Esaü Bukasa

esaubukasa@protonmail.com — +32 493 92 05 26 — https://github.com/pindjouf

Professional Summary

Security professional with a background in military communications and cyber security. Experience in secure communications systems, protocol implementation, and SIEM deployment. Strong foundation in technical analysis and operational security with focus on threat detection and monitoring.

Work Experience

SOC Intern *Jan 2025 – Present*
Ampacimon, Loncin, Belgium

- Leading deployment and configuration of ELK-based SIEM solution for enterprise security monitoring.
- Built internal tooling that resulted in a 19% increase of threat actor findings.
- Configuring log ingestion pipelines and optimizing incident response procedures.

Cybersecurity Apprenticeship *July 2024*
Cyber summer school, Brussels, Belgium

- Admission to the bootcamp through solving different challenges linked to Cybersecurity.
- Lectures and workshops given by instructors from the Cyber Command: Digital Forensics, Monitoring, Malware Analysis, OSINT, ...

Cybersecurity Trainee *Mar 2024 – Sep 2024*
BeCode, Brussels, Belgium

- Developed secure code for database operations.
- Performed vulnerability assessments and implemented secure system configurations.

ICT Operator *Apr 2023 – Feb 2024*
Belgian Defence, Peutie, Belgium

- Managed critical communications systems and maintained strict operational security.
- Coordinated with multinational teams in various operations through satellite communication.

Projects

Noir Chapeau (*https://noirchapeau.com*) *Launched Oct 2024*

- Cybersecurity collective focused on ransomware recovery research & data breach investigations.

Personal Website (*https://pindjouf.xyz*) *Launched Jan 2022*

- An educational resource focused on technical writing.

IDY (*https://idy.pindjouf.xyz*) *Launched Jan 2025*

- Visualization web app for the nmap network scanner.

Technical Skills

- **Security:** ELK Stack (SIEM), Wireshark, Burp Suite, Metasploit, Nmap, Nessus, OWASP, MITRE ATT&CK, IDA free, Ghidra, Splunk, Malware Analysis, Pentesting, Reverse Engineering, Forensics, Linux, Active Directory
- **Programming & Scripting:** Rust, Python, JavaScript/TypeScript, Bash, Verilog, C/C++, Powershell, Batch, ARM assembly, SQL
- **Web:** WebAssembly, React, Svelte/SvelteKit, Node.js, REST APIs, Flask, Jinja