Nathaniel Roberts

Systems and Security Engineer | Incident Response, Networks, Automation

contact@nathanielroberts.tech | nathanielroberts.tech | linkedin.com/in/nathaniel-g-roberts | Central Coast, NSW

About

Systems engineer with a Bachelor of Cyber Security, four years across a ten-school, 2000-device environment, and a career moving into incident response. I run detection and response with Sentinel, QRadar and Defender, have led the response to real incidents including a critical CVSS 9.8 vulnerability, and design and secure the networks I defend: Juniper Mist, Palo Alto and Cloudflare Zero Trust, brought under Terraform. I keep offensive and forensic skills current through penetration testing, CTF and bug bounty. In October 2026 I join PepsiCo as a Cyber Security Incident Response Analyst.

Experience

Cyber Security Incident Response Analyst , PepsiCo — From Oct 2026

- Joining the Cyber Fusion Center to work the full incident lifecycle across a global enterprise environment.

Systems Engineer , Melos Education — Jun 2023 to present

- Led incident response across the full lifecycle for a group of 10 schools (about 1500 students, 250 staff, 2000+ devices). Contained a critical CVSS 9.8 vulnerability in the core school information system by isolating it behind the Cloudflare WAF before exploitation, timing the outage for the end of the school day, validating the vendor patch and restoring service, then wrote the incident response process the organisation had lacked.
- Monitored and investigated alerts across SIEM (Microsoft Sentinel, IBM QRadar) and EDR (Microsoft Defender, Jamf Protect), correlating firewall, identity and endpoint logs to establish root cause. Deployed QRadar on premises with endpoint agents and built a Cloudflare Logpush pipeline into it for web and DNS visibility.
- Delivered the first Juniper Mist deployment by an Australian education institution: designed and rolled out wired and wireless across 6 sites (57 switches, 160+ access points), each from High Level and Low Level Design through to as-built documentation and handoff.
- Designed and built network access control on Juniper Mist with 802.1X and EAP-TLS, pushing SCEP certificates through MDM so managed and BYO devices authenticate with certificates rather than passwords.
- Ran the edge and segmentation: Palo Alto NGFW policy, zones and NAT, VLAN segmentation across sites, and Cloudflare Zero Trust (ZTNA, WAF, Tunnel) in front of internal services.
- Brought network and platform configuration under Infrastructure as Code: Terraform for Palo Alto, Juniper Mist, Jamf and Okta, Ansible for Windows Server and Azure Arc, with every change through a Git pull request and senior approval after an early change took switches offline at several sites.
- Wrote and rolled out the organisation-wide information security and acceptable use policies against the ASD Essential 8 and NIST CSF, and led cyber assessments of newly acquired schools, producing risk registers that drove prioritised remediation.
- Migrated the student analytics platform (academic and wellbeing data) to Azure and Power BI, designing controls from the risk assessment up: MFA, RBAC, data segregated by student group, SIEM audit logging, and vendor access locked to a dedicated VPN with a firewall allow-list.
- Hardened email against a targeted business email compromise attempt with layered Cloudflare Email Security and Microsoft Defender for Office 365, plus staff awareness training.
- Relocated server rooms and replaced switches and access points within school hours with zero downtime. Automated student and staff provisioning between the student information system and Okta with Node-RED, removing a manual task that consumed helpdesk time every term.
- Mentor junior engineers and write runbooks so service desk staff can run site deployments with remote support. Progressed from Junior Systems Engineer (part-time, Jun 2023 to Nov 2024) to Systems Engineer.

Ethical Hacker, university placement , Setup International (WebSchool.au) Feb 2024 to Jun 2024

- Penetration tested a live client stack from web front end through APIs to the database using SQLmap, XSStrike, Kali Linux and custom scripts, covering injection, authentication and web application weaknesses, with threat hunting and forensic analysis of the environments tested.
- Documented severity-rated findings with remediation steps and presented them to client stakeholders, who adopted the guidance.

Service Delivery Officer , Melos Education Aug 2022 to Jun 2023

- First point of contact for technical support across school sites: incident handling and triage, onsite troubleshooting, and building the internal knowledge base.

Front End Team Supervisor , Woolworths Supermarkets Sep 2019 to Jun 2023

- Supervised a team of 15 or more in a high-volume store: rostering, shift operations, manager on duty, escalations and mentoring new team members.

Security activities

Compete in Capture The Flag events across web exploitation, forensics and reverse engineering, with write-ups published on nathanielroberts.tech. Research and report real-world vulnerabilities through bug bounty programs (Bugcrowd). Run a segmented homelab (OPNsense, VLAN per device class, Terraform-managed, monitored and backed up) and a local LLM stack for AI-assisted engineering.

Education

Bachelor of Cyber Security, Macquarie University, 2022 to 2024. Coursework included threat detection and response, digital forensics, penetration testing, privacy and risk assessment, and red, blue and purple team exercises.

Key skills

Incident response and detection: full incident lifecycle, triage, root cause analysis, post-incident review and playbooks; Microsoft Sentinel, IBM QRadar, Microsoft Defender (endpoint and email), Jamf Protect, log and artefact analysis, Cloudflare Logpush.

Networking and edge: Juniper Mist (wired, wireless, NAC), Palo Alto NGFW, Fortinet, Ubiquiti UniFi, HPE, VLAN segmentation, 802.1X / EAP-TLS, SCEP via MDM, site-to-site VPN, Cloudflare Zero Trust (ZTNA, SWG, Tunnel, WAF).

Identity and endpoint: Okta, Entra ID, Microsoft PIM, MFA, RBAC, Microsoft 365 multi-tenant, Intune, Jamf.

Automation and code: Terraform, Ansible, Node-RED, Python (advanced, 8+ years), Node.js and JavaScript, PowerShell, Bash, REST APIs, AI-assisted engineering.

Cloud and platforms: Microsoft Azure and Azure Arc, Power BI, Windows Server, Linux, Nutanix AHV, Kubernetes, Proxmox.

Risk and frameworks: ASD Essential 8, NIST CSF, risk assessments and registers, privacy impact assessment (GDPR, Australian Privacy Principles), Microsoft Purview, Tenable and Nessus; familiar with ISO 27001 and MITRE ATT&CK.

Offensive: penetration testing (web, API, database), Kali Linux, SQLmap, XSStrike, Burp Suite, Nmap, CTF, bug bounty.

Volunteering

Production and Network Leader, EV Church, 2024 to present. Designed and deployed the complete network for a 500-person annual camp (firewalls, switches, servers, wireless), operational in one day through pre-staging and planning. Serve on the camp head board and lead the production team.

Australian citizen, eligible for security clearance. Current Working With Children Check. Selected reports and write-ups: nathanielroberts.tech/projects. Last updated September 2026.