Splunk® Security Essentials
Install and Configure Splunk Security Essentials

Generated: 1/14/2021 12:38 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, 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 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://??../en-US/app/Splunk_Security_Essentials/contents", page: "contents", splunk_version: "7.3.1"}

Install Splunk Security Essentials

Install Splunk Security Essentials

Install the Splunk Security Essentials app in a single-instance or distributed Splunk Enterprise environment. Splunk Security Essentials is compatible with Splunk Enterprise versions 7.1, 7.2, 7.3, 8.0, and 8.1.

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.

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.

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

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

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	Use the Data Source Check dashboard to verify if data sources exist for examples.	In Splunk Security Essentials, every example has defined prerequisites to help you know if a search works in your environment. You can verify if the data sources exist for examples using the Data Source Check dashboard.	See Check data sources with the Data Source Check dashboard in *Use Splunk Security Essentials*.