Cloud of Assets and Threats: A Playful Method to Raise Awareness for Cloud Security in Industry

Tiange Zhao
Siemens AG, München, Germany
Universität der Bundeswehr München, Germany

Ulrike Lechner
Universität der Bundeswehr München, Germany

Maria Pinto-Albuquerque
Instituto Universitário de Lisboa (ISCTE-IUL), ISTAR, Portugal

Ece Ata
Siemens AG, München, Germany
Technische Universität München, Germany

Abstract

Cloud computing has become a convenient technology widely used in industry, providing profit and flexibility to companies. Many enterprises embrace cloud service by migrating their products and solutions from on-premise to cloud environments. Cloud assets and applications are vulnerable to security challenges if not adequately protected. Regulations, standards and guidelines aim to enforce cloud security controls in the industry and practitioners need training to raise awareness of cloud security issues and learn about the defense mechanisms and controls. We propose a serious game Cloud of Assets and Threats (CAT) for enhancing cloud security awareness of industrial practitioners. This study extends first results of applying such a serious game in industry [25] and refines its design in two iterations. In the first design iteration, we implemented a digital game platform with six attack scenarios and developed a new player versus environment gaming mode. In the second design iteration, we adjusted the attack scenarios and introduced different difficulty levels for the scenarios. We present, analyse, and discuss the game events. We conclude that CAT is a promising method to raise awareness for cloud security in the industry.

2012 ACM Subject Classification Computer systems organization → Cloud computing; Social and professional topics → Computer and information systems training

Keywords and phrases Cloud security, Cloud control matrix, Shared-responsibility model, Industry, Training, Gamification

Digital Object Identifier 10.4230/OASIcs.ICPEC.2022.6

Funding 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.

1 Introduction

Nowadays, companies are moving their products and solutions from on-premises to cloud deployment. The size of the cloud computing and hosting market grows at a steady speed, as shown statistically [22]. On the one hand, the convenience and flexibility of cloud services contribute to the market growth. On the other hand, cloud deployment could expose industry systems to serious cybersecurity threats. The traditional vulnerabilities become more dangerous as cloud deployment increases system exposure and new types of cloud specific threats, e.g. breach of cloud storage object, are emerging. Several stakeholders, including cloud asset managers, cloud asset owners and cloud service providers, are involved in

Third International Computer Programming Education Conference (ICPEC 2022).
Editors: Alberto Simões and João Carlos Silva; Article No. 6; pp. 6:1–6:13
OpenAccess Series in Informatics
OASICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

the design and development life cycle of cloud services. Each stakeholder needs to understand its role and responsibility to secure a cloud asset. Standards and white papers aim to regulate the industry field and provide the basis for a shared understanding of roles and responsibilities in securing cloud assets among all stakeholders involved. However, security training is important to convey concepts and strategy to decision makers, developers, system architects and cloud service users. In cybersecurity, serious games can be a method to raise awareness and enable learning by doing in a playful, safe environment. This research contributes to enrich and improve the existing training methods in cloud security through a serious game. Our goal is to increase the level of cloud security by increasing cloud security awareness with a special focus on shared roles and responsibilities in securing cloud assets.

We have designed a board game, Cloud of Assets and Threats(CAT), which can be used for cybersecurity educational purposes for industry practitioners. We address different roles and their shared responsibilities to secure cloud asset as one of the topics of our serious game. This study presents a refinement of our board game dedicated to tackling different aspects of cloud security and facilitating awareness and improving cloud security for the industry. This initial prototype is described in our previous work [25]. It is a game in which attacker and defender develop strategies to attack or defend the cloud assets. This study presents a refinement: single players or teams play defenders for cloud-based systems in various attack scenarios and a evaluator component assesses the effectiveness of defense. This refinement of the game logic allows for a more effective training as defense is what professionals in industry need to understand. Two contexts of the game are used in the two design iterations: in the first design iteration, the game is part of a larger serious game experience, in the second it is a stand-alone game used to bring contents from a training session into practical application. These two different contexts allow to understand how to tailor the game to specific user groups and insights on raising awareness. This paper describes the design, implementation, and evaluation of such a game performed in first and second design iterations. We reflect on the effectiveness of the game to raise awareness and the understanding of how to tailor the game to various user groups.

This article is structured in the following sections: section 2 introduces the related work in the areas of information security standards relevant for cloud security, and serious games in information security. Section 3 gives an overview of the design science research method we followed in our research. Section 4 describes the framework of our game and the two design iterations we went through. Section 5 shares the game dynamic data and results we collected from our game events and our thinking upon them. Section 6 concludes this work and gives an outlook into the future research direction.

2 Related work

Existing information security standards in the industry describe the requirements and necessary controls on cloud security. The cloud controls matrix (CCM) [1] from cloud security alliance (CSA) provides mapping and comparison of various control specifications and 44 relevant industrial standards. Best known is the ISO/IEC 2700X family [8, 18, 19, 20], which provides information security requirements in general, or specifically address information security controls for cloud service. In addition to the standards mentioned above, MITRE ATT&CK cloud matrix categorizes possible attacks towards cloud systems based on real-world observation and groups them in different techniques and tactics [5]. For each possible attack, the defense mechanisms are listed. Our work uses the MITRE framework as a reference for the attack and defense models. This helps to bring industry standard requirements to the practitioners by introducing the cloud security concepts through a serious game.

Dörner et al. [7] presents seminal concepts for designing serious games. They describe that serious games are designed with a goal instead of pure entertainment. It guides us in the design and instantiation of our game. The goal of the serious game is to raise the cybersecurity awareness of the participants.

There are numerous examples of serious games application in information security that help raise awareness and serves educational purposes directly or indirectly. Frey et al. [9] focus on the human factor and use a serious game as a novel method to study the decision-making process in the field of information security. Shostack lists more than forty tabletop serious games for cybersecurity [23], and the list is still growing. One of them is the game Riskio [14], which is successful in increasing cybersecurity awareness for people without technical backgrounds working in organizations. Apart from tabletop games, the work of Gasiba et al. [10, 11, 13, 12] present a serious game inspired by the capture-the-flag genre, yet dedicated to software developers in the industry to raise their awareness on secure programming and improve their secure coding skills in a variety of programming languages.

However, none of the games mentioned above specifically addresses the issues in cloud security, e.g., the shared-responsibility model and the newborn types of threats that are unique in the cloud environment. This article is based on our design and evaluation of a cloud security game firstly introduced in our previous research [25, 24]. This work extends and improves the existing game prototype by implementing a digital platform, designing game mode variations, and refining the game to address the feedback collected.

3 Method

Our research is guided by the design science paradigm proposed by Hevner et al. [16, 15]. They describe the design of a useful artefact as a creative search process. Hevner et al. describe the cycle of design & implement and justify & evaluate to be the core of design science. We use explanatory design theory proposed by Baskerville et al. [6] to guide design and evaluation. Baskerville et al. present an approach which differentiates between the process to design the artefact and the evaluation of the artefact and emphasises on the design process to be a creative endeavor. This approach describes a general design solution as a class of problems that relates a set of general components to a set of general requirements [17].

We identify the requirements and relate them to components in our design. General requirements (GR) for the game are listed as the following:

- **GR1**: The game artefact should reflect facts or characteristics about cloud security.
- **GR2**: The game artefact should be understandable and straightforward to the players.
- **GR3**: Players' cloud security awareness should increase by playing the game.
- **GR4**: The game should be fun and interactive in that it motivates the participants to learn about cloud security.

General components (GC) are also identified and could be mapped to the general requirements:

- **GC1, mapped to GR1**: Attack scenarios developed are based on actual attacking activities observed from real-world as well as standards as the MITRE attack vectors.
- **GC2, mapped to GR2**: Tutorials and different difficulty levels are available in the game.
- **GC3, mapped to GR3**: The game concept encourages players to act as defenders against the game´s attack scenarios. This addresses the specific skills needed in the everyday job.
- **GC4, mapped to GR4**: Participants see hints and suggestions from the platform to strengthen their defense strategy until the threshold of defense success rate is reached.

Table 1 Overview of the game events in iteration 1 and 2.

	Iteration 1 (I1)	Iteration 2 (I2)
Number of participants	17	14
Date	January 26, 2022	March 15, 2022
Teams / single players	4 Teams	14 Single players
Game time	~60 mins	30 mins
Number of submissions	175	656
Avg. submission per scenario per team/player	7.3	7.8

This study builds on a game idea and a prototype with its evaluation presented in [25]. This study continues the creative search process for a solution that is more effective in raising the level of cloud security awareness and to a deeper understanding of players needs, and players level of cloud security knowledge. Our game design is developed in two design iterations. In both iterations we organized game events to collect feedback for evaluation of the artefact. Table 1 provides an overview of the two iterations and the serious game event conducted as empirical basis for the evaluation. All players are professionals in industry and they are invited to game event after awareness training or during a CyberSecurity Challenges (CSC) event [13, 12], which normally has a group size of 10 to 20 trainees or participants. The table provides information about the number of participants, whether the game was played in single player or team mode, the number of solution submissions done in the game and the average number of submissions per team or per single player.

4 Game design

In this section, we describe the design of our game. Firstly, we briefly introduce our game prototype as a base line. Then we describe our game design in the first iteration. At last, we explain the improvement and adjustment we made in the second iteration.

4.1 Baseline – the Game prototype

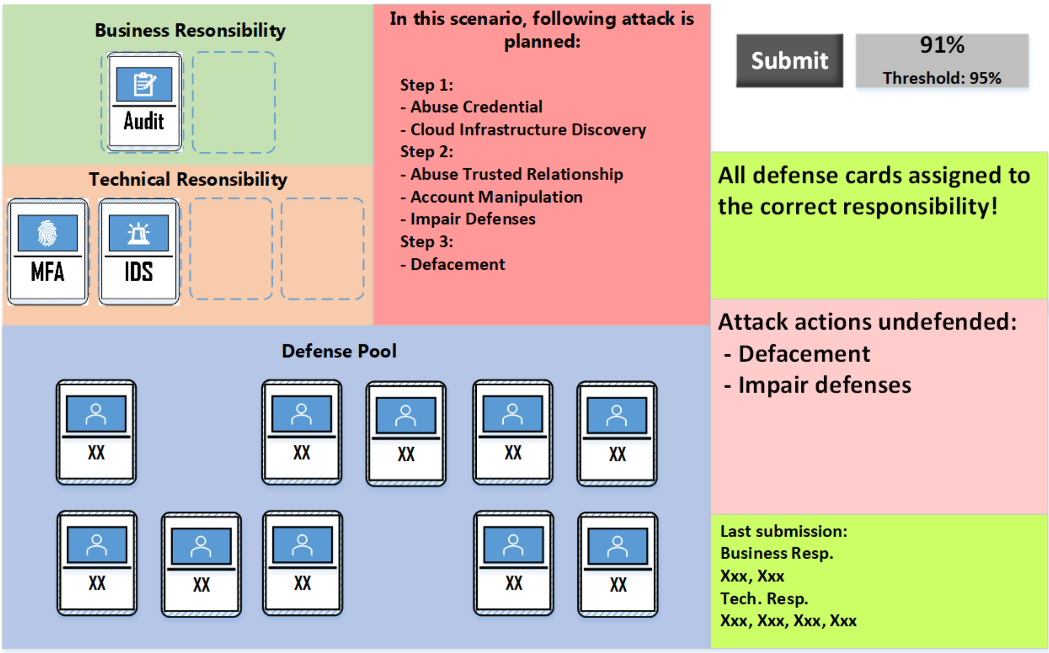
The original game artefact is an online board game. There is a game master (GM), and players play either as defender team or as attacker team against each other. The defender team uses the defense action cards to build a defense-in-depth defense plan within a given time by selecting cards and assigning the cards to the responsible roles. The attacker team uses the attack action cards to build a step-by-step attack plan. When time is up, an automated evaluator takes both the attack and defense plans as input and calculates the defense plan's probability of withstanding the attack plan. The higher the probability, the more likely the defender team would win. A wheel-of-fortune takes the probabilities calculated by the evalulator components and determines the winner. A more detailed description of the game prototype can be found in our previous publication [25]. This game was evaluated positively on the basis of a limited empirical basis. The game logic is validated and the trial run participants found the game engaging and they learned about how to build an effective defense for cloud assets in real world. Notwithstanding this first positive evaluation, we did an analysis to see whether there is room for improvement. In our previous work, we conducted online trial runs with the game prototype, where players played versus players (PvP) integrated either in defender team or attacker team. There are some disadvantages of such a game mode:

- The learning effect for the attacker team is not well aligned with the goal, since professionals need skills in defense, not in attack strategies.
- This game mode requires a game master to coordinate and the game master cannot take care of the training activities and questions while managing the game.
- There must be at least two players to build two teams, and the size of a team cannot be too big for effective communications and a good sense of involvement. So the game does not scale well in an industrial context.

4.2 First design iteration

In the first design iteration (I1), the previously-mentioned disadvantages are addressed. We implement a digital platform with a player versus environment (PvE) game mode and as a part of the environment, we build six attack scenarios derived from real-world cloud security attack activities. The implementation is based on the game board we designed as baseline in the prototype and we developed the digital platform using konva[4]. Konva is HTML5 2d canvas JavaScript library for desktop and mobile applications, which provides our the necessary features for the development. We introduce each element one by one subsequently and share the evaluation of the first iteration.

4.2.1 Digital platform



In this scenario, following attack is planned:

Step 1:
- Abuse Credential
- Cloud Infrastructure Discovery

Step 2:
- Abuse Trusted Relationship
- Account Manipulation
- Impair Defenses

Step 3:
- Defacement

All defense cards assigned to the correct responsibility!

Attack actions undefended:
- Defacement
- Impair defenses

Last submission:
Business Resp.
Xxx, Xxx
Tech. Resp.
Xxx, Xxx, Xxx, Xxx

Figure 1 Mock-up of the cloud security game board.

The digital platform is a single-page web application, on which the players play the game. When a player accesses the game homepage, the game interface depicted in figure 1 will be displayed. The web application has a back-end and a front-end. The evaluator algorithm runs in the back-end calculating the quality of the defense plan against the given attack. The front-end displays the cards and game interface, players can drag and drop cards. The defense plan area is designed with magnetic effect. When the player drags the cards near to the area, the card would be pulled to one of the reserved space. Magnetic effect assures the player that this is the place where the cards should be placed. If cards are placed outside this area, it would be sent to its original position in the defense pool. The The game interface has seven areas with specific purpose and functionality. Clockwise from the top left are:

- Defense Plan Area – The defense plan area consists of the business and technical responsibility zones. The players are supposed to pick cards from these sub-areas and place them in the correct responsibility zone.
- Attack Plan Description Area – This area describes the hypothetical attackers plan, step-by-step. In the mock-up of figure 1, we show the attack scenario I1S1. The players can search for technical terms that the attackers use in each step to build an effective defense plan.
- Submit Button and Threshold – The player can send the selected defense plan to the back-end for evaluation by hitting the Submit button. The calculated probability of the submitted defense plan withstanding the hypothetical attack is displayed in the top right corner. The player completes the challenge if the threshold is reached.
- Hint Area for Responsibility – Hint Area for Responsibility is the first hint area. It shows in the last submission if all the cards are assigned to the correct responsibility. The wrongly assigned ones will be listed here, and the players can improve their defense plan based on the hint.
- Hint Area for Undefended Attacks – Hint Area for Undefended Attacks is the second hint area. Based on the last defense plan submission, it shows the undefended cards in the given attack plan. The players can improve their defense success rate by trying to cover as many attack actions as possible.
- Last Submission Area – The defense plan in the last submission is shown here. It gives the player a reference as they are trying to improve their Defense.
- Defense Pool – The defense pool shows a wide range of defense cards from which the players can choose. There are 24 cards in total. The details regarding each defense card can be found in our previous work [25, 24].

In the game event of the first design iteration, CAT was a part of a full-day CyberSecurity Challenges (CSC) event [13, 12]. The game engine was hosted in a docker container in a cloud environment, and the backend logged the player submissions and access. After the end of the event, data were downloaded from the cloud virtual machine instance, and then the instance was cleaned up.

4.2.2 Player-vs-environment game mode

The player-vs-environment (PvE) mode allows all game participants to address cloud security from the security or defense perspective. We defined six different scenarios from real-world hacking activities as described in the section 4.2.3. In game, all players build defense plans to stop the attack.

Note that the PvE mode allows more flexibility with little overhead - there is no limitation on the number of players, and actions from a game master are not required. Participants can join as single players or play in teams. Since the task is to defend themselves against pre-defined attack scenarios, players dedicate the time spent in the event to learn about how to be a good defender for their cloud assets instead of learning to be strategic hackers. We argue that this new mode is more efficient in raising awareness for cloud security than the baseline game prototype. This is in line with design decisions we took in the design of the CyberSecurity Challenges and we argue that such a defense-only perspective might be successful in optimizing the outcome for the players gain.

Table 2 The attack scenarios Scenario 1 (S1) – Scenario 6 (S6) used in iteration 1 and 2.

	Attack Action Card	Scenario						
		I1S1	I1S2	I1S3	I1S4	I1S5	I1S6	I2S6
Step 1: Initial Access	Exploit Public-Facing Application			x	x		x	
	Abuse Credential	x				x		
	Cloud Infrastructure Discovery	x	x			x		x
	Network Service Discovery		x		x			x
	Brute Force			x			x	
Step 2: Launch Attack	Abuse Trusted Relationship	x	x	x		x	x	x
	Cloud Storage Breach			x	x			x
	Account Manipulation	x					x	
	Exploit Unused Region							x
	Impair Defenses	x	x	x	x	x	x	
	Infrastructure Manipulation		x					
	Monitoring Escaping				x	x		
Step 3: Make Impact	Defacement	x					x	
	Resource Hijacking		x		x	x		x
	Denial of Service			x				

4.2.3 Attack scenarios

As mentioned above, the game includes six attack scenarios in the PvE game mode. In the first design iteration, we presented attack scenarios I1S1–6 as shown in Tab. 2. Each scenario consists of three attack steps: Initial Access, Launch Attack and Make Impact. That reflects the attack kill chain [2]. Each step in the kill chain uses different attack actions, each represented in an attack card. Each step may consist of several attack actions.

Players are instructed to defend their cloud assets against these kill chains. Their task is to defend themselves by selecting helpful defense cards and assigning the cards to the responsible organizational role.

I1S1–4 are based on the examples listed in MITRE ATT&CK Cloud Matrix [5]. For instance, I1S1 is derived from the hacking activity of threat group Lazarus Group [3] and Sandworm Team [3]. In the first step, to gain initial access, the attackers have two attack actions in parallel: Abuse Credential and Cloud infrastructure Discovery. Abuse Credential means the attacker tries to obtain and abuse account credentials to access the system [21]. "Cloud Infrastructure Discover" means the attackers discover resources that are available within the environment [21]. In the second step to launch the attack, the attackers have three attack actions in parallel: Abuse Trusted Relationship, Account Manipulation, and Impair Defense. Abuse Trusted Relationship means the attackers breach the organization to access the protected resource in the environment [21]. Account Manipulation refers to the attack that they manipulate the stolen account to open a backdoor and maintain access to victim systems [21]. In the meantime, Impair Defenses symbolizes that they maliciously modify the components of a victim environment in order to hinder defensive mechanisms [21]. In the last step, Make Impact, the attackers choose Defacement, which means they modify the homepage of the enterprise homepage to cause a panic and gain fame [21]. I1S5 is a collection of historically attackers' most-chosen cards from early trial runs of PvP mode. I1S6 is a collection of attack cards that can be defended by the least number of defense cards, which are supposed to be difficult to defend. The table 2 gives an overview of the pre-defined attack cards. Every scenario consists of 3 steps, and each step has 2, 3, or 1 card(s) chosen. In the table, "X" means this attack action card is chosen for the given scenario.

In all the scenarios, the players are required to build a complete defense plan from the beginning. The defense plan is assessed by the evaluator and a probability of withstanding the given attack scenario will be calculated. Players solve the challenge if the calculated probability is higher than 90%. Additionally, during the game time, a brief description of each scenario is distributed to the players. In the description, each attack action on the three attack steps are explained. The players can use the description as assistance material or background information.

4.2.4 Evaluation of first design iteration

As shown in table 1, we conducted the game event on January 26, 2022. In the game event, 17 participants formed four teams with 4 or 5 players per team. One player in each team shared the screen with other teammates and was in charge of submissions. Submissions were first discussed within the team and agreed upon by all the team members. The six scenarios of I1 were included in a full day CyberSecurity Challenge [13, 12] event as six challenges one after another. The teams were free to choose when to work on these challenges within the full day event. Therefore, we cannot precisely determine the exact game time. According to our observation, each team spent about 60 minutes on the six scenarios. We collected 175 valid submissions from the four teams over six scenarios. On average, each team makes 7.3 submissions per scenario. A submission was captured when player hit the “Submit” button. It included the defense cards the team has chosen in a certain scenario. Feedback from the players were collected and analyzed as evaluation of the first design iteration. The collected feedback and observation can be summarized as following:

- **S1:** Players enjoyed the game and found it helpful for understanding cloud security.
- **S2:** Players liked the interactive game as a hands-on exercise.
- **S3:** For some, it is challenging to build a full defense plan from scratch.
- **S4:** For some, the feedback of incorrectly assigned cards is not clear.
- **S5:** Some teams discovered some cards, e.g. “Account Management” was useful in all the scenarios and has an strong positive effect on the success rate.
- **S6:** All teams solved all scenarios in approximately one hour.

S1 and **S2** are positive feedback that implies the game logic is correct and the game itself is interesting and helpful for player. So we kept organizing game events and maintained the game logic in the second design iteration.

4.3 Second design iteration

We aim to improve our game artefact by addressing the issues exposed in the first design iteration. After adapting the game artefact, we conducted another game event to validate the improvement on March 15, 2022, as shown in table 1. In this iteration, the game event was a standalone game event following a full-day security awareness training. Recall, in the first design iteration, the cloud game was part of a full-day CyberSecurity Challenge. In this section, we introduce the changes we made and summarize the second design iteration (I2).

4.3.1 Design changes in second design iteration

To address the issues exposed in the first design iteration, we made the following changes in the second iteration:

- The first two scenarios were used as tutorials. We pre-selected cards on I1S1 and I1S2 and guided the players through the scenarios as a tutorial. This was meant to reduce difficulty as reflected in **S3**.

Table 3 Comparison of the presented scenarios in I1 and I2.

	Iteration 1 (I1)	Iteration 2 (I2)
I1S1	Full scenario	Tutorial scenario w. pre-selected cards
I1S2	Full scenario	Tutorial scenario w. pre-selected cards
I1S3	Full scenario, same for I1 and I2	
I1S4	Full scenario, threshold = 90%	Full scenario, threshold = 95%
I1S5	Full scenario, threshold = 90%	Full scenario, threshold = 95%
I1S6	Full scenario, only presented in I1	
I2S6	Full scenario, only presented in I2	

- We gave more detailed information to the players: We demonstrated in I1S1 that the success rate can be improved by covering more attack cards. In I1S2, we demonstrated that the success rate can be improved by correctly assigning a misplaced card to the proper role to cover **S4**.
- Transforming I1S1 and I2S2 into a tutorial reduced the difficulty of the game. We increased the success rate threshold to 95% from 90% for I1S4 and I1S5 to make the game more challenging. Note that **S6** implies that there is room for higher difficulty levels.
- As mentioned in **S5**, there are some overlaps in the attack scenarios. On one hand, repetition enhances learning. On the other hand, we could use the opportunity to show the importance of other defense mechanisms. So we decided to replace I1S6 with a new scenario I2S6 in which the defense card "Account Management" is not helpful. The last column of table 2 shows the exact attack actions in I2S6, which includes a new attack card, "Exploit Unused Region." That card means that the attacker creates cloud instances in new geographic service regions to evade detection [21]. Note that this type of attack is not covered in previous scenarios and it is an attack not often seen in practice.

Table 3 shows a summary of the differences in each scenario presented in iteration 1 (I1) and iteration 2 (I2).

4.3.2 Evaluation of second design iteration

Based on the feedback we collected in the first iteration, we made improvements in second design iteration. As shown in table 1, in the game event there were 14 participants, and everyone interacted with the platform as single players. The game was meant to deepen the understanding of cloud security topics covered in a "classic" training the day before the game.

Since the defense plans in the first two scenarios were partially pre-selected, we assigned 30 minutes for the players to solve all the six scenarios. We collected 656 valid submissions from the 14 participants over the six scenarios. On average, one player had 7.8 submissions on each scenario, slightly more than in Iteration 1. One of the reasons contributing to this might be that the single players cannot discuss with the teammates, so they sometimes choose the strategy to figure out the solution by trial and error.

As expected, with the help of the tutorials, we did not receive any feedback like **S3** or **S4** after the second game event. Even though we increased the threshold for I1S4 and I1S5, participants understood the tasks well and some managed to solve all the scenarios. Additionally, we continued to receive positive feedback as **S1** and **S2**. Some participants mentioned: "It would be nice to have more exercises like this one." and "Last exercise was quite good, quite interactive. The game was very good!". It seems interactive hands-on exercises are highly welcomed by the participants and add fun to the overall training experience. Also, the participants learned about the cloud security concept by building defense plans that are more solid and have better coverage. One of the participants shared the experience of reaching 99% of success rate for all six scenarios and spending quite some time trying to get 100%. It was not mentioned at the beginning that 100% security exists neither in the real world nor in the game. It was very well reflected in the game. Our lesson learned is that this needs to be better explained when introducing the game to the participants to avoid confusion.

5 Result and analysis

In the game event of both iterations, we captured the submissions of the teams and players. In this section, we will share our observations in the captured data.

5.1 Growth of success rate

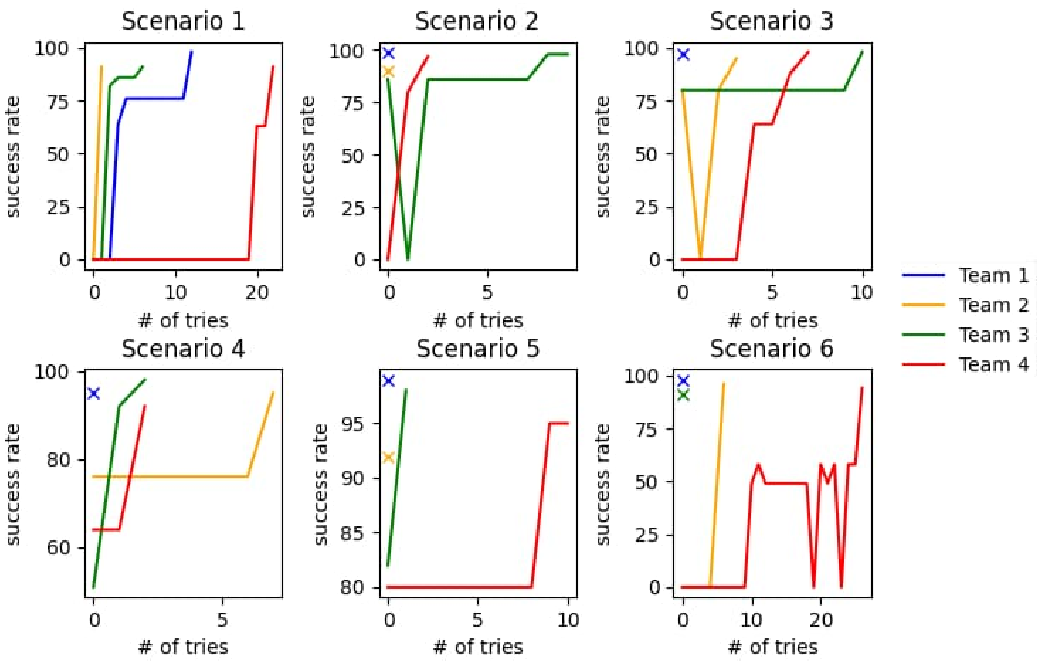
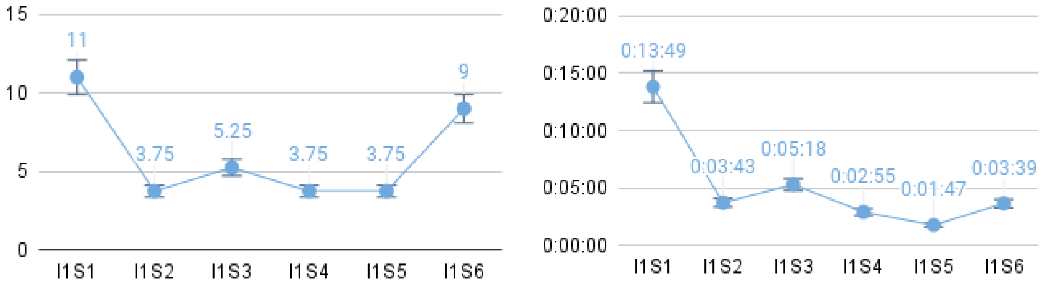


Figure 2 Success rate rising during gaming process per scenario.

In I1, all the teams are asked to build full defense plans for six attack scenarios. Figure 2 illustrates the growth of success rate across the submissions in six scenarios. The X-axis is the order of submission, and the Y-axis is the success rate of each submission. Despite some turbulence, the success rate increases as the team continues to try. The observed tendency in submission data shows that the game logic is understandable to the players. It implies that the participants learned from each submission and used the hint to improve their defense plan until the threshold was reached for them to solve the task. As in real life, 100% security does not exist. In our game, we set the threshold for a success defence to be 90%. The drops of success rate in scenario 2, 3 and 6 suggest that the teams could also make mistakes and weaken the defense plan, but finally every team manage to correct the mistakes and reach the threshold. The "x" symbol on the figure means that the team solved the task on the first try. We observed that Team 1 was having some quick success in solving the scenarios. It could be a sign that the difficulty level should be increased.

5.2 Average number of attempts and duration to complete each scenario



(a) Average submission numbers per scenarios.

(b) Time spent on each scenario.

Figure 3 Average data collected from trial runs.

Figure 3a illustrates the average number of attempts the teams made in six scenarios in I1. Teams made more attempts in I1S1 since it was the first scenario. As players became more familiar with the platform, the attempts number reduces in I1S2–5. We observe no significant difference among I1S2–5, since they are designed to be equally difficult. Besides, figure 3b presents the average time spent for each scenario, which shares the same tendency with figure on the left. In the last scenario I1S6, the teams made more attempts. However, if we compare it with right figure in 3a, there is no significant difference in the spent time. This might suggest the players entered the gaming mode, i.e. the players try to beat the game engine without considering the learning goal. We need to investigate further this observation and understand the reason behind it.

6 Conclusion and future work

In this paper, we presented CAT, an online board game with attack scenarios in different difficulty levels designed for industrial practitioners. We implemented and improved CAT in two iterations starting from a prototype, with a limited yet positive evaluation. Based on the feedback collected in the first iteration, we refined and validated the game in the second iteration. CAT provides an interactive and enjoyable way to convey critical concepts in cloud security. By engaging in attack scenarios derived from actual attacks, CAT enables a proactive thinking. Through building and strengthening a defense plan, the participants can gain a straightforward impression of cloud security roles and responsibilities and raise awareness about cloud security in the industry. In the future, we would like to collect further feedback for improvement in additional game events.

References

1 Cloud Security Alliance. Cloud controls matrix v4. https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/, 2021.

2 Michael J Assante and Robert M Lee. The industrial control system cyber kill chain. *SANS Institute InfoSec Reading Room*, 1, 2015.

3 MITRE ATT&CK. Hacking group. https://attack.mitre.org/groups/, May 2017.

4 MITRE ATT&CK. Techniques. https://attack.mitre.org/techniques/, May 2017.

5 MITRE ATT&CK. Mitre att&ck cloud matrix. https://attack.mitre.org/versions/v8/matrices/enterprise/cloud/, 2020.

6 Richard L. Baskerville and Jan Pries-Heje. Explanatory design theory. *Business & Information Systems Engineering*, 2:271–282, 2010. URL: https://aisel.aisnet.org/bise/vol2/iss5/2.

7 Ralf Dörner, Stefan Göbel, Wolfgang Effelsberg, and Josef Wiemeyer. *Serious Games: Foundations, Concepts and Practice*. Springer, 2016.

8 International Organization for Standardization. Iso/iec 27001 information security management. https://www.iso.org/isoiec-27001-information-security.html, 2017.

9 Sylvain Frey, Awais Rashid, Pauline Anthonysamy, Maria Pinto-Albuquerque, and Syed Asad Naqvi. The good, the bad and the ugly: a study of security decisions in a cyber-physical systems game. *IEEE Transactions on Software Engineering*, 2017.

10 Tiago Espinha Gasiba, Kristian Beckers, Santiago Suppan, and Filip Rezabek. On the requirements for serious games geared towards software developers in the industry. In *2019 IEEE 27th International Requirements Engineering Conference (RE)*, pages 286–296. IEEE, 2019.

11 Tiago Espinha Gasiba, Ulrike Lechner, and Maria Pinto-Albuquerque. Sifu-a cybersecurity awareness platform with challenge assessment and intelligent coach. *Cybersecurity*, 3(1):1–23, 2020.

12 Tiago Espinha Gasiba, Ulrike Lechner, and Maria Pinto-Albuquerque. Cybersecurity challenges for software developer awareness training in industrial environments. *Innovation Through Information Systems. WI 2021. Lecture Notes in Information Systems and Organisation*, 47, 2021. doi:https://doi.org/10.1007/978-3-030-86797-3_25.

13 Tiago Espinha Gasiba, Ulrike Lechner, and Maria Pinto-Albuquerque. 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*, February 2021.

14 Stephen Hart, Andrea Margheri, Federica Paci, and Vladimiro Sassone. Riskio: A serious game for cyber security awareness and education. *Computers & Security*, 95:101827, 2020. doi:10.1016/j.cose.2020.101827.

15 Alan Hevner. A three cycle view of design science research. *Scandinavian Journal of Information Systems*, 19:4, January 2007.

16 Alan Hevner, Salvatore March, and Jinsoo Park. Design science in information systems research. *Management Information Systems Quarterly*, 28:75–105, 2004.

17 IEEE. IEEE standard glossary of software engineering terminology. *IEEE Std 610.12-1990*, pages 1–84, 1990. doi:10.1109/IEEESTD.1990.101064.

18 ISO27002. Iso/iec 27002:2013information technology – security techniques – code of practice for information security controls. https://www.iso.org/standard/54533.html, 2013.

19 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.

20 ISO27018. Iso/iec 27018:2019information technology – security techniques – code of practice for protection of personally identifiable information (pii) in public clouds acting as pii processors. https://www.iso.org/standard/76559.html, 2019.

21 konva. Konva.js - html5 2d canvas js library for desktop and mobile applications. https://konvajs.org/, May 2022.

22 Kimberly Mlitz. Size of the cloud computing and hosting market market worldwide from 2010 to 2020 (in billion u.s. dollars). https://www.statista.com/statistics/500541/worldwide-hosting-and-cloud-computing-market/, January 2021. Accessed: 2021-05-08.

23 Adam Shostack. Tabletop security games & cards. https://https://shostack.org/games.html, 2021.

24 Tiange Zhao, Tiago Gasiba, Ulrike Lechner, and Maria Pinto-Albuquerque. Raising awareness about cloud security in industry through a board game. *Information*, 12(11), 2021. doi:10.3390/info12110482.

25 Tiange Zhao, Tiago Espinha Gasiba, Ulrike Lechner, and Maria Pinto-Albuquerque. Exploring a Board Game to Improve Cloud Security Training in Industry. In Pedro Rangel Henriques, Filipe Portela, Ricardo Queirós, and Alberto Simões, editors, *Second International Computer Programming Education Conference (ICPEC 2021)*, volume 91 of *Open Access Series in Informatics (OASIcs)*, pages 11:1–11:8, Dagstuhl, Germany, 2021. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. URL: https://drops.dagstuhl.de/opus/volltexte/2021/14227, doi:10.4230/OASIcs.ICPEC.2021.11.