Vulnerability Assessment

A RICOH Company

In today's world it is important for organisations to take all effective steps they can to make it harder for cyber-attacks and threats to breach their infrastructure. One area that can be overlooked is the basic housekeeping of ensuring your organisation is up to date with software patches and updates. While this can be one of the simplest things to address, it's also very easy to neglect. But if patches and updates are not up to date, they can provide one of the simplest ways for criminals and malicious actors to gain unauthorised access to your network.

By assessing and addressing those potential vulnerabilities, you can reduce the exposure of your organisation to potential attack. Assessing the condition of deployed devices within your external and internal infrastructure is an integral part of maintaining a secure network and should be the first step towards securing it.

The Service

MTI's Managed Vulnerability Assessment identifies the most vulnerable systems and prolific vulnerabilities on your network as the primary step to securing workstations, servers, routers, switches and more.

The results of our Managed External and Internal Vulnerability Assessment service are reviewed by our skilled CHECK and CREST penetration testing consultants. False positive results are omitted and the additional context of likelihood of exploitation and ease of exploitation is added to the results.

The information provided by the assessment enables your organisation to implement targeted remediation, reducing the overall threat surface and eliminating critical issues in an effective timeframe.

Tracking the remediation progress of vulnerabilities within the network helps the business to understand the mean time a threat will remain a risk within the network prior to its remediation.

Stage 1
Scanning

Our scanning software has the deepest and broadest vulnerability coverage in the industry, with more than 45,000 unique vulnerabilities and over 100,000 test/audit plugins. Scans are conducted and managed remotely from our offices and test over a range of areas, including router filtering, firewall filtering, missing software patches, out of date or unsupported software, and operating system software flaws.

All scans are monitored to ensure they run and complete correctly. Any exceptions or irregularities in scan behaviour or results will be investigated by our team.

Stage 2
Reporting

The results of the testing phases are presented in a formal report that includes the following outputs:

· **Native Tool Report Outputs**

· **MTI Summary Report** - including a Remedial Action Plan highlighting key vulnerabilities and remedial actions. MTI will highlight the number of existing High-Risk vulnerabilities, those that have been fixed since the previous scan and any new ones.

· **Pre-vetted Results** - we suppress superfluous information from the scan outputs and remove known false positive results to enable you to focus on genuine findings.

· **Critical Alerts** - in the event MTI discovers critical vulnerabilities that require immediate attention, we will contact you to provide details of the vulnerabilities, affected hosts and remediation steps.

Reports are delivered within seven working days of completion of each scan.

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

Stage 3
Feedback & progressions

Over the course of the contract, we will provide you with:

Single point of contact: When the contract is awarded, a lead consultant will be allocated as your primary point of contact for service delivery. The consultant will run the scans, review the results, write the summary reports, and lead any debrief calls. This ensures a single primary contact will retain knowledge of your environment and the outcomes of previous scans and issue resolution.

Telephone debrief: After the report has been issued at the end of each vulnerability assessment, the lead tester will conduct a telephone debrief or online meeting with your staff. We will go over the report, answer any questions about the findings or remediation and highlight significant changes since the previous scan.

Quarterly Service Review: The account manager will conduct a quarterly service review to assess your experience of the service and provide feedback to our delivery team on any improvements required and requests for change.

Outcomes & Benefits

Our Managed Vulnerability Assessment:

- Identifies vulnerabilities that exist in the network and reveals gaps in your patching/update regime.
- Shows you where you can improve your patching/ update regime.
- Gives you the information to implement targeted remediation, reduce the overall threat surface and eliminate critical issues in an effective timeframe.
- Tracks remediation progress of vulnerabilities.
- Provides peace of mind by discovering vulnerabilities and outlining how they can be remediated.

Deliverables

The Managed Vulnerability Assessment provides:

· A full and detailed report documenting the findings within seven days of the scan.

· A summary report highlighting key vulnerabilities and remedial actions.

· Critical alerts detailing critical vulnerabilities that require immediate attention.

· Quarterly service review assessing your experience of the service, any improvements required and requests for change.

Why MTI?

A longstanding member of global cyber security bodies, CREST and CHECK, MTI has the security expertise and experience to help you deal with a wide-ranging number of threats and attacks. As one of the first companies to provide vulnerability assessment services, 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.

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

Datacentre Modernisation
Data & Cyber Security
Managed Services
IT Transformation