Cloud Identity & Access Management

This playbook outlines the process for managing identity and access in cloud applications. It aims to ensure the secure operation of cloud services by controlling user access and protecting credentials.

Step 1: **Assessment**

Review current identity and access management (IAM) policies, user roles, permissions, and access controls for your cloud services. Identify any gaps or potential vulnerabilities.

Step 2: **Plan**

Based on the assessment, develop a comprehensive IAM strategy that includes role-based access control, minimum privilege policies, and secure credential management practices.

Step 3: **Roles**

Define clear roles within your organization, aligning them with specific access rights and permissions necessary to perform their functions.

Step 4: **Permissions**

Assign permissions to the defined roles using the principle of least privilege, ensuring users have the minimum level of access required to accomplish their tasks.

Step 5: **Credentials**

Implement stringent credential management policies, including the use of strong passwords, multi-factor authentication (MFA), and periodic credential rotation.

Step 6: **Policies**

Establish IAM policies that enforce user authentication and authorization procedures, ensuring compliance with regulatory standards and organizational security best practices.

Step 7: **Tools**

Select and deploy IAM tools and software solutions that support centralized identity management, single sign-on (SSO), and activity monitoring across your cloud environment.

Step 8: **Training**

Conduct training sessions for employees to understand IAM policies, recognize phishing attempts, and follow secure password practices.

Step 9: **Audit**

Regularly audit IAM processes, user activities, and permission usage to identify and remediate unauthorized access or policy violations.

Step 10: **Update**

Periodically review and update IAM policies and roles to accommodate organizational changes, evolving threats, and new compliance requirements.

General Notes

Compliance

Ensure that IAM policies and controls are compliant with legal, regulatory, and industry-specific requirements.

Incident Response

Develop and test an incident response plan to address IAM-related breaches or security incidents.