RONI BIJU

Glenroy, VIC | 0433 645 614 | roniibiju@gmail.com | ronibiju.com | linkedin.com/in/ronibiju

PROFESSIONAL SUMMARY

Cybersecurity postgraduate at RMIT University specialising in Security Operations and Threat Analysis, currently working as a SOC Analyst Level 1 at Borderless CS — an ISO 27001 certified, CREST-accredited cybersecurity company. Gaining hands-on SOC experience triaging real alerts using Wazuh in a live client environment. Actively training daily through TryHackMe SOC Level 1 and LetsDefend. Pursuing CompTIA Security+ and BTL1. Seeking a junior SOC Analyst role in Melbourne to continue building on practical security operations experience.

CORE COMPETENCIES

SOC Analysis | Alert Triage | Threat Detection | Incident Response | Security Monitoring | Log Analysis
SIEM — Wazuh, Splunk | Vulnerability Management | ASD Essential Eight | NIST CSF | ISO 27001
Wireshark | Nmap | Burp Suite | Python | SQL | Bash | Linux | Windows | Azure | AWS

WORK EXPERIENCE

SOC Analyst Level 1 — Borderless CS, Melbourne | Apr 2026 – Present
ISO 27001 certified, CREST-accredited Australian cybersecurity company providing 24/7 SOC services to enterprise and government clients.

- Monitor and triage security alerts across multiple client environments using Wazuh SIEM in a live 24/7 SOC environment.
- Investigate and classify alerts including phishing attempts, brute force attacks, and suspicious network activity as true or false positives.
- Document all findings, actions taken, and escalations in line with SOC incident response procedures and client reporting requirements.
- Conduct daily client environment health checks and contribute to security monitoring across enterprise and government client environments.

Customer Success Engineer — MDrones, Melbourne | 2026 – Present
Australia's first drone gaming startup — technical support and customer success across all channels.

- Triaged and resolved complex technical issues across multiple channels using structured incident analysis and documentation practices aligned with SOC-style response workflows.
- Identified, reproduced, and escalated product vulnerabilities and technical faults to engineering teams, mirroring vulnerability reporting and ticketing processes used in security operations.
- Communicated security and technical concepts clearly to non-technical stakeholders through demonstrations and training sessions.
- Contributed to establishing data handling procedures, access controls, and secure operational practices within an early-stage startup environment.

Tech Facilitator & IT Support — Christu Jyothi Public School, India | Feb – Jun 2024

- Managed IT infrastructure including networks, servers, and end-user devices for 200+ staff and students.
- Implemented cybersecurity controls to protect sensitive student and staff data.
- Managed user access, device configuration, and first-level technical support.
- Documented incidents, technical actions, and user guidance in line with organisational procedures.

General Services Officer — Opal Healthcare, Melbourne | May – Sep 2025

- Worked in a highly regulated aged-care environment adhering to strict privacy, safety, and compliance requirements.

Retail Assistant (Part-time) — Sacca's Fine Foods & Big Fields, Melbourne | Apr 2025 – Present

- Part-time roles while completing Master's degree, demonstrating reliability and ability to manage competing priorities.

EDUCATION

Master of Cyber Security — RMIT University, Melbourne | Feb 2025 – Dec 2026
Specialisation: Information Security and Threat Analysis

Bachelor of Computer Applications (IT) — SRM University, Chennai | Sep 2021 – Mar 2024
GPA: 8.33 / 10

CERTIFICATIONS

- CompTIA Security+ (SY0-701) — CompTIA | In Progress
- Blue Team Labs Level 1 (BTL1) — Security Blue Team | In Progress
- Google Cybersecurity Professional Certificate — Google / Coursera | Jun 2023
- Cisco Introduction to Cybersecurity — Cisco / Coursera | Jan 2024
- Google IT Support Professional Certificate — Google / Coursera | Apr 2022

UNIVERSITY PROJECTS

Cybersecurity Risk Assessment — National Water Authority Case Study | RMIT University | Mar – May 2026

- Conducted a comprehensive cybersecurity risk assessment for a simulated National Water Authority undergoing digital transformation, targeting SCADA, OT networks, and enterprise IT environments.
- Applied qualitative and quantitative risk analysis as part of a seven-member team to evaluate threats, vulnerabilities, and cost-effective security controls.
- Identified critical risks including SQL injection vulnerabilities, weak Active Directory security, lack of MFA, phishing exposure, and business continuity gaps.
- Conducted ROSI analysis and identified controls mitigating up to $125M in potential annual cyber risk exposure; strategy aligned with NIST CSF and ISO 27001.

Secure Electronic Voting Platform | RMIT University | Oct – Nov 2025

- Designed 20 SMART security requirements addressing confidentiality, integrity, accountability, and non-repudiation.
- Implemented AES encryption, MFA (TOTP), RBAC, and audit logging mechanisms.
- Prevented SQL injection using parameterised queries; designed vote integrity controls using cryptographic hashing.