Splunk® Enterprise Security
Splunk Enterprise Security Tutorials 7.0.2

Generated: 10/05/2022 7:28 pm

Table of Contents

Introduction

Splunk Enterprise Security tutorials

Take full advantage of the features and functionality in Splunk Enterprise Security. Learn how to create a correlation search in Splunk Enterprise Security with the correlation search tutorial.

See Create a correlation search to start the correlation search tutorial.

Correlation Search Tutorial

Create a correlation search

A **correlation search** is a type of search that evaluates events from one or more data sources for defined patterns. When the search finds a pattern, it creates a notable event, adjusts a risk score, or performs an **adaptive response action**. A correlation search is a saved search with extended capabilities making it easier to create, edit, and use searches for security use cases.

This tutorial is for users who are comfortable with the Splunk Search Processing Language (SPL) and who understand data models and the Splunk App for Common Information Model.

You will learn how to create a correlation search using the guided search creation wizard.

Part 1: Plan the use case for the correlation search

Create a correlation search to address a security use case or problem that you want to solve. If you want to know when vulnerability scanners scan your network, or a high number of devices are infected with the same strain of malware, you can create a correlation search to detect that behavior and alert you.

Correlation searches allow you to search across one or more types of data and identify patterns that could indicate suspicious or malicious activity in your environment.

When to use a correlation search

Use a correlation search to identify patterns in your data that can indicate a security risk.

- You want to know when high-risk users log in to machines infected with malware.
- Identify vulnerability scanning behavior in your network.
- Validate that your access control deprovisioning process is working as expected by monitoring inactive and expired account activity.
- Look for compromised accounts by identifying geographically impossible logins.

Define the use case for the search

Develop a use case that you want the search to address before you start creating the search. This tutorial walks you through creating the Excessive Failed Logins search, which is designed to detect brute force access attempts.

For example, a security analyst wants to know all the users that attempted to log in to an application and failed to type their passwords correctly at least six times. The Excessive Failed Logins correlation search included in Splunk Enterprise Security captures that use case and performs the following functions:

- Search the authentication source events from an application.
- Count the number of failures by user.
- Create an alert for more than six failures over a selected time period.

This search addresses the use case by searching authentication events, counting the number of access failures, and alerting if there are too many failures over a specific period of time.

As another example, a security analyst wants to know if more than ten computers on the network failed to update their virus signatures for a week. The High Number of Hosts Not Updating Malware Signatures correlation search included in Splunk Enterprise Security captures that use case and performs the following functions:

- Search the antivirus source events.
- Evaluate the date of the last antivirus signature file update on a host.
- Compare the last updated date to the time that the search is running.
- Collect events where the last updated date is more than seven days before the time that the search is running.
- Count the collected events.
- If there are more than 10 collected events, create an alert.

Find the data to fit the use case

After you determine the security use case that you want your correlation search to address, determine which data sources are relevant to the use case.

- Determine what data you need to address the use case.
- Determine which data models and data model objects contain that data in the Splunk App for CIM.
- Make sure that the data is in the data model.

In this case, the **Excessive Failed Logins** search looks for data related to logins, so it uses the Authentication data model as the data source. By using a data model rather than searching a specific source type directly, the correlation search can search a wide variety of data sources related to authentication, such as operating systems, applications, or RFID badge readers, without needing to be changed. Relying on data models in correlation searches allow you to write one search for multiple types of data.

Next step

Part 2: Create a correlation search.

Part 2: Create a correlation search

After you plan the use case that the correlation search covers, create the search.

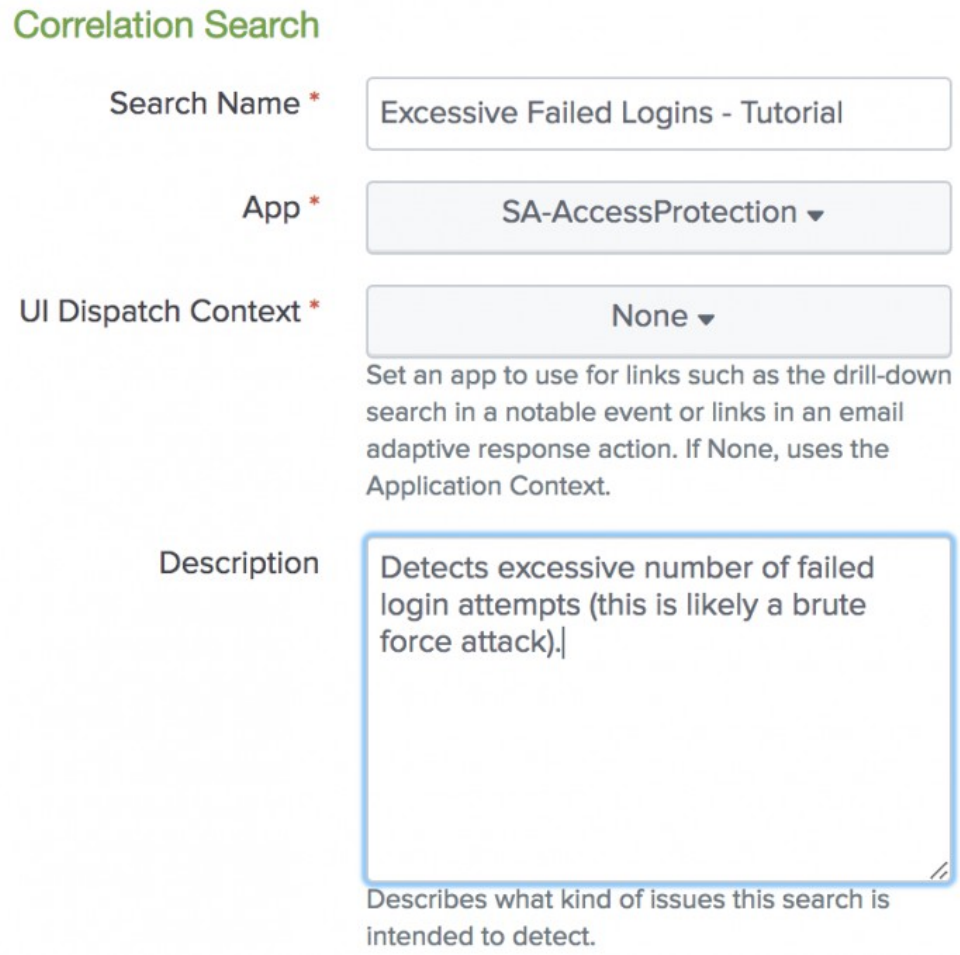
Create a search

To create a correlation search, start on the Content Management page.

1. From Splunk Home, select Splunk Enterprise Security.
2. Select **Configure > Content > Content Management**.
3. Select **Create New Content > Correlation Search** to open the correlation search editor.
4. In the **Search Name** field, type **Excessive Failed Logins - Tutorial**.

Correlation search names cannot be longer than 83 characters. However, if you include the string prefix, such as "Threat - " and the string suffix such as "-Rule" to the correlation search name, the maximum character count for correlation searches is 99 characters.

5. In the **App** drop-down list, select **SA-AccessProtection** as the app where you want the correlation search to be stored. Choose an app context that aligns with the type of search that you plan to build. If you have a custom app for your deployment, you can store the correlation search there.
6. In the **UI Dispatch Context** drop-down list, select **None**. This is the app used by links in email and other adaptive response actions. The app must be visible for links to work.
7. In the **Description** field, type a description of what the correlation search looks for, and the security use case addressed by the search. For example, **Detects excessive number of failed login attempts (this is likely a brute force attack)**.



If you disable or remove the app where the search is stored, the correlation search is disabled. The app context does not affect how or the data on which the search runs.

Next Step

Part 3: Create the correlation search in guided mode.

Part 3: Create the correlation search in guided mode

After you define the title, app context, and description of the search, it is time to build it. The best way to build a correlation search with syntax that parses and works as expected is to use guided search creation mode.

Open the guided search creation wizard

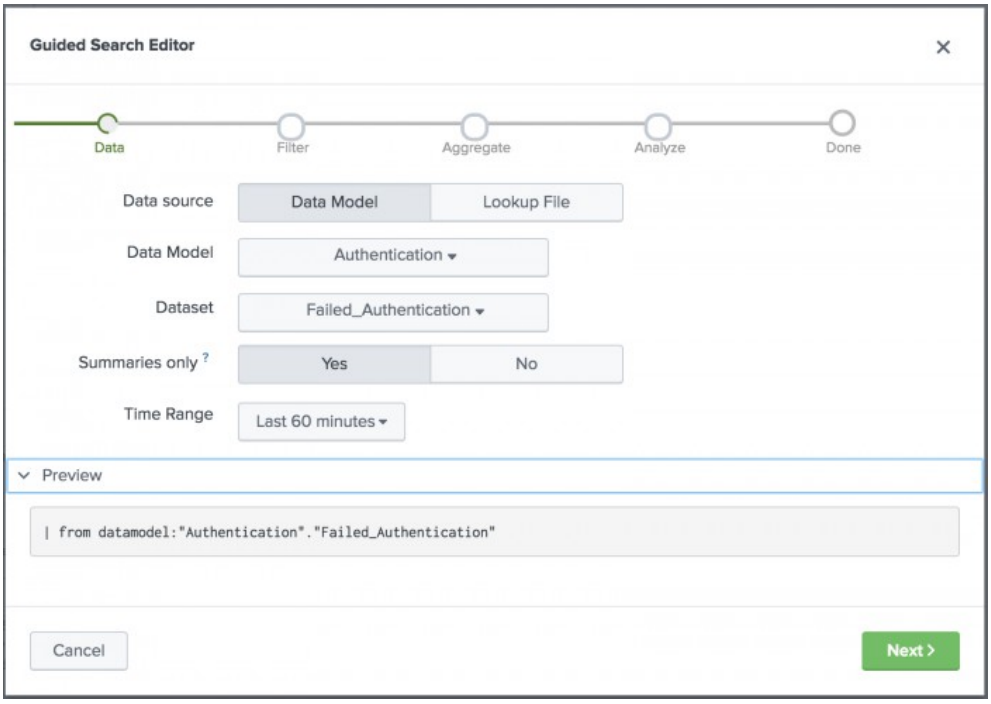
1. From the correlation search editor, click **Guided** for the **Mode** setting.
2. Click **Continue** to open the guided search editor.

Select the data source for the search

Start your correlation search by choosing a data source.

1. For the **Data source** field, select the source for your data.
   - Select **Data Model** if your data is stored in a data model. The data model defines which objects, or datasets, the correlation search can use as a data source.
   - Select **Lookup File** if your data is stored in a lookup. If you select a lookup file for the **Source**, then you need to select a lookup file by name.

   To recreate the Excessive Failed Logins search, select **Data Model**.
2. In the **Data model** list, select the data model that contains the security-relevant data for your search. Select the **Authentication** data model because it contains login-relevant data.
3. In the **Dataset** list, select the **Failed_Authentication** dataset. The Excessive Failed Logins search is looking for failed logins, and that information is stored in this data model dataset.
4. For the **Summaries only** field, click **Yes** to restrict the search to accelerated data only.
5. Select a **Time range** of events for the correlation search to scan for excessive failed logins. Select a preset relative time range of **Last 60 minutes**. The time range depends on the security use case for the search. Excessive failed logins are more of a security issue if they occur during a one hour time span, whereas one hour might not be a long enough time span to catch other security incidents.
6. Click **Preview** to review the first portion of the search.



7. Click **Next** to continue building the search.

Filter the data with a where clause

Filter the data that the correlation search examines for a match using a `where` clause. The search applies the filter before applying statistics.

The Excessive Failed Logins search by default does not include any where clause filters, but you can add one if you want to focus on failed logins for specific hosts, users, or authentication types.

The search preview shows you if the correlation search string can be parsed. The search string appends filter commands as you type them, letting you see if the filter command is a valid `where` clause. You can run the search to see if it returns the results that you expect. If the where clause filters on a data model dataset such as `Authentication.dest`, enclose the data model dataset with single quotes. For example, a where clause that excludes authentication events where the destination is local host would look as follows: `| where 'Authentication.dest'!="127.0.0.1"`.

1. Leave the **Filter** field blank and click **Next**.

Analyze your data with statistical aggregates

Analyze your data with statistical aggregates. Each aggregate is a function that applies to a specific attribute in a data model or field in a lookup file. Use the aggregates to identify the statistics that are relevant to your use case.

For example, the **Excessive Failed Logins** correlation search uses four statistical aggregate functions to surface the important data points needed to define alerting thresholds. For this search, the aggregates identify the following:

- Tags associated with the authentication attempts.
- Number of users involved.
- Number of destinations involved.
- Total count of attempts.

To replicate this search, create the aggregates.

Create the tags aggregate

Identify the successes and failures in authentication attempts with tags.

1. Click **Add a new aggregate**.
2. Select the **values** function from the **Function** list.
3. Select **Authentication.tag** from the **Field** list.
4. Type `tag` in the **Alias** field.

This aggregate retrieves all the values for the `Authentication.tag` dataset.

Create the user count aggregate

Identify the number of distinct users involved.

1. Click **Add a new aggregate**.
2. Select the **dc** function from the **Function** list.
3. Select **Authentication.user** from the **Field** list.
4. Type `user_count` in the **Alias** field.

This aggregate retrieves a distinct count of users.

Create the destination count aggregate

Identify the number of distinct destinations involved.

1. Click **Add a new aggregate**.
2. Select the **dc** function from the **Function** list.
3. Select **Authentication.dest** from the **Field** list.
4. Type `dest_count` in the **Alias** field.

This aggregate retrieves a distinct count of devices that are the destination of authentication activities.

Create a total count aggregate

Identify the overall count.

1. Click **Add a new aggregate**.
2. Select the **count** function from the **Function** list.
3. Leave the attribute and alias fields empty.

This aggregate identifies the total count for statistical analysis.

Fields to split by

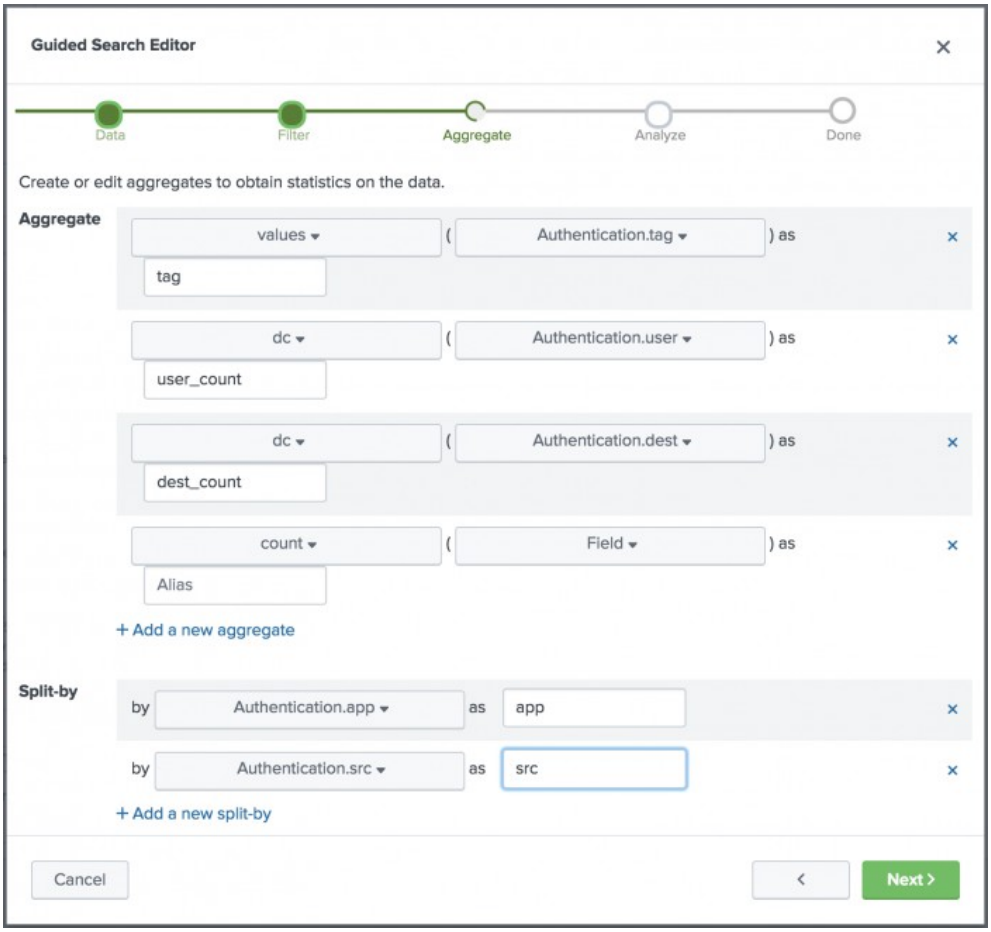
Identify the fields that you want to split the aggregate results by. Split-by fields define the fields that you want to group the aggregate results by. For example, you care more about excessive failed logins if the users were logging into the same application and from the same source. In order to get more specific notable events and to avoid over-alerting, define split-by fields for the aggregate search results.

Split the aggregates by application.

1. Click **Add a new split-by**.
2. From the **Fields** list, select **Authentication.app**.
3. Type `app` in the **Alias** field.

Split the aggregates by source.

1. Click **Add a new split-by**.
2. From the **Fields** list, select **Authentication.src**.
3. Type `src` in the **Alias** field.


Guided Search Editor
Data
Filter
Aggregate
Analyze
Done
Create or edit aggregates to obtain statistics on the data.
Aggregate
values
Authentication.tag
as
tag
dc
Authentication.user
as
user_count
dc
Authentication.dest
as
dest_count
count
Field
as
Alias
+ Add a new aggregate
Split-by
by
Authentication.app
as
app
by
Authentication.src
as
src
+ Add a new split-by
Cancel
Next

Click **Next** to define the correlation search match criteria.

You can find information on split-by fields in the Splunk platform documentation.

- For Splunk Enterprise, see Optional arguments in the Splunk Enterprise *Search Reference*.
- For Splunk Cloud Platform, see Optional arguments in the Splunk Cloud Platform *Search Reference*.

Define the correlation search match criteria for analysis

Identify the criteria that define a match for the correlation search. The correlation search performs an action when the search results match predefined conditions. Define the statistical function to use to look for a match.

For **Excessive Failed Logins**, when a specific user has six or more failed logins from the same source and attempting to log in to the same application, the correlation search identifies a match and takes action.

1. In the **Field** list, select the function **count**. The **Field** list is populated by the attributes used in the aggregates and with the fields used in the split-by.
2. In the **Comparator** list, select **Greater than or equal to**.
3. In the **Value** field, type **6**.
4. Click **Next**.

Test the correlation search string

The guided mode wizard ensures that your search string parses and produces events. You can run the search to see if it returns the preliminary results that you expect.

> The correlation search results must include at least one event to generate a notable.

1. Open a new tab in your browser and navigate to the Splunk platform Search page.
2. Run the correlation search to validate that it produces events that match your expectations.
    1. If your search does not parse, but parsed successfully on the filtering step, return to the correlation search guided editor aggregates and split-bys to identify errors.
    2. If your search parses but does not produce events that match your expectations, adjust the elements of your search as needed.
3. After you validate your search string on the search page, return to the guided search editor and click **Done** to return to the correlation search editor.

Next Step

Part 4: Schedule the correlation search.

Part 4: Schedule the correlation search

Decide how often you want the search to run, and how often you want response actions to be triggered in response to search matches. You can adjust the schedule window and throttling to make sure that duplicate events are not created, which could result in duplicate actions being taken by analysts or the automated response actions that you set up.

Configure a schedule for the correlation search

Correlation searches can run with a real-time or continuous schedule.

- Use a real-time schedule to prioritize current data and performance. Searches with a real-time schedule are skipped if the search cannot be run at the scheduled time. Searches with a real-time schedule do not backfill gaps in data that occur if the search is skipped.
- Use a continuous schedule to prioritize data completion, as searches with a continuous schedule are never skipped.

As excessive failed logins matter most when you hear about them quickly, select a real-time schedule for the search. If you care more about identifying all excessive failed logins in your environment, you can select a continuous schedule for the search instead.

Set a cron schedule to run the search every five minutes.

1. In the **Cron Schedule** field, type `*/5 * * * *`.
2. For **Scheduling**, select **Real-time**.

Optionally, you can set a schedule window and a schedule priority for the search. The schedule priority setting overrides the schedule window setting, so you do not need to set both.

When there are many scheduled reports set to run at the same time, specify a schedule window to allow the search scheduler to delay running this search in favor of higher-priority searches. When detecting excessive failed logins, time matters but there are other searches that are more important so you want to use the automatic setting to rely on the search scheduler.

1. Type a **Schedule Window** of **0** to not use a schedule window. If you want, type **auto** to use the automatic schedule window set by the scheduler, or type a number that corresponds with the number of minutes that you want the schedule window to last. For example, type **15** to set a schedule window 15 minutes long.

If this search is more important to run and see results from than other searches, you can change the schedule priority to "Higher" or "Highest" instead of the default. Detecting excessive failed logins is a priority, but not higher than other potential security incidents.

1. Select a **Schedule Priority** of **Default**.

Define trigger conditions for the alerts

You can choose to trigger an alert based on a number of factors associated with the search. By default, the trigger conditions are set to alert you when the number of results is greater than zero. For this search, leave the default value.

Set up throttling to limit the number of alerts

Set up throttling to limit the number of alerts generated by your correlation search. By default, each result returned by the correlation search generates an alert. Typically, you only want one alert of a certain type. You can set up throttling to prevent a correlation search from creating more than one alert of a certain type.

1. Type a **Window Duration** of **1** and select **day(s)** from the drop-down list to throttle alerts to 1 per day.
2. Type **app** and **src** as **Fields to group by**. You want to select the fields here that you split the aggregates by.

This means that no matter how many Excessive Failed Logins correlation search matches there are in one day that contain the same app and source field values, only one alert is created.

Next Step

Part 5: Choose available adaptive response actions for the correlation search.

Part 5: Choose available adaptive response actions for the correlation search

After you write the correlation search and determine how often the search runs and performs actions, choose which response actions the search should perform. Determine which response actions are appropriate for your search and add them to the search.

The Excessive Failed Logins search creates a notable event alerting security analysts to the fact that a host has a large number of failed logins, and modifies the risk score of the host by 60 to ensure that analysts are able to identify that it is a host that people are attempting (and failing) to log in to.

Create a notable event for analysts to triage.

1. Click **Add New Response Action** and select **Notable** to add a notable event.
2. Type a **Title** of **Excessive Failed Logins - Tutorial**.
3. Type a **Description** of **The system src has failed app authentication $count$ times using $user_count$ username(s) against $dest_count$ target(s) in the last hour**.
4. Select a security domain of **Access**.
5. Select a **Severity** of **medium**.
6. Leave the **Default Owner** and **Default Status** as **leave as system default**.
7. Type a **Drill-down name** of **View all login failures by system src for the application app**.
8. Type a **Drill-down search** of

   ```
   | from datamodel:"Authentication"."Failed_Authentication" | search src="$src$" app="$app$"
   ```

   This search shows the contributing events for the notable event.
9. Type a **Drill-down earliest offset** of **$info_min_time$** to match the earliest time of the search.
10. Type a **Drill-down latest offset** of **$info_max_time$** to match the latest time of the search.
11. (Optional) Add **Investigation Profiles** that apply to the notable event.
    For example, add an investigation profile that fits a use case of "Malware" to malware-related notable events.
12. Add the `src`, `dest`, `dvc`, and `orig_host` fields in **Asset Extraction** to add the values of those fields to the investigation workbench as artifacts when the notable event is added to an investigation.
13. Type the `src_user` and `user` fields in **Identity Extraction** to add the values of those fields to the investigation workbench as artifacts when the notable event is added to an investigation.
14. (Optional) Add **Next Steps** for an analyst to take when triaging this notable event. Use next steps if you want to recommend response actions that should be taken in a specific order. For example, "**Ping a host to determine if it is active on the network. If the host is active, increase the risk score by 100, otherwise, increase the risk score by 50**." You can only type plain text and links to response actions in the format of `[[action|ping]]`.
15. (Optional) Add **Recommended Actions** for an analyst to run when triaging this notable event.

Create a second response action to increase the risk score of the system on which the failed logins occurred.

1. Click **Add New Response Action** to add a risk score.
2. Click **Risk Analysis**.

3. Type a **Risk Score** of **60**.
4. Type a **Risk Object Field** of **src**.
5. Select a **Risk Object Type** of **System**.

Save the correlation search

1. Click **Save** to save the correlation search.

Next Step

Additional resources for creating a correlation search.

Additional resources for creating a correlation search

Additional resources to assist you with creating your own correlation searches can be found in the following places.

Data source selection

For information on choosing a data model as a data source, see What data models are included in the *Splunk Add-on for Common Information Model*.

For information about choosing a lookup table as a data source, see Introduction to lookup configuration in the *Knowledge Manager Manual* and Create and manage lookups in Splunk Enterprise Security in *Use Splunk Enterprise Security*.

Defining your search

For information about aggregate functions, see the Splunk platform documentation.

- For Splunk Enterprise, see Use the stats command and functions in the Splunk Enterprise *Search Manual*.
- For Splunk Cloud Platform, see Use the stats command and functions in the Splunk Cloud Platform *Search Manual*.

For examples of time modifiers, see the Splunk platform documentation.

- For Splunk Enterprise, see Specify time modifiers in your search in the Splunk Enterprise *Search Manual*.
- For Splunk Cloud Platform, see Specify time modifiers in your search in the Splunk Cloud Platform *Search Manual*.

Search scheduling

For information on real-time and continuous search scheduling, see the Splunk platform documentation.

- For Splunk Enterprise, see Real-time scheduling and continuous scheduling in the Splunk Enterprise *Reporting Manual*.
- For Splunk Cloud Platform, see Real-time scheduling and continuous scheduling in the Splunk Cloud Platform *Reporting Manual*.

For information on search schedule priority, see the Splunk platform documentation.

- For Splunk Enterprise, see Prioritize concurrently scheduled reports in Splunk Web in the Splunk Enterprise *Reporting Manual*.
- For Splunk Cloud Platform, see Prioritize concurrently scheduled reports in Splunk Web in the Splunk Cloud Platform *Reporting Manual*.

Alerting conditions

For information on trigger conditions and configuring those conditions for a search, see the Splunk platform documentation.

- For Splunk Enterprise, see Configure alert trigger conditions in the Splunk Enterprise *Alerting Manual*.
- For Splunk Cloud Platform, see Configure alert trigger conditions in the Splunk Cloud Platform *Alerting Manual*.

Notable event details

For details about how to make sure that additional fields appear in the notable event details, see Change notable event fields in *Administer Splunk Enterprise Security*.