EXAMPLE M&A Playbook – Block Public Access for Amazon S3 at account level

BACKGROUND

Warning

If performing this remediation is going to negatively affect your applications or production environment, please contact your security lead.

Definitions

Level of Effort (LOE) – Agile Size: Number of sprints. For example – 2 = two sprints.
Skill Level – Level of skill needed to accomplish the task.
1: Beginner. No AWS experience necessary
2: Intermediate. Understanding of console actions. Some understanding of CloudFormation, Terraform, or CLI commands.
3: Proficient. Strong understanding of Console actions. Comfortable with CloudFormation, Terraform, or CLI commands. Some understanding of infrastructure as code.
4: Expert. Fluent understanding of console actions. Strong understanding of CloudFormation, Terraform, and CLI commands. Proficient with infrastructure as code.

Ensure that Amazon S3 buckets are configured to block public access at the account level. Account level settings override settings on individual objects. Configuring your account to block public access will override any public access settings made to individual objects within your account.

Risk

Configuring public access for S3 buckets may expose sensitive information stored in the S3 objects to unintended users, resulting in data compromise.

SOLUTIONS

AWS CloudFormation Solution

Here is a sample CloudFormation code to block public access for Amazon S3 buckets. When you create a new bucket, all Block Public Access settings are automatically enabled. We recommend that you keep all Block Public Access settings enabled.

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  ExampleBucket:
    Type: AWS::S3::Bucket
    Properties:
      BucketName: example
      PublicAccessBlockConfiguration:
                BlockPublicAcls: true
                BlockPublicPolicy: true
                IgnorePublicAcls: true
                RestrictPublicBuckets: true
```

Hashicorp Terraform Solution

Here is a sample Terraform code to block public access for Amazon S3 buckets.

```
resource "aws_s3_bucket" "example" {
  bucket = "example"
}

resource "aws_s3_bucket_public_access_block" "example" {
  bucket = aws_s3_bucket.example.id

  block_public_acls       = true
  block_public_policy     = true
  ignore_public_acls      = true
  restrict_public_buckets = true
}
```

AWS Console Solution

In order to block public access for Amazon S3 buckets, follow the steps using the AWS Management console. By default, new buckets, access points, and objects don't allow public access.

1. Open the Amazon S3 console at https://console.aws.amazon.com/s3/
2. Choose **Block Public Access settings for this account**.
3. Choose **Edit** to change the block public access settings for all the buckets in your AWS account.
4. Choose the settings that you want to change, and then choose **Save changes**.
5. When you're asked for confirmation, enter confirm. Then choose **Confirm** to save your changes.

AWS Command Line Solution (CLI)

In order to block public access for Amazon S3 buckets at the account level, use the `put-public-access-block` command using the AWS CLI.

```
aws s3control put-public-access-block –account-id <value> --public-access-
block-configuration
"BlockPublicAcls=true,IgnorePublicAcls=true,BlockPublicPolicy=true,RestrictP
ublicBuckets=true"
```

Audience

This document is intended for those involved in planning, designing, and implementing the AWS cloud security solutions. The audience includes the following roles: Engineering, Architecture, Operations, Networking, Development, and Security.

Control Title:	Block Public Access for Amazon S3 at account level.
Risk Severity:	Critical
Priority:	4 (High)
LOE – Hours:	2
Agile Size (1-4):	2
Skill Level (1-4):	3
Tags:	#s3 #public-access #public #Control-ID: “CRY-CS-3” #Control-TR: “DCH_CRY-TR-2600” #AWS-Config-Rule: “s3-account-level-public-access-blocks” #AWS-SecHub-ID: “S3.1” #Policy-Signatures: “AWS_000073”

Notices

This document is provided for informational purposes only. It represents AWS’s current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS’s products or services, each of which is provided “as is” without warranty of any kind, whether expressed or implied.

This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.