Role:	Red Team Specialist
Reporting to:	Red Team Practice Lead
Package:	Competitive Base + Bonus
Location:	Home Based

Summary of Role

CSA Cyber provide security testing and information assurance consultancy to a wide range of organisations, assisting them with understanding and improving their cyber security posture and risk profile.

As part of our growth strategy, we are seeking an Offensive Security Consultant (Red Team) to:

- With support from the wider red team perform penetration testing and simulated cyber attacks including red and purple team exercises, delivering reporting, concise debriefs and performing client workshops to technical, non-technical and C-suite audiences.
- Work closely with clients to understand their business needs and information security objectives, identify where they may have potential weaknesses and create innovative solutions and propositions to satisfy those objectives and needs.
- Participate in the red team sales function, working with both sales and delivery teams to attend client calls/meetings and create suitable technical scopes, statements of work and red team scenario planning whilst managing internal/external stakeholder expectations.
- Provide expert advice and oversight to key client accounts to enable successful and value driven delivery through bespoke offerings.
- Ensure the smooth running of the Tech Lead initiative.
- Use client solutions to enhance service development by providing regular input to CSA Cyber Sales, Delivery, Marketing, Customer Success, Product teams and the SOC.
- Participation in the bid management process within Offensive Security to ensure the efficient and consistent response to RFTs, RFPs, ITTs etc.

Overview

CSA Cyber offer a wide range of Cybersecurity testing and assurance services, providing support through the entire test lifecycle from scoping through to vulnerability discovery and remediation. Certified by the National Cyber Security Centre (NCSC) and CREST, delivered using the innovative Pentest-as-a-Service (underpinned by a highly configurable technology platform), CSA Cyber acts as an extension of your in-house security team and ensures you have everything you need to improve your risk posture.

The team established in 2006, and was subsequently acquired in 2024 by Cyber Security Associates Ltd, backed by FluidOne Limited. CSA Cyber is headquartered in the United Kingdom with offices in Gloucester and London. CSA Cyber have more than 400 customers throughout the UK, US and EMEA from the Retail, Financial Services, Government and other sectors.

Key Responsibilities and Objectives

- You will often be involved in simulated cyber attacks to test an organisation's security defences, and require a diverse set of skills. These skills span various domains, including technical, analytical, and soft skills.

- Work closely with clients to understand their business needs and objectives for protecting their organisation, identify where they may have potential gaps and create innovative solutions for managing and improving their cyber posture.
- Enable and support growth through a combination of client pre-sales and internal management and process improvement activities.
- Provide expert advice and strategic oversight to key client accounts to enable successful and value driven delivery through bespoke offerings.
- Actively participate within the CSA Cyber Community and wider security industry as an advocate and advisor.
- Maintain the knowledge base of methodologies and recommendations aligned with standards such as Penetration Testing (Crest, CHECK, ITHCs, OWASP), PCI DSS, ISO 27001, ISO 22301, GDPR and other regulatory and industry oversight groups.

Personal Qualities

- Proven experience with a good background in security testing, information assurance, risk management or cyber security.
- Understanding of security frameworks and control sets such as NIST, ISO 27001, GDPR, CHECK, CBEST/GBEST/STAR-FS, OWASP, ITHCs.
- Credible, confident and articulate, with excellent verbal and written communication and presentation skills.
- Ability to build relationships and convey issues clearly and concisely to stakeholders, at all levels of businesses with tact and diplomacy and balance differing interests.
- Self-motivation and good personal organisation skills.
- Able to focus on specific targets and demonstrate target achievement.
- Able to build collaborative and create effective working relationships with clients and colleagues at all levels.
- Strong analytical, judgement and decision-making skills.
- Ability to organise own time and prioritise workload.

Competencies

- Proficiency in manual and automated penetration testing methodologies and tools such as Metasploit, Burp Suite, Nmap, Wireshark and C2 frameworks such as Cobalt Strike/Outflank/Brute Ratel/Mythic/Havoc/Empire.
- Expertise in multiple operating systems and enterprise technologies, including Windows / Active Directory, Linux, and macOS and familiarity with OS-level exploits and privilege escalation techniques.
- Knowledge of common web vulnerabilities (e.g. SQL injection, XSS, CSRF) and experience with web application testing tools and methodologies.
- Techniques for phishing, pretexting, and other social engineering attacks and understanding human psychology to manipulate targets.
- Experience with wireless network penetration testing. Knowledge of wireless protocols (Wi-Fi, Bluetooth) and related vulnerabilities.

Preferable Skills:

- Reverse engineering binaries using tools like IDA Pro, Ghidra, or OllyDbg. Understanding of malware behavior and analysis techniques.

- Demonstrated ability writing code in at least one programming language relevant to the field (eg. Python, Ruby, C/C++, .NET and scripting languages such as bash/PowerShell etc..)
- Deep understanding of networking protocols (TCP/IP, DNS, HTTP/S, etc.) and experience with network scanning, packet sniffing, and traffic analysis.
- Preferred qualifications:
    - Certified Red Team Operator (CRTO/CRTO2)
    - CREST Certified Simulated Attack Specialist (CCSAS)
    - Offensive Security Certified Professional (OSCP)
    - Certified Ethical Hacker (CEH)
    - Offensive Security Certified Expert (OSCE)
    - Certified Red Team Professional (CRTP)

Other Important Information

- This is a home-based role, however, travel is expected in the context of client site visits, meetings and industry events.
- Remuneration includes a variable component tied, but not limited, to overall team sales and revenue targets.
- This role may require background security clearance due to the nature of the work CSA Cyber carries out, therefore, you must be willing and able to undergo the vetting process.
- Our team will endeavour to respond to every application if your skills and experience meet the needs of the role requirement.
- All personal data is held in accordance with the CSA Cyber Privacy Policy.