CloudTrail Logs Impairment Through S3 Lifecycle Rule

Archived: 2026-04-05 14:50:32 UTC

Platform: AWS

Mappings

- MITRE ATT&CK
  - Defense Evasion
- Threat Technique Catalog for AWS:
  - Impair Defenses: Disable Cloud Logs (T1562.008)

Description

Set a 1-day retention policy on the S3 bucket used by a CloudTrail Trail, using a S3 Lifecycle Rule.

References: https://www.justice.gov/usao-sdny/press-release/file/1452706/download

Warm-up:

- Create a CloudTrail trail logging to a S3 bucket.

Detonation:

- Apply a S3 Lifecycle Rule automatically removing objects after 1 day.

Instructions

Detonate with Stratus Red Team

```
stratus detonate aws.defense-evasion.cloudtrail-lifecycle-rule
```

Detection

Identify when lifecycle rule with a short expiration is applied to an S3 bucket used for CloudTrail logging.

The CloudTrail event `PutBucketLifecycle` and its attribute `requestParameters.LifecycleConfiguration.Rule.Expiration.Days` can be used.
