New tables queried by a Salesforce cloud peer group

You might need to detect first-time query attempts to sensitive tables by a peer group that has previously not accessed the tables when doing the following:

- Protecting a Salesforce cloud deployment

Prerequisites

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

- Splunk Enterprise or Splunk Cloud Platform
- CRM, ERP, and other business application data
- Splunk Add-on for Salesforce

Example

A search might show first-time query attempts to sensitive tables by a peer group that has previously not accessed the tables in question. This detection can help prove that individuals within the organization are not abusing or misusing legitimate access to assets that store and process personal data. Because so many people in your organization have access to Salesforce, you want to monitor regularly for new table queries.

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

1. Populate the lookup_sfdc_usernames lookup provided by the Salesforce Add-on with live values from your site.
2. Run the following search:

```shell
QUERY=* EVENT_TYPE=API OR EVENT_TYPE=BulkAPI OR EVENT_TYPE=RestAPI
| rex field=QUERY max_match=12 "is(?!)fromis(?<QUERY_TABLE>[l_w_.]*)"
| search QUERY_TABLE="Account*" OR QUERY_TABLE="Contact*" OR QUERY_TABLE="Opportunity*"
| lookup lookup_sfdc_usernames USER_ID
| stats earliest(_time) AS earliest latest(_time) AS latest BY Username, QUERY_TABLE
|where earliest > relative_time(now(), "-1d@d")
```

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>QUERY=* EVENT_TYPE=API OR EVENT_TYPE=BulkAPI OR EVENT_TYPE=RestAPI</td>
<td>Filter for API-related events where a query is defined.</td>
</tr>
<tr>
<td>rex field=QUERY max_match=12 &quot;\s(?i)from\s*(?&lt;QUERY_TABLE&gt;[\w_]*)&quot;</td>
<td>Extract the table name from the query. The rex captures all the word characters after the &quot;from&quot; clause in the SQL query.</td>
</tr>
<tr>
<td>search QUERY_TABLE=Account* OR QUERY_TABLE=Contact* OR QUERY_TABLE=Opportunity*</td>
<td>Filter the results to include only queries of sensitive tables (Account, Contact, or Opportunity), or their derivatives.</td>
</tr>
<tr>
<td>lookup lookup_sfdc_usernames USER_ID</td>
<td>Convert the SFDC USER_ID into a friendly username via a lookup.</td>
</tr>
<tr>
<td>stats earliest(_time) AS earliest latest(_time) AS latest BY USER_NAME, QUERY_TABLE</td>
<td>Calculate the earliest and the latest time this combination of fields occurred.</td>
</tr>
<tr>
<td>where earliest &gt; relative_time(now(), &quot;-1d@d&quot;)</td>
<td>Determine whether the earliest time this value was seen was within the last day.</td>
</tr>
</tbody>
</table>

Result

While there are no traditional false positives in this search, there will be a lot of noise. Every time this search runs, it will accurately reflect the first occurrence in the time period you’re searching over (or for the lookup cache feature, the first occurrence over whatever time period you built the lookup). You should not review these alerts directly (except for high sensitivity accounts), but instead use them for context or to aggregate risk.

For most environments, these searches can be run once a day, often overnight, without a lag. If you want to run this search more frequently, or if this search is too slow for your environment, leverage a lookup cache.

When this search returns values, initiate your incident response process and identify the peer group demonstrating this behavior. Capture the time of the event, the user’s role, and tables queried. If possible, determine the system used and its location. Contact the user and their manager to determine if the download is authorized, and then document that it was authorized and by whom. If you cannot find authorization, the user credentials may have been used by another party and additional investigation is 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.
**GDPR Relevance:** This search can be considered an effective security control, as required by Article 32. This is applicable to processing personal data from the controller and needs to also be addressed if contractors or sub-processors from third countries or international organizations access and transfer personal data (Article 15).