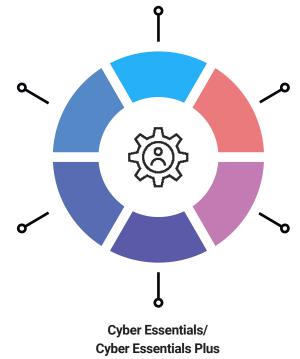


Penetration Testing

Penetration testing is a core tool for analysing the security of IT systems. Penetration testing can be viewed as a method for gaining assurance in your organisation's vulnerability assessment and management processes.

Our CREST approved penetration testing services can give your organisation confidence that the products and security controls tested have been configured in accordance with good practice and that there are no common or publicly known vulnerabilities in the tested components, at the time of the test. Methods provides comprehensive assessments of weaknesses vulnerabilities and potential attack vectors following industry standards.

Our Services



Cyber Essentials is an NCSC scheme designed to secure organisations against commodity-based threats. Cyber Essentials Plus is a technical assessment of the controls outlined in the Cyber Essential requirements

API Testing

Penetration testing of APIs allows the identification of security vulnerabilities within the API to prevent potential attacks

External Instructure Testing

External testing focuses on finding vulnerabilities that can be exploited from outside of the organisation's network to potentially gain access to the inside of the network

Internal Infrastructure Testing

Internal infrastructure testing focuses on what a threat actor with access to the organisations internal network could subsequently achieve

Web Application Testing

Web App testing audits web applications and sites for security vulnerabilities that an attacker could exploit

IASME Cyber Baseline

International cyber hygiene certification which shows your organisation's commitment to cyber security even if you're outside the UK - providing global supply chains a standardised and respected accreditation

Our Process

| 1) Planning ×_↑ └ × | Engagement call with an allocated tester to identify goals, compliance requirements, and timeframe |
|---------------------------|---|
| 2) Scoping | Determining testing depth, and resources, creating a testing plan considering critical assets |
| 3) Testing | Our expert testers will conduct thorough testing, using industry standard penetration testing methodologies |
| 4) Report/ Remediation | Production of a comprehensive report including vulnerabilities found and some potential remedial action We have resources to help if you need additional support |
| 5) Retesting | Follow-up testing to ensure remediation actions are correctly implemented Improvements to your organisation's security will be reflected in an updated report |



