Markus Walker

Security and Cloud Engineer | Security Operations, IAM, and Offensive Security
Brisbane, Queensland | markus@markuswalker.com | +61 439 802 060
linkedin.com/in/markus-walker-au | markus-doc.github.io/cybersecurity-writeups

PROFESSIONAL SUMMARY

Cyber security and cloud practitioner with 7+ years delivering IT and infrastructure support across Shell QGC and QCLNG operational environments, backed by AWS Solutions Architect Associate, Oracle Cloud Infrastructure certifications, and a completed Certificate IV in Cyber Security.

Experience spans cloud and endpoint security, Microsoft Entra ID identity and access management, network transformation, and operational technology environments where reliability, access control, and service continuity were critical. Active hands-on practitioner across security operations, offensive security, and cloud security, with practical experience in Splunk SIEM monitoring, incident response design aligned to NIST SP 800-61, Active Directory tradecraft, web application testing, and AI security aligned to OWASP LLM Top 10 and MITRE ATLAS.

TECHNICAL SKILLS

Security Operations and Detection. Splunk Enterprise, SIEM operations, log analysis and ingestion, Windows host and network adapter monitoring, Windows Security Events, alert triage, anomaly detection, incident response lifecycle, evidence preservation, chain of custody, SOC and CSIRT concepts, SOAR concepts

Offensive Security and Red Team Tradecraft. Kali Linux, Metasploit Framework, Meterpreter, msfvenom, Impacket, Searchsploit, Rubeus, mimikatz, evil-winrm, pywinrm, chisel, hashcat, Nmap, Rustscan, Wireshark, tcpdump, Burp Suite, Nikto, ffuf, WhatWeb, Active Directory Kerberos attacks including Golden Ticket and DCSync

AI Security and Governance. prompt injection and defence, jailbreaking, LLM security, AI threat modelling, AI supply chain security, RAG security, data poisoning, sensitive information disclosure, AI forensics, AI system reconnaissance, secure AI system design

Cloud and Cloud Security. AWS, Amazon VPC, EC2, RDS Multi-AZ, ALB, Auto Scaling, Route 53, AWS WAF, Shield, CloudTrail, CloudWatch, GuardDuty, Security Hub, Inspector, Macie, AWS Config, IAM Identity Center, Cognito, Secrets Manager, KMS, Systems Manager Session Manager, CloudFormation, Oracle Cloud Infrastructure, Microsoft Azure, Microsoft 365, Microsoft Intune, Azure AD Join, Windows Autopilot, Entra ID

Identity, Endpoint, and Network Security. Identity and access management, role-based access control, MFA and conditional access, Active Directory security, vulnerability management, firewalls and NGFW, IDS and IPS, EDR and XDR concepts, network segmentation, VLAN design, PKI, SSL and TLS, VPN and OpenVPN, Cisco, Aruba, Cel-Fi, Starlink, Motorola TETRA

Frameworks, Standards, and Regulations. NIST Cybersecurity Framework, NIST SP 800-61, MITRE ATT&CK, MITRE ATLAS, Essential Eight, CIS Controls, OWASP Top 10, OWASP LLM Top 10, ISO 27001, PCI DSS, ISM, PSPF, Privacy Act 1988, Australian Privacy Principles, Notifiable Data Breaches scheme, GDPR, Consumer Data Right, Security of Critical Infrastructure Act 2018

Scripting, Automation, and Delivery. Python, PowerShell, shell scripting, defensive coding, CSV processing, cross-platform Windows and Linux automation, system audit tooling, ServiceNow, Maximo, Power BI, Cisco Unified Communications Manager, Microsoft Teams Rooms, ClickUp, Obsidian, vendor coordination, change management, technical documentation

PROFESSIONAL EXPERIENCE

Independent Cyber Security Practitioner | **Independent** | Aug 2025 to Present

Dedicated upskilling period focused on cyber security, cloud, offensive security, and AI security practice.

- Completed Certificate IV in Cyber Security and achieved AWS Solutions Architect Associate, Oracle Cloud Infrastructure 2025 Architect Associate, Oracle Cloud Infrastructure 2025 Foundations Associate, and Oracle Cloud Infrastructure 2025 Generative AI Professional credentials.
- Actively preparing for ISC2 Certified in Cybersecurity and CompTIA Security+, with exams scheduled within two weeks.
- Built active offensive security practice through a personal home lab and TryHackMe under the handle Triage, progressing through Active Directory red team tradecraft including Kerberos abuse, credential harvesting, tunnelling, pivoting, and GPU-accelerated cracking.
- Completed structured AI security learning covering prompt injection and defence, jailbreaking, LLM security, AI threat modelling, AI supply chain security, RAG security, and data poisoning, aligned to OWASP LLM Top 10 and MITRE ATLAS.
- Published the Red Team Capstone Crawl-Through to a GitHub Pages portfolio site, with additional write-ups in active preparation.

IT Field Engineer | **Tata Consultancy Services** | May 2019 to Aug 2025

Embedded contractor supporting Shell QGC and QCLNG upstream and midstream operations across remote Queensland energy and gas infrastructure environments.

- Delivered IT field engineering across 20+ remote operational sites including camps, plants, and drilling environments in a FIFO role covering planned delivery, escalations, and after-hours support.
- Maintained business-critical Microsoft 365, Entra ID, networking, and telecom platforms across a large distributed operational footprint, supporting field productivity and site safety.
- Executed network transformation and wireless uplift, including 300+ Cisco to Aruba access point replacements, covering patching, cabling, cutovers, and stabilisation.

- Delivered connectivity uplift across 600+ field vehicles using Cisco IR829 and Cel-Fi, and extended remote operations with Starlink, improving deployment reliability through fault diagnosis and SIM standardisation.
- Managed endpoint lifecycle across six annual refresh cycles, deploying and validating enterprise laptops and rugged devices under strict change control and security standards.
- Administered Entra ID IAM across a dispersed workforce, supporting access governance, RBAC, device compliance, and endpoint modernisation to Intune, Autopilot, and Azure AD Join.
- Coordinated with vendors and site teams across multiple locations to support telephony, AV, and workplace technology rollouts, including Microsoft Teams Rooms and CUCM environments.

Junior Network Engineer | **Data#3** | Jan 2019 to May 2019

Contractor supporting the Shell QGC Enterprise Network Transformation project.

- Contributed field execution and cutover coordination for the Shell QGC Enterprise Network Transformation project, covering live-environment switching, routing, cabling, and site delivery across operationally critical infrastructure.
- Supported early Cisco to Aruba network standardisation activity and vehicle connectivity uplift across remote QGC sites, building the operational foundation that carried into the later embedded TCS role.

SELECTED PROJECTS AND TECHNICAL PROOF

Red Team Capstone, Active Directory Forest Compromise. Executed a full compromise of a multi-domain Active Directory forest lab across segmented networks. Chained chisel and netsh portproxy tunnels through intermediate workstations, executed Kerberos attacks including Golden Ticket via Rubeus and DCSync against a domain controller, exploited unconstrained delegation, and used evil-winrm, pywinrm, Metasploit, and Covenant to support lateral movement and post-compromise activity. Write-up: markus-doc.github.io/cybersecurity-writeups/articles/tryhackme/rtcc/1-Red_Team_Capstone_Crawl-Through

Cloud Security Architecture, AWS. Designed a secure AWS target architecture for a two-tier web application covering availability, identity, encryption, monitoring, incident response, and disaster recovery. Services included VPC segmentation, ALB, EC2 with Auto Scaling, RDS Multi-AZ, Route 53, AWS WAF, GuardDuty, Security Hub, Inspector, Macie, IAM Identity Center, Secrets Manager, KMS, and Systems Manager Session Manager.

SIEM and SOC Lab, Splunk Enterprise. Installed and operated Splunk Enterprise to ingest, search, and report on security log data. Monitored Windows network adapter activity, built searches and reports, applied baselining and anomaly detection, and exported outputs for stakeholder reporting.

Web Application Penetration Testing. Performed authorised web application testing in controlled labs using Burp Suite, Nikto, and Nmap. Identified and demonstrated OWASP-aligned vulnerabilities including SQL injection, broken authentication, broken access control, IDOR, command injection, SSRF, and security misconfiguration, then produced structured test reports with remediation recommendations.

Incident Response Program Design. Planned and documented an enterprise-style incident response project including a charter, communications plan, team structure, metrics such as MTTD and MTTR, and stakeholder reporting. Evaluated an Incident Response Plan against NIST SP 800-61 and developed an improved IRP with clearer severity classification, escalation paths, evidence handling, recovery, and lessons learned processes.

AI Security Practice. Completed a structured learning path covering AI fundamentals, secure AI system design, prompt injection and defence, jailbreaking, AI supply chain security, RAG security, and data poisoning. Hands-on labs included ContAInment, LLMborghini, White Rabbit, Payload, UnIndexed, and Lockdown, reinforced by Oracle Cloud Infrastructure Generative AI Professional certification.

TryHackMe, Top 1%. Public profile with hands-on labs and documented write-ups across offensive, defensive, and incident response practice. tryhackme.com/p/Triage

EARLIER EXPERIENCE

QGC Contractor, Rotating Site Roles | MSS, ECM and Protech | 2012 to 2019. Maintained continuous employment across the QGC operational environment through security, site support, HSSE-adjacent, administrative, trades assistance, plant build, commissioning, and handover roles, building deep familiarity with the operational footprint.

Audio Engineer and Systems Technician | Airco Audio, USA | 2005 to 2012. Worked in live production environments with networked control systems, cabling, and real-time system management under operational pressure.

EDUCATION

Certificate IV in Cyber Security (22603VIC), TAFE Queensland | Completed and conferred Mar 2026

Selected areas included incident response, network security infrastructure, web security vulnerabilities, cloud-based security systems, automation, scripting, and enterprise incident response planning.

CERTIFICATIONS

- AWS Certified Solutions Architect Associate, Amazon Web Services | Issued Nov 2025, expires Nov 2028
- Oracle Cloud Infrastructure 2025 Architect Associate, Oracle | Sep 2025
- Oracle Cloud Infrastructure 2025 Foundations Associate, Oracle | Sep 2025
- Oracle Cloud Infrastructure 2025 Generative AI Professional, Oracle | Sep 2025
- ISC2 Candidate, (ISC)2 | Active, CC exam scheduled within two weeks

Referees: Available on request.