Best Practices and Guidelines for Cyber Security Training

Purpose

The purpose of this document is to provide common best practices and guidelines for Cyber Security Training. It is established as part of a collaborative project within the cyber security training sector in Denmark and supported by NCC-DK (The National Coordination Center for Cyber Security), co-funded by The European Union.

Background and partners

The main partners behind the project are ICS Range (icsrange.com), SagaLabs (sagalabs.dk), Campfire Security (campfiresecurity.com) and Dansk IT (dit.dk). However, we encourage all providers and other stake holders within cyber security training to contribute to the guidelines.

We are proud to work together on a set of common guidelines. We believe that when Danish providers of cyber security training work together, we both improve the level of cyber security training in Denmark – eventually making Denmark more cyber secure – and we improve the competitiveness and quality of the Danish cyber security training sector.

About the guidelines

The guidelines are not meant as a checklist to follow, but rather a set of best practices and guidelines to consider when designing cyber security training. Not all practices/guidelines are relevant for all aspects of cyber security training, and there can also be valid reasons for making different choices.

We hope the guidelines can serve as a quality mark for cyber security training made in Denmark, and we encourage providers of cyber security training to refer to the guidelines if they have been used.

In our context, we are mainly covering cyber security training for IT professionals, including software and security professionals. We do not aim to cover e.g. standard awareness training for non-IT employees, but of course everyone is welcome to gain inspiration.

The guidelines and best practices are organized as a number of principles.

This is version 1.0 of the guidelines.

Principles

1. Explain the purpose

To make sure the learners are motivated and see the value in the training, it is crucial to explain the purpose from the beginning: Why is this training important for them (and/or their company), what will they learn, and how will it help them?

2. Explain the teaching methodology

A common question from learners is: “Why do we have to do this?”. It is always recommended to explain why you have designed the learning experience as you have.

3. Active learning

Training should be based on active learning, rather than simply reading materials, or watching videos. Active learning not only improves retention and learning outcomes, but it is also more engaging and fun for the learners. Active learning can take many shapes and forms: Exercises, competitions, discussion sessions, and much more.

4. Combining theory and practice

The best learning happens when theory and practice is combined, and in general we recommend breaking down the learning blocks in small parts: It of course depends on topics, but in general it is good to have practical/hands-on problems, experiments or cases every time a new tool, concept or method is introduced. This reinforces the learning of this new tool/concept/method and makes the learner ready to build further knowledge on top. People learn differently and have different preferences in terms of learning styles, so the exact pattern and mix of theory and practice will always depend on the individual.

5. One thing at a time

For many learners who are new to cyber security, the initial learning steps can be overwhelming with many words, methods, concepts, and tools. Add on top that the learners also might need to accustom themselves to a new platform, including how to access the materials, different kind of cyber ranges or virtual labs, and point/scoring systems. We recommend that material is designed with this observation in mind, so the learning curve becomes manageable. On the other hand, it is also important that the learners feel they are learning something new: Therefore, it is recommended to think outside the “usual toolbox”.

6. Ease of use

A learning platform or a cyber range should be easy and intuitive to use for the learner. This means that it should be simple for inexperienced users to access resources and navigate the platform or cyber range. If platforms become too unpolished or too complex, the learner may use more energy navigating the platform or cyber range, rather than obtaining the skills and knowledge planned.

7. Collaborative learning

Learning together is always a great way of learning: Instead of solving exercises and problems alone, it is recommended to let learners work together: This often leads to good discussions which support the learning process, and situations where learners are helping each other is also good learning for all parties involved. Compared to working individually, it decreases the risk of being stuck and increases motivation and fun for the learner. As a bonus, learners get to know each other better. For most tasks, we recommend working in smaller groups of 2-4 learners, but this depends of course on the tasks at hand.

8. Gamification with a clear mission

Gamification is often setup as solving problems and getting points – or in the cyber security world to solve challenges and get flags – which then give points. This often works well, and it is impressive to see how much engagement and motivation gamification creates. However, the effects of gamification can be further boosted by working with missions and storylines instead of "just" getting flags or points. For example, building a storyline of infiltrating a malicious actor through their website might be more engaging for the learners than to simply find a website vulnerability (even though the actual task is the same). This principle is not to make the tasks more complex or less explained, but to build the right storylines where the goals are larger than simply getting a flag.

9. Clearly described tasks

In the cyber security community, there are many implicit understandings. When training people outside of this specific community, it is easy to get lost. A description of an exercise, where the learners were supposed to exploit a samba vulnerability, gain access to a server, and find a file on that server with the name flag.txt, once had the description "Have you ever tried dancing samba? Neither have we, but it might come in handy here". With this, the learner would have no clue where to start and what to achieve. It might be a fun description for a CTF competition, where part of the competition is to decode that specific language, but it is not suitable in a training context. This principle depends a bit on how supervised the learners are: The more they are expected to work independently, the more important it is that descriptions are clear. It is important to explain "implicit" terminology, like 0-day, SIEM etc. – at least it should always be carefully considered to write out abbreviations in full.

10. Hints are important

While some level of frustration is okay, it is important not to be completely blocked without any possibility to advance. That is why hints are important. On the other hand, there is also a lot of learning in figuring things out, and much satisfaction in succeeding with this. This makes it non-trivial to provide the right hints – also, it can be difficult to automatize, since the hints ideally are depending on the individual learner (or group of learners) and their progress.

11. A proper debrief

After finishing a course or learning lecture it is important to debrief and go through the learnings. This helps the learner retain what is learned. It is also a good opportunity to collect feedback for future improvements.

12. Real-world context and experience

Design training scenarios based on real-world cybersecurity threats and use cases, using current trends such as ransomware, supply chain attack, and cloud security challenges. This should help the student gain familiarity with concepts that are applicable to real threats.