[New Rule] AWS S3 Data Management Tampering #1145

Closed

austinsonger wants to merge 13 commits into `elastic:main` from `austinsonger:exfiltration_s3_data_management_tampering`

48 rules/aws/exfiltration_s3_data_management_tampering.toml

```
@@ -0,0 +1,48 @@
+ [metadata]
+ creation_date = "2021/05/05"
+ maturity = "production"
+ updated_date = "2021/05/05"
+
+ [rule]
+ author = ["Austin Songer"]
+ description = "Identifies when a user tampers with S3 configuration in Amazon Web Services."
+ false_positives = ["Unknown"]
```

austinsonger marked this conversation as resolved. Show resolved

```
+ from = "now-10m"
+ index = ["filebeat-*", "logs-aws*"]
+ interval = "10m"
+ language = "kuery"
```

```
14 + license = "Elastic License v2"
15 + name = "AWS S3 Data Management Tampering"
16 + references = [
17 +             "https://docs.aws.amazon.com/AmazonS3/latest/API/API_Operations.html",
18 +             "https://docs.aws.amazon.com/AmazonS3/latest/API/API_PutBucketLogging.html",
19 +             "https://docs.aws.amazon.com/AmazonS3/latest/API/API_PutBucketWebsite.html",
20 +
   "https://docs.aws.amazon.com/AmazonS3/latest/API/API_PutBucketEncryption.html",
21 +             "https://docs.aws.amazon.com/AmazonS3/latest/userguide/setting-repl-config-
   perm-overview.html",
22 +             "https://docs.aws.amazon.com/AmazonS3/latest/API/API_RestoreObject.html"
23 + ]
24 + risk_score = 21
25 + rule_id = "f3d8d0e1-5f9a-4afe-9722-d10bd28b18d2"
26 + severity = "low"
27 + tags = ["Elastic", "Cloud", "AWS", "Continuous Monitoring", "SecOps", "Asset Visibility"]
28 + timestamp_override = "event.ingested"
29 + type = "query"
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
34 +                 PutReplicationConfiguration or ReplicateObject or RestoreObject) and
   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?

austinsonger on Oct 4, 2021 Contributor Author

@w0rk3r This is on my list of this to do this week. This will completed by Friday.

w0rk3r on Oct 5, 2021 Contributor

Cool, thanks!

w0rk3r on Oct 11, 2021 Contributor

@austinsonger any updates on this?

```
36 +
37 + [[rule.threat]]
38 + framework = "MITRE ATT&CK"
39 + [[rule.threat.technique]]
40 + name = "Transfer Data to Cloud Account"
41 + reference = "https://attack.mitre.org/techniques/T1537/"
42 + id = "T1537"
43 +
44 +
45 + [rule.threat.tactic]
46 + name = "Exfiltration"
47 + reference = "https://attack.mitre.org/tactics/TA0010/"
48 + id = "TA0010"
```

Comment on lines +37 to +48

w0rk3r on Sep 22, 2021 Contributor

I think that no exfiltration activity can be detected with this one. This is more adequate https://attack.mitre.org/techniques/T1562 and https://attack.mitre.org/techniques/T1562/008/

👍 1