Geographic access to AWS S3 Buckets

You might want to view the geographic location of accounts accessing your 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
• AWS access logs
• Splunk Add-on for Amazon Web Services

Example

Visualizing where in the world Amazon Simple Storage Service (S3) buckets are being accessed from may help uncover various insights, such as S3 buckets which have been inadvertently granted public access, or whether or not certain content is being consumed and by whom.

You can use this search to visualize where and what S3 buckets are accessed.

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="AWS-INDEX" sourcetype="aws:s3:accesslogs"
   | iplocation remote_ip
   | geostats count BY bucket_name

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:s3:accesslogs&quot;</td>
<td>Search the index(s) where AWS data is stored filtered to just the AWS access logs.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>iplocation remote_ip</th>
<th>Enrich the data with geographic information related to the remote_ip (the IP address that was used to access the S3 bucket).</th>
</tr>
</thead>
<tbody>
<tr>
<td>geostats count BY bucket_name</td>
<td>Plot the access on a map per each location and bucket_name.</td>
</tr>
</tbody>
</table>

**Result**

Use the results of this search to verify that access to your S3 buckets is legitimate. Investigate further as needed.