Datasheet

Public Cloud Cyber Security Services

Security Posture Assessment & Host Vulnerability Assessment

Introduction

Today's organisations desire the accessibility and flexibility of the cloud, yet these benefits ultimately mean little if you're not operating securely. One misconfigured server and your company may be looking at financial or reputational damage that takes years to overcome.

Fortunately, there is no reason why cloud computing cannot be done securely. You need to recognise the most critical cloud security challenges and develop a strategy to minimise these risks. By doing so, you can get ahead of problems before they start, and help ensure that your security posture is strong enough to keep your core assets safe in any environment.

Security Posture Assessment

During a cloud security assessment, we evaluate your cloud security posture based on industry best practices. We have developed a unique cloud security framework covering critical risk and security controls based on the Centre for Internet Security (CIS) benchmarks for AWS and Azure, and our own operational experiences to help you create and ensure a secure cloud environment. LGA's internal systems deployed on public cloud infrastructure rigorously apply the same benchmarks.

The Security Posture Assessment is prescriptive guidance for establishing a secure baseline configuration when deploying public cloud services. Assessments are tested against listed Azure or AWS services. The scope of this assessment is to establish the foundation level of security for anyone adopting Microsoft Azure Cloud or Amazon AWS Cloud. The assessment is, however, not an exhaustive list of all possible security configurations and architecture. Customers typically use the assessment as a starting point and then follow up to do the required site-specific tailoring wherever needed and when it is prudent to do so.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined.

Automated: Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state.

Manual: Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected.

Benefits

- Provide a clear set of standards for configuring common digital assets - everything from operating systems to cloud infrastructure
- No need to 'reinvent the wheel'
- Clear path to minimise organisation's attack surface
- Build and maintain a security profile in line with industry best practice
- Eliminate configuration settings that are known to be insecure
- Protect the organisation from known threats
- Offload unnecessary cyber risk by narrowing the attack surface
- Protect organisation against financial hardship, as non-compliance can lead to costly fines - particularly in the event of a breach

Public Cloud Cyber Security Services

Areas of Recommendation

Identity and Access Management: Covers security recommendations to follow to set identity and access management policies. Identity and Access Management policies are the first step towards a defense-in-depth approach to securing a cloud platform environment.

Security Centre: Covers security recommendations to follow when setting various security policies (for Azure only).

Storage Accounts: Covers security recommendations to follow to set storage account policies on a cloud subscription. A cloud storage account provides a unique namespace to store and access cloud storage data objects.

Database Services: Covers security recommendations to follow to set general database services policies.

Logging and Monitoring: Covers security recommendations to follow to set logging and monitoring policies.

Networks: Covers security recommendations to follow in order to set networking policies in a cloud environment.

Virtual Machines: Covers security recommendations to follow in order to set virtual machine policies.

Other Security Considerations: Covers security recommendations to follow in order to set general security and operational controls e.g. management controls around keys, secrets, resource locks, key vault, RBAC, etc.

Application Services: Covers security recommendations for application services.

Cloud Host Vulnerability Assessment:

A vulnerability assessment is a systematic review of security weaknesses in an information system. It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed. In a cloud host vulnerability assessment, tools are used to check cloud VM servers, which may be vulnerable to attacks if not adequately tested or not generated from a tested machine image.

Areas of Recommendation

Identity and Access Management: Covers security recommendations that to follow to set identity and access management policies. Identity and Access Management policies are the first step towards a defense-in-depth approach to securing a cloud platform environment.

System Baseline Definition: Gather information about the systems before the vulnerability assessment e.g. what are the approved vendor software, versions, processes, drivers for each target device.

Vulnerability Scanning: Understand the business, and know the appropriate time to activate each scan. Collect the results.

Vulnerability Assessment Report: Reporting and recommendations based on the initial assessment goals.

Contact Us

LGA Telecom Pte Ltd

22 Sin Ming Lane
#04-72 Midview City
Singapore 573969

Tel: (65) 6892 2308
Email: sales@lgatelecom.net
Website: www.lgatelecom.net