Denis Wambold

Personal Website | GitHub

EDUCATION

08/2025 - 11/2025 **Carnegie Mellon University, Pittsburgh** Visiting Student Researcher
- Writing my Master's Thesis @Cylab
- Domain: Explainability of ML-based Attack Detection for Industry Control Systems

10/2023 - 2025 **Karlsruhe Institute of Technology** MSc Computer Science
- Focus on Cybersecurity and AI
- Minor: Business Economics (Data Science)
- Current grade: 1.3 (German grading system)

10/2019 - 09/2023 **Karlsruhe Institute of Technology** BSc Computer Science
- Bachelor's Thesis: „Subspace Generative Adversarial Learning for Unsupervised Outlier Detection" with grade 1.0
- Minor: Business Administration
- Final grade: 1.9

SCIENTIFIC WORK

2024 *Generative Subspace Adversarial Active Learning for Outlier Detection in Multiple Views of High-dimensional Data* (Preprint)

2024 *Prompt Injection Attacks against LLMs* (Seminar)

WORK EXPERIENCE

10/2023 – 05/2025 **IONOS – Software Engineer for Technical Security | Working Student**
- Development of security tools for internal use, e.g. monitoring of self-maintained work stations, automated security incident alerting, micro service development

11/2023 – 01/2024 **IPD Böhm - Assisting Student Researcher**
- Co-authored a scientific paper building upon the results of my Bachelor's Thesis
- Designed and implemented experiments to benchmark the model introduced in my thesis

07/2021 - 06/2023 **EnBW – Data Analysis | Working Student**
- Data Analysis and User Management, development of an interactive real-time dashboard to support daily operations planning

PROJECTS & UNIVERSITY COURSES

2025 **Shelly – Natural language to CLI commands**
- LLM wrapper that translates natural language instructions into terminal commands
- Features: command safety checks, explanations and optional execution

05/2023 – 09/2023 **Bachelor's Thesis**
- Extension of the GAN-framework to combine the generative power of GANs with an architectural Ensemble structure, enabling the learning of feature subspaces
- Design & conduct experiments to evaluate the model's performance

2023-2025 **Relevant University Courses**
- Application Security, Penetration Testing, IT-Security, Software Security Engineering, Data Science, several Machine Learning courses (including Deep Learning, Neural Nets, ML for Natural Sciences, Security of ML), Formal Systems, Advanced Software Engineering