Stefano Simonetto, PhD candidate

stefanosimonetto98@gmail.com
linkedin.com/in/stefano-simonetto-7778771b1
https://scholar.google.com/citations?hl=it&user=tWPkBt8AAAAJ

I am a PhD candidate in Cybersecurity and Artificial Intelligence at the University of Twente, understanding and analyzing software vulnerabilities, leveraging machine learning and large language models to extract, structure, and map cyber threat intelligence. I have recently been exploring the security of large language models, with a particular focus on prompt injection.

Education

2022 – 2026 **Ph.D., University of Twente** Cybersecurity and AI
Visiting PhD (Feb–Jul 2026): National University of Singapore

2020 – 2022 **M.Sc. Electronic engineering and informatics**, Networks and IoT, University of Trieste.
U-blox internship, Security and communication.
Thesis: Systematic literature review of adversarial machine learning attacks against O-RAN.
Erasmus Exchange (Feb–Jul 2022): Technical University of Eindhoven

2017 – 2020 **B.Sc. Electronic engineering and informatics,** Telecommunication, University of Trieste.

Publications

1. S. Simonetto, R. Oostveen, T. S. van Ede, P. Bosch, and W. Jonker, "Knowing your weaknesses is your greatest strength: Mapping cve to cwe by leveraging cwe hierarchy with llms," in *ACM ASIA Conference on Computer and Communications Security (ASIACCS)*, 2026.
2. Y. A. Krijnen*, S. Simonetto*, R. Oostveen, P. Bosch, and W. Jonker, "Threatcompass: A tool for identifying and mapping security issues to ttps," in *Proceedings of the 2025 Workshop on Large AI Systems and Models with Privacy and Security Analysis*, 2025, pp. 58–67.
3. S. Simonetto, R. Oostveen, T. S. van Ede, P. Bosch, and W. Jonker, "Beyond cwes: Mapping weaknesses in unstructured threat intelligence text," in *International Conference on Cryptology and Network Security (CANS)*, 2025.
4. S. Simonetto, R. Oostveen, T. S. van Ede, P. Bosch, and W. Jonker, "What matters most in vulnerabilities? key term extraction for cve-to-cwe mapping with llms," in *International Conference on Cryptology and Network Security (CANS)*, 2025.
5. S. Simonetto, "Strengthening cloud applications: A deep dive into kill chain identification, scoring, and automatic penetration testing," in *International Conference on Research Challenges in Information Science (RCIS)*, Springer, 2024, pp. 111–120.
6. S. Simonetto and P. Bosch, "Comprehensive threat analysis and systematic mapping of cves to mitre framework," in *1st International Conference on Natural Language Processing and Artificial Intelligence for Cyber Security, NLPAICS 2024*, 2024.
7. S. Simonetto, T. S. van Ede, P. Bosch, and W. Jonker, "Text2weak: Mapping cves to cwes using description embeddings analysis," in *KDD workshop. 4th Workshop on Artificial Intelligence-Enabled Cybersecurity Analytics*, 2024.
8. S. Simonetto and P. Bosch, "Are we reasoning about cloud application vulnerabilities in the right way?" In *8th IEEE European Symposium on Security and Privacy (EuroS&P)*, 2023.

Teaching

2026 **Software Security** — Lecturer — Bachelor
Contributed to design and delivery of the class regarding insecure configurations and secure coding practices.

24-25 **Distributed Systems** — Lecturer — Master
Supported lectures and lab sessions on distributed systems principles, architectures, and system design fundamentals.

22-25 **Internet of Things** — Lecturer and Teaching Assistant — Master
Designed and delivered 3 lectures on (i) IoT security; (ii) communication protocols and (iii) edge-to-cloud communication and design, and supported lab sessions; developed teaching material from scratch for the first course edition.

2023 **Embedded Machine Learning** — Teaching Assistant — Master
Delivered lab sessions and hands-on instruction on embedded machine learning; supported practical exercises on deploying ML models on constrained devices.

22-23 **Pervasive Computing** — Lecturer — Master
Designed and delivered lecture a lecture on security in pervasive computing; covered threats and protections across the ISO/OSI layers and supported course activities.

Supervision

- Supervised 11 Bachelor's students,including the following selected projects:
  - Max Wijnbergen — *Bridging the Gap: From CWEs to TTPs in Cybersecurity Attack Kill Chains*
  - Jagvir Singh Bal — *Software Updates in Internet of Things Devices: Monolithic vs. Containerized*
  - Alexandra Diana Stefania Murgea — *Docker: Advantages and Security Implications of a Python Client–Linux Application*
  - Alen Badrajan — *Technical and Security Challenges of Cloud-Based Storage Management for IoT Devices*
  - Hugo Liam van Wijngaarden — *Tracking the Evolution: Uncovering Concept Drift in Vulnerability Descriptions Over Time*
  - Berry Dominguez Adilova — *From Descriptions to Decisions: Classifying Vulnerabilities by Information Sufficiency*

- Supervised/co-supervised 3 Master's students:
  - Yan Senko — *IoC to TTP & Identifying Malware Attack Techniques in Cyber Threat Intelligence*
  - Thanuja Pujari — *Multiagent-Vuln-Assist: Multi-Agent Support for Automated Pentesting in Dockerized Applications*
  - Carmen Veenker — *Anomaly Detection in API Calls to Web Services Using Deep Learning*

Languages

- Native Italian speaker.
  Fluent in English, with strong reading, writing, and speaking skills.
  Basic proficiency in Dutch.

Academic Service and Recognition

- **Presentations**: Presented research at venues including *ACCSS*, *ICT Open*, *Intersect Roundtables*, *FUSE5G*, and the *Annual Cyber Security Next Generation Workshop (CSNG)*, as well as in connection with submissions to major conferences such as *CCS* and *KDD*.

  Organization: Served as local organizer for the *Computer Security Foundations Symposium (CSF)* in Enschede.
  Interdisciplinary Collaboration: Collaborated on interdisciplinary projects involving applications of AI in management and decision-making contexts.
  Professional Development: Completed academic and professional development courses, including *Academic Integrity* and *Taste of Teaching*.
  Institutional Service: Served in the PhD Working Group, contributing to initiatives aimed at improving PhD progression and timely completion.
  Award: Best Poster Award, *5G Security: Are We Forgetting Someone?*, EEMCS Days, University of Twente.

References

- Dr. Peter Bosch (PhD Supervisor), University of Twente — `h.g.p.bosch@utwente.nl`
  Dr. Willem Jonker (PhD Supervisor), University of Twente — `w.jonker@utwente.nl`
  Dr. Özlem Durmaz (Group Chair), University of Twente — `ozlem.durmaz@utwente.nl`
  Dr. Thijs van Ede (Co-author), University of Twente — `t.vanede@utwente.nl`