Job Description

Position Title: Security Operations Analyst

Reports to: Head of Security Operations

Location: London, 1 America Square

Summary of Position:

As a Security Operations Analyst, you will play a crucial role in ensuring the security and integrity of our organisation's information systems and data. You will be responsible for working independently and with our 24x7 SOC service to monitor, detect, investigate and respond to security incidents and threats. The role will involve analysis of security events and threats, implementing security measures, and providing actions or recommendations to mitigate potential risks and enhance our security posture.

The role will also involve helping to ensure that our security tools and controls are effectively configured and utilised to minimise security risks and to maintain compliance with our security standards, legislation and regulations.

This role is an Operational role requiring quick-thinking, decisive actions, along with good communications. This role could be required to respond to escalations and alerts raised from our 24x7 SOC Monitoring services and may on occasions, have extended demands on working hours.

Key Responsibilities & Accountabilities:

- **Monitoring and Incident Detection:**
  - Monitoring of security tools for events, alerts, and notifications to identify potential security incidents and anomalies.
- **Incident Response and Investigation:**
  - Investigate security incidents, including performing root cause analysis, forensic analysis and impact assessment.
  - Adherence to BMS incident response plans and procedures to contain and mitigate security incidents effectively.
  - Collaborate with cross-functional teams to coordinate incident response efforts and communicate findings to stakeholders

- **Security Analysis and Threat Intelligence:**
  - Analyse security TI feeds to identify emerging threats, attack patterns, vulnerabilities.
  - Maintain awareness about latest security threats, vulnerabilities and trends by monitoring threat intelligence sources and assessing potential risks to the organization.
  - Use of various security tools and technologies to analyse security threats and vulnerabilities.
- **Metrics and Assurance**
  - Assist in production of, and actions arising from, KRI metrics relating to SecOps controls.
- **Vulnerability Management**
  - Interaction with Vulnerability Management teams and tools to identify, assess and mitigate security vulnerabilities
- **Threat Hunting**
  - Perform periodic threat-hunting; using Intelligence-based, Hypothesis-based or Situational-based approaches
- **Security Tools Management:**
  - Administer and manage security tools and technologies such as SIEM, IDS/IPS, and EDR systems.
  - Configure, optimise and tune security tools to improve detection capabilities and reduce false positives.
- **Incident Reporting and Documentation:**
  - Create detailed incident reports, documenting findings, actions taken, and recommendations for improvement.
  - Maintain accurate records of incidents, investigations, and resolutions for compliance, audit and future reference.
- **Training and Awareness:**
  - Adhere to BMS and regulatory mandatory training requirements.
  - Promote a culture of security consciousness within the organisation.

Functional & Behavioural Competencies required:

- **Functional**
  - Accredited in Cyber Security certificate: CISSP, CompTIA/S+, CEH, etc
  - Good knowledge of Cyber frameworks: NIST/CSF, Mitre Att&ck, etc
  - Experience of Enterprise IT and Cloud platforms: Azure, AWS, etc
  - Experience in Security Operations Tools and Services

- **Behavioural**
  - Proactive and inquisitive with a passionate interest in Cyber Security.
  - A can-do attitude with confidence to challenge the status-quo.
  - Problem-solver and lateral thinker, meticulous attention to detail.
  - Personally demonstrate the five BMS values.
    - Accountable
    - Entrepreneurial
    - Collaborative
    - Empowering
    - Disciplined