Dimitrios Sofikitis

AI/ML Security Engineer

About Me

Passionate and results-driven Software Engineer with a strong foundation in AI, Cybersecurity and Consulting services

- ✉ d.sofikitis@icloud.com 🔗
- 🌐 dsofikitis.github.io 🔗
- in dimitrisofikitis 🔗

Skills

- Adaptability
- Critical Thinking
- Fast Learner
- Multitasking
- Problem Solving
- Project Management

Languages

- Native Greek
- English C2
- French B2

Hobbies

- Chess
- Coding
- Hackathons
- Seminars
- Photography
- Volunteering

Experience

Superbo AI
Hong Kong, SAR   Oct 2025 - Present

- **GenAI Trust & Reliability Engineer**
  Building safe, trustworthy generative AI systems. Developing evaluation frameworks for robustness and trustworthiness. Implementing MLOps pipelines for secure deployment. Mitigating critical AI risks including hallucinations, prompt injection, and adversarial attacks. Embedding reliability and trust throughout product development.

Hellenic Army
Greece   Nov 2024 - Jul 2025

- **Computer Programmer & Analyst** - **8 Months**

Energy Way O.E.
Athens, Greece   Jan 2024 - Nov 2024

- **Data Migration Consultant & Sales Advisor**
  Oversaw the seamless digital infrastructure migrations between digital platforms, ensuring compliance and customer satisfaction - **7 Months**

- **Digital Innovation Consultant**
  Drafting and evaluation of proposals for the "Digital Reform of Municipalities" co-funded ICT initiatives, assessing technical feasibility, budget alignment and implementation planning - **4 Months**

Academic Papers
During Bachelor Studies   Sep 2020 - Feb 2025

Stockholm University, Sweden
- **Paper** on "Applying Deep Learning and Data Analytics to identify Malware Attacks" - **3 Months**

University of Piraeus, Greece
- **Thesis** on "Information Security and Privacy in Smart Edge Computing and IoT Applications" with Prof. Stefanos Gritzalis - **1 Year**

Education

- **Bachelor's Degree in Software Engineering**
  Dept. of Digital Systems, University of Piraeus   2020 - 2025

Credentials

- **Fundamentals of Computer Science Course - 1 Month**
  by "The Johns Hopkins University", Anatolia College, CTY
- **ROS2 Programming Workshop - 2 Months**
- **58th and 59th Summer School of Sciences**
  Workshop & summer schools were hosted by NCSR 'Demokritos'
- **SOC Efficiency for the AWS Cloud Course by AWS & IEEE**
- **Data Analytics in Business Workshop by IBM Consulting**
- **Greece Section Co-Lead for IEEEXtreme 18.0**