Shiwantha Indunil Rodrigo

Cybersecurity Analyst

0094770858564 | shiwantha.rodrigo.it@gmail.com | LinkedIn | GitHub | Portfolio

PROFESSIONAL SUMMARY

Cybersecurity Enthusiast with practical knowledge in SOC operations, SIEM monitoring, network security and threat analysis. Strong background in Linux systems, vulnerability assessment and incident response, supported by multiple industry certifications and a foundation in software engineering. Proven ability to analyze security events and support risk mitigation through technical and analytical skills.

Career Focus : SOC Analyst | Cybersecurity Analyst | Blue Team

IT WORK EXPERIENCE

Software Engineer | Liveroom Technologies | Nugegoda | Internship | 1 Year

• Coded most of the core APIs (20+) for a NFT trading platform using Python (Django).

• Improved API latency from seconds to milliseconds using AWS Lambda and SQS.

• Applied hashing, salting and peppering with memory hardening techniques in 5+ API's.

• Wrote and maintained documentation for all the API's.

PROJECTS & PRACTICAL LABS

(All source code and documentation available on GitHub)

Network Security & Infrastructure Home Lab | 2024

• Designed and deployed a physical home lab simulating a SOC environment.

• Configured routing protocols (RIP, OSPF, EIGRP, BGP) and implemented VLAN segmentation and ACLs.

• Deployed VPNs and firewall rules to enforce access control and network isolation.

• Performed network traffic analysis and troubleshooting to identify misconfigurations and security risks.

WATCH TOWER - SIEM & Network Traffic Monitoring Tool | 2025

• Developed a SIEM-style web application to capture and analyze event logs.

• Implemented centralized logging, event aggregation and correlation logic for anomaly detection.

• Built dashboards to visualize alerts, threat indicators and incident response data.

ENIGMA - Credential Security Toolkit | 2023

• Built a secure deterministic password generation and file encryption tool to improve credential security.

• Integrated advanced cryptographic practices such as memory hardening to increase computational costs.

• Added a password strength evaluation tool to test against common attack vectors such as rainbow tables.

Hotel Reservation & Management Website (for Kings Garden View Hotel in Welimada **)**

• Developed a full-stack website using PHP, JavaScript, SQL, and CSS.

• Implemented backend logic for bookings, user management, and secure data storage.

• Applied secure input validation and handling techniques to reduce common web vulnerabilities.

CERTIFICATIONS

- Cisco Certified Network Associate - CCNA (Verify)
- CompTIA Linux+ V7 (Verify)
- Google Cybersecurity Professional V2 (Verify)
- Microsoft Python Development Professional (Verify)
- Palo Alto Networks Cybersecurity Certificate (Verify)
- Splunk Search Expert (Verify)

CORE SKILLS

Security Operations : SIEM Monitoring, Alert Triage, Incident Detection & Response, IOC Analysis, SOC Operations, MITRE ATT&CK, NIST CSF, Risk Assessment

Network Security : TCP/IP, DNS, DHCP, VLANs, NAT, Network Traffic Analysis, IDS/IPS, Firewall Rules, NGFW Fundamentals, Palo Alto Basics, Zero Trust

Systems & Linux Security : Linux Administration, Log Analysis, User & Permission Management, Process Monitoring, System Hardening, Bash Scripting

Automation & Scripting : Python Scripting, Log Parsing, Regex, Network Automation

Security Tools : Splunk, Wireshark (tshark), tcpdump, iptables, nftables

EDUCATION

Bachelor of Information Technology | University of Colombo School of Computing | Completed in 2024.

Higher National Diploma (HND) in Civil Engineering | ICBT, Mount Lavinia | Completed in 2015.

ADDITIONAL WORK EXPERIENCE

Technical Officer (Civil Engineering) | Anthony Builders | Kuliyapitiya | 2 Years

• Conducted site inspections and managed technical documentation.

Mixologist | Bar Capri | Battipaglia, Italy | 3 Years

• Delivered high quality customer service in a fast paced environment, managing multiple priorities.

Personal Interests : Cryptography, Game theory applications, Logical paradoxes, FOSS development.