Portfolio Book — Carlos Menezes

From tech passion to a home mini-SOC

A narrative view of cybersecurity, development and infrastructure projects.

1. Timeline

- **90s–2000** — BBS SysOp in Rio de Janeiro, managing users and connections.
- **2000s** — LAN house admin (>100 PCs), daily work with networking and hardware.
- **2017–2019** — BeiraZoo: admin and management support, operational discipline.
- **2019–2022** — INTELCIA: team supervision, KPIs and leadership.
- **2022–2024** — CUF: customer service, problem solving and people focus.
- **2024–...** — Technical Programmer Course (IEFP) + cybersecurity lab (Splunk, Linux, IDS/IPS).

2. Home SOC Overview

My main portfolio project is building a **mini-SOC** at home, using only open-source tools and my own Linux server. This SOC integrates:

- **Splunk** as SIEM, ingesting auth.log, syslog, UFW, Apache, MySQL and ban_script logs.
- **Suricata/Snort** as IDS/IPS, generating network alerts.
- **UFW + scripts** for automatic response to SSH brute force.
- **Threat Intel** via external malicious IP lookups.
- **Dashboards** split into "Command Center" (main) and "Advanced Center".

3. Highlighted Technical Projects

Each project has its own page on the site, with SPLs, scripts, screenshots and explanations:

- **Splunk SOC** — brute-force detection, auto-ban, threat intel, geoIP and risk scoring.
- **Webmin & Linux Admin** — user/service management, firewall and backups.
- **LDAP** — OpenLDAP with PAM/SSSD, centralized auth and password policies.
- **MEI (Java + SQL)** — CRUD app with MVC, persistence and ER diagram.

The Portfolio Book acts as a narrative index: readers can open internal pages (`splunk_soc.html`, `ldap.html`, `webmin.html`, `mei.html`) to see technical details, SPLs and screenshots.

4. Next Steps

- Add a secure API for manual bans and external integrations.
- Explore alerting automations via SMS/WhatsApp/Email.
- Experiment with other SIEMs (e.g. Wazuh, Elastic Security) using similar architecture.

- Study certifications (CompTIA Security+, CCST, etc.) aligned with the lab practice.

This document summarizes the portfolio and points to the others: CV, Casebook and SOC Playbook.