External Healthcheck

To stay safe in the modern era, all organisations need to ensure their internet boundaries are safe and secure from external attackers.

Any elements of the network infrastructure exposed to the Internet will be tested constantly by opportunists, ransomware gangs and criminal enterprises. To preserve the integrity of the internal infrastructure, regular examination, and remediation of issues on all Internet-facing equipment is required.

The Service

Our service is designed to help strengthen the security of your external facing infrastructure and identify vulnerabilities where equipment or services could be compromised or breached by an attacker. Our range of tests and reviews provides an overview of the state of your external network and evidence of the vulnerabilities and weaknesses that need to be addressed.

Our report includes recommendations on how to remediate those vulnerabilities and provides a path to secure your environment. You can choose to remediate the vulnerabilities yourself or take advantage of our professional services team and 20 years of experience to fix the issues on your behalf.

Stage 1
What we test

Our penetration testing for external facing networks covers a number of areas.

Manual penetration test: to determine the flaws and risks exposed through your Internet Gateway, we conduct a manual penetration test to provide an intelligent picture of all Internet-facing systems.

Tools-based vulnerability scan and manual verification: To provide a high quality of service, we combine the two methods of a tools-based vulnerability scan and bespoke manual verification to ensure all identified issues are fully investigated and false positives are eliminated.

Comprehensive service: Every service exposed to the Internet will be located and tested for known vulnerabilities, configuration errors, missing patches, out-of-date software, default passwords, guessable passwords and many other issues.

Advanced testing: Using our world-class penetration testing toolsets and exploit frameworks, we can thoroughly test systems against the latest known threats and weaknesses to identify, and where in-scope, exploit both known and unknown vulnerabilities including tests for vulnerabilities before a vendor has released a patch. This allows us to test whether an in-depth approach has been adopted to ensure other protections are in place.

Stage 2
Next steps

We conduct network level testing to identify vulnerabilities in router filtering, firewall filtering, OS and server application software flaws, configuration errors, web servers, web applications, and mail services. Potentially exploitable vulnerabilities will be discussed and exploited if agreed to verify their extent. Our own testing tools and scripts enable efficient testing of many hosts while maintaining high standards and minimising costs.
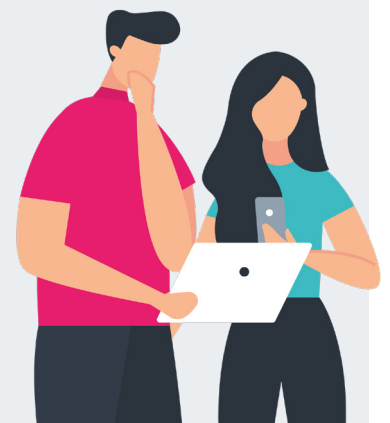
Datacentre Modernisation
Data & Cyber Security
Managed Services
IT Transformation

Stage 3
Reporting

The formal report on 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.

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. Due to the volume of issues usually found, this does not include issues discovered during automated testing.

Outcomes & Benefits

Our external health check delivers the following outcomes:

· Provides a thorough examination and test of the Internet-facing infrastructure.

· Details issues that comprise a threat to the integrity of the company infrastructure.

· Outlines where elements of the network are configured correctly and securely.

· Provides peace of mind by discovering vulnerabilities and outlining how they can be addressed.

Deliverables

The external health check service provides:

· A formal report that presents an overview of the Internet-facing infrastructure and what needs to be done.

· 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 defences to other parts of the business.

· An outline of your path to a more secure environment.

Reports are delivered after the completion of all testing. We will endeavour to release reports as soon as possible and fast track them where critical deadlines need to be met, provided notice is given prior to starting the work.

Why MTI?

MTI is a lifelong member of global cyber security body, CREST, and has been conducting penetration testing on Internet-facing infrastructure for 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 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.

The British Council chose MTI because of its extensive resources and unique experience in the provision of penetration testing services to public sector bodies, it's financial backing and ability to flex and scale operations to meet changing needs across the Council's extensive web estate, and the quality and cost-effectiveness of the solution offered.

"We needed a provider that could meet our volume of demand. We have over 300 web sites, apps and portals, in over 10 countries, each running in it's own silo, in local initiatives, collecting personal information. MTI is that provider."

Ian Livingstone
Cyber Security Manager
The British Council