Ray Goh

rayneorshine03@gmail.com 0456978335

SUMMARY

Final-year Computer Science student specializing in security operations, threat detection, and digital forensics, with offensive security exposure in web security, binary exploitation, and reverse engineering. Experienced in SIEM based alert triage, IOC enrichment, and malware analysis within enterprise environments.

CERTIFICATIONS

COMPTIA Security+ (2025) | Cisco CyberOps Associate (2025) | GIAC Certified Forensic Analyst (GCFA) (Apr 2026)

SKILLS

- **Security Operations:** SIEM (LogRhythm, ELK), EDR (Windows Defender, Trend Micro), MITRE ATT&CK, Cyber Kill Chain, Networking Fundamentals (TCP/IP, DNS, DHCP, WAN/LAN)
- **DFIR & Malware Analysis**: Volatility, Autopsy, Wireshark (PCAP Analysis), Proxmox/KVM, YARA, Memory/Disk Forensics, Static/Dynamic Analysis
- **Offensive Security**: WebApp Security (OWASP Top 10), Burp Suite, Pwn/Re CTFs, Nmap, GDB, Fuzzing
- **Programming & Tooling**: Python, SQL, Bash, PowerShell, C, x86_64 ASM | Git, Docker, Linux/Unix, Power BI

WORK EXPERIENCE

Cloudflare

Incoming Threat Detection and Incident Response Intern *May 2026 – Aug 2026*

- Focusing on enterprise scale threat hunting, EDR telemetry analysis, and incident response workflows within a global security infrastructure.

NETS Group

Cybersecurity Operations Analyst Intern *Dec 2025 – Feb 2026*

- Triaged 50+ weekly security alerts across SIEM (LogRhythm, ELK) and EDR (Windows Defender, Trend Micro), escalating confirmed incidents and supporting L2 analysts on phishing investigations.
- Extracted actionable IOCs and correlated internal logs with external feeds (VirusTotal, AbuseIPDB), enriching incident context and supporting detection updates that improved coverage by 12%.
- Authored 2 threat intelligence playbooks and updated incident response SOPs, standardizing processes for the team's developing intel capabilities.

Cyber Security Agency of Singapore

Cybersecurity Governance, Regulations & Compliance (GRC) Intern *May 2025 – Sep 2025*

- Evaluated incident reporting legislation across 8 jurisdictions to help shape Singapore's first cyber threat attribution framework, directly informing national policy on breach disclosure.
- Assessed 300+ firms against ISO 27001 and NIST CSF controls to identify strategic capability gaps, authoring 2 executive reports that guided regulatory investment and ecosystem resilience

Shopee

Commercial Analytics Intern, SG Business Development *Feb 2023 – Apr 2023*

- Developed dynamic seller segmentation models with SQL & Python to analyse 2023 sales performance across 4000+ merchants, enabling data driven go-to market strategies and personalized partner engagement.
- Analysed 5 million+ transactions to identify commercial trends using SQL & Python, partnering with stakeholders to translate insights into 20+ strategic initiatives driving revenue growth and marketplace expansion.

HSBC

Private Wealth Management Analyst Intern, Mutual Funds & ETFs *Sep 2022 - Feb 2023*

- Supported 100+ APAC relationship managers with fund analysis and performance attribution for HNWI portfolios using Bloomberg Terminal, ensuring data accuracy for high-value client decisions.
- Automated weekly regional sales reporting pipelines via VBA, reducing manual effort by 85% and eliminating human error in data aggregation.

EXTRACURRICULARS

Bsides Tokyo **Tokyo, Japan**
Co-Speaker *May 2026*

- Co-presenting **"Cheaters Leave Footprints: Forensics of Cheats in Modern Competitive Games,"** demonstrating how anti-cheat methodologies mirror enterprise EDR systems and applying digital forensics to reconstruct post-incident gameplay activity.

UNSW Security Society (SecSoc) **Sydney, Australia**
Conferences Director *Mar 2026 - Current*

- Leading a team of 5+ students to organize SCONES 2026, UNSW's flagship cybersecurity conference with over 500+ expected attendees.

PROJECTS

60secondstofinish Automated Vulnerability Tester | Python, C, Docker, Bash *Oct 2025 – Dec 2025*

- Led a team of 4 to build a parallelized black-box fuzzer targeting native binaries, identifying 20+ memory corruption vulnerabilities (buffer overflows, OOB access, format string bugs) across 12 test applications.
- Designed format aware mutators for CSV/JSON/XML/ELF/JPEG inputs, improving test coverage by 35% and reducing false negatives.

Security Operations Homelab | Proxmox, KVM, Linux, SSH, Tailscale, Bash *Sep 2025 - Current*

- Built a multi-VM isolated environment for malware analysis and security monitoring, simulating enterprise SOC workflows and incident response scenarios.
- Implemented network segmentation and secure remote access controls via Proxmox/SSH/Tailscale, enabling safe analysis of suspicious binaries.

Web Application Security Assessment | Burp Suite, OWASP, Python, Bash

- Conducted security testing via across 8 web apps, identifying 20+ vulnerabilities (XSS/SQLi/auth bypass), producing 2 technical + executive reports with risk ratings and remediation guidance.
- Developed reusable testing scripts in Python/Bash to automate reconnaissance and enumeration tasks, reducing manual testing time by 50%.

EDUCATION

University of New South Wales **Sydney, Australia**
Bachelor of Science, Computer Science (Cybersecurity)

- WAM: 79 (Distinction)
- Relevant Coursework: Cloud Security, Digital Forensics, Web Security, Security Engineering, Computer Networks

Nanyang Polytechnic **Singapore**
Diploma with Merit, Banking and Finance

- Cumulative GPA: 3.91/4.0 (Dean's List for all semesters)