Public S3 bucket identification

You might want to identify access control changes to Amazon S3 buckets when doing the following:

- Managing an Amazon Web Services environment

Prerequisites

In order to execute this procedure in your environment, the following data, services, or apps are required:

- Splunk Enterprise or Splunk Cloud Platform
- Amazon CloudWatch data
- Splunk Add-on for Amazon Web Services

Example

Amazon Simple Storage Service (S3) buckets may be inadvertently set with broader (public) access, which could lead to the loss or theft of confidential information. Based on the complexity of access control list (ACL) configurations, it's extremely difficult to determine the true accessibility of an S3 bucket via Cloudwatch logs.

You can use this search to review critical ACL changes made to S3 buckets access configurations.

To optimize the search shown below, you should specify a time range.

1. Ensure that your deployment is ingesting AWS data through one of the following methods:
   - Pulling the data from Splunk via AWS APIs. At small scale, pull via the AWS APIs will work fine.
   - Pushing the data from AWS into Splunk via Lambda/Firehose to Splunk HTTP event collector. As the size and scale of either your AWS accounts or the amount of data to be collected grows, pushing data from AWS into Splunk is the easier and more scalable method.

2. Run the following search:

   ```
   index=*
   sourcetype=aws:cloudtrail
   eventSource=s3.amazonaws.com
   eventName IN (*PublicAccessBlock*, *ACL*, PutBucketPolicy)
   | eval requestParameters=mvindex(split(mvindex(split(_raw, "requestParameters":""),1),"responseElements"),0)
   | table _time requestParameters.bucketName userIdentity.principalId eventName requestParameters
   ```

Search explanation

The table provides an explanation of what each part of this search achieves. You can adjust this query based on the
specifics of your environment.

<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>index=&quot;&lt;AWS index name&gt;&quot; sourcetype=&quot;aws:cloudtrail&quot;</td>
<td>Search the index(s) where AWS data is stored filtered to just the AWS Cloudwatch Logs sourcetype.</td>
</tr>
<tr>
<td>readOnly=False eventSource=&quot;s3.amazonaws.com&quot; eventName IN (<em>PublicAccessBlock</em>, <em>ACL</em>, PutBucketPolicy)</td>
<td>Filter to non-readOnly events associated with s3 activity where the eventName is indicative of a modification to bucket access.</td>
</tr>
<tr>
<td>eval requestParameters=mvindex(split(mvindex(split(_raw,&quot;requestParameters&quot;:&quot;&quot;),1),&quot;&quot;responseElements&quot;&quot;),0)</td>
<td>Parse out the parameters of the change. The parameter contents are dynamic and outline what change was requested.</td>
</tr>
<tr>
<td>table _time requestParameters.bucketName userIdentity.principalId eventName requestParameters</td>
<td>Display the results in a table with columns in the order shown.</td>
</tr>
</tbody>
</table>

**Result**

Being able to see who changed access policies that may impact an S3 buckets accessibility, and when the changes were made, allows you to perform further investigation on the bucket to determine if the access is appropriate and warranted.

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.