Reducing alert fatigue from external monitoring tools

Alerts originating from external monitoring tools can cause you frustration when they are high-volume and they lack the contextual information to determine their importance.

You can remedy this by using Splunk ITSI to group events together and reduce noise. You'll follow a four-step process to do this:

1. **Clean and prepare the raw alert events.**
2. **Create notable events from the alerts.**
3. **Apply service context and configure the event grouping.**
4. **Review episodes and take actions**, such as running a script, pinging a host, or creating tickets in external systems.

### Step 1 - Clean and prepare the raw alert events

1. Ingest the raw monitoring tool alerts into Splunk. Splunk provides supporting add-ons in Splunkbase for many monitoring tools which you can use to help get alerts in.

   ```splunk
   index=itsidemo sourcetype=[sourcetype] perfdata=SERVICEPERFDATA
   ```

2. Once the alerts are ingested, expand one of the alerts and review the raw event as well as the extracted fields.

   ```splunk
   index=itsidemo sourcetype=[sourcetype] perfdata=SERVICEPERFDATA
   ```

3. Normalize the data. While each monitoring tool will express events differently, they all communicate the same fundamental information. For example, how severe is the event? To which machine is the event associated? What type of check or test was performed? To facilitate the grouping of multiple events from multiple monitoring tools, you'll need to normalize this key information so that a common set of field names and values is used.

   Use this SPL to create normalized severity, instance, and test fields.

   ```splunk
   index=itsidemo sourcetype=[sourcetype] perfdata=SERVICEPERFDATA
   | eval norm_severity=case(severity="CRITICAL",6,severity="WARNING",4, severity="OK", 2)
   | eval norm_instance= src_host
   | eval norm_test=name
   | table _time, name, severity, norm_severity, norm_instance, norm_test
   | sort _time
   ```

4. You'll need to do some deduplication of events before you include them in Splunk ITSI. Adjust your SPL to do this.

   ```splunk
   index=itsidemo sourcetype=[sourcetype] perfdata=SERVICEPERFDATA
   ```

---

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.
5. Next, add some service context if you need to see the services affected by an alert by adding which field in the data is used to match to the service, making correlation possible for different alerts in a service.

index=itsidemo sourcetype=[sourcetype] perfdata=SERVICEPERFDATA
| eval norm_severity=case(severity=="CRITICAL",6,severity=="WARNING",4, severity=="OK", 2)
| eval norm_instance= src_host
| dedup consecutive=true src_host severity name
| sort - _time
| table _time, name, norm_instance, severity, norm_severity
| eval total=1

Step 2 - Create Notable Events from the alerts

Next, you'll convert normal Splunk events into notable events by creating a correlation search in Splunk ITSI. Correlation searches are built to regularly scan for interesting events, such as your alerts, and document them as notable events in Splunk ITSI.

1. Click the Configure menu in the top toolbar of Splunk ITSI, then click Correlation Searches and Create a new search.
2. Fill in the search properties:
   - Name your search.
   - Paste the SPL in the search.
   - Time range: Last 5 minutes (select ‘relative’ in time picker)
   - Run Every: 5 minutes
   - Entity Lookup Field: host
   - Populate Notable Event Title
   - Populate Notable Event Description
   - Severity: Advanced Mode
   - Click Save.

Now you have created a correlation search that will continuously scan for new events and, when they are found, will create ITSI Notable Events.

Step 3 - Apply service context and configure the event grouping

Now that you've created notable events, ensure you are grouping them together by time and by service. To configure
how notable events will be grouped, you'll need to build an aggregation policy which describes how to group related notable events.

1. Click the Configure menu in the top toolbar of Splunk ITSI, then click Notable Event Aggregation Policies.
2. Edit the policy you are interested in.
3. Review the configurations:
   1. Include the events if
   2. Split events by field
   3. Break episode. You may want to modify the “Break episode” configuration from the default 3600 seconds as an hour may be too long.
4. Click Preview Results to see how Splunk ITSI is now grouping events together based on your configurations.
5. Click Save to save the changes to the policy.

---

**Step 4 - Review episodes**

When notable events are grouped by aggregation policies, the resulting groups are called episodes. Episodes are 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.

After you have reviewed episodes, you can also configure episode action rules if you want to perform actions such as sending an email, pinging a host, or creating a ticket.

1. Click Episode Review in the top toolbar of Splunk ITSI. The episode review page provides information in a heads-up display and is like a cockpit view for Operations teams.
2. Note the Noise Reduction.
3. Scroll down and review the list.
4. Filter the results. Click the Filter button, then select the Severity field. Tick only Critical and High events.
5. Now you can review an episode to better understand the flow of events, and make sure that someone has ownership.
6. Click on the episode you are interested in. Review the details for each tab, and add any comments as necessary. Here you can also change the status of an episode, for example from Pending to In Progress, and review possible actions.
Next steps

These additional Splunk resources might help you understand and implement these recommendations:

- Splunk Docs: Event Analytics Manual