Florida International University

Spring 2023 Senior Design Project

Multifactor Authentication Enforcement

Student: John Clifford Hill
Instructor/Faculty: *Masoud Sadjadi*, Florida International University

INTRODUCTION

The purpose of this project is to develop a multifactor authentication (MFA) enforcement tool for AWS accounts to enhance security.
Contributions: Design, implementation, and testing of IAM policies, Lambda, and Cloudwatch

CURRENT SYSTEM

Limitations of the existing system: Users and roles can access AWS resources without using MFA, exposing the account to security risks.
Need for a solution to enforce MFA on all users and roles in the AWS account.

SOLUTION OVERVIEW

MFA enforcement tool developed using IAM policies, Lambda function, CloudWatch events, and SNS notifications.
Tool automatically checks for users and roles without MFA and revokes access for non-compliant users and roles.
Unique features: Customizable MFA settings, real-time notifications, and automated compliance checking.

IMPLEMENTATION

Technologies used: AWS services including IAM, Lambda, CloudWatch, and SNS.
Coding languages: Python for Lambda function.
Configuration and deployment: AWS CloudFormation templates for easy deployment..

PROBLEM STATEMENT

AWS accounts without MFA enforced pose a security risk, including potential unauthorized access, data breaches, and account compromise.

Threat Identification	Risk Rating	Recommended Controls
Unauthorized access to AWS resources due to weak or compromised passwords	High	1. Enforce MFA for all user accounts 2. Implement strong password policies 3. Conduct regular security awareness training for users 4. Implement account lockout policies to prevent brute force attacks
Insider threats from privileged users with unauthorized access	Medium	1. Limit the number of privileged users with access to critical resources 2. Implement just-in-time access control for privileged accounts 3. Monitor and audit privileged user activities for unauthorized actions 4. Enforce MFA for all privileged accounts
Social engineering attacks targeting users to bypass MFA	Medium	1. Implement additional authentication factors beyond MFA, such as biometric or hardware-based authentication 2. Educate users about the risks of social engineering attacks and provide guidelines for safe authentication practices 3. Implement anomaly detection and behavioral analysis tools to detect suspicious activities
Misconfiguration or improper implementation of MFA enforcement tool	Low	1. Follow AWS best practices and documentation for implementing MFA enforcement 2. Regularly review and audit the configuration of the MFA enforcement tool for compliance 3. Implement automated testing and validation of MFA enforcement settings 4. Maintain a backup and recovery plan for the MFA enforcement tool configuration
Service disruptions or failures of AWS services used for MFA	Low	1. Implement redundant and geographically distributed AWS services for MFA 2. Monitor and receive notifications on service health and status using AWS CloudWatch or other monitoring tools 3. Have a documented incident response plan for addressing service disruptions or failures 4. Regularly review AWS service-level agreements (SLAs) and ensure compliance

FIU Engineering & Computing

REFERENCES

The MFA enforcement tool was developed based on AWS documentation and best practices for IAM policies, Lambda functions, CloudWatch events, and SNS notifications.