Simulated AWS Security Review

This document presents a simulated review of an AWS environment's security posture based on mock data and settings. The review focused on key security areas to identify potential vulnerabilities.

Review Overview

Using a mock AWS environment and documentation, a security review was conducted to assess the following aspects:

- IAM (Identity and Access Management) group and policy setup.
- MFA (Multi-Factor Authentication) enforcement settings.
- Logging and CloudTrail status.
- Classification and access labeling of S3 buckets.

Findings

IAM Group and Policy Setup

The IAM configuration was examined to assess the organization of users into groups and the associated policies.

Item Type	Name	Status
User	user1	Active
User	user2	Active
User	adminUser	Active
Group	developers	Active
Group	admins	Active
Group	testGroup	Inactive

Note: The "admins" group is identified as having administrative privileges.

Policy Details

An example of an inline policy for a user was reviewed.

Policy Type: Inline Policy

Policy Name: ExampleAdminPolicy

Policy Document:{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Action": "*",

"Resource": "*"

}

```
  ]

}
```

Note: This policy grants full administrative access, which is a high privilege concern.

MFA Enforcement Settings

MFA enforcement was checked to ensure all users, especially those with high privileges, are protected with multi-factor authentication.

Security Warning: MFA is not enabled for at least one high privilege user. Review user MFA settings immediately.

Logging and CloudTrail Status

The status of logging and CloudTrail was examined to ensure adequate tracking of activities within the AWS environment. This is critical for auditing and incident response.

Further details on the specific logging status would be added here if available.

S3 Bucket Classification or Access Labeling

A review of S3 buckets was performed to determine if data classification policies or access labels were in place.

Cloud Data Classification Policy (AWS)

Purpose: To ensure sensitive data in cloud storage is appropriately labeled and protected.

Policy:

- All data stored in AWS S3 must be classified as Public, Internal, or Confidential.
- S3 bucket policies must reflect access rules for each classification.
- Encryption is required for all Confidential data.

- Bucket names must include classification tags (e.g., finance-confidential-2025).
- Monthly audits will be conducted via AWS Config rules.

Owner: Cloud Compliance Manager

Approved: 5/30/25

Conclusion

Based on this simulated security review, several key areas require attention, including MFA enforcement for all high privilege users, a thorough review of IAM policies granting full administrative access, and confirmation of adequate logging via CloudTrail. The data classification policy for S3 buckets is a positive step, but adherence and implementation should be closely monitored.