Protecting a Salesforce cloud deployment

Scenario: Your organization maintains business-critical information within the SaaS customer relationship management application, Salesforce.com. This data relates to customers, partners, prospects, and, often, employees. As part of your Salesforce.com deployment, other applications interact with this sensitive data, via push or pull APIs that automate data exchange. For example, you might have integrations into finance and human resources applications, such as Workday, or marketing automation tools, such as Eloqua and Marketo. You know that attackers can attempt to use the Salesforce.com API as a vector to gain access to sensitive data. Because Salesforce.com is a cloud application with a publicly accessible domain, this vector only requires valid credentials and can be exploited for access to sensitive data by adversaries, even if they lack access to internal resources. You need searches that you can run regularly to help detect any malicious behavior in your Salesforce environment. You can use Splunk software to monitor queries, especially queries that are new for certain users or peer groups. You can also monitor downloads of records and files, and set up searches to alert you to other high-risk events.

Prerequisites

To succeed in implementing this use case, you need the following dependencies, resources, and information.

- People: IT service owner
- Technologies: Splunk Enterprise or Splunk Cloud Platform
- Data: Salesforce data

How to use Splunk software for this use case

You can run many searches with Splunk software to protect a Salesforce cloud deployment. Depending on what information you have available, you might find it useful to identify some or all of the following:

- New application accessing the Salesforce API
- New high-risk event types for a Salesforce cloud user
- New tables queried by a Salesforce cloud peer group
- New tables queried by a Salesforce cloud user
- Spike in downloaded documents per user on Salesforce cloud
- Spike in exported records from Salesforce cloud

Results

To maximize their benefit, the how-to articles linked in the previous section likely need to tie into existing processes at
your organization or become new standard processes. These processes commonly impact success with this use case:

- Compliance office processes
- Security and Identity access management

Measuring impact and benefit is critical to assessing the value of security operations. The following are example metrics that can be useful to monitor when implementing this use case:

- Counts of object access over time
- Counts identity access over time
- Number of reports for compliance attestation

**Additional resources**

This use case is also included in the [Splunk Security Essentials](#) app, which provides more information about how to implement the use case successfully in your security maturity journey. In addition, these Splunk resources might help you understand and implement this use case:

- Docs: [About the Splunk Add-on for Salesforce](#)
- App: [Details on Splunk App for Salesforce](#)