PENTEST CYBER

Pricing & Service Description

G-Cloud 15 – Penetration Testing

PUBLIC

V 1.0

CESG Certified Professional

TIGERSCHEME Providing excellence in penetration testing

OFFENSIVE Security OSCP

CISCO CERTIFIED CCNP ENTERPRISE

CISCO CERTIFIED SPECIALIST

CISCO CERTIFIED CCNA

Assured Service Provider in association with National Cyber Security Centre

Crown Commercial Service Supplier

IASME GOVERNANCE AUDITED GOLD CERTIFIED

GDPR CERTIFIED

QUALITY PRINCIPLES CERTIFIED

CYBER ESSENTIALS CERTIFIED PLUS

1. Pricing Table

Prices are exclusive of **VAT**.

Service Name	Service Description	Day Rate
Penetration Testing & Vulnerability Assessment	Our full range of penetration testing and vulnerability assessment services.	£1000 p/d
Vulnerability Scan	Vulnerability scanning for any network size based on the number of IP addresses, e.g. a /24 (254 IP addresses) could consist of 16 /28s.	£300 per 16 Ip addresses (/28).

2. What is Penetration Testing?

Penetration testing is an authorized cyberattack against computing systems to evaluate the quality of deployed defences. The activity involves incorporating techniques from real-life attacks while attempting to prevent damage to production systems. The goal of the test is to identify weaknesses and prevent unauthorized access to features, systems and data.

A penetration test is not to be confused with a vulnerability scan or assessment that aims to identify, quantify and prioritize vulnerabilities without the granularity of targeting obscure or undocumented exposure that a penetration test aims to achieve.

© Pentest Cyber 2026 www.pentestcyber.co.uk

3. What are the types of Penetration Testing?

Penetration testing, a vast and complex subject that spans a multitude of subject areas. Pentest Cyber offer Application Testing, Infrastructure Testing, Build Review and Cloud Testing.

- Application Testing – Assessment of web applications and associated services, such as API and other data services.
- Infrastructure Testing – Review of exposure to internal and external assets with varying vector avenues, including wireless.
- Build Reviews – Simulate a host compromise scenario with an attempt to escalate privilege and laterally move.
- Cloud Testing – Testing of cloud deployment, both IaaS and SaaS, where authorisation allows.

4. Are your testers suitably certified?

Pentest Cyber operate entirely within the UK, offering clearance to a high government standard and are appropriately qualified with **OSWE, OSCP**, CSTL, **Cisco CCNP, NCSC CCP IA-Auditor, SIRA qualified** and are **Cyber Essentials, Cyber Essentials Plus,** and **IASME Auditors.**

5. How much does a penetration test cost?

The cost of a penetration test depends on the specification and outcome set to achieve. Each project requires a technical scope specification to capture the testing boundary and prompt notification of issues that may arise.

Pentest Cyber, by this nature, do not provide a set price for these services to enable confidence and assurance in our delivery. We aim to be competitive, so please contact us to discuss pricing vs competition of similar quality.

© Pentest Cyber 2026 www.pentestcyber.co.uk

6. What is included in a penetration test report?

Pentest Cyber provides a full testing report, which covers the following:

- Executive Summary – A non-technical summary of issues for management and executives.
- Project Scope – An area defining the agreed scope
- Detailed technical write-up – The anatomy of found issues, severity and references.
- Risk level – Overall risk to listed issues aligned with OWASP Top 10 and CVSS.
- Recommendations – Pragmatic recommendations and references to remedy the cause.

7. How do we work compared to other providers?

Pentest Cyber penetration testing services are designed to comply with international best practice standards and methodology, tiered by levels of complexity. These relate to both Infrastructure and Web Application environments in external, internal or cloud formats.

- Level 1 – Vulnerability Scan
- Level 2 – Vulnerability Assessment
- Level 3 – Penetration Test

Levels are progressive in terms of complexity, with each subsequent level incorporating previous levels. The term Penetration Testing is subjective and often used interchangeably to describe Levels 1 and 2.

Pentest Cyber does not undertake Denial of Service (DoS) type testing or defacement activities unless expressly authorised to do so. In all cases, Pentest Cyber require proof of ownership of systems, documented permission, and legal disclaimers where appropriate.

All penetration testing engagements require a definitive scope agreement, ensuring a clear objective and tailored service.

© Pentest Cyber 2026 www.pentestcyber.co.uk

8. About Pentest Cyber

Pentest Cyber, a world-class resource for remote penetration testing services. We specialise in subject areas such as web application, cloud and infrastructure testing. Pentest Cyber deploys a vast array of professional tools, techniques, and bespoke methodologies to every engagement. UK personnel are appropriately vetted "to a high government standard" and qualified to national and international certification pathways (**OSCP, QSTM, CCNP, CCP IA Auditor, CCP SIRA**).

We operate under UK law and comply with all relevant legislation. We require proof of ownership and explicit permission to undertake tasks to ensure compliance with applicable law.

Pentest Cyber operates in all sectors, including those requiring strict international security protocols. We operate remotely, use pseudonyms, and secure communication protocols as standard to protect our personnel and clients.

Pentest Cyber methodology and code of conduct align with leading international standards, consistently upholding quality through progressive elaboration, formal peer review, and sign off.

Delivered using best practice policies and procedures, carried out by highly qualified and vetted individuals with knowledge and skills of the prevailing threat landscape; covered by a rigorous code of conduct.

If you need an intuitive, autonomous test team "vetted to a high government standard" who understand CABs, ISO 27001, ITIL, "follow the sun", DCPP or the many other industry acronyms indicating specific security needs; then look no further.

© Pentest Cyber 2026 www.pentestcyber.co.uk

9. Security Accreditations and Affiliations

Cyber Essentials is the UK Government standard for cyber security. The protections you need to have in place for Cyber Essentials Plus are the same, but this time the verification of our cyber security is carried out via a technical audit.

The audited IASME Governance standard is IASME's highest level of certification and is an excellent alternative to ISO 27001 for small and medium-sized organisations.

IASME GDPR Certified demonstrates that we have considered the General Data protection regulation (GDPR) and acted accordingly to standard.

The Quality Principles standard is an IASME certification and is an excellent alternative to ISO 9001 for small and medium-sized organisations.

© Pentest Cyber 2026 www.pentestcyber.co.uk

An OSCP has demonstrated the ability to use persistence, creativity, and perceptiveness to identify vulnerabilities and execute organised attacks under tight time constraints. OSCP holders have also shown they can think outside the box while managing time and resources.

Tiger Scheme provides a way in which skills and experience can be formally recognised and is more than a statement of previous work or a reference. Skills assessments leading to certification are rigorous and are based on academic standards.

The CCP assured service has been developed by the NCSC in consultation with government, industry, and academia to address the growing need for specialists in the cyber security profession and sets the standard for UK cyber security professionals.

© Pentest Cyber 2026 www.pentestcyber.co.uk