Verifying multifactor authentication usage

Applicability

- Product: Splunk Enterprise or Splunk Cloud Platform
- Feature: Search
- Function: Auditing AWS logins

Problem

The CIS Benchmark recommends the use of Multi-Factor Authentication (MFA) on accounts with a console password (Section 1.2) and root accounts (1.14). Enabling MFA helps secure accounts, so conversely, the lack of MFA may result in accounts that are more easily compromised. You want to see if users are logging in without MFA.

Solution

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

1. Run the following search:

   ```
   sourcetype=aws:cloudtrail eventName=ConsoleLogin
   | stats count BY username, additionalEventData.MFAUsed
   ```

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>eventName=ConsoleLogin</td>
<td>Search for login events.</td>
</tr>
<tr>
<td></td>
<td>stats count BY username, additionalEventData.MFAUsed</td>
</tr>
</tbody>
</table>
Additional resources

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

- Blog: Digital breadcrumbs for AWS
- Blog: The importance of enforcing multifactor authentication in your AWS environment