Analyzing AWS service action errors

Applicability

• Product: Splunk Enterprise or Splunk Cloud Platform
• Feature: Search
• Function: AWS service actions

Problem

CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. Any user, role, or service that attempts successfully or unsuccessfully to act as a service in AWS will generate a log containing information about that event. You want to use errors in those logs not only for alerting, but for proactive security hunting.

Solution

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

1. Run the following search:
   ```splunk
   sourcetype=aws:cloudtrail
   |stats count BY errorCode
   |sort - count
   ```

2. After you find errors you want to investigate, run the following search:
   ```splunk
   sourcetype=aws:cloudtrail errorCode=<error name>
   |table awsregion eventName userName src_ip userAgent errorMessage
   ```

Explanations

<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourcetype=aws:cloudtrail</td>
<td>Search only AWS CloudTrail logs.</td>
</tr>
<tr>
<td></td>
<td>stats count BY errorCode</td>
</tr>
</tbody>
</table>

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.
<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>sort - count</td>
<td>Sort with the most frequently occurring first.</td>
</tr>
<tr>
<td>errorCode=&lt;error name&gt;</td>
<td>Search for more information on a specific error.</td>
</tr>
<tr>
<td>table awsregion eventName userName src_ip userAgent errorMessage</td>
<td>Display the results in a table with columns in the order shown.</td>
</tr>
</tbody>
</table>

### Additional resources

These additional Splunk resources might help you understand and implement these recommendations:

- Blog: [Digital breadcrumbs for AWS](#)
- Blog: [Using Splunk to detect abuse of AWS permanent and temporary credentials](#)