AR. MOHAMED RIMSAN

SOC ANALYST INTERN | IT UNDERGRADUATE

P +94 77 404 7471 E mohamedrimzanabdulraheem@gmail.com A Colombo, Sri Lanka

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

EXECUTIVE SUMMARY

Motivated 3rd-year IT undergraduate specializing in defensive cybersecurity with hands-on experience in SOC and Blue Team labs. Skilled in SIEM monitoring, alert triage, log analysis, and incident response aligned with the MITRE ATT&CK framework. Backed by professional experience in IT support, strengthening troubleshooting, documentation, and communication skills. Seeking a SOC Analyst Intern role to contribute to real-world security operations while further developing defensive security expertise.

EDUCATION

- **Bachelor of Science (Honours) in Information Technology**
  The Open University of Sri Lanka (OUSL)
  Expected Graduation: November 2027

EXPERIENCE

1. **Help Desk Representative**
   Tech Bridge Solutions Ltd, United Kingdom
   February 2025 – Present

   - Resolved 50+ technical support tickets weekly, achieving a 95% first-call resolution rate.
   - Reduced average downtime by 20% through proactive troubleshooting and escalation.
   - Documented incidents and resolutions in ticketing systems, ensuring compliance with ITIL service desk standards.
   - Identified potential security-related issues (e.g., phishing indicators) and escalated incidents following established procedures.

2. **Inventory Manager & Cashier/Clerk**
   Bilaal Kidz Sri Lanka
   January 2022 – January 2024

   - Implemented an inventory tracking system, improving stock accuracy and reducing errors.
   - Maintained financial records and prepared inventory reports to support management decisions.
   - Processed transactions and maintained reliable financial and stock records.

TECHNICAL SKILLS

- SIEM Monitoring & Alert Triage
- Incident Response Fundamentals
- Networking Fundamentals (TCP/IP, DNS, HTTP)
- Scripting: Python, PowerShell, Bash
- Operating Systems: Windows, Linux
- Log Analysis (Windows & Linux)
- Blue Team Operations
- MITRE ATT&CK Framework

SOFT SKILLS

- Problem Solving
- Communication
- Analytical Thinking
- Critical Thinking
- Teamwork
- Adaptability
- Attention to Detail
- Documentation

CERTIFICATIONS

- Google Cybersecurity Professional Certificate - Coursera
- Automate Cybersecurity Tasks with Python - Google (Coursera)
- Security Operations Center (SOC) - Cisco (Coursera)
- IT Security: Defense Against the Digital Dark Arts - Google
- Operationalizing MITRE ATT&CK for SOC - Picus Security
- Junior Cybersecurity Analyst - Cisco Networking Academy
- Cyber Threat Management, Endpoint Security, Network Defense - Cisco Networking Academy
- Practical Help Desk - TCM Security
- Cyber Kill Chains - Cybrary

PROJECTS

1. **SOC Home Lab (Defensive Cybersecurity)**

    - Designed and deployed a virtual SOC lab using virtual machines, SIEM, and IDS tools.
    - Automated repetitive security tasks using Python scripts, reducing manual triage time by 40%.
    - Triaged and investigated simulated alerts, applying incident response procedures aligned with the MITRE ATT&CK framework.
    - Documented workflows and incident reports, ensuring structured Blue Team operations for future reference.

2. **Mastercard Cybersecurity virtual experience program on Forage - January 2026**

- Completed a job simulation as a Security Analyst within Mastercard's Security Awareness Team.
- Helped identify and report security threats such as phishing.
- Analyzed and identified which areas of the business needed more robust security training and applied training courses and procedures for those teams.

3. **IT Help Desk Case Studies**

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

4. **LetsDefend SOC Platform**

- Completed real-world SOC analyst simulations on the LetsDefend SOC platform.
- Investigated alerts, examined malicious activities, and utilized incident response procedures.

LANGUAGE PROFICIENCY

- Tamil (Native) ●●●●●●
- English (Proficient) ●●●●●○
- Sinhala (Conversational) ●●●●○○

REFERENCES

1. G**ayeshan Hewa Mithige**

   Managing Director, **TECH BRIDGE SOLUTIONS LTD.**

   Address: Bartle House, 9 Oxford Court, Manchester, M2 3WQ, United Kingdom.

   Email: info@techbridgehub.co.uk

   Tel: +447951710913

2. **Mohamed Sajah Sheriff Ali**

   Head of Productions, **Fourth Milling Company**

   Address: Battoyor Tower-14th Floor, As-Safa District, Dammam, Saudi Arabia

   Email: M.sajah@mc4.com.sa

   Tel: +966509940313