TAKAFUL BRUNEI | CAREER OPPORTUNITIES

IT Security Specialist

Reporting To Head of IT

Responsibilities

- Coordinate and oversee Managed Security Service Provider (MSSP) and Security Operations Center (SOC) operations.
- Monitor and review security alerts and incidents reported by SOC and Security Information & Event Management (SIEM) platforms.
- Investigate, validate, and respond to security alerts and incidents.
- Administer and monitor Extended Detection and Response (XDR) and endpoint security solutions.
- Investigate endpoint security alerts and suspicious activities.
- Administer and maintain security devices including firewalls, web application firewalls, intrusion detection and prevention systems, and network security appliances.
- Implement and maintain firewall and security rules.
- Coordinate vulnerability assessments and penetration testing activities.
- Review vulnerability assessment reports and assess risks.
- Coordinate remediation with relevant IT units and external vendors.
- Track remediation progress and ensure timely closure.
- Verify effectiveness of remediation actions.
- Support cybersecurity incident response activities including investigation, containment, eradication, and recovery.
- Perform root cause analysis and recommend preventive measures.
- Maintain incident documentation and reports.
- Perform periodic user access review across systems and platforms.
- Ensure compliance with least privilege principle.
- Support security assessment of third-party vendors and service providers.
- Assess security posture of cloud systems and services.
- Support implementation of secure architecture for systems and infrastructure.
- Review and recommend security controls for new systems and integrations.
- Support development and delivery of security awareness programs.
- Conduct security awareness training for staff.
- Support the implementation and maintaining security baselines and configuration standards.
- Support development and enforcement of security policies and procedures.

Requirements

- Good understanding and hands-on experience in SIEM and SOC operations, incident response, firewall and security device administration, vulnerability management, security monitoring, and log analysis.
- Good understanding of cloud security, API security, and security architecture.
- Strong analytical and investigative skills.
- Strong problem-solving ability.
- Good communication and documentation skills.
- Bachelor's Degree in Cybersecurity, Computer Science, Information Security, Information Technology, or a related field.
- Professional certifications such as CISM, CompTIA Security+, CEH, ISO/IEC 27001, Microsoft or cloud security certifications and firewall administration and certifications will be an added advantage.
- At least three (3) to five (5) years of work experience in IT Security or Cybersecurity with preferred experiences in financial services or takaful/insurance industry, working with MSSP or SOC, and in managing firewalls and security tools.

All applicants must submit their application by **6th March 2026.**
Only short-listed candidates will be notified.