FORTIS CYBER®

CREST SECURITY TESTING Vulnerability Assessment

CREST SECURITY TESTING Penetration Testing

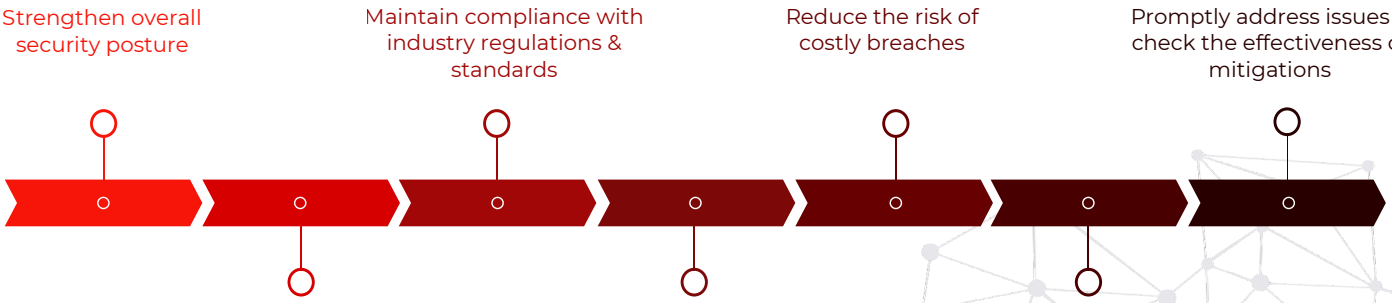
Automated Penetration Testing (PTaaS)

Automated penetration testing (Penetration Testing as a Service) enables organisations to perform penetration testing within their environment at any given time to quickly identify and validate security weaknesses. By simulating real-world attacks with minimal manual effort, it provides faster, cost-effective, and continuous testing, making it ideal for keeping up with evolving threats. Automated network penetration testing:

- combines the knowledge, methodology, processes, and toolsets of a hacker into a single solution for organisations of any size
- delivers substantial value at a lower cost compared to traditional security assessments making penetration testing accessible to SMEs

What are the benefits?

Automated testing provides organisations with fast, cost-effective, and scalable security assessments. It enables continuous monitoring, integrates easily into development workflows, and delivers consistent results across systems.



Overview

Fortis Cyber® offers two distinct automated penetration testing services designed to strengthen your organisation's security posture and maturity.

- **INTERNAL NETWORK PENETRATION TESTING:** Conducted using a device connected to your organisation's internal environment, testing identifies security vulnerabilities within your internal network. These activities simulate the actions of a malicious insider or an attacker who has gained internal access.

- **EXTERNAL NETWORK PENETRATION TESTING** Assuming the role of a malicious attacker from the public-facing internet, testing uncovers security flaws within your external-facing systems, such as gaps in patching, configuration errors, and authentication issues.

www.fortiscyber.co.uk
enquiries@fortiscyber.co.uk
+44 (0)207 898 3971

Engagement Methodology

Automated penetration testing combines multiple security testing methodologies that were traditionally performed manually and delivers them in an automated, repeatable way to provide organisations with consistent, high-value insights.

- **EGRESS FILTERING TESTING:** Automatically perform egress filtering to ensure that your organisation is effectively restricting unnecessary outbound traffic. Weak egress controls can allow attackers to exfiltrate data from your organisation's environment using traditional methods and unmonitored ports.
- **AUTHENTICATION ATTACKS:** When user account credentials are discovered, they are automatically validated and assessed for potential misuse. This is a common process executed by both malicious attackers and penetration testers and is performed during privilege escalation.
- **PRIVILEGE ESCALATION AND LATERAL MOVEMENT:** Using a valid set of credentials, the test attempts to move through the network to identify high-value systems and assets at risk within the environment.
- **DATA EXFILTRATION:** Confidential and/or sensitive data leaving an organisation is a major threat. If access to critical data can be attained, activity is simulated and logged to highlight weaknesses in data exfiltration controls.
- **SIMULATED MALWARE:** With elevated access, automated testing will attempt to upload malicious code onto remote systems to test the organisation's end-point anti-malware controls.
- **TIMELY REPORTING:** An executive summary, detailed technical report and vulnerability report are delivered once testing is completed. The comprehensive reports provide actionable insights and enable your organisation to validate monitoring and alerting capabilities.

Fortis Cyber® Penetration Testing Services

Automated penetration testing can also be combined with consultant-led testing for a hybrid approach, using automated testing for continuous coverage and consultant-led testing for deep, complex, or highly sensitive environments. Fortis Cyber® offers the following types of penetration testing services:

Red Teaming → **Purple Teaming** → **Consultant-led Pen Testing** → **Automated Pen Testing** → **Vulnerability Assessments**

Fortis Cyber® CREST Accreditation

Fortis Cyber® is a CREST accredited organisation for both Penetration Testing and Vulnerability Assessments. Through CREST's demanding accreditation process, organisations buying security testing services get the assurance that:

CREST SECURITY TESTING — Penetration Testing

CREST SECURITY TESTING — Vulnerability Assessment

- The services will be delivered by trusted companies with best practice policies and procedures.
- The work will be conducted by highly qualified individuals with up-to-date knowledge, skills, and competence to deal with all the latest vulnerabilities and techniques used by real attackers.
- Both the company assessments and individual qualifications are underpinned by meaningful and enforceable codes of conduct.

For more information or to arrange a call with our team to discuss how Fortis Cyber® can support your organisation visit our website www.fortiscyber.co.uk or email enquiries@fortiscyber.co.uk