PSN IT Healthcheck

mti
A RICOH Company

Securing IT infrastructure from external and internal threats is imperative for public sector organisations that hold and share large amounts of confidential and restricted information.

To share information and services in a secure and reliable manner on the UK government's Public Services Network (PSN), public sector organisations need to meet a strict set of security standards and be certified as compliant by an approved PSN IT Health Check (ITHC) provider.

The Service

Our service incorporates testing of all areas of exposure within your organisation: external, internal, and cloud-based.

MTI consultants can assess all parts of the existing IT infrastructure to help you understand the level of risk from the technologies and systems in use.

We provide an overview of your network and evidence of the vulnerabilities and weaknesses that need to be addressed. Our report includes remediation recommendations and outlines a path to secure your environment.

Outcomes & Benefits

The 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 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.

Stage 1
What we test:
External Network

External network penetration testing: to determine the flaws and risks exposed through your Internet Gateway we conduct a manual penetration test to provide a complete picture of all Internet-facing systems.

We use a combination of tools-based vulnerability scan and manual testing to investigate all identified issues and eliminate false positives. We locate and test all Internet-facing systems for vulnerabilities, configuration errors, out-of-date software, weak passwords, and other issues. We use penetration testing toolsets and exploit frameworks to identify both known and unknown vulnerabilities.

Stage 2
What we test:
Internal Network

- **Internal network penetration testing**
- **Domain compromise assessment**
- **Operating system hardening build review**
- **Password reviews**
- **PSN segregation test**
- **PSN-P segregation test (PSN-P Only)**
- **Wireless infrastructure assessment**
- **PSN firewall ruleset review**
- **Automated firewall configuration review**
- **VPN review**
- **Mobile device reviews**

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

Datacentre Modernisation
Data & Cyber Security
Managed Services
IT Transformation

Stage 3
Reporting

The results of the testing phases will be presented in a formal report including the following information:

· A stated objective or aim for the Security Assessment

· The Scope of the Security Assessment as agreed with the customer

· Executive Non-Technical Summary of Findings

· Executive Technical Summary of Findings

· Details of findings

· Grading of risks from High to Low severity (including a marker to show ease of exploitation)

· CVSS Scoring

· Description of Vulnerabilities discovered

· Recommendations to address each vulnerability

· Contact details of the Customer Contact and assigned test team

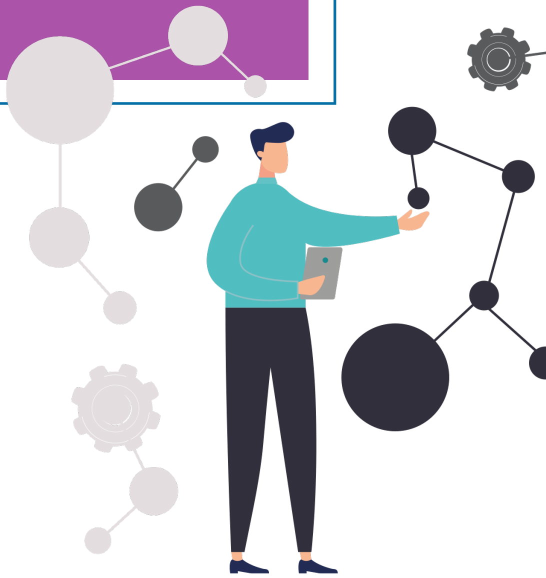
· Details of CHECK/CREST/Cyber Scheme consultants' certifications

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.

Deliverables

The health check service provides:

- A formal report detailing all issues found, identifying the severity and exploitability of each condition with severity ratings based on CVSS scoring.
- A report, submitted to NCSC, to support access to the PSN networks via the Code of Connection.
- An action plan that sets out the recommended remediation steps and details the stages that help you track your remediation progress.
- Summaries of the business and technical risk that make the results accessible to all stakeholders.
- An outline of your path to a more secure environment.



Why MTI?

A longstanding member of global cyber security bodies, CREST and CHECK, MTI has been conducting penetration testing on IT infrastructure for more than 30 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 your organisation and outline remediation measures to counter those risks. Our aim is to provide greater security without sacrificing functionality in any given environment.

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

Datacentre Modernisation
Data & Cyber Security
Managed Services
IT Transformation