

João Miguel de Sousa Ferro

Cybersecurity Analyst | SOC & Purple Team

Lisbon, Portugal joaoferro.contact@gmail.com joaoferro.pt

linkedin.com/in/joaomdsferro github.com/joaomdsferro

Summary

Cybersecurity Analyst in Worten's SOC, focused on alert triage, lead-driven threat hunting and purple-team work (exposure investigations, pentest support). Background in GRC and security engineering: built Python (Django/FastAPI) platforms that automate Security by Design for **500+ application components** and centralize vulnerability management.

Experience

Cybersecurity Analyst, Worten Portugal – Lisbon, Portugal Jan 2026 – present

- **SOC Monitoring & Incident Response:** Triage and investigate alerts in **Microsoft Sentinel** and **Palo Alto Cortex XDR**, performing root-cause analysis and escalation, with automation through **Cortex XSOAR**.
- **Threat Hunting:** Run lead-driven hunts from **Recorded Future** intelligence and OSINT, adapting and tuning **KQL/XQL** queries to scope exposure across the environment.
- **Purple Team:** Investigate credential leaks and external exposure through dark-web monitoring, and support pentests by validating findings and their remediation.
- **SIEM Modernization:** Co-lead the technical evaluation of next-generation SIEM platforms (**Datadog Cloud SIEM**, **Cortex XSIAM**), including vendor and commercial discussions.
- **Phishing Awareness:** Support monthly **KnowBe4** simulations reaching **~1,500 employees/month**, with the click rate falling from **11% to 5%** (Jul–Sep 2026).
- **Vulnerability Management:** Lead developer of a **FastAPI/Next.js** platform centralizing vulnerability management across **Qualys** and **Trivy** findings (thousands of vulnerabilities).

GRC Analyst, Worten Portugal – Lisbon, Portugal Sept 2024 – Dec 2025

- **Security Engineering:** Architected and built a **Django** platform that automates Security by Design requirements and TPRM for **500+ application components**, replacing manual risk assessments.
- **DevSecOps:** Integrated security gates (**SonarQube**, **Trivy**) into **GitLab CI/CD** pipelines.
- **Risk Visualization:** Built Power BI dashboards for risk-based decision-making.
- **Phishing Simulations:** Managed enterprise-wide **KnowBe4** campaigns across a ~5,000-employee organization.

Projects

Personal Security Lab & Systems Research

- Maintain a self-hosted **Fedora Server** infrastructure acting as a service provider for tools such as **Vaultwarden, Portainer, and Uptime Kuma** (and many others).
- Utilize a **CachyOS (Arch-based)** workstation as a primary environment for development and **security research**, utilizing virtualization for **network security testing**.
- Manage service containerization and orchestration via **Docker**, focusing on infrastructure availability and **container security** experimentation.

Education

Iscte - Instituto Universitário de Lisboa, BSc in Computer Science & Business Management – Lisbon, Portugal — Sept 2020 – July 2024

- **Relevant coursework:** Cybersecurity Fundamentals, Software Architecture, Web Development, Project Management
- **Leadership:** AIESEC Director of Finance & Operations (managed a €10k+ budget); Spark Agency Ambassador; Team Leader (2022-23)
- **Achievement:** Co-founded "Finance 101", winner of Lisbon's Junior Achievement startup competition

Skills

Security Operations: Microsoft Sentinel (KQL), Palo Alto Cortex XDR (XQL) & XSOAR, Recorded Future, VirusTotal, MITRE ATT&CK

AppSec & Vulnerability Management: Qualys, Trivy, SonarQube, OWASP Top 10, CWE, Security by Design, TPRM

Languages: Python (FastAPI, Django), Bash, JavaScript, React/Next.js

Systems & Cloud: Linux (Fedora Server, Arch), Docker, custom security tooling, AWS, Azure AD, GCP (basics), GitLab/GitHub CI/CD

Databases: PostgreSQL, SQLite, MongoDB

Languages

Portuguese: Native

English: Proficient | Cambridge English C1 Advanced (CAE)

Spanish: Beginner