JOIN THE MOST AWARDED BANK IN SRI LANKA

With an enduring vision of being the most technologically advanced, innovative and customer friendly financial organization, we, the most awarded Bank in Sri Lanka, continue to progress steadily while being listed amongst the Top 1000 Banks in the world for the 12th consecutive year. Our unparalleled record of success is supported by an unmatched suite of digital offerings and superior standards in service, stability and performance. We are poised to ascend to even greater heights in the near future.

Assistant Manager – Information Security Operations

Job Profile

We are looking for highly motivated, enthusiastic and dynamic individuals to join our Information Security Team under the Chief Information Security Officer (CISO), to strengthen the information security operations functions.

Key duties and responsibilities of the selected candidate would include the following:

- Develop / maintain the vulnerability management programme of the Bank including devising polices, planning and conducting the system security compliance reviews / security assessments as mandated by regulations, compliance standards and Bank policies. Critically analyze assessment results and act as an information security consultant for correcting identified gaps.

- Operate a hands-on role involving penetration testing, Red teaming activities, vulnerability / configuration assessment, etc activities of operating systems, wired and wireless networks, applications including mobile applications, etc.

- Formulate meaningful security metrics / reports to reflect the true posture of the environment allowing the organization to make educated decisions based on risk. Produce actionable, threat-based, reports on security testing results.

- Define / validate system security requirements and baselines necessary to protect systems (OS/ DB), applications, networks, hardware, cloud environments, etc.

- Support ongoing eligibility for annual certification of all applicable standards including ISO 27001, PCI DSS and conformance to regulatory and other mandatory requirements imposed by relevant bodies such as SWIFT, etc.

- Collaborating with the CISO and relevant stakeholders to build on the existing information security programme and manage security projects.

- Evaluating the information security risks and vulnerabilities involved in system changes and launching of new technologies / products / business activities and make appropriate recommendations.

- Independently review / analyze / investigate the security alerts / events via sophisticated cyber security / event management tools to identify areas for improvement and provide recommendations and support for incident response / recovery where necessary.

- Support security operations functions which include but not limited to SIEM, EPP, DLP, and other security implementations and administration as required.

- Research, recommend and provide guidance on mitigating information security vulnerabilities and enhancements for information security related technologies, including developing business cases for security investments.

- Stay abreast on latest information security threats / vulnerabilities, regulations / legislation, advisories and alerts pertaining to the business and make recommendations to the Management as applicable.

Applicant's Profile

- Bachelors or Masters Degree in Information Security or Computer Science / Computer Engineering/ Information Technology by a university or a degree awarding institute recognised by the University Grants Commission of Sri Lanka.

- Professional qualifications such as CISSP, CISM, GISP, CEH, CCNA Security would be an added advantage.

- Minimum 03-04 years proven work experience in information or system security engineering / technical security assessment and/or related functions / areas. Hands on experience in vulnerability assessments and log correlation technologies are a must.

- Understanding of information security concepts, information security and risk management frameworks, standards and regulations (ISO 27001, ISO 27005, PCI DSS, NIST, etc).

- Thorough technical knowledge and exposure of IT infrastructure components such as operating systems, databases, application languages / platforms for application development, network and security technologies such as SIEM, DLP, firewalls, IDS / IPS, end-point security, VPN, etc.

- Strong knowledge of network and application protocols and their associated security implications (TCP/IP, HTTP, TLS, SSH, DNS etc) and web architectures and technologies.

- Excellent interpersonal and communication skills including technical report writing and strong analytical skills.

- Ability to prioritize work and design schedules to meet the desired requirements under pressurizing timescales.

- Ability to work collaboratively with other team members as well as work independently with minimum supervision.

successful candidate will be provided with an attractive remuneration package including fringe benefits, commensurate with benchmarked financial institutions.

Applications with all relevant information should be submitted to reach the under - mentioned by email within 10 days of this advertisement with the respective post marked as the subject.

Deputy General Manager – HRM
Commercial Bank of Ceylon PLC
E-mail : dgm_hrm@combank.net
Web site : www.combank.lk

⟨⟨b COMMERCIAL BANK

Our interest is in you