CyberEscape Approach to Advancing Hard and Soft Skills in Cybersecurity Education

Rūta Pirta-Dreimane[1](✉), Agnė Brilingaitė[2], Evita Roponena[1], Karen Parish[3], Janis Grabis[1], Ricardo Gregorio Lugo[4], and Martiņš Bonders[1]

[1] Institute of Information Technology, Riga Technical University, Riga, Latvia
{Ruta.Pirta-Dreimane,Evita.Roponena,Grabis,Martins.Bonders}@rtu.lv

[2] Institute of Computer Science, Vilnius University, Vilnius, Lithuania
Agne.Brilingaite@mif.vu.lt

[3] Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Gjøvik, Norway
Karen.Parish@ntnu.no

[4] Faculty of Health, Welfare and Organisation, Østfold University College, Halden, Norway
Ricardo.G.Lugo@hiof.no

Abstract. Incorporating gamification elements and innovative approaches in training and educational programs are promising for addressing cybersecurity knowledge gaps. Cybersecurity training should consider a combination of hard and soft skills to deal with the diversity of cyber incidents. Therefore, this research aims to investigate if soft skills such as communication and collaboration enhances students' performance in practical task execution and if the CyberEscape approach promotes students engagement and self-efficacy.

This paper presents a cybersecurity game CyberEscape based on the intervention mapping methodology previously defined in the research. A virtualised infrastructure simulating the business environment works as a hybrid escape room. Physical resources and prepared information materials complement the game to support the scenario and ensure student engagement. The work employs a multiple-methods research approach. Participants filled out questionnaires in the pre-event and post-execution phases. Additionally, the participants were involved in small group semi-structured interviews. Results of the pilot study show a positive impact on student competence improvement and increased interest in cybersecurity.

Keywords: Cybersecurity education · Incident response · Incident management training · Crisis communication and collaboration · Gamification · Escape room design

D. D. Schmorrow and C. M. Fidopiastis (Eds.): HCII 2023, LNAI 14019, pp. 441–459, 2023.
https://doi.org/10.1007/978-3-031-35017-7_28

1 Introduction

Cyber crises require deep technical knowledge, but in addition general skills and behavioural traits are essential to ensure good team collaboration, responsibility distribution, and efficient work in problem-solving during incident management processes. Escape rooms have recently become popular in higher education as they provide an engaging way to develop students' competences [21]. Escape rooms have been used in group exercises to build critical thinking and problem-solving skills and to enhance students' communication and collaboration [12,26]. Incident management is a vital capability of companies, as it helps to ensure company readiness to respond to cyberthreats and minimise their negative impact effectively. Incident management processes might involve several roles, such as incident commander, incident responders, forensics investigators, communication leads and legal counsels. Technical expertise, communication, analytical, problem-solving, and collaboration skills are also essential in incident response. Behavioural aspects also play a significant role in incident management as the nature of incident response duties can be stressful and emotionally challenging [3]. Self-regulation and the ability to stay calm and focused can enhance the performance of cybersecurity specialists. Cybersecurity education programs must therefore consider the above dimensions to ensure specialists are prepared to handle incidents during cyber-attacks and ensure the continued operations of ICT systems.

This paper presents the CyberEscape approach to advancing hard and soft skills in cybersecurity education. The CyberEscape approach combines student-centred education methods, such as gamification [33], problem-based learning [19] and flipped classroom principles [14]. This pilot study applies the CyberEscape approach for IT bachelor level students. It considers crisis communication and crisis collaboration along with technical competences in incident management scenarios. In planning the education program, the design science problem-solving method [18] is used which enables multi-perspective examination of the problem and solution design. The pilot study is designed using the ADVANCES methodology [29] applying the competence model, course design process, and learning & training environment design. A wide range of on-site and online tools are used in the pilot study. The virtual laboratory and incident management tools promote students' hard skills. The collaboration tools support teamwork. The on-site environment is enriched with different game elements, such as Lego figures and posters, to promote student engagement.

The main objectives of the study are: (1) to investigate if communication, collaboration and team dynamics enhances students' performance in practical task execution and (2) to evaluate if the CyberEscape approach promotes students engagement and self-efficacy.

The paper is structured as follows. Section 2 reviews related work as a research background, and Sect. 3 presents the research methodology. The CyberEscape design, including competences, scenario, and setup environment, are presented in Sect. 4, and pilot study results are covered in Sect. 5. Section 6 provides conclusions and future research directions.

2 Background

In recent years, several studies using gamification methods for cybersecurity education and training have grown as these methods show positive outcomes. Cybersecurity-related tasks are adaptable for gamification that helps to engage students, develop interest in cybersecurity, and motivate them to solve tasks [27].

Various gamified educational tools are available online for cybersecurity training, for example, Cyber Threat Defender, CyberCIEGE, Cyber Protect, and Network Defense Training Game (NDTG). In the digitalized table-top card game Cyber Threat Defender, players can defend their assets and attack their opponents within the time limit [4]. CyberCIEGE [34] is another game-based training tool, but it is a 3D simulation of an office space where a player can interact with virtual employees while implementing security policies. The game provides different scenarios with multiple solutions and functionality to monitor the players' progress. Cyber Protect [11] encourages players to purchase and deploy tools for network protection against attackers. The NDTG [1] cybersecurity training platform includes cybersecurity scenarios in which players must defend the network. Most of these tools require technical knowledge to play. We drew inspiration from these different tools to develop our own approach.

Malone et al. [23] presented the framework Riposte, a browser-based game applicable to cybersecurity education. The framework enables the development of tasks with progressive difficulty and uses two styles of play: player versus player (PvP) and player versus environment (PvE). However, it is executed in the online environment with no possibility of observing team dynamics or improving students' soft skills. The study also highlighted that students interested in gamification before the case study achieved better learning outcomes.

Cybersecurity training often includes Capture the Flag (CTF) exercises. However, due to the informal nature of the CTF, it is challenging to map the competences defined by security experts [35]. In the jeopardy CTFs, the most common format, the player chooses the challenges with different point values from provided categories. The CyberEscape integrates a similar approach. Švábenský et al. [35] concluded that CTFs games mainly improve data and network security knowledge. However, technical competences are not enough for the player in real life cybersecurity challenges, where team collaboration and a calm mind during stressful situations are as important as technical knowledge.

The escape room game format has been introduced previously for educational gamification. The escapeED framework [7] provides a development methodology and highlights six core elements of an educational escape room: participants, objectives, theme, puzzles, equipment, and evaluation. The participant-centred escape room has objectives, defined as expected outcomes, within some theme as a context. Participants complete puzzles associated with the theme, and the equipment creates the room environment. The evaluation explains how the participants performed the puzzle-related tasks according to the objectives. These six core elements were also used to create the CyberEscape game setup.

Debello et al. [9] describe how they transformed their usual Cybersecurity study courses into gamified exercises proposing them as Escape the Classroom tasks. The task setup was changed compared to the traditional approach used in their university, as they proposed a strategy allowing students to compete with each other within the given time limit.

Virtual escape rooms are a popular approach for cybersecurity education. The CySecEscape 2.0. [22] virtual escape room created based on a physical escape room has gained mainly positive feedback from the participants. It includes puzzles addressing different topics, e.g., password hygiene, source code security, phishing, and identity theft. The ARI 3D [10] virtual escape room consists of a tutorial and three game levels including different tasks designed as mini-games, e.g., bad practices, password security, Internet fraud, and network security. The focus of both escape rooms is on improving cybersecurity awareness and not mimicking a real-life cybersecurity environment. These virtual and individually played games do not allow tracking the change in soft skill development.

The escape rooms can also improve information privacy competences. For example, Papaioannou et al. [28] developed an exciting scenario where the guardian angel helps the player with tasks. However, it has a dark end (the suicide of the main character) and this could be psychologically harmful to some players.

Beguin et al. [2] designed two on-site escape rooms—for the defense scenario (participants try to mitigate the vulnerabilities found in the room) and the attack scenario(participants play the hacker role and try to steal information). The students accepted this approach positively and stated that it improved their knowledge more than the same-length lecture could. However, there needs to be evidence of how useful the approach is for cybersecurity education. Another study [25] focuses on the deciphering and cybersecurity-unrelated tasks in the on-site escape room game. However, the researchers could not conclude whether the game engaged the participants' interests in cybersecurity.

The reviewed studies highlighted the importance of defining game objectives, understanding participant needs, and designing evaluation strategies in educational game development. The game should consider the time required to solve the tasks, needed tools, and background information.

Most reviewed studies on gamification applications in cybersecurity training described the design of virtual games played individually or in a team. The main advantage of this approach is that players can be in a different room, in the same room, or a specific place while participating in the game. However, this feature leads to the main disadvantage of virtual educational games—it is complicated to evaluate the player's soft skills essential for competent cybersecurity specialists.

All reviewed studies mainly focus on cyberthreat detection or mitigation. We contribute to the development of the field by adding additional incident management steps. In addition, we focus not only on the technical skill development, but also soft skills and collaboration. In this way we provide scenario training by mimicking a simplified cybersecurity work environment where the participant identifies the possible incidents in the fictional company and also learns how to classify and report them correctly.

3 Methodology

In planning the CyberEscape game, the work used the design science problem-solving method [18]. It is a systematic approach, connecting practical problems with domain-specific solutions by conducting multiple studies. The investigated challenge is integrating multi-dimensional areas in the education programs for better human performance in cyberspace [30].

Design science research seeks to enhance human knowledge by creating innovative artifacts: construct (chooses language for problem and solution definition and communication), model (uses constructs to represent a real-world problem and its solution), method (defines processes and provides guidance on how to solve problems), and instantiation (shows how the construct, models or methods can be implemented in a working system) [18].

The design science research process consists of three cycles to create one or many of the previously listed artifact types: relevance cycle, design cycle, and rigor cycle [17]. The relevance cycle usually starts with the design science research using the environment context. It provides research requirements to improve the knowledge base and solve the research problem. The design cycle includes artifact development and evaluation.

As part of the evaluation process we employ a social science research methodology with a multiple-methods approach that includes both post-positivistic and social constructionist constructs in the research design [20]. This approach to research design has the purpose of expanding the scope of the study as both quantitative and qualitative methods are used to explore the research objectives [15]. The first and second research objectives were addressed using a quantitative approach to measuring the students' performance, communication, collaboration, group dynamics self-efficacy and motivation. The participants completed the questionnaires during the pre-work and post-work phases of the teaching session.

In addition, to address the second objective, the research team adopted a qualitative approach using semi-structured group interviews to focus on the following: the student experiences of engagement during the practical CyberEscape, the student's perceptions of how the pre-exercise training (flipped learning approach) enhanced their self-efficacy. The design science framework was adapted from [18] to conduct the study (see Fig. 1). This study is the first design cycle of planned research aiming to evaluate the overall approach and find the improvements for the next design cycle. The intention is to determine if there is a need to repeat the relevance cycle. The rigor cycle supports the research with prior knowledge and ensures that the solution is innovative. Each cycle can be repeated several times if it is needed to achieve the best results.

Interviews with participants were conducted according to the established Code of Ethics for students, academic and administrative personnel of Riga Technical university (RTU) and the Code of Ethics of scientists published by the Charter of Latvian Academy of Sciences. All ethical principles were assured, and students' consent was collected as part of the registration form. The signs of ongoing photography were posted in the event area. All participants had the possibility to leave the game and stop the interviews at any time.

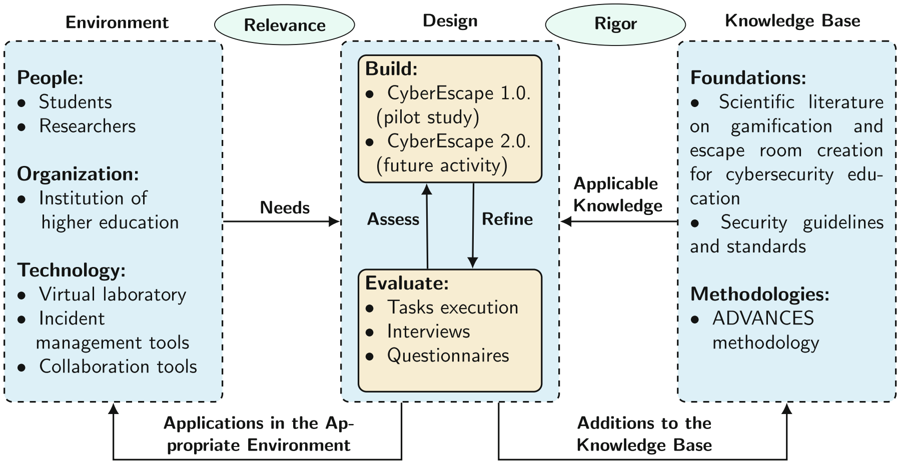

Environment
Relevance
Design
Rigor
Knowledge Base
People:
• Students
• Researchers
Organization:
• Institution of higher education
Technology:
• Virtual laboratory
• Incident management tools
• Collaboration tools
Needs
Build:
• CyberEscape 1.0. (pilot study)
• CyberEscape 2.0. (future activity)
Assess
Refine
Evaluate:
• Tasks execution
• Interviews
• Questionnaires
Applicable Knowledge
Foundations:
• Scientific literature on gamification and escape room creation for cybersecurity education
• Security guidelines and standards
Methodologies:
• ADVANCES methodology
Applications in the Appropriate Environment
Additions to the Knowledge Base

Fig. 1. Design science approach for CyberEscape (adapted from [18])

Figure 1 presents the environment, design and knowledge base of the CyberEscape approach. The knowledge base used to create the CyberEscape game are formed from the related literature on applications of the gamification for the cybersecurity education (see Sect. 2), security guidelines, standards [6,13], and ADVANCES methodology [29] guidelines. ADVANCES methodology is the foundation of the game design. It suggests to integrate different dimensions of cybersecurity competences into the education programs, considering the needs of study program participants, the context of real live cybersecurity scenarios, the associated work roles and tasks.

4 CyberEscape Design

In the game scenario design, the ADVANCES methodology [29] is applied as guidelines for the competence model, course design process, and learning and training environment design.

4.1 Competence Model

The core of the competence model is the work role *Cyber Incident Responder* defined by the European Union Agency for Cybersecurity (ENISA). Cyber Incident Responder [13] has duties to “monitor the organisation’s cybersecurity state, handle incidents during cyber-attacks and assure the continued operations of ICT systems". The role has several tasks, such as: (1) Identify, analyse, mitigate and communicate cybersecurity incidents, (2) Assess and manage technical vulnerabilities, (3) Document incident results analysis and incident handling actions, (4) Cooperate with Secure Operation Centres (SOCs) and Computer Security Incident Response Teams (CSIRTs), and (5) Cooperate with key personnel for reporting of security incidents according to applicable legal framework. A wide set of competences are required for effective defined tasks execution (see Fig. 2).

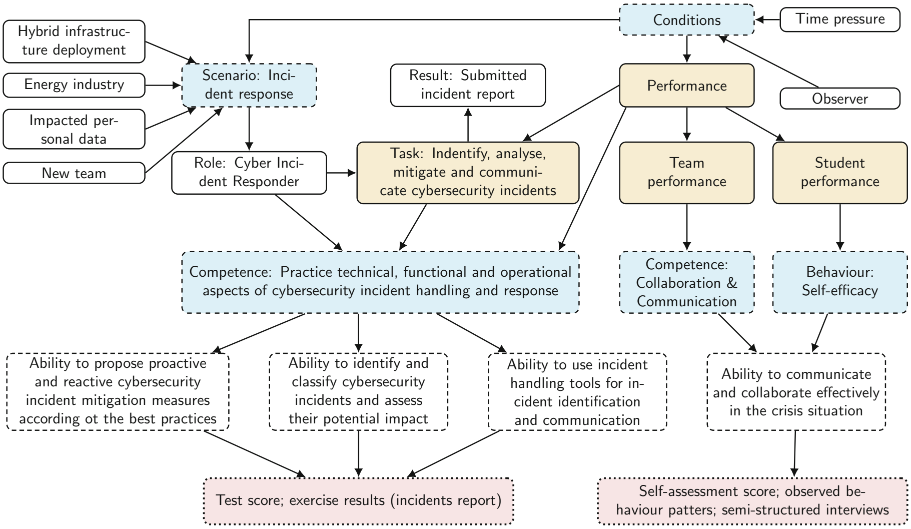

Conditions
Time pressure
Hybrid infrastructure deployment
Energy industry
Impacted personal data
New team
Scenario: Incident response
Result: Submitted incident report
Performance
Observer
Role: Cyber Incident Responder
Task: Indentify, analyse, mitigate and communicate cybersecurity incidents
Team performance
Student performance
Competence: Practice technical, functional and operational aspects of cybersecurity incident handling and response
Competence: Collaboration & Communication
Behaviour: Self-efficacy
Ability to propose proactive and reactive cybersecurity incident mitigation measures according ot the best practices
Ability to identify and classify cybersecurity incidents and assess their potential impact
Ability to use incident handling tools for incident identification and communication
Ability to communicate and collaborate effectively in the crisis situation
Test score; exercise results (incidents report)
Self-assessment score; observed behaviour patters; semi-structured interviews

Fig. 2. CyberEscape competence model (a fragment)

The competence model of the learning scenario is prepared following the recommendations of the ADVANCES methodology [29], integrating hard and soft skills and expected behavior.

The ENISA defines main technical and operational competences, such as: (1) Technical, functional and operational aspects of cybersecurity incident handling and response; (2) Work on operating systems, servers, clouds and relevant infrastructures; (3) Incident handling communication procedures; (4) Computing networks and operating systems security, and (4) Incident handling recommendations and best practices.

Psychology experts and related industry and research studies [5,32] distinguish vital soft competences to promote specialist performance in the incident response: (1) Teamwork (collaboration); (2) Communication, presentation and reporting and (3) Working under pressure. Incident management can elicit a wide range of emotions, and cognitive and behavioral changes, such as increased stress levels and difficulty concentrating. Thus, not only individual competences, but also behavioral aspects play a significant role in effective task execution.

Self-regulation, confidence and adaptability may raise individual performance in crisis situations.

The hard and soft skills and expected behavior are the basis for learning outcomes of the scenario: (1) Ability to identify and classify cybersecurity incidents and assess their potential impact; (2) Ability to proactively and reactively mitigate cybersecurity incidents; (3) Ability to communicate confidently; (4) Ability to use incident handling tools for incidents identification, analysis, mitigation and communication; (5) Ability to collaborate effectively in a critical situation.

4.2 Game Scenario Overview

The learning scenario reflects the lifecycle of the information security incident management based on National Institute of Standards and Technology (NIST) incident handling recommendations [6]. The NIST suggests four interconnected incident management stages: (1) preparation for an incident, (2) detection and analysis of an incident, (3) incident discovery and recovery, and (4) post-incident analysis. The students take the role of Computer Security Incident Response Team (CSIRT) in a fictional mid-size energy sector company, and they must perform specific tasks across information security incident management lifestyle (see Fig. 3).

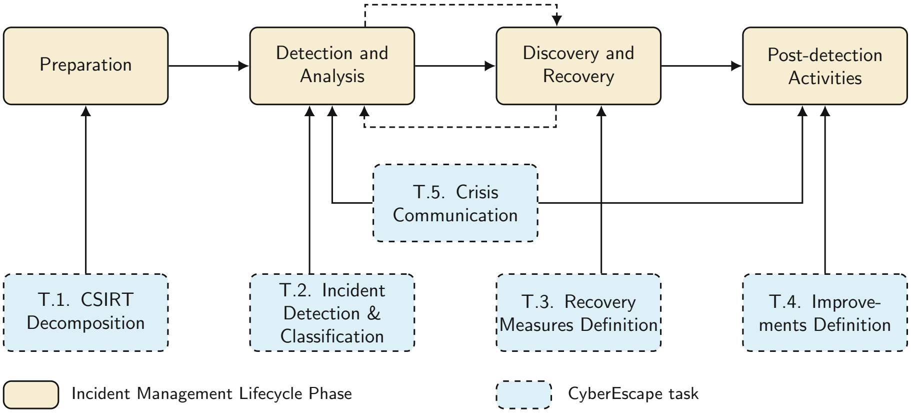

Preparation
Detection and Analysis
Discovery and Recovery
Post-detection Activities
T.5. Crisis Communication
T.1. CSIRT Decomposition
T.2. Incident Detection & Classification
T.3. Recovery Measures Definition
T.4. Improvements Definition
Incident Management Lifecycle Phase
CyberEscape task

Fig. 3. CyberEscape tasks

Preparation for the incident requires creating an incident management policy, incident handling procedures, communication plan, team structure and acquiring the necessary resources and tools. The first task of the students (T.1.) is to formalize their roles and responsibilities to ensure the CSIRT function in the fictional company. The hybrid exercise incorporates both table-top exercises and virtual exercises that require definition of roles and responsibilities, taking into consideration the team size.

According to NIST [6], incident detection and analysis include 1) the definition of possible attack vectors, 2) incident detection using various sources, such as security software alerts, people, and logs, 3) incident analysis and validation, 4) incident documentation, 5) incident prioritisation, and 6) incident notification. Based on NIST the second task of the students (T.2.) is therefore to identify three incidents placed in a room: logical incident, physical incident, and organizational incident, and to classify them by specifying the incident name, short description, type (logical, physical, or organizational), category (incident subtype) and its impact (low, medium, high, or critical). The students used video materials to learn how to correctly fill out the provided incident classification table.

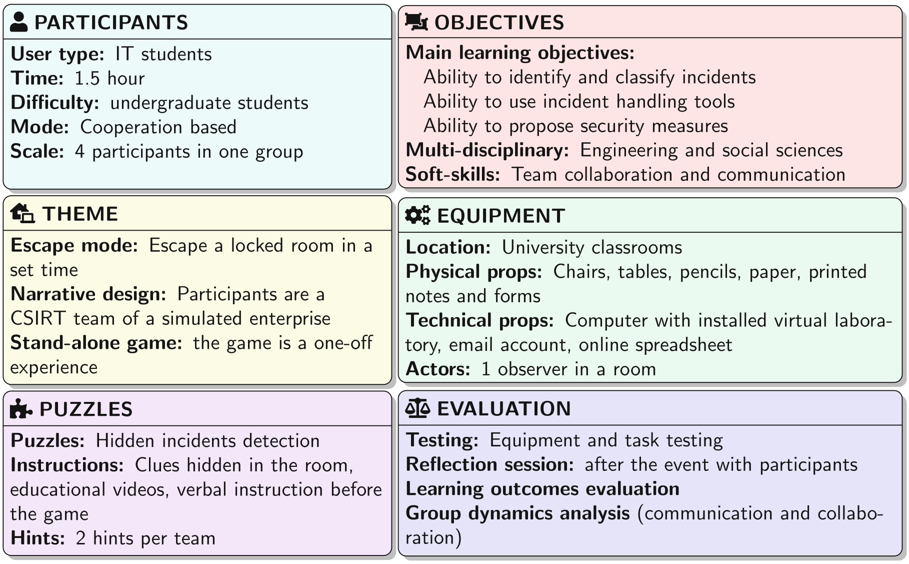
The third incident management stage is incident discovery and recovery. The phase includes incident containment, evidence gathering and recovery, and post-activities to gather incident knowledge and data to prevent those threats in the future. The third task of the students (T.3.) is to define the vulnerabilities that lead to the incident and to describe the immediate incident prevention actions. The fourth task (T.4.) is to describe actions to minimize identified vulnerability in the future, and it is associated with the last phase of the incident management life-cycle, i.e., post detection activities.

Crisis communication is an essential part of incident management, and it is integrated in several incident management life-cycle phases. The incident communication plan and communication channels (e.g., email, website, phone call, in person) are defined in the incident preparation phase to help CSIRT report the incidents to the appropriate roles such as CIO, head of information security, system owner, and others. The actual crisis communication is ongoing through incident detection and analysis, discovery and recovery and post-incident phases. The last task for the students (T.5.) is to create an incident report, choose appropriate communication channel, and report recipients.

4.3 Physical and Digital Environment

The game was executed in physical rooms and participants used a computer to access the virtual laboratory and office tools (e-mail, online collaboration tools). Students were asked to watch 5 learning videos before the practical tasks execution. Also, supplementary training materials were placed on the E-learning system. Printed instructions and a Lego corner (see Fig. 4) also provide the necessary game puzzle parts. Each group of students was located in a separate room in one geographical location and monitored by an observer.

The students were presented with a fictional company *Jurpils HES* (Jurpils Hydroelectric Power Plant) that contained a hydropower plant, a customer service shop, and a website. The fictional company maintains its ICCT services and is not relying on third-parties. The students received tasks and clues in the form of notes or emails from different employees in the company, e.g., the IT department manager, HR, communication department manager, and IT support. The main goal for each students team was to find hidden clues and use their knowledge to solve all tasks. Each team had an email address created for



PARTICIPANTS

User type: IT students
Time: 1.5 hour
Difficulty: undergraduate students
Mode: Cooperation based
Scale: 4 participants in one group

OBJECTIVES

Main learning objectives:
Ability to identify and classify incidents
Ability to use incident handling tools
Ability to propose security measures
Multi-disciplinary: Engineering and social sciences
Soft-skills: Team collaboration and communication

THEME

Escape mode: Escape a locked room in a set time
Narrative design: Participants are a CSIRT team of a simulated enterprise
Stand-alone game: the game is a one-off experience

EQUIPMENT

Location: University classrooms
Physical props: Chairs, tables, pencils, paper, printed notes and forms
Technical props: Computer with installed virtual laboratory, email account, online spreadsheet
Actors: 1 observer in a room

PUZZLES

Puzzles: Hidden incidents detection
Instructions: Clues hidden in the room, educational videos, verbal instruction before the game
Hints: 2 hints per team

EVALUATION

Testing: Equipment and task testing
Reflection session: after the event with participants
Learning outcomes evaluation
Group dynamics analysis (communication and collaboration)

Fig. 4. CyberEscape game setup (adapted from [7])

event purposes and was used to send additional information. Table 1 contains a brief description of the hidden incidents of the CyberEscape.

Table 1. Description of the hidden incidents

Incident name	Incident type	Identification source
Denial of service attack	Logical	Network log file analysis, situation description
Data loss (natural disaster)	Physical	Physical company model, situation description
Phishing	Organizational	Spam email, situation description

The provided notes contain the situation description but are insufficient to identify the incidents listed in Table 1. Therefore, participants needed additional sources to validate if the incident is an actual incident. They had to reconstruct the physical company model using Lego pieces hidden in the room to determine that the company data storage and server room are in a flooded river area.

The spam email contained a form asking the receiver to fill in the sensitive data and was sent to each team. The organizers intended to see if anyone filled it out and planed to use it to initiate the scenario of the phishing campaign.

The students were offered the opportunity to use the Wireshark tool for network log analysis of the *Jurpils HES* website in the virtual laboratory to identify a Denial-of-Service (DoS) attack. This incident required performing an additional task to decrypt a password using a hidden key for the virtual machine.

The virtual laboratory was a central component of the CyberEscape game. Virtualization technologies enabled the development of a controlled environment to simulate DoS attacks safely. Moreover, this environment could be easily scaled according to the number of students. The CyberEscape utilized bare metal virtualization and nested virtualization technologies (see Fig 5). Bare metal virtualization uses the open-source Proxmox Virtual Environment (Proxmox VE) as a hypervisor based on the KVM hypervisor and Linux containers (LXC). Proxmox VE supports all the infrastructure necessary for DoS simulation, e.g. virtual machines, containers, virtual networks, network rate limit, and centralized management of DoS scripts. The DoS attack was performed against the fictional company environment developed using nested virtualization. Each student group had an Ubuntu Desktop 22.04 virtual machine with the Apache web server deployed in a dedicated nested Proxmox VE hypervisor. Any remote communication with the virtual machine was lost during a DoS attack, and services like VNC, SSH were unavailable. Therefore, nested virtualization enabled direct connection to the virtual machine from the Proxmox VE hypervisor console.

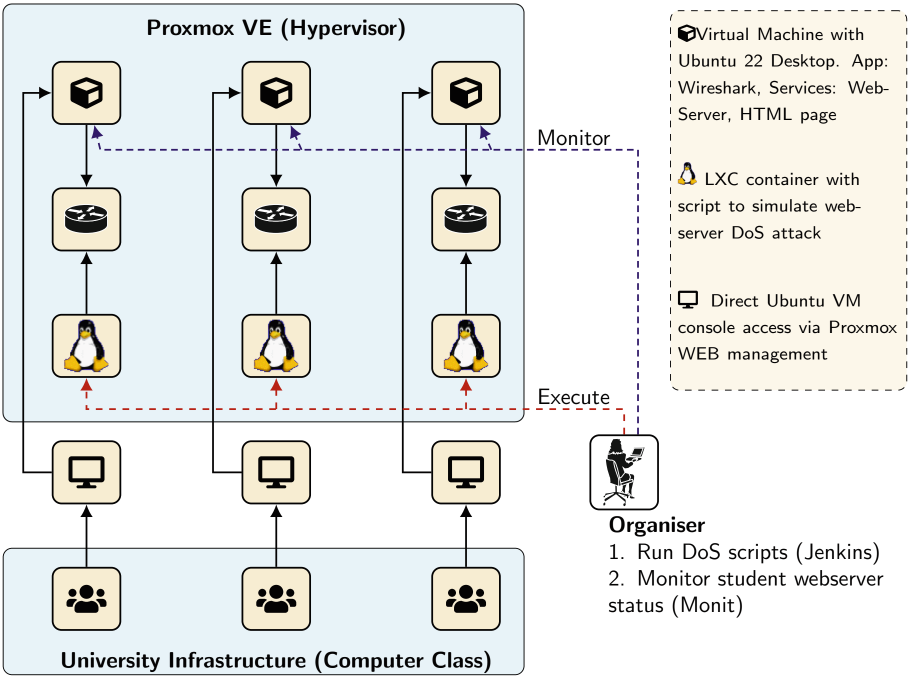

Proxmox VE (Hypervisor)
Monitor
Execute
University Infrastructure (Computer Class)
Virtual Machine with Ubuntu 22 Desktop. App: Wireshark, Services: Web-Server, HTML page
LXC container with script to simulate web-server DoS attack
Direct Ubuntu VM console access via Proxmox WEB management
Organiser
1. Run DoS scripts (Jenkins)
2. Monitor student webserver status (Monit)

Fig. 5. Virtual laboratory architecture

CyberEscape participants were able to trace and analyze this DoS attack using the network protocol analyzer Wireshark. They were expected to block the attack using a virtual machine hypervisor firewall that simulates the company's main firewall in real life. DoS scripts were executed from specially created LXC containers. Each LXC container attacked the specified hypervisor and the Ubuntu Apache Web server.

The organizers managed the DoS attack from a separate virtual machine with the open-source automation server Jenkins installed. Using Jenkins, for each student group, it was possible to configure individual automatically executed scripts to perform different scenarios and set attack parameters, e.g. at specific and predefined time intervals.

The Hping3 network tool was used to simulate web server SYN Flood Attack—the most common and effective way to attack a Web server and make its services unavailable. The attack also made the entire virtual machine network adapter and all protocols unavailable. The open-source process supervision tool Monit enabled monitoring of the progress of the attack and the effectiveness of blocking.

The architecture is a completely isolated environment and could not harm the external infrastructure of the university. Users could access it from any place via the Internet, and the attack automatization enabled implementation of dynamic scenarios.

4.4 Evaluation Approach

Evaluation incorporates three key aspects: Students' competence evaluation, Students' behavior evaluation, and Training approach and content evaluation. The evaluation methodology is presented in Table 2.

Table 2. Evaluation methodology

Evaluation Goal	Learning Outcome/Evaluation Criteria	Measurement
Students competence	To identify and classify cybersecurity incidents	T.2. results (detected and classified incidents)
	To reactively mitigate cybersecurity incidents	T.3. results (identified incident reaction measures)
	To proactively mitigate cybersecurity incidents	T.4. results (identified improvement measures)
	To communicate confidently in a crisis situation	T.5. results (prepared crisis communication message)
	To use incident handling tools	T.2. results (infrastructure monitoring tool usage)
Students behavior	To collaborate effectively in a crisis situation	T.1. results (team structure), TWLQ results & Group interaction observation
Training approach	Engagement increase	Students feedback results
	Competence increase	Students feedback results

Students' competences are evaluated by considering execution results of the practical tasks and self-assessment before and after the CyberEscape game. Students' behavior is evaluated by team assessment that help to identify factors that may influence communication and performance both at the individual and team level. The Team Workload Questionnaire (TWLQ) [31] was used to measure workload demands in the teams. The TWLQ Items are scored on an 11-point Likert scale (range: very low - very high) with higher scores indicating higher levels of subjective workload. The TWLQ has two dimensions, the Teamwork component (communication, coordination, team performance monitoring) and Task-Team component (time-share, team emotion, team support). The TWLQ shows good reliability on all subscales (Cronbach's a ¿.70) and also for this research (Teamwork Cronbach's $a = .673$; Task-team Cronbach's $a = .626$). Statistical analysis was done with JASP version .16.1. All variables were not normally distributed, therefore non-parametric analyses are used. Alpha levels for hypothesis testing were set at the 0.05 level. A multiple linear regression was computed with the TWLQ entered as predictors and the score of the teams as the dependent variable. For the training approach and content evaluation students feedback results were captured (questionnaire, interviews).

5 CyberEscape Delivery Results

The CyberEscape game event was organized for bachelor students from different study levels (1st-3rd year). They were invited to participate and compete in the CyberEscape. Five groups of students applied with four students in each.

The study included a quantitative and qualitative assessment according to the evaluation methodology presented in Table 2.

5.1 Objective 1: Communication, Collaboration and Group Dynamics

In the interviews, CyberEscape participants reflected that team collaboration is a critical success factor in the incident reaction and overall the game have increased relevant competences. Meanwhile, the longer team cooperation experience is required to work effectively as a team.

Students demonstrated the ability to solve practical tasks. The average tasks completion score was 60%, the best result was 80% of total 100%. The result is perceived as good, given the students' low competences level in IT incident management prior to the assignment, as well as the limited time of the task execution (1.5 h for all five tasks).

Students self-assessment showed improvement in all competences included in the learning scenario (see Fig. 6). Meanwhile, the competence level still is improvable, as the CyberEscape was a "stand-alone" game and the students' previous knowledge level in cybersecurity was low.

CyberEscape was most helpful in improving the following knowledge: (1) Incident reaction roles and (2) Incident handling tools. Incident reaction roles

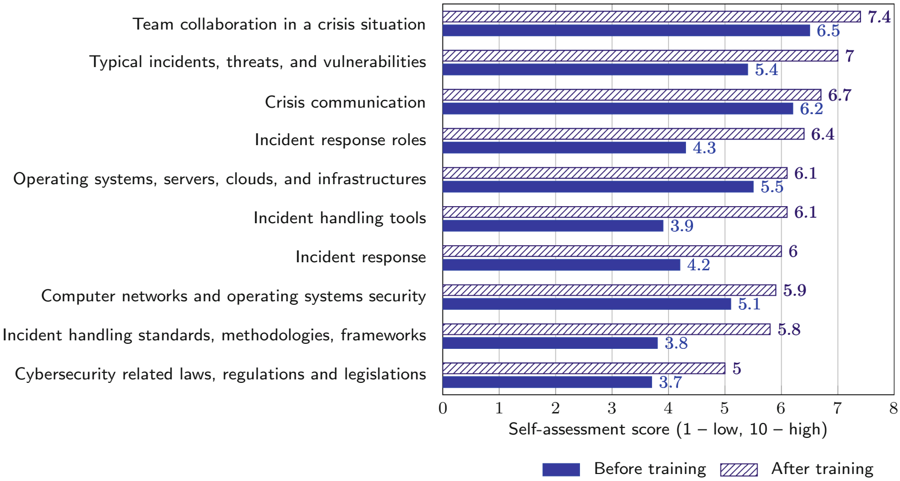


Fig. 6. Student competences self-assessment

were presented in the learning video, supplemented by the NIST Incident management guide [6], that recommended the structure of the team. The incident management team setup was integrated also in the practical task (T.1). Incident handling tools were used in the practical tasks as part of the virtual laboratory (T.2, T.3).

CyberEscape was less helpful in improving the following knowledge: (1) Crisis communication and (2) Operating systems, servers, clouds and infrastructures. Crisis communication recommendations were included in the learning video, supplemented by the A Guide to Effective Incident Management Communications [24]. Crisis communication was integrated also in the practical task (T.5). However, it is important to note that students rated their ability to communicate effectively in a crisis situation relatively highly before the training, although they admitted in interviews that they had not put these skills into practice. The slight increase in competence may therefore be due to an overly high initial assessment. Operating systems, servers, clouds and infrastructures was assumed as prerequisite of the training, no additional learning materials were provided. In order to complete the tasks, coordinated collaboration within the team is required. Each team nominated a leader, mostly servant-leadership style was observed what is one of the suggested leadership styles in the cybersecurity [8]. Still the observations showed that the coordination of the tasks can be improved for effective tasks execution. Teams with previous experience of working together demonstrated more efficient execution of tasks what is a common pattern in teams collaboration. This indicates the importance of teamwork requiring exercises in the cybersecurity education.

The TWLQ results showed that participants rated their team collaboration as good (8.6 of 10 points). Also the communication effectiveness was rated as good (8 points). However the teams have faced some difficulties, such as time share demand, e.g., share and manage time between task-work (work done individually) and team-work (work done as a team). Descriptive statistics and correlations (ρ) for the outcome score and workload items can be found in Table 3.

Table 3. Descriptive statistics and correlations (ρ)

Score	Mean	SD	1	2	3	4	5	6	7
Communication Demand	31.98	21.15	–						
Coordination Demand	8.00	1.92	.125	–					
Team Performance	6.32	2.50	$.527^{*}$	$.519^{*}$	–				
Monitoring Demand	4.11	2.58	.274	.311	$.480^{*}$				
Time Share Demand	5.79	3.14	$.581^{*}$	.033	$.520^{*}$	.450	–		
Team Support	4.37	3.22	.147	$-.170$	.096	.300	$.519^{*}$	–	
Team Emotion Demand	3.05	2.97	.366	.423	.346	.330	$.605^{**}$	.253	–

$^{*}p < .05,^{**} p < .01,^{***} p < 0.001$

To see the influence of team workloads on performance, hierarchical multiple regressions were performed where Team Workloads were entered in the first step and Task-team workloads entered in the second step. Team workloads (Communication $\beta = -.096$, Cooperation $\beta = .480$, Team Performance Monitoring $\beta = .445$) could positively predict team performance in the exercise ($R^2 = .487$, $F = 4.11$, $p = .030$) but task-team workloads factors (team support $\beta = .241$, team emotional demand $\beta = -.291$, timeshare demands $\beta = .311$) were not significant in influencing performance ($\Delta R^2 = .172$, $F = 1.69$, $p = .233$).

5.2 Objective 2: Engagement and Self-efficacy

When evaluating if the CyberEscape approach promotes student engagement and self-efficacy, the results from the questionnaires reveal that student engagement in the CyberEscape was high. Nearly 90% of students stated that the CyberEscape game had increased their interest in cybersecurity. This result is supported by the interview data where students stated that they were interested in similar games in the future and enquired about further education possibilities to study cybersecurity. All student groups admitted that the game was interesting and had a good atmosphere. In addition, students reported increased self-efficacy and rated the CyberEscape higher than the theoretical videos. 88.8% of students agreed that the CyberEscape had increased their knowledge of IT incident management. Meanwhile, the importance of the videos was acknowledged by 61.3% of students to be helpful. In the interviews, students suggested that the videos should include more technical tutorials, as currently the main focus was on operational, leadership and general competences [16] related knowledge units. However, the flipped learning approach was evaluated positively. Students suggested that the including subtitles and English terms in the videos would increase their perception. Students also mentioned that they found the phishing incident distracting from other tasks because of the spam email. However, it was one of their tasks and was included to show possible situations of real life. Moreover, one group stated that they preferred traditional task presentation over the more active CyberEscape game approach. They may prefer to have a more passive approach, however, further investigation is needed to explore why.

6 Conclusions and Future Work

The main objectives of the study were: (1) to investigate if communication, collaboration and team dynamics enhances students' performance in practical task execution; (2) to evaluate if the CyberEscape approach promotes students engagement and self-efficacy. Using an escape room approach to gamification in cybersecurity education promotes field-specific competence development, integrating hard and soft skills. The approach stimulates creative and critical thinking and requires efficient communication and collaboration in solving complex cyber puzzles and tasks. An Escape room is a fun activity keeping high student engagement. Meantime, the approach has several limitations and challenges. The escape room setup is time-consuming and requires human and specific technical resources. More importantly, the gamification scenario might unbalance the distribution of hard and soft skills within a small participant group. Therefore, it cannot ensure comparable personal development in all cybersecurity knowledge areas compared to traditional learning methods.

In the future, we plan to develop an upgrade for the game, CyberEscape 2.0. The lessons learned and knowledge acquired from the CyberEscape 1.0 delivery will be used as a basis for further development. A new version could include the following key improvements: extensive technical tutorials about computer and operating system protection, enhanced video material for training, and learning analytics components powered by computer vision and data science.

The long-term vision is to create an internationally reusable program for running an educational escape room game. It will enhance cybersecurity capabilities and attract young specialists as the world experiences increasing cybersecurity threats and a vast demand for cybersecurity professionals.

We also have identified the need for further investigation as to the students perceptions of active learning approaches such as CyberEscape.

Acknowledgements. The "Advancing Human Performance in Cybersecurity", ADVANCES, benefits from nearly €1 million grant from Iceland, Liechtenstein and Norway through the EEA Grants. The aim of the project is to advance the performance of cybersecurity specialists by personalizing the competence development path and risk assessment. Project contract with the Research Council of Lithuania (LMTLT) No is S-BMT-21-6 (LT08-2-LMT-K-01-051).

References

1. Ashley, T.D., Kwon, R., Gourisetti, S.N.G., Katsis, C., Bonebrake, C.A., Boyd, P.A.: Gamification of cybersecurity for workforce development in critical infras-

tructure. IEEE Access **10**, 112487–112501 (2022). https://doi.org/10.1109/access.2022.3216711

2. Beguin, E., et al.: Computer security oriented escape room. IEEE Secur. Priv. **17**(4), 78–83 (2019). https://doi.org/10.1109/MSEC.2019.2912700
3. Budimir, S., Fontaine, J., Huijts, N., Haans, A., Loukas, G., Roesch, E.: Emotional reactions to cybersecurity breach situations: a scenario-based survey study. J. Med. Internet Res. **23**, e24879 (2020). https://doi.org/10.2196/24879
4. Center for Infrastructure Assurance & Security: Cyber Threat Defender - The UTSA CIAS. University of Texas at San Antonio. https://cias.utsa.edu/ctd/. Accessed 1 Feb 2023
5. Chen, T.R., Shore, D.B., Zaccaro, S.J., Dalal, R.S., Tetrick, L.E., Gorab, A.K.: An organizational psychology perspective to examining computer security incident response teams. IEEE Secur. Priv. **12**(5), 61–67 (2014). https://doi.org/10.1109/MSP.2014.85
6. Cichonski, P., Millar, T., Grance, T., Scarfone, K.: Computer security incident handling guide. NIST Spec. Publ. **800**(61) (2012). https://doi.org/10.6028/NIST.SP.800-61r2. Revision, National Institute of Standards and Technology
7. Clarke, S.J., Peel, D.J., Arnab, S., Morini, L., Keegan, H., Wood, O.: EscapED: a framework for creating educational escape rooms and interactive games to for higher/further education. Int. J. Serious Games **4**(3) (2017). https://doi.org/10.17083/ijsg.v4i3.180
8. Cleveland, S., Cleveland, M.: Toward cybersecurity leadership framework. In: The Thirteenth Midwest Association for Information Systems Conference Proceedings, MWAIS, p. 49 (2018). https://aisel.aisnet.org/mwais2018/49
9. Debello, J.E., Schmeelk, S., Dragos, D.M., Troja, E., Truong, L.M.: Teaching effective cybersecurity through escape the classroom paradigm. In: IEEE Global Engineering Education Conference, EDUCON, pp. 17–23. IEEE (2022). https://doi.org/10.1109/EDUCON52537.2022.9766684
10. Decusatis, C., et al.: A cybersecurity awareness escape room using gamification design principles. In: 12th IEEE Annual Computing and Communication Workshop and Conference, CCWC, pp. 765–770. IEEE (2022). https://doi.org/10.1109/CCWC54503.2022.9720748
11. Department of Defense: Cyber Protect - DoD Cyber Exchange. https://public.cyber.mil/training/cyber-protect/. Accessed 1 Feb 2023
12. Duncan, K.J.: Examining the effects of immersive game-based learning on student engagement and the development of collaboration, communication, creativity and critical thinking. TechTrends **64**(3), 514–524 (2020). https://doi.org/10.1007/s11528-020-00500-9
13. European Union Agency for Cybersecurity: European cybersecurity skills framework (ECSF). ENISA reports (2022). https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles
14. Gilboy, M.B., Heinerichs, S., Pazzaglia, G.: Enhancing student engagement using the flipped classroom. J. Nutr. Educ. Behav. **47**(1), 109–114 (2015). https://doi.org/10.1016/j.jneb.2014.08.008
15. Greene, J.C.: Engaging critical issues in social inquiry by mixing methods. Am. Behav. Sci. **56**(6), 755–773 (2012). https://doi.org/10.1177/0002764211433794
16. Hajny, J., Ricci, S., Piesarskas, E., Levillain, O., Galletta, L., De Nicola, R.: Framework, tools and good practices for cybersecurity curricula. IEEE Access **9**, 94723–94747 (2021). https://doi.org/10.1109/ACCESS.2021.3093952
17. Hevner, A.: A three cycle view of design science research. Scand. J. Inf. Syst. **19**(2), 87–92 (2007)

18. Hevner, A.R., March, S.T., Park, J., Ram, S.: Design science in information systems research. MIS Q. **28**(1), 75–105 (2004)
19. Hmelo-Silver, C.: Problem-based learning: what and how do students learn? Educ. Psychol. Rev. **16**, 235–266 (2004). https://doi.org/10.1023/B:EDPR.0000034022.16470.f3
20. Kuckartz, U.: Qualitative Text Analysis: A Guide to Methods, Practice & Using Software. SAGE Publications Ltd., Thousand Oaks (2014). https://doi.org/10.4135/9781446288719
21. López-Belmonte, J., Segura-Robles, A., Fuentes-Cabrera, A., Parra-González, M.E.: Evaluating activation and absence of negative effect: gamification and escape rooms for learning. Int. J. Environ. Res. Publ. Health **17**(7) (2020). https://doi.org/10.3390/ijerph17072224
22. Löffler, E., Schneider, B., Asprion, P.M., Zanwar, T.: CySecEscape 2.0–a virtual escape room to raise cybersecurity awareness. Int. J. Serious Games **8**, 59–70 (2021). https://doi.org/10.17083/ijsg.v8i1.413
23. Malone, M., Wang, Y., James, K., Anderegg, M., Werner, J., Monrose, F.: To Gamify or not? On leaderboard effects, student engagement and learning outcomes in a cybersecurity intervention. In: Proceedings of the 52nd ACM Technical Symposium on Computer Science Education, SIGCSE, pp. 1135–1141. ACM (2021). https://doi.org/10.1145/3408877.3432544
24. Manley, B., McIntire, D.: A guide to effective incident management communications. Software Engineering Institute, Cargenie Melon University, February 2021. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=651816
25. Mello-Stark, S., VanValkenburg, M.A., Hao, E.: Thinking outside the box: using escape room games to increase interest in cyber security. In: Daimi, K., Francia III, G. (eds.) Innovations in Cybersecurity Education, pp. 39–53. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-50244-7_3
26. Murphree, C., Vafa, S.: Use of escape rooms in education. In: Proceedings of Society for Information Technology & Teacher Education International Conference, pp. 1837–1842. Association for the Advancement of Computing in Education (AACE) (2020). https://www.learntechlib.org/p/215961
27. Nieto-Escamez, F.A., Roldán-Tapia, M.D.: Gamification as online teaching strategy during COVID-19: a mini-review. Front. Psychol. **12** (2021). https://doi.org/10.3389/fpsyg.2021.648552
28. Papaioannou, T., Tsohou, A., Bounias, G., Karagiannis, S.: A constructive approach for raising information privacy competences: the case of escape room games. In: Katsikas, S., Furnell, S. (eds.) Trust, Privacy and Security in Digital Business (TrustBus), vol. 13582, pp. 33–49. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-17926-6_3
29. Pirta-Dreimane, R., et al.: Application of intervention mapping in cybersecurity education design. In: Frontiers in Education, vol. 7 (2022). https://doi.org/10.3389/feduc.2022.998335
30. Pirta-Dreimane, R., Brilingaitė, A., Roponena, E., Parish, K.: Multi-dimensional cybersecurity education design: a case study. In: IEEE International Conference on Dependable, Autonomic and secure Computing, International Conference on Pervasive Intelligence and Computing, International Conference on Cloud and Big Data Computing, International Conference on Cyber Science and Technology Congress, DASC/PiCom/CBDCom/CyberSciTech, pp. 1–8. IEEE (2022). https://doi.org/10.1109/DASC/PiCom/CBDCom/Cy55231.2022.9927931

31. Sellers, J., Helton, W.S., Näswall, K., Funke, G.J., Knott, B.A.: Development of the team workload questionnaire (TWLQ). In: Proceedings of the Human Factors and Ergonomics Society 58th Annual Meeting, vol. 58, no. 1, pp. 989–993 (2014). https://doi.org/10.1177/1541931214581207
32. Steinke, J., et al.: Improving cybersecurity incident response team effectiveness using teams-based research. IEEE Secur. Priv. **13**(4), 20–29 (2015). https://doi.org/10.1109/MSP.2015.71
33. Subhash, S., Cudney, E.A.: Gamified learning in higher education: a systematic review of the literature. Comput. Hum. Behav. **87**, 192–206 (2018). https://doi.org/10.1016/j.chb.2018.05.028
34. Thompson, M.F., Irvine, C.E.: CyberCIEGE: a video game for constructive cyber security education. Call Signs **6**(2), 4–8 (2015)
35. Švábenský, V., Čeleda, P., Vykopal, J., Brišáková, S.: Cybersecurity knowledge and skills taught in capture the flag challenges. Comput. Secur. **102**, 102154 (2021)