Manager – Cybersecurity

SCOPE OF RESPONSIBILITIES

- **Develop and Implement Security Policies:**
  Define, implement and maintain corporate security policies, standards and guidelines (e.g., GDPR, HIPAA, ISO 27001).
- **Manage Risks & Compliance:**
  Conduct risk assessments, implement security solutions, ensure regulatory compliance, and oversee internal and external audits.
- **Manage Security tools:**
  Evaluate, recommend and manage security-related tools and services, and ensure the latest solutions are deployed within the organization. Supervise implementation and maintenance of firewalls, antivirus software, SIEM systems and intrusion detection systems (IDS/IPS). Oversee real-time security monitoring, analyze security alerts, and prepare security status reports for senior management.
- **Lead Incident Response:**
  Develop and manage incident response plans, lead investigations into security breaches, response to security incidents, and coordinate recovery. Communicate with stakeholders and report incidents appropriately.
- **Team Leadership & Training:**
  Lead and mentor a team of cybersecurity specialists, develop and conduct security awareness training for employees to foster a security-conscious culture within the organization.
- **Collaborate Across Departments:**
  Work closely across all departments within MEASAT to align security initiatives with organizational goals.

REQUIREMENTS (Education, Experience, Skills, Attributes / Behaviors, Others)

Education

- Bachelor’s degree in computer science, Information Security, Information Technology or a related field.
- Other relevant certifications (highly preferred):
  - *Certified Information Systems Security Professional (CISSP)*
  - *Certified Information Security Manager (CISM)*
  - *Certified Ethical Hacker (CEH)*
  - *CompTIA Security+*
  - *Certified Cloud Security Professional (CCSP)*

Experience

- 5–8 years of progressive experience in IT security or cybersecurity roles.
- Proven experience managing security operations, incident response and risk assessments.
- Experience with security frameworks and best practices (e.g. ISO 27001, NIST, GDPR, HIPAA).
- Hands-on experience with security technologies like firewalls, SIEM, anti-virus, IDS/IPS, VPN, MFA, EDR.

Skills

- Strong knowledge of network and system security, firewalls, IDS/IPS, SIEM and endpoint protection.
- Familiarity with cloud security (AWS, Azure, GCP).
- Proficiency in security tools and scripting (e.g. PowerShell, Python).
- Excellent in risk analysis, vulnerability management and threat modeling.
- Strong analytical, problem-solving and project management skills.

Attributes / Behaviors

- Strong sense of ethics and responsibility in handling sensitive information.
- Strong leadership and decision-making abilities.
- Excellent communication skills – able to explain technical issues to non-technical stakeholders.
- Proactive, detail-oriented, and adaptable to fast-changing environments.

Others

Experience with security tools and technologies (Trend Micro's products, PAM, DLP, etc.).