CHANCELLE AHINON

Cybersecurity Analyst (Entry-Level) | SOC Analyst Candidate

Cotonou, Republic of Benin | +229 01 55 36 73 30 | rayp5464@gmail.com

PROFESSIONAL PROFILE

Entry-level cybersecurity professional with 37 hands-on labs completed under the Google Cybersecurity Certificate, demonstrating practical skills in SIEM analysis, network packet capture, IDS rule writing, Linux administration, SQL querying, and Python scripting. Completed the Women Techsters Bootcamp (Tech4Dev), where a live digital safety platform was designed, built, and deployed. Actively practicing threat analysis, incident response, and SOC workflows through TryHackMe and Hack The Box Academy. Interested in cloud security, incident response, and data protection. Bilingual (French/English), currently pursuing a B.Sc. in Information Security & Forensics.

EDUCATION

B.Sc. Information Security & Forensics — Admission in Progress *2026 – Present*

Actively undergoing the admission process for this undergraduate program in information security.

Diploma in Management Information Systems (Incomplete) *2023 – 2025*

National School of Applied Economics and Management

Scientific Baccalaureate *2015 – 2022*

Certificate in Computer Secretarial & Internet *Aug 2015*

CERTIFICATIONS & SPECIALIZED TRAINING

Google Cybersecurity Professional Certificate *Completed Feb 2026*

- Linux & System Administration: user management, file operations, grep, find, I/O redirection, software installation.
- SQL & Data Querying: filtering, AND/OR/NOT operators, multi-table joins for security data analysis.
- Cryptography & Security Ops: hash value creation/verification, message decryption, network packet capture with tcpdump, packet analysis with Wireshark, IDS/IPS alert and rule analysis with Suricata.
- Hands-on portfolio artifacts: incident handler's journal, vulnerability assessment report, risk register, PASTA threat model, access control worksheet, data leak worksheet, alert ticket escalation, Python IP-allow-list automation algorithm.

Expadox Lab Project-Based Mentorship Cohort 2 — Cybersecurity Track *Present*

AI-Assisted Threat Detection

SecOpsAI

An intelligent threat detection platform that combines machine learning with modern security engineering to identify malicious network activity. Built with secure APIs, engineered network features, and enterprise-grade security controls.

- Machine learning-based network attack detection
- Secure REST APIs with JWT authentication and RBAC
- Detection engineering using Zeek and Suricata telemetry
- Audit logging, rate limiting, and security analytics

Case Study | GitHub Repository

ShieldFlow

A DevSecOps platform designed to integrate automated security testing into the software development lifecycle, helping identify vulnerabilities before deployment through continuous security validation.

- Automated SAST, DAST, and dependency scanning
- Secret detection and container image security
- CI/CD security automation with GitHub Actions
- Secure software development lifecycle implementation

Case Study | GitHub Repository

FireOps

A hybrid security monitoring architecture that provides centralized visibility across cloud and on-premises environments by integrating enterprise security monitoring, cloud telemetry, and network detection technologies.

- Centralized security monitoring and log collection
- CloudTrail integration for AWS visibility
- Network intrusion detection with Suricata
- Containerized deployment and secure remote access

Case Study | Documentation

Women Techsters Bootcamp — Cybersecurity Track*Mar 2026 – Apr 2026 · Certificate expected Apr 10, 2026*

- Completed intensive cybersecurity bootcamp covering defensive security, threat modeling, and secure application development.
- Capstone project: SafeSocial — a live digital safety platform for teenagers with AI-powered cyberbullying detection (Gemini API), predator alert system, and privacy risk checker. Built with React/TypeScript, deployed on Netlify.

OpenClassrooms — Data & Programming Courses*Apr 2024 – Jan 2025*

- Certificates earned: Python for Data Analysis, R for Data Analysis, Data Cleaning & Analysis, Clear Statistical Reporting, Introduction to Machine Learning.
- Additional courses completed: Command Line, Algorithms, REST APIs, Python (maintainable code & testing), SQL, Power BI, Data Culture.

Data Analysis Training (ATUT Program)*Jul 2025 – Nov 2025*

- Trained in data analysis techniques, workflow automation, and reporting tools.

TECHNICAL TOOLKIT

Tools, platforms, and technologies used daily.

Security Operations	Splunk, Wazuh, Zeek, Suricata, AWS CloudTrail, OpenSearch
Security Engineering	Python, FastAPI, Docker, REST APIs, GitHub Actions
Offensive Security	Burp Suite, SQLMap, Metasploit, Greenbone, OWASP ZAP, OWASP Top 10
Enterprise Infrastructure	Windows Server, Active Directory, Networking, Zabbix, Ubuntu, Kali Linux
Development & Collaboration	Git, GitHub, Tailscale, VS Code, Docker Compose

CYBERSECURITY PRACTICAL EXPERIENCE

TryHackMe & Hack The Box (HTB Academy)*Present*

- Completed OSINT challenges (OhSINT room): web steganography, metadata extraction, geolocation techniques.
- Linux command-line operations: file system navigation, find, stderr/stdout redirection, standard I/O streams, binary inspection.
- SSH authentication log analysis: identifying brute-force patterns and suspicious login activity.
- Networking concepts: ephemeral ports, SYN flood behavior, DNS-over-HTTPS.
- Following SOC Analyst Prerequisites Path and SOC Analyst Job Role Path on HTB Academy.

Threat Intelligence — VirusTotal & MITRE ATT&CK*2026*

- Investigated file hashes via VirusTotal; identified the Flagpro malware attributed to threat actor BlackTech (50+ vendors flagged).
- Mapped attacker TTPs, C2 infrastructure, domain names, and IP indicators using the Pyramid of Pain model.
- Compared network protocol analyzers: tcpdump (CLI, lightweight) vs. Wireshark (GUI, advanced filtering).

PROFESSIONAL EXPERIENCE

Personal Assistant (Internship)*Dec 2022*

- Managed executive scheduling, communications, and administrative coordination.
- Maintained organizational documentation and handled digital correspondence.

TECHNICAL SKILLS

Security Tools	Wireshark, tcpdump, Suricata (IDS/IPS), VirusTotal, SIEM fundamentals, TryHackMe, HTB Academy
Frameworks	NIST CSF, NIST SP 800-30/800-53, MITRE ATT&CK, PASTA, Pyramid of Pain, CIA Triad
Programming	Python (file I/O, list operations, automation), SQL (joins, filters), React, TypeScript, HTML/CSS
OS & Networking	Linux (proficient), Windows, TCP/IP, DNS, SSH, packet analysis, port & stream concepts
Cloud & APIs	Gemini API, EmailJS, Netlify deployment, REST APIs, OpenClassrooms ML fundamentals
Productivity	Notion, Trello, Power BI, Microsoft Office Suite
Interests	Cloud security, incident response, data protection, security awareness

LANGUAGES

French (Native) · Fon (Native) · English (Professional)

KEY PROJECT

SafeSocial — AI-Powered Digital Safety Platform*March 2026*

- Built a full-stack web app protecting teenagers from cyberbullying, online predators, and privacy risks.
- Integrated Google Gemini AI for real-time content analysis; EmailJS for automated alert notifications.
- Tech stack: React, TypeScript, Gemini API, EmailJS. First hands-on API integration experience.
- Delivered a formal group presentation and live deployment as the bootcamp final capstone.