CATS: A serious game in industry towards stronger cloud security

Tiange Zhao[1,2][0000−0003−1518−4730], Ulrike Lechner[3][0000−0002−4286−3184], Maria Pinto-Albuquerque[4][0000−0002−2725−7629], Ece Ata[3][0000−0003−0924−6325], and Tiago Gasiba[1][0000−0003−1462−6701]

[1] Siemens AG, 81739, München, Germany
{tiange.zhao,tiago.gasiba}@siemens.com
[2] Universität der Bundeswehr München, 85579, München, Germany
[3] Technische Universität München, 80333, München, Germany
[4] (ISCTE-IUL), ISTAR, University Institute of Lisbon, 1649-026, Lisboa, Portugal

Abstract. Cloud computing has become a widely applied technology in the industry. Broad network access as a characteristic of cloud computing brings business value. It poses threats to cloud assets due to a greater attack surface than on-premises and other service models. Industry standards aim to regulate cloud security by enforcing best practices. To comply with the standards, practitioners in the industry are mandated to be trained to understand basic concepts of attack and defense mechanisms in cloud security to protect assets in the cloud. This work presents a serious game: Cloud of Assets and Threats (CATS), as an enrichment to the traditional training material to raise awareness about the cloud security challenges. In this paper, we introduce the design elements and implementation details of CATS. We organized eight game events with 94 industrial practitioners to validate our design. We applied a questionnaire and conducted semi-structured interviews with the game participants to evaluate the impact of the game and collect feedback. The evaluation indicates that CATS is a promising innovative method for promoting awareness of cloud security issues among practitioners in the industry, regardless of their technical background. Our main contributions are the design of such a game and the understanding of the impact of playing the CATS game in the industry.

Keywords: Serious Game · Cloud security · Awareness · Industry

1 Introduction

The size and number of cloud-based applications have risen significantly in the industry. The National Institute for Standards and Technology (NIST [32]) summarizes five characteristics of cloud computing [33]: On-demand Self Service; Broad network access; Resource Pooling; Rapid Elasticity, and Measured Service. The great flexibility and convenience contribute to development efficiency and business success. However, cloud assets are prone to various cyber-security threats [1]. Due to the broad network exposure and architecture that involves

cloud service providers and customers, the attack surface increases compared to on-premise and other service provisioning models. Also, there are security challenges that are specific to the cloud. The Cloud Security Alliance (CSA[5]) provides a ranking table of the top 11 threats in cloud computing [8]. One possible way to counter the increase of threats in cloud systems is to raise awareness of industry practitioners about cloud security. Due to the complexity of cloud deployments, a better understanding on the individual responsibilities of each stakeholder on how to secure the company assets is desired.

Numerous industry security standards propose requirements and best practices in cloud security. The Cloud Control Matrix [2] from CSA maps and compares the different existing standards. The study of Gleeson [19] has shown the complexity of those standards. Shared-responsibility model describes the responsibility of cloud service providers and cloud service customers for a cloud service based on different service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). In all three service models, it is the cloud service customers' responsibility to configure the cloud service securely. Cloud service customers are the users of a cloud service, and among them, there are different roles and responsibilities too.

Cloud security is a complex yet important topic that industry practitioners need to understand. In the work of Andrei-Cristian et al. [3], they examined the quality of infrastructure as code (IaC) in open code repositories in terms of security and found almost 300,000 security violations from over 8000 code repositories. Their study concludes that the developers miss basic concepts of cloud security and that we need to improve awareness about certain issues on cloud deployment in an industrial environment. Those fundamental concepts are generally conveyed to the developers through training. Traditional training is typically lecture-based in a face-to-face or virtual format. In recent years, there are various cyber-security serious games designed to enrich or provide an alternative to the traditional training method. Yet, none of the existing games targets the challenges in cloud security. Therefore, we designed a serious game, Cloud of Assets and Threats (CATS) to help raise awareness of cloud security in the industry. In this work, we present the design of the game and evaluate the impact of the game on industrial practitioners by means of open discussion, semi-structured interviews, and surveys.

Our work contributes to the existing body of knowledge by proposing the design of the CATS game following the design science research paradigm [24, 23]. The evaluation process of CATS gives insight into the impact of such a game on the cloud security awareness of industrial practitioners and validates the usefulness of CATS. Industrial practitioners benefit from the game as their awareness on cloud security improves by participating in the game events. Researchers could utilize the design and evaluation details of CATS as a blueprint for the further serious game and understand the possible impact of serious games on raising IT security awareness.

[5] https://cloudsecurityalliance.org/

This paper is organized as follows. After the introduction, in section 2 we analyze some work related to the application of the serious game in the context of the cyber-security field. Then, we describe the method we propose to guide our research activity in section 3. In section 4, we share details of the CATS game design and implementation. Section 5 presents the result of eight game events that took place in the industry. Section 6 shares our thought and discussion on the collected results. Section 7 concludes our work and briefly presents an outlook on the future study.

2 Related work

In the industry, standards define necessary protections for cloud assets. The best known among them is the ISO 27017 [26] and ISO 27001[25], which require the practitioners to participate in training to learn about security technologies and raise awareness on cyber-security issues. The CSA CCM (Cloud Security Alliance Cloud Controls Matrix) [2] compares 44 cloud security standards and shows an overview of the coverage of cloud security controls. MITRE ATT&CK cloud matrix [5] categorizes cloud attack actions and defense mechanisms based on real-world observations. It provides us with an adequate framework to derive the important game elements in CATS.

In the field of serious game design, Dörner et al. established a baseline for developing serious games [9]. In their seminal work, serious games are a type of game with more than just entertainment purposes. These types of games contrast with gamification. However, Landers [30] shows that both methods contain parallels and similarities. Our game, CATS, is a serious game with the purpose of assisting the players in learning important concepts in cloud security and raising awareness on cloud security problems. Raising awareness of cyber-security topics is important in practice, and various serious games have been designed in recent years for the cyber-security domain, hinting that serious games are a possible solution to cyber-security issues. Nevertheless, these games need to be well designed to achieve their goal, as shown by Landers [31]. A well-established register of games designed for cyber-security is maintained by Shostack [35].

One example is the game Riskio from Hart et al. [22], which successfully increases cyber-security awareness for people without technical backgrounds working in organizations. Riskio is a tabletop game that focuses on both defensive and offensive skills in IT security in general, however, the complicated topic of cloud security involving different stakeholders and cloud specific security challenges and mitigation are not included in depth in Riskio.

Another example is Another Week at the Office (AWATO) [13] by Ferro et al. They designed the game based on a systematic literature review and focus on the human factor that provides possibilities for phishing attacks. The primary use case is phishing attack instead of cloud security. The evaluation of AWATO shows that it is an effective tool for improving users' awareness of cyber-security best practices. Their work hints that serious game is a useful approach to solving awareness issues.

The work of Valdemar et al. [36] shows that creating serious games contributes to fostering adversary thinking. In their study over three semesters, undergraduate students learn methods of network attack and defense by creating educational games in a cyber range. The students report they had a unique opportunity to deeply understand the topic. The game is played by their collegemate, who rated the quality and educational value of the games overwhelmingly positively. Their work shows exciting results in the academic environment. Our work focuses on the specific topic of cloud security with a setting in the industry.

One work that emphasizes security mitigation in cloud deployment is the CyberSecurity Challenges from Gasiba et al. [11]. They extend their secure coding teaching platform SiFu [14, 15] with challenges addressing Terraform-aided [6] cloud deployment on Amazon Web Services [12]. The player gets flags by fixing vulnerabilities in Terraform code. It requires more technical know-how on secure coding for the players to participate and benefit the most from the game. However, their work does not cover different roles and their responsibilities in cloud security.

In [28], Jakóbik et al. present a theoretical framework to model security attack scenarios for cloud environments. Their model enables to automatically find strategies and decisions that minimize the impact that attackers can cause while maximizing the impact of the defense strategy. These derived decisions can be used by cloud administrators and also by service providers. Jakóbik refines his game and model in [27] to address a defensive strategy for threats on information confidentiality and integrity in terms of leakage and corruption. However, both these previous works do not cover industry standards, such as the Cloud Control Matrix.

The present work also builds on the work on IT security awareness by Hänsch et al. [21], and on its extension by Gasiba [17]. In their work, Hänsch et al. define three dimensions of IT security awareness: perception, protection, and behavior. These three dimensions are used to evaluate our artifact in the industry, and also to understand how the game affects the cyber security awareness of the players on cloud security.

3 Method

Gleasure [18] describes that 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'. Such problems are not suitable for traditional science approaches and instead require the situated theorizing afforded in the context of active design. Our work is guided by the design science research paradigm [24, 23] proposed by Hevner et al., since design science research can handle the changing and unstable requirements we encounter in practice and in the industry. In the work of Hevner et al., they describe the core of design science research as the cycle of Design & Implement and Justify & Evaluate. We

[6] https://www.terraform.io/

applied the method in our research. We designed and implemented the serious game artifact and organized game events for justification and evaluation.

We organize our study in a two-phase approach: in phase 1, we organize game events. Directly after each game event, we use survey and round-table open discussion to collect feedback. In phase 2, we randomly choose players who have participated in the game event two weeks to one month after the game events take place to understand the impact of the game on the players.

In phase 1, eight game events were organized in the first half of 2022. During these events, a total of 94 industry practitioners took part in our study. Some of the game events were integrated into a CyberSecurity Challenge (CSC) [15, 16] event. CSC is a type of event similar to Capture-the-flag (CTF), where CATS is a category of challenges to be solved. Players work in teams and get points by solving attack scenarios in CATS. Other game events are integrated into training. Players first attend a full-day cyber-security awareness training, in which cloud security is included as a topic. Then, the players are invited as single players instead of in teams to join the CATS game. In all the eight game events, we collected 2077 submissions, as shown in table 1.

Table 1. Overview of game events organized in the first half of 2022 - phase 1

Game Event	Date	Player	Team	CSC or Training	Valid Submissions
1	2022-01-21	17	4	CSC	177
2	2022-03-15	14	-	Training	477
3	2022-03-22	14	-	Training	493
4	2022-03-29	13	-	Training	312
5	2022-04-14	13	4	CSC	178
6	2022-04-26	11	-	Training	100
7	2022-05-03	8	-	Training	171
8	2022-06-02	4	2	CSC	169
Total number of players		94			
Total number of submissions		2077			

In the survey we distributed in phase 1, we collected 24 answers. The focus of the questionnaire is on the impact of awareness, game experience, and security knowledge, as shown in table 2. Awareness of IT security is not standardized. In this work, we extended the classification proposed by Hänsch et al [21] from IT security to cloud security. In their work, they suggest a classification of the different meanings of IT security awareness into three groups: Perception, Protection, and Behavior. In the questionnaire, we included questions to measure Perception and Protection. Behavior is evaluated in the game's dynamic activities.

In phase 2, we randomly selected 22 of the 94 players that participated in phase 1 and invited them into a semi-structured interview (SSI) in online meetings, 15 of them showed up in the meeting, and 7 of them turned down the invitation due to time conflict, as shown in table 3. The focus of a SSI is on the impact of awareness. Table 4 shows the questions for SSI. In questions 2 to question 8 (Ph2Q2 to Ph2Q8), we ask the respondent to assign a certain de-

Table 2. Overview of questions and theoretical construct - phase 1

Theoretical Construct	ID	Questions
Perception	**Ph1Q1**	Playing this cloud security game helps me to understand roles and responsibilities.
Perception	**Ph1Q2**	Playing this cloud security game helps me to understand cloud attacks and defenses.
Game Experience	**Ph1Q3**	I benefit from the collaboration with teammates in this cloud security game.
Game Experience	**Ph1Q4**	I benefit from the discussion with teammates in the cloud security game.
Protection	**Ph1Q5**	I feel my cloud security know-how has improved by playing this cloud security game.
Game Background	**Ph1Q6**	I would recommend this cloud security game to other colleagues.
Protection	**Ph1Q7**	Our strategy for cloud security will improve by repeatedly playing this cloud security game.
Security Knowledge	**Ph1Q8**	I think it is hard to calculate the actual probability of a successful defense.
Security Knowledge	**Ph1Q9**	I think it is hard to consider all relevant factors for a successful defense.

fense card to either business responsibility or technical responsibility. The asked defense cards are; Logging & Monitoring, Network Segmentation, Audit, Password Policy, Account Use Policy, Account Management, and Intrusion Detection System (IDS).

Table 3. Overview of semi-structured interview - phase 2

Number of game event participants	94
Number of invited interviewees	22
Number of show-up interviewees	15
Date of SSI	2022-04-29 ∼2022-05-25
Average duration of interview	11 min. 13 sec.
Number of questions	15

4 Design and implementation

In this section, the game design and the implementation are introduced. We detail the CATS game and the game process with the important elements in game design and implementation.

Table 4. Overview of questions in SSI - phase 2

Theoretical Construct	ID	Questions
Perception	**Ph2Q1**	Please rate how much do you still remember from the cloud security game.
Protection	**Ph2Q2∼8**	Does the defense XXX belong to Business Responsibility or Technical Responsibility?
Protection	**Ph2Q9**	Please identify the cards that was helpful in your defense strategy.
Perception	**Ph2Q10**	What is the most important thing you learn from the Cloud Security Game?
Behavior	**Ph2Q11**	What have you changed in your daily work after the game?
General	**Ph2Q12**	Do you want to add any feedback or suggestion about the Cloud Security Game?
Perception	**Ph2Q13**	The game helped me in understanding the weakness in cloud security.
Behavior	**Ph2Q14**	I think my cloud asset is secure.
Behavior	**Ph2Q15**	I think I still need more training in cloud security.

4.1 Overview of CATS

We first proposed our serious game Cloud of Assets and Threats (CATS) in our previous work [40]. To the best of our knowledge, CATS is currently the only serious game that focuses solely on raising awareness about different roles and responsibilities in secure cloud deployments. In the beginning, it was designed to be a board game with cards for two to six players. The players are divided into defense and attack teams and play cards to build attack and defense plans. More details about the game prototype and organized trial runs can be found in [39]. We initiated and refined the game design in two design iterations [41]. In the current pandemic, many face-to-face events are adapted to a virtual format. To cope with this situation, we designed and built a digital platform for CATS, where players can join as a single player or play in a team online. The players can drag and drop cards to defend themselves against cloud security attacks. In the next sections, we give a brief overview of the important game elements in CATS. We refer to CATS as the virtual board game on the digital platform.

Game process The flowchart in figure 1 shows the game process. As the game starts, the players first follow a tutorial to learn about the rules and game elements. The players are free to choose from the available attack scenarios. Details about the attack scenario are provided in the next section. During the game event, we offer the players two attack scenarios for the tutorials and four attack scenarios to be solved. We will introduce the details of attack scenarios in the next sections. The goal of the game is for players to build a defense plan by assigning defense cards to the correct responsibility. When the defense plan is

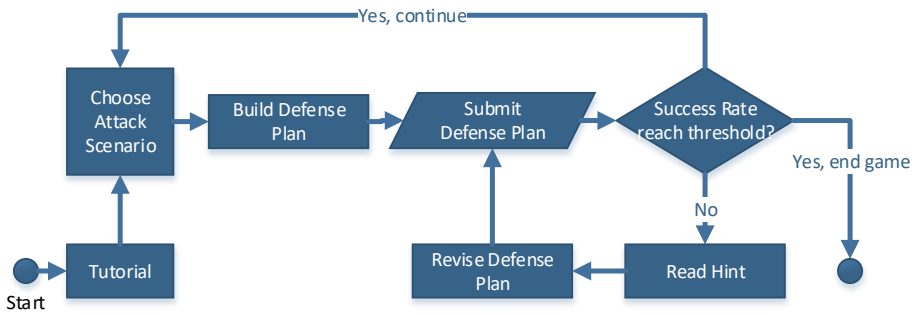

Fig. 1. The game process from player perspective

ready, players submit their defense plan to the back end by clicking a "submit" button. The back end then performs an evaluation of the chances of the cloud deployment being attacked based on the scenario and the players' selected cards and their positions. The evaluator calculates a success rate, which is the probability that the submitted defense plan withstands the given attack scenario. The game is pre-configured with a threshold, which is visible to the player in the game interface. If the calculated success rate is bigger or equal to the given threshold, the player has successfully solved the scenario and can move on to the next one. If the success rate does not reach the threshold, hints are automatically generated and sent back to the player. These hints provide a justification to the player why the card selection did or did not work. At this stage, the player is given a further chance to adjust the defense plan based on the received hints. The player can change the defense plan and submit the new plan to the back end until the game scenario is solved.

Game interface In figure 2 we show an example of the game interface. Depicted on the left side are the six chosen cards that are assigned either to "Business Responsibility" or "Technical Responsibility" area. "Business Responsibility" refers to the high-level defense actions in which important business-related decisions should be made, typically by the asset owners. "Technical Responsibilities" refers to the concrete technical defense actions, typically implemented by the asset manager. On the right side, the attack scenario is listed with three steps: step 1, initial access; step 2, launch attack; and step 3, make impact. In the first step, attack "Abuse Credential" can be mitigated by defense card "Audit"; attack "Cloud Infrastructure Discovery" can be defended by "Account Management." In the second step, attack "Abuse Trusted Relationship" and "Account Manipulation" can also be secured with the defense "Account Management." The defense card "Logging & Monitoring" can detect "Impair Defense." In the last step, the defense card "Backup Concept" can alleviate the attack "Defacement." There are in total 24 defense cards for the players to choose from. In

this example, all the attack actions are defended by at least one defense card, which results in a defense success rate of 98% according to the evaluator. If the threshold is set to 95%, this attack scenario will be solved by the card placement as depicted on the right.

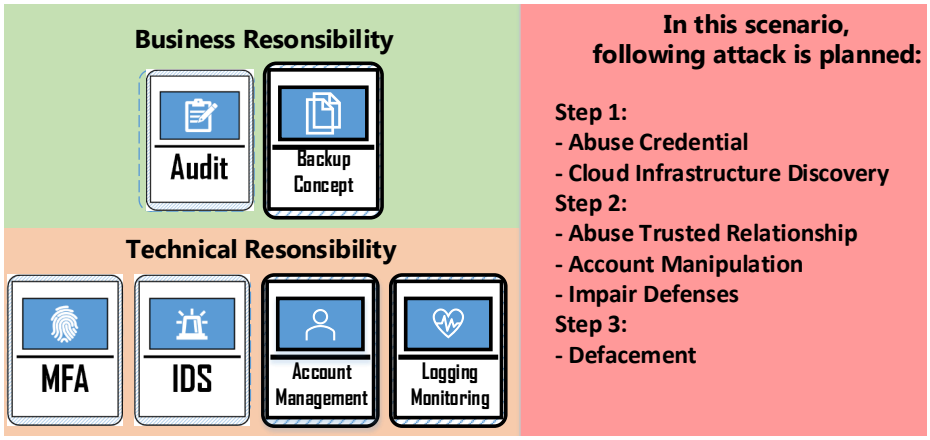

Fig. 2. Illustrative example of the game design elements

4.2 Design of CATS

In this section, we explain the design details of the important elements in CATS: Attack scenario, Submission, and Success rate.

Attack scenario and defense action To reflect facts in cloud security, the attack scenarios are derived based on real-world cyber-security attacks that have occurred and were reported in practice. In 2022 Koay et al. proposed SDGen as an approach to generate real-world cyber-security datasets[29], which is a promising proof-of-concept. In our research, we use MITRE ATT&CK cloud matrix as the source for acquiring such information [5]. We simplified the attack kill-chain into a three-step pattern: initial access, launch attack, and make impact. The effective defense actions are based on the mitigation listed for each technique [4] in the cloud matrix. In table 5, we summarize the difficulty level and goal of each attack scenario. We derived 6 attack scenarios in total. AS1 and AS2 are the tutorial attack scenarios, where we show the impact of effective cards and correct roles. AS3 is the first attack scenario where the players are required to build a full defense plan without pre-selected cards. In AS4 and AS5, the difficulty is increased by raising the threshold. In AS6, a seldom-used attack "Exploit Unused Region" is used to increase the coverage of different attack actions and reduce repetitions from previous scenarios.

Table 5. The difficulty level and goal of each attack scenario

Attack Scenario	Difficulty Level	Goal
AS1	Tutorial	Show the player the impact of choosing effective defense cards.
AS2	Tutorial	Show the player the impact of assigning effective cards to the correct roles.
AS3	Elementary	Let the player build the first full defense plan without pre-selected cards.
AS4	Advanced	Increase the difficulty by raising threshold.
AS5	Advanced	Increase the difficulty by raising threshold.
AS6	Expert	Increase defense coverage by using seldom used card.

Submission By hitting the "Submit" button on the game interface, the player triggers the back end to calculate the defense success rate. The submission that is sent to the back end is encoded in a JSON format [10]. It sent data includes the chosen defense cards and their corresponding assignment to the responsibilities and roles. Each submission is captured in the back end as dynamic game data for analysis. We present a brief statistic on the captured submission data in section 5.

Success Rate The success rate describes the quality of the submitted defense plan against the given attack scenario. The result is a percentage value that is limited between 0% to 99%. The success rate never reaches 100%, reflecting that in reality, a perfectly secure system does not exits. An evaluator calculates the success rate; the algorithm that is used for the computation is described in [39]. There are two reasons for a low success rate: 1) the defense card chosen does not mitigate the attack actions used in the attack scenario, and 2) the defense card is assigned to an incorrect responsibility, and thus, the defense cannot be performed.

4.3 Implementation of CATS

The game platform is implemented as a single-page web application. In the front end, we use Konva [20], a Javascript library providing the gadget necessary for the game interface, for instance, a canvass, floating images of defense cards, and a magnetic effect when the player is dragging and dropping the cards in the supposed area. In the back end, we implemented the evaluator with Python3 [34]. It calculates the success rate based on the presented attack scenario and the submission, then sends results and hints to the front-end. The application is packed into a docker image and deployed in AWS EC2 virtual machine [6]. Previous to each game event, we prepare a new virtual machine in AWS with automated scripts, and after the game event, we collect the data and dispose of the used AWS resources.

5 Design Evaluation

This section presents the design evaluation obtained during the eight game events that took place in the industry in phase 1 and the result obtained from the SSI in phase 2. In the first part, we show the result from game dynamic data on the correlation of the player behavior in relation to our expectancy. In the second part, we present the result collected from the questionnaire and SSI. In the third part, we share the feedback in open discussion.

5.1 Game dynamic evaluation

The players can choose from the 24 defense cards provided during the game. Each card can be helpful or useless in defending different attack actions in the given scenario, depending on if it is assigned to the correct role and if it defends any of the attack actions as provided in the attack scenario. We count the number of attack actions in our attack scenarios, to which the defense card is a proper mitigation. In that way, we can get a ranking of theoretically most helpful cards, as table 6 shows in the third column. The card "Account Management" is in the first place, which indicates it is helpful mitigation in most of the attack actions in our scenarios.

In the game dynamic data, we counted the number of each card that appeared in all the valid submissions and got another "Ranking in Game" list in the fourth column of table 6. In the most optimal condition, assuming the players know completely which defense cards are helpful against which attack action in all scenarios, we should get the same ranking list in the third and fourth column in table 6. Measuring the similarity and correlation helps to gain an insight of how well the players performed over all. There are various ways to compare the similarity and correlation of the two ranking lists. In this work, we use Spearman's ρ [38] as a way to measure the correlation of two ranking lists.

5.2 Questionnaire and SSI evaluation

Directly after each game event, we distributed a questionnaire to the participants in phase 1. Based on the eight game events we organized, we have obtained 24 valid answers from 94 participants. Table 7 gives an overview of the questions asked and the distribution of the answers. We listed nine statements in the questionnaire in table 7. The respondents were asked to answer whether they "Strongly Disagree (- -)", "Disagree (-)", "Neutral (N)", "Agree (+)", or "Strongly Agree (++)" to the statement.

Two weeks to one month after each game event, we randomly selected game participants and invited them to join an SSI in phase 2. We list the questions in table 4. The table 8 depicts the result of question Ph2Q1, Ph2Q13 to Ph2Q15.

We present the results of questions Ph2Q2 to Ph2Q8 in figure 3. The blue bar shows the players' performance in-game and the red bar shows the percentage of the correct answer in the survey in terms of assigning the defense actions to a correct role. We see that the players perform nicely in the game and survey for

Table 6. The defense cards ranking in theory, in game and in survey

No.	Defense Card	Ranking in Theory	Ranking in Game	Ranking in SSI
1	**Account Management**	1	7	2
2	**Network Segmentation**	2	3	1
3	**Restrict Permission**	3	11	2
4	**Logging & Monitoring**	4	1	6
5	**Asset Management**	5	12	2
6	**Filter Network Traffic**	5	8	6
7	**Password Policy**	7	2	6
8	**Audit**	7	6	11
9	**MFA**	7	13	2
10	**Critical Data Protection**	10	10	11
11	**Update Software**	10	18	17
12	**Information Encryption**	10	16	20
13	**Backup Concept**	13	14	6
14	**Application Isolation and Sandboxing**	13	9	6
15	**Vulnerability Scan**	13	15	11
16	**OS Hardening**	13	16	17
17	**IDS**	13	5	11
18	**Remove Unnecessary Feature**	13	21	22
19	**Application Developer Guidance**	19	19	22
20	**User Training**	19	20	11
21	**Account Use Policy**	19	4	11
22	**Software Configuration**	22	22	20
23	**Code Signing**	23	24	17
24	**ACP Process**	24	23	22
Spearman's ρ			0.66	0.75

some defenses such as Intrusion Detection System (IDS) and Network Segmentation. However, in some other defenses, the players made more mistakes in the survey at least two weeks after the game event.

In Ph2Q9, we asked them to identify the helpful cards. We ranked their answer and summarized the result into the last column in table 6. As shown in the table 6, the correlation to the ranking in theory is reflected by Spearman's ρ and the SSI value is higher than the game value. The rest of the questions are open-ended questions and the result will be summarized and presented in the next part.

5.3 Evaluation from open discussion and open-ended questions in SSI

We asked the players for their opinion in the open discussion after each game event. In table 9, we present a selection of the feedback and answers to the open-ended questions. The second column represents whether the feedback is collected

Table 7. Questionnaire after each game event - phase 1

No.	Questions	- -	-	N	+	++
Ph1Q1	Playing this cloud security game helps me to understand roles and responsibilities.	0%	0%	16%	63%	21%
Ph1Q2	Playing this cloud security game helps me to understand cloud attacks and defenses.	0%	0%	4%	79%	17%
Ph1Q3	I benefit from the collaboration with teammates in this cloud security game.	0%	8%	38%	29%	25%
Ph1Q4	I benefit from the discussion with teammates in the cloud security game.	0%	8%	29%	42%	21%
Ph1Q5	I feel my cloud security know-how has improved by playing this cloud security game.	0%	13%	8%	75%	4%
Ph1Q6	I would recommend this cloud security game to other colleagues.	0%	8%	4%	58%	30%
Ph1Q7	Our strategy for cloud security will improve by repeatedly playing this cloud security game.	0%	12%	29%	42%	17%
Ph1Q8	I think it is hard to calculate the actual probability of a successful defense.	0%	0%	25%	42%	23%
Ph1Q9	I think it is hard to consider all relevant factors for a successful defense.	0%	0%	21%	42%	27%

Table 8. Questions in SSI - phase 2

No.	Question	- -	-	N	+	++	N.A
Ph2Q1	Please rate how much do you still remember from the cloud security game	0%	0%	20%	67%	13%	-
Ph2Q13	The game helped me in understanding the weakness in cloud security	13%	0%	13%	67%	7%	-
Ph2Q14	I think my cloud asset is secure.	0%	6%	7%	27%	20%	40%
Ph2Q15	I think I still need more training in cloud security.	13%	7%	27%	20%	33%	-

in the discussion of phase 1 (Ph1D) or the answers to open-ended questions in phase 2 (Ph2Q10, Ph2Q11 and Ph2Q12). In general, the comments we received were quite positive. We will discuss the feedback in more depth in the next section.

6 Discussion

In this section, we discuss the results and share our thoughts upon them.

In table 6, we see that in theory, the card "Account Management" helps defend against most of the attack actions. The importance and account management is sufficiently discussed in the work of Tang et al. in [37]. However, in the game it is not the most selected card, being at the seventh position in the ranking list in the game. In the game, the most selected card is "Logging & Monitoring". This indicates that participants believe relying on logging and monitoring will

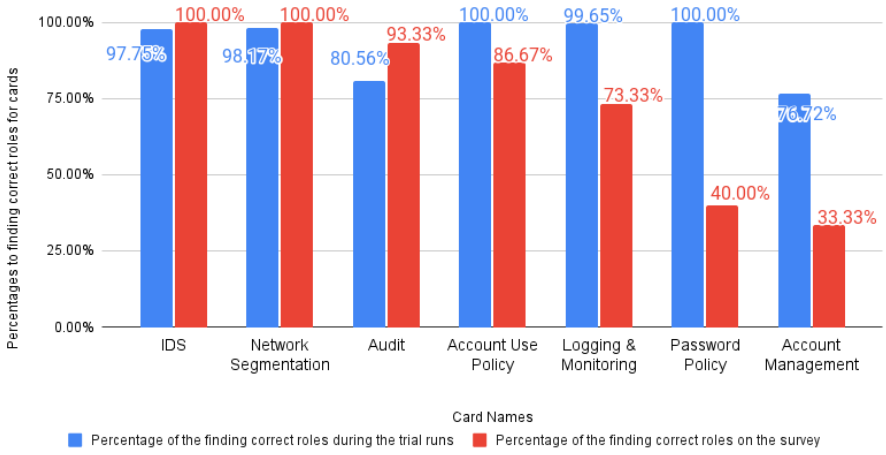

Fig. 3. The percentage of finding correct roles for cards on the survey

improve cloud security, whereas account management contributes more in defending cloud assets. We use Spearman's ρ as a way to measure the correlation between two ranking lists. We refer to the table 10 to interpret the calculated value as proposed in [7]. Spearman's ρ has a range between "-1" and "1". The value "-1" suggests that the two compared ranking lists are negatively correlated. That is the case when one list is the reserve of the other. "0" suggests there is no correlation between the two lists. "1" suggests that the two compared ranking lists are perfectly correlated. That is the case when two lists are identical. In our case, Spearman's ρ of our expectancy and the players' behavior in the game reached 0.66, which suggests a moderate correlation as shown in table 10. This is a positive indicator that players' performance in the game seconds our expectancy. The players understand the game logic and grasp the fundamental concept of cloud security. In the last column of table 6, we calculated the correlation of the expectation and the SSI, the value reached 0.75, which shows a strong correlation according to table 10. We take it as a positive sign that the players' understanding of cloud security defense actions has improved. One possible explanation could be, during the game, the player is learning about the defenses and attacks, thus players might make mistakes. By correcting the mistakes, players deepen their knowledge about defenses and attacks and remember them. In the survey, when they are asked again, their answer shows more similarity to the optimal case. Since the SSI was conducted two weeks to one month after the game event, we can interpret the results as a possible indicator on the retention of knowledge and also on the impact of the game on the players.

Table 7 summarizes the answers to the questionnaire in phase 1. Most respondents agree that CATS helps them understand roles and responsibilities in cloud security, and know-how is improved by playing CATS. We imply that the player's perception of cloud security is improved by the game and the player

Table 9. Selection of representative feedback collected in phase 1 and 2

No.	Questions	Feedback / Answer
FB1	**Ph1D**	"Thank you so much! It is possible to learn new technical vocabulary (with the game)."
FB2	**Ph1D**	"It is great to have hands-on experiences in building a cloud defense strategy! I enjoyed the game."
FB3	**Ph1D**	"Provide some explanations for both responsibilities (Asset Owner/Manager) as well as for the cards."
FB4	**Ph1D**	"Less abstraction and more context would be helpful. E.g. an architecture overview about the system under attack would be helpful."
FB5	**Ph1D**	"More time for the game."
FB6	**Ph2Q10**	"Cloud deployment is not one person responsibility but shared responsiblity."
FB7	**Ph2Q10**	"I improve my awareness"
FB8	**Ph2Q10**	"The game is too abstract to learn anything."
FB9	**Ph2Q11**	"I did't change anything."
FB10	**Ph2Q12**	"Add animations to the hints."

Table 10. Degree of Correlation according to Spearman's Rho

Range	Degree of Correlation
$0<\|\rho\|<0.3$	Weak
$0.3<\|\rho\|<0.7$	Moderate
$\|\rho\|>0.7$	Strong

is more aware of how to protect cloud assets. Most of them would recommend CATS to other colleagues. We interpret those answers as a positive sign that the players enjoyed CATS and could benefit from it. In question Ph1Q6, 30% of the respondents strongly agree and 58% of them agree that they would recommend the game to other colleagues, which hints at a good design of the game. In the questionnaire, we did not get any "strongly disagree" answers to all the questions, which shows the game was well received by the participants.

Table 9 shows some of the feedback and answers collected in open discussion in phase 1 and open-ended questions in phase 2. Most of them are excited about using the game as a method to learn (FB1). They are embracing the interactive exercises (FB2) and want to spend more time with the game (FB5). For some of them, the game is too abstract (FB8) and more concrete examples (FB4) and explanations (FB3) are wished. The players learned that cloud security is a shared responsibility (FB6) and they feel their awareness of cloud security is improved by playing the game (FB7). Some give constructive feedback on how to improve the game interface (FB10). We will take it into consideration in the next design iteration. In question Ph2Q11, we received lots of answers that the game did not trigger any change in their daily work (FB9) despite the increase in awareness. We would like to conduct future research on the reason behind that and to improve the game further. According to the feedback and answer

we collected, it is safe to conclude that the game is suitable to raise awareness of cloud security, especially the defenses versus the attacks and the roles and responsibilities.

In our observation of eight game events, the participants mostly identify the card "Account Management" to be helpful in lots of attack scenarios. They learn about the impact of this card in the game and in the SSI in phase 2, they rank "Account Management" as the second most helpful card as shown in table 6. This indicates that they use the game to correct their wrong understanding. Additionally, the participants seem to enjoy the game.

In phase 2, we asked the respondents to assign certain defense cards to the correct role. The results are illustrated in figure 3, which reflects what the players still remember after the game. For some cards such as "IDS" (Intrusion Detection Systems), "Network Segmentation", and "Audit", the correct rate increases in SSI of phase 2. For cards such as "Account Use Policy", "Logging & Monitoring", "Password Policy" and "Account Management", the correct rate decreases. Surprisingly, although the participants understand the importance of "Account Management", only 33% of the participants assigned it to the correct role in the SSI of phase 2. The card "Password Policy" has a 100% of correct rate on the role assignment during the game, however, the correct rate drops to only 40% in the SSI. There might be multiple factors that could lead to such results, e.g. daily work and chores. We need to conduct further research to understand the cause of decreasing in correct rate. It might be an indicator that the game should be played more often to solidify the lessons learned, which seconds with the results of Ph1Q7 in table 7, almost 60 % of the participants agree or strongly agree that their defense strategy for cloud security will be improved by repeatedly playing CATS.

7 Conclusion

In this work, we present CATS, a serious game dedicated to raising awareness about cloud security issues in the industry. We introduced the design elements and implementation details of CATS, and we invited 94 industrial practitioners to join the game and collect feedback from them. There are positive indicators that the participants enjoyed the interactive game, and their understanding of basic concepts in cloud security was improved. We validated our design and ideas with eight game events. We provided a preliminary analysis of collected game dynamic data and proposed a measurable way to evaluate the level of understanding of cloud security basic concepts of our game participants. We used questionnaires and semi-structured interviews to collect feedback, and the result is presented and discussed. Our work shows CATS has the potential to be applied as a useful artifact to raise awareness of cloud security in the industry. The contribution of this work is: 1) to propose an innovative serious game as an enrichment of traditional lecture-based virtual and physical training; 2) to extend the understanding of the usage of CATS in an industrial environment.

In the future, we would like to refine the evaluator algorithm and collect further feedback for improvement in additional CATS game events.

Acknowledgements This work 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. Furthermore, the third author thanks the Instituto Universitário de Lisboa and ISTAR, for their support. We acknowledge funding for project LIONS by dtec.bw.

References

1. Al Nafea, R., Almaiah, M.A.: Cyber security threats in cloud: Literature review. In: 2021 International Conference on Information Technology (ICIT). pp. 779–786. IEEE (2021)
2. Alliance, C.S.: Cloud controls matrix v4. https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/ (2021)
3. Andrei-Cristian, I., Gasiba, T.E., Zhao, T., Lechner, U., Pinto-Albuquerque, M.: A large-scale study on the security vulnerabilities of cloud deployments. 1st International Conference on Ubiquitous Security (UbiSec 2021) (2021)
4. ATT&CK, M.: Techniques. https://attack.mitre.org/techniques/ (May 2017)
5. ATT&CK, M.: Mitre att&ck cloud matrix. https://attack.mitre.org/versions/v8/matrices/enterprise/cloud/ (2020)
6. aws: Amazon ec2 secure and resizable compute capacity for virtually any workload. https://aws.amazon.com/ec2 (May 2022)
7. Casinillo, L., Tavera, G.: On the dark side of learning calculus: Evidence from agribusiness students. IJIET (International Journal of Indonesian Education and Teaching) **5**, 52–60 (01 2021). https://doi.org/10.24071/ijiet.v5i1.2825
8. CSA: Top threats to cloud computing: The egregious 11. BLACKHAT2019 (2019)
9. Dörner, R., Göbel, S., Effelsberg, W., Wiemeyer, J.: Serious Games: Foundations, Concepts and Practice. Springer (2016)
10. ECMA-404: Json format. https://www.json.org/json-en.html (May 2022)
11. Espinha Gasiba, T., Andrei-Cristian, I., Lechner, U., Pinto-Albuquerque, M.: Raising security awareness of cloud deployments using infrastructure as code through cybersecurity challenges. In: The 16th International Conference on Availability, Reliability and Security. ARES 2021, Association for Computing Machinery, New York, NY, USA (2021). https://doi.org/10.1145/3465481.3470030, https://doi.org/10.1145/3465481.3470030
12. Espinha Gasiba, T., Andrei-Cristian, I., Lechner, U., Pinto-Albuquerque, M.: Raising security awareness of cloud deployments using infrastructure as code through cybersecurity challenges. In: The 16th International Conference on Availability, Reliability and Security. pp. 1–8 (2021)
13. Ferro, L.S., Marrella, A., Catarci, T., Sapio, F., Parenti, A., De Santis, M.: Awato: A serious game to improve cybersecurity awareness. In: Fang, X. (ed.) HCI in Games. pp. 508–529. Springer International Publishing, Cham (2022)
14. Gasiba, T., Lechner, U., Pinto-Albuquerque, M.: Sifu-a cybersecurity awareness platform with challenge assessment and intelligent coach. Cybersecurity **3**(1), 1–23 (2020)

15. Gasiba, T., Lechner, U., Pinto-Albuquerque, M.: Cybersecurity challenges for software developer awareness training in industrial environments. In: Ahlemann, F., Schütte, R., Stieglitz, S. (eds.) Innovation Through Information Systems. pp. 370–387. Lecture Notes in Information Systems and Organisation, Springer International Publishing, Cham (2021)
16. Gasiba, T., Lechner, U., Pinto-Albuquerque, M.: Cybersecurity challenges: Serious games for awareness training in industrial environments. Federal Office for Information Security (ed.): Germany. Digital. Secure. 30 Years BSI - Proceedings of the 17th German IT Security Congress 2021 (2 2021)
17. Gasiba, T.J.E.d.M.: Raising Awareness on Secure Coding in the Industry through CyberSecurity Challenges. Ph.D. thesis, Universität der Bundeswehr München (2021)
18. Gleasure, R.: What is a 'wicked problem' for is research? In: SIG Prag Workshop on IT Artefact Design & Workpractice Improvement, 5 June, 2013, Tilburg, The Netherlands (2013)
19. Gleeson, N., Walden, I.: 'It's a Jungle Out There'?: Cloud Computing, Standards and the Law. SSRN Electronic Journal (01 2014). https://doi.org/10.2139/ssrn.2441182
20. Group, K.: Konva.js - html5 2d canvas js library for desktop and mobile applications. https://konvajs.org/ (May 2022)
21. Hänsch, N., Benenson, Z.: Specifying IT security awareness. In: 2014 25th International Workshop on Database and Expert Systems Applications. pp. 326–330. IEEE (2014)
22. Hart, S., Margheri, A., Paci, F., Sassone, V.: Riskio: A serious game for cyber security awareness and education. Computers & Security **95**, 101827 (2020). https://doi.org/10.1016/j.cose.2020.101827
23. Hevner, A.: A three cycle view of design science research. Scandinavian Journal of Information Systems **19** (01 2007)
24. Hevner, A., March, S., Park, J.: Design science in information systems research. Management Information Systems Quarterly (2004)
25. ISO27002: Iso/iec 27002:2013information technology — security techniques — code of practice for information security controls. https://www.iso.org/standard/54533.html (2013)
26. ISO27017: Iso/iec 27017:2015 information technology — security techniques — code of practice for information security controls based on iso/iec 27002 for cloud services. https://www.iso.org/standard/43757.html (2015)
27. Jakóbik, A.: Stackelberg game modeling of cloud security defending strategy in the case of information leaks and corruption. Simulation Modelling Practice and Theory **103**, 102071 (2020)
28. Jakóbik, A., Palmieri, F., Kołodziej, J.: Stackelberg games for modeling defense scenarios against cloud security threats. Journal of network and computer applications **110**, 99–107 (2018)
29. Koay, A.M.Y., Xie, M., Ko, R.K.L., Sterner, C., Choi, T., Dong, N.: Sdgen: A scalable, reproducible and flexible approach to generate real world cyber security datasets. In: Wang, G., Choo, K.K.R., Ko, R.K.L., Xu, Y., Crispo, B. (eds.) Ubiquitous Security. pp. 102–115. Springer Singapore, Singapore (2022)
30. Landers, R.N.: Developing a theory of gamified learning: Linking serious games and gamification of learning. Simulation & gaming **45**(6), 752–768 (2014)
31. Landers, R.N.: Gamification Misunderstood: How Badly Executed and Rhetorical Gamification Obscures Its Transformative Potential. Journal of Management inquiry **28**(2), 137–140 (2019)

32. NIST: National institute of standards and technology. https://www.nist.gov/ (2022)
33. Peter Mell (NIST), T.G.N.: Sp 800-145the nist definition of cloud computing. https://csrc.nist.gov/publications/detail/sp/800-145/final (Sep 2011)
34. Python3: Python is a programming language that lets you work quickly and integrate systems more effectively. https://www.python.org/ (May 2022)
35. Shostack, A.: Tabletop security games & cards. https://https://shostack.org/games.html (2021)
36. Švábenskỳ, V., Vykopal, J., Cermak, M., Laštovička, M.: Enhancing cybersecurity skills by creating serious games. In: Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education. pp. 194–199 (2018)
37. Tang, Y., Zhang, D., Liang, W., Li, K.C., Sukhija, N.: Active malicious accounts detection with multimodal fusion machine learning algorithm. In: Wang, G., Choo, K.K.R., Ko, R.K.L., Xu, Y., Crispo, B. (eds.) Ubiquitous Security. pp. 38–52. Springer Singapore, Singapore (2022)
38. Wiki, E.: Spearman's rank correlation coefficient. https://www.viewer.vn/wiki (1988)
39. Zhao, T., Gasiba, T., Lechner, U., Pinto-Albuquerque, M.: Raising awareness about cloud security in industry through a board game. Information **12**(11) (2021). https://doi.org/10.3390/info12110482
40. Zhao, T., Gasiba, T.E., Lechner, U., Pinto-Albuquerque, M.: Exploring a Board Game to Improve Cloud Security Training in Industry. In: Henriques, P.R., Portela, F., Queirós, R., Simões, A. (eds.) Second International Computer Programming Education Conference (ICPEC 2021). Open Access Series in Informatics (OASIcs), vol. 91, pp. 11:1–11:8. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany (2021). https://doi.org/10.4230/OASIcs.ICPEC.2021.11, https://drops.dagstuhl.de/opus/volltexte/2021/14227
41. Zhao, T., Lechner, U., Pinto-Albuquerque, M., Ata, E.: Cloud of Assets and Threats: A Playful Method to Raise Awareness for Cloud Security in Industry. In: Simões, A., Silva, J.a.C. (eds.) Third International Computer Programming Education Conference (ICPEC 2022). Open Access Series in Informatics (OASIcs), vol. 102, pp. 6:1–6:13. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany (2022). https://doi.org/10.4230/OASIcs.ICPEC.2022.6, https://drops.dagstuhl.de/opus/volltexte/2022/16610