Ross Partridge

Mobile: 0272796965
E-Mail: rjpartridge@windowslive.com
Location: Auckland based

Skills

Security Operations

- Incident response & triage
- Threat containment & remediation
- Log investigation & correlation
- Email security & mail flow analysis
- MFA security & token compromise response

Identity & Access

- AD / Entra ID Hybrid environments
- Conditional Access fundamentals
- AAA (Authentication, Authorization, Accounting)
- Secure RDP architecture

Security Technologies

- Exchange Online protection rules
- VPN security configuration
- SharePoint ACL security
- OAuth concepts

Foundations

- Networking fundamentals
- Windows Server administration
- Risk awareness & mitigation mindset

Certifications

CompTIA Security+ 05/2025

Summary

Security-focused IT professional with hands-on experience in incident response, identity security, and Microsoft 365 environments. Demonstrated ability to detect, contain, and mitigate real-world threats, including SQL injection and MFA token compromise. Strong practical experience securing hybrid AD/Entra environments and implementing access controls. Seeking to transition into a dedicated security role.

Experience

Systems Engineer/Administrator - 07/2023 to Present
First-IT, Auckland, New Zealand

Security & Incident Response

- Mitigated live SQL injection attack causing email flooding; implemented containment via Exchange rules and evidence capture
- Responded to MFA token theft incidents and secured affected accounts
- Investigated suspicious Entra ID sign-ins and correlated audit log activity to identify potential account compromise
- Performed phishing email analysis including header inspection, sender validation, and threat assessment
- Monitored Entra ID and Microsoft 365 audit logs for anomalous behavior and security indicators
- Designed secure RDP environments with Authentication, Authorization, and Accounting (AAA) controls

---

Identity Security

- Administration of hybrid AD–Entra ID environments
- Management of secure provisioning of domain and Entra-joined devices
- Investigation of identity-related alerts and unusual sign-in behaviors
- Assisted with remediation steps for potentially compromised accounts

---

Security Hardening

- Implemented VPN security configurations
- Designed SharePoint permission structures following least-privilege principles
- Provided recommendations to mitigate web form injection risks
- Implemented Exchange mail flow rules to reduce abuse and spam impact