FORTIS CYBER®

CREST SECURITY TESTING Vulnerability Assessment

CREST SECURITY TESTING Penetration Testing

Cloud Security Review

The aim of a Cloud Security Review is to identify potential security gaps or weaknesses within the cloud environment that could be exploited by threat actors and develop recommendations for mitigating these risks. This proactive approach helps organisations ensure that their cloud deployments are secure, compliant, and resilient against cyber-attacks.

There are variations in specific features, services, and configurations offered by different cloud service providers including AWS, Microsoft Azure, and Google Cloud Platform (GCP); however, the Fortis Cyber® testing methodology aligns to the industry standard CIS Benchmarks and the fundamental principles of cloud security apply across all providers.

What are the benefits?

A Cloud Security Review is an essential component of maintaining a robust security posture in the cloud and offers numerous benefits for organisations leveraging cloud services including:

- Identify security vulnerabilities & gaps in the cloud environment before attackers & optimise security controls
- Improve risk management to protect against data breaches, service disruptions, & compliance violations
- Maintain compliance with industry regulations & standards e.g. GDPR, HIPAA and avoid financial penalties
- Enhance incident response capability to detect, respond to, and mitigate security incidents
- Build customer and stakeholder trust by demonstrating a proactive approach to cloud security
- Support business continuity by reducing the likelihood of service disruptions, downtime, or data loss
- Enhance data protection to ensure information is protected from unauthorised access & attacks

Cloud Security Overview

The Fortis Cyber® Cloud Security Review covers both infrastructure, which takes a broad view of the entire cloud architecture and its security foundations; and configuration, which zeroes in on specific settings and configurations within the cloud environment.

Infrastructure

- Involves a broad assessment of the overall architecture and design of the cloud infrastructure to identify security weaknesses or gaps in the underlying infrastructure components.
- Examines the design and implementation of foundational elements such as network architecture, identity and access management (IAM), data storage and management, disaster recovery, resilience, and compliance frameworks.
- Focuses on evaluating the effectiveness of security controls and measures implemented at the infrastructure level to protect against various threats and risks, including malicious attacks, data breaches, and system failures.
- Assesses the integration of security technologies and solutions, such as firewalls, intrusion detection systems, encryption mechanisms, and security monitoring tools into the cloud infrastructure.

Configuration

- Focuses on evaluating the configuration settings of various cloud services and resources to ensure they align with security best practices, compliance requirements, and organisational policies.
- Involves examining settings such as access controls, encryption configurations, network configurations, authentication mechanisms, logging and monitoring configurations, and any other relevant configurations within the cloud environment.
- Identifies misconfigurations or vulnerabilities that could potentially expose the cloud infrastructure to security risks, such as unauthorised access, data breaches, or service disruptions.

Engagement Methodology

The Fortis Cyber® testing methodology follows recognised best practice and as such is aligned to the industry standard CIS Benchmarks which include the following key areas:

- **Identity and Access Management** - ensure Multiple Factor Authentication (MFA) for high privileged accounts; ensure Identity Access Management (IAM) is enforced; review password and security policies for IAM users; ensure sustained access to the management portal is available.
- **Logging and Monitoring Configurations** - ensure logging and reporting is enforced; ensure the logging and reporting is accessible and not available to the public; assign security and retention policies to activity logs.
- **Virtual Networking Security Settings** - ensure network security policies are enforced; review public and privileged access to key services.
- **Virtual Machine Instance Settings** - ensure system and application updates are performed regularly; ensure endpoint protection is enforced where applicable; review the disk encryption policy.
- **Storage Security Configuration** - review storage accounts that allow insecure connections; review storage accounts that allow unrestricted access; review storage accounts that do not allow trusted services.
- **Database Services Settings** - ensure auditing is performed against the database services; ensure the database servers are configured for encryption ; review the security settings of the database nodes.
- **Kubernetes Engine Configuration** - ensure that key vault objects are recoverable in case of accidental deletion; ensure role-based access is managed within the Kubernetes cluster; review the security settings of the Kubernetes cluster.
- **Built-in Security Applications** - ensure security centre is functional; ensure security policies to assist in monitoring and reporting; ensure vulnerability management to Virtual Machines where applicable.

Fortis Cyber® CREST Accreditation

Fortis Cyber is a CREST accredited organisation for both Penetration Testing and Vulnerability Assessments. Through CREST's demanding accreditation process, organisations buying security testing services get the assurance that:

CREST SECURITY TESTING — Penetration Testing

CREST SECURITY TESTING — Vulnerability Assessment

- The services will be delivered by trusted companies with best practice policies and procedures.
- The work will be conducted by highly qualified individuals with up-to-date knowledge, skills, and competence to deal with all the latest vulnerabilities and techniques used by real attackers.
- Both the company assessments and individual qualifications are underpinned by meaningful and enforceable codes of conduct.

For more information or to arrange a call with our team to discuss how Fortis Cyber® can support your organisation with penetration testing and security assessments visit our website www.fortiscyber.co.uk or email enquiries@fortiscyber.co.uk