SECURITY INNOVATION
A BUREAU VERITAS COMPANY

Top 5 Cloud Misconfigurations

Cloud Storage Exposed

Misconfigured cloud storage services (e.g. S3 buckets, Azure blob etc.) that store sensitive information if exposed publicly, either inadvertently or due to incorrect permissions, could allow an attacker to gain access to sensitive information present on the storage e.g. credentials, logs, backup files etc

Overly Permissive IAM Roles and Permissions

Identity and Access Management (IAM) roles and policies that grant excessive permissions can allow an attacker to escalate privileges, move laterally within the cloud infrastructure, or provide access to sensitive resources which they are not authorized to.

Lack of Logging and Monitoring

Cloud environments missing proper logging and monitoring configurations, for critical devices could lead to lack of visibility into potentially threats or misuse.
This makes it much more difficult to detect attacks or anomalous behavior within the network.

Unrestricted Inbound/Outbound Security Groups

Misconfigured security groups, network ACLs or firewall rules that allow unrestricted access to cloud resources such as databases, containers etc. This could allow an attacker to remotely exploit services or launch variety of attacks to exfiltrate data.

Default Credentials or Weak Passwords

Use of default credentials or weak passwords for cloud services, virtual machines or databases. The attackers can easily gain unauthorized access to resources by performing brute-force attacks or using default credentials for services like databases, storage or VMs.