PERSONAL INFORMATION

Pedro Manuel Branco Fernandes

Lisbon, Portugal
(+351) 967 427 924
hello@pedrof.com
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.

TRAINING RECEIVED FROM

WORK EXPERIENCE

Since 2025

National Cybersecurity Centre | National Security Cabinet | Portugal
Cybersecurity Engineer

Note: Specific details are confidential due to National Security reasons

- Cooperating with the SOC (Security Operations Center), to Investigate Security Incidents
- Cooperating with CERT.PT (Computer Emergency Response Team), providing technical assistance
- Using MITRE ATT&CK to understand the TTPs (Tactics, Techniques, and Procedures)
- Vulnerability assessment and patching management
- Investigating suspected phishing emails
- Systems Hardening, for increased security
- Maintaining IT Infrastructure, including virtualization and servers

© 2025 Pedro Fernandes

WORK EXPERIENCE

2024 - 2025

Microsoft

Microsoft

Cybersecurity Support Engineer, working on Microsoft Defender for Endpoint (MDE)

At Microsoft, I worked as a **Technical Support Engineer** with **Microsoft Defender for Endpoint** (MDE), delivering solutions to large-scale enterprise customers, as part of the **Microsoft Security** business unit, also known as Security, Compliance, Identity and Management (SCIM).

My team's focus was on Microsoft's strategic customers, the S500, which includes Banking, Airlines, Energy, Healthcare, Car manufacturing, Telecoms, telecommunications and networking infrastructure, Nanotechnology and Semiconductor Equipment Manufacturing, Retail, Pharmaceutical, Insurance, Global Consumer Goods, Food and Beverages, Software Development and Delivery, Transportation and logistics, Law firms, Hotel management, Consulting, and Government sector, including agencies of the European Union.

The day-to-day work consisted of assisting Cybersecurity Analysts, Security Operations (SOC and SecOps), Global Security Operations Center (GSOC), MSPs, MSSPs and IT teams, helping fix technical issues and providing advice.
I helped with diagnosing, investigating and troubleshooting to provide solutions related to Defender for Endpoint
Previously: Advanced Threat Protection

I also assisted Microsoft's CIRT (Cybersecurity Incident Response Team) to respond and contain ongoing Cyber attacks by APTs (Advanced Persistent Threats), by cooperating with international teams to deliver timely and effective mitigations.

I also worked with other internal security teams, like Microsoft Defender for Office 365 (MDO), Microsoft Defender for Cloud Apps (MDC), Microsoft Defender for Identity (MDI) and Purview (DLP).

- Antivirus (AV), EDR, EPP
- Alerts and Incidents, XDR
- Microsoft Defender Vulnerability Management (MDVM)
  - previously: Threat and Vulnerability Management (TVM)
- Secure Score and Exposure score
- Onboarding and offboarding devices into Defender for Endpoint, also using the Unified Agent
- Real Time Protection
- Tamper Protection
- Attack surface reduction (ASR) rules
- Controlled Folder Access (CFA)
- Live Response
- Isolation of devices
- Automatic Attack Disruption and User Contain
- Investigate Indicators of Compromise (IoC): Domain, URL, IP and Certificate Indicators
- URL Blocking, Smart Screen, Network Protection and Web filtering
- Advanced Hunting
- Kusto Query Language (KQL)
- Microsoft Graph API
- Device Discovery
- Antivirus and EDR Exclusions
- Reproducing Cyber attacks and attack vectors
- Working with the *Microsoft Security intelligence* team (WDSI) to help determine False Positive and False Negative detections

© 2025 Pedro Fernandes

WORK EXPERIENCE

2023 - 2024

MONDEGODATA & Business Services, Lda

MondegoData & Business Services, Lda
Cybersecurity and IT Consulting

Note: MondegoData bought the company Info2000 in 2023

- Incident response to Cyberattacks
- Supporting customers in the following areas:
  - Opticians
  - Retail commerce
  - Healthcare
  - Recycling Industry
  - Metalworking Industry
  - Glass Industry
  - Coffee shops and Pastry Shops
- Routers e Firewalls
  - WatchGuard
  - Ubiquiti
  - Untangle
- VPNs
  - Ubiquiti
  - ZeroTier
  - SoftEther
- Supporting computers and servers
  - Windows 10
  - Windows 11
  - Windows Server
  - Ubuntu Server
- Supporting macOS
  - Installing applications from the App Store and via .dmg and .pkg files.
  - VPN Configuration
  - Remote Desktop configuration (RDP and VDI)
  - Installing applications, including Antivirus
  - System and Application updates
- Endpoint security with cloud management: WatchGuard and ESET
- Supporting business management software and POS (Point of sale)
  - Eticadata
  - Wintouch
- Managing Microsoft 365 licensing
  - Buying license keys
  - Installation and activation
  - Renewing existing account
- Incident response to website cyberattacks
  - Detecting and removing Web shells
  - Recovery and restoring of the website
  - Coordinating with the vendors of the web hosting service
- Installation and configuration of QNAP, NAS (Network Attached Storage)
  - Installing hard drives
  - Initial setup and configuration
  - Network configuration: Static IP, subnet mask, Gateway, and DNS
  - Configuration of hard drives in mirrored mode
  - Troubleshooting issues and escalation to the manufacturer, when necessary
  - Configuring of shared folders, users, groups, and permissions
  - Configuring access to network shares, on Windows
  - Setup the synchronization between two NAS devices in different locations, for backups
  - VPN configuration using QVPN
  - Configuration of NetBak Replicator, for workstation backups
- Installing and configuring thermal printers
- Installing and configuring Microsoft SQL Server

© 2025 Pedro Fernandes

WORK EXPERIENCE

2018 – 2023

Info2000 - Sinergias Empresariais, Lda
Cybersecurity and IT Consulting

- Incident response to Cyberattacks
- Support to customers mainly in the areas of Opticians, Recycling industry, Metalworking Industry, Glass Industry, Clothing and Accessories stores and Restaurants
- Coordinating and implementing information security policies
- Mitigating ongoing cyberattacks against Microsoft Remote Desktop (RDP) services
- System and Network hardening, including management of security updates and patches
- Managing routers and Firewalls:
  - WatchGuard, DrayTek, pfSense, ClearOS, Cisco Meraki, MikroTik and GL.iNet (OpenWrt)
- Managing ISP routers from MEO (Altice), Vodafone, NOS and Cabovisão:
  - Fiber Optic, DSL, Coaxial Cable and cellular network (3G / 4G)
- Implementing remote access via VPN: L2TP/IPsec, SSTP, SoftEther, OpenVPN and WireGuard
- Network segmentation (Ethernet and Wi-Fi) with routers, Access Points and VLANs
- Wireless Access Point (Wi-Fi AP) Configuration: Aruba and TP-LINK
- Configuring redundant internet access, with cellular network (WAN Failover)
- Assessment of security vulnerabilities in networks and systems, with:
  - Nessus Vulnerability Scanner e Kali Linux
- Managing Active Directory, Group Policy, Microsoft 365 and Google Workspace (G Suite)
- Managing domains, web hosting and emails with WHM (Web Host Manager) and cPanel
- Support and maintenance of end user operating systems: Windows and macOS
- Administration and maintenance of Windows and Linux servers: Windows Server and Ubuntu
- Endpoint Security with cloud management: WatchGuard and ESET
- Standalone Antivirus: Microsoft Defender, Kaspersky, AVG, Malwarebytes and Norton 360
- Virtualization with VMware ESXi, Microsoft Hyper-V and Proxmox
- Installation, configuration and administration of Windows Server Core and Hyper-V Server
- Interventions on desktop computers:
  - Replacing HDD disks with SSD
  - Replacing disks due to wear
  - Installing RAM memory modules
  - Replacing power supplies
  - Internal cleaning with compressed air
- Interventions on laptop computers:
  - Replacing HDD disks with SSD
  - Installing RAM memory modules
  - Replacing the battery
- Installation of Gigabit networks with Cat 6 UTP Ethernet cable, including termination with RJ45 connectors
- Installation and configuration of office and store printers:
  - HP, Brother, Epson, Xerox, Kyocera, Konica Minolta, Ricoh, Toshiba, among others
- Installation and configuration of computers:
  - HP, Dell, Acer, ASUS, Lenovo and Toshiba
- Installation and configuration of servers:
  - HPE, Dell, Lenovo and Fujitsu
- Configuration of PINs for logging into computers, with Windows Hello
- Installation and configuration of USB barcode readers, wired and wireless:
  - Zebra and Honeywell, among others
- Installation and configuration of UPS (Uninterruptible Power Supply), including battery replacement
- Installation and configuration of label printers, for product labeling
- Remote Technical Support by phone, email, SMS and WhatsApp
- Onsite technical assistance regarding computers, servers and networking equipment
- Implementation of GDPR compliance, including encryption with BitLocker and secure data deletion
- Creating documentation for internal use and for clients

© 2025 Pedro Fernandes

WORK EXPERIENCE

2014 – 2017

Orbital Apps
Portable Apps for Linux

- Design, planning and development
- Programming and development of the web platform
- Architected the ORB (Open Runnable Bundle) format, a container for the Applications
  - Based on ISO 9660 file format
  - Documented and published the ORB Specification as open-source and royalty-free
- Developed the runtime to be included in each ORB file
  - Developed using Bash, in order to be cross-platform across Linux distributions and architectures
  - Includes both machine-readable and human-readable data
- Developed ORB Launcher: Software that can be installed on the user's computers, to allow the easy launch of ORB Applications with one click
  - Automatically downloads from the internet the digital signature (PGP) associated with each ORB, to verify the file authenticity and security
- Developed the "ORB Creator": to package software from several sources into an ORB
  - Packages software that is already portable and includes dependencies either as separate files or is statically linked
  - Packages software from APT (Advanced Packaging Tool) software repositories
  - Creates "SuperDebs": the .deb files of an application and dependencies, which can then later be installed completely offline due to a custom-developed installer, developed in Bash
- Developed a set of Bash scripts to automate the generation of web pages for each ORB application
  - Populated with each ORB file's metadata
  - Adds the application logo from the .deb package
  - Adds the download URL

2013 - 2014

Loja Bitcoin
Bitcoin Store - Selling of Bitcoin cryptocurrency

- Development of the website, based on WordPress
- Marketing
- Sales and payment processing
- Customer Service and Technical Support
- Advising users regarding Bitcoin wallets and appropriate computers security measures

2011 - 2012

1 2 9 0
FACULDADE DE LETRAS
UNIVERSIDADE D
COIMBRA

Faculty of Arts and Humanities, University of Coimbra
Technical Support

- Setting-up new computers
  - Unboxing and setting-up computers in place
  - Setting up peripherals: monitor, mouse and keyboard
  - Connecting computers to the ethernet network
  - Updating and setting-up the required software
- Maintenance and updating software, including the operating system and applications
- Technical Support to end-users

© 2025 Pedro Fernandes

EDUCATION AND TRAINING

2025	eID (Electronic Identification) and Electronic Certification, INA and GNS ★
2025	CSIRT in a Box: Initial Training for Incident Response Teams, FCT ★
2024	Endpoint Protection - Microsoft Defender for Endpoint, Microsoft internal training ★
2024	Introduction to Microsoft Defender XDR, Microsoft ★
2024	Introduction to Microsoft Defender for Endpoint, Microsoft ★
2024	Introduction to Microsoft Sentinel, Microsoft ★
2024	Introduction to Microsoft Defender for Cloud, Microsoft ★
2024	Foundations of Cybersecurity, Google ★
2023	Certified Ethical Hacker (CEH), EC-Council ★
2023	TP-Link Network Associate Enterprise Wireless (TPNA), TP-Link ★
2023	Introduction to Classified Information Security, National Security Cabinet of Portugal ★
2023	Implementation of ISO 27001 Information Security Management Systems, SGS ★
2022	Cyberinformed Citizen, National Cybersecurity Centre of Portugal ★
2022	Cybersecure Citizen, National Cybersecurity Centre of Portugal ★
2021	18th General Cybersecurity Course, National Cybersecurity Centre of Portugal ★
2021	2nd General CyberHygiene Course, National Cybersecurity Centre of Portugal ★
2020	Metasploit Advanced, CyberS3c ★
2020	Ethical Hacking Fundamentals, CyberS3c ★
2020	Network Security Essentials, WatchGuard ★
2017 - 2018	IT Technician Academy, Rumos ★
2009 - 2012	Attended the Art History course Faculty of Arts and Humanities, University of Coimbra
2006 - 2007	Attended the Informatics Engineering course Faculty of Science and Technology, University of Coimbra
2003 - 2006	Computer Science Technological Course ★ Dr. Joaquim de Carvalho Secondary School, Figueira da Foz
2003	Completed the 9th Grade, being considered the best student of the year ★ Dr. Joaquim de Carvalho Secondary School, Figueira da Foz

© 2025 Pedro Fernandes

PERSONAL SKILLS

Mother tongue Portuguese

Other language(s)

	UNDERSTANDING		SPEAKING		WRITING
	Listening	Reading	Spoken interaction	Spoken production	
English	C2	C2	C2	C2	C2
Spanish	B1	A1	A1	A1	A1

Communication skills

- Ability to communicate in a clear and concise manner
- Experience with customer service and sales, dealing with clients in Portugal and the rest of the world - mainly Europe, South America and North America; communicating in English and Portuguese
- Capable of communicating technical concepts in a simple and accessible manner

Organisational / managerial skills

- Rigorous and with strong quality control
- Ability to learn and adapt to new situations
- Capable of establishing priorities

Digital competence

	SELF-ASSESSMENT			
Information processing	Communication	Content creation	Safety	Problem solving
Proficient user	Proficient user	Proficient user	Proficient user	Proficient user

Computer Science Technological Course (3 years)

Additional Technical skills

- Administration of Windows servers: Malware detection and removal, monitoring using Batch scripts, updating Operating System and Applications, managing permissions and user accounts
- Administration of Linux and Unix-Like servers - Access with SSH, Managing OS updates, software installation, automation of tasks with Bash scripts, diagnostic and problem resolution
- Using Sysinternals tools, like Process Explorer, Autoruns and TCPView
- Configuring VPNs for remote access on Windows, macOS, Android and iOS devices
- Disk cloning and imaging using Acronis True Image, Macrium Reflect, Norton Ghost and Disk2vhd
- Managing disks using Windows Disk Management, DiskPart, MiniTool Partition Wizard and GParted
- Experience with desktop virtualization: VMware Workstation and Oracle VirtualBox
- Remote access using TeamViewer, AnyDesk, N-Able Take Control (formerly SolarWinds), SupRemo, UltraVNC, RustDesk and Microsoft Remote Desktop (RDP)
- Managing servers with HPE iLO, Windows Admin Center and VMware Remote Console
- Using Backup Software: Veeam, Cobian Backup and Cobian Reflector
- Installing and configuring printers (USB, Ethernet and Wi-Fi), locally and for Remote Desktop
- Source-code versioning using Git and GitLab
- Configuring NAS (Network Attached Storage): QNAP, Synology and openmediavault
- Implementing Secure Boot by enabling the settings in the UEFI Firmware (BIOS)
- Configuring redundant disks, in RAID 1 (mirror mode)
- Creating network diagrams and IT infrastructure documentation
- Experience working with Office tools: Microsoft Word/Excel/PowerPoint, OpenOffice and LibreOffice
- Creating documents in HTML, PDF, wikitext (MediaWiki/Wikipedia) and text with Markdown
- Image editing with Adobe Photoshop

Other skills

- Knowledge of Intellectual Property: Copyright, Patents and Trademarks
- Experience receiving payments via Bank Transfer, PayPal and Bitcoin
- Bricolage and “Do it yourself”

Driving licence

- Driving License for cars - Class B

© 2025 Pedro Fernandes

ADDITIONAL INFORMATION

Presentations

- 2020 - Authored and presented Cybersecurity and Remote Work - PWS Consulting

Projects

- **Fixer for CrowdStrike incident**: Tool to fix the faulty CrowdStrike update
- **CloudVPN**: Connectivity between computers, encrypted, without configuring routers or Firewalls
- **SoftEther Installer**: All-in-one tool to automatically provision SoftEther VPN Server on Linux, supports more than 15 parameters. Compatible with Debian, Ubuntu and Raspberry Pi OS
- **Daily Backup**: Backup Windows folders, encrypted, with configurable retention (up to 365 days), backup to/from: Local Folders, Network Shares and USB Drives
- **Kali Linux Updater**: Easily update and upgrade the system, with a graphical interface
- **Zenmap installer for Kali Linux**: Installs Zenmap onto Kali Linux, automatically downloads dependencies, converts and install the packages and sets the correct launching parameters
- **CloudBackup**: Backups highly resistant to malware and ransomware, encrypted, on AWS Cloud (Amazon Web Services), S3, made with Lazarus IDE and Object Pascal
- **Passphrase Generator**: Create phrase-based “passwords”, graphical application, made with Visual Studio, C# and .NET
- **XMRig Detector**: Tool to detect instances of unauthorized Cryptocurrency mining, using hashes
- **Open Runnable Bundle (ORB)**: File format based on the ISO 9660 standard, used for Orbital Apps
- **AppRunner**: Application to easily run scripts and executables on Linux systems
- **CD2USB**: Windows graphical application to easily create a bootable Linux LiveUSB, using an ISO, CD/DVD, or by automatically downloading the required file; was included in SuperOS
- **SuperOS**: Originally called “SuperUbuntu” - Linux Distribution based on Ubuntu, totalling more than half a million downloads and reaching Top 10 at DistroWatch

Honours and awards

- Best student of the 9th Grade in 2002 / 2003 - Dr. Joaquim de Carvalho Secondary School ★

Event Participation - Offline

- 2024 - C-DAYS 2024 - conference organised by the National Cybersecurity Centre of Portugal ★
- 2024 - Workshop Reverse Engineering of Malicious Scripts on Windows, CERT.PT ★
- 2019 - BSides Lisbon 2019 - information security conference
- 2019 - Cyber-hygiene awareness event, by the National Cybersecurity Centre of Portugal ★
- 2018 - Hacking Kung Fu: The best defense is knowing how to attack, Rumos ★
- 2017 - Volunteer at Web Summit 2017 ★
- 2017 - Workshop: Better Programmer, Galileu ★

Event Participation - Online

- 2024 - Microsoft Discovery Hour: Modernize Your Security Operations Center
- 2022 - AWS Discovery Day - Cloud Essentials ★
- 2021 - MultiCloud Experience ★
  Event with focus on AWS, Microsoft Azure, Google Cloud Platform and Oracle Cloud Infrastructure
- 2018 - Practical Network Troubleshooting with Wireshark, CompTIA ★
- 2018 - Penetration Testing for the New World, CompTIA ★
- 2018 - Demystifying Metasploit, CompTIA ★

Personal Development

- 2022 - Coaching Workshop, Newcode ★
- 2022 - Neurolinguistic Programming Workshop, Newcode ★
- 2020 - Master Your Life, ALLCAN ★

Additional Technological Interests

- Artificial Intelligence, Distributed Systems, Product Design and User Experience

Artistic and Scientific Interests

- Art, Photography, Cinema, Architecture, Design, Nature, Science, History, Psychology

© 2025 Pedro Fernandes