Zachary McGill

Sydney, NSW | zmcg.dev@proton.me | linkedin.com/in/zac-mcgill | github.com/z-evm

PROFESSIONAL SUMMARY

Entry-level Cyber Security Analyst with hands-on experience in log analysis, IDS alert investigation, and controlled attack simulation through structured labs and self-directed projects. Strong foundation in networking and security fundamentals, with exposure to tools such as Splunk and Suricata. Brings disciplined analytical reasoning, clear documentation habits, and calm decision-making developed in high-pressure operational environments.

SECURITY LABS & PRACTICAL EXPERIENCE

- Analysed Windows event logs and Sysmon telemetry to identify suspicious process execution, parent-child anomalies, and persistence techniques
- Investigated IDS alerts generated by Suricata in a segmented lab environment, assessing alert fidelity, false positives, and coverage gaps
- Conducted controlled attack simulations using Atomic Red Team to validate detections and understand attacker behaviour across network and host telemetry

WORK EXPERIENCE

Concurrent casual roles (2022 – Present)
Hospitality Operations (Supervisor / Manager / Senior Staff)
Sydney, NSW | 2005 – 2022

- Operated in high-pressure, time-critical environments requiring rapid prioritisation, situational awareness, and error reduction
- Managed incident-driven situations involving safety, compliance, and operational risk under strict time constraints
- Coordinated teams across shifting conditions with incomplete information, maintaining service continuity and accountability
- Communicated issues clearly to stakeholders, escalating problems decisively during peak operational periods

CERTIFICATIONS

- **Cisco CCNA: Introduction to Networks**
- **Cisco IT Essentials**

EDUCATION

- **Diploma of Advanced Programming**
- **Certificate IV in Cyber Security**
- **Certificate IV in Programming**
- **Certificate III in Web Development**

TECHNICAL SKILLS

Analysis: Log analysis, event correlation, IDS/IPS alert investigation, network traffic analysis
Systems & Networking: TCP/IP, routing, network segmentation, Windows and Linux fundamentals
Tools & Scripting: Splunk, Suricata, PowerShell, Bash