Flynn Townsend

Darlinghurst, Sydney NSW | 0414 304 579 |
flynntown@hotmail.com | flynntownsend.com | linkedin.com/in/flynntownsend | github.com/FlynnTownie

PROFESSIONAL SUMMARY

Bachelor of Cybersecurity graduate from the University of Technology Sydney, conferred July 2026 with Distinction (WAM 76.57). Hands-on across the blue-team stack through university project work: built a machine-learning IoT anomaly-detection pipeline feeding an Elastic and Kibana dashboard, co-authored an incident response plan for an APT38 intrusion against a bank and owned its response, recovery and lessons-learned sections, and authored an investigative Windows digital forensics expert report. Also ships software: a bar sales and reconciliation tracker in current use at a five-star Sydney hotel during events where guests purchase their own beverages, and a self-directed sales pipeline CRM built and deployed end to end to learn the sales domain and practise AI-assisted development. Also works the governance side: contributed to a group security assessment and risk report for a healthcare provider case, and planned a system replacement project end to end with a costed schedule and stakeholder plan. Strong with SIEM monitoring, detection rule authoring, log analysis, incident triage, Linux and virtualised lab environments, and Python automation, and known for staying accurate and composed under pressure from many years in high-volume customer-facing roles. Strong interest in exploring the potential of AI integrations. Australian citizen, eligible for security clearance. Available for an immediate start.

TECHNICAL SKILLS

- **Security operations and monitoring:** SIEM (Elastic and Kibana), log analysis, anomaly detection, security event triage and escalation
- **Incident response and threat intelligence:** NIST and SANS IR lifecycles, ACSC incident response planning, cyber threat intelligence, cyber kill chain and MITRE ATT&CK awareness
- **Digital forensics:** Autopsy, FTK Imager, Eric Zimmerman tools (Registry Explorer, EvtxECmd), The Sleuth Kit, ProDiscover, DB Browser for SQLite, CyberChef, hex analysis (HxD, WinHex, xxd), E01 and EnCase image handling, Windows, Linux and macOS artefact and timeline analysis, deleted-file recovery, evidence integrity and hashing, chain of custody, ENFSI-structured expert reporting
- **Networking:** Wireshark, tshark, tcpdump, Nmap, Netwox and Netwag, Aircrack-ng, Bind9, Cisco Packet Tracer, TCP/IP and OSI models, DNS, DHCP, IPv6 and 6LoWPAN, VPNs and IPSec, TLS, firewalls, protocol analysis
- **Cloud security:** AWS (EC2, IAM), ACSC-aligned cloud configuration, shared-responsibility model, IaaS, PaaS and SaaS security design, compliance-by-design, private-to-public migration risk, multi-cloud concepts
- **Programming and automation:** Python (scikit-learn, TensorFlow, PyTorch, pandas, NumPy, Matplotlib), C for embedded targets, Bash, PowerShell, SQL, Flask, Jupyter and Anaconda, KNIME, Git and GitHub Actions (CI/CD runners and secrets) and LLMs (Anthropic Claude CLI and UI)
- **Machine learning and NLP:** TF-IDF vectorisation and GloVe word embeddings, NLTK pre-processing (tokenisation, stopword removal), Keras LSTM and CNN architectures, adversarial machine learning (FGSM attack and adversarial-training defence), model evaluation with accuracy, precision, recall, F1 and confusion matrices
- **Detection engineering:** detection rule authoring, Snort IDS/IPS rule writing, KQL and Lucene queries, Packetbeat network capture, adversary emulation, Isolation Forest and Random Forest detection, intrusion, spam and DDoS detection
- **Application and offensive security:** OWASP Top 10, server-side request forgery attack and defence, SQL injection and cross-site scripting, buffer overflow and privilege-escalation concepts (Dirty COW), STRIDE threat modelling, Nmap, sqlmap, John the Ripper, WebGoat, DVWA and SEED Labs lab environments, iptables firewall policy, credential-harvesting and phishing mechanics, vulnerability management, system hardening
- **Other domains:** cryptography and PKI, blockchain and private Ethereum networks, EDR and SOAR awareness, GRC fundamentals, IoT and embedded security, iOS platform security (Secure Enclave, secure boot chain, code signing, sandboxing, data protection)
- **Risk, governance and frameworks:** NIST CSF 2.0 and SP 800-61, ASD Essential Eight, ACSC Information Security Manual, ISO/IEC 27017 and 27018, STRIDE, DREAD and CVSS risk models, SFIA 9 skills framework, Privacy Act 1988 and the Australian Privacy Principles, SOCI Act and Critical Infrastructure Risk Management Program, ACS Code of Professional Ethics, risk registers and asset inventories, business continuity and contingency planning, security awareness training design
- **Platforms and virtualisation:** Windows 10/11, Linux (Debian, Ubuntu, Kali), macOS, VMware and Oracle VirtualBox, Docker and Docker Compose, multi-VM lab topologies, Active Directory, Microsoft 365
- **Professional:** clear written and verbal stakeholder communication, structured executive communication (SCQA and the Minto Pyramid Principle), requirements elicitation and modelling (BPMN, ERD, use cases, user stories),

project scoping and estimation (work breakdown structures, activity-on-node scheduling, effort and cost estimation, PMBOK), technical documentation, peer review, high-pressure multitasking and process adherence

EDUCATION

Bachelor of Cybersecurity, University of Technology Sydney Aug 2023 to July 2026

Graduated with Distinction, WAM 76.57, conferred 22 July 2026

Tropical Data Science School, Penang, Malaysia (UTS short exchange) Jan 2025

Two-week applied data science exchange using Tableau and TensorFlow, credited towards the degree as a 6 credit-point subject. The assessed component (Distinction) was a skills-gap report benchmarking the skills demanded across ten advertised Australian cyber security and IT roles against my own, covering risk assessment and ISM/PSPF documentation, SIEM and incident response, cloud security and clearance requirements.

Diploma of Information Technology, Deakin University Feb 2022 to Jan 2023

Year 12 HSC, St Francis De Sales Regional College, Leeton 2019

Relevant coursework: System Security (HD, 88), Information Security and Management (HD, 86), Communication for IT Professionals (HD, 86), Professional Practice in Computing (HD), Cloud Security (D, 82), Business Requirements Modelling (D, 82), Cyber Threat Intelligence and Incident Response (D, 81), Network Fundamentals (D, 81), Programming 1 (D, 81), Data Analytics in Cybersecurity (D, 78), Project Management and the Professional (D, 77), IoT Security (D, 76), Digital Trace and Identity (D, 76), Cybersecurity (D, 75), Introduction to Data Analytics (D, 75), Digital Forensics (C, 73), Cryptography, Cybersecurity for Mobile Platforms, Cybersecurity Capstone Studio.

TECHNICAL PROJECTS

Digital Forensic Investigation, Windows Disk Image Analysis UTS, 2026

- Examined a 128 GB Windows host image (12 EnCase E01 segments) and a 7.8 GB USB image in a single correlated Autopsy case, verifying integrity with MD5, SHA-1 and SHA-256 hashes before analysis.
- Recovered and correlated Windows artefacts with Autopsy, FTK Imager and Eric Zimmerman tools, including registry (USBSTOR, MountedDevices), prefetch, LNK and recent-file records, deleted files and browser history.
- Proved tool execution and device usage by tying prefetch run counts and registry timestamps to a reconstructed UTC and CET timeline, and identified counter-forensic concealment (a JPEG and ZIP polyglot, AES-encrypted archives and targeted deletions).
- Answered six investigative questions in a court-style expert report for a non-technical audience, structured to the ENFSI format (context, investigative questions, summary of findings, exhibits, analysis, conclusion), with separate laboratory and analysis notes citing exact paths, timestamps and artefacts for every finding.
- Ran a second examination in the same subject on an alleged financial fraud (case 0487), recovering VersaCheck cheque-writing artefacts and account records from a Windows host image and reporting them individually, then again as part of a group report and presentation.

IsoSense, Machine-Learning IoT Anomaly Detection Pipeline (Capstone) UTS, 2025

- Trained an Isolation Forest model on the IoT-23 network dataset to flag anomalous device traffic and command-and-control beaconing, then served it through a Flask /predict API deployed on a Raspberry Pi 4 Model B acting as an IoT gateway, capturing live traffic with tcpdump.
- Built an end-to-end detection pipeline with a device simulator feeding live predictions into an Elastic and Kibana dashboard for real-time alert triage, with severity banding on the anomaly score and inference latency returned on every call.
- Benchmarked unsupervised Isolation Forest against a supervised Random Forest on accuracy, precision, recall, F1 and PR-AUC, and chose Isolation Forest for deployment because it needs no labelled samples and fits the edge-hardware budget the team set (under 50 per cent CPU and 300 MB RAM during inference).
- Delivered the team product prototype for a six-person team, covering data preparation, model training and retraining, GitHub Actions secrets for the Elasticsearch sink, and local Windows Elastic stack setup; presented twice at subject roadshows and peer-reviewed another team member's design journal.

Cyber Threat Intelligence and Incident Response, SOC Labs and Response Plan UTS, 2025

- Built a detection stack from scratch: Elasticsearch and Kibana via Docker Compose on a Kali VM, shard allocation and refresh intervals tuned for larger datasets, Packetbeat deployed for network capture, security detection rules written against that traffic, and a Windows agent enrolled for endpoint log and security data.
- Worked an APT29-style adversary emulation in the MITRE dmevals environment against a dockerised Pupy command and control listener, recording for every attack step the technique, the command, the source and target hosts, the KQL or Lucene detection query that finds it, and an analyst reading of what a hit means.

- Annotated the Cobalt Kitty threat-actor report in the MITRE ATT&CK Navigator against v16.1, producing 21 tactic and technique entries each with a written rationale, and completed a threat-actor attribution exercise on the ThreatDefence platform in an ACSC incident responder role.
- Co-authored a 42-page incident response plan for a simulated APT38 (Lazarus) intrusion against a bank, structured on the ACSC Cyber Incident Response Plan template with the NIST and SANS lifecycles, personally owning the response, recovery and lessons-learned sections, which cover containment, evidence preservation, remediation, stand-down and post-incident review.

Machine Learning for Security Detection UTS, 2025

- Built email spam and network intrusion classifiers in Python (scikit-learn, TensorFlow, PyTorch), evaluating accuracy, precision and recall on labelled datasets.
- Extended the work with a deep-learning DDoS detection model, building the training set from scratch by flooding a target with hping3 from a Kali Linux attacker VM and capturing the traffic in Wireshark, then compared LSTM, GRU and RNN architectures, with LSTM best at 97.25 per cent accuracy and 97.21 F1.
- Benchmarked four classifier architectures (SVC, logistic regression, scikit-learn MLP, and a Keras LSTM over GloVe embeddings) on the UCI SMS Spam Collection with a TF-IDF and NLTK pre-processing pipeline, reaching 97.97 per cent accuracy with the best performer.
- Implemented the Fast Gradient Sign Method against CNN and MLP classifiers trained on MNIST and CIFAR-10, driving undefended accuracy down to 13.50 per cent and 25.64 per cent respectively, then applied adversarial training across a sweep of epsilon values.
- Reported the defence honestly rather than favourably: adversarial training held above 88 per cent on MNIST across the sweep but collapsed to 9.96 per cent on CIFAR-10 at epsilon 0.03, effectively chance on a ten-class problem, and wrote it up as a failure of the defence under dimensionality.
- Published as a public repository: github.com/FlynnTownie/Cyber-Security-Data-Analytics

Security Assessment and Risk Report, Metro Healthcare UTS, 2024

- Contributed to a group security assessment report for a healthcare provider case holding 800,000 patient health records and 2 million administrative records, working each policy gap through the same structure: risks, threats, issues, possible countermeasures, legal and ethical exposure under the Privacy Act 1988, and policy improvement suggestions.
- Set out four action areas: undocumented security procedures, a password policy untouched in three years, unrestricted nationwide remote access, and low staff awareness, and recommended multi-factor authentication, password rotation, role-based access control and VPN restriction against each.
- Earlier in the same subject, contributed to a group information-asset inventory and risk assessment for the same organisation, scoring findings on likelihood, severity, vulnerability and asset sensitivity.
- Designed the management-facing half as well as the technical half: the key messages to retain from training and two training delivery methods, grounded in published cybersecurity awareness training research rather than assertion.
- Subject result High Distinction, 86.

Cross-Platform Browser Forensics, Linux and macOS UTS, 2024

- Produced an 85-page forensic comparison of Brave, Firefox and GNU IceCat across Kali Linux and macOS with two teammates, contributions recorded as an equal three-way split on the cover sheet, replicating identical user activity on each browser and each operating system so the artefacts could be compared like for like.
- Examined cookie and history databases with DB Browser for SQLite, plus cache handling, local and session storage, IndexedDB and tracker blocking, and captured the traffic side in Wireshark, then wrote per-browser business recommendations on which to deploy and why.
- Scored 75 out of 75 on the report and 20 out of 20 on the accompanying presentation.
- In the same subject's individual lab reports, acquired and analysed disk evidence with The Sleuth Kit (fsstat, fls) and ProDiscover, recovered deleted files from FAT and NTFS USB partitions, read MBR partition structures from a raw xxd hex dump, ran live response on a non-privileged Linux user against the order of volatility, and validated tool choices against the NIST Computer Forensics Tool Testing programme.

Project Management, Guest Hospitality System UTS, 2025

- Planned a hotel guest hospitality system replacement for a simulated hospitality group across five interim reports and a final briefing report to the customer, in a six-person team that produced a project charter, measurable organisational value statement, scope, stakeholder and communications plans, risk and quality strategies, a 100 to 150 task work breakdown structure and a costed schedule.
- Personally owned the executive summary, the network diagram and activity-on-node schedule, and the conclusion, with the section-by-section allocation and each member's reasoning recorded in the team's task-allocation charter.

- Sole-authored the subject ethics report on a CEO directorship conflict of interest, argued against the ACS, IEEE and PMI codes of ethics, and the individual final reflection.
- The nearest thing in the degree to scoping a client engagement: a brief in, and a defensible scope, schedule and critical path out, written for a non-technical customer audience.

Server-Side Request Forgery, Attack and Defence UTS, 2024

- Co-authored a project report on SSRF for System Security, personally owning the defence half against a partner's attack half, with the split recorded on the submission cover sheet.
- Designed the defence layer by layer: a helper server to break direct client-to-internal requests, client input validation and sanitisation, and blacklisting, whitelisting and access control, each argued together with its known bypass cases.
- Demonstrated attack and mitigation in WebGoat and grounded the analysis in the OWASP Top 10 listing of SSRF as its own category, and in research finding 52 of 68 analysed web applications weak to server-side request forgery.

Medibank Ransomware Incident Report UTS, 2026

- Wrote a short incident brief on the 2022 Medibank breach: 520 GB exfiltrated covering 9.7 million people by a threat actor linked to BlogXX, an REvil offshoot, set against ASD figures of 138 ransomware incidents in 2024-25 and a 95 per cent compromise rate once a healthcare target was engaged.
- Traced the root cause chain from a contractor's browser-saved administrative credentials through infostealer malware to a VPN that did not enforce MFA, and to EDR alerts that fired and were never triaged, with exfiltration found only by a threat intelligence analyst seven weeks later.
- Proposed a four-layer defence mapped to the ASD Essential Eight at Maturity Level 3 and zero trust: phishing-resistant MFA and just-in-time privileged access, EDR triage service levels and user behaviour analytics on data egress, micro-segmentation with field-level encryption, and an incident response plan tested against NIST CSF 2.0.

Embedded IoT Security in C, Contiki and Cooja UTS, 2025

- Added sender-side and receiver-side authentication to Contiki's RPL-UDP stack, writing C for a constrained embedded target and running two motes over 6LoWPAN under the Cooja network simulator.
- Implemented SHA-256 integrity checking across the link and demonstrated the full encrypt, transmit, decrypt and acknowledge cycle between motes with the payload recovered correctly at the receiver. The payload cipher is a Caesar cipher, a teaching cipher rather than encryption of any strength.

Applied Cryptography and Public Key Infrastructure UTS, 2025

- Built a working certificate chain end to end on Linux: generated a 4096-bit RSA key pair and installed it for key-based SSH authentication with correct permissions, stood up a certificate authority, generated a server key and certificate signing request, signed the server certificate, then configured and tested an HTTPS server against it and installed the CA into the browser trust store.
- Completed hands-on labs on one-way hash functions (SHA-256 and SHA-512), message authentication codes (HMAC and CMAC) using openssl, and the SSL/TLS handshake, and analysed an SSH man-in-the-middle attack.
- With a partner, initialised and ran a private Ethereum network under geth in isolation from the public chain, covering password-protected accounts, etherbase configuration, mining and verified transactions, framed around public-key signatures, hash functions and proof of work.

Network Attack and Defence Labs UTS, 2024

- Ran client, server and attacker labs across a three-VM topology, verifying every result in Wireshark and tshark: sniffing plaintext HTTP credentials, extracting an image from unencrypted HTTP, and OSINT footprinting of a live domain down to host, web server, reverse DNS and registrar contact.
- Executed and observed SYN flooding with randomised source addresses to defeat firewall blocking, ARP cache poisoning with MAC table verification on the target, TCP RST injection against telnet and SSH sessions, and ICMP blind connection-reset and source-quench attacks.
- Exploited SQL injection for login bypass, UNION-based extraction and file write; built a working credential-harvesting clone of a login page to understand the attack from the inside; and configured iptables on a server to permit HTTP and HTTPS and drop all other traffic.

Loan Default Classification Pipeline UTS, 2026

- Built and cross-validated a seven-classifier pipeline over 35,000 labelled records in scikit-learn with median and most-frequent imputation, one-hot encoding, scaling and three date-derived features, evaluated under 5-fold stratified cross-validation, and selected HistGradientBoosting on mean ROC-AUC of 0.860 rather than on raw accuracy because the classes are imbalanced at roughly 39 to 61.

- Caught a silent data-quality defect that would have nulled all three engineered date features on exactly the rows being scored: the training file used ISO dates and the scoring file used day-first dates, so one parse format would have coerced much of the scoring set to missing. Parsed each file with its own explicit format.

Additional academic projects UTS, 2025

- **Cloud security:** wrote a 19-page advisory report on AWS adoption for an Australian organisation covering misconfiguration, identity compromise, insecure interfaces, tenancy isolation, availability and data sovereignty, against ACSC guidance and the Information Security Manual, ISO/IEC 27017 and 27018, IRAP-assessed services and the Privacy Act 1988.
- **Wireless security:** demonstrated wireless weaknesses by cracking WEP and WPA2 in a lab and comparing both against WPA3.
- **Industry briefing:** produced a briefing document and formal speech with a group of five and delivered it to industry partner Microsoft, structured on the Minto Pyramid Principle and the SCQA framework, and owned the threat-model section covering prompt injection against a university Microsoft Copilot tenant.
- **Cloud security design:** contributed to a group design task securing a financial services workload on AWS, covering the private-to-public migration path, IaaS, PaaS and SaaS boundaries, a prevent, detect, respond and recover lifecycle, compliance-by-design, and quantitative against qualitative risk assessment.
- **Mobile platform security:** studied the iOS security architecture end to end, covering the secure boot chain, Secure Enclave, code signing, sandboxing, data protection, Face ID and Touch ID, and iOS network security across TLS, VPN, Wi-Fi, AirDrop and single sign-on.
- **Application security in IoT:** exploited and remediated web application vulnerabilities on IoT management interfaces with sqlmap, and ran Nmap port-scanning and service-fingerprinting exercises against IoT targets.

SHIPPED SOFTWARE

Dispense, bar sales and reconciliation tracker 2026

- Built and deployed a point-of-sale style tracker in current use at Sofitel Sydney Wentworth banquet bars during events requiring guests to purchase their own beverages, running on a mounted iPad through live service.
- Offline-first progressive web app: localStorage persistence, service worker caching, Supabase Postgres with row-level security, and a Node test suite over the reconciliation logic.
- Captured a real service of $985 across 37 transactions and reconciled it to the cent against the physical EFTPOS settlement slip, removing manual re-keying into MICROS.

Function., sales pipeline CRM (self-directed project) 2026

- Designed, built and deployed end to end from an empty repository to learn the sales process and practise AI-assisted development: a Kanban pipeline, enquiry tracking, activity logging and revenue analytics modelled on hotel event sales. Not deployed at the hotel.
- Next.js 16, TypeScript, Tailwind v4 and Supabase (Sydney region) with owner-only row-level security, and found and fixed a timezone defect where UTC conversion shifted Sydney dates, after verifying stored values against displayed values rather than trusting the output.

Portfolio site, flynntownsend.com 2026

- Hand-built static site with no framework, deployed on Vercel, with structured data, light and dark themes, and WCAG AA contrast verified across every page.

EXPERIENCE

Food and Beverage Attendant (Banquets), Sofitel Sydney Wentworth, Sydney NSW Aug 2024 to Present

- Earned lead bar responsibility for banquet events within three months, managing stock control, MICROS POS consumption reporting and end-of-shift reconciliation.
- Train new banquets staff on service standards and venue procedures, building clear handover and documentation habits.
- Operate under fast-paced, high-volume conditions with shifting priorities, developing the calm, accurate communication that transfers directly to a SOC environment.

Packing Line, SunRice, Leeton NSW Aug 2021 to Dec 2021

- Worked to production throughput and quality standards in a high-volume food processing environment.

Printer, Multicolor, Griffith NSW Jan 2020 to June 2021

- Operated industrial lithographic equipment to strict quality thresholds, developing process discipline and methodical troubleshooting.

Retail Assistant, Mitre 10, Leeton NSW Nov 2017 to Jan 2020

- Advised customers on technical product queries, translating complex information into plain language, and kept accurate POS and stock records.

CERTIFICATIONS AND LICENCES

- Certificate II in Hospitality (Food and Beverage)
- RSA (Responsible Service of Alcohol)
- Barista Certificate
- Driver Licence (NSW)