CYBER CROWD

CREST

PEN TEST

Penetration Testing

Proactively Identify and Secure Vulnerabilities

cybercrowd.co.uk

Ensure Robust Security with Regular Testing of Your IT and AI Environments

Good security practice involves regularly testing your IT infrastructure, including AI and LLM environments, for vulnerabilities and exploitable weaknesses. Penetration testing, also known as Pen Testing or ethical hacking, is an authorised simulation of an attack on a computer system, such as a network, application, or other critical infrastructure. This process mimics the actions of a hacker, allowing your organisation to uncover and address security weaknesses before they can be exploited.

By assessing whether your IT and AI systems are susceptible to a cyber-attack, you can effectively plan, repair, and strengthen your organisation's defences. Our Pen Testing services provide comprehensive evaluations to ensure all aspects of your technology environment are secure.

Internal Pen Test

An internal pen test identifies vulnerabilities within your network by simulating insider threats, such as rogue employees or compromised devices. This helps you gauge how deeply an internal attacker could penetrate your systems.

External Pen Test

An external pen test examines your outward-facing infrastructure, such as web applications, servers, and network defences, to assess and fortify your systems against external attacks..

AI and LLM Environment Test

Our specialised testing services also cover your AI and Large Language Model (LLM) environments. We assess these advanced systems for unique vulnerabilities and ensure they are robust against potential exploitation.

With CyberCrowd's CREST-certified assessment services, organisations bolster their defences against evolving cyber threats

Types of Pen Test

Applications

A test to look for vulnerabilities in apps and related systems, including web apps, websites, mobile and IoT apps, cloud apps and APIs.

Hardware

A test for vulnerabilities in devices connected to the network, such as laptops, mobile and IoT devices, and operational technology (OT).

Red Teaming/ Social Engineering

Evaluate employee cybersecurity hygiene and assess vulnerability to social engineering and physical security breaches.

Network/Wi-Fi

A test to identify and exploit any weaknesses within the company's entire computer network: external facing, internal and wireless.

AI & Large Language Models (LLMs)

A test to identify and mitigate security vulnerabilities in AI and LLMs.

Vulnerability Assessments

An automated procedure using a range of scanners and tools to identify vulnerabilities.

Cloud Review & Test

Essential for organisations using AWS, Azure, and Google Cloud: ensure best practices and test configurations.

Expertise You Can Trust: Certified Pen Testers for All Sectors

CREST PEN TEST

Our certified Pen Testers, equipped with Security Clearance (SC) and Non-Police Personnel Vetting (NPPV) level 2 certifications, specialise in testing organisations of all sizes, including critical national infrastructure, defence, government, and NHS sectors. Their expertise ensures thorough testing to uphold strong security measures and safeguard against evolving cyber threats.

The Aim:

Identify Vulnerabilities: Discover security weaknesses in your IT systems to prevent breaches and data loss.

Enhance Security: Gain actionable insights and remediation advice to reduce the impact of identified vulnerabilities, strengthen defences, and ensure robust protection against evolving threats.

How it works

As a CREST-certified provider of penetration testing services, our approach and methodology meet the highest standards of approval

Intelligence Gathering

This phase of the engagement involves using a range of tools and techniques such as active scanning, open-source intelligence (OSINT.)

This involves using public sources such as websites or other data points to detect data leaks, accidental data exposure and software or hardware versions.

Vulnerability Analysis

The vulnerability analysis aims to discover and identify security weaknesses that can be exploited by an attacker.

The flaws can be misconfigurations or insecure platforms. Techniques used vary from automated vulnerability scanners, metadata analysis, traffic monitoring, public research, common/default password databases.

How it works

Pre-Exploitation

During this stage, the tester will use their experience and knowledge to plan how to exploit any vulnerabilities identified during the scanning phase.

Sometimes these will be well known vulnerabilities due to out-of-date patches or end of life systems, other times it may require some creativity and research. All engagements are different, the value that the CyberCrowd testers bring to the table is their experience and knowledge, covering both infrastructure and applications. The good thing about all this planning is that if you want us to replicate the vulnerability, we can walk you through exactly what we did.

Exploitation

The exploitation phase of a penetration test focuses on gaining access to the system or resource using different methods depending on the intelligence gathered in previous steps.

This phase should be a well-planned and specific attack. Methods vary from, but are not limited to, initial access, execution, privilege escalation, lateral movement, and credential access.

Reporting and Client Portal Access

Reporting

In the final phase, we generate a detailed report outlining any misconfigurations and vulnerabilities discovered.

Through our secure client portal, you can easily access and manage your cybersecurity assessments. The portal offers real-time visibility into pen testing results, risk scores, and personalised remediation recommendations, enabling swift and effective security improvements.

Contact us today to arrange a demo of the client portal and discover how it can enhance your security management.

1000+

Completed tests

We have delivered over 1000 penetration tests to our customers and partners.

Enhance Security Posture and Resilience with Tailored CyberCrowd Services

Managed Detection & Response Services via CyberCrowd's 24/7/365 UK Security Operations Centre

Proactive threat detection, investigation, and response whether your infrastructure is on the cloud or on-premises. Watch the video: www.cybercrowd.co.uk/solutions/soc

Incident Response

Gain access to both remote and onsite support. This rapid response capability allows for quick decision-making and containment, minimising the disruption caused by cyber incidents.

Data Protection

Our data protection consultancy includes a thorough data gap analysis, ensuring compliance and seamless backup and recovery.

Incident Response Tabletop

Exercises that simulate security breaches to test response plans, identify weaknesses, foster team cohesion, and boost preparedness.

Training & Awareness

Incorporate security by design into your organisation through customised or platform-based cybersecurity training and awareness.

Experts as a Service & Consultancy

Whether it's a DPO or a CISO, your needs are covered with a professional and capable team available to you as a service.

Strategy & Transformation

We offer expert guidance to help organisations develop a strategic vision for advancing their cybersecurity maturity.

Certification & Readiness

Offering a complete range of certification readiness, including Cyber Essentials, ISO 27001, SOC 2, and DSP Toolkit.

Ethical Hacking

Drop us an email or give us a call with any questions or to find out more.

We endeavour to answer all enquiries within **24 hours** on business days.

✉ sales@cybercrowd.co.uk

☎ 0203 858 7372

CYBER CROWD

Embrace proactive cybersecurity measures with our penetration testing services, ensuring your defences are robust and up to date across all your technology environments.

Contact us today...

Engage with confidence

Citation ISO Certification ISO 27001: 2013 Information security management REGISTERED

Citation ISO Certification ISO 9001: 2015 Quality management REGISTERED

Citation ISO Certification ISO 20000-1: 2018 IT service management REGISTERED

CYBER ESSENTIALS CERTIFIED PLUS

CYBER ESSENTIALS CERTIFIED

CREST PEN TEST

Crown Commercial Service *Supplier*

AUDITED IASME CYBER ASSURANCE LEVEL TWO

Assured Service Provider in association with National Cyber Security Centre Cyber Incident Response (Level 2)

Assured Service Provider in association with National Cyber Security Centre Cyber Advisor (Cyber Essentials)

Assured Service Provider in association with National Cyber Security Centre Cyber Incident Exercising

Contact us
info@cybercrowd.co.uk
cybercrowd.co.uk