Cloud Security Assessment

autodata

Auditing your AWS/Azure/O365 instances to identify misconfigurations and best practices for remediation

CREST

CHECK
IT Health Check Service

Our Cloud Security Assessment audits your AWS, Azure and Office 365 instances to identify misconfigurations and secure configurations from a 'Blue Team' perspective, allowing you to remediate the vulnerabilities before they are exploited.

Cloud infrastructures vary in size, complexity, technologies and in approaches to configuration, so our exact technical approach to each infrastructure may be very different. However, there are certain fundamental areas that are routinely examined:

Cloud Security Risks

Due to the rapid rate of cloud adoption, companies end up facing cyber risks new and old that can compromise their cloud platforms and any on-premise infrastructures with hybrid cloud setups.

Assessment Benefits

- Understand the security issues existing within your cloud network
- Assure your infrastructure and cloud services are secure enough to withstand cloud-based attacks
- Establish sufficient logging and controls to mitigate such attacks
- Focus your departmental efforts on the high-risk items identified in the report
- Achieve regulatory compliance by evidencing that professional testing has been performed on your cloud infrastructure

Open-Source Intelligence (OSINT)

The Cloud Security Assessment has a strong focus on publicly available information that could be leveraged in targeted attacks. Information such as links to cloud resources, document metadata, email addresses and leaked credentials are all gathered to identify common and applicable attacks from unauthenticated attackers.

AWS/Azure Configuration Review

The configurations of AWS/Azure environments and all encased services are systematically investigated to establish a secure baseline that conforms with best practices. This assessment will cover all entities based in your environment to highlight misconfigurations and bad practices and establish a secure environment which is resilient to modern cyber-attacks.

We understand that there are requirements and external factors that need to be satisfied – the consultant will take these into consideration when completing the post assessment report.

Office 365 Configuration Review

Office 365 and all connected apps, both first and third-party are reviewed to identify various issues. This can include (but is not limited to) application misconfigurations, weak security configurations and 'low-hanging fruit' issues that could be utilised by an attacker to escalate their access or access sensitive information.

The testing is performed remotely from our office and data-centre locations using credentials to your AWS, Azure and Office 365 Portals.

256-260 Old Street, London, EC1V 9DD
t. +44 (0) 20 7749 7949 | e. sales@autodata.co.uk