About event grouping and correlation

Generated: 12/20/2019 5:47 am
About event grouping and correlation

Event correlation is finding relationships between seemingly unrelated events in data from multiple sources to answer questions like, "how far apart in time did a specific set of events occur?" or "what's the total amount of time it took for a transaction to complete?"

Splunk software supports event correlations using time and geographic location, transactions, sub-searches, field lookups, and joins.

- Identify relationships based on the time proximity or geographic location of the events. Use this correlation in any security or operations investigation, where you might need to see all or any subset of events that take place over a given time period or location.
- Track a series of related events, which may come from separate IT systems and data sources, together as a single transaction. Identify the amount of time it took to complete the transaction and the number of events within a single transaction.
- Use a sub-search to take the results of one search and use them in another. Create conditional searches, where you see the results of a search only if the sub-search meets certain thresholds.
- Correlate your data to external sources with lookups.
- Use SQL-like inner and outer joins to link two completely different data sets together based on one or more common fields.

This chapter discusses three methods for correlating or grouping events:

- Use time to identify relations between events
- Use subsearch to correlate events
- Use transactions to identify and group related events

You can also use field lookups and other features of the search language. Depending on your search criteria and how you want to define your groupings, you may be able to use a search command, such as append, associate, contingency, join, or stats. Sometimes, there is no single command that you can use.

If you're not sure where to start, the following flow chart can help you decide whether to use a lookup, define a transaction, or try another search command to define your event grouping.
In most cases, you can accomplish more with the stats command or the transaction command; and these are recommended over using the join and append commands. You can read more about when to use stats and transaction in the topic "About transactions" later in this chapter. You can also read more about the stats commands in the "Calculate Statistics" chapter of this manual.

Note: The information for this diagram was provided by Nick Mealy.