New application accessing the Salesforce API

You might need to find users who connect to SFDC's reporting API with new clients 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

Your Salesforce cloud deployment contains your company's most critical customer information. To help protect this data, you want to regularly monitor users who connect to SFDC's reporting API with new clients.

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:

   ```splunk
   CLIENT_NAME=* EVENT_TYPE=API OR EVENT_TYPE=BulkAPI OR EVENT_TYPE=RestAPI
   |lookup lookup_sfdc_usernames USER_ID
   |stats earliest(_time) AS earliest latest(_time) AS latest BY USER_ID, CLIENT_NAME
   |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>CLIENT_NAME=*</td>
<td>Filter for events where the CLIENT_NAME is set to a value.</td>
</tr>
</tbody>
</table>
Splunk Search

EVENT_TYPE=API OR EVENT_TYPE=BulkAPI OR EVENT_TYPE=RestAPI

Explanation
Filter for API-related events.

|lookup lookup_sfdc_usernames USER_ID

Convert the SFDC USER_ID into a friendly username via a lookup.

|stats earliest(_time) AS earliest latest(_time) AS latest BY USER_NAME, CLIENT_NAME

Calculate the earliest and the latest time this combination of fields occurred.

|where earliest > relative_time(now(), "-1d@d")

Determine whether the earliest time this value was seen was within the last day.

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 user demonstrating this behavior. Capture the time of the event, the user’s role, and application. 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.

**GDPR Relevance:** Under the GDPR Article 30, organizations are required to maintain a record of processing activities, including contact details of the controller, the purposes of processing, description of the categories of data subjects and personal data processed—as well as the categories of recipients to whom the personal data has been or will be disclosed including recipients in any other countries. Interactions from new applications—whether for legitimate purposes or as a result of malicious activity—can create a non-compliance condition if they are not documented properly. This situation may not impact organizations who employ fewer than 250 persons and, therefore, may not have critical categories of personal data for processing.

Monitoring Salesforce.com API activity can help identify connections from new applications or clients that might not be
whitelisted or documented. The timely and accurate reporting of a non-compliance state can prompt the Data Privacy Officer to proactively follow up and update documentation, and report to the authorities in a timely manner if appropriate.