Splunk® Enterprise Security
Administer Splunk Enterprise Security 7.0.1

Create correlation searches in Splunk Enterprise Security

Generated: 4/29/2022 10:14 pm

Create correlation searches in Splunk Enterprise Security

You can create your own correlation searches to create notable events, modify risk scores, and perform other adaptive response actions automatically based on a correlation in events. There are two ways to create correlation searches in Splunk Enterprise Security.

- Create a correlation search manually if you are an expert with SPL. You can review the included correlation searches for examples of the search methodology and available options. Test your correlation search ideas on the **Search** page before implementing them.
- For more assistance with the syntax of correlation searches, use the guided search creation wizard to create a correlation search. The guided search creation wizard allows you to create a correlation search that uses data models or lookups as the data source. The wizard takes your choices about the data source, time range, filtering, aggregate functions, split-by fields, and other conditions and builds the syntax of the search for you. See Create a correlation search in *Splunk Enterprise Security Tutorials* for a step-by-step tutorial of creating a correlation search.

For details about how to make sure that additional fields appear in the notable event details for a custom correlation search, see Change notable event fields.

See also

- Configure correlation searches in Splunk Enterprise Security
- List correlation searches in Splunk Enterprise Security