
		IDS		x	
		Information Encryption	x		

As soon as the trial run games were over, we gathered the participates and observers to share their opinions about the game in an open discussion. In general, the majority of the players agreed that the game was helpful to understanding cloud security concepts, and it was engaging playing the game. There was also constructive feedback on improvement. We reveal some of the reviews we collected below.

The student who participated in the TR 1 mentioned, "*I think it was pretty cool. It has some cybersecurity notions that I still don't really know, so I tried to see both the cheat sheet and the task. Team environment helped*". From this piece of review, we understand that people with limited background knowledge are able to enjoy the game with the assistance of a prepared cheat sheet and benefit from teaming up with experienced ones.

One of the security experts mentioned, "*The number of rectangles you can assign to the roles represents the resource-you cannot do everything*". In the designing phase of the game prototype, we learned that in the real world, there is never enough resource to implement every defense mechanism. The defenders should make decisions on the priority and consider the countermeasures individually. That implies the game design manages to reflect real-world defensive thinking to a certain extent.

Some participants in TR 2 noted, "*We can improve our strategy by repeatedly playing the game*". By repeating and debriefing the game, the participants can familiarize themselves with the concept of cloud security and therefore improve their strategy.

There was also feedback such as "*Why the attack 'Impair Defenses' is covered by the defense 'Logging & Monitoring' is not clear to me...*". As we described in Section 4, the evaluator checks the card mapping of attack and defense pairs. For such feedback, we learned that there is a lack of rationale for the participants, and further refinement needs to be done to the evaluator's algorithm.

5.3. Discussion on the Game Results

Table 3 provides details of which cards are chosen in TR 1, 2, and 3 by the corresponding attacker teams and the defender teams.

In these trial runs that we have conducted, some interesting patterns can be observed from the gathered results. Some cards are frequently chosen, such as Abuse Credential and Abuse Trusted Relationship for the attacker team.

In step 1 of the attack plan, abuse credentials almost always provide an attack surface for further attack actions. This might be the reason why the card "Abuse Credentials" was always chosen. The reason for the teams choosing those cards might also be related to previous cybersecurity awareness training of the participants.

Abuse trusted relationship was also chosen in all trial runs for step 2. This is probably since, in cloud security, we rely more on the product and services by a trusted third party, and it worries us if the trusted relationship gets abused. Playing this card can also indicate that the participants consider the insider threat important for cloud systems. A surprising result was that all the attacker teams had selected the card Monitoring Escaping in their second step. This could be related to the participants' thinking that cloud-deployed systems are more heavily monitored than non-cloud deployed systems. It is important first to disable the monitoring mechanism to avoid being caught. Further investigation is needed to understand this point.

Also, on the third step of the attacker plan, Resource Hijacking was selected two times compared to Defacement, only one time. We think this might be related to the fact that cloud resources are a "popular" victim of crypto-mining and distributed denial of service. However, further investigation is needed to understand the attackers' motivation.

For the defender team, Application Developer Guidance and Network Segmentation were chosen all the time. This indicates that the players believed it is essential to teach application developers to write code securely employing developer guidelines. According to our experience in the industry, this result was expected, as the participants also have an industry background. Furthermore, the importance of network segmentation was also prominent in our results. This result is in line with previous internal training in the company where the game took place, which raises awareness about network segmentation to enhance cybersecurity.

An unexpected result was that only the defender team selected the Information Encryption card in the first trial run. Previous incidents in the past have shown that information placed in cloud environments can be leaked. Encrypting the information can drastically reduce the usability of the data by malicious parties. According to our experience, data in the cloud should be stored encrypted. Therefore, the results that we have collected are surprising since only the first team chose to play this card.

Finally, we would like to mention that our preliminary results indicate that attackers choose the following attack path: abuse credentials, abuse trusted relationship, and escape monitoring, while defenders have consistently chosen the following defense plan: application developer guidance and network segmentation.

5.4. Conclusion on the Game Logic and Material

The purpose of organizing the trial run is to test the game logic, collect players' direct feedback, and gather new ideas for the next design iteration. The participants agreed that the game was engaging and could reflect the difficulties in implementing helpful defenses for cloud assets in real life from the feedback we collected. On the other hand, we would like to integrate constructive feedback as a part of future work. From the aspect of the designer, the trial runs showed the game logic is reasonable. Additionally, the prepared material, including the game board, cards, and cheat sheets, have fulfilled their design purposes and provided help to the players during the game. There are positive indicators that the game is adequate for the industry.

5.5. Threats to Validity

Our results give us a positive indicator of the validity and adequacy of the game for the industry. However, further work needs to be performed to collect more players' additional results and solidify our conclusions. Nevertheless, our results align with previous research

done in the field, particularly in the industry, and the number of participants is in line with previous empirical work. Limitations on the number of players and variations in the participants' background and experience are inherent to this industrial setting, preliminary study, and (wicked) problem.

Our results and conclusions are obtained based on participants from industry and no other user groups have been included up to now. Nevertheless, since the goal of the design of our game is to address industry practitioners, we do not see this as an issue.

6. Conclusions and Future Work

More and more products and solutions in the industry are being developed and deployed in cloud environments in recent years. Cloud systems provide us with both opportunities and challenges at the same time. The high number of cloud security incidents has shown that companies are not protecting their cloud assets adequately. In this work, we propose an approach of a serious game to address this issue. This is the first step in conducting such research in the industry guided by the design science research methodology. The framework of the game is based on MITRE ATT&CK [13], and CSA cloud control matrix [10] to cope with the real-life situations encountered by enterprises in the deployment of cloud environments. Our game aims to help the participates (1) understand the different threats that cloud systems are exposed to, (2) raise awareness of the responsibilities of different roles, and (3) encourage proactive defensive thinking. Towards this goal, we present a preliminary design of the serious game and evaluate such a game with real industry players in three trial runs.

In this work, we lay the foundations for the cloud security awareness game designed in the industry, for the industry. We present the main idea of the game mechanics and introduce a novel component—the evaluator. The goal of the is to reflect the principle that perfect security cannot be achieved.

We also validated the game in three trial runs that were held in the industry. During these trial runs, valuable feedback was collected during and after the game, which enabled us to steer our design research effort. We have invited industry and academic experts to review the algorithm for the usefulness and for increasing awareness and went through two rounds of feedback and improvement.

To address the constructive feedback collected in the trial runs, e.g., regarding the granularity of the, we would like to investigate the algorithm further, refine the defense and attack game cards, and the mapping between them.

Furthermore, in the future, we would like to invite more participants to join further trial runs and understand the participants' choices in the game when choosing their defense and attack strategies. Analysis of this data can assist us in better designing the game to raise cybersecurity awareness of cloud deployments and help the participants protect cloud assets in the industry.

Author Contributions: Conceptualization, T.Z., T.G., U.L. and M.P.-A.; Methodology, U.L.; software, T.Z.; validation, T.Z., T.G., U.L. and M.P.-A.; writing—original draft preparation, T.Z.; writing—review and editing, T.Z., T.G., U.L. and M.P.-A.; visualization, T.Z.; supervision, U.L. and M.P.-A. All authors have read and agreed to the published version of the manuscript.

Funding: This work (Maria Pinto-Albuquerque) is partially financed by Portuguese national funds through FCT—Fundação para a Ciência e Tecnologia, I.P., under the projects FCT UIDB/04466/2020 and FCT UIDP/04466/2020. Ulrike Lechner acknowledges partial funding of this work in project LIONS by dtec.bw.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: Not applicable, the study does not report any data.

Acknowledgments: Maria Pinto-Albuqueque thanks the Instituto Universitário de Lisboa and ISTAR, for their support. Ulrike Lechner acknowledges partial funding of this work in project LIONS by dtec.bw.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Petrik, D.; Herzwurm, G. TiIoT ecosystem development through boundary resources: A Siemens MindSphere case study. In Proceedings of the 2nd ACM SIGSOFT International Workshop on Software-Intensive Business: Start-Ups, Platforms, and Ecosystems, Sokos Hotel Viru, Tallinn, Estonia, 26 August 2019.
2. Simunic, D.; Kerner, A.; Gajovic, S. Digital mediators as key enablers of navigation toward health in knowledge landscapes. *Croat. Med. J.* **2018**, *59*, 178–182. [CrossRef] [PubMed]
3. Top Threats to Cloud Computing: Egregious Eleven Deep Dive. Available online: https://cloudsecurityalliance.org/artifacts/top-threats-egregious-11-deep-dive/ (accessed on 15 February 2021).
4. UpGuard Team: Black Box, Red Disk: How Top Secret NSA and Army DataLeaked Online. 2017. Available online: https://www.upguard.com/breaches/cloud-leak-inscom (accessed on 15 November 2021)
5. Paladion: Poorly Configured S3 Buckets—A Hacker's Delight. Available online: https://www.paladion.net/blogs/poorly-configured-s3-buckets-a-hackers-delight (accessed on 15 November 2021)
6. Michael Scheffler, Datensicherheit in der Cloud: Best Practices Gegen Man-in-the-Cloud-Attacken. Available online: https://tinyurl.com/h2u3ky (accessed on 15 November 2021)
7. Requirements for Bodies Providing STAR Certification. Available online: https://cloudsecurityalliance.org/artifacts/requirements-for-bodies-providing-star-certification/ (accessed on 12 March 2020).
8. Di Giulio, C.; Sprabery, R.; Kamhoua, C.; Kwiat, K.; Campbell, R.H.; Bashir, M.N. Cloud standards in comparison: Are new security frameworks improving cloud security? In Proceedings of the 2017 IEEE 10th International Conference on Cloud Computing (CLOUD), Honolulu, HI, USA, 25–30 June 2017; pp. 50–57.
9. Zhao, T.; Gasiba, T.E.; Lechner, U.; Pinto-Albuquerque, M. Exploring a Board Game to Improve Cloud Security Training in Industry. In Proceedings of the Second International Computer Programming Education Conference (ICPEC 2021), Online, 27–28 May 2021; Volume 11, pp. 1–8.
10. Cloud Controls Matrix v4. Available online: https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/ (accessed on 16 February 2020).
11. Security Guidance for Critical Areas of Focus in Cloud Computing v4.0. Available online: https://cloudsecurityalliance.org/artifacts/security-guidance-v4/ (accessed on 26 July 2017).
12. ISO/IEC 27001 Information Security Management. Available online: https://www.iso.org/isoiec-27001-information-security.html (accessed on 22 October 2021).
13. Cloud Matrix. Available online: https://attack.mitre.org/versions/v8/matrices/enterprise/cloud/ (accessed on 16 February 2021).
14. Muñoz, A.; Maña, A.; González, J. Dynamic Security Properties Monitoring Architecture for Cloud Computing. In *Security Engineering for Cloud Computing: Approaches and Tools*; IGI Global: Hershey, PA, USA, 2013; pp. 1–18.
15. Popović, K.; Hocenski, Ž. Cloud computing security issues and challenges. In Proceedings of the 33rd International Convention Mipro, Opatija, Croatia, 24–28 May 2010; pp. 344–349.
16. Dörner, R.; Göbel, S.; Effelsberg, W.; Wiemeyer, J. *Serious Games: Foundations, Concepts and Practice*; Springer: Berlin/Heidelberg, Germany, 2016.
17. Bundesamt für Sicherheit in der Informationstechnik. *BSI IT-Grundschutz-Katalog*; Reguvis Fachmedien GmbH: Köln, Germany, 2016; pp. 1–5082. Available online: https://tinyurl.com/2vbs3dka (accessed on 15 November 2021).
18. Alotaibi, F.; Furnell, S.; Stengel, I.; Papadaki, M. A Review of Using Gaming Technology for Cyber-Security Awareness. *Int. J. Innov. Sci. Res.* **2016**, *6*, 660–666. Available online: https://tinyurl.com/368jhnfh (accessed on 15 November 2021). [CrossRef]
19. Tabletop Security Games & Cards. Available online: https://adam.shostack.org/games.html (accessed on 16 February 2021).
20. Shostack, A. Elevation of privilege: Drawing developers into threat modeling. In Proceedings of the 2014 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 14), San Diego, CA, USA, 18 August 2014.
21. Frey, S.; Rashid, A.; Anthonysamy, P.; Pinto-Albuquerque, M.; Naqvi, S.A. The good, the bad and the ugly: A study of security decisions in a cyber-physical systems game. *IEEE Trans. Softw. Eng.* **2017**, *5*, 521–536.
22. The NeoSens Training Method: Computer Security Awareness for a Neophyte Audience. Available online: https://airbus-seclab.github.io/dnd/us-16-Romand-Latapie-Dungeons-Dragons-And-Security-wp.pdf (accessed on 16 February 2021).
23. Beckers, K.; Pape, S. A Serious Game for Eliciting Social Engineering Security Requirements. In Proceedings of the 2016 IEEE 24th International Requirements Engineering Conference (RE), Beijing, China, 12–16 September 2016; pp. 16–25.
24. Gasiba, T.; Beckers, K.; Suppan, S.; Rezabek, F. On the Requirements for Serious Games geared towards Software Developers in the Industry. In Proceedings of the Conference on Requirements Engineering Conference, Jeju Island, Korea, 23–27 September 2019; pp. 286–296. [CrossRef]

25. Gasiba, T.; Lechner, U.; Pinto-Albuquerque, M. Sifu—A CyberSecurity Awareness Platform with Challenge Assessment and Intelligent Coach. In *Special Issue of Cyber-Physical System Security of the Cybersecurity Journal*; Avgeriou, P., Shepherd, D., Eds.; SpringerOpen: New York, NY, USA, 2020; pp. 1–23. Available online: https://cybersecurity.springeropen.com/articles/10.1186/s42400-020-00064-4 (accessed on 15 November 2021)
26. Gasiba, T.; Lechner, U.; Pinto-Albuquerque, M. CyberSecurity Challenges: Serious Games for Awareness Training in Industrial Environments. In *Bundesamt für Sicherheit in der Informationstechnik: Deutschland*; Digital. Sicher. 30 Jahre BSI—Tagungsband zum 17; Deutschen IT-Sicherheitskongress: 2021; pp. 43–56. Available online: https://www.secumedia-shop.net/Deutschland-Digital-Sicher-30-Jahre-BSI (accessed on 15 November 2021)
27. Gasiba, T.; Lechner, U.; Pinto-Albuquerque, M. CyberSecurity Challenges for Software Developer Awareness Training in Industrial Environments. In Proceedings of the 16th International Conference on Wirtschaftsinformatik, Online, 8–11 March 2021; pp. 1–17. Available online: https://aisel.aisnet.org/wi2021/NInformation12/Track12/2 (accessed on 15 November 2021).
28. Hevner, A.; March, S.; Park, J. Design science research in information systems. *MIS Q.* **2004**, *28*, 75–105. [CrossRef]
29. Gleasure, R. What Is a 'Wicked Problem' for Is Research? SIG Prag Workshop on IT Artefact Design & Workpractice Improvement. 2013 Tilburg, The Netherlands. Available online: https://research.cbs.dk/en/publications/what-is-a-wicked-problem-for-is-research (accessed on 11 November 2021).
30. Konva. JavaScript 2D Canvas Library. Available online: https://https://konvajs.org/ (accessed on 20 October 2021).