# Gianluca **De Stefano**

*Muhlenstrasse 16, Saarbrücken, 66111, Germany*

(+39) 3403885257 | destgianluca@gmail.com | gianlucadestefano.github.io | Scholar


## Summary


I am a Ph.D. candidate at the CISPA Helmholtz Center for Information Security, where I research the application of advanced AI techniques to real-world cybersecurity challenges. My current work focuses on developing AI agents that automatically identify software vulnerabilities in web applications. I have practical experience applying machine learning to tasks such as code/data analysis and vulnerability detection. I actively follow and engage with the latest advancements in AI, with a strong interest in their security implications and potential for automation.

**Technologies:** Pytorch, Transformers, Unsloth, LLMs, Retrieval Augmented Generation, Langchain, Ai Agents, Sklearn, Python, JavaScript.

**Languages:** Italian, English, German


## Experience

### CISPA Helmholtz Center for Information Security
*Saarbrücken, Germany*

PhD student — *Aug. 2022 - Ongoing*

- **Rag and Roll**: framework to study Retrieval Augmented Generation pipelines under knowledge corruption attacks.
- **YURAScanner** (NDSS 2025): intelligent security scanner using LLMs for the detection of web vulnerabilities. (Follow-ups coming soon.)
- **Web rationales** (CHI 2025): study on web permission rationales using LLMs to distill crawled knowledge.
- **Call Me Maybe**: enhancing Javascript call-graph construction using graph neural network.
- Led the development of a RAG and an agentic pipeline to query the internal documentation.
- Managed students for internal projects and thesis.

### CISPA Helmholtz Center for Information Security
*Saarbrücken, Germany*

Internship — *Nov. 2021 - Aug. 2022*

- **Clickbait PDFs campaigns** (EURO S&P 2024): Built and deployed a system to cluster 4M+ malicious documents using a Siamese Networks and DBSCAN.

### MMLAB, university of Trento
*Trento, Italy*

Master thesis — *Apr.2021 - Mar. 2022*

- **Adversarial mimicry attacks against deep forensic detectors** (Pattern Recognition Letters 179): Novel adversarial attack against AI-based image forensics detectors, to conceal manipulations and induce false positive detections.

### PRIMA
*Trento, Italy*

Full-stack developer — *Jan. 2018 - May. 2021*

### Fondazione Bruno Kessler
*Trento, Italy*

Junior Research Assistant — *Jun. 2015 - Jul. 2015*

## Education

### University of Saarland
*Saarbrücken, Germany*

Erasmus program — *Sep. 2020 - Sep. 2021*

### University of Trento
*Trento, Italy*

Bachelor and Master degrees in Computer Science — *Sep. 2016 - Mar. 2022*

### Istituto Tecnico Economico Tambosi
*Trento, Italy*

Diploma in Computer Science & Economics — *Sep. 2011 - Jun. 2016*