Evaluation Concept

Cybersecurity Education Platform

CSEP
Cybersecurity Education Platform

Executive Summary

Assessors needed for evaluation of a cybersecurity education platform

Why

As part of my master thesis I have developed CSEP (Cybersecurity Education Platform) - a web platform, with which collaborative, scenario-based trainings for cybersecurity can be created and conducted.

I am now looking for assessors to help me evaluate the usefulness of this platform.

Who

For the evaluation I require the opinion of cybersecurity professionals who conduct trainings and workshops for non-domain experts and senior management.

When

At an individually agreed time slot, sometime between the 29th of September and 8th of October.

What

For the evaluation you will conduct either one or all three of the major use cases of the platform: scenario design, training a group and participating in a training.

The evaluation of each use case will consist of the following steps:

- Filling out a micro-survey on expectations.
- Performing the steps of the use case.
- Filling out a hotwash survey.

More detailed information on how each of the use cases will be evaluated, can be found in the following pages of this document.

How

The evaluation of each use case will take between 30 minutes and 1 hour.

For the evaluation, I will set up a video conference. You will also receive a link to the prototype of the CSEP.

Many thanks in advance!

Elias Ladenburger

If you have any questions, please do no hesitate to contact me at csep@eliasladenburger.com.

CSEP
Cybersecurity Education Platform

General Information

Problem Statement

As a cybersecurity professional, you have likely encountered „the human factor“ as a risk vector. With a high probability, you have used e-mails, workshops and e-learning programs to increase cybersecurity awareness, so as to reduce this risk.

Chances are, however, that you want a more potent and sustainable way to improving cybersecurity awareness in your organization.

Approach

CSEP aims to support you and other security professionals in developing and conducting more effective trainings.

The premise behind CSEP is that collaborative, scenario-based learning is an effective approach to raising awareness and shaping attitude toward security.

As the CoVid-19 situation has shown, trainings and workshops should be possible both on-site and remote. A computer-supported solution, perhaps accessible through the internet, could satisfy this requirement.

Being scenario-based, the participants of your training will be actively involved, making their own decisions when facing realistic problems. Collaboration occurs, because every participant in the training group has exactly the same information and the same objectives as every other participant – all participants are therefore encouraged to work together at all times.

At the core, the scenarios that can be created with CSEP can perhaps be compared to cyber exercises, such as those performed by ENISA. However, because the focus of CSEP is on educating non-security experts, the scenarios will have a different scope than those you may be familiar with.

Evaluation Approach

The evaluation will be conducted in the form of a peer inspection. The main evaluation criteria will be *ease of use* and *perceived usefulness*, as suggested by the technology acceptance model (TAM) (Venkatesch & Davies, 1989).

Each use case will be evaluated by a minimum of 5 cybersecurity professionals. The use case *participate in a game* may also be evaluated by laypeople. Each person who evaluates the platform is hereafter called an *assessor.*

One assessor may evaluate either one or all three of the use cases. The evaluation of each use case is timeboxed to 30 minutes. Before each evaluation, assessors will be asked to fill out a micro-survey (see appendix A). After each evaluation, assessors will be asked to fill out a hotwash-survey (see appendix B).

Assessors may agree to a recording of the evaluation session by signing the consent form (appendix C). Recordings will only be processed on a local device and will be deleted according to the DoD5220.22-M(ECE) standard after a period of four weeks at the latest.

Evaluation of Use Case *Participate in a Game*

Objectives

1. Determine whether it is possible to participate in learning games.
2. Determine whether participation in learning games can be done with good ease of use.
3. Determine whether participation in learning games leads to a high level of engagement.
4. Determine whether participation in learning games leads to a good level of retention.

Task

Please participate in the training session, in which the pre-selected scenario will be played.

During the training, communicate with the other participants on how to best solve the scenario.

One week after the training session, you will receive a short survey on how much you feel you have learned from the scenario. Please fill out this survey shortly after receiving it.

Evaluation of Use Case *Facilitate a Game*

Objectives

1. Determine whether it is possible to facilitate learning games.
2. Determine whether the trainer dashboard has a good ease of use.
3. Determine whether any information is missing from the trainer dashboard.
4. Determine whether the trainer dashboard should allow any more actions.

Tasks

Please not that for this evaluation session I will have to see the screen on which you conduct these tasks.

Please think out loud during the entire evaluation session and openly talk about every action you are taking.

Imagine yourself in the following situation: you are giving a cyber security awareness workshop to a group of executives from different business functions.

You will be given the name of a scenario. Please make yourself familiar with the scenario in the *manage scenarios* view.

After you have familiarized yourself with the scenario, please open a new game for this scenario. Send the link to the instructor and wait until 3 participants have joined.

Explain the rules of this scenario to your (imaginary) participants. Then start the game.

During the course of the game, use at least one variable change to influence which inject is being shown next. Make sure the game is finished before 10 minutes are over.

Evaluation of Use Case *Scenario Design*

Objectives

1. Determining whether it is possible to create learning scenarios.
2. Determining whether learning scenarios can be created with good ease of use.
3. Determine whether the functionality of learning scenarios is adequate.

Task

Please not that for this evaluation session I will have to see the screen on which you conduct these tasks.

Imagine that you want to create a new scenario for an awareness workshop.

To do so, please use CSEP to add a new scenario with the title *CISO Budget Allocation* and the description *simulate the allocation of a security budget.* Please add three variables to the scenario:

- *Budget (€)*, a numeric variable that is visible to participants and has a starting value of 20,000€,
- *Time (days),* another numeric variable that is visible to participants and has a starting value of 5 and
- *ISO 27001 certified? a* boolean variable that is hidden from the participants and has a starting value of *false*.

Please also insert four scenarios to your story, with the titles *budget choices*, *budget evaluation* and *final report*. The injects must have the default order of *budget choices, budget evaluation, final report*.

Introduction will be the entry point to the scenario and must have two choices: *invest in ISO certification* and *invest in awareness trainings*. The choice *invest in ISO certification* must reduce the *budget* by 10,000€.
The choice *invest in awareness trainings* must lead to a fourth inject called *conduct awareness trainings.*

The inject *budget evaluation* must have a pre-condition that the *budget* cannot be greater than 5,000€, otherwise the participants must be redirected to *budget choices*.

Feel free to insert any value of your choosing for any parameters of the scenario and injects that have not been mentioned in this task.

Appendix

Appendix A: Micro-survey

1. What branch of cybersecurity do you associate yourself most with?
    a. Security Management
    b. Security Audit and Compliance
    c. Security Education
    d. Security Development
    e. Other (please specify): _____

2. How experienced are you in conducting cybersecurity trainings?
    a. I have not yet given any trainings
    b. I have given between one and three trainings
    c. I have given between four and seven trainings
    d. I have given more than seven trainings

3. Have you developed material for cybersecurity trainings before?
    a. Yes
    b. No

4. Have you conducted collaborative trainings (where all participants share a task and goal) before?
    a. Yes
    b. No

5. Have you conducted scenario-based trainings (such as tabletop exercises) before?
    a. Yes
    b. No

6. What do you expect from a platform for collaborative, scenario-based trainings?

    _____

    _____

    _____

Link to survey: https://www.surveymonkey.de/r/YGXJGX2

Appendix B: Hotwash-Survey

1. What do you think are the three strongest aspects of the platform?
    1. _____
    2. _____
    3. _____

2. What do you think are the three weakest aspects of the platform?
    1. _____
    2. _____
    3. _____

3. On a scale of 1 to 4, how easy to use would you consider the platform?
    1. Not easy at all – I could not figure out how to use any of the features
    2. Difficult most of the time
    3. Somehwat easy
    4. Very easy – everything was clear to me throughout

4. On a scale of 1 to 4, how helpful would you consider the platform?
    1. Not helpful at all
       I would not use this for trainings
    2. Not very helpful
       I would still need to invest considerable effort into developing additional materials
    3. Somewhat helpful
       I would use this platform to complement my trainings
    4. Extremely helpful
       I would use this platform as the major component of some of my trainings and workshops

5. What further comments and suggestions do you have?

    _____

    _____

    _____

Link to survey: https://www.surveymonkey.de/r/YGSF6JY

Appendix C: Consent Form for Video Recording

To be able to better evaluate the reactions of each assessor, I would like to record the video conference of each evaluation session.

These recordings will only be stored locally. Furthermore, they will be deleted four week after the session has occurred.

You may opt out of the recording at any moment during a session.

I have read and understood above statement on video recording of evaluation sessions and agree to be recorded during sessions that I participate in.

_____

Appendix D: Glossary

Term	Definition
Learning Scenario	An set of injects, variables and rules that has been created by a cybersecurity educator. A scenario can be played any number of times.
Game	An instance of a scenario that is being or has been played by one or more participants.
Participant	A participant in a training session.
Trainer	A cybersecurity professional who currently conducts a training session.
Training Session	An event during which one or more participants and one or more trainers communicate synchronously. Includes the playing of a game, as well as a hotwash after the game.
Inject	A single event or task within a game.
Scenario Variable	Represents one aspect of the scenario. Can change value during the course of a game.
Branch	An inject that may be followed by two or more different injects, depending on the choices of the participants and/or the value of one or more game variables.
Fork	See branch.
Assessor	A cybersecurity professional who evaluates the usability and feature scope of CSEP.

Cybersecurity Education Platform