Sérgio Miguel Antunes Ribeiro

(+351) 912908459 | sergioaribeiro@hotmail.com | www.linkedin.com/in/sergiomaribeiro

ACTIVE SECURITY CLEARANCE: NATO / EU SECRET

Cyber Security Defender and Information Management Specialist with over 18 years of operational experience across NATO headquarters and military maritime environments. Proven expertise in securing Command and Control (C2) systems, executing Information Management (IM) workflows during live exercises, and deploying IT infrastructure for forward operational sites. Combining over a decade of disciplined military leadership with advanced academic engineering in threat hunting, SIEM monitoring, and adversary emulation.

KEY CYBERSECURITY ENGINEERING PROJECTS

- **Adversary Emulation & Detection (MITRE Caldera & Wazuh SIEM):** Architected a virtualized enterprise defense lab to emulate APT28 threat behaviors using MITRE Caldera. Mapped automated attacks (Discovery, Lateral Movement) directly to defensive monitoring by ingesting and analyzing logs via Wazuh SIEM agents to validate real-time security events.
- **Automated Threat Hunting (Project Aegis):** Developed and deployed a zero-trust defense framework utilizing Cowrie honeypots, AWS serverless cloud architectures, and Python-based data analysis to detect and isolate automated threats.

PROFESSIONAL EXPERIENCE

Information Management Officer | STRIKFORNATO

Oeiras, Portugal | *10/2023 – Present*

- Direct and secure mission-critical Information Management (IM) flows between NATO Commands and deployed units during high-stakes live exercises and operations.
- Enforce strict information security protocols and ITIL-aligned governance across classified networks.
- Administer and secure NATO Information and Knowledge applications (EDMS, NIP, TT+) and enterprise SharePoint portals in a highly classified NATO Secret environment.

SOC Analyst - Cyber Security | SIBS Multicert

Oeiras, Portugal | 08/2023 – 10/2023

- Executed real-time enterprise monitoring utilizing SIEM platforms to detect and analyze cyber threats.
- Conducted active vulnerability assessments and endpoint security management.
- Acted as a first-line incident responder for triage and containment.

IT Asset & Infrastructure Manager | STRIKFORNATO (NATO)

Oeiras, Portugal | 03/2019 – 07/2023

- Managed, prepared, and rapidly deployed Command, Control, and Information Systems for forward operational sites and NATO field exercises.
- Administered and secured static and deployable LAN infrastructure, maintaining operational readiness for mission-critical VTC and communication hubs.
- Coordinated enlisted watch bills and served as a lead System Administrator under stringent operational timelines.

Cloud (AWS) Consultant | Edge-Intel Consulting Startup

Alcabideche, Portugal | 09/2022 – 07/2023

- Configured and managed secure Cloud services utilizing Amazon Web Services (AWS) and performed Linux administration (freelancer/voluntary).

IT Instructor & Communications Operator | Portuguese Navy

Almada, Portugal | 03/2013 – 01/2017

- Instructed personnel in information technologies, Microsoft Office applications and Project Management tools at the Military Naval School.
- Operated communications circuits and handled secure cryptographic publication distribution.

Head of Electronics Section | Portuguese Navy (Warships: N.R.P. João Roby & N.R.P. António Enes)

Almada, Portugal | 01/2011 – 03/2013

- Led the maintenance, security, and operational readiness of critical warship infrastructure, including surface radars, internal communications, and cryptographic systems.
- Operated secure military communication networks and cryptographic equipment during live maritime deployments.
- Managed technical troubleshooting and preventative maintenance in high-pressure, austere maritime environments.

EDUCATION & CERTIFICATIONS

- **Network and Cybersecurity Engineer Degree (EQF 6)** – ISTEC (180 ECTS)
- **Certified in Cybersecurity (CC)** – ISC2 (01/2025)
- **Associate's Degree (EQF 5) in Cybersecurity** – ISTEC (Final Grade: 17, 120 ECTS)
- **Cybersecurity Specialist Certification** – Academia Nacional de Cibersegurança
- **IT Service Management & Leadership:** Certified Associate in Project Management (CAPM) - PMI
- **Technical Certifications:** AWS Certified Cloud Practitioner, CompTIA Network+ (TOTAL Udemy), Endpoint Security & Cyber Threat Management (Cisco Networking Academy), Openfire Server Administrator (NATO CIS School), Windows Server 2019 Administration.

TECHNICAL & OPERATIONAL SKILLS

- **Cyber Defense:** SIEM Monitoring, Threat Hunting, MITRE ATT&CK Framework, Vulnerability Assessment, Incident Response, Digital Forensics (Autopsy, FTK Imager), Malware Analysis.
- **Infrastructure & Platforms:** AWS Cloud Computing, Linux (Ubuntu, Debian) & Windows Server Administration, Active Directory, SharePoint, Microsoft 365, Docker.
- **Operational & Compliance:** NATO Secret clearance operations, ITIL principles, ISO27001, GDPR, Command and Control (C2) systems deployments.