CloudMapper AWS Security Assessment Summary

# 1. Overview

This report summarizes the findings from the AWS CloudMapper assessment conducted against the EC2 instance and other AWS configurations. It highlights publicly exposed resources, potential security misconfigurations, and provides recommendations to mitigate the associated risks.

# 2. Key Findings

- Publicly Accessible Resources: EC2 instances are accessible from the internet.

- Wide IAM Permissions: Certain IAM users or roles may have excessive privileges (AdministratorAccess).

- Open Security Groups: Security groups with wide open access (0.0.0.0/0) detected on multiple ports including SSH (22), HTTP (80).

- S3 Buckets Review: S3 access not detailed in provided files, but should be reviewed in future assessments.

- CloudSearch Domain Error: Attempted scans reported 'NotAuthorized', indicating potential unused services or misconfigurations.

# 3. Recommendations

- Restrict EC2 access using more specific IP CIDR blocks in security groups.

- Apply least privilege principle to IAM roles and users. Avoid using overly permissive policies like AdministratorAccess.

- Ensure all IAM users use MFA and rotate access keys regularly.

- Audit S3 bucket permissions manually or using other tools like ScoutSuite to ensure they are private by default.

- Review and remove any unused AWS services (like CloudSearch) to minimize attack surface.

- Enable AWS Config, GuardDuty, and CloudTrail for ongoing security monitoring.