# Florida International University

*Spring 2023 Senior Design Project*

# Multifactor Authentication Enforcement

**Students:** Daniel Esquijerosa

**Instructor/Faculty:** *Masoud Sadjadi*, Florida International University

## INTRODUCTION

The purpose of this project was to develop a multifactor authentication (MFA) enforcement tool using features and services built into AWS.

Contributions: Design, Implementation, IAM users and roles, MFA policy.

## SOLUTION OVERVIEW

MFA enforcement tool developed using an AWS Lambda function, IAM policies, CloudWatch events, and SNS notifications. The tool automatically checks for users and roles without MFA and revokes access for non-compliant users. It features customizable MFA settings, real-time notifications, and automated compliance checking

## REFERENCES

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

## CURRENT SYSTEM

Before the MFA enforcement tool was implemented, each user could access AWS resources without using MFA, which left those areas vulnerable.

## PROBLEM STATEMENT

The main problem with the system before the tool was that AWS accounts without enforcement of any form of MFA posed a security risk. These risks included the following: unauthorized access to AWS services, data breaches, and compromised accounts.

## RISK ANALYSIS

| Threat Identification | Risk Rating | Recommended Controls |
|---|---|---|
| Unauthorized access due to weak or compromised passwords. | High | 1. Enforce MFA for all user accounts.<br>2. Implement strong password policies.<br>3. Conduct security awareness training for users.<br>4. Implement account lockout policies to prevent brute force attacks. |
| Insider threats from privileged users with unauthorized access. | Medium | 1. Practice separation of concerns.<br>2. Implement just-in-time access control.<br>3. Monitor privileged users for unauthorized actions.<br>4. Enforce MFA for all user accounts. |
| Social engineering attacks targeting users to bypass MFA. | Medium | 1. Implement other forms of authentication.<br>2. Conduct security awareness training for users.<br>3. Implement anomaly detection and behavioral analysis to detect suspicious activities. |
| Misconfiguration or improper implementation of MFA tool. | Low | 1. Follow AWS best practices for MFA enforcement.<br>2. Regularly review and audit MFA tool for compliance.<br>3. Implement automated validation of MFA settings. |
| AWS service disruptions | Low | 1. Implement redundancies for distributed AWS services.<br>2. Monitor service health and status using CloudWatch.<br>3. Prepare a documented incident response plan.<br>4. Regularly review AWS service-level agreements (SLAs) to ensure compliance. |