CASE STUDY

SECURITY OPERATIONS PLATFORM

Self-built, documented, demoable

Built a 15-service security operations platform

Coeus SOC · 103 Python modules · Designed, built, and operated by one person

Outcome: Fifteen security tools run behind one login: alert analysis, threat intel, incident playbooks, case management, email analysis, enrichment, metrics, and analyst training. The platform has its own audit trail: a full code and security review is part of the documentation.

The Situation

SOC tooling is priced for enterprises. Small teams get spreadsheets and browser tabs. I wanted to find out how much of a real security operations workflow could be built and run by one person, and to have a working platform to show for it.

What Was Built

- **Fifteen integrated services**: alert analyst, threat intelligence, incident response playbooks, case manager, email analyzer, enrichment, metrics, triage, and a training module for analysts.
- **One front door**: an authentication gateway and reverse proxy put every tool behind a single login.
- **Playbook engine** with its own database, so incident response steps are tracked instead of remembered.
- **Test harnesses** for the classifier, sanitizer, and platform itself. Tests are part of the codebase, not an afterthought.
- **A written audit of the platform**: a deep codebase sweep covering security and code quality, with findings and a remediation plan. I audit my own work the way I audit other people's networks.

Results

- The full workflow from alert to closed case runs on one machine, behind one login.
- A scripted 10-minute demo walks through the whole platform.
- The documentation includes architecture maps, hardening notes, and the audit findings. Another engineer could pick it up.

Stack & Methods

Stack: Python · Flask/FastAPI · reverse proxy + auth gateway · SQLite · incident playbooks · threat intel feeds · automated test harnesses