Splunk® Enterprise Security
Administer Splunk Enterprise Security 7.0.1

Download a threat intelligence feed from the Internet in Splunk Enterprise Security

Generated: 6/13/2022 9:46 am

Download a threat intelligence feed from the Internet in Splunk Enterprise Security

In a Splunk Cloud Platform environment, all threat intelligence downloads (including taxii feeds) must contain URLs with the https:// protocol. URLs that do not use the https:// protocol are blocked in the Splunk Cloud Platform environment, which impacts downloading threat intelligence feeds. Additionally, the default threat intelligence feed called hailataxii_malware that uses a URL with the http:// protocol, http://hailataxii.com/taxii-data does not work in a Splunk Cloud Platform environment even if the URL is updated to use https://.

Splunk Enterprise Security can periodically download a threat intelligence feed available from the Internet, parse it, and add it to the relevant KV Store collections.

1. (Optional) Configure a proxy for retrieving threat intelligence.
2. Follow the procedure that matches the format of the threat source:
    - Add a URL-based threat source
    - Add a TAXII feed

If you manually disable a threat artifact in a collection, but the threat intelligence source provides the same indicator in a download again, then the entry in KVStore gets overwritten, and does not preserve your flag.

Configure a proxy for retrieving threat intelligence

If you use a proxy server to send threat intelligence to Splunk Enterprise Security, configure the proxy options for the threat source.

The user must correspond to the name of a Splunk secure stored credential in Credential Management. If you remove an existing proxy user and password in the Intelligence Download Setting editor, the download process no longer references the stored credentials. Removing the reference to the credential does not delete the stored credentials from Credential Management. See Manage credentials in Splunk Enterprise Security.

For more information on configuring proxy server settings, see Configure proxy server settings.

Add a URL-based threat source

Add a non-TAXII source of intelligence that is available from a URL on the Internet.

1. On the Enterprise Security menu bar, select **Configure > Data Enrichment >Threat Intelligence Management**.
2. Click **New** to add a new intelligence source.
3. Type a **Name** for the threat download. The name can only contain alphanumeric characters, hyphens, and underscores. The name cannot contain spaces.
4. Select or deselect the check box for **Is Threat Intelligence**.
5. (Optional) Select or deselect the check box for **Sinkhole**. Select the check box to delete the downloaded file after processing.
6. Type a **Type** for the threat download. The type identifies the type of threat indicator that the feed contains.
7. Type a **Description**. Describe the indicators in the threat feed.
8. Type an integer to use as the **Weight** for the threat indicators. Enterprise Security uses the weight of a threat feed to calculate the risk score of an asset or identity associated with an indicator on the threat feed. A higher weight indicates an increased relevance or an increased risk to your environment.
9. (Optional) Change the default download **Interval** for the threat feed. Defaults to 43200 seconds, or every 12

hours.

10. (Optional) Type POST arguments for the threat feed. You can use POST arguments to retrieve user credentials from Credential Management. Use the format `key=$user:<username>$` or `key=$user:<username>,realm:<realm>$` to specify a username and realm.
11. (Optional) Type a **Maximum age** to define the retention period for this threat source, defined in relative time. Enable the corresponding saved searches for this setting to take effect. See Configure threat source retention. For example, `-7d`. If the time that the feed was last updated is greater than the maximum age defined with this setting, the threat intelligence modular input removes the data from the threat collection.
12. (Optional) If you need to specify a custom **User agent** string to bypass network security controls in your environment, type it in the format `<user-agent>/<version>`. For example, `Mozilla/5.0` or `AppleWebKit/602.3.12`. The value in this field must match this regex: `([A-Za-z0-9_.-]+)/([A-Za-z0-9_.-]+)`. Check with your security device administrator to ensure the string you type here is accepted by your network security controls.
13. Fill out the **Parsing Options** fields to make sure that your threat list parses successfully. You must fill out either a delimiting regular expression or an extracting regular expression. You cannot leave both fields blank.

Field	Description	Example
Delimiting regular expression	A regular expression string used to split, or delimit, lines in an intelligence source. For complex delimiters, use an extracting regular expression.	`,` or `:` or `\t`
Extracting regular expression	A regular expression used to extract fields from individual lines of a threat source document. Use to extract values in the threat source.	`^(\S+)\t+(\S+)\t+\S+\t+\S+\t*(\S*)`
Fields	Required if your document is line-delimited. Comma-separated list of fields to be extracted from the threat list. Can also be used to rename or combine fields. Description is a required field. Additional acceptable fields are the fields in the corresponding KV Store collection for the threat intelligence, visible in the local lookup files or the `DA-ESS-ThreatIntelligence/collections.conf` file. Defaults to `description:$1,ip:$2`.	`<fieldname>:$<number>,<field name>.$<number>` `ip:$1,description:domain_blocklist`
Ignoring regular expression	A regular expression used to ignore lines in a threat source. Defaults to ignoring blank lines and comments beginning with #.	`^\s*$)`
Skip header lines	The number of header lines to skip when processing the threat source.	`0`
Intelligence file encoding	If the file encoding is something other than ASCII or UTF8, specify the encoding here. Leave blank otherwise.	latin1

14. (Optional) Change the **Download Options** fields to make sure that your threat list downloads successfully.

Field	Description	Example
Retry interval	Number of seconds to wait between download retry attempts. Review the recommended poll interval of the threat source provider before changing the retry interval.	60
Remote site user	If the threat feed requires authentication, type the user name to use in remote authentication, if required. The user name you add in this field must match the name of a credential in Credential Management. See Manage input credentials in Splunk Enterprise Security.	buttercup
Remote site user realm	If the threat feed requires authentication, type the user name to use in remote authentication, if required. The realm you add in this field must match the realm of a credential in Credential Management. See Manage input credentials in Splunk Enterprise Security.	paddock
Retries	The maximum number of retry attempts.	3
Timeout	Number of seconds to wait before marking a download attempt as failed.	30

15. (Optional) If you are using a proxy server, fill out the **Proxy Options** for the threat feed. See Configure a proxy for retrieving threat intelligence.
16. Save your changes.

Next step

To add another custom threat source, see Add threat intelligence to Splunk Enterprise Security and follow the link that matches the source that you want to add.

If you are finished adding threat intelligence sources, see Verify that you have added threat intelligence successfully in Splunk Enterprise Security.

Add a TAXII feed

Add threat intelligence provided as a TAXII feed to Splunk Enterprise Security.

Prerequisite

Determine whether the TAXII feed requires certificate authentication. If it does, add the certificate and keys to the same app directory in which you define the TAXII feed. For example, DA-ESS-ThreatIntelligence.

1. Follow the steps to add a new certificate to Splunk Enterprise Security to add both the certificate and the private key files. See Manage credentials in Splunk Enterprise Security.
2. Follow the steps for adding a TAXII feed to Splunk Enterprise Security, using the `cert_file` and `key_file` POST arguments to specify the file names of the certificate and private key file.

Steps

1. On the Enterprise Security menu bar, select **Configure** > **Data Enrichment > Threat Intelligence Management**.
2. Click **New** to add a new TAXII feed.
3. Type a **Name** for the threat intelligence feed.
4. Type a **Description** and **URL** for the threat intelligence field.
5. Verify that the check box for **Is Threat Intelligence** is selected.
6. (Optional) Select or deselect the check box for **Sinkhole**. Select the check box to delete the downloaded file after processing. The sinkhole option works for anything in the pickup directory that has been processed. The pickup directories follow:
   ```
   $SPLUNK_HOME/etc/apps/SA-ThreatIntelligence/local/data/threat_intel
   $SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel
   $SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel
   $SPLUNK_HOME/etc/apps/<custom>
   ```
7. Type a **Type** of **taxii**.
8. Type a **Description** for the threat intelligence feed.
9. Type a URL to use to download the TAXII feed.
10. (Optional) Change the default **Weight** for the threat intelligence feed. Increase the weight if the threats on the threat feed are high-confidence and malicious threats that should increase the risk score for assets and identities that interact with the indicators from the threat source.
11. (Optional) Adjust the interval at which to download the threat intelligence. Defaults to 43200 seconds, or twice a day.
12. Type TAXII-specific space-delimited **POST arguments** for the threat intelligence feed.
    ```
    <POST argument>="<POST argument value>"
    ```

Example POST argument	Description	Example

collection	Name of the data collection from a TAXII feed.	`collection="A_TAXII_Feed_Name"`
earliest	The earliest threat data to pull from the TAXII feed.	`earliest="-1y"`
taxii_username	An optional method to provide a TAXII feed username.	`taxii_username="user"`
taxii_password	An optional method to provide a TAXII feed password. If you provide a username without providing a password, the threat intelligence modular input attempts to find the password in Credential Management. See Manage credentials in Splunk Enterprise Security.	`taxii_password="password"`
taxii_username_realm	An optional method to provide a realm for the TAXII feed username. Used with the `taxii_username` to locate the user credential password in Credential Management.	`taxii_username_realm="realm"`
cert_file	Add the certificate file name if the TAXII feed uses certificate authentication. The file name must match exactly and is case sensitive.	`cert_file="cert.crt"`
key_file	Add the key file name for the certificate if the TAXII feed uses certificate authentication. The file name must match exactly and is case sensitive.	`key_file="cert.key"`

13. TAXII feeds do not use the **Maximum age** setting. To configure file retention for TAXII files, see Configure intelligence file retention.
14. TAXII feeds do not use the **User agent** setting.
15. TAXII feeds do not use the **Parsing Options** settings.
16. (Optional) Change the **Download Options**.
17. (Optional) Change the **Proxy Options**. See Configure a proxy for retrieving threat intelligence.
18. Save the changes.

You cannot use an authenticated proxy with a TAXII feed because the libtaxii library used by Enterprise Security does not support authenticated proxies. If possible, use an unauthenticated proxy instead.

Next step

To add another custom threat source, see Add threat intelligence to Splunk Enterprise Security and follow the link that matches the source that you want to add.

If you are finished adding threat intelligence sources, see Verify that you have added threat intelligence successfully in Splunk Enterprise Security.