Rohinth Rathna

Aspiring Blue Team Analyst

+91 6385806454 | rohinthrathna2004@gmail.com | www.linkedin.com/in/rohinth-rathna-s-355272254 | 0xrohinth.github.io

PROFESSIONAL SUMMARY

Cybersecurity student with hands-on experience in Security Operations Center (SOC) concepts, penetration testing, malware analysis, and SIEM deployment. Google Cloud Cybersecurity Certified with practical experience building a home SOC lab using Wazuh/OpenSearch, analyzing security logs, and simulating cyber attacks. Passionate about Blue Team operations, incident detection, and continuous learning in defensive security

EXPERIENCE

IoT & Embedded Systems Intern — Taras Solutions *Jun 2025 — Aug 2025*

Remote

- Assisted in developing IoT and embedded system applications.
- Explored secure communication between IoT devices.
- Documented project progress and technical findings.
- Learned embedded hardware fundamentals and secure data transmission.

EDUCATION

Bachelor of Engineering in Computer Science and Engineering *Sep 2022 — Jun 2026*

Dr. Sivanthi Aditanar College of Engineering

SKILLS

Python, Bash, C, Java, Flutter, Linux, Windows, Penetration Testing, Web Security, Malware Analysis, Log Analysis, Threat Detection, Incident Response Fundamentals, TCP/IP, DNS, Wazuh, OpenSearch,

Burp Suite, Wireshark, Nmap, Metasploit, Vulnerability assessment, Incident response, Data protection strategies, Risk management, Encryption standards, Access control principles, Security auditing

PROJECTS

Home SOC & SIEM Lab

- **Deployed a multi-node home SOC environment** using **Wazuh SIEM** and **OpenSearch** to centralize telemetry, monitoring, and threat detection across Linux endpoints.
- **Ingested and parsed system logs** (/var/log/auth.log, syslog) to baseline standard system activity and identify anomalous behavior.
- **Engineered custom Wazuh detection rules** in XML to identify SSH and web-based brute-force authentication attacks.
- **Simulated web application attacks** against **DVWA** and **OWASP Juice Shop** using tools like Hydra and Burp Suite to validate detection coverage.
- **Executed end-to-end incident response workflows**, triaging alerts, mapping activity to **MITRE ATT&CK**, and authoring detailed incident reports.

Personal Portfolio Website

• **Developed a modern, cross-device compatible portfolio** utilizing HTML, CSS, and JavaScript.

• **Hosted and maintained on GitHub Pages** using Git version control for efficient updates.

• **Structured content to feature hands-on cybersecurity labs**, detailed incident reports, and professional credentials.

Personal Blog Site

• **Architected a static site generation (SSG) blog platform** leveraging Node.js, HTML, and CSS for fast rendering and low latency.

• **Automated content build workflows** by creating a Node.js script that dynamically converts raw Markdown files into styled HTML pages.

• **Streamlined deployment pipeline** using GitHub Pages to host static technical write-ups and threat analysis reports.

Stock Manager App

• **Developed a cross-platform mobile inventory management application** using Flutter and Dart for Android devices.

• **Designed a local relational database architecture** utilizing SQLite for reliable offline data persistence, CRUD operations, and fast query response times.

• **Implemented core business logic** including real-time stock quantity tracking, product categorization, SKU management, and pricing calculations.

Malware Behavior Analysis

• **Executed static and dynamic malware analysis** within hardened, network-isolated virtual lab environments (sandboxes).

• **Extracted Indicators of Compromise (IOCs)**—including C2 IP addresses, file hashes (MD5/SHA256), registry modifications, and dropped payloads.

• **Analyzed suspicious binaries** using tools like Process Hacker, Regshot, Wireshark, and PEStudio to disassemble and trace behavioral patterns.

• **Authored comprehensive threat analysis reports** detailing attack vectors, behavioral chains, and recommended remediation strategies.

DevSecOps Automated Infrastructure & SOC Monitoring Lab

Ansible, Docker, GitHub Actions, Prometheus, Grafana, Loki, Trivy, Linux (Ubuntu)

• **Architected an automated DevSecOps infrastructure** deploying Docker-containerized applications on Ubuntu Linux using Ansible playbooks.

• **Constructed CI/CD security pipelines** in GitHub Actions, integrating Trivy for automated vulnerability scanning of container images and dependencies before deployment.

• **Established a central observability stack** using Prometheus, Grafana, and Grafana Loki to ingest, visualize, and correlate infrastructure metrics and log telemetry.

• **Engineered custom SOC monitoring dashboards** and alerting rules to track system health, container metrics, and anomalous log patterns in real time.

• **Automated vulnerability triage and system monitoring**, documenting incident playbooks and remediation steps for pipeline security flaws.

CERTIFICATIONS

Google Cloud Cybersecurity Professional Certificate — Google Cloud