RONI BIJU

Glenroy, VIC | 0433 645 614 | roniibiju@gmail.com | ronibiju.com | linkedin.com/in/ronibiju | Full-time work rights — 485 visa in progress

PROFESSIONAL HIGHLIGHTS

IT Support Engineer and SOC Analyst with hands-on experience across security operations, technical support, and governance, risk, and compliance. Currently completing a Master of Cyber Security at RMIT University.

- Triaged real alerts in a live 24/7 SOC at Borderless CS, an ISO 27001-certified, CREST-accredited provider, and apply the same structured troubleshooting discipline as an IT Support Engineer at MDrones.
- Built real GRC experience through an internship at miiFile, developing privacy, consent, and AI governance frameworks against the Australian Privacy Principles, GDPR, and ISO/IEC 42001.
- Built and open-sourced a Sigma detection-engineering project mapped to the ASD Essential Eight, and a live Wazuh Alert Triage Assistant automating L1 alert analysis — an AI-augmented approach to building security tooling.

SKILLS: SOC Analysis, Alert Triage & Incident Response | IT Support — Active Directory, Windows/macOS, Device Deployment | GRC & Privacy — Data Governance, Regulatory Compliance, Responsible AI | SIEM (Wazuh, Splunk) | ASD Essential Eight | ISO 27001 | NIST CSF | Python, SQL, Bash | Linux, Windows, Azure, AWS

EXPERIENCE

MDRONES **MELBOURNE, VIC**
IT Support Engineer *Mar 2026 – Present*

- Diagnosed hardware and system issues via log analysis and fault reproduction — fixed root causes, not just symptoms.
- Triaged and escalated technical issues to engineering with structured tickets and reproduction steps — faster turnaround, no back-and-forth.
- Tracked patterns across tickets to catch systemic faults early, not just one-off fixes.
- Used AI models as part of an AI-augmented troubleshooting workflow — faster root-cause analysis, always validated against logs before escalating.
- Delivered technical onboarding, configuring systems and explaining functionality clearly — fewer early-stage support tickets.
- Kept structured documentation of incidents and resolutions for consistent knowledge transfer.

MIIFILE **MELBOURNE, VIC**
GRC, Ethics & AI Governance Intern *Aug 2026 – Present*

- Developed a Data Source Acceptability Matrix evaluating data types by consent requirement, sensitivity, and legal risk.
- Built Privacy & Consent and Data Governance frameworks covering data minimisation, third-party consent handling, access control, and retention.
- Created a Responsible AI Framework addressing bias, impersonation risk, and human oversight.
- Completed a Regulatory Compliance Assessment and Privacy Impact Assessment against the Australian Privacy Principles, GDPR, EU AI Act, NIST AI RMF, and ISO/IEC 42001.
- Assessed copyright and IP risk for AI training data.
- Collaborated with a technical security team to align policy with system implementation.

BORDERLESS CS **MELBOURNE, VIC**
SOC Analyst L1 Intern *Apr 2026 – Aug 2026*

- Worked a queue of 50,000+ security alerts across multiple client environments using Wazuh SIEM in a live 24/7 SOC environment.
- Investigated and classified alerts including phishing attempts, brute force attacks, and suspicious network activity as true or false positives.
- Documented findings, actions, and escalations in line with SOC incident response procedures and client reporting requirements.
- Conducted daily client environment health checks and contributed to security monitoring across enterprise and government client environments.
- Led exploration of OpenAEV, an open-source Adversarial Exposure Validation platform, as part of a Threat-Informed Defense proof-of-concept initiative.
- Worked as part of a 24/7 security operations team protecting Australian businesses and government organisations from cyber threats.

CHRISTU JYOTHI SENIOR SECONDARY SCHOOL **RAJAKKAD, INDIA**
Tech Facilitator & IT Support *Apr 2024 – Mar 2025*

- Provided first-level technical support for staff and students, diagnosing issues across systems, software, and connectivity through direct troubleshooting rather than blanket resets — keeping classroom and administrative technology usable with minimal downtime.
- Managed user access (Active Directory, Microsoft 365), device configuration, Freshdesk tickets and classroom technology support, setting up accounts and permissions correctly from the start — reducing avoidable access issues for staff and students across 200+ users.
- Supported secure operation of networks, servers, and end-user systems, monitoring for issues and applying fixes before they affected day-to-day teaching and administrative operations.
- Implemented cybersecurity controls to protect sensitive student and staff data, applying access restrictions and safeguards appropriate to a school environment handling minors' information — reducing exposure to unauthorised access.
- Documented incidents, technical actions, and user guidance in line with organisational procedure, creating a reference point that reduced repeat troubleshooting for common issues and supported consistency across the IT support process.

PROJECT EXPERIENCE

WAZUH ALERT TRIAGE ASSISTANT **MELBOURNE, VIC**
Personal Project — Live Tool *Sep 2026*

- Built a browser-based tool that automates the first five minutes of L1 alert triage for a Wazuh alert: extracting and enriching every indicator, mapping the rule to MITRE ATT&CK and the ASD Essential Eight, producing a scored, explainable verdict, and generating a ready-to-use markdown ticket.
- Indexed 4,423 Wazuh rules offline and integrated AbuseIPDB and VirusTotal enrichment via a rate-limited proxy with 24-hour caching, keeping API keys server-side and the tool functional even when an enrichment service is down.
- Built a 20-alert test suite covering realistic true- and false-positive scenarios (SSH brute force, encoded PowerShell, shadow-copy deletion, MFA fatigue, scanner noise) to validate and tune the scoring logic line by line rather than by guesswork.

VIRTUAL SOC LAB **MELBOURNE, VIC**
Personal Project *Aug – Sep 2026*

Network Segmentation & Threat Detection

- Built a self-hosted SOC lab to practice network defence and detection engineering end-to-end.
- Deployed OPNsense as a virtualised firewall to segment LAN/WAN traffic, configure firewall rules, and monitor interface and traffic statistics in real time.
- Integrated the firewall with Wazuh SIEM to log and alert on firewall events, simulating real-world SOC monitoring workflows.

ESSENTIAL EIGHT DETECTION LAB **MELBOURNE, VIC**
Personal Project *Mar – Apr 2026*

- Built Sigma detection rules mapped directly to each ASD Essential Eight control, closing a gap left by generic MITRE ATT&CK-only coverage.

EDUCATION

RMIT UNIVERSITY **MELBOURNE, VIC**
Master of Cyber Security — Specialisation: Information Security and Threat Analysis *Feb 2025 – Dec 2026*

SRM UNIVERSITY **CHENNAI, INDIA**
Bachelor of Computer Applications (IT) — GPA: 8.33 / 10 *Sep 2021 – Mar 2024*

CERTIFICATIONS

- CompTIA Security+ (SY0-701) — CompTIA | In Progress, expected 2026
- Blue Team Labs Level 1 (BTL1) — Security Blue Team | In Progress, expected 2026
- Google Cybersecurity Professional Certificate — Google / Coursera | Jun 2023
- Google IT Support Professional Certificate — Google / Coursera | Apr 2022