Portfolio Book — Carlos Menezes

Da paixão por tecnologia ao mini-SOC em casa

Uma visão narrativa dos projetos de cibersegurança, desenvolvimento e infraestrutura.

1. Linha do Tempo

- **Anos 90–2000** — SysOp de BBS no Rio de Janeiro, gestão de utilizadores e ligações.
- **Anos 2000** — Administração de LAN House com >100 PCs; contacto diário com redes e hardware.
- **2017–2019** — BeiraZoo: apoio administrativo e gestão, desenvolvimento de disciplina operacional.
- **2019–2022** — INTELCIA: supervisão de equipas, análise de indicadores e liderança.
- **2022–2024** — CUF: atendimento ao cliente, resolução de problemas e foco em pessoas.
- **2024–...** — Curso Técnico de Programador (IEFP) + laboratório de cibersegurança (Splunk, Linux, IDS/IPS).

2. Visão Global do SOC Caseiro

O meu principal projeto de portfólio é a construção de um **mini-SOC** em casa, usando apenas ferramentas open source e o meu próprio servidor Linux. Este SOC integra:

- **Splunk** como SIEM, ingestão de auth.log, syslog, UFW, Apache, MySQL e ban_script.
- **Suricata/Snort** como IDS/IPS, gerando alertas de rede.
- **UFW + scripts** para resposta automática a brute force SSH.
- **Threat Intel** através de lookups externos de IPs maliciosos.
- **Dashboards** divididos em "Central de Comando" (main) e "Centro Avançado".

3. Projetos Técnicos em Destaque

Cada projeto tem página própria no site, com SPLs, scripts, prints e explicações:

- **Splunk SOC** — detecção de brute force, auto-ban, threat intel, geoIP e scoring de risco.
- **Webmin & Linux Admin** — gestão de utilizadores, serviços, firewall e backups.
- **LDAP** — OpenLDAP com PAM/SSSD, autenticação centralizada e políticas de senha.
- **MEI (Java + SQL)** — aplicação CRUD com MVC, persistência e diagrama ER.

O Portfolio Book funciona como índice narrativo: o leitor pode abrir as páginas internas (`splunk_soc.html`, `ldap.html`, `webmin.html`, `mei.html`) para ver detalhes técnicos, SPLs e screenshots.

4. Próximos Passos

- Adicionar API segura para banimento manual e integrações externas.

- Explorar automações de alerta via SMS/WhatsApp/Email.
- Experimentar outros SIEMs (p.ex. Wazuh, Elastic Security) com arquitetura semelhante.
- Estudar certificações (CompTIA Security+, CCST, etc.) alinhadas com a prática do laboratório.

Este documento resume o portfólio e aponta para os restantes: CV, Casebook e SOC Playbook.