Working with event analytics in ITSI

Event Analytics in Splunk ITSI is where you can streamline your incident management workflows, from alert management to incident response triggers.

Get Started with Event Analytics

Ingest events through correlational searches.

The data itself comes from Splunk indexes, but ITSI only focuses on a subset of all Splunk Enterprise data. This subset is generated by correlation searches. A correlation search is a specific type of saved search that generates notable events from the search results.

See Overview of correlation searches in ITSI.

Configure aggregation policies to group events into episodes.

Once notable events start coming in, they need to be organized so you can start gaining value from them. Configure an aggregation policy to define which notable events are related to each other and group them into episodes. An episode contains a chronological sequence of events that tells the story of a problem or issue. In the backend, a component called the Rules Engine executes the aggregation policies you configure.

For more information, see Overview of aggregation policies in ITSI.

Set up automated actions to take on episodes.

You can run actions on episodes either automatically using aggregation policies or manually in Episode Review. Some actions, like sending an email or pinging a host, are shipped with ITSI. You can also create tickets in external ticketing systems like ServiceNow, Remedy, or VictorOps. Finally, actions can also be modular alerts that are shipped with Splunk add-ons or apps, or custom actions that you configure.

For more information, see Configure episode action rules in ITSI.

To learn more about event analytics, see the documentation and Event Analytics section (step 7 / 8) on the Splunk ITSI interactive demo.

Event Analytics Best Practices for Third-Party Data Sources

To avoid duplicate events, use the same frequency and time range in correlation searches.

When configuring a correlation search, consider using the same value for the search frequency and time range to avoid duplicate events. For example, a search might run every five minutes and also look back every five minutes.
If there's latency in your data and you need to look for events you might have missed, consider expanding the time range. For example, the search could run every minute but look back 5 minutes.

**To reduce load on your system, don't use a time range greater than 5 minutes.**

Exceeding a calculation window of 5 minutes can put a lot of load on your system, especially if you have a lot of events coming in. If you want to avoid putting extra load on your system, consider reducing the time range to 5 minutes or less.

One exception is if your data is coming in more sporadically. For example, if your data comes in every 15 minutes, consider using a 15-minute time range.

**Normalize all the important fields in your third-party events.**

When you're creating correlation searches, don't only normalize on obvious fields that exist in a lot of data sources, like host, severity, event type, message, and so on. It's also important to normalize fields that you know are important in your events. For example, when you're looking at Windows event logs, what do you look at to know if something is good or bad? Normalize those fields as well and use them to build out a common information model.

Perform this normalization process for every data source you have so you can easily identify important fields when creating aggregation policies.

**Create one correlation search per data source.**

For every third-party data source you're bringing into ITSI, create a single correlation search to normalize those fields and generate notable events. For example, one for SCOM, one for SolarWinds, and so on.

**Don't create too many aggregation policies.**

Limit the number of aggregation policies you enable in your environment. Too many aggregation policies create too many groups, which produces an overly granular view of your IT environment. By limiting the number of policies, you create more end-to-end visibility and avoid creating silos of collaboration between groups in your organization. Make sure to group events according to how those events are related, not based on how people work to resolve those issues.

**Only select 5-10 fields for Smart Mode analysis.**

---

**Additional Resources**

- Webinar: [Getting Started with ITSI part 2](#)
- Blog post: [Event Storms with ITSI](#)

---

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.