

Position description



Title Site Reliability Engineer - Network	Reports to Network & Security Manager
Division Transformation & Technology	Department Network & Security
Location Auckland	Last updated October 2023

Our commitment as a Crown Entity

Ka mahitahi mātou o te ratonga tūmatanui kia hei painga mō ngā tāngata o Aotearoa i āiane, ā, hei ngā rā ki tua hoki. He kawenga tino whitake tā mātou hei tautoko i te Karauna i runga i āna hononga ki a ngāi Māori i raro i te Tiriti o Waitangi. Ka tautoko mātou i te kāwanatanga manapori. Ka whakakotahingia mātou e te wairua whakarato ki ō mātou hapori, ā, e arahina ana mātou e ngā mātāpono me ngā tikanga matua o te ratonga tūmatanui i roto i ā mātou mahi.

In the public service we work collectively to make a meaningful difference for New Zealanders now and in the future. We have an important role in supporting the Crown in its relationships with Māori under the Treaty of Waitangi. We support democratic government. We are unified by a spirit of service to our communities and guided by the core principles and values of the public service in our work.

Role purpose

The role reports to the Network & Security Manager and will be responsible for maintaining and implementing network & security solutions that meet LNZ's security, availability and capacity requirements.

The role is best suited to someone who has a desire to learn the elements of network & security design as well as be hands on to work with network, security and CI/CD technology. The role will support the LNZ cybersecurity capability in the areas of network architecture, security operations, threat intelligence and incident response.

The role will collaborate closely with other members of the LNZ Security and Risk teams to ensure solutions are fit for purpose and are compliant with applicable regulations and standards.

What you will focus on

System Availability & Support

Production system availability:

- Support the production environment and resolve issues, ensuring a high level of availability of production systems to meet agreed SLA's.
- Ensure all production networks have necessary monitoring in place to ensure reliable delivery of services to customers, and issues are proactively mitigated where possible.
- Ensure production networks are adequately sized to meet agreed business expectations.

Environment Support:

- Ensure all production systems and networks comply with Lotto NZ BCP guidelines and adequate capacity planning is in place to scale to meet growth.
- Work with the QA and Development managers to ensure all non-production networks are fit for purpose & are available to meet project demands and production support requirements without delay.
- Work closely with the IT team to improve end-to-end automation of provisioning and eliminate repetitive manual tasks.

Network & Security Operations

- Working closely with other Security and Risk team members to both proactively monitor threat intelligence sources and reactively respond to incidents.
- Assist with the day-to-day operations of the LNZ networks and related security systems, including upgrades and project-driven changes when required.
- Working closely with project teams to ensure end-to-end security design is provided satisfying the requirements of the business.
- Experience with working in a DevOps/Site Reliability Engineering environment, including Agile project methodology and code creation/maintenance.
- Assist LNZ with reducing cyber risk in the areas of network architecture, security operations, threat intelligence and incident response.
- Work toward gaining professional membership of one or more external security organisations (e.g., ISACA, NZITF, SANS, etc.).
- Respond to security incidents at a technical level as directed by the authorised LNZ incident coordinator.
- Design and implement overlay network components capable of leveraging underlay networks to support dynamic workloads as required.
- Assist the Network and Security Manager and Senior SRE with delivering the security goals and milestones as specified in the LNZ technology roadmap.

Change Control

- Adhere to the internal software change control process for changes.
- Ensure that external suppliers are following Lotto NZ Change Control processes and to test their processes when required.

Other

- Any other duties as reasonably required by your manager or other key stakeholders.
 - Ensure all company policies, procedures and guidelines are followed and adhered to.
 - Take an active role in promoting and ensuring a safe and healthy workplace at Lotto NZ for yourself and others.
 - Lotto NZ's purpose is to provide safe gaming that allows New Zealanders to play and win while contributing money back to New Zealand communities: Ensure that minimising the potential for harm from our games is a key consideration in all day-to-day activities and decision making, through adhering to all Lotto NZ responsible gaming processes and policies.
-

-
- Ensure the Lotto NZ Health and Safety policy is adhered to (including procedures in the Health and Safety Manual) and hazards, incidents and near misses are reported in the Health and Safety system in a timely manner.
 - Comply with all Lotto NZ security policies and instructions, complete all required security awareness training and report any security incidents or concerns in a timely manner.
 - Due to the sensitive nature of your role, you will comply with undertaking criminal conviction history checks during your employment, adhering to Lotto NZ vetting procedure.
 - Due to the sensitive nature of your role, you will comply to completing a credit check at the start of your employment.
-

Your skills and experience

Technical skills

- Capable of rapid and in-depth understanding of emerging technologies and their relevant application.
- Experience with and some knowledge of hosting provider network systems.
- Exposure to incident response situations.
- Development using Python and Shell Scripting.
- Virtualization - VMWare and AWS.
- Agile and DevOps engineering practices and CICD tools.
- Proficient in network and security infrastructure, including routers, switches, firewalls, and VPNs. Familiarity with CI/CD tools and practices.
- Ability to design, implement, and manage secure and scalable network architectures that meet the company's requirements

Core Competencies

- **Problem-Solving:** Strong analytical skills to troubleshoot and resolve complex network issues, ensuring high availability and performance.
- **Security Operations:** Knowledge of security operations, including monitoring, threat detection, and incident response. Ability to implement security measures to protect systems against cyber threats
- **Collaboration:** Work effectively with cross-functional teams to develop security strategies and ensure compliance with industry standards and regulations.
- **Continuous Learning:** Eagerness to stay updated with the latest network and security technologies and trends. Commitment to continuous improvement and professional development.
- **Risk Management:** Understanding of risk management principles and the ability to apply them in the context of network security to mitigate potential threats.
- **Communication:** Excellent communication skills to articulate technical concepts clearly to non-technical stakeholders and to document network designs and procedures.
- **Regulatory Compliance:** Familiarity with applicable laws, regulations, and standards affecting network security, and the ability to ensure that all solutions are compliant.
- **Innovation:** A forward-thinking mindset to explore new network technologies and security solutions that could benefit the organization.

Experience

- Previous experience in operating network and security technologies.
-

-
- Exposure to the handling and responding of Internet security attacks/incidents.
 - Experience with automated CI/CD pipelines.
 - Experience with the operation of large-scale network topologies.
 - Experience of containerization and container hosting solutions such as Kubernetes.
 - Experience with DevOps practices & tools.
 - Understanding of security principles associated with networks, proxies, internet, firewalls, routers & VPNs.
 - Limited understanding of current legislation and governing network security standards.
 - A desire to learn more about emerging security technologies and strategies and their application to enterprise.

Qualifications

- Bachelor's degree in the field of computer science or equivalent.
 - Vendor certifications as appropriate.
-

Authorities

People responsibilities:

- 0 people

Signature authority of:

- \$0
-