JOIN THE MOST AWARDED BANK IN SRI LANKA

SENIOR ENGINEER - IT SECURITY

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.

JOB PROFILE

- Lead the design and maintenance of advanced security detection and response frameworks by driving detection engineering to develop and tune complex logic within SIEM and XDR platforms, moving beyond standard rules to hunt for sophisticated TTPs.
- Serve as the primary architect for security automation by designing end-to-end SOAR orchestration playbooks that streamline incident response workflows, significantly reducing MTTR and eliminating repetitive manual triage.
- Collaborating with Red Teams to perform "Purple Teaming" exercises developing adversary countermeasures that translate offensive findings into durable, automated defensive controls.
- Leading hypothesis-based strategic threat hunting missions to uncover dormant threats that evade traditional signature-based detection.
- Oversee the onboarding of new log sources and ensure all security systems (SIEM, XDR, EDR) are optimized for peak performance.
- Serving as the technical escalation point for high-impact security incidents, conducting deep-dive forensics and root cause analysis.
- Provide technical documentation, detailed reporting, and lead "lessons learned" sessions to drive process improvements across the SOC.
- Work closely with cross-functional IT and application teams to ensure the timely mitigation of identified threats and the implementation of security controls.

APPLICANT'S PROFILE

Education & Certification :

- Bachelor's degree in IT, Computer Science, or a Cybersecurity-related field.
- Professional certifications such as CEH, CHFI, CySA+, CSXP, or SSCP would be an added advantage.

Experience & Technical Expertise:

- Minimum 3-5 years in Information Security, with at least 3 years focused on advanced SIEM/XDR administration, detection engineering, or SOC Tier 2/3 roles.
- Proven expertise in architecting and optimizing core Security Operations platforms (SIEM, XDR, SOAR), including developing custom detection logic and complex correlation rules to identify advanced threats.
- Strong hands-on knowledge of Windows and Linux environments, security technologies, and complex network/application protocols (TCP/IP, HTTP, TLS, SSH, DNS, etc.).

Automation & Threat Intelligence:

- Proven expertise in security automation and orchestration, with a strong ability to develop custom scripts and automated workflows that integrate disparate security tools to enhance operational efficiency.
- Advanced proficiency in scripting (Python, PowerShell, or Bash) for security automation, tool integration, and developing automated SOAR workflows to enhance operational efficiency.
- Deep expertise in leveraging the MITRE ATT&CK framework for detection mapping and MITRE D3FEND for defensive gap analysis.

Successful candidate will be provided with an attractive remuneration package, commensurate with benchmarked financial institutions.

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 > Senior Engineer - IT Security

COMMERCIAL BANK