AR. MOHAMED RIMSAN

SOC ANALYST INTERN | IT UNDERGRADUATE

📍 No 2/1, Perara Avenue, Meethotamulla, Kolonnawa, Western Province, Sri Lanka.

📞 +94 77 404 7471   ✉️ mohamedrimzanabdulraheem@gmail.com

in. linkedin.com/in/mohamed-rimsan-a-r   🌐 mohamedrimsan.github.io

ABOUT ME

Motivated IT undergraduate focused on cybersecurity and defensive operations. Built hands-on experience through SOC labs, threat-hunting exercises, and forensic practice. Strong communicator and problem solver seeking an internship or entry-level SOC / Blue Team role to apply practical skills and continue professional growth.

EDUCATION

Expected Graduation: Nov 2026

Bachelor of science in Information Technology
The Open University of Sri Lanka (OUSL)

Expected Completion: Dec 2025

Blue Team Junior Analyst
Security Blue Team

Expected Completion: Dec 2025

Google Cybersecurity professional
Coursera

Jan 2025 - Jul 2025

Junior Cybersecurity Analyst
Cisco Networking Academy

EXPERIENCE

Feb 2025 - NOW

Tech Bridge Solutions Ltd

Help Desk Representative
- Resolved technical issues and provided first-line IT support to end users.
- Registered incidents, updated user records, and escalated unresolved issues to senior IT staff.
- Ensured timely resolution by coordinating with other teams to reduce downtime.

Jan 2022 – Jan 2024

Bilaal Kidz

Inventory Manager & Cashier Cum Clerk
- Implemented an inventory tracking system, reducing errors and improving accuracy.
- Processed transactions and maintained reliable financial and stock records.
- Coordinated stock reviews and reporting to support business decisions.

TECHNICAL SKILLS

- SIEM Monitoring
- Incident Response
- Threat Detection
- Log Analysis
- Networking Fundamentals
- Blue Team Operations
- Python & Scripting
- SIEM

SOFT SKILLS

- Problem Solving
- Analytical Thinking
- Teamwork
- Collaboration
- Communication
- Critical Thinking
- Adaptability
- Documentation

CERTIFICATIONS

Aug 2025

Foundations of Cybersecurity

Google

Aug 2025

Operationalizing MITRE ATT&CK for SOCs

Picus Security

May 2025

Student SOC Program

Microsoft

Jan 2025 - Jul 2025

Cyber Threat Management, Endpoint Security, Network Defense

Cisco Networking Academy

Jan 2025

Practical Help Desk

TCM Security

PROJECTS

SOC Home Lab (Defensive Cybersecurity)

- Built a virtual lab with VMs, SIEM, and IDS to simulate alerts.
- Practiced log analysis, alert triage, and incident response.

LetsDefend SOC Platform

- Completed real-world SOC analyst simulations on the LetsDefend platform.
- Investigated alerts, analyzed malicious activities, and applied incident response workflows.
- Strengthened knowledge of log correlation, threat detection, and escalation processes.

IT Help Desk Case Studies

- Documented real-world support workflows: ticketing, troubleshooting, escalation, and resolution.

LANGUAGES

- English — Proficient
- Tamil — Native / Fluent
- Sinhala — Basic / Conversational

REFERENCES

- Available upon request.
- LinkedIn recommendations and certificates are linked on my portfolio.