Cyber and Fraud Centre Scotland

Job Description

Job title: CREST-Accredited Penetration Tester

The Role

You will deliver high-quality, ethical penetration testing engagements aligned with CREST standards. You will work across a diverse range of organisations, helping them understand their exposure to cyber threats and supporting practical, proportionate improvements.

A hands-on technical role with scope to influence service development, mentor others, and contribute to Scotland's wider cyber resilience ecosystem.

Key responsibilities

- Deliver CREST-aligned penetration testing engagements, including:
  - Infrastructure and network testing.
  - Web and application testing.
  - Cloud and hybrid environments.
- Plan, scope and execute tests in line with agreed methodologies and best practice.
- Produce clear, high-quality technical and executive-level reports.
- Communicate findings and risk in a clear, constructive manner to a range of stakeholders.
- Support remediation discussions and re-testing where required.
- Maintain accurate records and testing artefacts in line with governance and assurance requirements.
- Contribute to continuous improvement of tools, methodologies and internal knowledge sharing.
- Stay informed about emerging cyber threats, fraud trends, and regulatory changes affecting organisations.
- Maintain CREST accreditation.

Leadership & Stakeholder Engagement

- Work closely with the CEO and senior leadership team to shape strategy and operational planning.

- Build trusted relationships with clients, partners, and national stakeholders.
- Ensure compliance with internal processes, data handling requirements, and sector best practice.

Any other duties as required.

About you

We are looking for someone who is as passionate as we are about strengthening cyber and fraud resilience across Scotland.

Essential Skills & Experience:

- CREST accreditation.
- Proven experience delivering penetration testing in professional or client-facing environments.
- Strong understanding of common vulnerabilities and attack techniques (e.g. OWASP Top 10, MITRE ATT&CK).
- Experience with industry-standard tools (e.g. Burp Suite, Nmap, Metasploit, Nessus or equivalents).
- Ability to write clear, high-quality technical reports.
- Strong ethical mindset and commitment to responsible disclosure.

Desirable:

- Experience in cloud security testing (AWS, Azure, GCP).
- Knowledge of secure architecture or defensive controls.
- Experience mentoring junior testers.
- Additional certifications (e.g. OSCP, CHECK, CISSP, cloud security certs).

You must have the right to work in the UK.

What We Offer

- Meaningful work with real-world impact across Scotland's cyber ecosystem.
- Flexible and hybrid working arrangements.
- Support for continued professional development and certification.
- A collaborative, mission-driven culture.
- Competitive salary and benefits package (commensurate with experience).

More information

To apply, please submit your CV and a short covering statement to Kara.McLaughlin@cyberfraudcentre.com outlining your experience and CREST accreditation by 5pm 29th April 2026.