COMMERCIAL BANK OF CEYLON PLC

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 tenth consecutive year. Our unparalleled record of success over the past decade is supported by a network of 268 branches and superior standards in service, stability and performance. We are poised to ascend to even greater heights in the near future.

INFORMATION SECURITY ENGINEER - SIEM

We are looking for a highly motivated, enthusiastic and dynamic individual for our Information Technology Department as "Information Security Engineer".

Job Profile :

The selected candidate will be responsible for,

- Administration of SIEM platform and establishing Security operation (SOC) – This includes task automation, enhancing tool monitoring, ensuring overall health of the SIEM platform and oversee or perform remediation of security / management platform issues.
- Managing the SIEM and fine tuning use cases as continuous task.
- Custom Log Source integration and parsing.
- Integrate endpoint security systems in to platform.
- Serve as an expert to the organization on malware and other endpoint vulnerabilities and risks.
- Continuously research and learn about additional endpoint security solutions.
- Maintain knowledge of current security trends and be able to clearly communicate.
- Held responsible for security monitoring functions and oversee the roster.
- Develop written processes and procedures for use of help-desk personnel and IRT teams.
- Working closely with Incident Response teams in helping reduce MTTD and MTTR.
- Assist in development and support enforcement of IT policy, procedures and standards.
- Participate in Technical Evaluation Committees.

Applicant's Profile :

- Bachelor's degree in Computer Engineering / Computer Science / Information Security / Information Technology, specializing Information Security or Cyber Security.
- Professional Qualifications such as GISP, SSCP, CEH, RHCSA, MCSA.
- 2 to 3 years experience as an Information Security Engineer in a reputed organization, preferably in financial sector or Information Security Firm with the exposure to SIEM.
- Hands-on experience on SIEM administration, use case development, information security monitoring, information security incident handling, analysis and reporting.
- Strong knowledge of network application and protocols and their associated security Implications (TCP / IP, HTTP, TLS, SSH, DDNS, etc.)
- Understanding the security technologies like firewalls, VPN, PKI, cryptography, antivirus, IPS / IDS, end point security, WAF, MDM.
- Exposure on System and network security administration – exposure on various networking products, security products, databases and operating systems.
- Knowledge on Windows and Linux environments.
- Functional knowledge of current platform technologies managed by security products including SQL, IIS, Windows, Linux and MAC.
- Knowledge of common scripting tools, Powershell, Python, Bash.
- Strong in-depth analytical and problem-solving skills.
- Strong work ethics with attention to detail.

The 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 within 10 days of this advertisement with the respective post marked as the subject by e-mail.

Deputy General Manager - HRM
COMMERCIAL BANK OF CEYLON PLC
Email : dgm_hrm@combank.net
Web site : www.combank.lk

COMMERCIAL BANK

All applications will be treated with strict confidence. Canvassing in any form will be an immediate disqualification.