Afonso Gomes

Security Engineer / Software Engineer

Faro, Portugal • afonsopamg@gmail.com • LinkedIn: afon-gomes • GitHub: AfonsoG6

PROFESSIONAL EXPERIENCE

S21SEC — **PORTUGAL (REMOTE)**
Malware Analyst — **MAR 2024 - Present**

- **Analyzing EDR and XDR Incidents:** Working with platforms like Microsoft Defender for Endpoint, CrowdStrike Falcon, Palo Alto Networks' Cortex, Trellix Endpoint Security, and SentinelOne Singularity. Resolved more than 250 incidents in less than 6 months.
- **Investigating Malware Campaigns:** Conducting thorough investigations and reporting on active or recently active malware campaigns. Responsible for performing approximately 1 investigation per month.
- **Creating Detection Rules:** Developing detection rules to identify threats effectively.
- **Developing Automation Scripts:** Taking the initiative to create helpful scripts that support everyday tasks performed by the team.
- **Purple Team:** Collaborating in purple team exercises to identify successful attack vectors and improve the detection and blocking capabilities of the EDR and XDR platforms.
- **24/7 Incident Response:** Providing 24/7 on-call support to critical incidents. Successfully contributed to the mitigation of an actively spreading ransomware attack that affected over 400 devices.

FREELANCE — **PORTUGAL (REMOTE)**
Security Researcher — **Jan 2024 - Present**

- Part of the Red Team for a scientific paper entitled "Prompt-to-SQL Injection Attacks in LLM-Integrated Web Applications: Risks and Defenses" (accepted at ICSE'25).
- Developing and enhancing resources for the highly successful course of Forensics Cybersecurity at Instituto Superior Técnico. These resources include Lab tutorials for students and project generation guides and documentation for future teaching assistants.

CISCO — **LISBON, PORTUGAL**
Technical Consulting Engineer / Network Engineer (Internship) — **Sep 2023 - Feb 2024**

- Completed the CCNA, Devnet and CyberOps certifications.

INSTITUTO SUPERIOR TÉCNICO (UNIVERSITY OF LISBON) — **LISBON, PORTUGAL**
Teaching Assistant — **Sep 2022 – Feb 2024**

- Taught practical classes in Forensics Cyber-Security (twice), Network and Computer Security and Computer Networks to a total of over 150 undergraduate students.
- Planned around 50 classes and helped design and grade projects.
- Coordinated with faculty members to align course content with department goals.
- Assisted students with their projects during extra-class hours, providing guidance and support to enhance their learning experience.
- Awarded 4 Diplomas of Teaching Excellence based on exceptionally high evaluations and feedback from students.

EDUCATION

INSTITUTO SUPERIOR TÉCNICO (UNIVERSITY OF LISBON) **LISBON, PORTUGAL**
Master's degree in computer science and engineering (Specialization in Cyber-Security) **Graduated in 2023**

- Achieved top of the class grades in:
  - Forensics Cyber-Security (Top 8%).
  - Network and Computer Security (Top 1%).
  - Software Security (Top 4%).
- Awarded a Diploma of Academic Merit (2022/2023).

INSTITUTO SUPERIOR TÉCNICO (UNIVERSITY OF LISBON) **LISBON, PORTUGAL**
Bachelor's degree in computer science and engineering **Graduated in 2021**

- Achieved top of the class grades in:
  - Object-Oriented Programming (Top 5%).
  - Introduction to Algorithms and Data Structures (Top 4%).
- Awarded 2 Diplomas of Academic Merit (2019/2020 and 2020/2021).

CERTIFICATIONS

CISCO
Cisco Certified CyberOps Associate **Feb 2024**

CISCO
Cisco Certified Devnet Associate **Dec 2023**

CISCO
Cisco Certified Network Associate (**CCNA**) **Nov 2023**

FORTINET
NSE: Network Security Associate **Mar 2023**

ADDITIONAL INFORMATION

Programming:	Python | Java | C | C++ | C# | Shell | JavaScript | SQL
Technologies:	Linux | Git | Docker | Unity | Maven | Gradle | Android SDK | gRPC | Py Flask | Py Requests
Cyber-Security:	Ethical Hacking | Cryptography | Firewalls | Forensics | OWASP Top 10 | Wireshark OpenSSL | Kali-Linux | EDR/XDR | Reversing | Malware | MITRE ATT&CK
Spoken languages:	English (Fluent), Portuguese (Fluent), Spanish (Intermediate)