ISCTE IUL
REPOSITÓRIO
INSTITUTO UNIVERSITÁRIO DE LISBOA

Repositório ISCTE-IUL

Deposited in *Repositório ISCTE-IUL*:
2026-07-21

Deposited version:
Accepted Version

Peer-review status of attached file:
Peer-reviewed

Citation for published item:
Zhao, T., Gasiba, T., Lechner, U. & Pinto-Albuquerque, M. (2024). Thriving in the era of hybrid work: Raising cybersecurity awareness using serious games in industry trainings. In Andreas Bollin, Ivana Bosni, Jennifer Brings, Marian Daun, and Meenakshi Manjunath (Ed.), 2024 36th International Conference on Software Engineering Education and Training (CSEE&T), Proceedings. Würzburg, Germany: IEEE.

Further information on publisher's website:
10.1109/CSEET62301.2024.10663040

Publisher's copyright statement:
This is the peer reviewed version of the following article: Zhao, T., Gasiba, T., Lechner, U. & Pinto-Albuquerque, M. (2024). Thriving in the era of hybrid work: Raising cybersecurity awareness using serious games in industry trainings. In Andreas Bollin, Ivana Bosni, Jennifer Brings, Marian Daun, and Meenakshi Manjunath (Ed.), 2024 36th International Conference on Software Engineering Education and Training (CSEE&T), Proceedings. Würzburg, Germany: IEEE., which has been published in final form at https://dx.doi.org/10.1109/CSEET62301.2024.10663040. This article may be used for non-commercial purposes in accordance with the Publisher's Terms and Conditions for self-archiving.

Use policy

Creative Commons CC BY 4.0
The full-text may be used and/or reproduced, and given to third parties in any format or medium, without prior permission or charge, for personal research or study, educational, or not-for-profit purposes provided that:

- a full bibliographic reference is made to the original source
- a link is made to the metadata record in the Repository
- the full-text is not changed in any way

The full-text must not be sold in any format or medium without the formal permission of the copyright holders.

Serviços de Informação e Documentação, Instituto Universitário de Lisboa (ISCTE-IUL)
Av. das Forças Armadas, Edifício II, 1649-026 Lisboa Portugal
Phone: +(351) 217 903 024 | e-mail: administrador.repositorio@iscte-iul.pt
https://repositorio.iscte-iul.pt

Thriving in the era of hybrid work: Raising cybersecurity awareness using serious games in industry trainings

Tiange Zhao and Tiago Gasiba
Siemens AG
Otto-Hahn-Ring 6
81739, München, Germany
Email: tiange.zhao@siemens.com
Email: tiago.gasiba@siemens.com

Ulrike Lechner
University of the Bundeswehr Munich
Werner-Heisenberg-Weg 39
85579, Neubiberg, Germany
Email: ulrike.lechner@unibw.de

Maria Pinto-Albuquerque
Instituto Universitário de Lisboa
(ISCTE-IUL)
ISTAR, Av. das Forças Armadas
1649–026 Lisboa, Portugal
Email: maria.albuquerque@iscte-iul.pt

Our work [1] has been accepted in Journal of Systems and Software. It was first received on 30th January 2023 and revised on 31st October 2023, accepted 23rd December 2023. It is available online since 2nd January 2024; Version of Record 24th January 2024.

Abstract: Modern software engineering education aims to prepare software engineers for hybrid work environments. The shift to work-from-home (WFH) or work-from-anywhere (WFA) has increased the importance of cybersecurity. An industrial case study revealed that raising awareness is crucial. We developed two serious games, CyberSecurity Challenges (CSC) and Cloud of Assets and Threats (CATS) to enhance cybersecurity training. These games empower practitioners to address hybrid work challenges while ensuring secure software development and cloud security. Empirical evidence supports the effectiveness of serious games in raising awareness among software professionals.

Introduction: Nowadays, an increasing number of the training in the industry are conducted online or hybrid. Hybrid work refers to the work mode where a part of or all of the training participants join the training online instead of staying together in a classroom physically. This work provides a unique industry experience report on adapting the traditional cyber-security training with the enrichment of two novel serious games that we designed under the design science research paradigm.

Methodology: Our work is motivated by a case study highlighting the need to establish secure coding guidelines in the industry and raise awareness of cloud security issues. Following the guidance of the design science research paradigm, we designed the first serious game CSC and validated our design with the target group in 15 game events. By reusing the infrastructure and inspired by the success story of the CSC, we designed the second serious game, CATS, which focused on cloud security. We evaluate CATS in a hybrid environment in trainers, trainees, and organizational perspectives in 9 game events with 108 participants.

Result: Based on the data we collected, the results show that applying CSC and CATS in training is helpful in raising awareness among participants. According to our semi-structured survey, the result also shows the challenges that trainer faces in hybrid work and serious games can be a solution to those challenges.

Contribution: The contribution of our work is that we present the valuable experience in combining the advantage of different training modes and mitigating the disadvantage of online training. We observe the impact of serious games through a scientifically sound approach based on the data and feedback we collected systematically from the trainers', trainees', and the organization's perspectives in the industry. We show through empirical evidence that serious games are a successful approach for training conducted in hybrid work mode while providing authentic and immersed experiences that empower and raise cybersecurity awareness of current and future software professionals.

References

[1] T. Zhao, T. Gasiba, U. Lechner, and M. Pinto-Albuquerque, "Thriving in the era of hybrid work: Raising cybersecurity awareness using serious games in industry trainings," *Journal of Systems and Software*, vol. 210, p. 111946, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0164121223003412

Acknowledgment

This research task was partially supported by Fundação para a Ciência e a Tecnologia, I.P. (FCT) [ISTAR Projects: UIDB/04466/2020 and UIDP/04466/2020]. Ulrike Lechner acknowledges funding by dtec.bw for project LIONS and dtec.bw is funded by the European Union — NextGenerationEU and for project CONTAIN by the Bundesministerium für Bildung und Forschung (FKZ 13N16581). Tiange Zhao and Tiago Gasiba acknowledge the funding provided by the Bundesministerium für Bildung und Forschung (BMBF) for the project CONTAIN with the number 13N16585.