OpenSecOps SOAR S3 Buckets

Standard Operating Procedure

Table of Contents

1 Introduction

The purpose of this document is to specify baseline settings for AWS S3 Buckets so that teams can provision S3 Buckets in a safe, conformant way.

2 Scope of SOP

This document covers AWS S3 Buckets and their configuration options in OpenSecOps.

Document Versions

Version	Date	Changes	Author
1.0	2022-09-12	First version	Peter Bengtson
1.1	2025-04-07	Replaced “Delegat” with “OpenSecOps” throughout	Peter Bengtson
1.2	2025-04-27	Removed obsolete information	Peter Bengtson

3 Make your S3 Bucket Non-Public

Always explicitly set your bucket to be non-public, unless it needs to be publicly accessible (for which see next section). Failing to make it inaccessible to the world is a `CRITICAL` security issue that immediately will be detected by OpenSecOps's automated security monitoring. A security incident will be created, which your team is recommended to fix as a show-stopping silver bullet, i.e. with immediate priority over all ongoing work in the team as a whole.

3.1 CloudFormation

```
ExampleBucket:
    Type: AWS::S3::Bucket
    Properties:
      PublicAccessBlockConfiguration:
        BlockPublicAcls: true
        BlockPublicPolicy: true
        IgnorePublicAcls: true
        RestrictPublicBuckets: true
```

3.2 Terraform

```
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
}
```

4 Public S3 Buckets

If you need an S3 bucket to be publicly readable and/or writable – which should be very rare – you must set one or both of the following tags on your S3 bucket:

```
soar:s3:request-publicly-readable
soar:s3:request-publicly-writable
```

The tags are case-sensitive. The value of the tags should be empty (“”). (NB: `publicly` is the correct spelling; “-ally” would be incorrect.)

When one or both of the above tags are present, the S3 bucket will be left open.

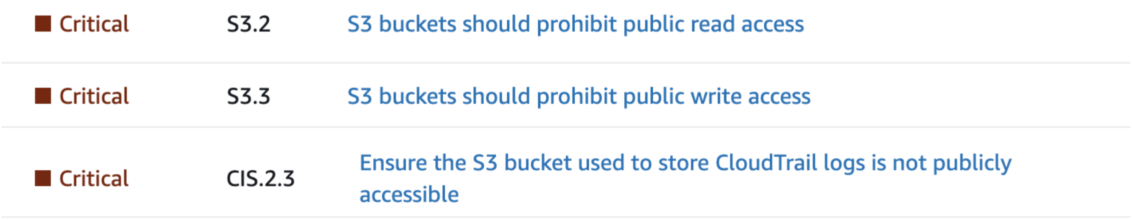
SOC, if configured, will be notified of your request via a Jira incident. You will be contacted about the reasons for wanting to create a storage volume open to the world. Should SOC deny the request, you will also be contacted prior to the removal of the tag.

If the S3 bucket already has been closed by the OpenSecOps SOAR, adding the tags after the fact will *not* open the bucket again. You must add the tag(s), then open the bucket for read and/or write again either manually in the console, using the CLI, the API, or in code.

5 Security Hub Controls for S3 Buckets

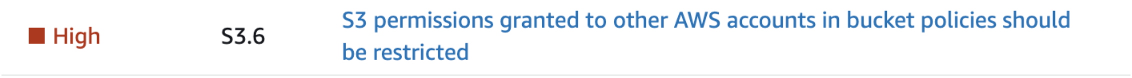
Below are the enabled controls in AWS Security Hub pertaining to S3 buckets..

5.1 CRITICAL



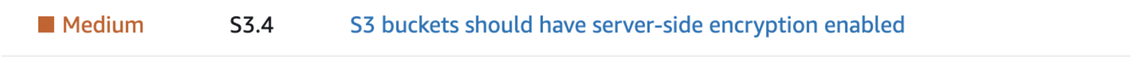
■ Critical	S3.2	S3 buckets should prohibit public read access
■ Critical	S3.3	S3 buckets should prohibit public write access
■ Critical	CIS.2.3	Ensure the S3 bucket used to store CloudTrail logs is not publicly accessible

5.2 HIGH



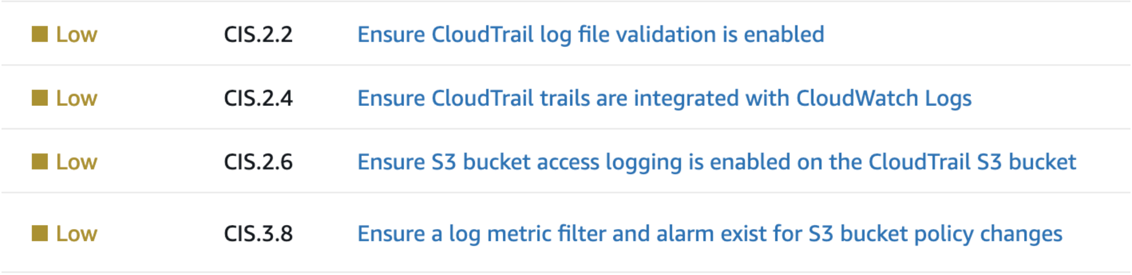
■ High	S3.6	S3 permissions granted to other AWS accounts in bucket policies should be restricted

5.3 MEDIUM



■ Medium	S3.4	S3 buckets should have server-side encryption enabled

5.4 LOW



■ Low	CIS.2.2	Ensure CloudTrail log file validation is enabled
■ Low	CIS.2.4	Ensure CloudTrail trails are integrated with CloudWatch Logs
■ Low	CIS.2.6	Ensure S3 bucket access logging is enabled on the CloudTrail S3 bucket
■ Low	CIS.3.8	Ensure a log metric filter and alarm exist for S3 bucket policy changes