Evanildo Ribeiro

Junior Cyber Security Consultant (IT / OT Environments)

dejaines@hotmail.com | 07411 269534 | London, UK | linkedin.com/in/evanildoribeiro | https://evanildo22.github.io/portfolio/

Personal Statement

Junior Cyber Security professional with a strong foundation in security monitoring, detection engineering and risk-based analysis, now developing a focused interest in Operational Technology (OT) and Critical National Infrastructure environments.

Experience includes security testing and SOC-style monitoring in lab and research settings, log and network traffic analysis, and supporting incident response simulations. Comfortable working with security telemetry, assessing cyber risks, and documenting findings in a structured and auditable manner.

Particularly interested in the secure design and operation of industrial and energy systems, with an emphasis on availability, safety and resilience. Motivated to develop under senior engineers in regulated OT environments and to align work with frameworks such as NCSC CAF and IEC 62443.

Cyber Security Foundations (IT & OT-Relevant)

- **Security Monitoring & Detection:** SIEM-based monitoring using Elastic Stack and Splunk; authentication anomalies, scanning activity, beaconing and suspicious outbound connections.
- **Network Visibility:** PCAP and Wireshark analysis; Zeek telemetry (conn/http/files/notice); understanding of segmented networks and monitored zones, including IT/OT boundary awareness.
- **Detection Engineering:** Threshold and behaviour-based alerts; MITRE ATT&CK mapping; alert tuning to reduce false positives and minimise operational disruption.
- **Endpoint & Host Analysis:** Windows and Linux log analysis; Sysmon telemetry; basic static malware analysis; first-line host triage.
- **Risk-Aware Analysis:** Alert investigation with consideration for system availability, operational impact and escalation thresholds.
- **Scripting & Automation:** Python and Bash for log parsing, aggregation and alerting; cron scheduling; SIEM ingestion workflows.
- **Incident Response Support:** Evidence preservation, memory capture, Volatility analysis, timeline creation and structured handover to senior analysts.
- **Documentation & Reporting:** Clear technical notes, detection logic documentation and remediation guidance suitable for audits and regulated environments.

Experience

Research Assistant in Cybersecurity (Internship).
University of West London (UWL)

London, UK · Jun 2025 – Dec 2025

Role bridging academic research and practical security operations, involving security testing, SOC-style monitoring and incident response simulations in controlled lab environments.

- Monitored Linux authentication logs and Windows/Sysmon telemetry using Splunk and Elastic, reviewing alerts for brute-force attempts, suspicious egress and persistence-related behaviour.
- Built a lightweight detection pipeline for /var/log/auth.log using Python and Bash, aggregating failures by user and IP, triggering alerts on defined thresholds and forwarding results to the SIEM.
- Converted PCAP data into Zeek logs and ingested into Elastic and Splunk, creating dashboards and alerts for port scanning, authentication abuse and beaconing patterns.
- Authored and tuned SPL and Elasticsearch queries, balancing detection coverage with false-positive reduction to avoid unnecessary operational disruption.
- Correlated Sysmon Event IDs (1, 3, 8, 11, 13, 22) with Windows Security events (e.g. 4698/4703) to identify scheduled task persistence and potential process injection.
- Supported end-to-end incident response simulations following staged phishing intrusions, including host isolation, memory capture and Volatility analysis.
- Documented detections with MITRE ATT&CK mappings (e.g. T1110.001, T1053.005, T1003) and produced detection-to-recovery timelines for senior analysts, with practical remediation notes.

Selected Security Projects (Lab & Research)

London, UK · 2023 – 2024

Projects completed in controlled lab and academic environments, with increasing focus on applicability to industrial and OT security contexts.

- **IoT Anomaly Detection System (Final Year Project):** Designed an anomaly detection solution using a hybrid Convolutional Autoencoder (CAE) with attention mechanisms to improve detection accuracy in IoT-style environments.
- **Linux Log Monitoring & Alerting:** Real-time monitoring of /var/log/auth.log; Python/Bash scripts aggregating failed logins by IP/user, sending alerts via email and syslog for SIEM ingestion.
- **Network Traffic Analysis to SIEM:** PCAP to Zeek conversion; extraction of IPs, domains and hashes; enrichment using VirusTotal; Elastic visualisations highlighting SSH failure spikes and unusual outbound activity.
- **Endpoint Telemetry & Persistence Detection:** Deployed Sysmon and correlated process, network, file and registry events to surface persistence techniques such as scheduled task creation.

- **Threat Hunting with MITRE ATT&CK:** Developed hypotheses and wrote SPL/Elasticsearch queries targeting brute-force activity, remote thread injection and registry-based persistence.
- **Memory Forensics Support:** Captured memory from compromised lab VMs; analysed with Volatility (pslist, pstree, netscan, malfind) to identify anomalous processes and network connections.
- **Vulnerability Recon & Basic Pentesting:** Conducted Nmap, Gobuster and Nikto scans against lab targets to understand common attack paths and improve realism of detection use cases.

Earlier Experience

IT Support Technician / Help Desk — Gráfica Rio LTDA

Linhares, Brazil · 2015 – 2019

- Provided first- and second-line support for Windows and macOS users, resolving authentication issues, application errors and hardware faults.
- Managed user accounts in Active Directory and Microsoft 365, including password resets, group membership and mailbox permissions.
- Installed and configured Windows workstations and laptops, applying updates and ensuring systems met baseline security requirements.
- Supported VPN connectivity, Wi-Fi access and shared drive issues for remote users, escalating complex network faults when required.
- Logged and prioritised incidents via the help desk system, maintaining clear communication with users throughout resolution.

Manager — Headmasters Ltd

London, UK · 2010 – 2014

- Managed daily operations and supervised a small team in a commercial environment.
- Delivered structured training, procedures and checklists, improving consistency and compliance.
- Produced concise reports for stakeholders, summarising performance, issues and actions — experience directly transferable to incident reporting and audit documentation.

Education

BSc (Hons) Cyber Security — 1st Class
University of West London, London, UK · 2020 – 2024

CMI Level 3 Award in First Line Management (QCF)
Chartered Management Institute, London, UK · 2013 – 2014

Certifications & Training

- **CompTIA Security+** (Target exam date: March 2026)
- **Certified Ethical Hacker (CEH)** (studying)
- **Microsoft SC-200 Security Operations Analyst** (studying)

Currently building certifications aligned with cyber risk management and industrial security principles.

Tools & Platforms

Elastic Stack · Splunk · Zeek · Wireshark · Sysmon · Windows Event Viewer · Volatility · Linux CLI · Nmap · Metasploit · Burp Suite · john/hashcat · Git (basics)

Languages

English – Fluent | Portuguese – Native | Spanish – Beginner/Intermediate

Interests

Capture-the-Flag (CTF) · Security research write-ups · Brazilian Jiu-Jitsu