Splunk® Enterprise Security
Administer Splunk Enterprise Security 7.0.1

Configure the intelligence sources included with Splunk Enterprise Security

Generated: 4/21/2022 9:09 am

Configure the intelligence sources included with Splunk Enterprise Security

Splunk Enterprise Security includes several intelligence sources that retrieve information across the Internet.

The following generic or non threat intelligence sources are enabled by default:

- Mozilla Public Suffix List
- MITRE ATT&CK Framework
- ICANN Top-level Domains List

Review the types of intelligence provided by the sources, and determine if the included intelligence is useful to your team before enabling specific sources.

Prerequisites

- Your Splunk Enterprise deployment must be connected to the Internet. If your deployment is not connected to the Internet, disable these sources or source them in an alternate way.
- To set up firewall rules for these sources, you might want to use a proxy server to collect the intelligence before forwarding it to Splunk Enterprise Security and allow the IP address for the proxy server to access Splunk Enterprise Security. The IP addresses for these sources can change.

Steps

1. From the Enterprise Security menu bar, select **Configure > Data Enrichment > Threat Intelligence Management**.
2. Review the **Description** field for all defined intelligence sources to learn more about the types of information or threat indicators that can be correlated with your events.
3. Enable the intelligence sources that fit your security use cases.
4. Configure the enabled intelligence sources that fit your security use cases, using the links to the source websites to review the source provider's documentation. Each source website provides suggestions for polling intervals and other configuration requirements separate from Splunk Enterprise Security.

Splunk Enterprise Security expects all intelligence sources to send properly-formatted data and valuable intelligence information. Feed providers are responsible for malformed data or false positives that might be identified in your environment as a result.

If you determine that your Splunk Enterprise Security installation is retrieving data from unexpected IP addresses, perform a WHOIS or nslookup to determine if the IP address matches that of one of the intelligence sources configured in your environment.

Next step

To add a 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 intelligence sources, see Verify that you have added intelligence successfully in Splunk Enterprise Security.

Included threat intelligence sources

The threat intelligence sources are parsed for threat indicators and added to the relevant KV Store collections.

Threat source	Threat list provider	Website for the threat source
Emerging Threats compromised IPs blocklist	Emerging Threats	https://rules.emergingthreats.net/blockrules
Emerging Threats firewall IP rules	Emerging Threats	https://rules.emergingthreats.net/fwrules
Malware domain host list	Hail a TAXII.com	http://hailataxii.com
iblocklist Logmein	I-Blocklist	https://www.iblocklist.com/lists
iblocklist Piratebay	I-Blocklist	https://www.iblocklist.com/lists
iblocklist Proxy	I-Blocklist	https://www.iblocklist.com/lists
iblocklist Rapidshare	I-Blocklist	https://www.iblocklist.com/lists
iblocklist Spyware	I-Blocklist	https://www.iblocklist.com/lists
iblocklist Tor	I-Blocklist	https://www.iblocklist.com/lists
iblocklist Web attacker	I-Blocklist	https://www.iblocklist.com/lists
Phishtank Database	Phishtank	https://www.phishtank.com/
SANS blocklist	SANS	https://isc.sans.edu

Some of the feeds may require subscription.

Included generic intelligence sources

Splunk Enterprise Security also includes generic intelligence that is not added to the threat intelligence KV Store collections and are instead used to enrich data in Splunk Enterprise Security.

Data list	Data provider	Website for data provider
Cisco Umbrella 1 Million Sites	Cisco	https://umbrella.cisco.com/blog/2016/12/14/cisco-umbrella-1-million/
ICANN Top-level Domains List	IANA	https://data.iana.org/TLD/
MaxMind GeoIP ASN IPv4 database	MaxMind	https://dev.maxmind.com/geoip/geoip2/geoip2-anonymous-ip-csv-database/
MaxMind GeoIP ASN IPv6 database	MaxMind	https://dev.maxmind.com/geoip/geoip2/geoip2-anonymous-ip-csv-database/
Mozilla Public Suffix List	Mozilla	https://publicsuffix.org
Mitre Att&ck	Mitre	https://attack.mitre.org/

You can configure the generic intelligence source to use for top one million sites:

1. From the Splunk ES menu bar, select **Configure > General > General Settings**
2. Scroll down to Top 1M Site Source and select **Cisco**.