

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 the first Sri Lankan bank to be listed amongst the Top 1000 Banks in the World.

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.

Engineer – IT Security

JOB PROFILE

- Continuously monitor security alerts and events across the organization's systems, applications and networks using SIEM/XDR platform
- Administering a SIEM/XDR solution, on board log sources, developing enhanced detection rules and capabilities, with a focus on automating defense capabilities where possible
- Automate response actions through SOAR platform
- Triage and respond to reported security incidents to ensure they are appropriately prioritized, and remediated
- Engage in performing threat hunting to identify targeted threats and suspicious activities
- Create detailed reports on incidents, responses, and lessons learned to ensure continuous improvement in security practices
- Work with cross-functional teams, including network, system and application teams, to mitigate risks and improve security posture
- Stay up-to-date on emerging threats, vulnerabilities and advisories

APPLICANT'S PROFILE

- Bachelor's degree in Information Technology / Computer Science / specializing in Information Security or Cyber Security
- IT security related professional qualifications such as CEH, CHFI, Security+, CySA+, CSXP, SSCP would be an added advantage
- Minimum 2 year's proven experience as an Information Security Engineer or SOC Analyst
- Experience in security incident management
- Excellent communication skills, with the ability to manage relationships with internal and external stakeholders effectively
- Experience in scripting languages such as PowerShell, Python, Bash would be an advantage
- Strong understanding of MITRE ATT&CK and D3FEND frameworks
- Strong knowledge of network application and protocols and their associated security implications (TCP / IP, HTTP, TLS, SSH, DNS, etc.)
- Understanding the security technologies like firewalls, EDR, SIEM, IPS / IDS, WAF, MDM, etc.
- Knowledge on Windows and Linux environments
- Strong work ethics with attention to detail

Successful candidate will be provided with an attractive compensation package benchmarked with highest paid IT organizations in Sri Lanka along benefits.

Interested candidates are invited to apply for the position, all applications should be routed through our corporate website.

To apply, please visit,

www.combank.lk

► [Careers](#)

► [Open Positions](#)

► [Engineer - IT Security](#)

 **COMMERCIAL BANK**