

```
14
    + license = "Elastic License v2"
    + name = "AWS S3 Data Management Tampering"
16
    + references = [
                   "https://docs.aws.amazon.com/AmazonS3/latest/API/API_Operations.html",
17
                   "https://docs.aws.amazon.com/AmazonS3/latest/API/API_PutBucketLogging.html",
18
19
                   "https://docs.aws.amazon.com/AmazonS3/latest/API/API_PutBucketWebsite.html",
20
      "https://docs.aws.amazon.com/AmazonS3/latest/API/API_PutBucketEncryption.html",
                   "https://docs.aws.amazon.com/AmazonS3/latest/userguide/setting-repl-config-
21
      perm-overview.html",
                   "https://docs.aws.amazon.com/AmazonS3/latest/API/API_RestoreObject.html"
22
   + 1
23
24 + risk_score = 21
25 + rule id = "f3d8d0e1-5f9a-4afe-9722-d10bd28b18d2"
26 + severity = "low"
   + tags = ["Elastic", "Cloud", "AWS", "Continuous Monitoring", "SecOps", "Asset Visibility"]
   + timestamp_override = "event.ingested"
    + type = "query"
29
30
31 + query = '''
32 + event.dataset:aws.cloudtrail and event.provider:iam.amazonaws.com and
33 + event.action:(PutBucketLogging or PutBucketWebsite or PutEncryptionConfiguration or
      PutLifecycleConfiguration or
                      PutReplicationConfiguration or ReplicateObject or RestoreObject) and
34
      event.outcome:success
35 + '''
```

Comment on lines +32 to +35



w0rk3r on Sep 22, 2021

Contributor

@austinsonger can you provide example data to these actions?

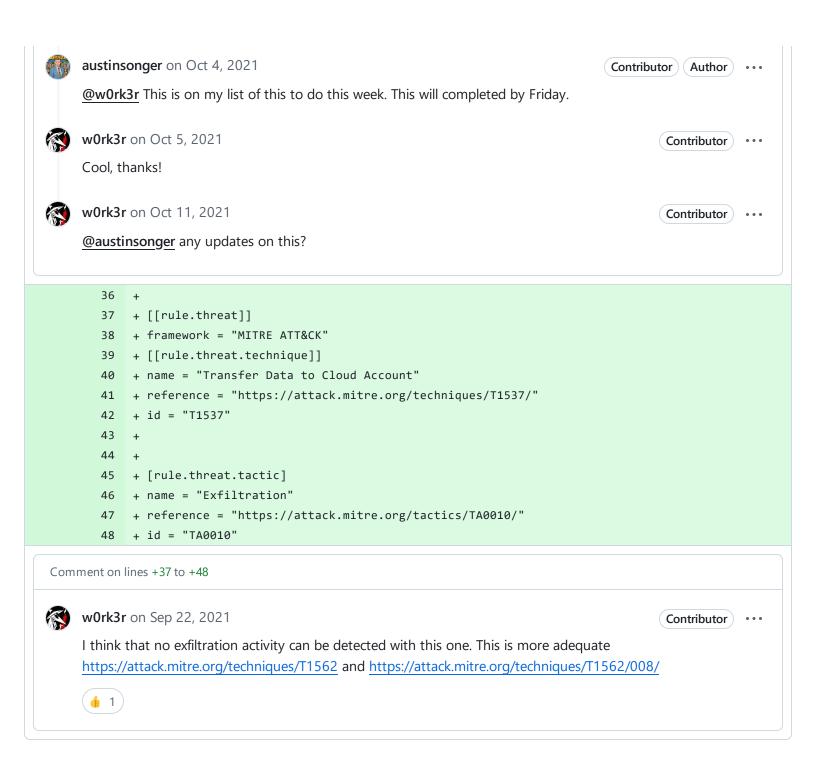
- PutBucketLogging is also used to enable Logging, I don't see why to alert on that case, so we need more data to make a filter
- PutEncryptionConfiguration: I could not find this on the API reference, do you mean
 PutBucketEncryption?
- PutLifecycleConfiguration, ReplicateObject and RestoreObject are permissions, do event.action field contains this?
- PutReplicationConfiguration seems to be related with AWS ECR, not s3



w0rk3r on Oct 4, 2021

Contributor

@austinsonger any updates on this one?



Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information © 2024 GitHub, Inc.