Iason Somarakis

Heraklion, Greece | +30 (694)469-1325 | info@isomarakis.eu | https://isomarakis.eu

PERSONAL HIGHLIGHTS

- Over a decade of IT experience, with several years focused on engineering and cybersecurity.
- Participated in Capture the Flag (CTF) competitions, ranked in the **top 4% in Cyber Apocalypse 2024**, and top 10% on several occasions.
- Participated in specialized trainings by organizations including SANS (e.g., AD Attacks with Empire), and ENISA (e.g., NIS2018: Threat Intelligence and Incident Response).
- Achieved **Pro Hacker** rank in Hack the Box, ranked **391st** globally in 2024; aquired Hacker rank in TryHackMe, ranked in the top 9% globally.

WORK EXPERIENCE

RHEA Group | NEXOVA **Redu, Belgium**

External Contractor, Security Engineering *Aug 2022 - Present*

- Designed and delivered cybersecurity courses, hands-on labs, on topics such as CTFs, social engineering, OT/IT vulnerabilities in Modbus/OPC UA, and threats in satellite-ground communication.
- **Led and implemented a solution to simulate business, attack, and defense flows** in space manufacturing. Supporting tailored specification language, automated infrastructure provisioning and an event execution engine using Finite State Machines, leveraging **MITRE ATT&CK t**o model the cyber kill chain.
- **Developed an asset discovery solution** integrating network scanners and IT solutions, to map attack surfaces and create "evil twins".
- Developed diverse automation solutions and command-line tools to enhance lab and scenario development, including a wrapper for Metasploit's RPC API and a generator for malicious macro-enabled documents.

RAVEN Cybersecurity **Heraklion, Greece**

Founder, CEO, and CTO *Dec 2022 - Present*

- **Built and led a team of five** to deliver agile projects tailored to client needs, sourced and allocated resources, managed client relationships, established strategic partnerships to enhance business growth, and supervised financials.
- **Conducted security assessments,** including penetration tests, phishing campaigns, WiFi security, and physical security, and proposed customized mitigation strategies to reduce risk.
- **Managed post-incident investigations** for phishing and ransomware attacks, implementing remediation strategies to restore operations and prevent recurrence.
- Deployed Endpoint Detection and Response (EDR) solutions and integrated security tools like VPNs, **improving the cybersecurity posture of multiple businesses** and **mitigating hundreds of incidents.**
- Designed and maintained a testing environment using Proxmox, Virtual Machines, and Containers to simulate attacks and test security solutions.

SPHYNX Technology Solutions **Nicosia, Cyprus**
Software & Security Engineer *April 2018 - Oct 2022*

- **Led offensive security initiatives** and performed penetration tests and threat modeling across multiple sectors, including healthcare and energy.
- **Led a team and developed a cyber range product,** integrating threat modeling, infrastructure automation, including over a dozen tailored training modules.
- **Designed and implemented a dynamic testing product** for modeling and executing automated security assessments, integrating tools such as OpenVAS.
- **Directed and executed technical implementation** on EU projects, engineering solutions, designing threat scenarios, and integrating security solutions.
- Delivered field demonstrations to stakeholders, highlighting KPIs and the effectiveness of security implementations, leading to increased adoption of cybersecurity solutions and a reduced attack surface.
- **Published research papers** on **Cyber Ranges,** IoT, and Healthcare Security, and was recognized as **Employee of the Year (2020)** for outstanding contributions.

CURVATURE **Amsterdam, Netherlands**
IT Support & Administrator *Oct 2015 - Dec 2016*

- Managed Active Directory users and policies, ensuring secure access and compliance across branches.
- Enforced data protection, access controls, and network security measures, reducing the attack surface and potential vulnerabilities.

EDUCATION

Hellenic Mediterranean University **Heraklion, Greece**
Bachelor of Science (B.S.) in Information Engineering *Sep 2010 - Sep 2018*
Thesis: LSTM Network Intrusion Detection

City University of London **London, UK**
[Withdrawn] Doctor of Philosophy - PhD *Sep 2019 - Sep 2024*
Thesis: Asset and Threat Emulation for Cybersecurity Training

SKILLS

Engineering	Python3, Docker, Powershell, Bash, Ansible, VMWare vSphere, AWS, Terraform, GNS3, Django, ChatGPT, C#
Offensive Security	Burp Suite, Nessus, GoPhish, Cobalt Strike, Sliver, MSF, Web Fuzzing Tools, Cracking Tools, Mobsf, OSINT Tools, WiFi Pineapple, FlipperZero, iCopy-X
Defensive Security	OpnSense, Acronis Suite, Malcolm, MISP, Elastic, Wireshark, Snort, T-Pot, YARA
Cybersecurity Frameworks & Standards	ATT&CK MITRE, OWASP, STRIDE, NIST CSF, PTES, EBIOS