Introduction Cloud Security Assessment

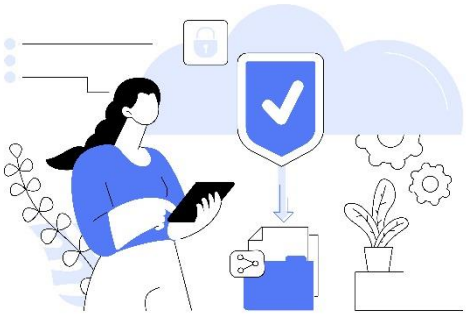
When it comes to the cloud, a cloud security assessment is critical to bringing Security First. Every year, hundreds of data leaks are reported as a result of improperly designed clouds. This can put the company in an awkward situation, resulting in long-term reputational harm and substantial financial loss.

Our Cloud security team at Infopercept will assess the cloud security posture using industry standards. We perform interviews with application stakeholders (market analysts, developers, program and product managers, and so on) as part of a Cloud VAPT and Configuration Review to clarify the application's business background and security requirements. Following that, we assess the tool analysis of your cloud environment.

Traditional Infrastructure vs Aws Pentesting:

Cloud security infrastructure and traditional security infrastructure vary in a number of ways. The technology stacks could not be more different, from setup and configuration to identity and user permissions.

The most important distinction is the control of the systems, which means that a cloud service provider (AWS, Assure, GCP, etc.) must obtain statutory approval for penetration testing, which must be performed on predetermined dates. The aim of this policy is to prevent attacks of "ethical hacking" that would breach reasonable usage policies because the testing is affecting their own infrastructure (and may provoke incident response actions by the cloud provider team). We maintain a comprehensive and secure security evaluation by making these testing windows clear.



Methodology

- Determining cloud misconfigurations and security vulnerabilities
- Conducting a cloud security review to record existing security controls and analyze current framework and cloud technology strengths and weaknesses
- We evaluate the security framework's maturity level using the most up-to-date criteria and methods.
- We ensure that we address all of the business cases posed during the cloud infrastructure assessment.
- Examine the efficacy of existing initiatives and their compatibility with long-term company objectives.
- Identifies existing system flaws that can threaten cloud security and recommends solutions to close the gaps.

Assessment Details

Governance, Risk and Compliance

- Cloud policies and standards
- Cloud governance and services
- Vulnerability management
- Threat risk assessments
- Regulatory compliance requirements

Security Architecture and Networking

- Network segmentation and on-premise integration
- Cloud architecture and security controls
- Disaster recovery
- Remote system connectivity and management
- Containers, configurations and security control

Infopercept follows testing checklist for

- Kubernetes
- AWS
- Azure
- GCP
- Docker Containers

Cloud Security Strategies

- Security Audit of cloud Environment
- Configuration Review of Cloud Infrastructure
- Manual Methodology of testing
- Testing APIs and microservices
- Testing the communication Channel

Identity and Access Management

- Identity management
- Cloud authentication infrastructure, including on-premise connectivity (e.g., ADFS)
- Role-based access controls
- Privilege access management

Secrets and Data Protection

- Encryption
- Database security
- Certificates and keys management
- Data protection and loss prevention

DevOps

- System and application deployment
- Pipeline configurations
- Code repository security controls
- Secure software development life cycle

Threat Detection and Response

- Security logging and centralization
- System, database, and application logging
- Cloud incident response processes
- Endpoint and network security controls

About Infopercept - Infopercept is one of the fastest-growing comprehensive cybersecurity companies in India, serving global clients. It provides platform led managed security services that covers all areas of cybersecurity, including defensive, offensive, detection and response, and security compliance. Infopercept has its own cybersecurity platform, 'Invinsense,' which integrates tools such as SIEM, SOAR, EDR, deception, offensive security, and compliance tools. Its cybersecurity and MDR services include dedicated teams of experts, ensuring that organizations have 24x7 cybersecurity operations support.

Imprint

Publisher

3rd floor, Optionz Complex, CG Rd, Opp. Regenta Hotel, Navrangpura, Ahmedabad, Gujarat 380009, INDIA

Contact

sos@infopercept.com
www.infopercept.com/knowledge/datasheets