CIRCULAR MEMORANDUM
NO. 29 OF 2026

MY REF: STAFF/GEN/2/10/26 (12) Vol. XI

FROM: **Chief Executive Officer, Ministry of the Public Service and Disaster Risk Management**

TO: Office of the Governor General, Chief Justice, Auditor General, Solicitor General, Financial Secretary, Cabinet Secretary, Chief Executive Officers and Heads of Department

SUBJECT: VACANCY NOTICE – TWO (2) POSTS OF CYBER SECURITY ANALYST – CENTRAL INFORMATION TECHNOLOGY OFFICE (CITO), MINISTRY OF FINANCE – BELMOPAN

DATE: 21st April 2026

Applications are invited from suitably qualified applicants to fill two (2) posts of **CYBER SECURITY ANALYST,** Central Information Technology Office (CITO), Ministry of Finance, from across the country of Belize.

BASIC PURPOSE OF POSITION:
The Cybersecurity Analyst I is responsible for safeguarding the organization's hybrid IT environment - spanning both on-premises and cloud infrastructure - against evolving cyber threats. This role leverages a comprehensive suite of advanced security tools, including Microsoft Sentinel, Microsoft 365 Defender for Cloud and Endpoint, Office 365, Microsoft Entra ID Protection, and Microsoft Purview, along with on-premises platforms such as Splunk, FortiAnalyzer, ADAudit Plus, and Trellix DLP. The analyst uses these technologies to analyze security telemetry and determine appropriate response actions. The primary mission of the Cybersecurity Analyst I is to continuously monitor, detect, investigate, respond, and support the recovery of systems affected by security incidents across all vectors - network, identity, endpoint, email, and data. Operating under the direction of the Lead Information & Cybersecurity Officer, this role also ensures that security operations align with international standards and industry best practices such as - ISO/IEC 27001, ISO/IEC 27002, NIST, CIS Critical Security Controls, and electronic legislation where applicable while actively collaborating with IT and business teams to support a secure and resilient GOB enterprise network.

ESSENTIAL DUTIES AND RESPONSIBILITIES:
1. CONTINUOUSLY monitor security events and logs from both cloud (e.g. Microsoft 365, Azure, AWS, Google Cloud and other cloud platforms) and on-premises systems using SIEM and log management tools to identify anomalies, suspicious activities, and indicators of compromise.
2. INVESTIGATE and analyse security alerts and incidents generated by SIEM and other monitoring platforms, performing triage to differentiate legitimate threats from benign or false-positive activity.
3. SERVE as a first responder to validated security incidents, executing containment and eradication steps in accordance with incident response playbooks established by CITO.

4. COLLABORATE with the Lead Information & Cybersecurity Officer and IT teams to coordinate response actions, remediation steps, and recovery activities following security incidents.
5. WORK with other cybersecurity personnel to develop and refine security orchestration, automation, and response (SOAR) playbooks within SIEM tools to streamline and automate repetitive incident response tasks.
6. CONFIGURE SIEM and SOAR workflows to rapidly address common threats, including automatic disruption or disabling of suspicious activity upon receiving high-severity alerts.
7. CONTINUOUSLY enhance detection and response capabilities by improving detection rules, correlation queries, analytic models, and playbook effectiveness to enhance both accuracy and response.
8. CONDUCT proactive threat hunting across enterprise environments using Kusto Query Language (KQL) and other analytical tools to uncover stealthy or unreported threats that may bypass automated detection.
9. ANALYZE anomalies in user behaviour, network traffic, and system logs, identifying patterns indicative of potential compromise and recommending mitigation actions as necessary.
10. UTILIZE detection and response technologies such as EDR and NDR to protect organizational devices, including workstations, servers, and mobile endpoints, network devices, from malware, ransomware, and advanced threats.
11. REVIEW and analyse logs from FortiAnalyzer and other network security tools, identifying signs of malicious activity such as abnormal outbound traffic, port scans, or intrusion attempts, and coordinate with network administrators to adjust firewall rules and access controls.
12. MONITOR Active Directory activity using ADAudit Plus or similar tools to detect misuse or suspicious behaviour, such as unauthorized privilege escalation, unexpected admin account creation, or repeated account lockouts, and assist in prompt remediation of AD-related security concerns.
13. PARTNER with IT support teams to deploy security patches, implement configuration hardening measures, and support compliance with NIST, CIS benchmarks, and CITO security policies to minimize vulnerabilities.
14. STAY current with emerging cyber threats, vulnerabilities, attack vectors, and malware campaigns; update detection queries, monitoring rules, and incident response processes based on new intelligence and proactively strengthen the organization' s defensive posture.
15. DESIGN and build SIEM and SOAR solutions to address emerging technology requirements.

QUALIFICATIONS:
Must have a Bachelor's degree in Cybersecurity from a recognized institution with a minimum of three (3) years' experience in a cybersecurity role with at least two (2) years focused on cybersecurity analysis.

KNOWLEDGE, SKILLS AND ABILITIES:
1. Proficiency with Microsoft security technologies and SIEM/SOAR platforms: Demonstrated expertise in Microsoft Sentinel for log analysis, alert tuning, automation, and incident investigation, with familiarity in other SIEM solutions such as Splunk.

2. Ability to craft advanced queries (e.g., KQL) and develop custom detection rules

3. Hands-on experience with endpoint detection and response solutions: Practical knowledge of Defender for Endpoint, Defender for Office 365, and Defender for Cloud, including the ability to interpret alerts, assess threat severity, and execute appropriate defensive actions. Understanding of extended detection and response (XDR) integrations for end-to-end threat protection.

4. Strong understanding of identity security: Knowledge of Azure AD/Microsoft Entra ID and on-premises Active Directory security principles. Experience using Identity Protection or

similar tools to evaluate user risk, enforce MFA, and detect identity-based threats. Solid understanding of AD structure, group policies, and common identity attack vectors.

5. Solid foundation in network and system security: Strong understanding of networking fundamentals, firewalls, and IDS/IPS technologies, with the ability to analyze network traffic and logs for anomalies. Working knowledge of tools such as FortiAnalyzer or similar network log analyzers. Clear understanding of FortiAnalyzer log semantics.

6. Analytical and scripting capabilities: Demonstrable experience with KQL to support threat analysis, automation, and reporting.

Behavioural:

1. Strong leadership and personnel management skills.
2. Excellent written, oral, and interpersonal communication skills.
3. Ability to discharge duties in a fashion that aligns responsibilities with the goals of the department.
4. Highly self-motivated, self-directed, and attentive to detail.
5. Proven analytical and problem-solving abilities.
6. Strong customer service orientation
7. Ability to effectively prioritize and execute tasks in a high-pressure environment.
8. Ability to work in a team-driven, collaborative environment.
9. Experience working in a team-oriented, collaborative environment

WORK CONDITIONS: *(physical demands, job hazards, pressures)*

1. Available to work on weekends and holidays as required
2. Flexible working hours

REPORTING RESPONSIBILITY:

The Cyber Security Analyst will report to the Lead Information & Cybersecurity Officer

CONDITIONS OF SERVICE:

The Conditions of Service will be in accordance with the Belize Constitution (Public Service) Regulations, 2014, Financial and Store Orders, Finance and Audit (Reform) Act and any other instructions issued from time to time.

SALARY:

Government of Belize pay scale 21 of $39,821 x 1,718 - $72,463 per annum.

Interested persons in possession of the required qualification and who have the aptitude for the posts are asked to submit their complete application package, qualifications, at least two references and a valid police report through the Job Search and Employment Application Website at https://jobs.publicservice.gov.bz/ no later than **8th May 2026.**

ROLANDO ZETINA (MR.)
CHIEF EXECUTIVE OFFICER

c: *Chief Information Officer, CITO*
President, PSU
President, APSSM
GEN/4/01/01