Markus Walker

Brisbane, Queensland | markus@markuswalker.com | +61 439 802 060
Portfolio: www.markuswalker.com | LinkedIn: linkedin.com/in/markus-walker-au

Security Engineer | Cloud Security | AWS SAA, OCI Certified | Security Operations, IAM and IT/OT Infrastructure

PROFESSIONAL SUMMARY

Cybersecurity and cloud security engineer with 7+ years delivering IT, infrastructure and field engineering across Shell QGC and QCLNG upstream and midstream operational environments, supported by AWS Certified Solutions Architect Associate, Oracle Cloud Infrastructure certifications and Certificate IV in Cyber Security. Hands-on practitioner across security operations, cloud security architecture, identity and access management, offensive security and AI security, with applied work in Splunk SIEM threat detection, incident response design aligned to NIST SP 800-61, Active Directory red team tradecraft, web application penetration testing and AI security aligned to OWASP LLM Top 10 and MITRE ATLAS. Experienced in large-scale IT/OT adjacent environments where access control, endpoint security, network segmentation and service continuity are operationally critical.

TECHNICAL SKILLS

Security Operations and Threat Detection. Splunk Enterprise, SIEM operations, log analysis and ingestion, Windows Security Event monitoring, alert triage, anomaly detection, threat hunting foundations, incident response lifecycle, evidence preservation, chain of custody, SOC and CSIRT concepts, SOAR concepts

Offensive Security and Vulnerability Assessment. Kali Linux, Metasploit Framework, Nmap, Rustscan, Wireshark, tcpdump, Burp Suite, Nikto, ffuf, WhatWeb, Active Directory Kerberos attack chains including Golden Ticket and DCSync, credential harvesting, lateral movement, tunnelling and pivoting, GPU-accelerated password cracking, penetration testing, red team tradecraft

AI Security and Governance. LLM security, prompt injection and defence, jailbreak testing, AI threat modelling, AI supply chain security, retrieval augmented generation (RAG) security, data poisoning, sensitive information disclosure, secure AI system design, OWASP LLM Top 10, MITRE ATLAS

Cloud Security and Cloud Architecture. AWS, Amazon VPC, EC2, RDS Multi-AZ, ALB, Auto Scaling, Route 53, AWS WAF, AWS 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 (OCI), Microsoft Azure, cloud security architecture, cloud governance

Identity, Endpoint and Network Security. Identity and Access Management (IAM), role-based access control (RBAC), MFA, conditional access, Privileged Access Management (PAM) concepts, Active Directory security, Microsoft Entra ID, Microsoft Intune, Windows Autopilot, Azure AD Join, vulnerability management, endpoint detection and response (EDR) and XDR concepts, network segmentation, VLAN design, firewalls and NGFW, IDS and IPS, PKI, SSL and TLS, VPN and OpenVPN, zero trust concepts, Cisco, Aruba, Cel-Fi, Starlink, Motorola TETRA

Frameworks, Standards and Regulations. NIST Cybersecurity Framework, NIST SP 800-61, MITRE ATT&CK, 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, endpoint audit automation, CSV processing, cross-platform Windows and Linux automation, ServiceNow, Maximo, Power BI, change management, technical documentation, vendor coordination

PROFESSIONAL EXPERIENCE

Independent Cyber Security Practitioner | Independent | Aug 2025 to Present

Independent practice period focused on cybersecurity, cloud security engineering, security operations, offensive security and AI security.

- Achieved AWS Certified Solutions Architect Associate, Oracle Cloud Infrastructure 2025 Architect Associate, Oracle Cloud Infrastructure 2025 Foundations Associate and Oracle Cloud Infrastructure 2025 Generative AI Professional certifications alongside Certificate IV in Cyber Security.
- Built an active offensive security practice through a personal home lab and structured platform-based training, advancing through Active Directory red team tradecraft including Kerberos abuse, credential harvesting, lateral movement, tunnelling, pivoting and GPU-accelerated cracking.
- Completed structured AI security training covering prompt injection and defence, jailbreak testing, LLM security, AI threat modelling, AI supply chain security, RAG security and data poisoning, aligned to OWASP LLM Top 10 and MITRE ATLAS.
- Advancing preparation toward ISC2 Certified in Cybersecurity and CompTIA Security+ while maintaining practical lab work and a publicly documented technical portfolio.
- Designed and published a self-developed professional portfolio web application at www.markuswalker.com, linking resume, technical write-ups, GitHub and hands-on proof of work.

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, gas plants and drilling environments in a FIFO model, 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 across operationally critical sites, covering patching, structured cabling, cutovers and post-change stabilisation.
- Delivered connectivity uplift across 600+ field vehicles using Cisco IR829 and Cel-Fi, and extended remote operational coverage with Starlink, improving deployment reliability through fault diagnosis and SIM standardisation.
- Administered Entra ID IAM (Identity and Access Management) across a dispersed workforce, supporting access governance, RBAC, device compliance and endpoint modernisation including Microsoft Intune, Windows Autopilot and Azure AD Join.
- Managed endpoint lifecycle across six annual device refresh cycles, deploying and validating enterprise laptops and rugged field devices under strict change control and security standards.
- Coordinated with vendors and site teams to support telephony, AV and workplace technology rollouts including Microsoft Teams Rooms and CUCM environments across multiple remote locations.

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, structured cabling and site delivery across operationally critical infrastructure.
- Supported early Cisco to Aruba network standardisation and vehicle connectivity uplift across remote QGC sites, building the operational foundation extended through the later embedded TCS engagement.

SELECTED PROJECTS AND TECHNICAL PROOF

Red Team Capstone, Active Directory Forest Compromise. Executed a full end-to-end compromise of a multi-domain Active Directory forest lab environment across segmented networks. Chained tunnel pivots through intermediate workstations, executed Kerberos attack chains including Golden Ticket and DCSync against a domain controller, exploited unconstrained delegation, and used a range of offensive tooling to support lateral movement and post-compromise activity. Full portfolio write-up at www.markuswalker.com.

Cloud Security Architecture, AWS. Designed a secure AWS target architecture for a two-tier web application covering availability, identity, encryption, threat detection, 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 Operations Lab, Splunk Enterprise. Deployed and operated Splunk Enterprise to ingest, search and report on security log data. Monitored Windows host and network adapter activity, built detection searches and operational reports, applied baselining and anomaly detection, and produced stakeholder reporting outputs.

Web Application Penetration Testing. Performed authorised web application security testing in controlled lab environments 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, and produced structured test reports with remediation recommendations.

Incident Response Program Design. Planned and documented an enterprise-grade incident response program including charter, communications plan, team structure, detection and recovery metrics (MTTD and MTTR) and stakeholder reporting. Evaluated an existing Incident Response Plan against NIST SP 800-61 and produced an improved IRP with clearer severity classification, escalation paths, evidence handling, recovery procedures and lessons learned processes.

AI Security Practice. Completed a structured learning path covering secure AI system design, prompt injection and defence, jailbreak testing, LLM security, AI supply chain security, RAG security and data poisoning, with hands-on AI security lab work across a range of attack and defence scenarios. Reinforced by Oracle Cloud Infrastructure Generative AI Professional certification.

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

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

EDUCATION

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

Areas covered included incident response planning, network security infrastructure, web application security vulnerabilities, cloud-based security systems, automation and scripting, and enterprise incident response program design.

References available on request.