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

IT Health Check and Penetration Testing

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, reducing the organisation's risk appetite and cyber threats.

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 IT Health Check and Penetration Testing

Our IT Health Check and Penetration Testing are essential cybersecurity practices to help organisations identify and mitigate potential vulnerabilities and security risks.

Cyber Security Defence Consultants provide a service to secure organisations' perimeter and quickly remediate vulnerabilities through real-world attackers' techniques and tools. Whether you use SaaS, PaaS, IaaS, serverless solutions, Azure, AWS or VMWare virtualisation, we identify and mitigate the vulnerabilities and principal security concerns.

Part of this is to assess the configuration, security settings, and overall health of an organisation's networks, services, workstations, and other IT assets. While automated scanning provides some basic assurance within organisations, our skilled testers will identify false positives so that effort can be focused on areas of actual risk. This includes compliance checks to evaluate an organisation's adherence to relevant industry standards, regulations, and best practices.

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

Vulnerability assessments are conducted for more in-depth internal testing, identifying vulnerabilities in software, operating systems, and applications that cyber threats could exploit. They cover configuration and build reviews against industry and vendor recommendations and good practices, alongside NSCS guidance.

Specialist testing of mobile devices is carried out, including lost/stolen device scenario testing. Web application testing aligns with OWASP standards, ensuring that internet-facing applications are securely coded and role-based access controls are fully enforced. This extends to assessing the security awareness and training level among employees to identify potential risks associated with human behaviour.

The primary goal is to provide a comprehensive view of the organisation's IT security posture, identify potential weaknesses or areas for improvement, and recommend remediation measures to enhance overall security.

Specialist consultants conduct penetration tests to provide an 'outside-in test' simulated to exploit vulnerabilities and bypass security controls, just as a hacker would, but in a controlled and authorised manner.

We can use a range of phishing and social engineering engagements tailored to the business services and requirements.

Our skilled penetration testers will assist with scope definition, ensuring that all external and internal testing requirements are met. We then conduct structured automated and manual testing, exposing all vulnerabilities and improving an organisation's security posture.

The findings and recommendations can assist you in strengthening your overall security posture by addressing identified vulnerabilities and implementing additional security measures.

Build and configuration reviews are carried out as required, clearly communicating threats and risks and providing training and additional support to enhance 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.

Offering IT checks and penetration testing is essential to a comprehensive programme, enhancing an organisation's overall cybersecurity resilience.