# Michele Mastroberti

MicheleMastroberti • Mic52M • PersonalSite

## Education

**Master of Science in Cybersecurity** — **Milan, Italy**
*University of Milan* — *2023 – October 2025*
Thesis: *"Assurance Evaluation of AI Models"*
The thesis aims to define and implement assurance checks for artificial intelligence models. These checks are designed to ensure the models' compliance with the European AI Act, focusing on aspects that impact the final model and its application—such as the training dataset, the training process, and the resulting model. The evaluations assess several non-functional properties, including robustness to specific attacks and fairness.

**Bachelor of Science in Systems and Network Security** — **Milan, Italy**
*University of Milan* — *2020 – 2023*

**High School Diploma** — **Terni, Italy**
*Galileo Galilei Scientific High School* — *2015 – 2020*

## Work Experience

**Research Assistant for SesarLab**
*University of Milan* — *February 2024 – February 2025*

**Core Competencies and Research Interests:** Actively involved in research activities as part of the MUSAscarl initiative, focusing on the integration of trustworthy AI in public sector infrastructures. Specialized in the application and assurance of machine learning within distributed systems, with a particular focus on MLOps practices and the assurance of cloud-based systems. Expertise encompasses the development, deployment, and rigorous evaluation of machine learning models in distributed environments, ensuring reliability, scalability, and security in cloud infrastructures.

*Water Polo Instructor* — *September 2020 – September 2021*

*Lifeguard* — *Summer 2018, 2019, 2020*

## Projects

**Bachelor's Thesis: "Design and Implementation of a System for Analysis and Blocking of Malicious Encrypted Traffic"**:
The project concerned designing and implementing advanced network security probes, ensuring that the networks are monitored and secured against advanced threats in the form of encrypted traffic. With advanced monitoring and detection techniques, the system smoothly identifies and mitigates security threats through encrypted communications while keeping the network secure. The project penetrated the state-of-the-art cybersecurity methodologies and carried out an in-depth exploration of advanced techniques in network analysis and threat mitigation. The system proposed utilized a careful evaluation of diverse lightweight and modern technologies, including network fingerprinting, towards attaining accurate detections on network connections. With a comprehensive approach,

the project was using advanced tools and methodologies to lay a strong base for developing a dynamic solution that can handle encrypted communication—seamlessly integrating theoretical knowledge with hands-on innovation and skillfully navigating the intricate challenges posed by encrypted network traffic.

Mic/bachelor-thesis

**B. Future Challenge 2024**:
The B. Future Challenge, organized by BOOM Knowledge Hub, is a competition for students that fosters innovative solutions to environmental and social challenges. The initiative emphasizes sustainability and the creation of a positive societal impact, encouraging participants to design forward-thinking and impactful projects related to AI.

**On-going: AWS Certified Machine Learning Specialty 2025 - Hands On**:
Currently attending a hands-on course to prepare for the AWS Certified Machine Learning Specialty certification. The course provides in-depth knowledge of building machine learning models leveraging cloud services such as SageMaker and AWS AI frameworks.

**On-going: HuggingFace ML Games Course**:
Following the HuggingFace course on machine learning applications in video game development. The course focuses on leveraging large language models (LLMs) to enhance non-player character (NPC) behavior.

## Languages

**Italian**: Mother tongue

**English**: Cambridge B2 Level

**Chinese**: Beginner Level

## Skills

**Security and Security Assurance**: Network Monitoring and Analysis, Data Center Monitoring, Malware Analysis, Distributed Systems Security, Cloud Security, Cloud Infrastructure, Security Assurance, Network Analysis, MLOps, AI Assurance, Explainability.

**Tools and Languages**: Docker, Kubernetes, Prometheus, AWS Security Hub, Wireshark, Nmap, Metasploit, TcpDump, Zeek, Snort, Suricata, Bro IDS, Python, Bash, SciKit-Learn, TensorFlow, Keras, HuggingFace, XAI

*I authorize the processing of personal data according to Italian Law 196/03 and GDPR (EU Regulation 2016/679).*