Cloud Scan Methodology

Our Cloud Scanning service employs human-guided, semi-automated tools to assess the cloud environment using a user account with read-only access to all cloud resources. The output of this service would assist administrators in securing their cloud infrastructure in compliance with industry-leading security standards. Below is the methodology that is used for a comprehensive cloud security review: -

Cloud Resources - Profiling and Attack Surface Identification

Using the provided user account, the first step is profiling the environment. All resources are identified along with their detailed configurations using various cloud CLI tools, open-source tools, and proprietary scripts. Based on the collected configurations, relationships among cloud components, public exposure, and broadly scoped policies are determined. The aggregation of this information defines the attack surface of the cloud infrastructure.

Cloud Configuration & Controls Analysis

Based on configuration data and attack surface identification, each resource configuration is validated against known insecure practices. The access control and permissions of each component, user, role, and policy are scrutinized, and broad-scoped policies and roles are flagged as impersonation risks for accessing critical assets. Key cloud security measures such as logging, audit settings, firewalls, and incident response setups are also analyzed.

Security Control and Test Cases

Based on profiling, attack surface analysis, and configuration review, a comprehensive set of test cases and required security controls is developed for the application and cloud infrastructure.

Sample security categories include:

- Multi-factor Authentication (MFA)
- Role-based Access Control (RBAC)
- Data Protection (SSL/TLS, Encryption, Backup)
- Configuration Security
- Overly Permissive IAM Policies
- Insecure S3 Bucket/Azure Blob/GCP Permissions
- Improper Vault Usage (Secrets, Environment Variables)
- Insufficient Logging
- Alert Monitoring & Incident Response

Vulnerability Assessment

contactus@blueinfy.net

This phase involves identifying potential weaknesses in the cloud configuration with the combination of automated scans and manual verification techniques. Human intelligence plays a key role in validating results and eliminating false positives.

Mitigation Strategies

Based on the identified vulnerabilities and associated risks, a comprehensive set of mitigation strategies is proposed. These strategies prioritize addressing critical issues while following industry best practices and aligning with the customer's operational requirements.

Actionable Report with Zero False Positives

A key deliverable of the assessment is a highly actionable, well-structured report designed to drive immediate remediation. The report is curated to maintain zero false positives and includes the following critical components: -

- Vulnerability Descriptions: Detailed information about each identified issue
- Risk Ratings: Categorization of vulnerabilities by severity and potential business impact
- Evidence: Screenshots, logs, and step-by-step reproduction guides for validation
- Exploitation Evidence: Details of successful exploit scenarios (if required)
- Mitigation Strategies: Practical recommendations to address vulnerabilities and improve the overall security posture
- Report Walkthrough: Guidance for stakeholders and support in implementing remediation measures

Tools and Utilities

Blueinfy uses a combination of proprietary and open-source and licensed tools during the review. This includes utilities for reviewing configuration, vulnerability scanning, exploitation, and custom scripts to identify complex vulnerabilities effectively.

