Splunk® Security Essentials
Install and Configure Splunk Security Essentials 3.6.0

Generated: 9/19/2022 1:28 pm

Table of Contents

Splunk Security Essentials

Overview of Splunk Security Essentials

Splunk Security Essentials is a free Splunk app that helps you find security procedures that fit your environment, learn how they work, deploy them, and measure your success. Splunk Security Essentials has over 120 correlation searches and is mapped to the Kill Chain and MITRE ATT&CK framework. Within the app, there are detections with line-by-line SPL documentation that show why certain search commands are used and include context such as the security impact, implementation, and response. The app also includes content from Splunk Enterprise Security, Splunk Enterprise Security Content Update, and Splunk User Behavior Analytics.

To get started with Splunk Security Essentials, perform the following tasks:

- Install Splunk Security Essentials from a single-instance or distributed deployment. See Install Splunk Security Essentials.
- Configure Splunk Security Essentials by mapping data sources, running content introspection, and use the Data Source Check dashboard to verify if data sources exist for examples. See Configure Splunk Security Essentials.

Share data in Splunk Security Essentials

When Splunk Security Essentials is deployed on Splunk Enterprise or Splunk Cloud Platform, the Splunk platform sends anonymized usage data to Splunk Inc. ("Splunk") to help improve Splunk Security Essentials in future releases. For information about how to opt in or out, and how the data is collected, stored, and governed, see Share data in Splunk Enterprise in the Splunk Enterprise *Admin Manual*.

How data is collected

If you opt in globally on your Splunk Enterprise or Splunk Cloud Platform environment, Splunk Security Essentials enables an internal library to track basic usage and crash information. The library uses browser cookies to track unique visitors to the app, sessions, and sends events to Splunk using XHR in JSON format, with all user or system-identifying data resolved to GUIDs.

What data is collected

Splunk Security Essentials collects the following basic usage information:

Event	Description	Example
Example Opened	Reports that an example was opened.	`{status: "exampleLoaded", exampleName: "New Interactive Logon from a Service Account", searchName: "New Interactive Logon from a Service Account - Demo"}`
SPL Viewed	Reports that the SPL for an example was viewed.	`{status: "SPLViewed", name: "New Interactive Logon from a Service Account - Demo"}`
Schedule Search (Started)	Reports that an alert was scheduled.	`{status: "scheduleAlertStarted", name: "New Interactive Logon from a Service Account - Demo"}`

Event	Description	Example
Schedule Search (Finished)	Reports that an alert was scheduled.	{status: "scheduleAlertCompleted", searchName: "New Interactive Logon from a Service Account - Demo"}
Doc Loaded	Reports that an onboarding guide was opened.	{status: "docLoaded", pageName: "Windows Security Logs"}
Filters Updated	Reports that filters were updated to filter for specific examples.	{status: "filtersUpdated", name: "category", value: "Account_Sharing", enabledFilters: ["journey", "usecase", "category", "datasource", "highlight"]}
Selected Intro Use Case	Reports that from the home page, a use case was clicked on.	{status: "selectedIntroUseCase", useCase: "Security Monitoring"}
Added to Bookmark	Reports that an example was bookmarked.	{status: "BookmarkChange", name: "Basic Malware Outbreak", itemStatus: "needData"}
Data Foundation Configuration	Reports that available data sources were either configured or introspected.	{status: "DataStatusChange", category: "DS010NetworkCommunication-ET01Traffic", status: "good", selectionType: "manual"}
Custom Content Created	Reports that custom content was created.	{status: "CustomContentCreated", mitre_technique: "T1046"}
Unexpected Error Occurred	Reports that an error occurred.	{status: "ErrorOcurred", banner: "Got an error while trying to update the kvstore. Your changes may not be saved.", msg: "Access Denied", locale: "en-US", anon_url: "https://â ¦â ¦../en-US/app/Splunk_Security_Essentials/contents", page: "contents", splunk_version: "7.3.1"}

Splunk Security Essentials product compatibility matrix

Verify the version compatibility among the products in the table.

Splunk Security Essentials	Splunk Cloud Platform	Splunk Enterprise
3.4.0	8.2.2111 8.2.2112	8.2.3 8.1.7 8.1.6 8.0.9.2
3.5.0	8.2.211 8.2.2112.1 8.1.2103.3	8.2.4 8.1.9
3.5.1	8.2.2202 8.2.2112.1 8.2.211	8.2.4 8.1.9
3.6.0		

Splunk Security Essentials	Splunk Cloud Platform	Splunk Enterprise
	8.2.2203.2 8.2.2202.1	9.0.0 8.2.5

Install Splunk Security Essentials

Install Splunk Security Essentials

You can install the Splunk Security Essentials app on Splunk Cloud Platform, or you can install it on Splunk Enterprise in a single-instance or distributed environment.

Splunk Security Essentials doesn't interfere with or impact Splunk Enterprise Security. You can safely install Splunk Security Essentials on a Splunk Enterprise Security search head or search head cluster.

Prerequisites

Make sure Splunk Security Essentials is compatible with the version of Splunk Enterprise or Splunk Cloud Platform that you're using. See https://splunkbase.splunk.com/app/3435/ to find the updated compatibility for various Splunk Enterprise, Splunk Cloud Platform, and Splunk Security Essentials versions.

Install on a Splunk Enterprise single-instance deployment

In a single-instance deployment, you can install Splunk Security Essentials on your Splunk Enterprise search head using Splunk Web or a downloaded file.

Install the app using Splunk Web

1. Log in to your Splunk Enterprise search head.
2. In the Applications menu, select **Find More Apps**.
3. On the Browse More Apps page, select or search for Splunk Security Essentials and click **Install**.
4. Enter your splunk.com credentials.
5. Accept the license terms.
6. Click **Login and Install**.
7. Click **Done**.
8. Restart Splunk Enterprise to complete the installation.

Install the app from a downloaded file

1. Log in to splunkbase.splunk.com.
2. Search for and download the Splunk Security Essentials app and save it to an accessible location.
3. Log in to your Splunk Enterprise search head.
4. On the Apps menu, click **Manage Apps**.
5. On the Apps page, click **Install app from file**.
6. On the Upload app page, click the **Choose file** button and locate the app in your files.
7. Click **Upload**.
8. Click **Done**.
9. Restart Splunk Enterprise to complete the installation.

Install on a Splunk Enterprise distributed deployment

In a distributed deployment, install Splunk Security Essentials on search heads only. This app is safe to install in large clusters because it has no impact on indexers. For installation instructions, see Install an add-on in a distributed Splunk Enterprise deployment in the *Splunk Add-ons* menu.

Install on Splunk Cloud Platform

You can install Splunk Security Essentials on your Splunk Cloud Platform deployment. For more information, see Install apps in your Splunk Cloud Platform deployment in the *Splunk Cloud Platform Admin Manual*.

Configure Splunk Security Essentials

Configure Splunk Security Essentials

After you install Splunk Security Essentials, complete these tasks to ensure that Splunk Security Essentials works as intended. These tasks are listed in order in the **Set Up** menu in Splunk Security Essentials.

Checklist of tasks to configure Splunk Security Essentials

Complete the following tasks in the order they are listed to configure Splunk Security Essentials.

Step number	Task	Description	Documentation
1	Map data sources using Data Inventory Introspection.	Map data sources in Splunk Security Essentials using Data Inventory Introspection so that Splunk Security Essentials can assess your available data.	See Configure the products you have in your environment with the Data Inventory dashboard in *Use Splunk Security Essentials*.
2	Run Content Introspection.	Run Content Introspection to find content that you have already created such as searches or alerts and either map that content in Splunk Security Essentials, or define new content. Content Introspection also needs to be configured before you can use the MITRE ATT&CK dashboard.	See Track active content in Splunk Security Essentials using Content Introspection in *Use Splunk Security Essentials*.
3	Review the App Configuration.	Review or customize app configuration to ensure Splunk Security Essentials is setup correctly.	See Customize Splunk Security Essentials in *Use Splunk Security Essentials*.
4 (Optional)	Create Posture Dashboards.	In Splunk Security Essentials, create security posture dashboards to see overview dashboards of all your security content in Splunk Security Essentials.	See Create security posture dashboards in *Use Splunk Security Essentials*.

Edit permissions to provide write access to Splunk Security Essentials

All users of Splunk Security Essentials have read access to the various features, but if you want to allow a user to change or edit specific configurations you must grant write access to certain lookups. To grant write access to a lookup, you must be an administrative user and follow these steps:

1. Navigate to your Splunk Platform instance.
2. Click **Settings > All configurations**
3. Select **Splunk Security Essentials** from the **App** drop-down menu.
4. Search for the name of the lookup that you want to edit the permissions for and click **Permissions**.
5. Find the user that you want to change the access for and select **Write** access.
6. Click **Save**.

Lookups in Splunk Security Essentials

The following are important lookups in Splunk Security Essentials that you might want to edit the permissions for to allow a user to change configurations for data inventory, custom content, bookmarks, and so on.

Data Inventory lookups

Lookup name	External type	Description
`data_inventory_products_lookup`	kvstore	This kvstore collection contains a list of all the products configured for data availability. There is an entry for each product with associated metadata, the location of the data, and the data source categories this product is mapped to. The mapped data source categories are stored in the `eventtypeIds` field. For more information on data availability, see Track data ingest latency with the Data Availability dashboard in *Use Splunk Security Essentials*.
`data_inventory_eventtypes_lookup`	kvstore	This kvstore collection stores the status for each data source category. The mapped data source categories are stored in the `eventtypeIds` field.

Posture Dashboard lookups

Lookup name	External type	Description
`data_source_check_outputs_lookup`	kvstore	This lookup is deprecated.
`data_source_check_lookup`	kvstore	This lookup is used by the Data Source Check dashboard and shows the most recent result from Data Source Check. For more information on the Data Source Check dashboard, see Check data sources with the Data Source Check dashboard in *Use Splunk Security Essentials*.

Bookmarks

Lookup name	External type	Description
`bookmark_lookup`	kvstore	This lookup is a kvstore collection that stores the bookmark status and bookmark notes. The Content Search Introspection feature provides information to this lookup. For more information, see Track your content with the Manage Bookmarks dashboard in *USe Splunk Security Essentials*.
`bookmark_names`	kvstore	This collection allows you to add your own custom bookmark names on top of the standard ones. You can also rename the existing labels.

Content Updates

Lookup name	External type	Description
`external_content_lookup`	kvstore	Splunk Security Essentials has a collection of external content sources that can be updated. This includes automatically adding the latest data from the Splunk Enterprise Security Content Update (ESCU) app and adding the latest available MITRE ATT&CK information. Partners also have the option to add or create content channels.
`sse_json_doc_storage_lookup`	kvstore	Splunk Security Essentials has a collection of external content sources that can be updated. MITRE ATT&CK information is currently stored here, but it could be used for any other sources. When your browser grabs the latest MITRE ATT&CK JSON from the MITRE GitHub, it adds it to this kvstore collection.

Custom Content

Lookup name	External type	Description
`custom_content_lookup`	kvstore	Custom content is stored in the `custom_content_lookup`. Most information is stored in the JSON field, and as the custom content page loads, all of that content is loaded

Lookup name	External type	Description
		into the ShowcaseInfo lookup. For more information on custom content, see Customize Splunk Security Essentials with the Custom Content dashboard.
`deleted_custom_content_lookup`	kvstore	In the Custom Content dashboard, you can delete content but then recover it via the recycling bin. This lookup is that recycling bin.

Content Introspection

Lookup name	External type	Description
`local_search_mappings_lookup`	kvstore	If you choose to use content introspection, Splunk Security Essentials retains a connection of local saved searches to MITRE ATT&CK details. This lookup stores the association of a saved search name, search_title, to the internal `showcaseId`. For more information, see Track active content in Splunk Security Essentials using Content Introspection in *Use Splunk Security Essentials*.

Splunk Enterprise Security enrichment

Lookup name	External type	Description
`sse_content_exported_lookup`	kvstore	This lookup contains the names of local saved searches and enrichment fields in Splunk Security Essentials that are connected to notable events in Splunk Enterprise Security. This lookup is automatically maintained by Splunk Security Essentials and updated whenever there is an entry in the `local_search_mappings_lookup`.

Backup and Restore

Lookup name	File name	Description
`sse_bookmark_backup`	sse_bookmark_backup.csv	All configuration backups are stored in this CSV file.

Analytics Advisor

Lookup name	File name	Description
`mitre_threat_groups`	mitre_threat_groups.csv	This lookup contains a list view of the current MITRE ATT&CK Framework threat groups. It is automatically maintained by Splunk Security Essentials and updated whenever MITRE ATT&CK is updated.
`mitre_enterprise_list`	mitre_enterprise_list.csv	This lookup contains the list version of the entire MITRE ATT&CK enterprise matrix and is used for enrichment in Splunk Security Essentials. It can also be used for ad-hoc lookups to enrich events with MITRE ATT&CK data. It is automatically maintained by Splunk Security Essentials and updated whenever MITRE ATT&CK is updated.
`mitre_environment_count`	mitre_environment_count.csv	This lookup contains the count of content associated with each MITRE ATT&CK technique. It is automatically maintained by Splunk Security Essentials and updated when you load the MITRE ATT&CK Overview dashboard.