SECURITY OPERATIONS ANALYST

Applications are invited from interested and suitably qualified individuals for the position of **Security Operations Center Analyst,** Providenciales.

Description

The SOC Analyst is a seasoned professional with proven hands-on experience in monitoring, maintaining, and optimizing a suite of advanced security platforms. The ideal candidate will be a proactive practitioner, capable of independently managing and integrating multiple enterprise security solutions to ensure robust protection of organizational assets.

Main Duties & Responsibilities

1. **Monitoring & Maintenance of Security Platforms**
   - Continuously monitor, maintain (appropriate modules/ areas), and optimize advanced security platforms, including:
     - Microsoft Defender (Endpoint Protection)
     - Microsoft Purview (Data Governance, Compliance & DLP)
     - Microsoft Sentinel (SIEM)
     - BeyondTrust (Privileged Access Management)
     - Qualys (Vulnerability Management)
     - Field Effect (Managed Detection & Response, Threat Intelligence & Monitoring)
     - Mimecast (Email Security)
     - SolarWinds (Infrastructure Monitoring)
   - Manage outsourced security services
     - Liaise with external security service providers.
     - Monitor service delivery, SLAs, and ensure alignment with organizational security objectives.
   - Ensure seamless integration and interoperability across all platforms for real-time threat detection and response.

2. **Incident Response & Vulnerability Management**
   - Detect, analyze, and respond to security incidents, coordinating containment, eradication, and recovery efforts.
   - Lead vulnerability management activities, including scanning, assessment, prioritization, and remediation tracking.
   - Document incidents and remediation actions and conduct post-incident reviews to improve processes.
   - Act as the Incident Response Commander for declared cyber incidents.

3. **Threat Intelligence & Hunting**
   - Analyze threat intelligence feeds and indicators of compromise (IOCs).
   - Proactively hunt for threats within the environment using advanced analytics and tools.
   - Stay updated on emerging threats and attack techniques.

SECURITY OPERATIONS ANALYST

Main Duties & Responsibilities Cont'd

4. Risk Assessment & Security Architecture

- Perform regular risk assessments across IT and OT environments to identify and mitigate threats.
- Review and enhance security architecture, ensuring alignment with industry standards and regulatory requirements.
- Develop and maintain risk management plans and security controls IT and OT Environment Coverage
- Monitor and protect both Information Technology (IT) and Operational Technology (OT) environments.
- Address unique risks and requirements for OT systems, such as industrial control systems and critical infrastructure.
- Coordinate with the SCADA Analyst on maintaining, monitoring and updating security configurations for industrial control systems (ICS), SCADA, PLCs and other OT assets.

5. Compliance & Policy Enforcement

- Ensure adherence to regulatory requirements (e.g., ISO 27001 & 27002, NIST, NERC-CIP).
- Support audits and maintain documentation for compliance.
- Enforce security policies, standards, and procedures.

6. Reporting & Documentation

- Maintain detailed records of security events, incidents, and investigations.
- Prepare regular reports for management and stakeholders on security posture and incident trends.

Academic/ Technical/ Management Experience and Qualifications:

- Bachelor's degree (or higher) in Computer Science, Information Technology, Information Security, Cybersecurity, Network Engineering, Information Systems, or a closely related field.Having a Master's Degree in any of the abovementioned degrees is an advantage.
- Holds one or more of the following Core Certifications:
  - CompTIA Security+ – foundational cybersecurity knowledge
  - Certified Ethical Hacker (CEH) – penetration testing and ethical hacking
  - GIAC Security Essentials (GSEC) – security fundamentals
  - Cisco Certified CyberOps Associate – SOC operations and incident response
- Having any of the below Advanced/ Specialized Certifications is an advantage:
- Certified Information Systems Security Professional (CISSP) – broad security leadership and architecture
- GIAC Certified Incident Handler (GCIH) – incident detection and response
- GIAC Security Operations Certified (GSOC) – SOC-specific skills
- Certified SOC Analyst (CSA) – focused on SOC tools and workflows
- Splunk Certified Power User / Admin – for SIEM expertise
- Microsoft SC-200 – Microsoft Security Operations Analyst

SECURITY OPERATIONS ANALYST

Abilities, Skills, Experience, Aptitude & Judgement:

With at least seven (7) years of solid experience in cybersecurity and performing in the areas of:

- Threat Detection & Response
- Security Tools and Platforms
- Incident Management
- Scripting & Automation
- Compliance and Governance
- Excellent team player and team building skills
- Excellent written and oral communication skills
- Ability to deliver to strict deadlines and to work under pressure
- Goal-oriented
- Self- motivated

- **Compensation is commensurate with experience and qualifications.**