ATHANASIA KOLLAROU

Email: athanasia.kollarou@ntnu.no | LinkedIn: https://www.linkedin.com/in/athanasia-kollarou/ | Gjovik, Norway

WORK EXPERIENCE

MSCA PhD Fellowship | NTNU: Norwegian University of Science and Technology *Aug 2025 - Present*

- TUAI: Towards an Understanding of Artificial Intellegence

Researcher | NTNU: Norwegian University of Science and Technology *Apr 2025 - Aug 2025*

- NEWSROOM EU Project

Researcher | Systems Security Lab – University of Piraeus *Nov 2023 – Mar 2025*

- **Lab Assistant:** Developed lab materials for Network Security and Information Security courses, focusing on CISCO setups, protocols, and DORA compliance.
- **Training Content Developer:** Created materials for workshops, CTF competitions (Pwn, Reversing, Cryptography, Web Exploitation, Forensics) and developed content for cyber games.
- **CTF Challenges:** Designed forensic challenges for the PMKD 2024 national CTF competition for schools in Greece. Developed cryptography challenges and workshop for the Hack and Learn 2024 event, organized by SSL and IEEE at the University of Piraeus.
- **European Research Projects:** Provided technical support and contributed to deliverable writing for European research projects.

Information Security Consaltant | Cyber Noesis *Mar 2023 – Oct 2023*

- **Client Management:** Managed multiple clients for Training, Awareness, and Phishing services, delivering custom solutions.
- **Training Development:** Designed cybersecurity courses and materials for seminars, tailored to various audience levels.
- **Phishing Campaigns:** Planned, executed, and analyzed phishing campaigns.
- **Awareness Programs:** Created cybersecurity awareness content, including graphical material, games, and organized live events.

EDUCATION AND CERTIFICATION

Master's Degree in Digital Systems Security | University of Piraeus *Oct 2023 - Feb 2025*
Grade: 9.79 /10 | **Thesis**: Comparative Analysis of Adversarial Attacks on AI Models

Bachelor's Degree in Digital Systems Department | University of Piraeus *Oct 2019 – Sep 2023*
Grade: 8.20 /10 | **Thesis**: Secure Authentication and Authorization for APIs and Users with Keycloak

Information Security Management Systems Lead Auditor ISO 27001:2022 *Nov 2024*
Issued by TÜV AUSTRIA Group

PUBLICATIONS

The Emerging Role of Large Language Models in Threat Modelling: A Survey | ICMI 2026, IEEE 5th International Conference on Computing and Machine Intelligence
Petter Buseth, Ahmed Walid Amro, Athanasia Kollarou, Michail Takaronis, Riku Lehkonen, Sarang Shaikh

Testing the limits: Exploring adversarial techniques in AI models | PeerJ Computer Science, 2025
Apostolis Zarras, Athanasia Kollarou, Aristeidis Farao, Panagiotis Bountakas, and Christos Xenakis

Data Poisoning in FL: Clipping Malicious Updates | Availability, Reliability and Security (ARES), 2025
Georgios Spathoulas and Athanasia Kollarou