Splunk® Enterprise Security
Administer Splunk Enterprise Security 7.0.1

Correlation search overview for Splunk Enterprise Security

Generated: 6/09/2022 12:21 am

Correlation search overview for Splunk Enterprise Security

A **correlation search** scans multiple data sources for defined patterns. When the search finds a pattern, it performs an **adaptive response action**.

Correlation searches can search many types of data sources, including events from any security domain (access, identity, endpoint, network), asset lists, identity lists, threat intelligence, and other data in Splunk platform. The searches then aggregate the results of an initial search with functions in SPL, and take action in response to events that match the search conditions with an adaptive response action.

- To create a correlation search, see Create a correlation search in *Splunk Enterprise Security Tutorials*.
- To set up or modify correlation searches in your environment, see Configuring correlation searches.

Examples of correlation searches

- Identify an access attempt from an expired account by correlating a list of identities and an attempt to authenticate into a host or device.
- Identify a high number of hosts with a specific malware infection, or a single host with a high number of malware infections by correlating an asset list with events from an endpoint protection system.
- Identify a pattern of high numbers of authentication failures on a single host, followed by a successful authentication by correlating a list of identities and attempts to authenticate into a host or device. Then, apply a threshold in the search to count the number of authentication attempts.

Correlation searches with special characters

Correlation searches that have special characters may display an error message "Search Does Not Exist" if on-premise customers use a reverse proxy. Using Nginx as a reverse proxy in Splunk Enterprise Security may encode special characters that can prevent correlation searches from being discovered by Splunk Enterprise Security. As a workaround, you may clone the correlation search and remove the special characters in the clone, then disable the original correlation search. Additionally, it is recommended to configure your reverse proxy to not encode special characters.