RS FORM 2 - JOB DESCRIPTION

SECTION A – POSITION DETAILS

POSITION TITLE: SOC Analyst (Cyber Security)	
MINISTRY/OFFICE: Ministry of Finance & Treasury	
DIVISION: SIG ICT Services	**DUTY STATION:** SIG ICT Services, Lengakiki
POSITION NUMBER: 273- 10031	**MINISTRY VACANCY NUMBER:**
POSITION LEVEL: L9/10	**SALARY RANGE:** $60,084.18 -$76,488.05
THIS POSITION REPORTS TO: Deputy Director – Cyber Security	
POSITIONS SUPERVISED: NA	

SECTION B - SCOPE OF DUTIES

The Ministry of Finance and Treasury is mandated to facilitate the provision of sound advice on economic, financial, and fiscal policy; services include statistics, economic management, governance, financial reporting, revenue collection, border protection and ICT services across the public sector.

The SIG ICT Services (SIG ICTS) division within the Ministry of Finance & Treasury is mandated to deliver innovative, sustainable, and secure ICT solutions, in an environment that fosters talent and focus on standards, taking pride in the role of SIG ICT Services in enabling SIG to provide improved services to the public and private sectors.

The SOC Analyst is responsible for the Security Operations Centre and to Setup and Manage the Security Information and Event Management (SIEM) as the core system of the Security operations Centre (SOC).

SECTION C - KEY DUTIES

This position is required to undertake the following duties:

1. Setup and manage the Security information and event management (SIEM) as the core system of the Security operations Centre (SOC).

2. Setup and review all alert types within the SOC service levels.

3. Integrate the SIEM with the SIG ICT Information Systems, Network, application, databases and various ICT Services.

4. Perform scoping of alerts to identify additional compromises within the environment, develop and apply new hunting techniques to improve the overall ICT security of SIG

5. Develop security health reports for Deputy Director Cyber Security, Director ICT Services and stakeholders

6. Contribute to Community Protection events to raise awareness of ICT Security matters

7. Serve as an escalation point in hunting efforts for the rest of the SIG ICT Services team.

8. Develop and Measure SOC performance metrics to measure the state of security within SIG

9. Undertake any other duties as reasonably or directed by the Responsible Officer or Supervisor.

SECTION D - KEY DELIVERABLES

The incumbent of this position will have their performance assessed according to following key deliverables:

1. SIEM up to date and security alerts operating efficiently.

2. SOC service levels setup and reviews completed efficiently.

3. SIEM integrated with ICT Information Systems, Network, application databases and other ICT Services.

4. Quantity and quality of scoping of alerts identifying compromises and new hunting techniques developed.

5. Quantity and quality of health and compliance reports completed.

6. Quantity and quality of contribution to Community Protection events.

7. Efficient escalation of hunting efforts for ICT Services team.

8. IT Security Metrics developed and measured.

9. Other duties undertaken efficiently and timely.

10. 100% attendance and compliance with Code of Conduct

SECTION E – QUALIFICATIONS AND CAPABILITIES

Mandatory Qualifications and or Experience

- Tertiary Qualification in IT with previous cybersecurity experience.
- 3 years' experience in similar role and/or 5 years of progressive experience in information technology.

Desirable

- Undergraduate Qualifications in Information Technology with certifications in Cybersecurity.

Behavioural:

- Communication, Conflict resolution, resilience

SECTION F - KEY SELECTION CRITERIA

Suitability for this position will be assessed against the following key criteria:

KSC 1 Demonstrated ability to setup and manage a Security Information and Event Management (SIEM).

KSC 2 Demonstrated ability to develop Security metrics and report on security within a large complex organisation.

KSC 3 Demonstrated ability to develop incident reports to secure SIG ICT systems

KSC 4 Excellent written and verbal communication skills with demonstrated ability to translate technical specifications and concepts to layman terms.

KSC 5 Demonstrated strong ethical convictions, a commitment to quality service and ability to complete work in a high-pressure environment.

KSC 6 Outstanding work attendance record and a strong commitment to upholding Public Service Values and Code of Conduct.

SECTION G - TERMS AND CONDITIONS

Fortnightly Salary: $ 2,310.93-2,941.85	**Annual Salary**: $60,084.18 -$76,488.05
Annual Leave entitlement: As per Public Service Policy	
Other Conditions of Service relevant to this position: • Other *A Housing Allowance* • *B Other standard leave entitlements outlined in the General Orders for SIG Public Servants*	

SECTION H - APPROVAL *(Business use only)*

This Job Description is approved on the basis that I believe it accurately reflects the requirements of the position and will assist the Ministry/Office to achieve its corporate objectives:

..... 16/1 .....

Permanent Secretary/Responsible Officer **Date Approved**

Additional Comments:

Approve