Splunk® Enterprise Security
Administer Splunk Enterprise Security 7.0.1

Configure global threatlist settings to retrieve threat intelligence

Generated: 6/13/2022 9:46 am

Configure global threatlist settings to retrieve threat intelligence

Use the Splunk Enterprise app UI to configure global threatlist settings to extract value from your intelligence data and transform the data based on your requirements.

Configure proxy server settings

If you use a proxy server to send intelligence to Splunk Enterprise Security, you must apply the same proxy server settings to all the `[threatlist]` stanzas in the `inputs.conf` configuration file. Use Splunk Enterprise Security UI to configure the proxy server settings for all `[threatlist]` stanzas.

Steps

1. From the Enterprise Security menu bar, select **Configure > Data Enrichment > Threat Intelligence Management**. This displays the list of downloaded intelligence documents in the app that are sorted by Interval, Type, URL, Weight, and Status.
2. Click on the **Global Settings** tab.
   This displays the panel to configure the proxy server settings.
3. Use the following table to configure the proxy server settings:

Setting	Description	Example
Proxy Server	Proxy server IP address	The Proxy Server cannot be a URL. For example, `10.10.10.10` or `server.example.com`.
Proxy Port	Port to access the proxy server	`8956`
Proxy User	Proxy user credential for the proxy server.	Only basic and digest authentication methods are supported. The user must correspond to the name of a credential stored in Credential Management. This is a required field.
Proxy User Realm	Splunk Enterprise Security secure storage realm of the corresponding proxy user. Used to build the ID of the Splunk Enterprise secure storage array.	(Optional) This value is different from remote site credentials.

For more information on configuring a proxy, see Configure a proxy for retrieving intelligence.

Configure parse modifier settings

When threat intelligence data is ingested, fields are often embedded within each other. By configuring threatlist settings you can separate the fields. Extraction of field and their corresponding values is based on when threat documents are processed and written to their respective threat collections. Configure parse modifier settings to extract fields from the threat intelligence data.

Steps

1. From the Enterprise Security menu bar, select **Configure > Data Enrichment > Threat Intelligence Management > Sources**. This displays the list of downloaded intelligence documents in the app that are sorted by Interval, Type, URL, Weight, and Status.
2. Click on the **Global Settings** tab.
   This displays the **Parse Modifier settings** panel.
   You have the option to enable any of the following parse modifier settings:
   - ♦ **Certificate Attribute Breakout**

    - **IDNA Encode Domains**
    - **Parse Domain from URL**
3. Enable the parse modifier setting based on your requirements. Enable **Certificate Attribute Breakout** to parse fields in the `certificate_issuer` and the `certificate_subject` fields.
   For example: A raw certificate issuer field may be a single string as follows:
   `C = US, ST = CA, L = San Francisco, O = The Company Name, OU = The Organizational Unit Name, CN = The common name, emailAddress = theemailaddress@email.gov, STREET=123 main street`
   Multiple other potential fields may exist within this single string. When you parse fields in the `certificate_issuer` fields by enabling the **Certificate Attribute Breakout** parse modifier, all extra fields are parsed from the raw `certificate_issuer` field and stored into their own fields in the collection as follows:
    - 'certificate_issuer_common_name': 'The common name',
    - 'certificate_issuer_email': 'theemailaddress@email.gov',
    - 'certificate_issuer_locality': 'San Francisco',
    - 'certificate_issuer_organization': 'The Company Name',
    - 'certificate_issuer_state': 'CA',
    - 'certificate_issuer_street': '123 main street',
    - 'certificate_issuer_unit': 'The Organizational Unit Name'

   When you parse fields in the the `certificate_subject field` fields by enabling the **Certificate Attribute Breakout** parse modifier, parsing occurs as follows:
    - 'certificate_subject_common_name': 'The common name',
    - 'certificate_subject_email': 'theemailaddress@email.gov',
    - 'certificate_subject_locality': 'San Francisco',
    - 'certificate_subject_organization': 'The Company Name',
    - 'certificate_subject_state': 'CA',
    - 'certificate_subject_street': '123 main street',
    - 'certificate_subject_unit': 'The Organizational Unit Name'

   If you want to transform the names written in non-ASCII characters to their ASCII-based representation, you may enable **IDNA Encode Domains**. Enable **IDNA Encode Domains** to include both the IDNA and the international encoding for applicable domains in the `domain` field.
   If you want to extract a hostname from a URL, you may enable **Parse Domain from URL**. Enable the **Parse Domain from URL** to parse the `domain` field form the `url` field.