SKYFORMATION

SkyFormation for Salesforce Cloud Connector

Overview

Salesforce provides a broad set of customers and sales automation and management services delivered as a cloud service. Salesforce helps organizations move faster with infinite scalability and lower cost for their sales automation and management. But at the same time, the public cloud Software as a Service (SaaS) model presents the organization with new security challenges.

The main challenges and needs are to:

Get and retain visibility of in-service activities

Retrieve the Salesforce activities as users' access, permissions changes, security changes, files management and others into the organization central log or event management system.

Detect threats

Be able to detect threats as data exfiltration, compromised accounts and more, from both insider and external attackers.

Detect unapproved or risky security changes

Be able to detect security changes that are either done by unapproved people or violate the organization policy. For example, be able to detect when a new administrator is added to Salesforce from unknown location.

SkyFormation for Salesforce cloud connector

What is it

SkyFormation for Salesforce cloud connector, is part of the SkyFormation Cloud Connectors platform that monitor events across different cloud services and apps (e.g. Azure, AWS, Salesforce, Office 365 and more) and send them to the organization's SIEM / SOC systems in an actionable

Solution Highlights

SkyFormation for Salesforce Cloud Connector allows organizations to:

- Extend existing SIEM/Splunk system to get full audit and visibility of activities and events in their Salesforce service.
- Detect security threats in Salesforce using existing SIEM system
- Streamline Salesforce security incidents investigations using existing security operation system.
- Speed up regulatory compliance support

How it works

SkyFormation Cloud Connectors retrieve the events from the different cloud services events sources as log files, using the cloud service APIs (out-of-band), and send the events after enriching to the organization's SIEM / SOC system, using Syslog. No network security changes are needed in Firewall or else. SkyFormation Cloud Connectors could be deployed on any VM whether in the cloud or on-premise.

Main benefits

- Reduce development costs - No need to develop ad-hoc cloud services connectors
- Reduce maintenance costs - No need to maintain self-created connectors changes
- Improve cloud protection – Events are designed to meet detection needs.
- Speed up regulatory – Security events required by regulations are monitored and sent to SIEM

SkyFormation Salesforce Logs and Events *Supported

What is it

Cloud services monitored by SkyFormation cloud connectors, mostly support multiple audit logs and sources, where each contains different type of information and events.

SkyFormation cloud connectors monitor events in each "Supported Log" specified in the table below at the following way:

(1) Audit Events
The entire events available at the "Supported Log" are extracted and sent to the integrated SIEM/Central log, in their original structure.
This level of monitoring ensures no event from the original audit log is lost, and allow easier compliance and forensic process.

(2) SkyFormation Unified Events
These are cloud service original events SkyFormation connector transform into the the SkyFormation Unified Security Events .
These events allow easiest detection across multiple cloud services, in any SIEM. They also streamline investigation and incident response

Supported Log	Details
LoginHistory	○ Successful login ○ Failed login ○ Password locked out
SetupAuditTrail	○ Connected application ▪ Create ▪ Deleted ▪ Install ▪ Uninstall ▪ Block ▪ Unblock ○ Territory ▪ Create ▪ Delete ▪ Add user ▪ Remove user ▪ Opportunity access level update ▪ Contact access level update ▪ Create territory type ▪ Delete territory type ▪ Create territory model ▪ Update territory model state ▪ Add object territory assignment rule to territory model ▪ Remove object territory assignment rule to territory model ▪ Activate object territory assignment rule in territory model ▪ Deactivate object territory assignment rule in territory model ▪ Update object territory assignment rule in territory model ○ Delegated logout ○ Permission set ▪ Create ▪ Assign ▪ Unassign ▪ Rename ▪ Update of field level permissions ▪ Update of object level permissions ▪ Update of tab permissions ▪ Update of user (system) permissions

	▪ Update of apex class access permissions ○ Profile ▪ Clone ▪ Delete ▪ Rename ▪ Change user's profile ▪ Update of field level permissions ▪ Update of object level permissions ▪ Update of user (system) permissions ▪ Add "View All" permission ▪ Enable and disable connected application for the profile ▪ Change visibility of console with macros application for the profile ○ Group ▪ Create ▪ Delete ▪ Rename ▪ Membership update ○ Password ▪ Reset ▪ Change ○ User ▪ Create ▪ Freeze user ▪ Unfreeze user ▪ Deactivate ▪ Activate ▪ Unlock ▪ Email update ▪ Email update attempt ▪ Username update ▪ Nickname update ▪ Email approval preference update ▪ Salesforce classic enable/disable ○ Role ▪ Create ▪ Delete ▪ Assign ▪ Unassign ▪ Replace ○ Security controls ▪ IP white list • Add

	• Delete • Update ○ Password policy update ▪ Expiration policy ▪ History policy ▪ Minimal length policy ▪ Complexity policy ▪ Question policy ▪ Maximum invalid attempts policy ▪ Lockout period policy ▪ Enable and disable obscuring of secret answer ▪ Enable and disable requiring minimum password lifetime ▪ Forgot password message ▪ Forgot password help link ▪ Alternative home page ○ Session settings update ▪ Enable and disable session timeout Warning ▪ Session timeout ▪ Enable and disable force logout on session timeout ▪ Enable and disable lock session IP ▪ Enable and disable lock session domain ▪ Enable and disable relogin after login-as-user ▪ Enable and disable require HttpOnly attribute ▪ Enable and disable use POST requests for cross-domain sessions attribute ▪ Enable and disable enforce login IP ranges on every request ▪ Enable and disable login page caching ▪ Enable and disable clickjack protection for customer Visualforce pages ▪ Enable and disable content security policy protection for email template ▪ Logout URL ▪ Session security level
ContentVersion	○ File upload [1] (content document) ○ File content update [1] (content document) ○ File deleted [1] (content document)

ContentVersionHistory	○ File download [1] (content document)
ContentDistributionView	○ File download [1] (content document) ○ File preview [1] (content document)
ContentDistribution	○ File shared [1] (content document) ○ File un-shared [1] (content document)
ContentWorkspace	○ Directory create (library)
Document	○ File upload (document) ○ File delete (document)
Attachment	○ File upload (attachment) ○ File delete (attachment) ○ File properties update (attachment)
EventLogFile[2, 3]	○ Export report ○ Run report ○ Delegate login ○ Dashboard view ○ File upload ○ File download ○ File preview ○ Object view

Remarks

1. Salesforce CRM content, not applicable over private libraries
2. All other events, not specified, are sent as an audit event
3. Event monitoring – data created every 24hr

About SkyFormation

Founded in 2014, SkyFormation is a cloud application security company that provides visibility and mitigation of the risks associated with cloud services usage in the organization. Building on the strengths of your existing Security Operations, SIEM and other security investments, SkyFormation uniquely detect threats by delivering granular security information on the usage of business cloud services (e.g. Salesforce, Azure, Office365, AWS, etc.), internally developed applications, and shadow IT.