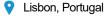
### **PERSONAL INFORMATION**

## Pedro Manuel Branco Fernandes





(+351) 967 427 924



www.pedrof.com

Sex Male | Date of birth 1988-11-22 | Nationality Portuguese



### **PROFESSIONAL OBJECTIVES**

I am an **Information Technology** and **Cybersecurity** professional, with experience in network management, security policies and **Blue Team** Operations, including response to information security incidents.

I'm looking for a role as a **Cybersecurity Engineer**, **SOC Analyst** or similar, where I can use my knowledge to strengthen the security of systems, information and people. What inspires me is investigating, learning, helping, designing solutions and creating a positive impact.

# **WORK EXPERIENCE**

Since 2025 • National Cybersecurity Centre of Portugal, part of the National Security Cabinet of Portugal - Cybersecurity Engineer

2024 - 2025 • Microsoft - Cybersecurity Support Engineer, focused on Microsoft Defender for Endpoint (MDE)

2023 - 2024 • MondegoData - Systems Administration, Cybersecurity and Technical Support in Retail, Industry and Healthcare

2018 - 2023 • Info2000 - Systems Administration, Cybersecurity Analysis and Technical Support, mainly in the Opticians area

2014 - 2017 • Orbital Apps - Design and implementation of platform for Portable Apps on Linux

2013 - 2014 • Loja Bitcoin - Bitcoin Store - Sales, managing orders, and customer support

2011 - 2012 • Faculty of Arts and Humanities, University of Coimbra - Preparing new computers, updating software and Technical Support

# **EDUCATION AND CERTIFICATES**

2024 • Microsoft Defender for Endpoint ★ | Microsoft Sentinel ★ | Microsoft Defender for Cloud ★ | Microsoft Defender XDR ★

2023 • Certified Ethical Hacker (CEH), EC-Council ★

Introduction to Classified Information Security, National Security Cabinet of Portugal ★

■ Implementation of ISO 27001 Information Security Management Systems, SGS ★

• 18<sup>th</sup> General Cybersecurity Course, National Cybersecurity Centre of Portugal ★

Network Security Essentials, WatchGuard ★

2017 - 2018 • <u>IT Technician Academy</u>, Rumos ★
2003 - 2006 • Computer Science Course, Dr. Joaquim de Carvalho Secondary School, Figueira da Foz ★



Microsoft



### **TECHNICAL SKILLS**

- Threat Hunting with Sysinternals tools, Wireshark, VirusTotal and sandboxing tools like Hybrid Analysis and Any.run
- Analysis of documents for malware, including malicious links and Macros; Analysis of email headers, to detect phishing
- Investigating IP addresses, including location and ASN; Investigating domain names, including DNS records and WHOIS
- Assessment of security vulnerabilities (CVE) in networks and systems, with Nessus and Kali Linux
- Windows operating system hardening with Secure Boot, Core Isolation, Controlled Folder Access and ASLR
- Implementing secure remote access via VPN, including site-to-site: OpenVPN, WireGuard, L2TP/IPsec, SSTP and SoftEther
- Endpoint Security (Antivirus, EPP, EDR) with cloud management: Microsoft Defender for Endpoint, WatchGuard and ESET
- Entry-level understanding of Microsoft Defender for Cloud and SIEM tools: Microsoft Sentinel and AlienVault
- Familiar with Cybersecurity frameworks like MITRE ATT&CK and the Cyber Kill Chain
- Implementation of GDPR compliance, including encryption with BitLocker and secure data deletion
- Managing Virtual Machines on Azure and AWS; On-prem virtualization with Microsoft Hyper-V and VMware ESXi
- Managing networks (LANs and VLANs); Implementing and managing DNS-based URL filtering at the network level
- Managing routers, switches and firewalls: WatchGuard, Ubiquiti, Aruba, TP-Link, DrayTek, MikroTik, pfSense and OpenWrt
- Support and Administration of Windows Server, Windows Client, and Linux: Debian and Ubuntu Server
- Managing Active Directory, Entra ID (Azure AD), Group Policy (GPO) and Microsoft 365; Supporting Microsoft Office
- Managing Servers with Microsoft Management Console (MMC), Windows Admin Center and Microsoft Remote Desktop
- Supporting Windows, macOS, iOS and Android systems that connect via VPN to Virtual Desktop Infrastructure (VDI)
- Scripting and automation with PowerShell, batch and Bash; Limited usage of .NET, C#, VBS and Python
- Experience with protocols: TCP/IP HTTP HTTPS FTP DNS DHCP ICMP SSL/TLS SSH RDP SMB POP3 IMAP SMTP
- Experience investigating and solving complex technical issues, often at the intersection of multiple products
- Focus on customer success, delivering solutions while having minimal impact on business operations and respecting SLAs
- Passion for continuous learning and training, to be able to address new challenges and deliver more value to the business

#### **PROJECTS DEVELOPED**

CloudVPN: Connectivity without configuring routers | CloudBackup: ransomware-proof backups on AWS | SuperOS: Linux Distribution with 500 000+ downloads