Cyber Security
Defence Consultants

Cyber Security Consultancy

January 2026

G-Cloud 15 Service Description

Cyber Security Defence Consultants Limited
St John's Innovation Centre
Cowley Road
Cambridge
CB4 0WS
T: 01223 421577
W: cybersecuritydefence.co.uk

Social Engineering Assessments/Phishing /Red Blue Teaming

Cyber Security Defence Consultants

Table of Contents

1 OVERVIEW

Cyber Security Defence Consultants work with organisations to improve and enhance their cybersecurity thresholds.

Our teams work within complex and diverse environments to achieve strategic, operational and realistic outcomes, including ISO/IEC27001, Cyber Essentials and Cyber Essentials Plus.

Over multiple consultancy contracts, we have developed and implemented information risk management processes that support our client's governance models and provide support to control specific target areas, improve processes and mitigate risk. This has increased security controls, ensuring that the organisation's risk appetite and cyber threats are reduced.

We engage experienced and qualified consultants who are up to date with all legislative practices to support organisations to manage risk effectively.

Our team hold qualifications including CISSP, CISM and ISO/IEC 27001 Lead Auditor and Lead Implementer.

Our cyber security consultancy engagement process aligns with the NCSC Certified Cyber Security Consultancy Standard, ensuring a high-quality client journey including agreed deliverables, transparent and regular reporting, defined escalation paths, suitably skilled and qualified resources and focused delivery.

2 SERVICES

2.1 Social Engineering Assessments/Phishing/Red Blue Teaming

Cyber Security Defence Consultants provide social engineering assessments as part of our accredited penetration testing and IT Health Checks, providing independent assurance that an organisation's internal and external cybersecurity meets its requirements.

The assessments identify weaknesses in an organisation's security awareness and determine how well an organisation is prepared to recognise and respond to social engineering attempts.

Using our approved penetration testers, we conduct ethical hacking to test and replicate the actions of an attacker to identify vulnerabilities within an organisation's defences.

Our infrastructure testing typically covers an organisation's exposed external perimeter, such as internet-facing firewalls, proxies, mail gateways, web services, and remote access services, which must be secured as a first line of defence.

We conduct vulnerability assessments and in-depth internal testing, covering configuration and building reviews against industry and vendor recommendations, good practice, and NCSC guidance. We also perform specialist mobile device testing, including lost/stolen device scenario testing.

We conduct web application testing in line with OWASP standards to ensure that internet-facing applications are securely coded and role-based access controls are enforced.

Being specialists in carrying our Red/Blue Teaming engagements, we can provide an 'outside-in' test.

The primary goal is proactively identifying and addressing security gaps before malicious actors can exploit them. It helps organisations understand their actual risk posture and strengthen their overall security posture.

This can include:

1. **Physical Security** – testing the effectiveness of physical access controls, such as locks, cameras, and guards.
2. **Social Engineering** – attempting to manipulate employees into revealing sensitive information or granting unauthorised access through phishing, pretexting or impersonation.
3. **Network and System Penetration** – attempting to gain unauthorised access to networks, systems, and applications by exploiting vulnerabilities or misconfigurations.
4. **Wireless Security** – testing the Security of wireless networks and devices
5. **Application Security** – identifying vulnerabilities in web applications, mobile apps, or other software
6. **Incident Response** – assessing the organisation's ability to detect, respond to, and recover from security incidents.

All exercises are conducted by specialists and qualified consultants with the skills, tools, and knowledge to simulate realistic attacks. The findings and recommendations from red teaming exercises help organisations understand their security posture, identify weaknesses, and prioritise remediation efforts to enhance Security.

Build and configuration reviews can be carried out as required, clearly communicating threats and risks in your organisational context. Vulnerabilities will be swiftly and accurately identified and explained.

Remediation and strategic fix advice will be provided, and consultants will be available to advise during the journey to enhanced Security.

Cyber Security Defence Consultants offers assessments across SaaS, PaaS, and IaaS hosted locally or within Microsoft Azure, Amazon Web Services (AWS) and on VMWare-based and open-source virtualisation platforms.