Cyber defence exercises (CDX) represent a popular form of hands-on security training. Learners are usually divided into several teams that have to defend or attack virtual IT infrastructure (red vs. blue teams). CDXs are prepared for learners whose level of skills, knowledge, and background may be unknown or very diverse. This is evident in the case of high-profile international CDXs with hundreds of participants coming from government agencies, military, academia, and the private sector.

We present three methods for distributing learners into teams with respect to their level of proficiency and the prerequisite skills required for the exercise.

- We aim to reach a balance between proficiency and the exercise to make the exercise beneficial for the learners and an effective investment for sponsors.

- We outline findings from an analysis of the learners’ self-assessment of various skills before and after the exercise.

This research was supported by the Security Research Programme of the Czech Republic 2015-2020 (BV III/ – V5) granted by the Ministry of the Interior of the Czech Republic under No. VZ101620904 – Simulation, detection, and mitigation of cyber threats endangering critical infrastructure.

For more information about the project, visit https://www.kypo.cz/.