Splunk® Security Essentials
Use Splunk Security Essentials 3.6.0

Generated: 9/26/2022 11:35 am

Copyright (c) 2022 Splunk Inc. All Rights Reserved

Table of Contents

Introduction

About the Splunk Security Essentials app

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.

Use Splunk Security Essentials to perform the following tasks:

- Review available content and the 120 plus detection searches to find the capabilities most relevant to you, see Review your content with the Security Content page in *Use Splunk Security Essentials*.
- Add custom content, see Customize Splunk Security Essentials with the Custom Content dashboard in *Use Splunk Security Essentials*.
- Use the Risk-based Alerting Content Recommendation dashboard to see potentially risky events in one place, see Gather events with the Risk-based Alerting dashboard in *Use Splunk Security Essentials*.
- View the MITRE ATT&CK coverage in your environment, see The MITRE ATT&CK Framework dashboard in *Use Splunk Security Essentials*.
- View the cyber kill chain coverage in your environment, see The Cyber Kill Chain dashboard in *Use Splunk Security Essentials*.
- Aggregate risk attributions, see Aggregate risk attributions with the Analyze ES Risk Attributions dashboard in *Use Splunk Security Essentials*.
- Check if your data is CIM compliant, see Check if your data is CIM-compliant with the Common Information Model Compliance Check dashboard in *Use Splunk Security Essentials*.
- Track active content, see Track active content in Splunk Security Essentials using Content Introspection in *Use Splunk Security Essentials*.

Get started using Splunk Security Essentials

Filtering procedures by security maturity in Splunk Security Essentials

Splunk Security Essentials offers default procedures for a variety of security use cases and for every stage of the security journey. The procedures provide a way to start ingesting your data into Splunk Enterprise and monitoring useful metrics within your environment. For more information on available procedures, see Review your content with the Security Content page.

Security maturity journey stages

There are six stages of security maturity. Go to **Security Content > Journey** to see the journey stages and to filter the procedures available at each stage. The following table describes the six stages:

Stage	Description
1. Collection	Collect basic security logs and other machine data from your environment.
2. Normalization	Apply a standard security taxonomy and add asset and identity data.
3. Expansion	Collect additional high fidelity data sources like endpoint activity and network metadata to drive advanced attack detection.
4. Enrichment	Augment security data with intelligence sources to better understand the context and impact of an event.
5. Automation and Orchestration	Establish a consistent and repeatable security operation capability.
6. Advanced Detection	Apply sophisticated detection mechanisms, including machine learning.

Search in Splunk Security Essentials

Splunk Security Essentials uses time series searches to detect spikes, first time seen searches to detect new values, and general Splunk searches. For more information on searching in Splunk, see the Search Tutorial.

Detect data spikes with time series searches

Use time series searches to track numeric values over time and look for spikes. The time series searches are performed on a per-entity basis, such as per-user, per-system, and per-file hash, for more accurate alerts.

Time series searches look at the standard deviation in the `stats` command and examine data samples many standard deviations away from the average, allowing you to identify outliers over time. For example, use a time series analysis to identify spikes in the number of pages printed per user, where a higher number can indicate malicious behavior. In a large-scale environment, use summary indexing for time series searches. To run a time series search, follow these steps:

1. From the main menu, click **Advanced > Search Assistants > Detect Spikes**.
2. Enter a search.
3. Refine the search by selecting the data points, subject, threshold method and multiplier.
4. Click **Detect Spikes** and review the outliers and total results.

Detect new values with first time seen searches

To identify suspicious or malicious activity, use first time seen searches to detect the first time that an action is performed. For example, service accounts typically log in to the same set of servers. If a service account logs into a new device one day or logs in interactively, that new behavior might indicate malicious activity.

You can also perform first time analysis based on a user group. Filter out activity that is new for a particular person, but not for the people in their group or department. For example, if User A hasn't checked out code from a particular git repository before, but User A's teammate User B regularly checks out code from that repository, User A's first time activity might not be suspicious.

Detect first time behavior with the `stats` command and `first()` and `last()` functions. Integrate user groups first seen activity using the `eventstats` command.

In a large-scale deployment, use caching with a lookup for first time seen searches. To run a first time seen search, follow these steps:

1. Click **Advanced > Search Assistants > Detect New Values**.
2. Enter a search.
3. Refine the search by selecting the primary and secondary fields.
4. (Optional) Select a filter for peer group and lookup cache.
5. Click **Detect New Values** and review the outliers and total results.

Use a Splunk search in Splunk Security Essentials

Splunk searches are used by the majority of the app and rely on tools included in the Splunk platform. You can get the most value from these searches if you copy the raw search strings to your deployment. For more information on searching in the Splunk platform, see the Search Tutorial. To run a Splunk search in Splunk Security Essentials, follow these steps:

1. Click **Advanced > Search Assistants > Simple Search**.
2. Enter a search.
3. Click **Detect New Values** and review the results.

To view custom search commands in Splunk Security Essentials, see Custom search commands for Splunk Security Essentials.

Custom search commands for Splunk Security Essentials

Splunk Security Essentials includes the following custom search commands to help streamline functionality.

mitremap

The `mitremap` command provides a tabular output of the MITRE ATT&CK and PRE-ATT&CK maps, based on the JSON files that ship with Splunk Security Essentials. By default, the command runs on ATT&CK and outputs labels.

Syntax

mitremap [name=mitre_kill_chain_phase] [pretty=true] [content_available=false] [popular_only=false] [min_popularity=5] [groups="APT1"] [group_only=false] [platforms="cloud"]

Example

| mitremap name=(preattack|attack) [pretty=true] [platforms="office 365,azure ad,windows"]

To filter detections where content is available, use `content_available=true`. To filter detections where a certain number of groups use a technique according to ATT&CK, use `popular_only=true` or `min_popularity=X` to specify the minimum number of groups. To highlight specific threat groups add `groups="APT1"` or `groups="APT1,APT28,APT29"`. To filter and hide techniques not associated by MITRE with those threat groups, add `group_only=true`.

mitremaplookup

The `mitremaplookup` command ingests a set of events and generates a MITRE ATT&CK map showing the techniques used in those events. By default, it looks for the search_name field seen in index=risk or index=notable and then looks up that value in Splunk Security Essentials to generate the actual techniques. Set the `mitre_technique` field to get the techniques from a specific field.

Syntax

mitremaplookup [search_name=search_name] [mitre_technique=mitre_technique] [delim="|"]

Example

| mitremaplookup

sseanalytics

The `sseanalytics` command provides a tabular output for the content shown by Splunk Security Essentials. By default, the `sseanalytics` command prints only key fields, but you can include the full JSON by adding `include_json=true`. The `sseanalytics` command automatically enriches with bookmarked status and data availability status.

Syntax

sseanalytics [cache=true] [app=appName] [include_all=false] [include_json=false]

Example

| sseanalytics [cache=true] [app=Splunk_Security_Essentials] [include_all=false] [include_json=false] | top mitre

sseidenrichment

The `sseidenrichment` command is used as a lookup for products, MITRE IDs, data source IDs, or data source category IDs. Define the type field as appropriate, and `field=` as a field in your dataset that contains the ID to be enriched.

Syntax

sseidenrichment type=(mitreid|productid|datasourceid|dscid) field=yourfield

Example

| sseidenrichment type=mitreid field=yourfield

sselookup

Use the `sselookup` command to accept the input from `index=notable` or `index=risk`, or run this search command as a part of your scheduled correlation searches. If you mapped your live correlation searches in Splunk Security Essentials, the `sselookup` command looks at the search_name field and the source and automatically adds key metadata fields.

Syntax

sselookup [search_name=field_containing_search_name] [all] [mitre] [metadata] [specific_field_name]

Example

| sselookup [all] [mitre] [metadata] [specific_field_name]

To add all fields, use | sselookup all. Use | sselookup mitre, to output just the MITRE fields. To hardcode the name of the search, pass the search name in through | sselookup search_name=myfield.

Customize Splunk Security Essentials

Use the Configuration menu to Customize Splunk Security Essentials

In the Configuration menu, you can include or exclude different sources of content, so that you can customize Splunk Security Essentials. These settings apply globally across Splunk Security Essentials.

To navigate to the Configuration menu from Splunk Security Essentials, select **Configuration**.

The following table describes the different settings in the Configuration menu:

Setting	Description
Enabled Apps / Channels	Toggle the different apps or channels on or off to customize what appears in Splunk Security Essentials.
Suggested Apps	Splunk Security Essentials leverages the capabilities of several other Splunk apps. Consider adding these to get full value out of the app, and out of the Splunk platform.
ES Integration	If you have Splunk Enterprise Security (ES) in your environment, Click **Update ES** to have Splunk Security Essentials push MITRE ATT&CK and Cyber Kill Chain attributions to the ES Incident Review dashboard, along with raw searches of `index=risk` or `index=notable`.
Content Mapping	The Bookmarked Content page lists your local saved searches and maps those to either default content in Splunk Security Essentials or to custom content you create.
Data Inventory	Data Source Categories use standardized searches to find data configured with the tags that are used in the Splunk Common Information Model.
Scheduled Searches	Enable or disable your scheduled searches.
Update Content	Select **Force Update** to manually update the Security Research content in Splunk Security Essentials. Otherwise, this content is automatically updated every 24 hours.
Demo Environment Setup	Use this setting to use demo configurations for data inventory, bookmarked content, and custom content.

Use Security Content in Splunk Security Essentials

Review your content with the Security Content page

The Security Content page is the main landing page for Splunk Security Essentials. The Security Content page provides a complete list of content and gives you the ability to dive deeper into any individual item using a variety of filters. Splunk Security Essentials includes more than 120 detection searches. These detection searches are documented in the app on the Security Content page. Navigate to **Security Content > Security Content** and click **Edit** under the **Filters** heading to add or remove filters to help find the capabilities most relevant to you. The filters that appear by default are described in the following list:

- Use the **Journey** filter to filter content based on where you are in your security journey. For more information on security journey stages, see Security maturity journey stages.
- Use the **Category** filter to filter content based on a specific category.
- Use the **Data Sources** filter to filter content from a specific data source.
- Use the **Analytic Story** filter to filter content based on a specific analytic story. An analytic story is a use case built to detect, investigate, and respond to a specific threat. A group of detections and a response make up an analytic story.
- Use the **Originating App** filter to filter content based on the source of the content, such as custom content originating from a third-party application. For more information on adding custom content from a third-party application or add on, see Create custom content from third-party applications.
- Use the **Risk Object Type** filter to filter content based on its level of risk.
- Use the **Threat Object Type** filter to filter content based on the type of threat.

After you configure your filters, corresponding content appears with a description, log sources, and the associated MITRE or Cyber Kill Chain phases. Click on a piece of content to learn more about it. Bookmark content using the bookmark icon to easily navigate to later using the Manage Bookmarks dashboard. For more information, see Track your content with the Manage Bookmarks dashboard.

> To manually update the Security Research content on this page, navigate to Configuration > Update Content > Force Update. Otherwise, this content is automatically updated every 24 hours.

Review MITRE ATT&CK techniques and find detections

As you review common cybersecurity attacks and threats, you might notice that most reports list the MITRE ATT&CK techniques used in the attack. You can search for these MITRE ATT&CK techniques in Splunk Security Essentials to quickly see if your environment has detections to help protect against them:

1. From the main menu in Splunk Security Essentials, navigate to the **Security Content** page.
2. Copy and paste or enter the list of MITRE ATT&CK techniques from the attack report into the search bar. Alternatively, you can add and use the ATT&CK Technique filter to select the MITRE ATT&CK technique IDs you want to find detections for.
3. Review the detections that appear to determine if your environment is protected against the potential attack.
4. (Optional) Click **Edit** to enable the **Content Enabled** filter and the **Data Availability** filter. Use the **Content Enabled** filter to filter the detections based on what detections are already running in your environment. If a detection is enabled, you already have some protection against the listed techniques. Use the **Data Availability** filter to filter the detections based on if you have the data available for them.

Example: Basic Brute Force Detection

Splunk Security Essentials includes more than 120 detection searches that include context so you can understand the impact of a search, how it works, adapt it to the particulars of your environment, and handle the alerts that will be sent afterward. If you click on one of these detection searches, such as Basic Brute Force Detection, you see the following information:

- **Data Source Links**: Click on these links to see several popular technologies, not just a list of technologies that provide those data sources. You can also find the Installation documentation here.
- **Related Splunk Capabilities**, **Known False Positives**, **How to Respond** and so on: Expand these boxes to learn how to implement and respond to these searches.
- **Enable SPL Mode**: Turn on SPL mode to see the prerequisite checks that make sure you have the right data onboarded, get the Open in Search buttons, and be able to click **Schedule Saved Search** to save this search right from the app.
- **View**: The View buttons show a list of what searches are available for each example.

Use Enterprise Security Content Update content

In addition to accessing the Splunk Security Essentials content, you can also deploy your Enterprise Security Content Update content.

1. In Splunk Security Essentials, navigate to **Security Content > Security Content**.
2. Click **Originating App > Enterprise Security Content Update**

Depending on the content, you might see information such as the search, additional information, the data sources, tactics and techniques, and compliance mapping. If the Enterprise Security Content Update app is installed, you can click **Open in ESCU** to open the content in the ESCU app and schedule in Splunk Enterprise Security.

See visualizations in the Overview dashboard

The Overview dashboard provides visualizations of your Splunk Security Essentials content. This page is a visual overview of data configured on the Security Content page. Use this page to see the number of data sources and examples in Splunk Security Essentials, the Top Kill Chain phases, how use cases map to different data sources and so on. Click **Only Bookmarked** to show only your bookmarked data. For more information on bookmarks, see Track your content with the Manage Bookmarks dashboard.

Track your content with the Manage Bookmarks dashboard

The Manage Bookmarks dashboard helps you track content in your environment, including content you've bookmarked or content that you've marked as successfully implemented. After you've bookmarked content, track the status of your bookmarked content by following these steps:

1. In Splunk Security Essentials, navigate to **Security Content > Manage Bookmarks.**
2. Set the status of your bookmarked content in the content table to **Bookmarked**, **Waiting on Data**, **Ready for Deployment**, **Deployment Issues**, **Needs Tuning**, **Successfully Implemented**, or **Custom**.
3. (Optional) Define a custom bookmark status through the Lookup File Editor app by using the lookup / `bookmark_names` and adding a name and description. You can modify any of the statuses other than **Bookmarked** or **Successfully Implemented**. To download the Lookup File Editor app, see

https://splunkbase.splunk.com/app/1724/ . The `referencekey` field in the `bookmark_names` lookup is optional for any of the statuses.
4. (Optional) Add notes to describe the status of the content.
5. (Optional) Remove the content once you're done using it.
6. (Optional) Click **Export** to export the content. Export options include XLSX, CSV, Doc, Snapshot JSON, and Print-to-PDF.

You can also use Content Introspection from this page. For more information on Content Introspection, see Track active content in Splunk Security Essentials using Content Introspection.

Customize Splunk Security Essentials with the Custom Content dashboard

Add custom content to use Splunk Security Essentials as a use case library to track what you have already built. Custom content gives you the option to map a search that you created to the Splunk Security Essentials content. If the search doesn't find any matches, you can create new custom content and track it from the Custom Content dashboard.

You can add custom content to Splunk Security Essentials by following these steps:

1. In Splunk Security Essentials, navigate to **Security Content > Custom Content**.
2. Select **Add Custom Content**.
3. Enter the required information for your custom content.
4. Select **Add**.

To provide good user experience, make sure that you provide your company information. Although you can't use HTML or Markdown in the description, if you enter `\n` it automatically converts to a line break.

After you add custom content, the configuration is added into the `custom_content_lookup` KV store collection. You can pull the JSON file from the kvstore collection.

> You must adjust this file slightly. Add the channel, which is configured in your essentials_updates.conf file, and the ID to this configuration when you migrate it to the final hosted file. You might also change the ID to indicate that it isn't custom content, but something from your organization. Also make sure to update the link in the dashboard attribute.

Create custom content from saved searches

You can add custom content from saved searches to Splunk Security Essentials by following these steps:

1. In Splunk Security Essentials, navigate to **Security Content > Custom Content**.
2. Select **Add Custom Content**.
3. Select **Create From Local Saved Search**.
4. Select the saved search you want to use to create your custom content. After you select your search, many fields autopopulate. If a field didn't autopopulate, enter the required information.
5. Select **Add**.

Create custom content from third-party applications

Create custom content from third-party applications in Splunk Security Essentials to better manage your security content all in one place by following these steps:

1. In Splunk Security Essentials, navigate to **Security Content > Custom Content**.
2. Select **Add Custom Content**.
3. Enter a name for your custom content in the **Name** field. Names have a maximum of 150 characters.
4. Select **Solved Outside of Splunk.**
5. Enter the application or add-on name of the source of your third-party content in **Originating App** field.
6. Select the **Bookmarked Status** of the content. For example, "Successfully Implemented."
7. Select the stage of the **Journey** that this custom content appears in.
8. Select the **Use Case** for this custom content. For example, "Insider Threat."
9. Select if this custom content is **Featured** or not. It is recommended that only 15 percent of content is featured.
10. Select the **Alert Volume** for this custom content from high to low.
11. Select the **Severity** of this custom content from high to low.
12. Select the **Category** for this custom content. For example, "Account Compromise."
13. Select the **Data Source Category** for this custom content.
14. Enter a description for this custom content in the **Description** field.
15. (Optional) Add metadata, descriptive, or search fields.
16. Select **Add**.

If your content was added successfully, a success message appears and your content will be listed on both the Custom Content page and on the Security Content page. You can filter any third-party custom content you added by **Originating App** on the Security Content page.

Find content to use in your ransomware defense with the Ransomware Content Browser

Plan your ransomware defense with the Ransomware Content Browser by first viewing a visualization of the lifecycle of a ransomware attack and then using the **Ransomware Content List** to find content to protect against a ransomware attack. View the **Total content by Type** table to see what types of content are available for each security phase.

You can navigate to the Ransomware Content Browser in Splunk Security Essentials by navigating to **Security Content > Ransomware Content Browser**.

Use the Ransomware Content List to find content to use in your ransomware defense

To find content to use in your ransomware defense, follow these steps:

1. Navigate to the **Ransomware Content List**.
2. Change the **Content Type** from the default of **Any** to reflect the type of content you are looking for.
3. Change the **Phase** from the default of **Any** to find content related to a specific type of security threat.
4. Change **Critical Control** from the default of **Any** to find content related to a specific type of security control.

The filters populate information about the stage and phase and if available, content appears in the **Content in selection** area of the page. You can then select the content to start using it in your ransomware defense plan, or if the content is a detection, you can schedule the detection to prevent ransomware on your system.

Find content with the MITRE ATT&CK-Driven Content Recommendation dashboard

Use MITRE ATT&CK to filter for the Splunk content related to MITRE ATT&CK techniques that are associated with many different threat groups.

Prerequisites

Configure the Data Inventory dashboard and Content Introspection. For more information, see Configure the products you have in your environment with the Data Inventory dashboard or Track active content in Splunk Security Essentials using Content Introspection.

Steps

1. In Splunk Security Essentials, navigate to **Security Content > MITRE ATT&CK-Driven Content Recommendation**.
2. In the **Categories** filter, click the issue category you're concerned with.
3. (Optional) Adjust the filters for data availability and popularity.

A list of content recommendations appears based on your filters.

Gather events with the Risk-based Alerting dashboard

The Risk-based Alerting Content Recommendation dashboard gathers possibly risky events together for analysts to view in one place.

Prerequisites

Configure the Data Inventory dashboard and Content Introspection. For more information, see Configure the products you have in your environment with the Data Inventory dashboard or Track active content in Splunk Security Essentials using Content Introspection.

Steps

1. In Splunk Security Essentials, navigate to **Security Content > Risk-based Alerting Content Recommendation**.
2. Select a category to see how many pieces of content you already deployed and how many are available with your existing data.
3. (Optional) Use the **Apps** filter to further filter on where you want the content recommendation to come from.

With one or more categories selected, the dashboard shows you all of the content that you can leverage. You can click through to any of these to enable them, bookmark them, or more.

Use the Analytics Advisor in Splunk Security Essentials

The Content Overview dashboard

The Content Overview dashboard is an important part of the Analytics Advisor suite. This dashboard takes into account what data you have in your environment, what searches are active, and helps you see what content you can use next. To use this dashboard, from the main menu click **Analytics Advisor > Content Overview**. Each number in this dashboard represents a step in using the dashboard.

1. The **Available Content** panel lets you see a high level of how your environment compares to the available content. You can switch between the tabs to change the visualization and click the **Split by** field to show different dimensions. Everything in this panel is clickable and allows you to drill down further.
2. The **Selected Content** panel contains further filters that allow you to drill into individual pieces of content.
3. The **View Content** panel lets you view full details of the selection inside the Security Essentials general content page.

Any content in this dashboard labeled **Active** means that you have content enabled in your environment. Content labeled **Available** means that you have content that can be enabled with data already in Splunk. Content labeled **Needs data** means that the data needed to support the content is missing.

The MITRE ATT&CK Framework dashboard

The MITRE ATT&CK Framework dashboard takes into account the data and active content in your environment to help you choose relevant MITRE ATT&CK content. Before you use the MITRE ATT&CK dashboard, Configure the Data Inventory dashboard and Content Introspection. For more information, see Configure the products you have in your environment with the Data Inventory dashboard or Track active content in Splunk Security Essentials using Content Introspection.

The dashboard is split into three pieces.

Available Content

The MITRE ATT&CK Matrix tab shows the coverage in your environment. By default, the app colors the matrix based on **Total** content, but you can adjust this to show only the **Active** content, the **Available** content to use with your data, or the content that **Needs data**. You can also adjust to show the **Threat Group Count** and **Bookmark Count**. The **Active** number is based on what you have bookmarked and set to active, or has been pulled from content introspection. **Available** shows the number of use cases mapped to the MITRE ATT&CK framework that you have data for but haven't been deployed. **Needs data** shows the number of use cases you can deploy if you add data. With **Threat Group Count** and **Bookmark Count** the matrix is a darker blue where more threat groups are present, or where you have more pieces of content bookmarked for the technique.

You can also use this tool to highlight the threat groups that target you. Select the **MITRE ATT&CK Threat Group** to highlight specific techniques in the matrix that are associated with a specific industry. Once you select a specific industry, numbers appear by certain techniques to indicate how many threat groups are associated with each technique. Click the numbers to view more information about the specific threats.

You can also select **Edit** and add the filter **Originating App** to filter the content based on the application it originated from. For more information on adding custom content from third-party applications, see Create custom content from

third-party applications.

Select **MITRE ATT&CK Software** to highlight techniques associated with a particular software and the **MITRE ATT&CK Matrix Platform** to highlight techniques associated with a specific platform. Use the **Highlight Data Source** filter to highlight a specific data source directly in the matrix. Use the **Filter** dropdown to filter based on techniques that have 3 or more threat groups associated with them, techniques with content, bookmarked content, or only cells associated with the threat group industry you selected. You can also change the visualizations using **Chart View**, **Radar View**, **Sankey View** and **Security Journey View**. If you choose to use these alternate views, you can use the **Split by** filter to filter techniques based on app, data source, index, sourcetype, and so on.

The MITRE ATT&CK Matrix also features sub-techniques. You can click on the side of any box in the table to expand a technique and view the associated sub-techniques.

Selected Content

The Selected Content panel lets you filter further into individual content pieces. You can view the content list to view content to use against specific threat groups based on the the popularity of threat groups using a certain technique, select content by data source or data source category, or select content by MITRE ATT&CK tactic, technique, or threat group. You can even view which tactics, techniques, and threat groups are covered by which app. You can also bookmark your filters to come back to later. To create a bookmark, follow these steps:

1. From the Selected Content panel, navigate to **Bookmark Selection**.
2. Select a **Bookmark Status**. Available options include **Bookmarked, Waiting on Data, Deployment Issues, Needs Tuning, Ready for Deployment, and Successfully Implemented.**
3. (Optional) Customize the **Note** field with notes about this bookmark.
4. Click **Add Bookmarks**.

Once you have added a bookmark, you can filter based on what you have bookmarked or the bookmark notes you added.

View Content

The View Content panel lets you go directly to full details of the selection inside the Splunk Security Essentials general content page.

The Cyber Kill Chain dashboard

The Cyber Kill Chain dashboard includes a custom visualization that shows what content is tied to different parts of the Cyber Kill Chain. The Cyber Kill Chain dashboard takes into account the data and active content in your environment to help you choose new cyber kill chain content. Each number in this dashboard represents a piece of content. Content labelled **Active** means that you have content enabled in your environment, **Available** means that you have content that can be enabled with data already in Splunk, and **Needs data** means that the data to support the content is missing in Splunk.

Before you use the Cyber Kill Chain, Configure the Data Inventory dashboard and Content Introspection. For more information, see Configure the products you have in your environment with the Data Inventory dashboard or Track active content in Splunk Security Essentials using Content Introspection.

Available Content

In the **Kill Chain View**, the **Cyber Kill Chain** tab shows the coverage in your environment against the Kill Chain steps. You can adjust what numbers are displayed in the Cyber Kill Chain visualization to show **Active** or **Available** content.

The **Chart View** shows on a high level how your environment stacks up against the content available and the Cyber Kill Chain. You can switch between the tabs to change the visualization.

Selected Content

The **Selected Content** panel contains further filters that allow you to drill into individual pieces of content.

View Content

The **View Content** panel allows you to go directly to the view full details of the selection inside the Security Essentials general content page.

Use Analytic Stories for actionable guidance in Splunk Security Essentials

The Splunk Security Research team writes Analytic Stories that provide actionable guidance for detecting, analyzing, and addressing security threats. An Analytic Story contains the searches you need to implement the story in another environment. It also provides an explanation of what the search achieves and how to convert a search into adaptive response actions, where appropriate. For more information about Analytic Stories, see Use Analytic Stories for actionable guidance in Splunk Enterprise Security in the *Use Splunk Enterprise Security* manual.

To access Analytic Stories in Splunk Security Essentials, follow these steps:

1. In Splunk Security Essentials, select the **Analytics Advisor** tab.
2. From the dropdown, select **Analytic Story Detail**.

Investigate an Analytic Story

The Analytic Story page in Splunk Security Essentials contains details about the Analytic Story and the searches used to find the data used to generate the Analytic Story.

To populate the dashboard, follow these steps:

1. Choose the Analytic Story you want to investigate from the **Selectâ ¦** menu.
2. Select **Run Analytics**.

See details

After the analytics finish running, these details is visible:

Field	Description
Category	The high-level category of the Analytic Story.
Version	The version of the particular Analytic Story.

Field	Description
Created	The date the Analytic Story is created.
Description	The high-level description of the Analytic Story.
Narrative	The in-depth narrative describing the Analytic Story.
ATT&CK	The MITRE ATT&CK codes.
Kill Chain Phases	The phases in the kill chain.
Data Model	The data that is in use by the detection searches for this Analytic Story as mapped to the Splunk data models via the CIM add-on. If the status icon shows a red exclamation mark, hover over the icon to see the reason.
References	URL links to references relevant to the Analytic Story.

Identify Analytic Story Searches

After the analytics finish running, this information about the search is visible:

Field	Description
Description	The high-level description of the search.
Search	The SPL search that has been used to generate data related to the Analytic Story.
How to Implement	Information about how to implement the SPL search.
Known False Positives	The known false positives in the SPL search.
ATT&CK	The MITRE ATT&CK codes.
Kill Chain Phases	The phases in the kill chain.
CIS Controls	The Center for Internet Security controls.
Data Models	The data that is in use by the detection searches for this Analytic Story as mapped to the Splunk data models via the CIM add-on. If the status icon shows a red exclamation mark, hover over the icon to see the reason.
Confidence	The degree of confidence in the analysis.
Creation Date	The date the search is created.

To reconfigure a search related to the Analytic Story, select the **Configure** button. That button redirects you to the Security Content page in Splunk Security Essentials.

Use Security Operations in Splunk Security Essentials

Aggregate risk attributions with the Analyze ES Risk Attributions dashboard

The Analyze ES Risk Attributions dashboard helps you understand the data provided by the Splunk Enterprise Security Risk Analysis Framework. The ES Risk Attributions dashboard looks at the content in the ES Risk Framework with default risk aggregations. It includes a customized MITRE ATT&CK Matrix based on your search filters which lets you see what techniques have been seen against a particular user, host, or network. You can enter any search string to use the dashboard to analyze a network or your entire organization.

Aggregating risk attributions is the core strength of this dashboard, and there is a series of charts that aggregate risk by various metrics.This dashboard also shows system wide metrics and information, many of which are focused on MITRE ATT&CK. For more information on MITRE ATT&CK, see The MITRE ATT&CK Framework dashboard.

There is also a straightforward sum of risk by object, which will let you see which objects are experiencing the greatest amount of risk.

Check if your data is CIM-compliant with the Common Information Model Compliance Check dashboard

Use the Common Information Model (CIM) Compliance Check dashboard to see if your data is CIM-compliant. This dashboard checks CIM compliance by comparing the most common field values against a regular expression. It aggregates those fields per-product and tells you how those products are doing with CIM compliance. To use this dashboard in Splunk Security Essentials, navigate to the main menu, **Security Operations > CIM Compliance Check**.

In order to start using this dashboard, you must set up Data Inventory introspection. For more information about setting up Data Inventory introspection, see Configure the products you have in your environment with the Data Inventory dashboard.

In this dashboard, there is a list of the products that you configured in Splunk Security Essentials broken out by data source category and the CIM compliance status of each key field for that DSC. If you expand the row, you can also see the actual values returned when searching that data.

Use Data in Splunk Security Essentials

Configure the products you have in your environment with the Data Inventory dashboard

Use the Data Inventory dashboard to configure the products you have in your environment. Products have a variety of metadata such as sourcetypes, event volume, and Common Information Model (CIM) compliance and are connected with data source categories. Because of this, the Data Inventory dashboard can show you what content can be turned on with your current data. To use the Data Inventory dashboard, follow these steps:

1. In Splunk Security Essentials, navigate to **Data > Data Inventory**.
2. From the pop-up window, select how you want to get your data into this dashboard.
    1. If Splunk Security Essentials is installed on your production search head, click **Launch Automated Introspection** to automatically import data.
    2. Click **Manually Configure** to manually enter your data.

Introspection lets Splunk Security Essentials see what data you have available to use across the app.

1. If you chose Automated Introspection, click **Automated Introspection** to see the five automated introspection steps that will pull in a variety of data.
2. If any of your sources or source types don't appear correctly, click **Update** in the Actions column to make changes.
3. Once your data appears in the menu, if there is an X or a question mark (?) beside a datasource in the menu, manually review the datasource to see whether or not you have that type of data in your environment.

When reviewing your sources, you can view the **Products for this Data Source Category** table. This table includes the following information:

Name	Description
i	Expand the arrow to see information on the number of hosts, average event size, typical events per day, CIM coverage, and TERM search.
Vendor	The company that sells the product.
Product	The name of the product.
Status	Describes whether or not there is data present in this product.
Coverage	Use this field to track how much of the data is in Splunk.
Base Search	The search string that can be used to detect the data source. If this has already been detected, it is automatically saved here.
Actions	Use the buttons to **Update** or **Delete** a product.

See an overview of your data inventory

If you want to see an overview of information about your data inventory, use the Data Inventory Overview dashboard. To see that dashboard in Splunk Security Essentials, navigate to **Data > Data Inventory Overview**. The Data Inventory Overview dashboard displays this information:

- Data Sources Observed: The number of data sources you are currently observing in your data inventory.

- Data Source Categories with Data Observed: The number of data-source categories you are observing. Those categories must contain data. If a data-source category doesn't contain data, that category won't be counted.
- Products with Data Observed: The number of products you are observing. Those products must contain data. If a product doesn't contain data, that product won't be counted.
- Products by Data Source: A table that displays the products you are observing and their related data sources. The table is color coded so you can easily identify products at a glance.

Troubleshoot Data Inventory Introspection

If you are experiencing issues with data inventory introspection, it might be helpful to reset and run the configuration. Most of the issues that have been seen with Data Introspection resolve after resetting and running the configuration.

Prerequisites

Use Splunk Security Essentials 3.0.3 or above.

Solution

Use the following troubleshooting steps to reset the Splunk Security Essentials system:

1. From the Splunk Security Essentials app, refresh the Data Inventory page.
2. Open the status dialog.
3. Click **Reset Configurations**.
4. When the prompt appears, click **Run Data Introspection**. If the prompt doesn't appear, repeat steps 2 and 3.
5. Review all Review configurations and define what product they belong to.

Track active content in Splunk Security Essentials using Content Introspection

Tracking the content you already have active helps you know what areas you might need to monitor. Content Introspection pulls a list of your enabled local scheduled searches that have an action associated with them and then automatically enables any enabled Splunk Enterprise Security, Enterprise Security Content Update (ESCU), or Splunk Security Essentials (SSE) content. Configure Content Introspection to track what content you currently have active in Splunk Security Essentials. To use Content Introspection, follow these steps:

1. From Splunk Security Essentials, navigate to **Data > Content Introspection**.
2. Click **Look for Enabled Content** to get a list of all of your local saved searches.

Filter on the **Status** to filter content based on whether it is **Mapped, Likely Match, Potential Match, Low Match, or No Match.** Review the list of likely and potential matches, and make a decision based on the following options:

Option	Description
Accept Recommendation	If Splunk Security Essentials finds a close match, click **Accept Recommendation** to map that local saved search to the recommended default Splunk content.
Search	This option opens a search dialog that looks through all of the content in Splunk Security Essentials and lets you select your desired content.
Create New	If you don't see any content in Splunk Security Essentials that represents this detection, you can create your own custom content.

Option	Description
Not a Detection	This option lets you mark content as not a security detection.
Clear	This option lets you clear any mappings you may have made on the content.
Edit	This option appears when Splunk Security Essentials automatically creates a new custom content card for you with default options. Use **Edit** to edit the default options and click **Update** when you have made any necessary changes.

If a scheduled search is enabled and is also a correlation search, Splunk Security Essentials automatically creates a new custom content card for you with default options. These cards then appear on the Security Content page and the MITRE ATT&CK Framework dashboard.

Troubleshoot Content Introspection

Here are some common issues that you can encounter when you use content introspection. Read the following sections to learn how to resolve those issues.

Troubleshoot lookups and permissions

Content introspection might fail if the lookups and permissions aren't generated or working correctly. Follow these steps to troubleshoot lookups and permissions with content introspection:

1. Run a search and verify that it generates results. Verify that the lookup is generated by running the following search:
   ```
   | inputlookup sse_content_exported_lookup
   ```
2. Test if the automatic lookup configuration in props.conf is working using the following search:
   ```
   index=notable OR index=risk | stats count as num_total count(eval(isnotnull(mitre_technique))) as num_with_mitre_technique
   ```
3. Test Splunk Enterprise Security permissions using the same search in Splunk Enterprise Security:
   ```
   index=notable OR index=risk | stats count as num_total count(eval(isnotnull(mitre_technique))) as num_with_mitre_technique
   ```
   If this doesn't work, run the Splunk Enterprise Security Integration in the Splunk Security Essentials Setup. If that fails, manually configure Splunk Enterprise Security, or upgrade to Splunk Enterprise Security 5.3+.
4. Open incident review to check if the custom fields were added to the log_review.conf file. If this doesn't work, run the Splunk Enterprise Security Integration in the Splunk Security Essentials setup. If that fails, manually configure the fields in Splunk Enterprise Security in the Configure Incident Review Settings, and add the fields you see in the lookup.

Troubleshoot annotations

If you use Splunk Enterprise Security, you might want to add the security framework metadata for correlation searches to the annotations framework. Simply doing content introspection doesn't add the annotations directly unless you navigate to the correlation search editor in Splunk Enterprise Security and manually fill out the fields you want to appear in your search. See Use security framework annotations in correlation searches in the *Administer Splunk Enterprise Security* manual for more information.
However, if you schedule the search through Splunk Security Essentials, the annotation information is automatically populated in Splunk Enterprise Security. To schedule a search in Splunk Security Essentials, follow these steps:

1. Click **Security Content > Security Content**.
2. Click on the detection you want to use.
3. Click **Detect New Values**.
4. Click **Save Scheduled Search**.

5. A modal appears where you can schedule an alert. Enter the number of outliers that must occur for you to be alerted and click **Next**.
6. Review the settings and make any desired changes.
7. Click **Save**.
8. A modal appears letting you know that the Splunk Enterprise Security Correlation Search is enabled. Click to keep editing the Notable Event to customize the display fields.

The correlation search editor page in Splunk Enterprise Security appears with the annotations populated.

Track data ingest latency with the Data Availability dashboard

The Data Availability dashboard is a machine learning-driven dashboard that tracks the typical data ingest latency of the products configured in Splunk Security Essentials. When a log source slows down, it is color coded in the dashboard, and you can click on it to see what detections are at risk.

Prerequisites

The Data Availability dashboard requires the Splunk Machine Learning Toolkit (MLTK). Verify that you have MLTK installed. See Install the Machine Learning Toolkit in the Splunk Machine Learning Toolkit *User Guide*.

Steps

1. In Splunk Security Essentials, navigate to **Data > Data Availability**.
2. Click **Run Baseline Search**.
3. Click the log sources in the search results to see if there are any detections at risk for that specific source.

Check data sources with the Data Source Check dashboard

In Splunk Security Essentials, every example has prerequisites defined to help you know if a search will work in your environment. The Data Check dashboard is a tool to verify if the data sources exist for examples in Splunk Security Essentials. To use the Data Source Check dashboard, follow these steps:

1. In Splunk Security Essentials, navigate to **Data > Data Source Check**.
2. Click **Start Searches**.

A green check mark indicates that all of the prerequisite checks were completed for the search so you can run it in your environment. A red exclamation point indicates that one or more of the prerequisite checks for the search failed. You can click the expand icon to find out what check failed, and how to fix it.

Create security posture dashboards

After you have verified your data sources exist, you can create security Posture dashboards to see an overview dashboard of all of your security content in Splunk Security Essentials. You can create up to 50 dashboard panels. To create a Posture dashboard, follow these steps:

1. In Splunk Security Essentials, navigate to **Data > Data Source Check**.
2. Click **Create Posture Dashboards**.
3. Select your desired dashboard type from the list. Some panels are unavailable if you don't have the required data.

4. (Optional) Click **Use Demo Datasets** to have all dashboards use CSV demo data.
5. Click **Create Dashboards** to get a link to the dashboard. The dashboard is also added to the main menu under **Security Operations**.

Understand the data sources used in Splunk Security Essentials with the Data Source On-boarding Guides

Use the Data Source On-boarding Guides as a method to improve standardization in on-boarding data. The Data Source On-boarding Guides page includes a list of the Data Sources that are commonly used in Splunk Security Essentials, along with some of the common products for each. In this list, many of the products have guides that show you how to configure the products in your environment to send the logs required to fire security detections. To view these guides, follow these steps:

1. In Splunk Security Essentials, navigate to **Data > Data Source On-boarding Guides**.
2. Click the data source you are interested in to see more information and the associated guides.