Cybersecurity Training: Improving Platforms Through Usability Studies

Mubashrah Saddiqa, Rasmus Broholm, and Jens Myrup Pedersen

Abstract The combination of technological advancements and gaps in cyber awareness is behind the increasing problem of cyber-attacks. Cyber-attacks are no longer just a concern for businesses and governments; they are also a concern for the public, especially the young, who are true digital natives. In this age of rapid technological advancement and access to various forms of social media and games, it is critical for the youth and private companies to acquire IT skills to protect their digital privacy. As new IT subjects are introduced in Middle School and Secondary Education, teachers will need access to hands-on environments with relevant exercises within the concepts of cybersecurity education (such as web exploitation, forensics, cryptography, binary, etc.) based on students' level of understanding. In this paper, we study how to design a cyber training platform to assist teachers in accessing relevant exercises for cybersecurity education. As a case study, we are testing the Haaukins administrative cybersecurity training platform, along with the connected learning material platform that will guide how to use the cybersecurity training platform along with supporting learning material. The usability of these two platforms has been investigated in a cybersecurity educational environment with high school teachers. The results show that the use cases assist teachers in providing training environments for students by utilizing ready-to-use exercises relevant to cybersecurity subjects and by providing access to learning material covering a wide range of cybersecurity topics aimed at students at a beginner and intermediate level.

Keywords Cybersecurity · Haaukins training platform · User studies · High schools · Teachers

M. Saddiqa (✉) · R. Broholm · J. M. Pedersen
Electronic Systems Department, Aalborg University, Copenhagen Campus, Copenhagen, Denmark
e-mail: mus@es.aau.dk

R. Broholm
e-mail: rbr@es.aau.dk

J. M. Pedersen
e-mail: jens@es.aau.dk

C. Onwubiko et al. (eds.), *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media*, Springer Proceedings in Complexity, https://doi.org/10.1007/978-981-99-6974-6_8

1 Introduction

With the advancement of technology and the expansion of the Internet, people can now experience two paradigms: real life and the virtual world. The virtual world is in the form of social networks, games, and applications. The digital transformation has transformed society with deepening effects on everyday life [1]. However, the advancement and development of digitization makes us more vulnerable to cyber-attacks, raising the demand for cybersecurity knowledge among young students (high school and onwards). The objective of cybersecurity is safeguarding computers, networks, programs, and data against cyber-attacks. With increasing dependence on computer systems and networks, cyber-attacks have become more common, advanced, and destructive in recent years [2]. There is a growing demand for a well-trained cybersecurity team to address holistic cybersecurity problems [3].

With the rise in cyber-attacks, cybersecurity professionals use enhanced cyber infrastructure techniques and platforms such as big data, machine learning, and cloud computing to analyze cyber risks, detect threats, and optimize protection. However, the gap between students' understanding of cyber-attacks and cybersecurity skills is widening due to a lack of training programs in their curricula [4]. Over the last decade, the demand for experts in the field of cybersecurity has steadily increased, exceeding the pool of qualified professionals [5].

Cybersecurity education is becoming increasingly important for the development of proficient cybersecurity experts and an engaged public, and there is a growing demand for cybersecurity education among young people who have an elevated level of general and expert knowledge. High school education plays a critical role in addressing this shortage by increasing awareness and interest in cybersecurity as well as providing students with the fundamental knowledge required to pursue cybersecurity career paths [1]. For example, CTF (Capture the Flag) competitions, in which students complete a variety of tasks ranging from basic programming exercises to hacking a server to steal data (usually to find a specific piece of text, that is hidden on the server or behind a webpage, that will trigger a point reward mechanism), can pique students' interest in the subject [6]. A US national survey involving over 900 K-12 educators revealed that most of them have limited knowledge of cybersecurity education [7]. The survey assessed participants' understanding of cybersecurity, which encompasses knowledge of digital device interactions, vulnerability protection, and ethical considerations. In response to the growing demand for cybersecurity, several higher education institutions worldwide have started to develop cybersecurity curricula, whereas others have implemented cybersecurity into their existing teaching curricula [8].

However, these courses mainly place a greater emphasis on theoretical teaching and offer fewer opportunities for students to practice their skills [9]. Since practical exercises are an important part of such curricula, several instructional platforms have been developed in recent years [8, 10, 11] to help teachers and students acquire skills in the field of cybersecurity. The Haaukins CTF platform [10] is an educational cyber training platform for high school students which was further upgraded to target students at higher education levels [8]. The platform provides a fully automated setup of secure and closed environments, where students can solve a wide range of exercises related to hacking and insecure systems—while gaining points to support a gamified experience.

Nonetheless, there are challenges in ensuring that students have opportunities to experience real-world modern technology, tools, and techniques while making sure to comply with budget and physical space limitations [9, 12]. Furthermore, many existing platforms are mostly run by technical experts or developers, and teachers are less flexible when it comes to creating a practical environment that meets their needs and requirements [8, 13]. As a result, it becomes critical to provide teachers with cyber training platforms that allow them to create relevant creative exercises and enable them to assign exercises to multiple students with ease. At the same time, it is essential to provide teachers and students with cybersecurity education learning materials that make it simple for teachers to learn how to use cyber training platforms, i.e., how to access, create, and deploy relevant exercises for students without the help of developer\technical experts of the training platforms. To understand how to design such platforms, we will investigate the following research questions in this paper:

RQ1. *How to design a cyber training platform to facilitate teachers to easily create a hands-on environment/event for practicing cybersecurity by selecting cybersecurity exercises for students relevant to their subject without the assistance of technical professionals or the developers of the cyber training platform?*

RQ2. *How to design a learning material platform to assist both teachers and students in relation to cyber education and supporting the use of a cyber training platform?*

To answer the research questions, we evaluated the design of a cyber training platform as a use case (developed by a team of developers of Aalborg University), that has an interface targeted toward students and teachers, as well as another platform with an interface and content directed toward educators of cybersecurity.

The study's main goal is to test the usability of the cyber training platform that makes it easier for teachers to provide practical exercises for students, in the form of CTF games, so they can better understand cybersecurity topics. To enhance the overall education process, the platform allows teachers to select tasks/exercises with complexity levels ranging from easy to difficult and includes various cybersecurity topics such as cryptography, online exploitation, forensics et al. In this research paper, we conducted usability tests on the below-mentioned platforms with high school teachers as participants to better understand the design for cyber training platforms and obtained their perspectives on integrating these platforms into cybersecurity education curricula. The two platforms are as follows:

1. **Haaukins Administrative Platform for Teachers**
2. **Cyber Training Learning Material Platform**

The Haaukins CTF platform [8] is an accessible and automated virtualization platform for security education and empowers both teachers and students with little technical knowledge of cybersecurity. To assist teachers in providing the best learning

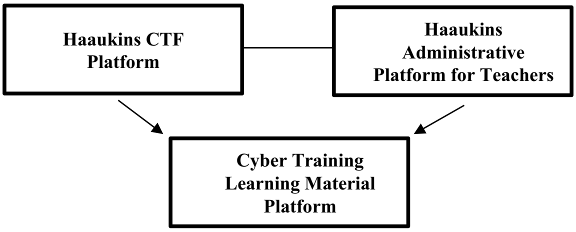

Haaukins CTF Platform
Haaukins Administrative Platform for Teachers
Cyber Training Learning Material Platform

Fig. 1 Overview of cyber training platforms

environment for cybersecurity education, an evolved version of the Haaukins Administrative Platform for Teachers has been developed, allowing teachers and professionals to create and monitor various cyber training events on Haaukins CTF platform for students whenever needed. The Haaukins Administrative Platform for Teachers is open source and can be accessed from the link https://admin.ntp-event.dk:8003/login. Users require sign up keys to register on the platform.

In addition, to familiarize both teachers and students with the functionality of the Haaukins CTF platform, a supporting Cyber Training Learning Material Platform (https://www.cybertraining.dk/haaukins/) has also been developed that facilitates teachers and students through self-paced cybersecurity learning materials and guide the use of the Haaukins CTF and Haaukins Administrative platforms.

An overview of Haaukins CTF, Haaukins Administrative, and Cyber Training Learning Material Platforms is shown in Fig. 1. In this study, we will investigate the usability of Haaukins Administrative Platform for Teachers and Cyber Training Learning Material Platforms. The two platforms can also facilitate other subjects within Information Technology but are more appealing to cybersecurity education because of CTF features which provide a practical experience to the students to understand several types of cyber-attacks.

In the rest of the paper, we will use Haaukins-APT to refer to the Haaukins Administrative Platform for teachers and CTLM to refer to the Cyber Training Learning Material Platform. The document is structured as follows. Section 2 describes the background of the research work, Sect. 3 presents the research methodology and test setups, Sect. 4 presents the usability results of the use cases, and Sect. 5 presents the implications of the results. Section 6 discusses the limitations of the study, while Sect. 7 concludes the paper.

2 Background

Ethical hacking, security auditing, digital forensics, network security, cryptography, malware analysis, and secure-software development, are common topics in cybersecurity education. To support this, teachers can create real-world exercises by applying theoretical knowledge and gaining access to industry challenges for hands-on learning activities [14]. With the lack of technical expertise and resources, however, creating exercises is a time-consuming and arduous task. Since practical training is part of cybersecurity education, cloud-based virtualization approaches to cybersecurity education are becoming more popular, and research has shown that this type of training benefits students' learning [13]. Such cloud-based virtualization platforms offer game-based cyber training exercises to students to test their cyber skills in real-world scenarios. However, in our experience, most teachers lack the technical skills and time required for designing security and risk-based challenges that are relevant to their chosen security subject while matching the students' level of understanding. Consequently, there is a need to design cyber training platforms where the teachers can easily identify and select challenges that meet teaching requirements.

To address these challenges, the Haaukins-APT platform was designed for teachers to help them provide the best training experiences for their students through game-based challenges. The CTML platform, on the other hand, provides relevant learning materials for the Haaukins CTF platform and cybersecurity education. We will investigate how the Haaukins-APT and CTML platforms can support teachers in the best way possible without the need for technical expertise, how to utilize Haaukins-APT, and how the learning materials available on the CTML platform help teachers and students understand how to use cyber training platforms. The two platforms are briefly described in the following sections.

2.1 Haaukins-APT (Haaukins Administrative Platform for Teachers)

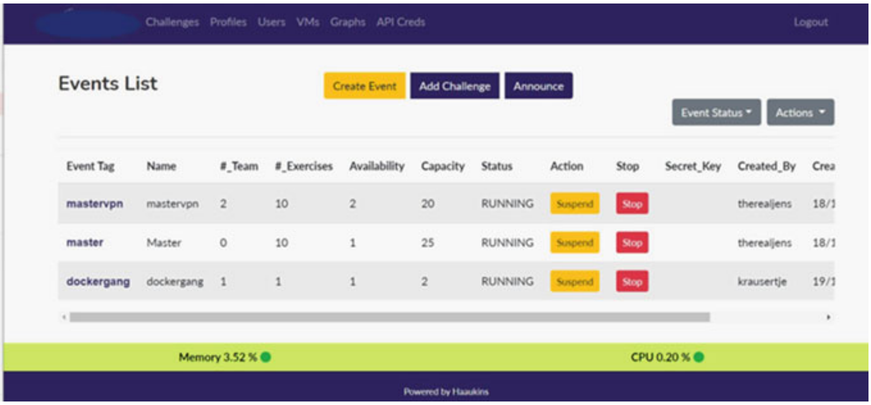
The Haaukins CTF platform [10] was created to make cybersecurity training easily accessible for Danish students. It works by creating virtual labs, which contain virtual machines representing computers or devices with various vulnerabilities. By accessing these labs, students get the chance to work with vulnerable machines/devices in a closed and secure environment. On top of this is a layer of gamification through challenges that must be solved in the virtual labs, and the teacher can customize the labs for a class by choosing which machines/challenges to include.

The platform is event-based, where an event can be a class or another type of training session. When a Haaukins cyber training platform is set up for an event, students are provided with several exercises/challenges that can be solved to gain points—and everyone in the event can see a scoreboard showing total points and who solved which exercise. It can be used for both teams and individuals and once an event is created, students simply register themselves (or their teams) to gain access to the challenges. This is similar to other "Capture the Flag" platforms. What makes this platform stand out, is that it provides each student/team access to a virtual lab, which is a collection of connected virtual machines that are used in the exercises. These are automatically created upon sign up and provide an easy and secure way access to a setup that provides a realistic "hacker experience" but would be very time-consuming to create in an ad-hoc manner. The platform has been used by several high schools receiving consistent positive feedback over the last few years, and to support higher education it has been revised and improved [8].

While the previous version provided an all-browser experience focused on ease of use, the most recent version for example includes an optional VPN (Virtual Private Network) feature, allowing students to use their own virtual machines and tools. Teachers can also access pre-defined profiles, i.e., sets of challenges often used together, for example, relevant for a typical introductory class in high schools and fitting those learning objectives. It not only saves time, but also serves as inspiration. Finally, the platform has been made more scalable to handle more students and longer concurrent events.

The Haaukins-APT supports the teachers' administrative role and enables educators without technical knowledge of the training platform to set up events as described above. Teachers should first sign up using the credentials provided by the Haaukins-APT administrator. The teacher can name the events, and specify the event's end date and capacity of the event (number of students). The teacher can also select challenges from pre-defined profiles or topics with complexity levels ranging from very easy to extremely difficult. An overview of the Haaukins-APT, showcasing a list of current events, is shown in Fig. 2. Once a teacher has created an event, the virtual labs are automatically created along with an event website representing the challenges to the students. The teacher chooses the subdomain address, where students can sign up for that event.

However, to better understand teachers and professional users of the Haaukins-APT, we will test the usability and user-friendliness of the Haaukins-APT to investigate the user experience and the requirements for improvements.



Events List

Event Tag	Name	#_Team	#_Exercises	Availability	Capacity	Status	Action	Stop	Secret_Key	Created_By	Crea
mastervpn	mastervpn	2	10	2	20	RUNNING	Suspend	Stop		therealjens	18/1
master	Master	0	10	1	25	RUNNING	Suspend	Stop		therealjens	18/1
dockergang	dockergang	1	1	1	2	RUNNING	Suspend	Stop		krausertje	19/1

Memory 3.52 % ●

CPU 0.20 % ●

Powered by Haaukins

Fig. 2 Overview of Haaukins-APT platform. This view shows the current events and their properties

2.2 *Cyber Training Learning Material Platform (CTLM)*

The Cyber Training Learning Material Platform (CTML) (https://www.cybertraining.dk/haaukins/) has learning material for self-paced learners to gain knowledge of the different subjects within cybersecurity, to solve the challenges of the Haaukins cyber training platform. The learning material is also targeted toward teachers who would like to know more about cybersecurity subjects and Kali Linux, in pursuance of utilizing the platform in their teaching. The learning material consists of a course with a walkthrough of the Haaukins-APT (Administrative Platform for Teachers) where the user is introduced to the platform, what it is about, how to create an event (from a teacher), which challenges to choose from, and how to start teaching students in cybersecurity. The course overview is given below.

1. Introduction

The first chapter of the course introduces the Haaukins-APT (Administrative Platform for Teachers), how teachers can use the administrative platform to create events, and how students can register to participate in the challenges event. The first chapter is divided into three sub-chapters:

(a) What is an Haaukins CTF platform?
(b) How to create an event?
(c) How to register as a student?

The course is in Danish and includes details and walkthrough videos that explain and demonstrate various steps for creating a relevant event for students. The course covers forensics, web exploitation, cryptography, binary, and other cybersecurity topics. The course also explains the learning objectives associated with a variety of challenges ranging from very simple to difficult. The challenges and descriptions, on the other hand, are available in English.

2. Challenges overview

The second chapter provides a walkthrough of how to solve some specific CTF challenges. The challenges chosen are from various themes, including Linux walkthrough (Starters Challenges), network scanning and Sniffing (Forensics), convincing visitation of URL, impersonating colleagues, and abusing credentials (Web Exploitation). The course includes introductory information as well as text and screenshots about the topics, challenges, associated learning objectives, and walkthrough videos (length from 4 to 18 min) explaining different steps to solve the challenges.

3. About the material

The final chapter of the course provides details about how the learning material was created. The material was developed with the support of Denmark's central and northern educational authorities.

3 Research Methodology

To test the usability of the Haaukins-APT with high school teachers, a variety of settings and methods can be used, such as controlled settings and natural settings, as described in [15]. In controlled settings, users perform tasks in a controlled environment and researchers observe certain behaviors related to the research questions. Usability tests and experiments are the main methods used for this setting. However, in a natural setting, there is little or no control over users' activities, making it possible to evaluate how a digital platform is used in the real world.

For our evaluation of the Haaukins-APT and associated learning materials, we chose controlled settings that directly involve users. We used both qualitative and quantitative research techniques, such as one-on-one interviews, usability tests, workshops, and online surveys, to gather participant responses and investigate our research questions. The two main research questions were subdivided into further sub-questions and investigated in two parts, with focused research areas:

Research Investigation 1: Focused on examining the usability of the Haaukins-APT as a use case. To better understand research question 1 (RQ1), we split it into further sub-questions as follows:

(1) What are the teachers' perspectives on utilizing the Haaukins-APT concerning cybersecurity teaching activities?
(2) What are the major or minor issues that will hinder the usability of the Haaukins-APT?
(3) What are teachers' views on the content of the challenges concerning cybersecurity education?

Research Investigation 2: Focused on the usability of the learning materials associated with the cyber training platform (using the CTML platform as a use case). Research Question 2 (RQ2) was further divided into sub-questions to provide additional clarity. The sub-questions are defined as follows:

(1) What are the teachers' perspectives of the current learning material on the CTLM platform?
(2) How useful are the learning material and the guide for the Haaukins-APT?
(3) Improvement suggestions for the learning material available at the CTML platform to best meet teachers' requirements?

3.1 Test Setups

The various methods used to investigate the research questions, i.e., testing the usability of the Haaukins-APT and the learning materials available on cyber training platforms for teachers and professionals are described below.

1. **In-Person Usability Test**: The usability test is used to gain knowledge about the user experience [16]. We use in-person testing methods to evaluate the usability of the Haaukins-APT platform and learning materials on the CTLM platform.
2. **One-on-One Interviews**: The interviews aimed to gather direct user feedback on the Haaukins-APT and its associated learning materials. The primary objective was to investigate participants' overall perceptions of using Haaukins-APT for teaching, including administrative roles, content relevance, and the usefulness of the learning materials.
3. **Workshops**: Workshops are widely used as a qualitative research approach, where researchers can work with participants to gather a rich collection of data about participants' views on an innovation [17]. We use this method to inform teachers about the CTF platform and how to use it in real scenarios.
4. **Online Surveys**: We also use the online survey method as it can help to poll individual customers as well as industry clients, and to collect concrete feedback from users about specific products [18].

3.2 Participants

According to previous research [19], four or five participants can reveal approximately 80% of the usability problems in most web interfaces. We recruited 4–5 participants for each test to assess the usability of the Haaukins-APT and the CTLM platforms. The participants of the data gathering process were all teaching the subject of Informatics at HHX (Higher Commercial Examination Program), which is equivalent to higher school education with a focus on commerce. They had varying levels of IT skills, with some having prior experience using CTF platforms and others being beginners. The interviews were conducted in both Danish and English and were recorded with the participant's consent. Participants were recruited using a simple random sampling method, and those who were willing to volunteer. Participant details are presented in Table 1.

Invitations were sent to potential test participants for both the Haaukins-APT and CTLM platforms. Upon acceptance, detailed instructions were provided through calendar invitations. In some test setups, the same participants who tested the Haaukins-APT also provided feedback on the learning materials available on the

Table 1 Data collection setup and participants

Test setup	Participants	Location	Duration (min)
Usability test	5	Aalborg, Viborg	30–45
One-on-one interviews	9	Aalborg, Aarhus, Viborg	20–30
Workshop	2	Aarhus	30–60
Online survey	11	Aalborg, Aarhus, Viborg, Odense, Horsens	5–10

CTLM platform. The procedural details are given in Table 2. A brief description of various tasks performed during the usability test is given in Table 3.

Table 2 Procedural details for test setup in research investigations 1 and 2

Test setup	Procedure
Usability test	**Research investigation 1**: Three physical tests and two online tests are being conducted based on participant availability. In both cases, participants' screens are recorded while they perform various tasks. Before the in-person usability test, participants receive a brief introduction to the Haaukins-APT, including guidance on using administrative features for teachers. They are then provided with a sign-up key to register and log in to the Haaukins-APT. Participants begin by testing various features of the Haaukins-APT before proceeding to different tasks to assess platform usability. Table 3 provides a brief description of the tasks performed during the usability test
One-on-one interviews	**Research investigation 1**: Participants participated in in-person usability tests in which they performed several tasks using the Haaukins-APT. Afterward, a short interview was conducted to investigate the participants' general perspective about the Haaukins-APT's cybersecurity education capabilities. Teachers provide their feedback on the content, tasks/exercises, and the overall design of the Haaukins-APT **Research investigation 2**: Participants engaged in individual interviews to examine distinct features of the CTLM platform. The interviews were conducted in Danish, with participants' consent for recording. The duration of the interviews ranged from 20 to 30 min, contingent upon participants' familiarity with the Haaukins cyber training platform and associated materials. Teachers provided feedback about the relevance of the learning material content, the identification of issues, and an evaluation of the overall design of the CTML platform
Workshop	**Research investigation 2**: The workshops aimed to test the revised format of learning materials with Informatics teachers. The revised format included shorter videos demonstrating challenges on the Haaukins CTF platform, an introduction to Kali Linux, an overview of the Haaukins-APT platform, and a guide for operating the virtual machine and troubleshooting errors. During the workshop, participants evaluated the current learning materials on the CTLM platform. Subsequently, they were presented with the new materials, comprising shorter videos, online content, and printed versions, to determine if the revised format constituted an improvement
Online survey	**Research investigation 2**: A survey was created to gather more data about the teachers' opinions of the learning materials available on the CTML platform https://www.cybertraining.dk/haaukins/. The survey is designed to shed light on the usability of the material and to figure out the focus points when initiating the improvement phase. Another goal of the survey is to discover which subjects the teachers prioritize, to guide new material development

Table 3 Task descriptions for the Haaukins-APT usability test

Task No.	Brief description
Task 1	Create a No VPN event
Task 2	Create a VPN only event
Task 3	Create an event with easy challenges
Task 4	Create an event using a profile
Task 5	Create an event with the hardest challenge within the subject Binary
Task 6	List all the 'very easy' challenges for the cryptography category
Task 8	Identify which challenges belong to a specific profile

4 Usability Results of Use Cases

In this section, we will discuss the key findings corresponding to the two main research questions. The findings demonstrate how the Haaukins-APT can assist teachers and young professionals in achieving their learning goals, as well as how the cyber training platform CTML can aid in understanding the Haaukins-APT and facilitate cyber education. The main themes that emerged from the findings are discussed in-depth in the following sub-sections.

Overall, the participants did not experience major usability issues with the Haaukins-APT. All participants were able to navigate and use both platforms and to solve all tasks with zero or minimal help from the observer. The two major themes and corresponding sub-themes are discussed below.

4.1 Usability of the Haaukins-APT

We have categorized the results under this major theme into four sub-themes that will accomplish research question 1. Overall, the results indicate that the Haaukins-APT benefits teachers and cybersecurity professionals in their teaching activities as well as in organizing independent Haaukins cyber training events for students. According to the feedback from teachers, the contents of the Haaukins-APT are relevant to informatics subjects and provide students with valuable practical experience. The feedback of one of the participants was:

> The Haaukins-APT is relevant to what we teach students as part of the cybersecurity subject, and the administrative role allows us to create practical tasks for students based on their level and knowledge. (Teacher 1, 17-01-2022)

Teachers' Perspective About the Haaukins-APT. The findings of the study revealed that there are perceived opportunities associated with the use of the Haaukins-APT in teaching activities. Some teachers have previous experience with general CTF platforms, which piques both students' interests and provides a platform for them to practice their knowledge. Teachers will have more flexibility in selecting challenges based on students' levels and subjects with the administrative role. However, the usability tests reveal some minor and major issues that must be addressed to provide the best experience for teachers and professionals. All five participants during one-on-one interviews acknowledge that the Haaukins-APT not only saves time for teachers in finding relevant exercises and challenges for the students, but it also provides access to labs according to students' curricula and level of understanding, with challenges ranging from easy to hard. One of the participants said:

> Haaukins-APT is an excellent training platform for cybersecurity education. With access to an administrative role, it becomes even more convenient because I can easily create a practical environment for students relevant to a topic using ready-to-go challenges whenever I want without spending time designing relevant exercises and challenges. (Teacher 2, 21-12-2021)

Usability and User-Friendliness Issues for the Haaukins-APT. This theme focuses on specific usability issues discovered during the usability tests of the Haaukins-APT platform. Our aim is to provide a list of issues for designers and developers to improve the platform's utility and ease of use for teachers. Participants tested various features of the Haaukins-APT through different tasks and experienced some issues while solving them. We discuss these issues in detail below.

Issues with labels: While creating an event on the Haaukins-APT, users reported issues. Some labels required a more detailed description or a new name. Participants, for example, are perplexed by the terms "event capacity" and "event availability."

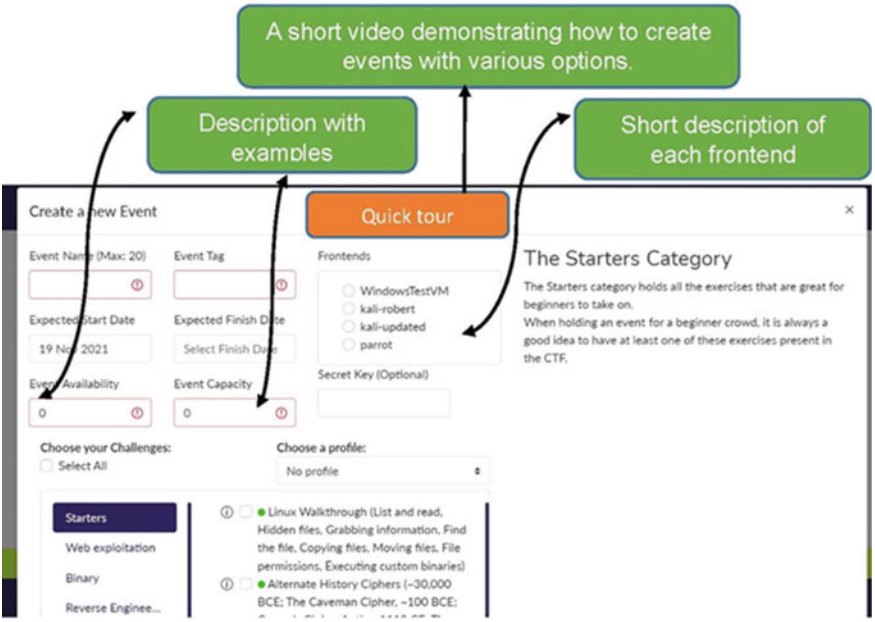
Proposal: Participants suggest having more detailed descriptions or labels on buttons. Figure 3 shows corresponding suggestions for different issues while creating an event.

Issues with dates: There are issues with the start and end dates. For example, if a user entered an incorrect date, the participant is still allowed to proceed, and the issue is only indicated at a later step when the user creates the event.

Proposal: This issue could be solved by not allowing users to proceed to the next step before the date and time entries have been validated. Also, if a user selects an incorrect date or time, the color should be changed to red to alert the user that they need to correct the date input.

Issues with selecting challenges from profile: Users identified another problem when choosing a challenge profile. This feature allows users to select a profile with a predefined set of challenges. The user can add or delete challenges from the profile when creating an event. Challenges in the profile are listed alongside the other available challenges. Users indicate that insufficient information is presented regarding the difficulty level of the available challenges, making it difficult to select appropriate challenges to include in the profile.

Proposal: Users suggest categorizing challenges in the profile based on difficulty level, as described on other Haaukins-APT pages, by using different colors for easy, hard, and very hard. A more detailed description of the challenges that are not in the profile, but can be added, could also aid the user in selecting additional appropriate


A short video demonstrating how to create events with various options.

Description with examples

Short description of each frontend

Quick tour

19 Nov 2021

0

0

The Starters Category

The Starters category holds all the exercises that are great for beginners to take on.
When holding an event for a beginner crowd, it is always a good idea to have at least one of these exercises present in the CTF.

ⓘ □ ● Linux Walkthrough (List and read, Hidden files, Grabbing information, Find the file, Copying files, Moving files, File permissions, Executing custom binaries)

ⓘ □ ● Alternate History Ciphers (~30,000 BCE: The Caveman Cipher, ~100 BCE:

Fig. 3 Proposal addressing issues on event creation page of Haaukins-APT

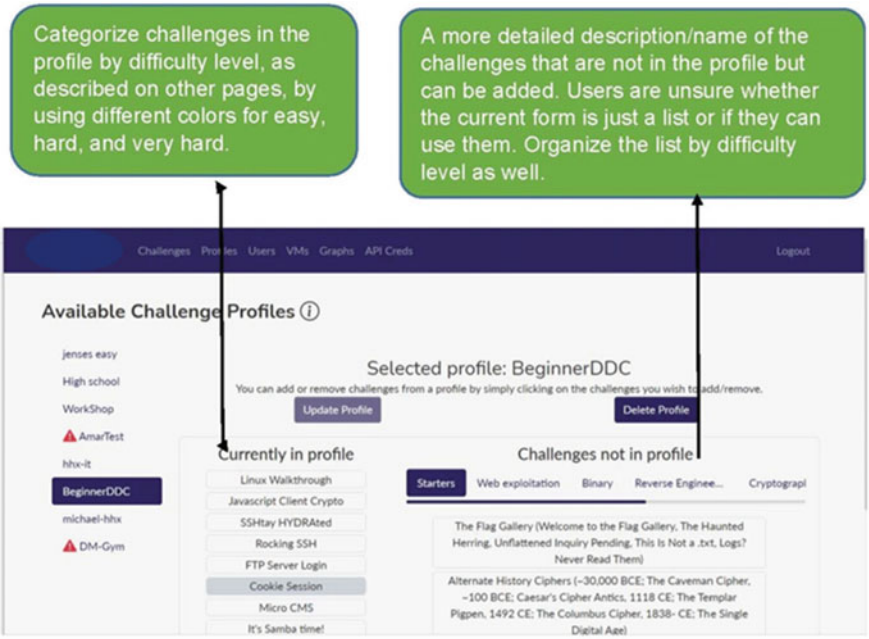
challenges. Users are unsure whether the current form is just listing the challenges for the profile or if it can be modified. Both lists of available challenges and those included in the profile should be consistently categorized by difficulty level using color codes. Figure 4 shows the issues on the profile page along with the proposed solutions.

Issue while selecting frontends: Users also have difficulties selecting a frontend from the available options. Three of five users are unfamiliar with these frontends; however, if a brief description of each frontend is provided, they can easily select a relevant frontend for their event.

Proposal: Users suggest including a brief description when a user clicks or hovers the mouse over a frontend.

Any web platform needs to be both user-friendly and visually appealing. When using the Haaukins-APT, the goal is to provide users with a clear and easy-to-follow structure. The Haaukins-APT can be accessed by users from a variety of internet-capable devices. In general, users are comfortable with the Haaukins-APT design, text, color, and layout. However, users also report a lack of user-friendliness features in some cases. For example, beginner Haaukins-APT users may not understand how to create an event and add challenges. One of the participants described his experience of using the Haaukins-APT as:

> I believe that the interface is very useful for cyber training education, but it lacks user-friendly functions for a first-time user, and more details and descriptions about how to use



Categorize challenges in the profile by difficulty level, as described on other pages, by using different colors for easy, hard, and very hard.

A more detailed description/name of the challenges that are not in the profile but can be added. Users are unsure whether the current form is just a list or if they can use them. Organize the list by difficulty level as well.

Available Challenge Profiles ⓘ

Selected profile: BeginnerDDC

You can add or remove challenges from a profile by simply clicking on the challenges you wish to add/remove.

Currently in profile

Challenges not in profile

The Flag Gallery (Welcome to the Flag Gallery, The Haunted Herring, Unflattened Inquiry Pending, This Is Not a .txt, Logs? Never Read Them)

Alternate History Ciphers (~30,000 BCE: The Caveman Cipher, ~100 BCE: Caesar's Cipher Antics, 1118 CE: The Templar Pigpen, 1492 CE: The Columbus Cipher, 1838- CE: The Single Digital Age)

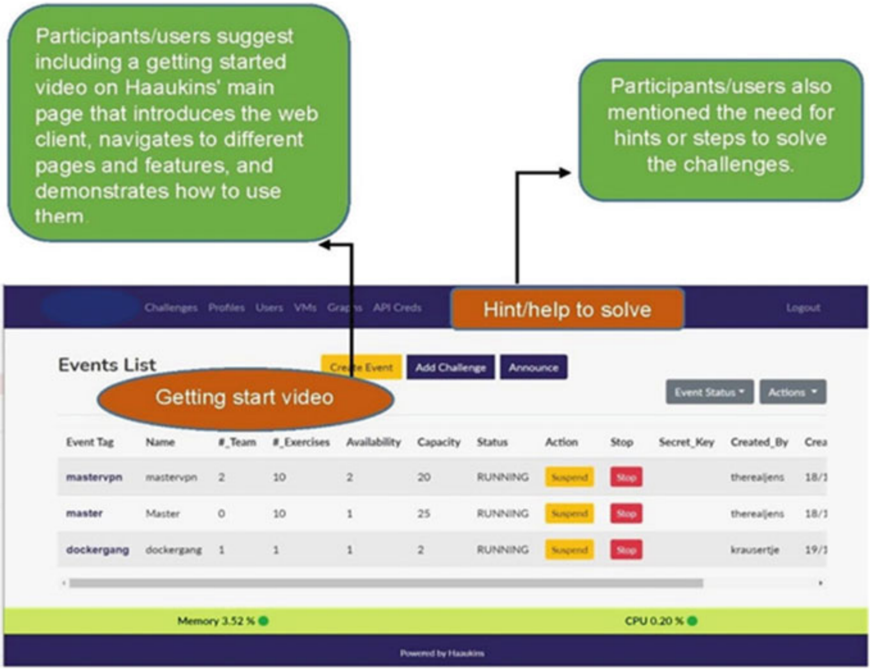
Fig. 4 Suggestion corresponding to challenges' profile page of the Haaukins-APT

> the various useful features of this platform are needed. For example, when I create an event using a pre-defined profile, I do not know which challenges are easy and which are difficult unless I navigate to the challenges list on another page. Furthermore, I'm not sure which frontends to use while creating an event. (Teacher 3, 28-02-2022)

First-time users accessing the Haaukins-APT require guidance to navigate the platform effectively. Specific areas where guidance is needed include event creation, VPN usage, and profile selection. User feedback suggests the inclusion of a short introductory video upon login, providing an overview of the Haaukins-APT and its various features. Additionally, users recommend a quick tour video on the event creation page to assist with navigating available options. A proposed solution addressing these user suggestions is depicted in Fig. 5.

Content Quality and Performance of the Haaukins-APT. Through one-on-one interviews, users provide valuable insights into the performance and content of the Haaukins-APT in the context of cybersecurity education training. Feedback indicates that the platform's content aligns with its cybersecurity curricula, and students benefit from the practical cyber training experience offered by the Haaukins-APT challenges. However, teachers recommend the inclusion of steps or hints specifically for their use in solving the challenges. One of the participants said:

> When students are engaged in solving challenges available on Haaukins cyber training platform and are confronted with one of the difficult/tricky challenges, and the teacher or organizer (especially if the teacher is new to Haaukins cyber training platform) is also unable



Participants/users suggest including a getting started video on Haaukins' main page that introduces the web client, navigates to different pages and features, and demonstrates how to use them.

Participants/users also mentioned the need for hints or steps to solve the challenges.

Hint/help to solve

Getting start video

Event Tag	Name	#_Team	#_Exercises	Availability	Capacity	Status	Action	Stop	Secret_Key	Created_By	Crea
mastervpn	mastervpn	2	10	2	20	RUNNING	Suspend	Stop		therealjens	18/1
master	Master	0	10	1	25	RUNNING	Suspend	Stop		therealjens	18/1
dockergang	dockergang	1	1	1	2	RUNNING	Suspend	Stop		krausertje	19/1

Fig. 5 Suggestions for improving usability of the Haaukins-APT

> to assist them, motivation and overall learning environment suffer, and student attention is diverted. However, if hints or step-by-step solutions are included on the Haaukins-APT version, the teacher can easily guide the students through the tough challenges. (Teacher 4, 17-12-2021)

The Haaukins-APT's overall performance was viewed as satisfactory according to users' feedback, including response time, wait time, load time, CPU utilization, and memory utilization.

4.2 Usability of the CTLM Platform's Learning Materials

The feedback highlighted a fundamental issue that teachers face when using the platform in a class setting. Teachers want to use the platform as an introduction to the subject, giving the students actual hands-on experience with real-life challenges to inspire them to pursue further studies in the field. Given that a teacher is likely to be working with students of various skill and interest levels, enough guidance must be available for the teacher to assist all students with completing the task based on individual ability.

Teachers' Perspective on the Usability of the Current CTLM Platform. The data collected from the survey indicates that the currently available learning materials of CTLM are considered useful to the teachers. All the participants agree that the language of the material is easy to understand, therefore when designing new material, it should match the current level of difficulty. Furthermore, Fig. 6 indicates that the overall title, introduction, and description are considered quite easy to understand by the teachers. This provides a positive foundation for further development of the CTLM. Figure 7 shows that most respondents stated that the length of the educational videos is very long.

Figure 8 shows the teachers' opinions on the usefulness of the available learning materials on the CTML platform. This demonstrates that it is considered a useful feature by most of the respondents, but it would gain a considerable increase in rating by being shortened and more focused. The interviews with the teachers uncovered similar points to the interview responses. Regarding the learning material, a teacher stated:

> You have to point out that there are some things that need to be explained before you get started. (Teacher 5, 17-10-2021)

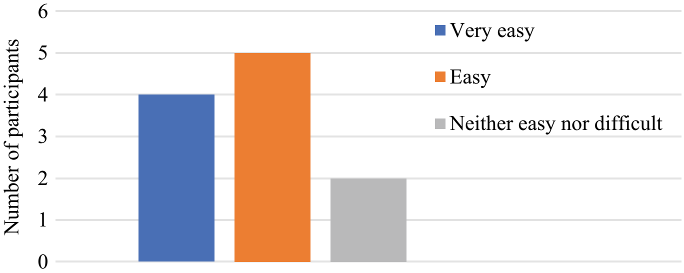


Fig. 6 Participants' response to the title, introduction, and description of the course on the CTML platform ($N = 11$)

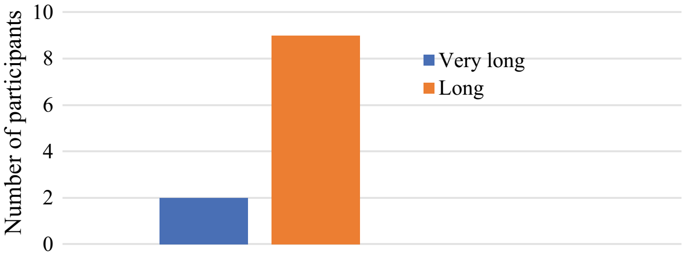


Fig. 7 Participants responses about the length of videos on CTML platform ($N = 11$)

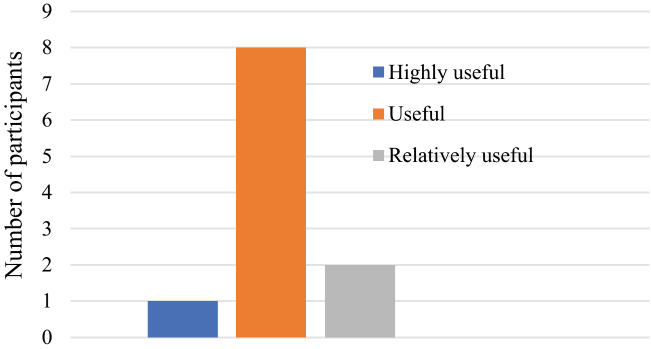


Fig. 8 Participants response about the use of CTML platform ($N = 11$)

The teacher is referring to the various terms in IT and cybersecurity that the students are familiar with before being introduced to the material. This is accomplished by supplying the teacher with a list of terms and brief descriptions that can be presented before or during the lecture. Another teacher states:

> There must be solutions to all challenges, it is really useful for the teachers and preferably an overview of Linux commands. (Teacher 6, 23-10-2021)

In addition to providing a comprehensive terminology list, it would be beneficial to create an overview of the required Linux commands, relevant to the Haaukins CTF platform-based challenges. Another key point raised by the teachers is to provide solutions to the challenges to assist their students without spending extra time. Another teacher's statement emphasizes this:

> It's a good idea to provide material that demonstrates how to solve various challenges so that you, as a teacher, can focus on teaching rather than on the platform – simply using Kali will be a big challenge and a potential show-stopper for some teachers. (Teacher 7, 23-09-2021)

Using the Haaukins-APT platform and related learning materials, the teacher emphasizes the importance of providing educators with a clear solution to each challenge, so they do not lose interest or confidence in their teaching. If a teacher spends extra time solving the challenges on their own in Kali Linux, they may prefer other learning platforms, where they do not need to solve the challenges or can easily solve them.

> I would like a more detailed description of what you can do with the platform. (Teacher 8, 15-11-2021)

The teacher emphasizes the importance of creating an introduction for educators, describing how the platform helps them teach cybersecurity and how the Haaukins CTF platform can be used to provide students with hands-on experiences working in the field. Regarding creating events using the Haaukins-APT a teacher said

> There is no email address for the person to whom a teacher must write to be added to the system as a user. (Teacher 8, 15-11-2021)

This is essential, as teachers need to have a Haaukins-APT platform login to create events with varying challenges for their students. User studies indicate that the teacher must feel confident in presenting the material and guiding students of different skill levels through the challenge-solving process. Considering the subject's novelty, teachers can't be expected to have extensive experience teaching it, so the provided guidance must be detailed enough to empower them to confidently assist their students.

Hypothesis Focused on the Usability of the Cyber Training Learning Material (CTLM) Platform. The ensuing hypothesis was conceived based on one-on-one interviews and survey feedback:

1. Enhancing the learning materials by enabling teachers to download the content as PDF files and print them would be beneficial, given that this is their preferred method of accessing the material.
2. Shortening the videos would facilitate a better comprehension of the content by teachers.

To validate these hypotheses, PDF descriptions of selected challenges were provided to two target audience members. Both found this to be an invaluable resource, assisting them in assessing the suitability of the challenges and supporting their students during these challenges. Additionally, revised descriptive videos were created for the same challenges, detailing the solutions step-by-step without delving into the underlying theory or the learning platform's mechanics. This was perceived as immensely useful by the users, who saw step-by-step solutions for teachers as a critical tool for building confidence when aiding their students in task completion.

Testing New Materials in Feedback Workshops. Participants provided extensive feedback on the structure of the introductory materials available to teachers. They expressed that an 18-min video was overwhelming and preferred a more concise approach. On-site workshops were conducted with a group of target high school computer science teachers, forming the basis for subsequent analyses. Mock-ups based on the original analysis and hypothesis were then presented to the same group of teachers, resulting in significant improvements in the perceived usability of the learning material platform for this audience. Key recommendations include:

1. Introduce the platform's capabilities and explain how it can be used in the classroom to support learning objectives. Predefined profiles should be presented, allowing teachers to choose the one that aligns with students' learning goals and skill level. A brief explanation of the covered technologies should accompany the profiles.
2. Provide detailed step-by-step solutions to the challenges to assist teachers in supporting their students. Additionally, offer guidance and hints at each step to aid students in solving the challenges. The guidance material should enable teachers to support their students without requiring in-depth technical knowledge of the challenges.

5 Implication for Cybersecurity Training Platforms

The rapid expansion of the cybersecurity industry has led to a global shortage of cybersecurity professionals. However, the lack of efficient and accessible real-world hands-on training platforms has created significant challenges for both students and teachers in cybersecurity education. In response to this challenge, it is essential to provide teachers with easy-to-use and accessible training platforms to provide a practical real-world emulating environment for cybersecurity education.

The study results reveal that cyber training platforms, such as Haaukins-APT and CTML, can be beneficial for teachers in providing ready-to-go challenges for their students. However, the current versions of these platforms require modifications before they can fully achieve their potential as learning tools. The study emphasizes the importance of having a learning material platform that supports both teachers and students in their cybersecurity education. To answer the first research question, the study recommends that the design of a cyber training platform should prioritize ease of use for teachers, enabling them to easily select relevant cybersecurity exercises for their students without technical assistance from developers. A user-friendly interface and ready-to-go challenges that are easily accessible would help achieve this. Additionally, the platform should be modular, allowing for customization and flexibility in terms of the content and level of difficulty of the exercises.

Regarding the second question, the study suggests designing a learning material platform that supports both teachers and students by including cybersecurity topics relevant to both parties, presented in a clear and accessible format. The platform should also offer support for teachers, such as training modules, lesson plans, and other resources to facilitate classroom teaching. For students, the platform should provide interactive and engaging content, such as gamification and simulations, to enhance their learning experience. The platform should aim to create a connected learning environment, where both teachers and students can easily collaborate and share resources.

The study findings suggest that a well-designed cyber training platform and learning material platform can greatly facilitate the teaching and learning of cybersecurity, even for those without technical expertise. The results highlight the importance of providing teachers with easy-to-use and accessible training platforms to provide a practical real-world emulating environment for cybersecurity education. As the cybersecurity industry continues to expand, and the global shortage of cybersecurity professionals persists, the need for such platforms has become even more critical.

6 Discussion and Limitation

This study demonstrates that cyber training platforms like Haaukins-APT and CTML can facilitate hands-on cybersecurity training for students, irrespective of their technical expertise. These user-friendly and flexible platforms allow more teachers to incorporate cybersecurity education into their subjects, thereby increasing student participation. The platforms offer customization of cybersecurity exercises based on students' needs and knowledge levels. The learning material platform incorporates interactive and engaging content, such as gamification and simulations, to enhance the learning experience.

However, certain limitations should be acknowledged. The study had a small sample size limited to Danish teachers, making it unclear if the platforms would be equally effective for educators from other countries or cultures. Some features may need adaptation for different educational systems or curricula. While Haaukins-APT and CTML are available in English, certain CTML platform walkthrough courses are in Danish, specifically targeting a Danish audience. Moreover, the study primarily focused on platform usability and did not assess their impact on improving students' cybersecurity skills. Future research should evaluate the platforms' effectiveness and compare them with other available cyber training platforms.

Lastly, although this study identified some usability issues, a larger sample size or more extensive testing could uncover additional concerns. Continuous evaluation and refinement of the platforms will be necessary to ensure their ongoing usability and effectiveness.

7 Conclusion

As digitization advances, the need for cybersecurity education grows due to the increasing prevalence of cyberthreats. Ongoing initiatives aim to raise awareness and support teachers in this field. To facilitate cybersecurity education, it is crucial to provide educators with training and learning platforms.

This research study focuses on the usability of two cyber training platforms, Haaukins-APT and CTML, in the classroom. It aims to design platforms that assist teachers in cybersecurity education and highlights the importance of a connected learning environment for collaboration and resource-sharing. The study emphasizes the necessity of training and learning material platforms to support teachers and students in cybersecurity education.

The study findings suggest that a user-friendly cyber training platform is essential for teachers, allowing them to easily select relevant exercises without technical assistance. The platform should be modular, customizable, and adaptable in terms of content and difficulty level. Clear and accessible presentation of cybersecurity topics is crucial for both teachers and students. Additionally, the platform should provide support for teachers, such as training modules and lesson plans, and engage students with interactive and captivating content to enhance their learning experience.

8 Future Work

In future research, we intend to investigate the effectiveness of cyber training platforms in enhancing students' cybersecurity skills. Additionally, we plan to expand the scope of the current study to include other cybersecurity learning platforms and conduct a more comprehensive evaluation. This would involve larger sample sizes and participants from neighboring countries, allowing for a broader assessment of the platforms' efficacy.

References

1. Rahman, N.A., Sairi, I.H., Zizi, N.A.M., Khalid, F.: The importance of cybersecurity education in school. Int. J. Inf. Educ. Technol. **10**, 378–382 (2020)
2. Center for Cyber Security. The Cyber Threat Against Denmark 2020. https://www.cfcs.dk/en/cybertruslen/reports/the-anatomy-of-targeted-ransomware-attacks/. Last accessed 05 April 2023
3. Jin, G., Tu, M., Kim, T.H., Heffron, J., White, J.: Game based cybersecurity training for high school students. In: Proceedings of the 49th ACM Technical Symposium on Computer Science Education, SIGCSE '18, pp. 68–73. Association for Computing Machinery, New York (2018). https://doi.org/10.1145/3159450.3159591
4. Purwanto, W., Wu, H., Sosonkina, M., Arcaute, K.: Deapsecure: Empowering Students for Data- and Compute-Intensive Research in Cybersecurity Through Training. PEARC '19. Association for Computing Machinery, New York (2019). https://doi.org/10.1145/3332186.3332247
5. Banerjee, S., Mazur, N.: Cybersecurity virtual summer workshop for secondary school teachers: an experience report. Faculty poster. J. Comput. Sci. Coll. **36**(8), 101–103 (2021)
6. Hanafi, H.A., Rokman, H., Ibrahim, A.D., Ibrahim, Z.A., Zawawi, M.N.A., Rahim, F.A.: A CTF-based approach in cybersecurity education for secondary school students. Electron. J. Comput. Sci. Inf. Technol. **7**(1) (2021). https://doi.org/10.52650/ejcsit.v7i1.107
7. The EdWeek Research Center. The State of Cybersecurity Education in k-12 Schools. https://cyber.org/sites/default/files/2020-06/The%20State%20of%20Cybersecurity%20Education%20in%20K-12%20Schools.pdf. Last accessed 04 April 2023
8. Mennecozzi, G.M., et al.: Bridging the gap: adapting a security education platform to a new audience. In: 2021 IEEE Global Engineering Education Conference (EDUCON), pp. 153–159. IEEE (2021). https://ieeexplore.ieee.org/document/9453985
9. Arora, A., & Mendhekar, A.: Innovative techniques for student engagement in cybersecurity education. In: Pattnaik, S.S., Mishra, A.R., Das, B. (eds.) Data Management, Analytics and Innovation: Proceedings of ICDMAI 2020, vol. 1, pp. 395–406. Springer Singapore (2021)
10. Panum, T.K., et al.: Haaukins: a highly accessible and automated virtualization platform for security education. In: 2019 IEEE 19th International Conference on Advanced Learning Technologies (ICALT), pp. 236–238. IEEE (2019). https://ieeexplore.ieee.org/document/8820918
11. Tobarra, L., Trapero, A.P., Pastor, R., Robles-Gómez, A., Hernández, R., Duque, A., Cano, J.: Game-based learning approach to cybersecurity. In: IEEE Global Engineering Education Conference (EDUCON), pp. 1125–1132 (2020)
12. Beason, R.E., Phelan, M., Devine, S., Aiken, M., Orban, J.: Evaluation of Hands-on Cybersecurity Skills Development. Technical Report, Idaho National Lab. (INL), Idaho Falls, ID (2021). https://doi.org/10.2172/1825671

13. Vykopal, J., Čeleda, P., Seda, P., Švábensky, V., Tovarňák, D.: Scalable learning environments for teaching cybersecurity hands-on. In: IEEE Frontiers in Education Conference (FIE), pp. 1–9 (2021). https://ieeexplore.ieee.org/document/9637180
14. Topham, L., Kifayat, K., Younis, Y.A., Shi, Q., Askwith, B.: Cyber security teaching and learning laboratories: a survey. Inf. Secur. **35**(1), 51–80 (2016). https://procon.bg/article/cyber-security-teaching-and-learning-laboratories-survey
15. Sharp, H., Preece, J., Rogers, Y.: Interaction Design: Beyond Human-Computer Interaction, 5th ed. Wiley (2019)
16. Hertzum, M.: Usability testing: a practitioner's guide to evaluating the user experience. Synth. Lect. Hum. Cent. Inform. **13**(1), i–105 (2020). https://doi.org/10.2200/S00987ED1V01Y202001HCI045
17. Ørngreen, R., Levinsen, K.: Workshops as a research methodology. Electron. J. E-learn. **15**, 70–81 (2017). https://eric.ed.gov/?id=EJ1140102
18. Wright, B., Schwager, P.H.: Online survey research: can response factors be improved? J. Internet Commer. **7**(2), 253–269 (2008). https://doi.org/10.1080/15332860802067730
19. Lindgaard, G., Chattratichart, J.: Usability testing: what have we overlooked? In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 1415–1424 (2007). https://doi.org/10.1145/1240624.1240839