CyberQ group

Penetration Testing

A Penetration Test is arguably the most important part of any cybersecurity journey as it will test an organisations 'final line of defence' against attackers.

Simulate Real-World Attacks. Test Your Defences. Build Cyber Resilience.

What is a Penetration Test?

Penetration Testing is a controlled cybersecurity exercise where certified ethical hackers simulate real-world attacks to uncover and safely exploit vulnerabilities within your organisation's digital infrastructure. This proactive approach goes beyond standard vulnerability scans by demonstrating how malicious actors could gain unauthorised access or disrupt services.

Our CREST accredited assessments combine exploitation of known attack vectors against vulnerable software and hardware, alongside less common, multi-layered attack paths that reflect the tactics of modern adversaries.

Our **award-winning**, easy-to-understand reports are designed to support both executive decision-makers and technical teams. They provide:

- Clear summaries for senior stakeholders
- In-depth technical analysis for IT and security teams
- Actionable, prioritised recommendations aligned with best practice

Types of Penetration Test:

We conduct comprehensive testing of your chosen technologies, including:

External: Simulates an attacker targeting the client from the internet.

Internal: Simulates an attacker already within the client network.

Other Types of Tests: Web Apps, Mobile (Android & iOS), API & Wi-Fi

Our Process:

1. **Scoping & Intelligence Gathering:**
   Collaborate with your team to define the scope and understand your environment.
2. **Vulnerability Discovery:**
   Identify potential security flaws using both automated tools and manual testing.
3. **Exploitation:**
   Safely exploit vulnerabilities to demonstrate their real-world impact.
4. **Post-Exploitation:**
   Assess what an attacker could do once inside your network.
5. **Reporting & Debrief:**
   Deliver a tailored report with practical, step-by-step recommendations to reduce risk.

Why Penetration Testing Matters:

Goes Beyond Automated Scanning. Real attackers don't stop at detection, they exploit. We simulate those tactics to test your true resilience.

Identifies Complex Attack Paths. We uncover chained vulnerabilities that automated tools may miss.

Supports Regulatory Compliance. Many standards (e.g. ISO 27001, PCI DSS, GDPR) require or recommend regular penetration testing.

Validates Your Cybersecurity Investments. Demonstrates whether your controls are working as intended, and where there may be gaps.

Key Benefits for Your Organisation:

Realistic Threat Simulation.
Test your systems against the same techniques used by cybercriminals.

Early Detection of Critical Vulnerabilities.
Address weaknesses before they're exploited.

Improved Incident Response.
Assess how effectively your teams can detect and respond to attacks.

Increased Stakeholder Confidence.
Show customers, regulators and partners you take cybersecurity seriously.

Why do you need a Penetration Test?

Boards are increasingly demanding greater insight to make informed decisions in managing risk and delivering better business outcomes. Usually compliance and regulatory fulfilments drive Penetration Testing. However, all organisations need to ensure they have the latest information about their security posture.

The Numbers That Matter:

Organisations using penetration testing save an average of £315,000 per data breach due to faster detection and containment.

93% of internal penetration tests reveal pathways to high-value systems and data.

75% of firms discover critical security gaps that automated tools failed to identify.

Over 80% of major regulatory frameworks either require or strongly recommend regular penetration testing.

Why CyberQ Group?

Collaboration

We work closely with our partners to mutually provide help and inspiration in our continual efforts in striving for cyber resilience.

Expertise

Our people are highly experienced, certified consultants, with international experience and proven track records.

Innovation

We continually seek to deliver what enables global organisations to achieve a higher level of security maturity and capability.

About CyberQ Group

Established in 2016, CyberQ Group's global team of cyber and business professionals have decades of combined experience within the cyber and technology sectors. We believe even the most daunting challenges can be overcome through collaboration, innovative technology and great people.

We bring together the best of all these components, keeping your business better protected. The result? Improved business risk profile, significant operational cost savings and long-term peace of mind.

Get in touch today to find out how we can keep your business secure.

theteam@cyberqgroup.com

www.cyberqgroup.com

CREST

UKAS ISO 27001