Cybersecurity Analyst - Endpoint

Position Description

Team:	Cybersecurity Team	**Location:**	Wellington
Reports to:	Cyber Operations Manager		
Role Type:	Permanent		

About Us

KiwiRail's Role in Aotearoa, New Zealand

KiwiRail, a proud State-Owned Enterprise, delivers sustainable and inclusive growth for our customers, communities, and people.

For more than 150 years, rail in New Zealand has connected communities, delivered freight and passengers around the country, and showcased our spectacular scenery to the world. Our purpose—Hononga Whaikaha, Oranga mo Aotearoa (Stronger Connections, Better New Zealand)—speaks to connection with our customers and the future needs of their businesses, connection with the communities we serve and operate in, and connection with each other. KiwiRail is carrying this legacy into the future, delivering connected rail and shipping transport services that create economic, social, and environmental value for New Zealand and New Zealanders.

KiwiRail is in a phase of significant transformation to modernise and grow our rail and Interislander ferry.

Our Workplace

At KiwiRail, our values define the behaviour we expect from everyone. We have a team of over 4500 people, and every connection we make with each other, our union partners, our customers and all our stakeholders must be of the highest standard.

Safety, health, and well-being are our number one priority, ensuring our people return home safe and healthy every day.

About the Role

Purpose of the role

The Digital and Information and Communication Technology Group (ICT), provides a wide range of ICT planning, implementation, operation and support services as a shared service to the KiwiRail Group.

The Cybersecurity Team ensures that KiwiRail can safely carry out its transformed activities whenever and wherever these activities involve ICT through assuring the Confidentiality, Integrity and Availability of information and information systems.

The Cybersecurity Analyst will assist in the support and development of the Security Operation capability, that include policies, standards, frameworks and processes, to ensure the IT/OT landscape is secure. The Cyber Analyst will carry out, assist with, and guide Security Operation activities to ensure that KiwiRail's IT/OT assets are acquired/designed, deployed, run, and operating in a secure manner, so they continue to enable business activities.

One of the Cybersecurity Analyst's focus areas will be endpoint security

Key

Accountabilities

Within the area of responsibility, this role is required to:

- Monitor and maintain server/workload and other endpoints protection-agent health and compliance,
- Monitor ICT and ICT enabled environments (including OT) for cyber 'events', and investigate and resolve cyber issues,
- Respond to cybersecurity events and incidents,
- Identify, assess, and manage vulnerabilities,
- Advise KiwiRail teams and projects on matters relating to cybersecurity,
- Work with KiwiRail teams and suppliers to follow cybersecurity policies and standards,
- Assist in the reporting of KiwiRail's cybersecurity risk profile.
- Manage small uplift projects enhancing cybersecurity posture
- Be on-call 24x7 for rostered periods.

Key challenges

- Understanding KiwiRail's diverse and complex IT and OT environments
- Assessing, prioritising, and managing alarms and issues as they arise
- Compliance with government, industry, and KiwiRail specific policies and frameworks
- Keeping abreast of industry, regional, and technology specific threat landscapes

Key Relationships Here are the key relationships relevant to this role		Manage /Lead	Deliver to	Collaborate with	Advise or inform
Internal	ICT			✓	✓
	Head of (ICT) Security		✓	✓	✓

	Cyber Operations Manager		✓	✓	✓
	ICT Operational Managers			✓	✓
External	Security Partners			✓	
	Service Providers			✓	✓

What you will do to contribute

Health Safety and Wellbeing	• Implement safety procedures and ensure team compliance • Analyse workplace risks and develop mitigation strategies • Support team members' physical and mental health
Customer Focus	• Provide a positive customer experience • Develop solutions to meet customer requirements • Solve complex customer issues • Work with colleagues to improve customer outcomes
Cybersecurity Operations	• Monitor assigned outsource vendors/partners to ensure they are carrying out their cybersecurity obligations and complying with KiwiRail cybersecurity policies in their scope of activity. • Guide and monitor assigned KiwiRail ICT teams to ensure they are carrying out their operational cybersecurity obligations and complying with KiwiRail cybersecurity policies in their scope of activity • Conduct real-time monitoring where appropriate or not in the scope of an outsource vendor. • Investigate cyber issues/events when they occur and are not in the scope of an outsource vendor. • Respond to assigned cyber incidents (working with internal teams and suppliers as appropriate). • Remediate or manage the remediation of assigned cyber issues
Continuous Improvement	• Ongoing improvement of endpoint protection capability and coverage. • Keep abreast of cybersecurity research and emerging cybersecurity trends – such as vulnerabilities, threats, attacks, and standards - to bring a proactive element to the cybersecurity team. • Look for opportunity to improve service delivery, reduce capital and operational costs. Contribute to Cybersecurity Awareness and Training materials and planning.
Risk Management	• Identify and forecast risks, issues, and opportunities in projects • Implement risk controls and engage stakeholders in risk management

Decision Making

The position is accountable for decisions regarding tasks and delegated areas of cybersecurity operations and in some instances cybersecurity assurance.

Key decision-making requirements of the position include:

- Assessing, prioritising, and managing alarms and issues as they arise
- Identifying and following/enforcing the relevant cybersecurity policies, standards, and processes
- Identifying cybersecurity risks and their remediating control

Human Resources Delegations	Nil
Direct reports	None
Finance Delegations	None
Budget (operating and capital)	Nil
Travel Delegations	Nil
Statutory powers	Nil

Physical demands and the nature of work

This role is administration-based and requires:

- prolonged sitting and high computer usage
- limited walking, standing, twisting, bending (at the waist), crouching (bend knee)
- carrying of laptop and paperwork when alternating between home and office
- limited lifting of up to 7 kg archive boxes

Your role may include other tasks suited to your level, as your manager directs. This job description shows your current duties. We'll review and update it with you if your responsibilities change.

About you

Knowledge and experience

- You will have 5+ Years of experience
- Cyber operations and incident management or similar roles
- Infrastructure, system, network, or server administration or similar roles
- Analyse and remediation of IT issues

Desirable:

- Experience working in Operational Technology / Industrial Controls Systems / SCADA environments
- Experience with security monitoring, EDR, IDAM, PAM, and SOC/SIEM; e.g. Trend Micro Vison One, Trellix, Cyber Ark, Level Blue, Azure Security Centre
- Experience with vulnerability scanning
- Experience with risk assessments
- Experience automating operational tasks: e.g. FortiSOAR
- Software development or, solution or systems design
- Experience in contract and vender management

Ways of working / Work-related qualities

- Work collaboratively with a wide range of KiwiRail staff, suppliers and partners to identify, quantify, and manage assigned security risks and remediation activities.
- Work collaboratively with a wide range of KiwiRail staff, suppliers and partners in the investigation and resolution of assigned security incidents.
- Independent thinker, highly motivated and self-directing
- You're flexible and practical

Other Requirements

- Experience with IT security standards, such as:
    - IEC 62443
    - ISO27001
    - NZISM
    - NIST 800 r53 v4
    - PCI DSS
- You can pass regular drug and alcohol screenings
- You have a current and valid NZ Driver's Licence

KiwiRail uses Skills Framework for the Information Age (SFIA 8) to describe the skills required for roles within ICT. The skill level descriptions provide a detailed definition of what it means to practice the skill at each level of competency. You will need to demonstrate the following skills at the level listed. You can find detailed description of the skills and levels here: SFIA 8 Skills List .

- Security Operations Level 3
- Incident Management: Level 2

Desirable

- Supplier management Level 3
- Risk Management Level 3

Qualifications

You need either:

- A relevant degree in Information Communications Technology

or

- Equivalent experience