JOIN THE MOST AWARDED BANK IN SRI LANKA

SENIOR ENGINEER - IT SECURITY (RED TEAM OPERATIONS)

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

Offensive Operations & Emulation

- Design and execute end-to-end red team engagements, covering all the stages of the cyber kill chain from initial access to data exfiltration.
- Simulate specific threat actor groups (e.g., APTs) targeting the financial sector using the MITRE ATT&CK framework as a roadmap.
- Develop "Threat Playbooks" based on real-world intelligence (TI) relevant to the banking sector and automate these simulations using Breach and Attack Simulation (BAS) tools to ensure continuous validation of security controls.
- Maintain and manage a secure "Red Team Infrastructure" (C2 servers, redirected domains, and phishing platforms).
- Perform deep-dive manual exploitation of web applications, mobile apps, and internal network protocols beyond what automated scanners can find.
- Develop custom malware, scripts, and payloads designed to bypass modern EDR/AV solutions and network defenses during assessments.
- Conduct social engineering campaigns (Phishing, Vishing, Smishing) to test the human element of the Bank's security.
- Translate technical exploit chains into clear executive summaries and actionable remediation plans.
- Collaborate directly with the Security Operations Center (SOC) to conduct Purple Team exercises and measure the Bank's defensive detection and response capabilities.
- Directly assist the SOC in writing Sigma or YARA rules based on the red team activities.
- Advise infrastructure and application teams on robust remediation strategies beyond simple patching.
- Playing a leadership role in guiding the team in the remediation of identified vulnerabilities and track the progress.

Purple Team & Collaboration

- Research, timely introduction and implementation of new tools and techniques to enhance the current security posture of the Bank addressing the emerging threats to the Bank IT infrastructure.
- Keeping vigilance of latest security threats, advisories, alerts and vulnerabilities and initiating appropriate mitigation controls.
- Implementation of new IT security projects as identified by management.

Strategy & Compliance

- Assist in development and enforcement of IT policy, procedures, and standards.
- Ensure offensive operations validate the effectiveness of controls defined by various compliance and regulatory bodies (e.g., PCI DSS, ISO 27001, CBSL, SWIFT, NIST CSF etc.)
- Participate in various compliance/regulatory and management initiated audits and provide the timely responses to the audit observations.

APPLICANT'S PROFILE

- Bachelor's degree in Information Technology / Computer Science / specializing in Information Security or Cyber Security.
- 5+ years in Offensive Security, including at least 3 years focused on Red Teaming or Advanced Penetration Testing.
- IT and IT security related professional qualifications such as OSCE, OSCP, GRTP, CEH, eJPT, SSCP, ISACA CSXP, GSEC would be an added advantage.
- Deep expertise in exploiting Windows/Active Directory environments.
- Proficiency in Python, PowerShell, Bash or C# for custom malware/tool development.
- Experience in conducting adversarial emulations in cloud and containerized environments.
- Hands-on experience with frameworks such as Cobalt Strike, Metasploit, Havoc, or Brute Ratel.
- The ability to "think like the enemy" to find unconventional paths into a network.
- Excellent communication skills, with the ability to translate deep technical findings into business risk for internal and external stakeholders.
- 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.
- Comprehensive knowledge on both Windows and Linux environments.
- Strong work ethics, strict adherence to Rules of Engagement (RoE), and meticulous attention to detail during sensitive operations.
- Knowledge on various regulatory and compliance requirements like PCI DSS, ISO 27001, NIST CSF, CBSL, SWIFT would be an added advantage.

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 (Red Team Operations)

COMMERCIAL BANK