

Darren Yee

Cybersecurity Professional — Security Operations & Incident Response, GRC · CISSP, CEH

Singapore · wandererdarren@gmail.com

PROFESSIONAL SUMMARY

CISSP and CEH certified security professional with over 10 years of experience across security operations (SecOps), governance, risk and compliance, network security, and infrastructure design. Proven record in leading incident response as a Regional CSIRT Lead, managing multi-vendor 5G security platforms under IMDA mandates, executing vulnerability assessments, and automating security reporting workflows. Skilled at bridging technical defence operations with regulatory compliance frameworks including NIST, CIS CSC, and IMDA.

CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP) — ISC2, May 2024
- Certified Ethical Hacker (CEH) — EC-Council, Oct 2018

PROFESSIONAL EXPERIENCE

Murata Electronics Singapore Pte Ltd — Senior IT Security Operation Engineer (CSIRT Lead)

March 2025 – Present · Singapore

- Serve as Regional CSIRT Lead for security operations, SOC escalations, and end-to-end incident response across regional IT environments and ASEAN business units.
- Conduct platform and application vulnerability assessments with CCoE and PSIRT teams, driving Zero Trust remediation plans.
- Evaluate and lead Proof-of-Concept deployments for emerging security solutions across IT/OT environments.
- Align regional infrastructure operations with the CIS Critical Security Controls framework to strengthen defence posture.
- Report incident metrics, threat vectors and operational risk to Regional IT leadership and the Global Security team; coordinate cross-border countermeasures with overseas business units.

Antina Pte Ltd — Security Engineer, GRC & Platform Security

November 2023 – March 2025 · Singapore · promoted to Senior Security Engineer, January 2025

- Promoted to Senior Security Engineer in January 2025, in the final two months of tenure.
- Managed security operations for the 3.5 GHz C-Band RAN platform, ensuring strict compliance with IMDA 5G security mandates.
- Oversaw multi-party governance with joint-venture partners (StarHub, M1) and vendors (Nokia, AsiaPac) on threat mitigation and platform upgrades.
- Led third-party VAPT projects and coordinated regulatory audits (TCS, Mobile TIRA).
- Administered IAM, SIEM logging (QRadar), EDR, and asset-inventory scanning for the 5G security platform.
- Authored governance procedures including a software whitelisting workflow requiring joint operational and security validation.

Singapore Armed Forces, Digital Intelligence Service

July 2012 – August 2023 · Singapore

- **IT Infrastructure Engineer & Security Lead (2020 – Aug 2023, concurrent with Cyber Ops Team Lead):** led daily IT and security operations for a 4-person team, including server hardening and quarterly vulnerability assessments; architected air-gapped infrastructure with pfSense, Wazuh, Snort and a hardware air gap; managed on-premise VMware environments and implemented IBM QRadar with the vendor.
- **Cyber Ops Team Lead (2017 – 2023):** directed a 4-person team on Cyber Ops Proof-of-Concept initiatives; worked with DSTA software engineers to build a network-analysis information system from multi-source data.
- **Ops Tech Analyst (2016 – 2017):** served as intelligence analyst on a Cyber Ops Proof-of-Concept project; delivered cyber and open-source intelligence training (Shodan, Censys, VirusTotal, ZoomEye, PassiveTotal).
- **Junior Ops Tech Analyst (2014 – 2016):** designed infrastructure solutions for Proof-of-Concept projects; built reporting automation that summarised analyst reports, removing hours of manual tabulation.

SELECTED PROJECT

Integrated Intelligence System (2021) — A PHP/MySQL system that automated raw-data intake, cleaning and analysis for intelligence reporting; QGIS and Tableau turned the output into decision metrics. Cut manual report-processing time by 90%.

TECHNICAL SKILLS

- **Frameworks & Compliance:** CIS CSC, NIST, IMDA 5G Security, threat modeling, GRC policy writing
- **Security Operations & Incident Response:** CSIRT leadership, SOC management, threat hunting, air-gapped operations
- **Vulnerability & Pen Testing:** Metasploit, Nessus, Nmap, Wireshark, static & dynamic scanning
- **Security & Network Infrastructure:** Check Point, Cisco switching, F5, Fortinet, Palo Alto Panorama, pfSense, Snort, Wazuh
- **SIEM, IAM & Endpoint:** IBM QRadar, McAfee ePO, Nokia IAM/SOAR, RSA, Splunk, Trend Micro, YubiKey
- **Cloud & Virtualization:** Entra ID, VMware ESXi/vCenter/vSAN, Windows Server
- **Development & Analytics:** Java, JavaScript, MySQL, PHP, Python, QGIS, Tableau

EDUCATION

- Bachelor of Science Cyber Security and Forensics — Murdoch University, September 2023
- Diploma in Business Information Systems — Republic Polytechnic, May 2012