

# NETWORKING & SECURITY PROFESSIONAL

Kanchuka Indurnga(Richard Grayson)

+9476 032 8881 • [richardgrayson2161@gmail.com](mailto:richardgrayson2161@gmail.com) • [linkedin](#) • [Portfolio](#)

---

Results-driven Software Engineering undergrad (3.67 GPA) specializing in cybersecurity, AI, and full-stack development. Proven ability to architect, lead, and deliver complex security and software projects from conception to completion. Experienced in developing advanced tools for threat analysis, automation, and system hardening, while leading multidisciplinary initiatives with strong communication and organizational skills. Active contributor to open-source security projects and passionate about bridging deep technical execution with strategic project management to deliver secure, high-impact solutions.

---

## Technical & Soft skills:

**Threat Detection & Response:** Threat Detection Engineering · SIEM (Splunk, ELK, Wazuh) · SOAR Automation (Shuffle, TheHive, Cortex) · Sigma & YARA Rule Writing · MITRE ATT&CK Mapping · Threat Hunting · Incident Response Lifecycle

**Network & Endpoint Forensics:** Network Forensics (Wireshark, Zeek, Suricata) · Endpoint Telemetry (Sysmon, Osquery, Velociraptor) · Memory & Disk Forensics (Volatility, Autopsy) · Malware Analysis (Cuckoo Sandbox) · Log Correlation (PCAP, Syslog, Auditd)

**Automation & Engineering:** Python & Bash Scripting · Detection-as-Code · GitHub Version Control · API Integration for Log Enrichment · Playbook Development & Automation Pipelines

**Security Operations & Monitoring:** SIEM Log Analysis · SOC Playbook Design · Incident Containment & Recovery · Alert Triage & Case Management · Threat Intelligence Integration

**Operating Systems & Environments:** Parrot OS Security (daily driver for detection labs) · Kali Linux (offensive security) · Windows (Sysmon, Event Viewer, PowerShell Forensics) · Linux (auditd, journald) · Virtual Labs (VMware, VirtualBox, Docker)

**Tools & Frameworks:** Wireshark · Zeek · Suricata · Sysmon · Osquery · Volatility · Autopsy · Cuckoo · Splunk · ELK Stack · Shuffle · TheHive · Cortex · Sigma · YARA · MITRE ATT&CK Navigator

**Soft Skills:** Project Management, Team Collaboration, Problem-Solving, Technical Writing, Communication, Adaptability & Learning, Organizational & Work Ethic

---

## Projects and Experiences

### Python Security Developer (Independent Project) | [fsocietyOS](#)

[Documentations](#)

- Reduced time-to-exploit by 90% during web penetration tests by developing a modular suite with 10+ components that fully automated discovery for critical vulnerabilities including SQLi, XSS, and LFI.
- Unified six pentesting domains (Network, Web, Mobile, OSINT, Wireless, Social Engineering) by engineering a Python framework that consolidated 50+ attack and reconnaissance scripts into a single CLI platform.

### Cybersecurity Tool Developer (Independent Project) | [BugHunter](#)

[Documentations](#)

- Reduced security audit reporting time by 80% by developing a tool that automatically correlated data from multiple threat intelligence feeds (NVD, Exploit-DB, GitHub) into a unified JSONL report.
- Achieved 92% accuracy in vulnerability prediction by integrating a scikit-learn model that identified 10+ potential zero-day patterns not listed in existing CVE databases.

### Cloud Security Engineer (Independent Project) | [CloudMonkey](#)

[Documentations](#)

- Reduced mean time to remediation (MTTR) by 60% by building a click-based CLI that delivered instant, actionable insights on critical exposures such as public S3 buckets and exposed .env files.
- Enabled full auditability of security scans by implementing a SQLite database manager that logged and timestamped all findings across 5,000+ scanned assets.

## **AI Developer (Independent Project) | CyberSamantha**

**Documentations**

- Boosted information retrieval efficiency by 95% by developing a Python-based RAG system that queried a 10,000+ chunk ChromaDB vector store, returning context-backed answers in under 2 seconds.
- Automated the entire Security knowledge base pipeline using LangChain to parse, chunk, and index 5+ unstructured document types, reducing manual data preparation time from 40 hours to 10 minutes.

## **Lead Security Developer (Independent Project) | Security Auditor Plugin**

**Documentations**

- Built a 7-in-1 security scanner that performed SAST, secret detection, and dependency analysis, delivering a unified 0–100 security score and consolidating 5+ tools into a single 2.34-second scan.
- Designed a fully offline, 4-phase zero-day detection engine using differential git analysis and fuzzy hashing to uncover 7+ high-confidence vulnerabilities, including SQLi and Command Injection, without network access or API keys.

## **Security Engineer (Independent Project) | HoneyTrap**

**Documentations**

- Delivered real-time threat visualization by deploying a containerized monitoring stack (Prometheus, Grafana) that ingested 10+ custom metrics and over 1,000 daily log events from a Python-based SSH honeypot.
- Captured complete attacker TTPs by developing a low-interaction SSH honeypot (Paramiko) that logged credentials, commands, and full session transcripts, enabling zero-risk analysis of live adversary behavior.

## **Security Tool Developer (Independent Project) | virusBugger**

**Documentations**

- Built a static analysis tool in Python that automatically extracted five key indicators of compromise (hashes, entropy, strings, imports, packer signatures) from PE files, automating the entire initial malware triage workflow.
- Cut malware analysis time by 90% by developing a pefile-based engine that generated a 1-page capability report, including all imported DLLs and functions, in under 2 seconds.

## **Software Developer (Independent Project) | cyberchef-cli**

**Documentations**

- Automated complex data transformation workflows by building a recipe parser that chained 10+ operations (xor, base64\_decode, json\_beautify) into a single command, cutting processing time by 95%.
- Built 21+ modular data manipulation functions (6 encoding, 5 crypto, 4 conversion, 6 analysis) using a scalable ABC-based registry, enabling instant integration of new user-requested features.

---

## **Publications & Write-ups**

- Anomaly Detection in Russian Ghost Radio Channels – Ongoing research analyzing unexplained signal patterns and developing ML-based anomaly detection pipelines for classifying covert radio communications.
- Malware vs. Malware Ecology: Interactions Within the Wild – Research study exploring behavioral interference, competition, and coexistence among active malware strains to understand self-replicating ecosystems.
- Training a Prompt Injection Rejection Plugin – Experimental work on building a self-learning defensive plugin to identify and neutralize prompt injection attacks across LLM-based systems.
- CTF & Cybersecurity Write-ups – Published detailed challenge solutions, exploit analyses, and reverse engineering breakdowns at [hacker.super.site](https://hacker.super.site).

---

## **Education**

### **BSc (Hons) in Software Engineering • Seagis Campus • (Expected Graduation: 2027) :**

- Current GPA: 3.67/4.00 (2 years completed)
- Relevant Coursework: Data Structures & Algorithms, Network Security, Object-Oriented Programming, Database Systems, Ethical Hacking, Web Application Development.