Cloud Health Check

While cloud service adoption has surged in the past few years, many organisations have been unaware of the security shortfalls in their cloud platforms and services. People have assumed that services provided on cloud platforms are “secure by default”. Unfortunately, this is not the case.

There are many areas where configuration or design errors could permit unintended access into the environment, expose sensitive data without proper security controls, or increase the likelihood of low-complexity attacks against the infrastructure succeeding. Our service gives you a much clearer view of how secure your cloud services are and what you can do to improve them.

The Service

We have built on our long-standing experience in traditional penetration testing to incorporate the adoption of cloud-based services and platforms. We have combined our experience gained during the growth of cloud with the services, testing methodologies and tooling used to assess cloud platforms. This enables us to evaluate cloud provider platforms and configurations to determine where issues or insecure configurations may exist.

Stage 1: The Tests

AWS tenancy review: configuration review of your AWS environment using a combination of automated and manual tools to ensure configuration is in line with AWS guidelines and security best practice.

Azure tenancy review: security configuration review of a single Azure tenancy against Microsoft guidelines and Security Best Practice using a combination of automated and manual tools.

Office 365 tenancy review: Security Review of the customer‘s Microsoft Office 365 Tenancy against the CIS Microsoft 365 Foundations Benchmark v1.3.0 at level 2 covering key areas such as Azure Active Directory, application permissions and data management.

Stage 2: What we test

Our AWS review will examine a number of key areas (as appropriate), including Amazon Machine Image (AMI) configuration, AMI Build review process, Key strength, Key rotation, AWS Root user account access, Account segregation and Access controls to buckets and objects.

- Azure tenancy review
- Office 365 tenancy review

Among the areas examined are:

- Confirm correct administration rights have been granted to Office 365 portal users, with segregation between functions and duties applied.
- Review Active Directory Connect/Synchronisation configuration.
- Review External Sharing Policies.
- Review Exchange Online Protection (EOP) configuration

Stage 3: Reporting

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

- 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.
- 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 CHECK/CREST team consultants.
- Benchmark Spreadsheet detailing adherence to common controls against the CIS framework.

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

Vulnerability Register

To aid with remediation and compliance tracking, an Excel based Vulnerability Register will be provided that lists 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 found during automated testing.

Outcomes & Benefits:

Our cloud health check delivers the following outcomes:

- Provides a thorough examination and test of cloud platforms and configurations.
- Details issues that comprise a threat to the integrity of cloud platforms and configurations.
- Outlines where elements of cloud platforms and configurations are configured correctly and securely.
- Provides peace of mind by discovering vulnerabilities and outlining how they can be addressed.
- Any critical issues or immediate threats will be communicated to you in real time, allowing for the earliest triage and remediation.

Deliverables of the service

- The cloud health check service provides:
- A formal report that presents an overview of cloud platforms and configurations 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.

Report delivery

- Reports are delivered typically within 10 working days after completion of all testing.
- After completion of the testing work, each report is independently reviewed by a member of the technical team to assess technical accuracy and readability of the report. The window of release allows for time in the schedule to conduct this review, conduct additional checks and agree suitable changes where required.
- The reports are then sent to you electronically as a PDF file, PGP encrypted during transit over and encrypted channel, both protected with a suitable passphrase..

Why MTI?

MTI is a lifelong member of global cyber security body, CREST, and has been conducting penetration testing for over 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. We have been able to take this expertise and extend it to cloud infrastructure, 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.

> **"Engaging and working with MTI performing our recurring penetration testing was a very smooth experience. The team quickly understood our specific needs, the technical environment, and any specific test scenarios we requested. Good feedback from the consultants during the actual penetration test and a very professional report with vulnerabilities in order of priority and suggested corrective measures. All in all a job well done."**
>
> Michael Zetterlund, Chief Product Officer, Ariane Systems

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

Datacentre Modernisation
Data & Cyber Security
Managed Services
IT Transformation