Splunk® Enterprise Security Splunk
Enterprise Security Tutorials 5.3.1

Part 2: Create a correlation search

Generated: 11/07/2019 9:40 am
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 100 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.