Denis Wambold

Personal Website | GitHub | X (Twitter)

EDUCATION

08/2025 - 11/2025 **Carnegie Mellon University, Cylab, Pittsburgh** Visiting Research Scholar

- Domain: Explainability of ML-based Attack Detection for Industry Control Systems

10/2023 - 2025 **Karlsruhe Institute of Technology** MSc Computer Science

- Focus on AI and Cybersecurity
- Minor: Business Economics (Data Science)

10/2019 - 09/2023 **Karlsruhe Institute of Technology** BSc Computer Science

- Bachelor's Thesis: „Subspace Generative Adversarial Learning for Unsupervised Outlier Detection"

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 paper building upon the results of my Bachelor's Thesis
- Domain: Extend the GAN architecture to allow anomaly detection in feature subspaces

07/2021 - 06/2023 **EnBW – Data Analysis | Working Student**

- Data Analysis, development of an interactive real-time dashboard to support daily operations planning

PROJECTS & UNIVERSITY COURSES

2025 **SecureSage – AI-Agent designed to conduct extensive code security analysis**

- Code review agent that uses static analysis, AST inspection, LLM reasoning, and dependency checks to identify and explain security vulnerabilities.
- Writes in-depth reviews highlighting critical sections and suggests fixes

2025 **LLM RL**

- Use Reinforcement Learning to improve the performance of LLMs on specific tasks
- Design evaluation environments, ranging from learning language dialects to security tasks

2025 **CTFs**

- Solve CTF challenges and produce write-ups for them

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