InfoSight®
www.infosightinc.com

CLOUD SECURITY ASSESSMENTS

305-828-1003 info@infosightinc.com

Overview

Cloud security is critically important for several reasons, as it plays a pivotal role in safeguarding an organization's data, applications, and infrastructure when using cloud computing services. Cloud security presents several challenges to protecting data, because although cloud providers have robust security measures, misconfigurations or weak access controls can be exploited by bad actors. And the proliferation of cloud services and resources can lead to "cloud sprawl", making it even more challenging to track and secure all assets effectively.

The Challenge

Companies using cloud services like Azure, AWS, and Google Cloud face a variety of security challenges. These challenges stem from the shared responsibility model of cloud computing, where the cloud provider and the cloud user both have roles to play in ensuring security. Common challenges include Data Security, Identity and Access Management, Regulatory Compliance, APIs Vulnerabilities, Insider Threats and Cyberattacks. Cloud environments are shared responsibility models where security configurations remain the customer's responsibility.

The Outcome

By completing a comprehensive cloud security assessment, your organization will significantly enhance the security of your cloud environment, ensuring it aligns with globally recognized best practices. The assessment serves as a testament to your organization's dedication to protecting clients' data and maintaining their trust. Your assessment is more than a technical achievement - it's a principal part of your organization's promise to deliver secure and reliable services to your clients.

After testing is complete, Digital reports are delivered via our proprietary **Mitigator Vulnerability and Threat Management Platform.** Reports can be exported in multiple formats and printed.

MITIGATOR™
VULNERABILITY & THREAT MANAGER

Bringing the Future into Focus

www.infosightinc.com

Other Assessments

Vulnerability & Penetration Testing

Consists of a multi-disciplinary, multi-faceted review of the organization's systems which identifies vulnerabilities outside and inside the network and attempts to exploit any vulnerabilities in the same way a malicious actor would.

Red Team/Blue Team Testing

Designed to test an organization's readiness to detect, withstand and respond to a targeted attack. The red team's goal is to find and exploit any identifiable weaknesses in the organization's security as the blue team works to defend the organization by finding and patching vulnerabilities and responding to successful breaches

Code Review, Mobile & API Testing

Involves the security testing of web, mobile, and software application interfaces to identify privilege escalation, authorization creep, and security controls bypass. It includes a detailed report outlining discovered vulnerabilities and remediation steps.

Social Engineering

Encompasses comprehensive security tests conducted to establish the current state of security among the organization's personnel. It identifies vulnerabilities within human resources as well as gaps in awareness training. Social Engineering assessments are performed against electronic messaging, telephony and other onsite and human vectors.

How We Solve It

Our cloud security assessment follows the CIS (Center for Internet Security) Benchmark which involves a comprehensive review of an organization's adherence to a set of best practices for securing cloud environments. The CIS Benchmarks are globally recognized as standard guidelines for securing IT systems and data against cyber threats.

Key steps and considerations in conducting a cloud security assessment include:

Understanding the Cloud Environment: Before the assessment, it's crucial to understand the specifics of the cloud environment being used, such as AWS, Azure, or Google Cloud Platform. Each platform has its unique configurations and security settings.

Familiarization with CIS Benchmarks: Review the CIS Benchmarks relevant to the specific cloud services in use. These benchmarks provide detailed security configuration guidelines for a variety of technologies.

Scope of Assessment: Define the scope of the assessment. This includes identifying the cloud resources, services, and data that will be evaluated.

Review of Identity and Access Management (IAM): Assess the policies and practices around user identities and access permissions. Ensure principles of least privilege and role-based access control are properly implemented.

Data Security Analysis: Evaluate data storage and transfer mechanisms to ensure that data is encrypted both at rest and in transit. Check for secure data backup and recovery processes.

Network Security and Firewall Configuration: Analyze network configurations, including firewalls, security groups, and subnets to ensure only necessary ports and protocols are allowed and properly secured.

Logging and Monitoring: Ensure that logging is enabled for all important events and that there is a robust system in place for monitoring and responding to security incidents.

Compliance with CIS Benchmark Controls: Compare the current state of the cloud environment against the CIS Benchmark controls. Identify areas of non-compliance or potential improvement.

Benchmark Reporting: Document findings, compare them against the CIS benchmarks, and prepare a detailed report outlining the level of compliance and areas for improvement.

Action Plan for Remediation: Develop a prioritized action plan to address any identified gaps or vulnerabilities in line with the CIS Benchmark recommendations.

Continuous Review and Improvement: Cloud security is an ongoing process. Regular assessments and updates to the security posture should be made in accordance with changes in the CIS Benchmarks and the evolving cloud environment.