WhiteHat Sentinel Connector for Tableau

Overview

Customers who would like to analyze Sentinel data, drill down into it, or create visualizations of Sentinel data using Tableau can do so using a connector that WhiteHat has built to pull Sentinel data into Tableau.

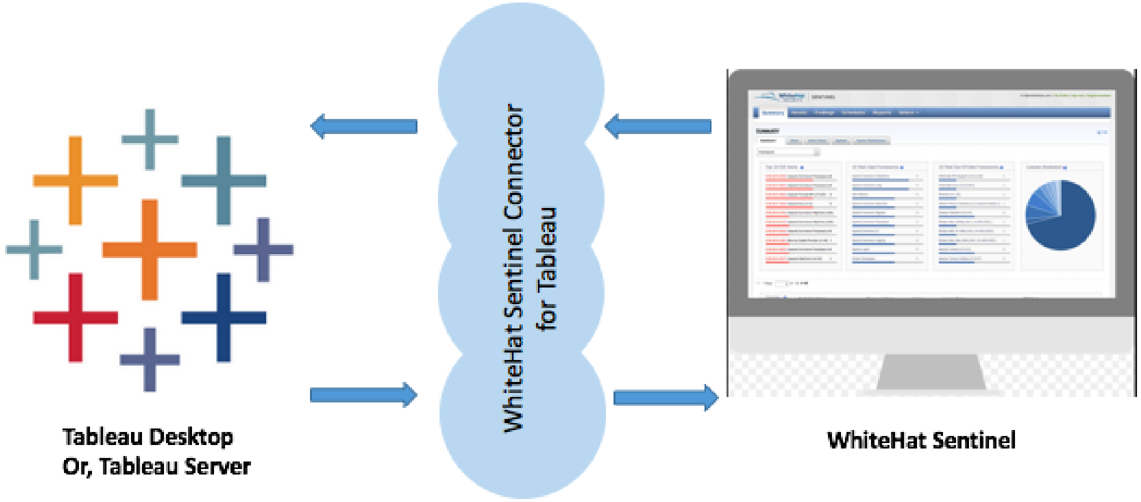
Prerequisites

To be able to use WhiteHat Sentinel Connector for Tableau, you will need the following:

- Tableau Desktop (Tableau license req'd)
- WhiteHat Sentinel Connector for Tableau (WhiteHat license req'd)
- One or more assets under Sentinel Service (WhiteHat license req'd)

The diagram below illustrates how the WhiteHat Sentinel Connector for Tableau works. It is available in the cloud and does not require users to download it to their own environment.

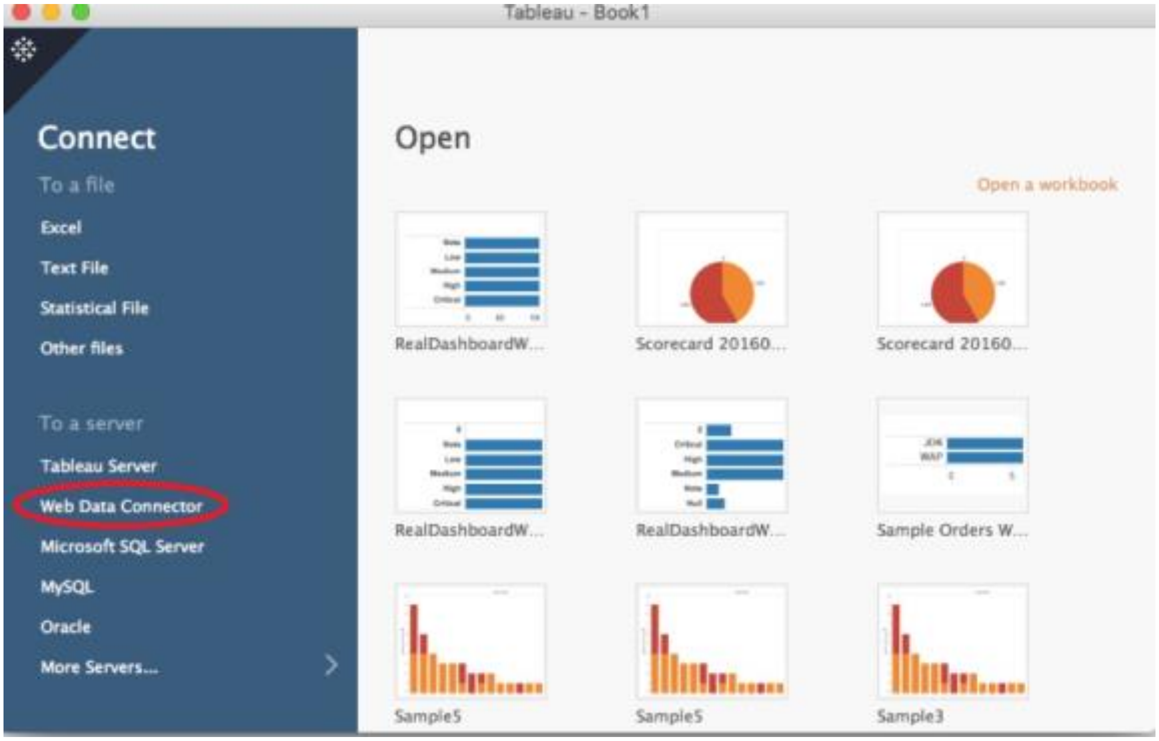
The WhiteHat Sentinel Tableau Connector makes API calls to Sentinel (using the API key the user enters) and receives data from Sentinel about the vulnerabilities and assets covered under Sentinel.



Using the Tableau Connector

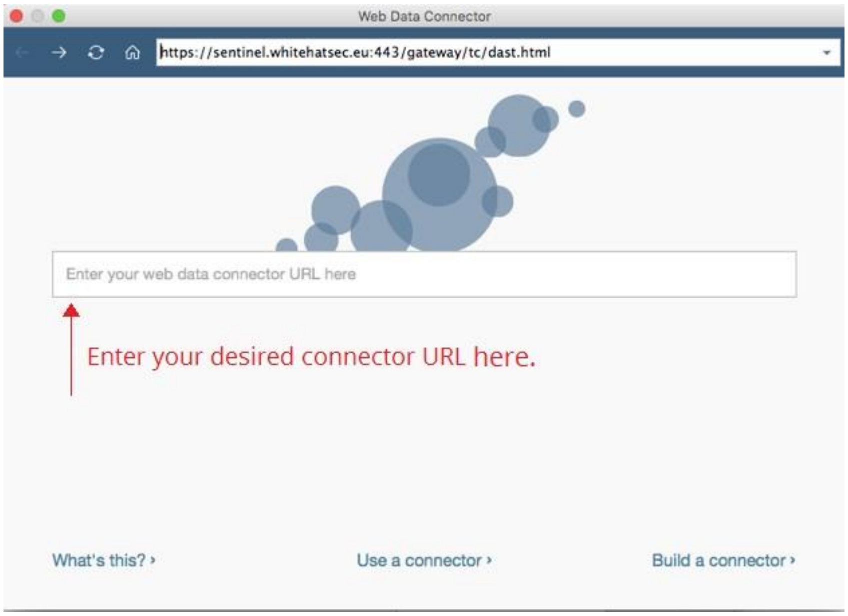
To begin using the Tableau Connector, follow these steps:

1. Start your Tableau application and click on "Web Data Connector."



(c) WhiteHat Security 2016

2. Enter the URL for the connector.



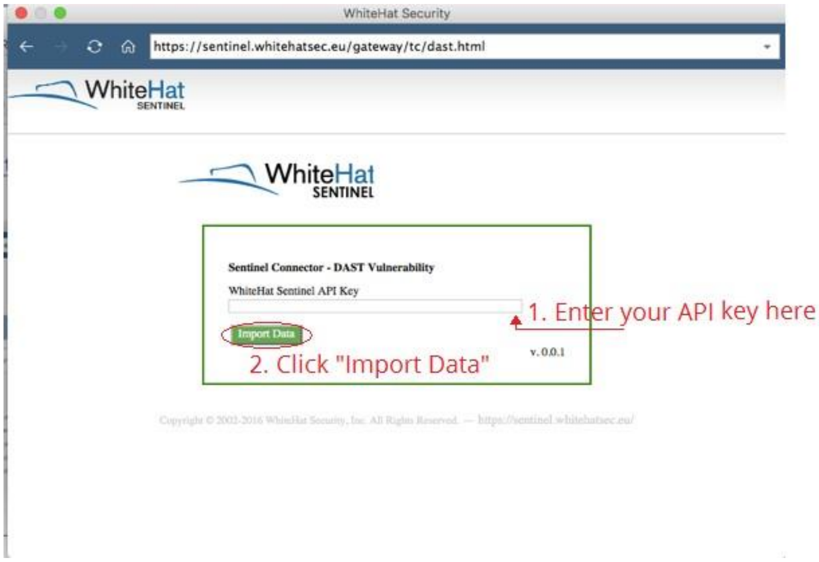
https://sentinel.whitehatsec.eu:443/gateway/tc/dast.html

Enter your desired connector URL here.

Sentinel offers the following connectors:

- DAST (Dynamic) Vulnerability Information:
    - US Customers: https://sentinel.whitehatsec.com/gateway/tc/dast.html
    - EU Customers: https://sentinel.whitehatsec.eu/gateway/tc/dast.html
- SAST (Source) Vulnerability Information:
    - US Customers: https://sentinel.whitehatsec.com/gateway/tc/sast.html
    - EU Customers: https://sentinel.whitehatsec.eu/gateway/tc/sast.html
- Asset Information:
    - US Customers: https://sentinel.whitehatsec.com/gateway/tc/asset.html
    - EU Customers: https://sentinel.whitehatsec.eu/gateway/tc/asset.html

3. Specify your API key.



WhiteHat Security

https://sentinel.whitehatsec.eu/gateway/tc/dast.html

Sentinel Connector - DAST Vulnerability

WhiteHat Sentinel API Key

1. Enter your API key here

2. Click "Import Data"

Copyright © 2002-2016 WhiteHat Security, Inc. All Rights Reserved. — https://sentinel.whitehatsec.eu/

Your API key is available from the Sentinel "My Profile" link; please see "About your Sentinel API Key" (below) or Getting Started with Sentinel for more information.

Using the Sample Dashboard Template

To use sample dashboard template provided by WhiteHat, download it from WhiteHat Security Customer portal under the [Documents and Tools]() tab.

- Customers using US version of Sentinel ([https://sentinel.whitehatsec.com)](https://sentinel.whitehatsec.com) will download the package "WHS Tableau Connector and Documentation (US)"
- Customers using EU version of Sentinel ([https://sentinel.whitehatsec.eu)](https://sentinel.whitehatsec.eu) will download "WHS Tableau Connector and Documentation (EU)"

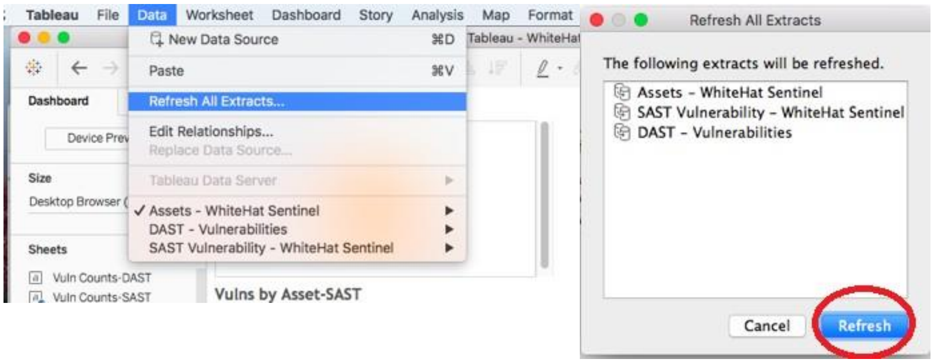
Unzip the files, which will include this document and the Tableau Connector and Dashboard Template.

> NOTE: the Sample Dashboard Template has been built with Tableau Desktop version 10.1

Once your download is complete and the files are unzipped, please refresh the Tableau Dashboard Template that is provided by WhiteHat:

1. Open the dashboard template, select the "Data" menu, and select "Refresh all Extracts." This will enable the "Refresh" button.

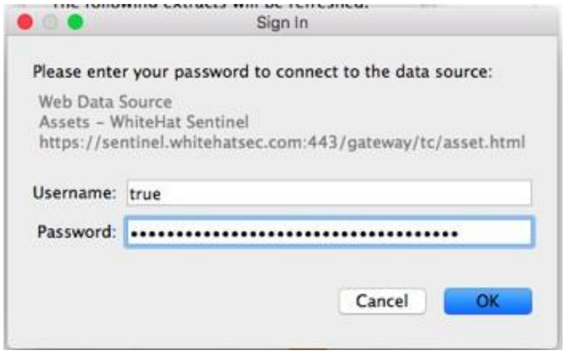
> NOTE: If you do not have a license for the Tableau Connector, you will not be able to refresh your extracts.



The following extracts will be refreshed.

Assets – WhiteHat Sentinel
SAST Vulnerability – WhiteHat Sentinel
DAST – Vulnerabilities

2. Click on "Refresh."
3. For each connector you want to refresh, enter your username and password if prompted: for Username enter "true" and for Password enter your API key. Click on OK.



Please enter your password to connect to the data source:

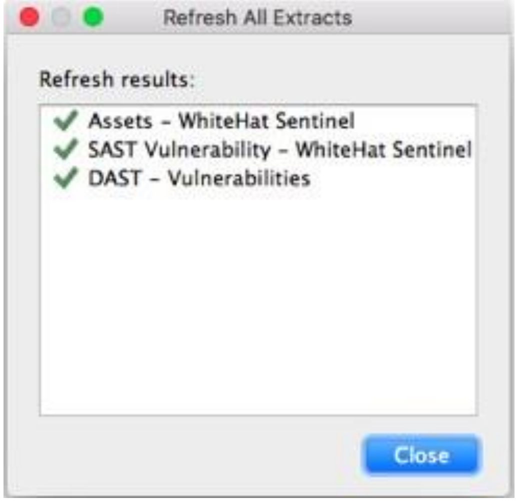
Web Data Source
Assets – WhiteHat Sentinel
https://sentinel.whitehatsec.com:443/gateway/tc/asset.html

Username: true

Password: ••

Repeat for each connector you want to refresh.

4. Once all connectors are refreshed, click on "Close."

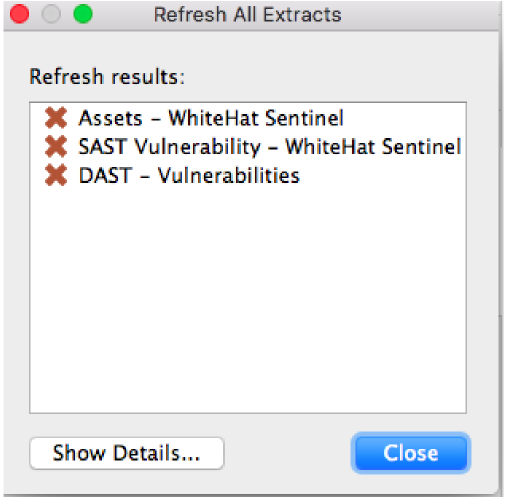


Refresh results:

✓ Assets – WhiteHat Sentinel
✓ SAST Vulnerability – WhiteHat Sentinel
✓ DAST – Vulnerabilities

Once this is done, the relevant Sentinel data can be extracted and you can save the dashboard changes. In the future, you can simply refresh all extracts from the data menu.

If you see the following error message, you do not have a Tableau license:



Refresh results:

✗ Assets – WhiteHat Sentinel
✗ SAST Vulnerability – WhiteHat Sentinel
✗ DAST – Vulnerabilities

Understanding the Fields in the Tableau Connector

Field Name	Description	Connector (s)
Asset ID	WhiteHat's unique identifier for the asset.	DAST/ SAST/ Asset
Asset Owner	Owner of the asset, as specified by the customer. This value will be empty if not specified.	DAST/ SAST/ Asset
Asset Phase	The asset phase may be set to Pre-production, Production, or Discontinued. This value will be empty if not specified.	DAST/ SAST/ Asset
Asset Type	Assets covered under Sentinel Dynamic testing are listed as "Site;" assets covered under Sentinel Source testing are listed	Asset
Closed	The date the vulnerability was closed, if any. For open vulnerabilities, this field is set to null.	DAST/ SAST
Class	The vulnerability class name	DAST/ SAST
Client ID	Unique identifier for the client to whom the asset belongs.	Asset
Custom Asset ID	Custom identifier for the asset, specified by the customer. This value will be empty if not specified.	DAST/ SAST/ Asset
Custom Risk	The custom risk rating set by the administrator, if any. If no custom rating has been set, this field will be null.	DAST/ SAST
Found	The date the vulnerability was found.	DAST/ SAST
Groups	Comma-separated list of the groups (by group name) to which the asset belongs.	Asset
Has Notes	If there are notes for this vulnerability, this field will be set to one (1). Other- wise, it will be zero (0).	DAST/ SAST
HREF	HREF	DAST/ SAST
Impact	The potential damage to your business if this vulnerability is exploited.	DAST/ SAST
Industry	Industry to which asset belongs. Industry field is available for sites only. Cus- tomers can modify industry setting by clicking on Edit Site Info button on site detail page.	Asset
Label	Site name	Asset
Likelihood	The risk that the vulnerability will be exploited.	DAST/ SAST
Modified	The date the vulnerability was modified, if any.	DAST/ SAST
Opened	The date the vulnerability was opened.	DAST/ SAST

Field Name	Description	Connector (s)
Rating	Specifies the risk associated with a vulnerability. If vulnerability risk rating has been customized, this field returns custom rating. If rating hasn't been customized, this field returns the risk rating assigned by WhiteHat. This is how numerical values map to various risk levels: 5 (critical), 4 (high), 3 (medium), 2 (low), or 1 (note).	DAST/ SAST
Retest State	This field shows the retest status (what sort of retest is available, whether a manual retest is in progress).	DAST/ SAST
Risk	The risk level WhiteHat has assigned to a vulnerability	DAST/ SAST
Service Level	Service level assigned to the asset on which the vulnerability was	DAST/ SAST
Site Name	Name of the Site.	DAST/ SAST
Status	Vulnerability status: Open, Closed, or Accepted.	DAST/ SAST
Tags	User-specified tags associated with an asset.	Asset
URL	URL at which the vulnerability exists	DAST/ SAST
Vuln ID	The unique identifier for a specific vulnerability	DAST/ SAST
WSI Global Rank	The WSI percentile in which this asset falls compared to the global	Asset
WSI Industry	The WSI percentile in which this asset falls compared to the rankings of other assets of that type in that industry.	Asset
WSI Score	WhiteHat Security Index score.	Asset

About your Sentinel API Key

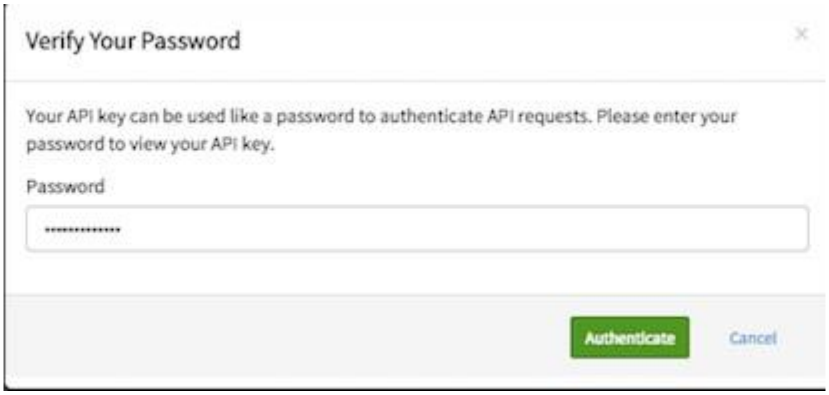
Each user account may generate a single unique 32-character Sentinel API Key, which functions to authenticate API requests. The Sentinel API key is intended for use inside the applications that are accessing the API. It is not intended for accessing the API through your browser.

Warning

Your API Key is exactly equivalent to your user name and password. Don’t write it down, don’t share it, and in all ways treat it exactly as you would a password. If someone else has your key, they will have access to your vulnerability information. WhiteHat Security Support will never ask for your API key.

Locating Your API Key

To see your API Key,select "View My API Key" in your profile. You will be asked to re-enter your password to view your API Key.



Verify Your Password

Your API key can be used like a password to authenticate API requests. Please enter your password to view your API key.

Password

•••••••••••••

Click on "Authenticate," and you will see a popup that contains your API Key.

Protecting Your API Key

Your API Key is the equivalent of a user name and password that gives access to all your vulner- ability data. Treat it as carefully as you would any business-critical password: do not write it down, do not share it, do not risk it leaving your hands at any time.

WhiteHat *strongly* recommends that you never use your Web API Key in your browser; it is only intended for use when accessing the API programmatically.

Moreover, if you use it directly in a URI, it is logged to your browser history. Therefore, if you *must* use your Web API Key in your browser, you are very strongly encouraged to clear your browser history/cache automatically every time you log out of Sentinel. Otherwise, your key will be visible to anyone who gets physical or electronic access to your browser history.

Note that to view your API key in "My Profile" you will need to enter your password.