

Why MTI offers this service

Securing IT infrastructure from external and internal threats is imperative for any organisation that wants to survive and thrive in the modern world. To better safeguard operations, it is important to conduct regular assessment of the IT infrastructure and areas of exposure.

By making organisations aware of the broad range of vulnerabilities within their infrastructure and reporting on remediation options to correct any identified issues, MTI can help minimise the risk of compromise and help prevent successful attacks from criminal enterprises, opportunist hackers and malicious users.



The Service

MTI can test all the areas of exposure within your organisation: external, internal and cloud-based. Our consultants can assess all parts of your existing IT infrastructure to help you understand the level of risk from the technologies and systems in use.

We can provide an overview of the state of your network and evidence of the vulnerabilities and weaknesses that need to be addressed. Our report includes recommendations on how to remediate those vulnerabilities and outlines a path to secure your environment.

You can choose to remediate the vulnerabilities yourself or take advantage of our professional services team and 30 years of experience to fix the issues on your behalf.



Stage 1: What we test: External network

External network penetration testing: We conduct external network penetration testing to identify risks and flaws in your Internet Gateway. Our approach combines a manual test and tools-based vulnerability scan to ensure a comprehensive assessment of all Internet-facing systems.

Our testing includes identifying known vulnerabilities, configuration errors, missing patches, out-of-date software, default and guessable passwords, and other issues. We use advanced tools and exploit frameworks to thoroughly test systems against the latest threats and weaknesses, including vulnerabilities that may not have a patch yet. This allows us to assess the effectiveness of existing protections and recommend additional measures if necessary.

Stage 2:

What we test: Internal network

- Internal network penetration testing
- Domain compromise assessment
- Operating system hardening build review
- Password reviews
- Wireless infrastructure assessment
- Automated firewall configuration review
- VPN review
- Mobile device reviews

Stage 3:

Testing of Cloud-Based Infrastructure

The majority of organisations have some form of hybrid infrastructure using common cloud-based services such as Office 365, Azure and AWS. MTI offers testing and security reviews of these services based on recognised standards such as CIS, which can be added to your IT Health Check.

Stage 4:

Reporting

A formal results report on the testing phases will include the Security Assessment's objective, scope, executive summary of findings, risk grading, CVSS scoring, vulnerability description, recommendations, and contact details for the customer and test team, as well as CHECK/CREST/Cyber Scheme consultants' certifications.



Contact MTI

T: +44 (0) 1483 520 200

E: ukmarketing@mti.com

W: mti.com

• Datacentre Modernisation
• Data & Cyber Security
• Managed Services
• IT Transformation

Vulnerability register:

To aid with remediation and compliance tracking, MTI will provide an Excel-based Vulnerability Register listing all issues found during manual testing, along with the CVSS scores in a sortable and editable format.



Outcomes & Benefits:

Our IT health check delivers the following outcomes:

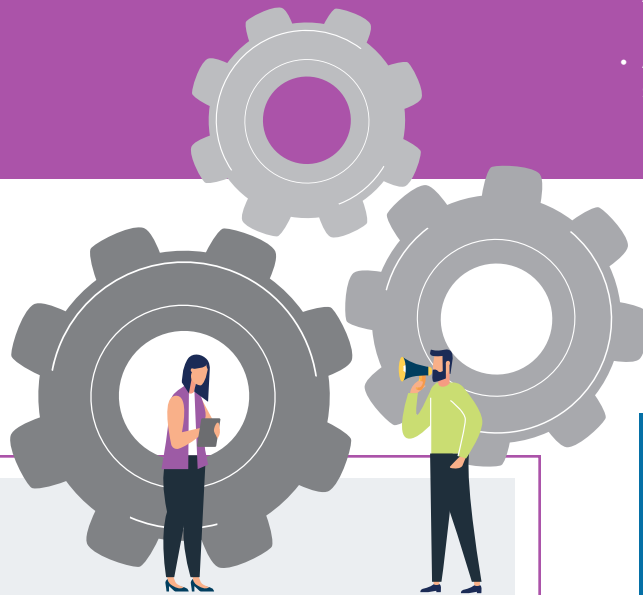
- Provides a thorough examination and test of the external internal and cloud-based infrastructure.
- Details issues that comprise a threat to the integrity of the company IT infrastructure.
- Outlines where elements of the IT infrastructure are configured correctly and securely.
- Provides peace of mind by discovering vulnerabilities and outlining how they can be addressed.



Deliverables of the service

The IT health check service provides:

- A formal report that presents an overview of the security posture of the IT infrastructure and suggested remediation steps for improvement.
- An action plan that sets out the recommended remediation steps and details the stages that help you track your remediation progress.
- A report that can be used to justify expenditure to improve infrastructure defences.
- An outline of your path to a more secure environment.
- A report which can be submitted to accreditation bodies.
- A report which demonstrates your commitment to security to your internal and external customers.



Why MTI?

MTI is a lifelong member of global cyber security body, CREST, and has been conducting penetration testing or more than 20 years. As one of the first companies to provide this service, we have developed a wealth of knowledge and skills in the tactics used by criminal enterprises, opportunist hackers and malicious users to gain access to corporate networks. This enables us to identify risks to the business and outline remediation measures to counter those risks.

If required, you can take advantage of our expertise to implement the necessary remediation measures via our professional services operation.

“Both consultants who came into our organisation to carry out pen testing services, were very respectful and a pleasure to work with. They made my job very easy.

They delivered within the timeframe as expected and it would be a pleasure to work with them again if we need more penetration testing”.

Kaelan Silver Sturdee
System Integration & Test Engineer
Motorola

Contact MTI

T: +44 (0) 1483 520 200
E: ukmarketing@mti.com
W: mti.com

Datacentre Modernisation
Data & Cyber Security
Managed Services
IT Transformation