Dr. Tiago Espinha Gasiba was born in Porto, Portugal. He received his engineering (Engº) degree from the Faculdade de Engenharia da Universidade do Porto (FEUP) in 2002, specializing in Telecommunications, Electronics and Computers. In 2002, he moved to Germany, where in 2004 he obtained his master's degree (M. Sc.) in Telecommunication Engineering from the Technical University of Munich (TUM). From 2004 to 2007 he attempted to obtain a PhD in telecommunications but decided against it to focus on practical work in the industry. He started working for Ericsson in 2007 in Nuremberg, where he remained for six years. During his work at Ericsson, Dr. Gasiba was part of a team that developed the first world-wide LTE mobile phone prototype. After leaving Ericsson in 2013 to NXP in Hamburg, Dr. Gasiba decided to shift his career focus to cybersecurity – this decision was motivated by his strong experience and interest in the field. During this time, he worked on the JavaCard Operating System (JACOP). In 2014, Dr. Gasiba joined Siemens AG in Munich, where he is still working today, and where he continues his strong focus on cybersecurity. He started as an incident handler, but quickly moved to the field of secure software development, where he established himself as a Senior Key Expert. In 2021 he obtained a PhD degree (Dr. rer. nat.) with high distinction (suma cum laude) from the Universität der Bundeswehr München (UniBwM). His PhD topic was on the field of cybersecurity and addressed the issue of "raising awareness of software developers towards secure software development". Dr. Gasiba has published several scientific articles and journal papers in international venues. One of his papers published in ACM has been distinguished with the "10-year impact award", and several papers have been distinguished with the "best paper" award. Through his work, Dr. Gasiba has supervised several master students and conducted several projects together with German and Portuguese universities. Dr. Gasiba lectured at the Technical University of Munich and delivered cybersecurity lectures at the Technische Hochschule Deggendorf. Dr. Gasiba holds several cybersecurity certifications, including CISM, CISSP, and GXPN. Additionally, Dr. Gasiba holds several patents in the field of mobile communications and cybersecurity. His free time is occupied by his lovely daughters and, whenever possible, with his enthusiasm for FreeBSD.

Serious Games for CyberSecurity

It is widely known and generally accepted that errors and vulnerabilities introduced during software development should be identified and fixed as early as possible – the later this happens, the higher the costs to fix and the higher the potential is for serious security threats. Ideally, vulnerable code should never leave the development environment and be present in any released software, i.e. should never hit any customer. However, we have seen again and again that this type of problem keeps on happening! Vulnerable software is present in products and services. Two recent prominent cases of the problems that vulnerable software can cause are illustrated by crowdstrike and log4j. There are several ways to address this issue, e.g. by means of SAST (static application security testing), code review, unit testing, fuzzing, and more recently through Artificial Intelligence (A.I.). All these methods employ technology as the main vehicle to address the issue. However, studies have shown that the problem is not only technical in nature, but also cause due to the human factor. Therefore, one possible way to address this problem, which focuses on individuals rather than technology, is by means of awareness and policy compliance. In this workshop, I will present and discuss the usage of serious games to achieve this goal. A serious game is defined as a game with *a purpose other than pure entertainment* [Dörner et al.] In our case, we make use of serious games to raise the awareness of software developers towards potential vulnerabilities in source code. This workshop will present the design of three serious games that have been developed, tested and validated in an industrial setting. We will explore the design criteria of these games and compare the design to existing games, in particular Capture the Flag (CTF) style of events. The first game we will discuss is the "CyberSecurity Challenges (CSC)", which adapts classical CTFs to industrial software developers. The second game we will present is the Cloud of Assets and Threats (CATS), which addresses the secure deployment of cloud infrastructure, e.g. in a DevSecOps context. Finally, the third game we will discuss is the DuckDebugger (DD), which aims to improve the security empowerment of software developers through the amelioration of code review practices. Not only will we discuss these games, but we will also give an overview of the motivating factors behind their development, it's design methodology (Action-Design Research [Sein. et. al]) together with its framing in the industrial context, present results from the evaluation obtained through industrial interventions, and finally discuss about the lessons learned over the last years of practice.