RED Team Specialist (on Contract)

1.0 The Job/Responsibilities:

(a) RED Team Testing / Breach and Attack Simulation (BAS)

Perform analysis of proactive information security incidents & advanced threat actors for further enhancement of Detection Catalog and Hunt missions by leveraging the MITRE ATT&CK Framework Adversarial Tactics, Techniques, Procedures and Common Knowledge.

(b) Proactive Threat Hunting and Threat Intelligence

- Hunt for and identify threat actor groups and their techniques, tools and processes (e.g.-Using different types of open source intelligence feeds)
- Work with the detections team to transform attacker TTP's (Tactics, Techniques & procedures) into viable, low false positive behavioral and signature detections using a variety of techniques including supervised, semi-supervised, and unsupervised Machine Learning with an emphasis on sequential classification and pattern matching
- Monitor and analyze cybercrime threat reports for a different vertical, a specific attack or APT groups to proactively create IOCs (Indicator of Compromise) for Threat Hunting
- Use a wide variety of Cyber Threat Intelligence tools & websites, including the dark web
- Participate in "hunt missions" using cyber threat intelligence, analysis of anomalous log data and results of brainstorming sessions to detect and eradicate threat actors on various networks
- Develop and implement a threat hunting framework to provide a comprehensive structure for planning, executing, and managing threat hunting initiatives.
- Continuously enhance threat hunting techniques, processes, and tools to improve the organization's overall cybersecurity posture.
- Conduct proactive threat hunting exercises to identify and investigate potential security incidents and suspicious activities within the network.
- Document all findings, analysis, recommendations and investigation results in a clear and concise manner and generate reports for management and stakeholders.
- Conduct in-depth analysis of threat actors, their motivations, capabilities, and tactics, and provide insights on potential risks and impacts to the organization's systems, networks, and data.
- Produce regular and ad-hoc reports, briefings, and alerts on emerging threats, trends, and risk assessments to relevant stakeholders, including senior management, incident response teams, and other cybersecurity teams. The report shall also provide technical information in a clear and actionable format for various stakeholders.
- Provide timely and accurate intelligence support during security incidents, assisting incident response teams in understanding the nature and scope of the threat, and providing guidance on containment, remediation and recovery strategies.
- Track ransomware groups, phishing kits, and fraud campaigns on the dark web and open sources.

2.0 Required Minimum Qualifications & Experience:

2.1 Educational/Professional Qualifications

- A Bachelor's or Master's Degree in Information Security/Computer Science/ Computer Engineering/Information Technology Specialized in Information Security from a university or a Degree awarding institute recognized by the University Grants Commission

  OR

- **One or more certifications from the following**
  - Offensive Security Certified Professional (OSCP)
  - Offensive Security Web Expert (OSWE)
  - Offensive Security Experienced Penetration Tester (OSEP)
  - Certified Ethical Hacker (CEH)
  - Certified Penetration Tester (CPT)
  - eLearn Security Certified Professional Penetration Tester (eCPPT)
  - GIAC Penetration Tester Certification (GPEN)
  - GIAC Web Application Penetration Tester (GWAPT)

2.2 Experience:

- Minimum of four (04) years' experience in Red Team or Penetration Testing activities, including maintaining advanced operational, technical, and authoritative situational awareness during threat emulation-based exploitation and operations.
- At least one (01) year of experience in a leadership role (e.g., Team Lead) will be considered an advantage.
- Participation in Bug Bounty Programs and Capture the Flag (CTF) competitions will be considered an added advantage.
- Proficiency in programming/scripting languages such as .NET, Python, Bash, and PowerShell.
- Demonstrated expertise in leading and executing intelligence-led red team engagements, from planning through closure. Skilled in developing and implementing Tactics, Techniques, and Procedures (TTPs) aligned with threat actor profiles, industry frameworks, and best practices.
- Strong project management skills, including meeting requirements and timelines, preparing documentation, and overseeing risk management aspects throughout the project lifecycle.
- Excellent written and verbal communication skills with the ability to present technical concepts to non-technical audiences.

3.0 Preferred Skills/Competencies:

- Enhance internal VAPT and red team capabilities by developing scripts, automating processes and researching the latest exploitation Tactics, Techniques and Procedures (TTPs) used by threat actors.
- Capability of Organizing and participating in Capture-The-Flag (CTF) events, both internally and externally.
- Problem solving skills on short timeframes and ability to "think outside the box" & Analytical thinking with the ability to break down a big problem into smaller chunks.

4.0 Age:

Below 30 years of age as at 31.10.2026

5.0 Employment:

On contractual basis for a period of not more than three (03) years.

6.0 Remuneration and Other Benefits:

Negotiable with contribution to EPF and ETF.

Selection Procedure

Candidates who fulfill the required minimum criteria as specified will be shortlisted for the selection interview/s.

Applications

Applicants who possess the required qualifications and experience and wish to apply for the above position should submit their applications only through the following link **on or before 31.10.2026**
Link: https://www.cbsl.gov.lk/en/careers

Applicants are strictly advised to adhere to the terms and conditions stipulated in the above link when submitting applications.

Those who do not possess the required qualifications and experience as at the closing date will not be eligible to apply for this post. Any application not meeting the required qualifications, received after the deadline or not in the prescribed format, will be rejected without any notice.

Applicants are strictly advised to upload scanned copies of the educational/professional qualifications and documents to verify service experience which meet the eligibility criteria for the above post. Any application without the copies of certificates relevant to Educational/Professional Qualifications and experience will be rejected without any notice at any stage of the recruitment process.

Candidates who fail to provide originals of relevant documents at the certificate verification conducted prior to the interview will not in any manner be considered as eligible candidates.

Any form of canvassing will be a disqualification. CBSL reserves the right to decide on the number of positions to be filled or postpone or cancel the recruitment. CBSL has the discretion to determine the relevancy of qualifications and experience based on the requirements of the position. Only shortlisted candidates will be contacted for the next step of the recruitment process.

Section 20 and 24 (1) of Central Bank of Sri Lanka Act, No 16 of 2023 shall apply to all selected candidates.

Director – Human Resources
Central Bank of Sri Lanka, No. 30, Janadhipathi Mawatha, Colombo 01.
Telephone : 011-2477330 Fax : 011-2477715