RiskIQ App For Splunk Installation And Configuration

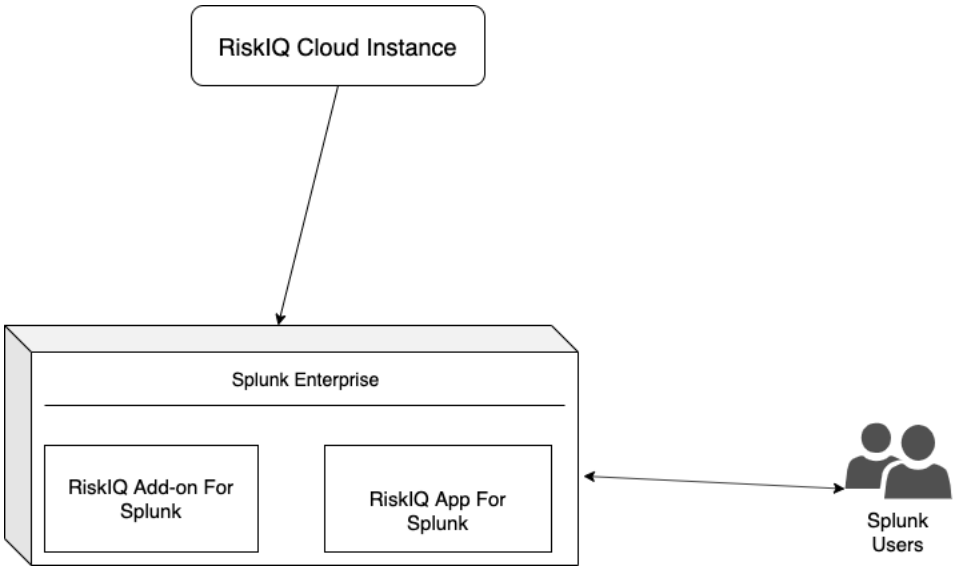
Introduction

RiskIQ App For Splunk allows user to collect assets and events data into Splunk, enrich them and provide dashboards for visualization.

Installing and Configuring RiskIQ App/Add-on For Splunk

Standalone Installation:

If you want to collect and visualize data on the standalone instance, then you need to install App and Add-on on the same Splunk instance.



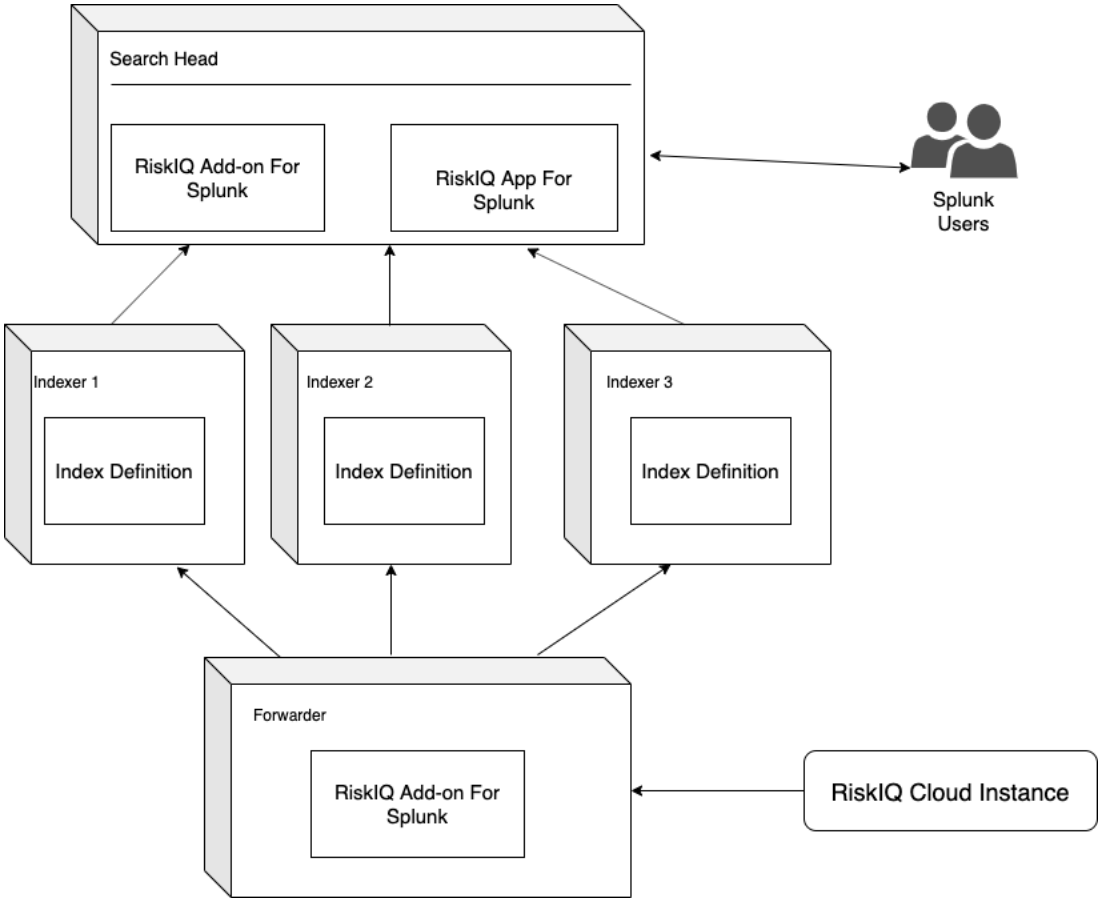
About the Installation
On a standalone Splunk installation, the App and TA can be installed either:

- Through the Splunk user interface from **Manage Apps**.

By extracting the compressed files (TA-RiskIQ-Sxx-x.x.x-x.tar.gz, RiskIQApp-Sxx-x.x.x-x.tar.g) into the $SPLUNK_HOME$/etc/apps folder and restarting Splunk

Distributed Installation

If you want to collect and visualize data on the distributed instance, then you need to install App and Add-on showed below in the diagram.



Component	Forwarder	Indexer	Search Head
RiskIQ Add-on For Splunk	Yes	No	Yes
RiskIQ App For Splunk	No	No	Yes

RiskIQ Add-on For Splunk

Technology Add-on in Splunk is responsible for getting data into Splunk and performing data normalization. TA-RiskIQ is responsible for collecting data from RiskIQ server and enriching the data.

The data collection from RiskIQ server is done in below way:

- Events Data
    - It will use /events/search REST endpoint and collect the data into Splunk with sourcetype riskiq:events
- Assets Information

    - It will use /inventory/search REST endpoint and collect the data into Splunk with sourcetype riskiq:assets

Setup Add-on For Data Collection

- After the installation, you'll be asked to restart the Splunk. Click on Restart Now.
- After the restart, you need to set up the data collection. From the UI navigate to `Apps->Manage Apps->RiskIQ Add-on for Splunk->Set up`.
- Enter the following details of your RiskIQ Instance and save it.
    - API Token: RiskIQ API token
    - Key: RiskIQ API key
    - Customer: Customer name
    - Page Size: Number of results to fetch in single API call. Defaults to 300
    - Enable events data collection: Check this to enable input and collect events data
    - Enable assets data collection: Check this to enable input and collect assets data from legacy endpoint
    - Enable GI assets data collection: Check this to enable input and collect assets data from global inventory endpoint
    - When you enable GI assets data collection, it will ask for tags, brand and organization for filtering data if you want. If you left them blank then we will collect all data.
    - Collect only new and changed assets: If this option is checked, only the new and changed assets will be collected. By default all assets are collected once in a day. To create/use default visuals displaying trend data, ingest all asset data every day by unchecking this option. To get only updated data then select this option.
    - Latest Updated Time :This option is shown when we check collect only new and changed assets. Provide the time in PST Time Zone with format(YYYY-MM-DDTHH:MM:SS.sss)
    - Enable Proxy: Check this option if you have proxy configured in your environment.
    - Proxy Scheme: Provide proxy protocol (http/https/socks4/socks5)
    - IP / Hostname: IP address or hostname of proxy instance.
    - Port: Port used to connect to proxy instance.
    - Require Authentication for Proxy: Check this option if your proxy configuration requires authentication.
    - Username: Provide proxy username
    - Password: Provide proxy password

* By default, SSL Verification will be true. If you don't want to verify your SSL certificate, follow steps:
  * Go to `$SPLUNK_HOME$/etc/apps/TA-RiskIQ/local`.
  * Open `appsetup.conf` file and find the stanza `app_config`.
  * Update value of `verify_ssl` from `true` to `false`.
  * Save the file and restart Splunk.

TA RiskIQ is configured and ready to be used.

Index, Source and Source type

In Splunk, any raw data is stored in indexes. For RiskIQ TA, user can select index while updating the scripted input
input and data collected from that scripted input will indexed to selected index.
Index and Source type are default Splunk fields to categorize and filter the indexed data to narrow down the search results. Below is the table which shows how the RiskIQ data is distributed in these fields.

Source Type	**Description**
riskiq:events	This data contains all the information which is collected from /events/search endpoint
riskiq:assets	This data contains all assets related information which is collected from /assets/search endpoint. It will collect data for different assets like WEBSITES, IPS, HOSTS, CERTS, ASN, DOMAINS, MAIL, NS, CONTACTS and with status CONFIRMED

Purpose of TA on different components

TA-RiskIQ has different purpose at different Splunk components

- **Heavy Forwarder:** It has been used at heavy forwarder to do data collection. So, User has to Add-on as described in Installation section below. Heavy forwarder does not have to be a separate component. It could be same as indexer or Search head. Heavy forwarder is nothing but a Splunk enterprise instance.
- **Indexer:** We only need to create index if we are collecting data in custom index
- **Search head:** It has been used at search head to do search time field extractions, which will be used by RiskIQ App for Splunk in visualizations

RiskIQ App For Splunk

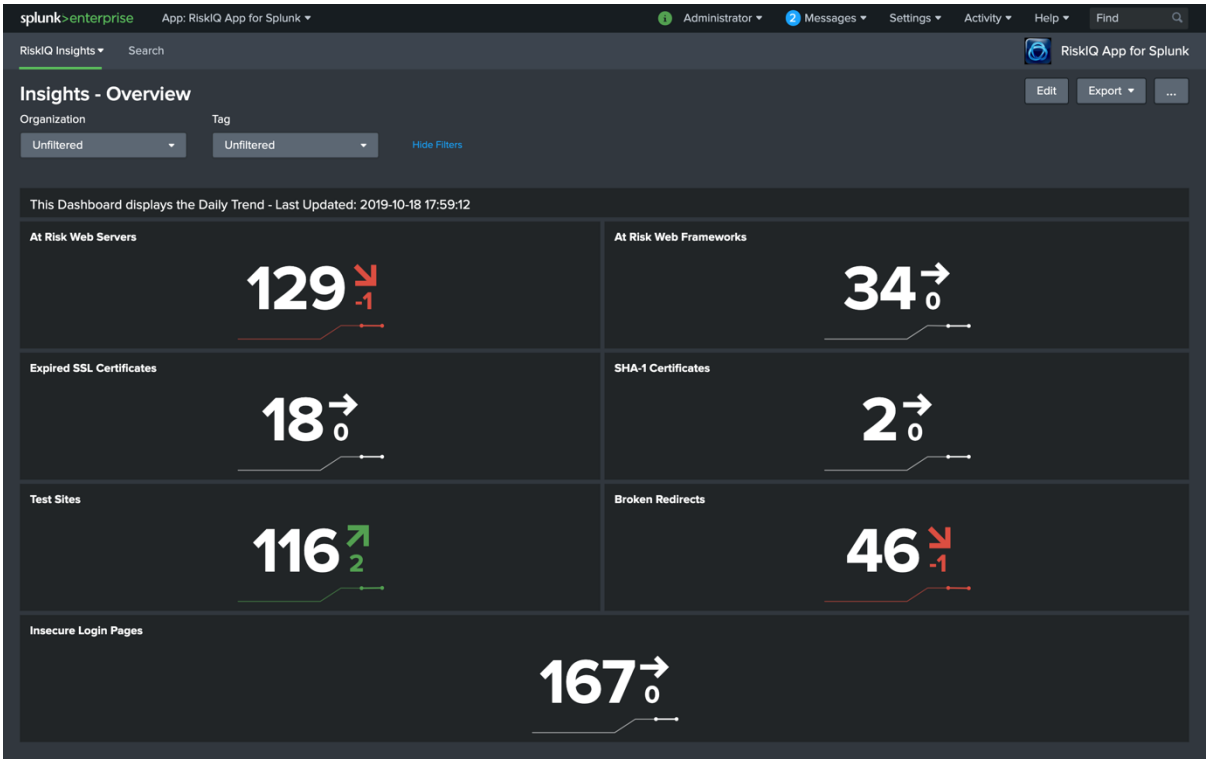
RiskIQ App For Splunk is for visualization and it contains different dashboards to visualize data which is collected from RiskIQ sever.

Dashboards

This application has multiple dashboards to cover overall assets information like WEBSITES, IPS, HOSTS, CERTS, ASN, DOMAINS, MAIL, NS, CONTACTS and with status CONFIRMED.

1. **Insights**

Insights dashboard will give you the overall picture of your assets and how many assets are added and removed from your RiskIQ



2. **At Risk Framework**
   At Risk Framework will give you deeper picture of the framework which can help you to identify the total framework in your organization, how many frameworks are added/removed over time.

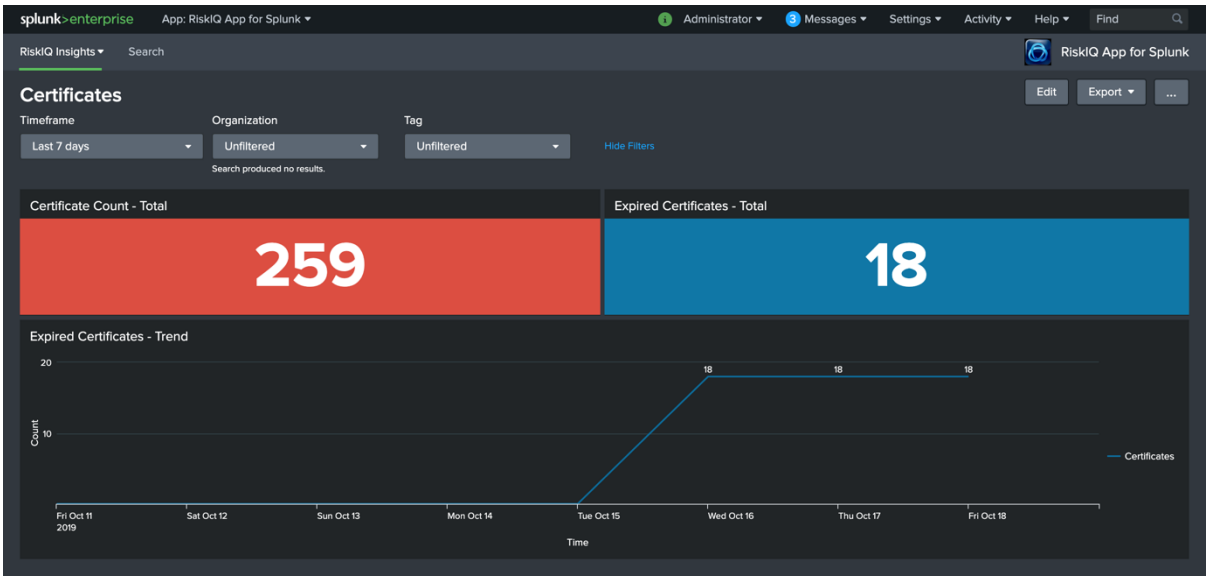

splunk>enterprise
App: RiskIQ App for Splunk
Administrator
Messages
Settings
Activity
Help
Find
RiskIQ Insights
Search
RiskIQ App for Splunk
RiskIQ - At Risk Frameworks
Edit
Export
...
Timeframe
Last 7 days
Organization
Unfiltered
Tag
Unfiltered
Hide Filters
At Risk Frameworks - Total
36
At Risk Frameworks - Organization
40
20
Fri Oct 11 2019
Sat Oct 12
Sun Oct 13
Mon Oct 14
Tue Oct 15
Wed Oct 16
Thu Oct 17
Fri Oct 18
Time
ANRC
BRC
IFRC
At Risk Frameworks - Remediated/Removed
1.5
1
0.5
Count
Websites
Time
At Risk Frameworks - Added
1.5
1
0.5
Count
Websites
Time
At Risk Frameworks - Trend
40
20
Count
35
34
34
Websites
Time

3. At Risk Servers

At Risk Servers will give you deeper picture of the servers which can help you to identify the total servers in your organization, how many frameworks are added/removed over time.

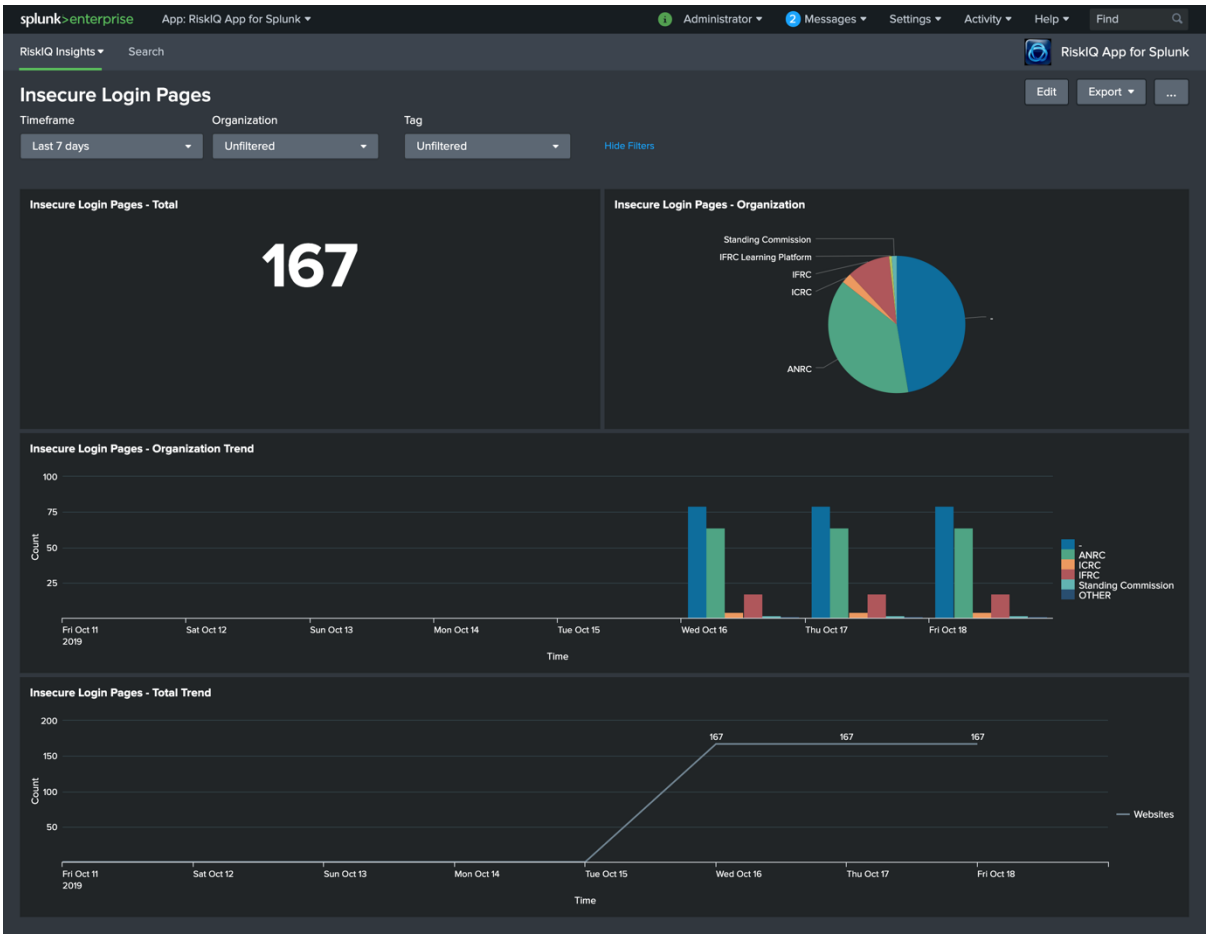
4. **Certificates**

Certificates will give you deeper picture which can help you to identify the total certificates in your organization, how many certificates are expired over time.



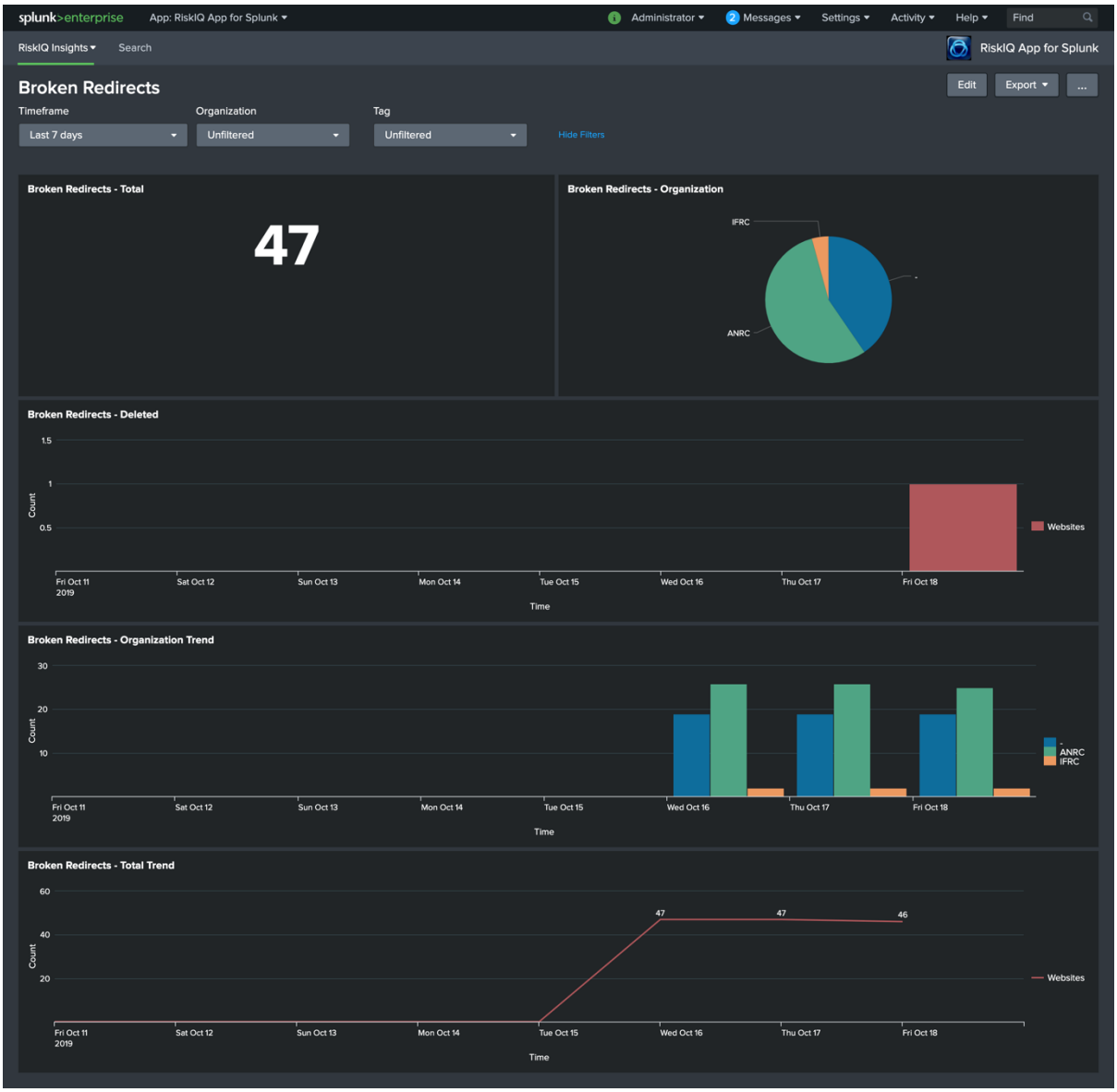
5. **Insecure Login Pages**

This dashboard will give you the overall picture of insecure logins in you organization. It will give you the number of insecure login by organization.



6. Broken Redirects

This dashboard will provide you the details of broken redirects. It will give you the overall count of broken redirects in your organization.



Installation

Pre-requisites

- You must set environment variable SPLUNK_HOME to the home location of the Splunk directory
- Splunk Enterprise 7.1, 7.2 or 7.3.

Single Server Deployment

In a single server deployment, single instance of Splunk Enterprise works as data collection node, indexer and search head. In such scenarios, install both TA-RiskIQ and RiskIQAppforSplunk applications on this node. Complete the setup of TA mentioned in the configuration section below.

Distributed Deployment

Configure Add-on on heavy forwarder mentioned in the configuration section below.

Cloud Instance

In Splunk Cloud, the data indexing will take place in cloud instance. The data collection can take place in on premise Splunk instance in user's environment that will work as heavy forwarder.
The application can be installed either through a command line or from Splunk UI.

- To install application from UI, log into Splunk. Go to App→Manage Apps and click on Install app from a file. Then choose the SPL file to install and click on upload the SPL.
- To install from the command window, go to $SPLUNK_HOME/bin folder and execute following

command:

./splunk install app TA-RiskIQ-XX-XXXX-XX.tar.gz
./splunk install app RiskIQAppForSplunk-XX-XXXX-XX.tar.gz