JOB DESCRIPTION

Security Engineer

A leading, diversified Information and Communications Technology (ICT) company is seeking to recruit a Security Engineer.

The firm provides comprehensive, enterprise-wide solutions tailored to clients' needs, from cybersecurity and cloud solutions to managed services. They are looking for a skilled and motivated Security Engineer to join our dynamic technical team and deliver exceptional value to our clients.

About the Role

The Security Engineer will primarily function as a Security Operations Center (SOC) Analyst responsible for monitoring, detecting, analyzing, and responding to cybersecurity incidents. The engineer will also participate in penetration testing engagements and support networking-related security tasks as required.

Responsibilities

A. SOC Analyst Duties

- Monitor security alerts and investigate potential threats using SIEM/XDR and related security tools.
- Perform end-to-end incident response, including detection, containment, eradication, recovery, and post-incident review.
- Conduct forensic analysis and detailed log reviews to determine root cause of security incidents.
- Produce and maintain clear incident tickets, documentation, and root cause analysis reports for major incidents.
- Provide periodic threat intelligence reporting on emerging threats, trends, and indicators of compromise.

B. Penetration Testing Duties

- Take part in conducting internal and external penetration tests on web applications, networks, and cloud environments under agreed scopes.
- Perform manual and automated vulnerability assessments, including web application testing (e.g., SQLi, XSS, CSRF, SSRF, API security).
- Assist with basic Active Directory security testing (e.g., user enumeration, weak password identification).
- Develop proof-of-concept exploits for key findings where appropriate.

- Prepare clear, structured vulnerability and penetration test reports, including risk ratings and remediation recommendations.

C. Networking Security Duties

- Network security monitoring across firewalls, IDS/IPS, VPNs, and related infrastructure.
- Support firewall rule reviews, network segmentation and micro-segmentation audits, and network hardening activities.
- Troubleshoot network-related security incidents within agreed SLAs, including analysis of packet captures and logs.
- Run and review network vulnerability scans (e.g., Nessus, OpenVAS) under supervision and track remediation progress.
- Configuration and auditing of NAC (Network Access Control) policies and secure network architecture changes.

Required Skills and Qualifications

- A minimum of 2 years of hands-on experience in a Cyber Security or a Similar role.
- Bachelor's degree in computer science, IT, or related field.
- Certifications. e.g., CompTIA Security+, EC Council CEH, CompTIA CYSA, ECIH, EC Council CSA, etc., will be an added advantage.
- Strong interest in cybersecurity and information technology, with the ability to learn quickly and adapt to new technologies.
- Hands-on experience with security tools and technologies, including SIEM, IDS/IPS, and firewalls.
- Familiarity with incident response methodologies and procedures.
- Good analytical and problem-solving skills, with attention to detail and accuracy.
- Strong communication and interpersonal skills, with the ability to work effectively as part of a team.
- Understanding of security fundamentals, network protocols and topology (TCP/IP, HTTP/S, DNS, DHCP, VPN, VLANs).
- Experience with operating systems such as Windows, Linux, and macOS.
- Basic scripting ability in languages such as Python or PowerShell.
- Familiarity with penetration testing processes (planning, scanning, exploitation, reporting) and common vulnerabilities (OWASP Top 10, basic MITRE ATT&CK techniques).

- Ability to use tools such as Nmap, Burp Suite, Metasploit, Nessus/OpenVAS, Wireshark/TShark.

Other Requirements

- Must have a valid ICTAZ practicing license.
- Must have a driver's license.
- Must provide a police clearance certificate upon being selected for the role.

Application submission:

Interested candidates should submit applications to: **jobs@ictaz.org.zm**

Application Deadline: 30th April 2026