RNZ TE REO IRIRANGI O AOTEAROA

Security Engineer

Job Description

Date	August 2026
Location / Business Unit	Auckland/Wellington Hybrid
Reporting to	Cyber Security Lead
Functional Relationships	Cyber Security Lead IT Operations / System Administrators Network Administrators Managed Security Service Providers Support Analysts Wider Technology and Product Team All users of RNZ technology and IT systems
Position Type	Full-time Permanent

Te Tūranga - About the Role

RNZ's security programme has grown significantly, establishing foundational controls across endpoint, identity, and cloud environments. As the programme matures, there is a growing need for dedicated technical delivery capacity to ensure security controls are continuously operating, improved, and expanded. This role exists to provide that capability and maintain, configure and continuously improve RNZ's security tooling stack, including detection, endpoint management, identity, and data governance platforms.

Additionally, the Security Engineer will be responsible for the day-to-day operation of RNZ's security environment — managing and maturing the security tooling stack (XDR, SIEM/SOAR, endpoint management, cloud identity, and data governance platforms), driving vulnerability remediation, and expanding detection capability.

This is a hands-on technical role for a security practitioner who thrives on building and maintaining security controls.

Te Mahi – About the job

- Be the first point of contact with managed security service providers, coordinating escalations, track resolution progress, and tuning detection rules to improve alert quality and reduce false positives.
- Investigate and respond to security alerts by reviewing escalations, conducting detailed analysis, coordinating remediation activities, and driving incidents through to closure.
- Monitor and assess the evolving threat landscape impacting RNZ, identify emerging risks and recommend mitigation strategies and security improvements to the Cyber Security Lead.
- Support incident response processes, including participating in after-hours on-call incidents, in accordance with RNZ's incident response framework.
- Manage RNZ's end-to-end vulnerability remediation process by maintaining scanning coverage, prioritising findings based on risk and SLAs, coordinating remediation efforts, validating closure, and reporting progress.
- Manage device security configuration, compliance policies, and application protection across the organisation.
- Develop and maintain SIEM analytics rules, detection workbooks, and automation playbooks to enhance threat detection capabilities and improve operational efficiency.
- Manage and strengthen identity, access, application, and data protection controls, including conditional access, privileged access management, identity governance, SSO, SAML/OIDC identity federation, DLP, sensitivity labels, and data lifecycle policies.
- Maintain security documentation, technical runbooks, configuration baselines, and audit records; contribute to security policy development; and provide security guidance and technical support to IT teams and kaimahi.

Ōu Pūkenga - About You

Qualifications	• Relevant IT or security qualification preferred. Job experience and demonstrated practical skills will also be considered. • Vendor security certifications preferred: security operations, identity and access management, or cloud security certifications from a recognised vendor. Equivalent hands-on experience considered.
Knowledge & Experience	• Extensive experience in a hands-on IT security, security engineering, or systems/infrastructure role with significant security responsibilities. • Practical experience operating and maintaining security controls across endpoint, identity, and cloud environments, with specific hands-on experience across the security tooling stack (XDR, SIEM/SOAR, endpoint management, cloud identity, and data governance platforms). • Experience with vulnerability management programmes — scanning, tracking, prioritising, and verifying remediation. • Strong working knowledge of the cloud identity and endpoint management platforms — conditional access, privileged access management, compliance policies, and device management.

	• Experience managing device security configuration, compliance policies, and application deployment via the endpoint management platform across a corporate environment. • Awareness of security frameworks such as NIST CSF, ISO 27001, or equivalent. Familiarity with NZISM or NZ government cyber security guidance advantageous. • Ability to write clear technical documentation, runbooks, and standard operating procedures. • Experience working with a managed SOC/MDR provider — reviewing detections, escalating incidents, and ensuring SLA alignment. • Practical sysadmin or infrastructure experience is a strong advantage — comfortable navigating the environments being secured.
Skills	• Strong diagnostic and problem-solving ability — works through novel or ambiguous security issues methodically. • Good organisational ability — prioritises effectively, follows through, and manages multiple concurrent workstreams without losing detail. • Clear written communication — produces accurate technical documentation, runbooks, and incident reports. • Works effectively both independently and collaboratively, communicating clearly with technical and non-technical colleagues alike.
Personal Attributes	• Ownership mentality — takes initiative and follows tasks through to completion without needing to be directed. • Curiosity and continuous learning — stays current with the threat landscape and emerging security tooling. • Comfortable operating in a lean environment where priorities can shift quickly. • Supports colleagues and end users with patience and clear communication regardless of their technical level. • Dependable and methodical in handling sensitive security matters with appropriate discretion.

Te Ahurea – Our Culture

RNZ Attitudes

RNZ Attitudes are all about how we work. These attitudes are how we demonstrate our culture through our everyday actions, behaviour and decisions. They drive how we do things, what we value and what's expected of us. They exist so that RNZ is a culture for everyone to enjoy and flourish in.

We're bold and think big. We find a way to make things happen. We learn best by doing. We believe that trying and failing is better than not trying at all.

We deal with problems or new tasks with energy and creativity. We try new things, we evolve and we move fast.

We encourage people to flourish. we extend love and compassion to others and nurture relationships. We have collective strength and cherish individuality.