AWS CHECKS Security and Compliance Report

IAM pillar

1. Topic: Governance procedures for access rights, identity & privileges

Requirement:

Mapping and grouping of business roles with IT roles

Need to Achieve:

Need to check that all users belong to a group, and policies are assigned to the group.

Result of the Script:
Summary: (-) All users belong to a group, but not all groups have policies.
Users Without Groups: All users belong to a group.
Groups Without Policies: ['Test']

2. Topic: Governance procedures for access rights, identity & privileges

Requirement:

Rules for granting and revoking access

Need to Achieve:

Need to check IAM access analyzer is enabled.

Result of the Script: Status: ['Analyzer: Test2, Status: ACTIVE']

3. Topic: Governance procedures for access rights, identity & privileges

Requirement:

Strict enforcement of access policies across infrastructure components

Need to Achieve:

Enabling IAM Group and assigning roles in the Group.

Result of the Script: Summary: (-) All users are in groups, but not all groups have policies. Users Without Groups: All users are in groups. Groups Without Policies: ['Test']

4. Topic: Governance procedures for access rights, identity & privileges

Requirement:

Correlation between physical and logical access

Need to Achieve:

Need to check every resource having least privilege access.

Result of the Script:

Summary: (-) Policies with wildcard (*) permissions found.

Users with Wildcard Permissions: ['CLI', 'Demo', 'Test1']

Roles with Wildcard Permissions: ['AWS-QuickSetup-StackSet-Local-ExecutionRole']

Groups with Wildcard Permissions: No groups with wildcard permissions.

5. Topic: Governance procedures for access rights, identity & privileges

Requirement:

Role-based access control, Authorization as per security access matrix

Need to Achieve:

User having granular access attached to them. Limited resources-level admin user which need to be listed.

Result of the Script:

Summary: (-) Users with wildcard permissions found.

Users with Granular Access: ['sudha']

Users with Wildcard Permissions: ['CLI', 'Demo', 'Test1']

Admin Users: No admin users found.

6. Topic: Governance procedures for access rights, identity & privileges

Requirement:

Strict control of special privileges ? duration, purpose, monitoring

Need to Achieve:

Need to check Root user is disabled and admin user is limited. The activity should be monitored periodically using IAM access analyzer.

Result of the Script: Root User Status: Root user is disabled. Enabled Access Analyzers: ['Test2'] Disabled Access Analyzers: No disabled analyzers found.

7. Topic: Authentication & authorization for access

Requirement:

Multifactor authentication

Need to Achieve:

Need to check that, every user should have policy enforced to enable MFA.

Result of the Script: Summary: (-) Users without MFA enabled. Users without MFA: ['CLI', 'Demo', 'sudha', 'Test1']

8. Topic: Authentication & authorization for access

Requirement:

Directory services

Need to Achieve:

AWS AD connect can be utilized to connect with the existing AD.

Result of the Script: Summary: (-) No AWS Directory Service directories found. Directories Found: None

9. Topic: Password management

Requirement:

12 character complex, alphanumeric password

Need to Achieve:

All IAM users should have a password policy enforced with the required standards.

Result of the Script: Summary: (-) No password policy is set for the account.

10. Topic: Password management

Requirement:

Strict adherence to password standards

Need to Achieve:

All IAM users should have a password policy enforced with the required standards.

Result of the Script:

Summary: (-) No password policy set for the account.

Non-Compliant Users: []

11. Topic: Credential monitoring

Requirement:

Log generation and retention of all user account related activity

Need to Achieve:

CloudTrail logs should be enabled in the account level.

Result of the Script:

Summary: (+) CloudTrail logging is enabled for: Desmo1, management-events

Trail Logs Status: [{'trail_name': 'Desmo1', 'logging_status': 'Enabled'}, {'trail_name': 'management-events', 'logging_status': 'Enabled'}]

12. Topic: Segregation of duties

Requirement:

Segregation of duties

Need to Achieve:

Need to check that all the users have least privilege access. And IAM Groups are created and policies are attached to groups.

Result of the Script:

Summary: (-) Not all users have least privilege access, but all belong to a group, and not all groups have policies.

Users Not Compliant: [{'user': 'CLI', 'reasons': ['Policy contains wildcard permissions.']}, {'user': 'Demo', 'reasons': ['Policy contains wildcard permissions.']}, {'user': 'Test1', 'reasons': ['Policy contains wildcard permissions.']}]

Groups Without Policies: ['Test']