Mandiant

CORRELATED EVENTS

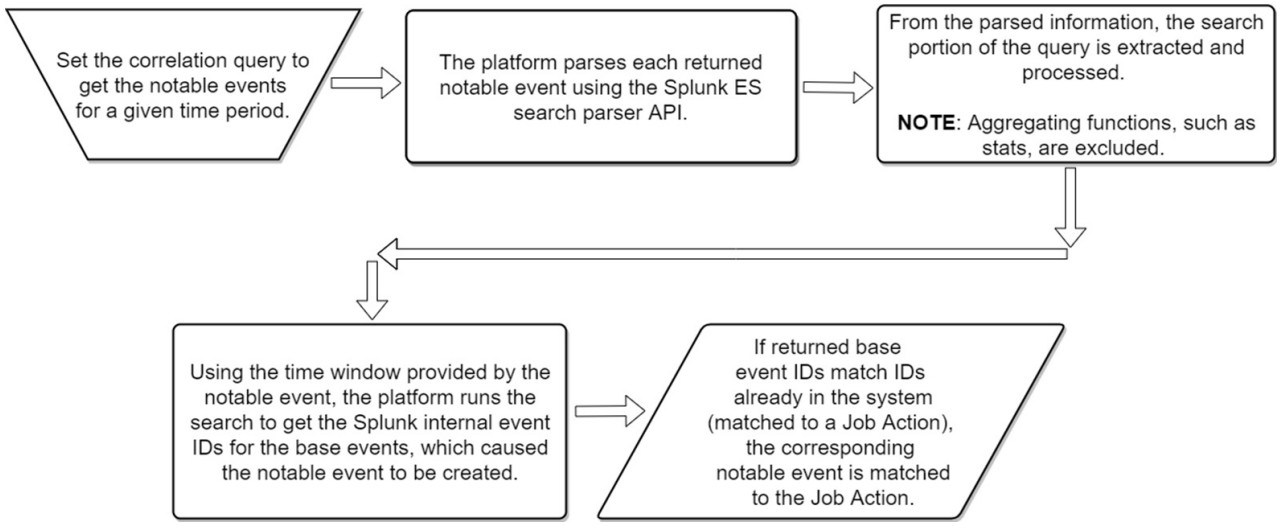
Event correlation is a method that uses security technology event data to analyze and identify relationships. Different events are connected to identifiable patterns through event correlation. If those patterns pose a threat to security, event correlation offers a full context and logical analysis through a sequence of related events. As a result, security analysts are able to make a well-thought-out decision on what to do next to respond and investigate.

The Security Validation integrations work on a premise of getting `raw_events` and `raw_alerts` from a security technology. Integrations convert raw events and alerts into a standard data model (such as `src_ip`, `dst_ip`, `host`) by means of translation. At this translation stage, the UID is determined for an event. Often times, it's a value that is taken from the security technology API data. However, not all technologies provide an acceptable UID. In these cases, a UID is synthesized by MSV through a process of combining multiple fields and generating a unique value. This UID for each event is fundamental to the alert, as it's the value that makes up the `base_events_uids` in the alert. If an event has a UID that matches a UID from the alert's `base_events_uids` list, it's considered to be correlated.

Not all events are correlated with an alert, and in certain systems, not all alerts will have a correlated `base_events_uids` list.

Correlated Events in Splunk Integration

As an example, consider the Splunk integration. In this integration, you can correlate events when the data is indexed. The Security Validation Platform matches correlated events to a Job Action only if one of its base events was matched to a Job Action. When a base event is matched, the platform uses the correlation query to find events that matched Actions and their corresponding base events. See the following image for an example of a correlation query workflow.



Example of a correlation query for Splunk ES

Event correlation is summarized in the following steps:

1. **Event Filtering**: In this step, you set the time period to get the notable events using a correlation query.
2. **Event Parsing**: Extract the search portion of the query and process it using the Splunk ES search parser API.
3. **Event Aggregation**: In this step, the exact duplicates of the same event are also merged. Such duplicates may have been caused by network instability. For example, suppose that the same event is sent twice by the event source. The first instance was not acknowledged in time, but both instances eventually arrived at the event destination.

4. **Get Splunk internal Event IDs**: Using the time window provided, the platform runs the search to get the Splunk internal event IDs for the base events.
5. **Root Cause Analysis**: It consists of analyzing dependencies between events. In this step, you detect whether some events can be explained by others. If the base event IDs match to a Job Action, the corresponding notable event is matched to the Job Action.

Intrusion detection is a scenario where event correlation can be used. For instance, suppose that an employee account has not been accessed for a long time and suddenly many login attempts are noticed. That account may start executing suspicious commands. Event correlation can be used in this scenario to send an alert that indicates an attack is in progress.

See **Splunk (https://docs.mandiant.com/home/msv-splunk)** and **Splunk Enterprise Security (https://docs.mandiant.com/home/msv-splunk-enterprise-security)** articles for more information and sample correlation queries.