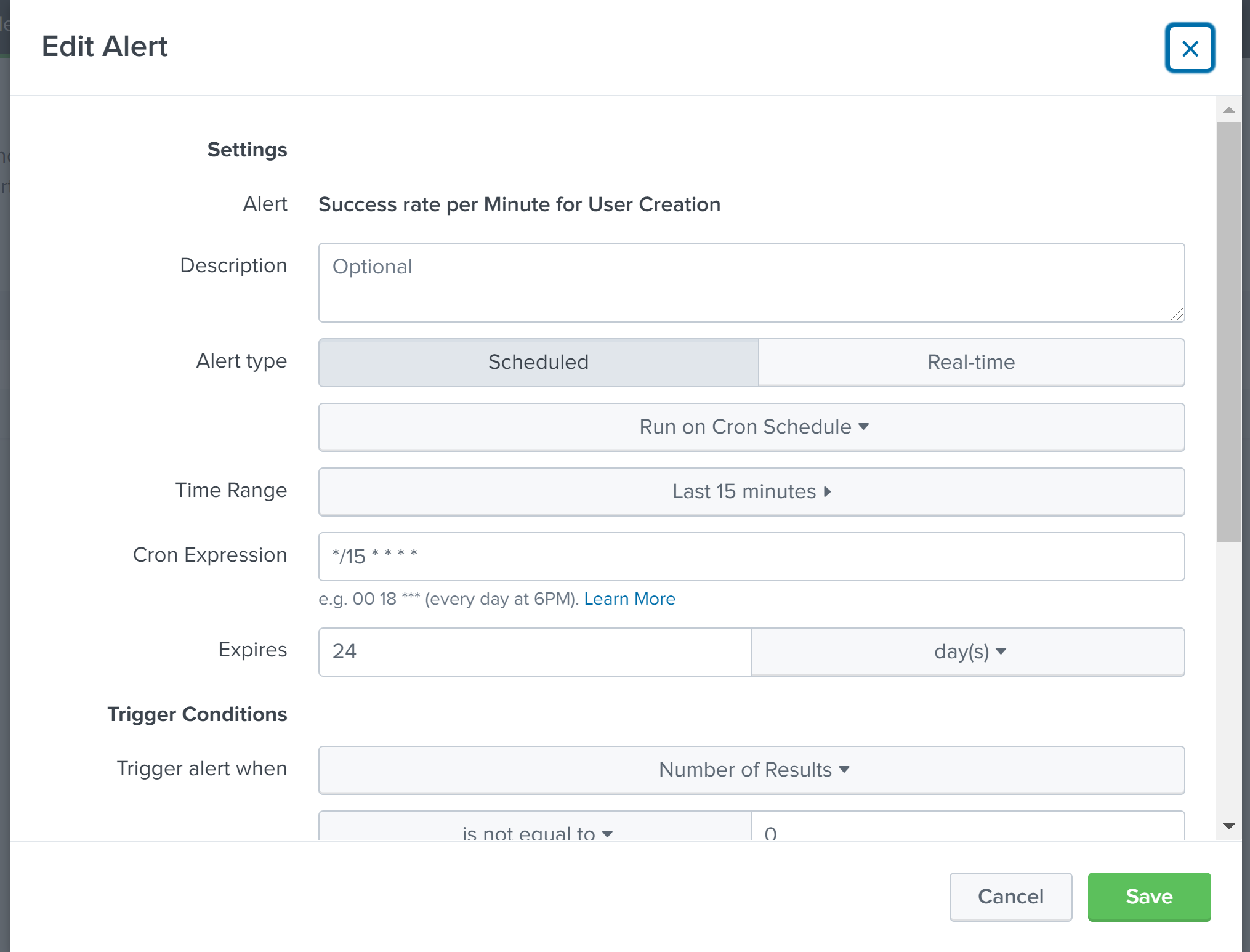
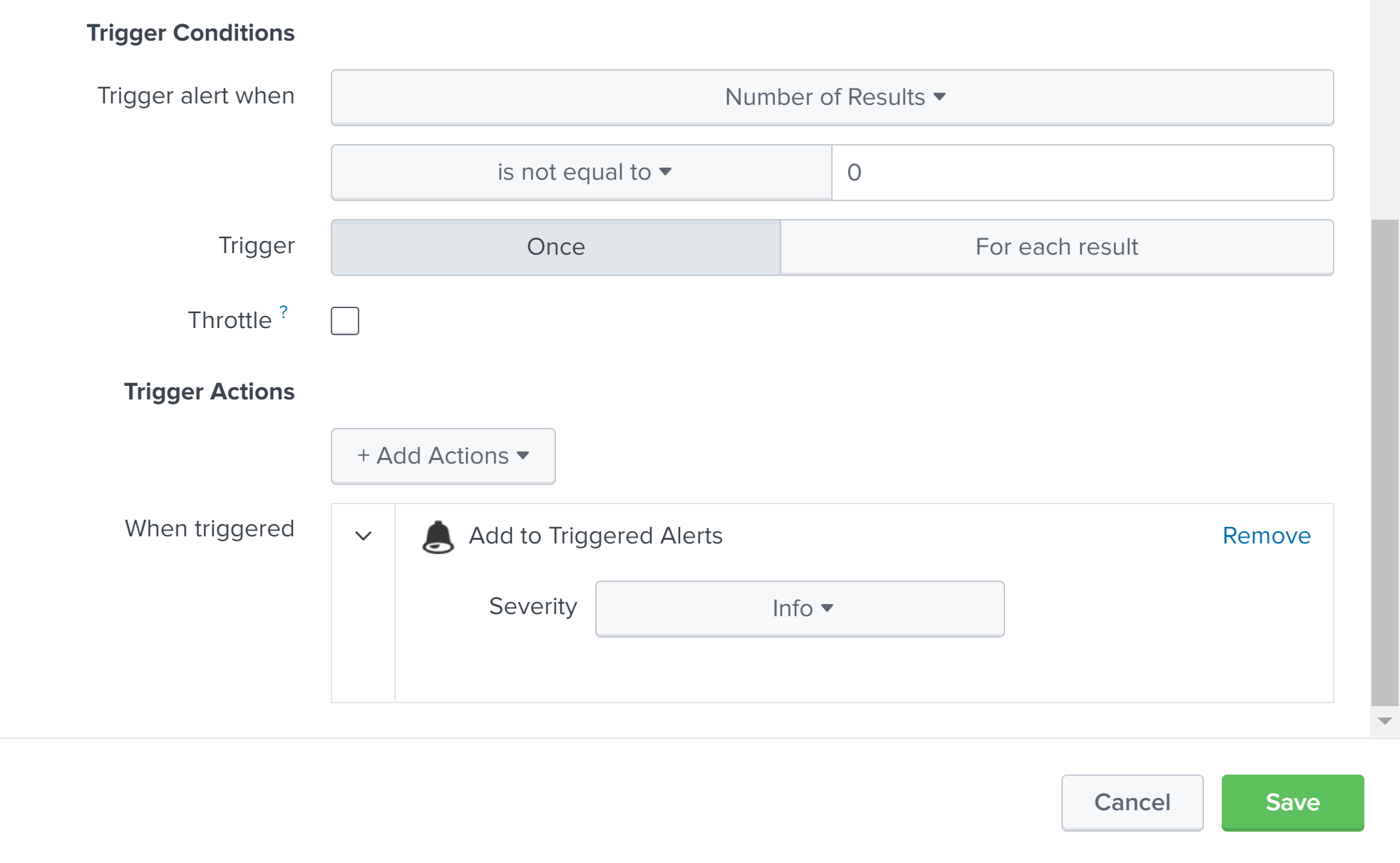
Integrated Splunk with Spring Boot application by directly sending logging information in JSON format to Splunk, to enable fast and efficient searches.

Configured two alerts:

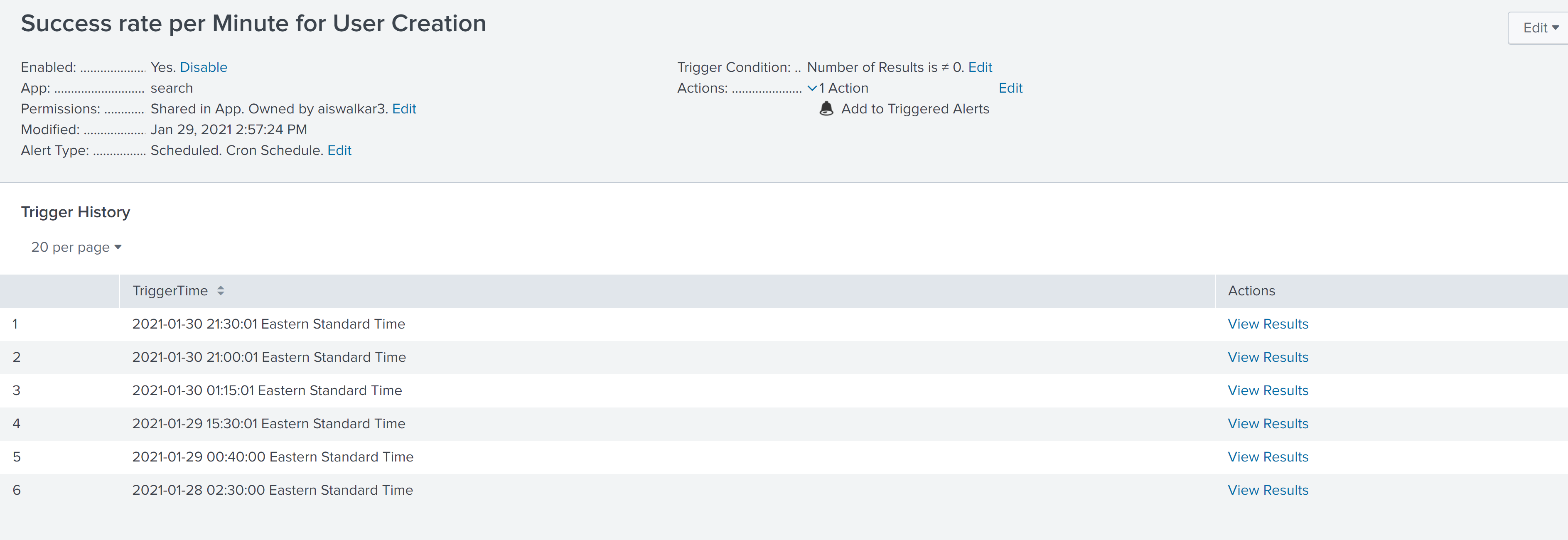
1. User creation: In User Creation, we get the success rate per minute for every 15 minutes. The alert is scheduled for every 15 minutes if we have valid user creation events. The search query is as below.

index="user\_creation" earliest=-15m@m latest= @m | spath responseCode | search responseCode != 0 | timechart span=1m count(eval(match(responseCode,"20\*"))) as count\_success count(eval(match(responseCode,"40\*") or match(responseCode,"50\*"))) as count\_failure | where count\_success > 0 or count\_failure > 0 | eval time = strftime(\_time,"%H:%M:00") | stats sum(count\_success) as count\_success sum(count\_failure) as count\_failure by time | eval success\_percent = round((count\_success/(count\_success+count\_failure))\*100,2)





Triggered alerts are as below.

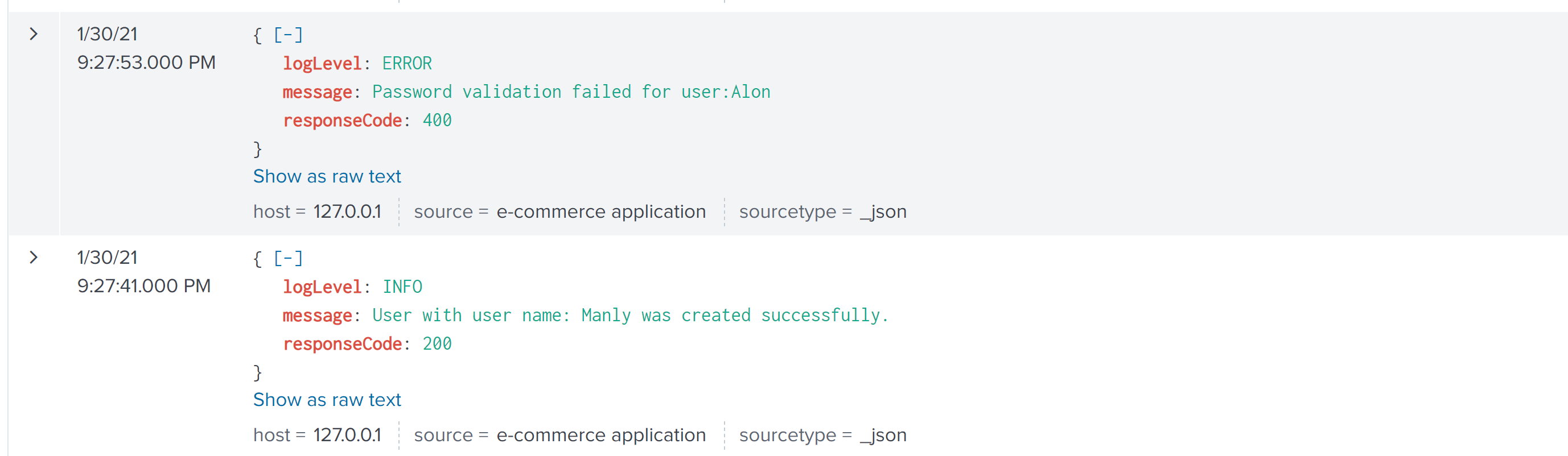


Below is the search query and the results of the latest alert.



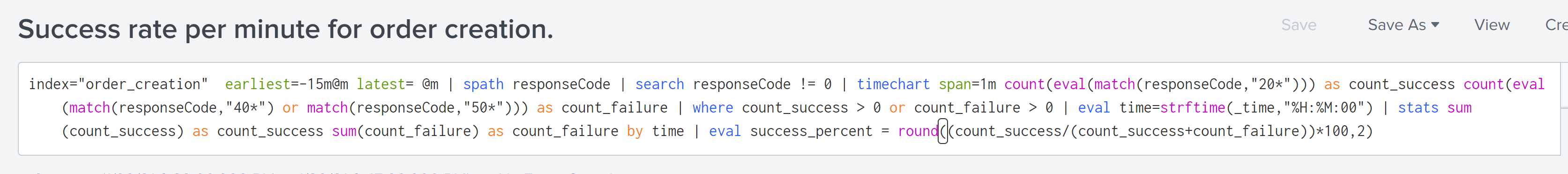
Below are the logs for the two results above.

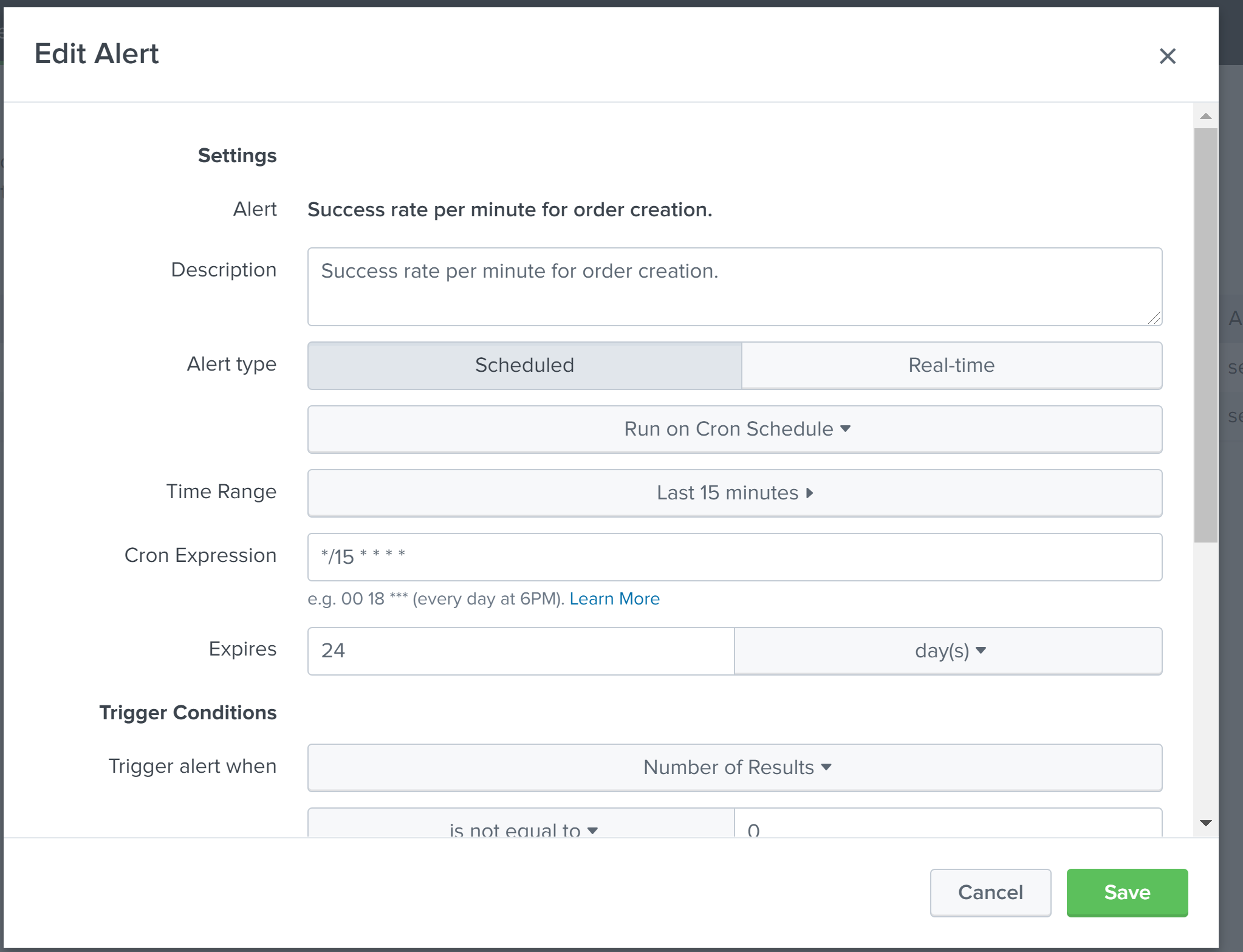


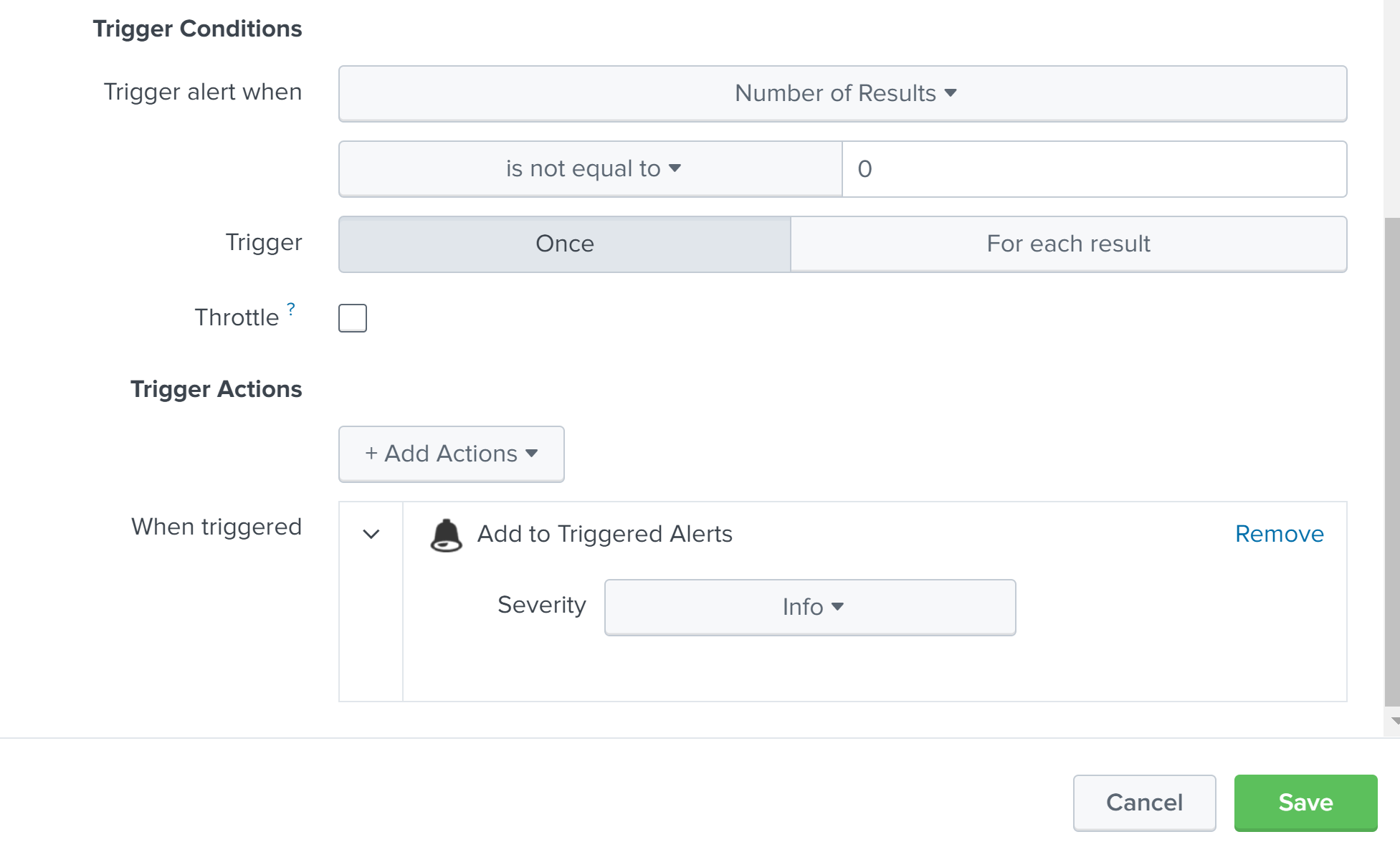


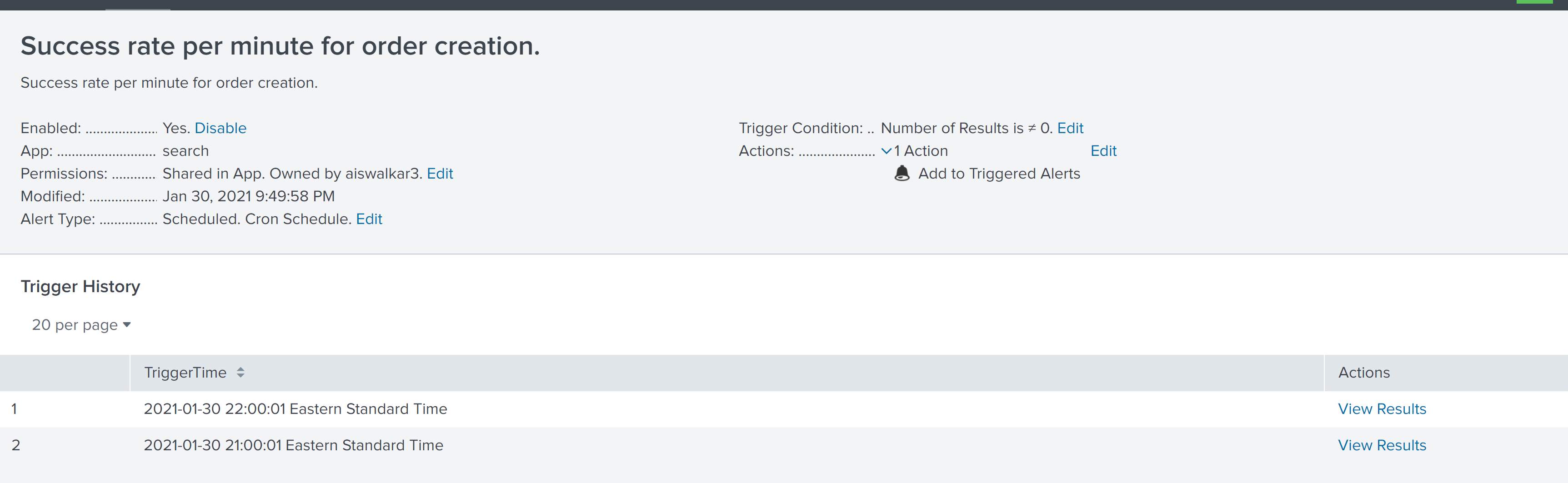
1. Order creation: In Order Creation, we get the success rate per minute for every 15 minutes. The alert is scheduled for every 15 minutes if we have valid order creation events. The search query is as below.

index="order\_creation" earliest=-15m@m latest= @m | spath responseCode | search responseCode != 0 | timechart span=1m count(eval(match(responseCode,"20\*"))) as count\_success count(eval(match(responseCode,"40\*") or match(responseCode,"50\*"))) as count\_failure | where count\_success > 0 or count\_failure > 0 | eval time=strftime(\_time,"%H:%M:00") | stats sum(count\_success) as count\_success sum(count\_failure) as count\_failure by time | eval success\_percent = round((count\_success/(count\_success+count\_failure))\*100,2)

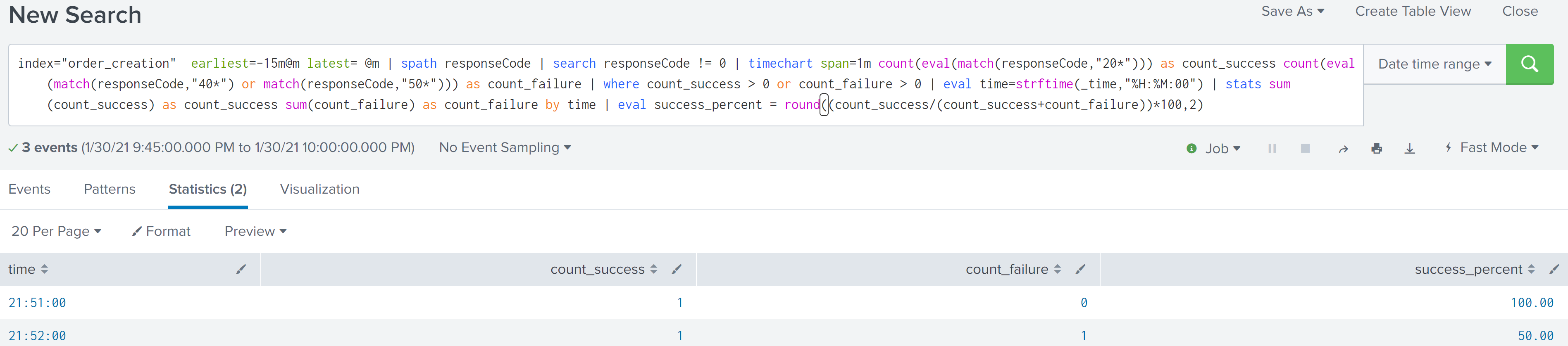


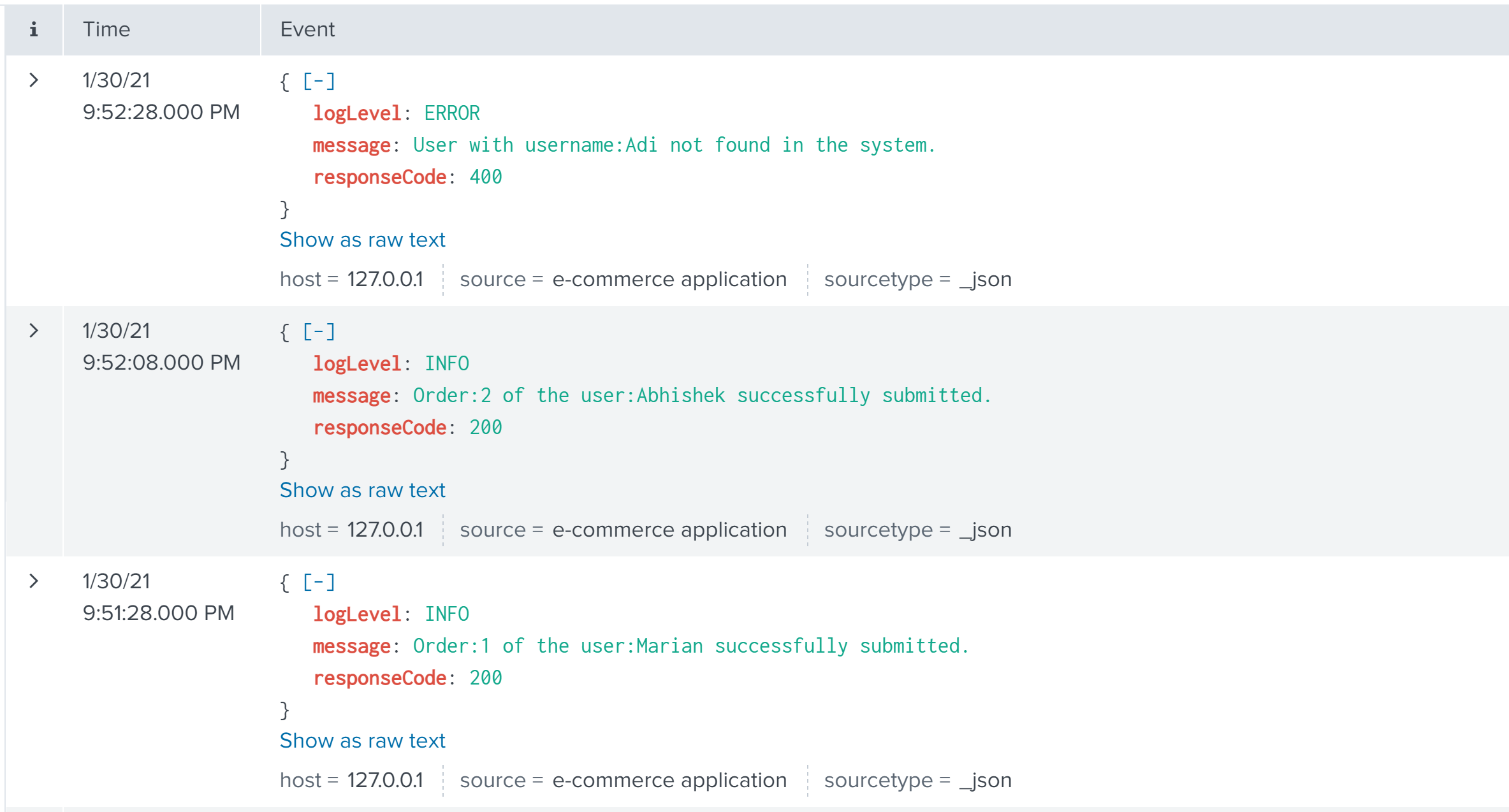






On entering the latest alert, we can see the success count, failure count and success percent.

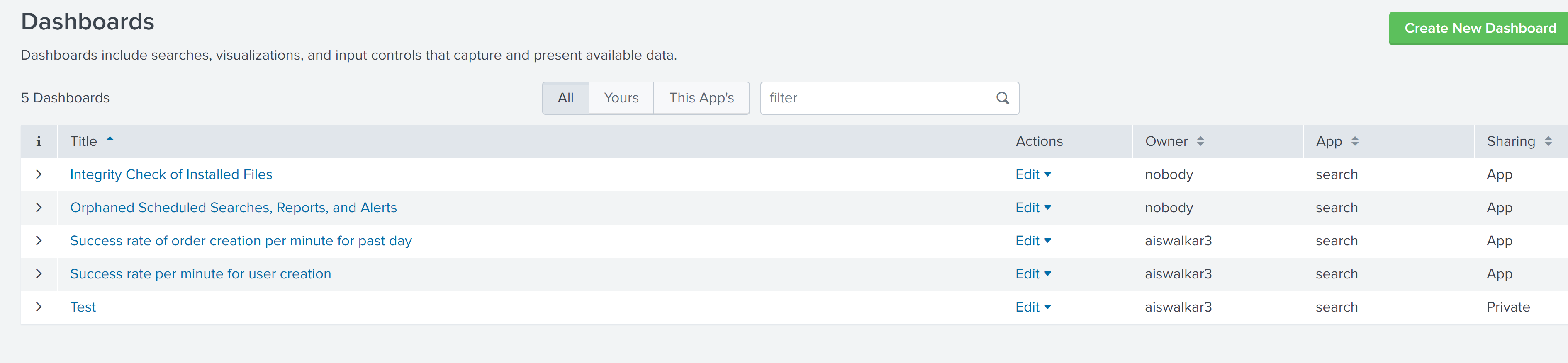




**Dashboards:**

We have two dashboards for User and Order creation.

1. Success rate of order creation per minute for past day.
2. Success rate per minute for user creation.



1. Success rate per minute for user creation. Below is the source code for it.

<form>

<label>Success rate per minute for user creation</label>

<fieldset submitButton="false">

<input type="time" token="field1">

<label></label>

<default>

<earliest>-24h@h</earliest>

<latest>now</latest>

</default>

</input>

</fieldset>

<row>

<panel>

<title>Success rate per minute for user creation for past day</title>

<chart>

<search>

<query>index="user\_creation" | spath responseCode | search responseCode != 0 | timechart span=1m count(eval(match(responseCode,"20\*"))) as count\_success count(eval(match(responseCode,"40\*") or match(responseCode,"50\*"))) as count\_failure | where count\_success &gt; 0 or count\_failure &gt; 0 | eval time = strftime(\_time,"%Y-%m-%dT%H:%M:00") | stats sum(count\_success) as count\_success sum(count\_failure) as count\_failure by time | eval success\_percent = round((count\_success/(count\_success+count\_failure))\*100,2)</query>

<earliest>$field1.earliest$</earliest>

<latest>$field1.latest$</latest>

<sampleRatio>1</sampleRatio>

</search>

<option name="charting.axisLabelsX.majorLabelStyle.overflowMode">ellipsisNone</option>

<option name="charting.axisLabelsX.majorLabelStyle.rotation">0</option>

<option name="charting.axisTitleX.visibility">visible</option>

<option name="charting.axisTitleY.visibility">visible</option>

<option name="charting.axisTitleY2.visibility">visible</option>

<option name="charting.axisX.abbreviation">none</option>

<option name="charting.axisX.scale">linear</option>

<option name="charting.axisY.abbreviation">none</option>

<option name="charting.axisY.scale">linear</option>

<option name="charting.axisY2.abbreviation">none</option>

<option name="charting.axisY2.enabled">0</option>

<option name="charting.axisY2.scale">inherit</option>

<option name="charting.chart">column</option>

<option name="charting.chart.bubbleMaximumSize">50</option>

<option name="charting.chart.bubbleMinimumSize">10</option>

<option name="charting.chart.bubbleSizeBy">area</option>

<option name="charting.chart.nullValueMode">gaps</option>

<option name="charting.chart.showDataLabels">none</option>

<option name="charting.chart.sliceCollapsingThreshold">0.01</option>

<option name="charting.chart.stackMode">default</option>

<option name="charting.chart.style">shiny</option>

<option name="charting.drilldown">none</option>

<option name="charting.layout.splitSeries">0</option>

<option name="charting.layout.splitSeries.allowIndependentYRanges">0</option>

<option name="charting.legend.labelStyle.overflowMode">ellipsisMiddle</option>

<option name="charting.legend.mode">standard</option>

<option name="charting.legend.placement">right</option>

<option name="charting.lineWidth">2</option>

<option name="refresh.display">progressbar</option>

<option name="trellis.enabled">0</option>

<option name="trellis.scales.shared">1</option>

<option name="trellis.size">medium</option>

</chart>

</panel>

</row>

<row>

<panel>

<title>Success rate per minute for user creation for past day</title>

<table>

<title>Success rate for user creation per minute</title>

<search>

<query>index="user\_creation" | spath responseCode | search responseCode != 0 | timechart span=1m count(eval(match(responseCode,"20\*"))) as count\_success count(eval(match(responseCode,"40\*") or match(responseCode,"50\*"))) as count\_failure | where count\_success &gt; 0 or count\_failure &gt; 0 | eval time = strftime(\_time,"%Y-%m-%dT%H:%M:00") | stats sum(count\_success) as count\_success sum(count\_failure) as count\_failure by time | eval success\_percent = round((count\_success/(count\_success+count\_failure))\*100,2)</query>

<earliest>$field1.earliest$</earliest>

<latest>$field1.latest$</latest>

<sampleRatio>1</sampleRatio>

</search>

<option name="dataOverlayMode">none</option>

<option name="drilldown">none</option>

<option name="percentagesRow">false</option>

<option name="refresh.display">progressbar</option>

<option name="rowNumbers">false</option>

<option name="totalsRow">false</option>

<option name="wrap">true</option>

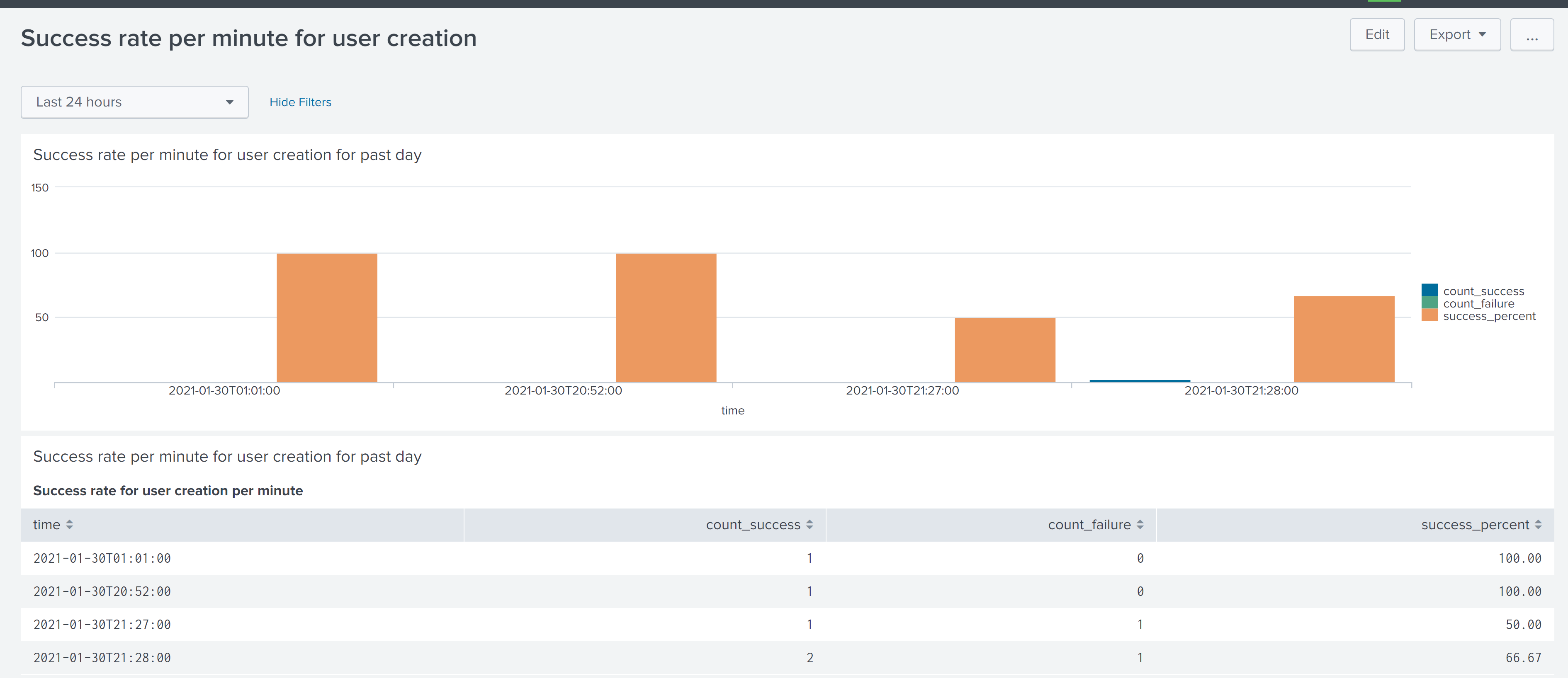
</table>

</panel>

</row>

</form>

Below is the UI for it. As can be seen, we also have a date picker which updates both the bar chart and report below it which is made inline. We have two panels for dashboard and another for report.



1. Success rate of order creation per minute for past day.

The below is the source code for it.

<form>

<label>Success rate of order creation per minute for past day</label>

<description>Success rate of order creation per minute</description>

<fieldset submitButton="false">

<input type="time" token="field1">

<label></label>

<default>

<earliest>-24h@h</earliest>

<latest>now</latest>

</default>

</input>

</fieldset>

<row>

<panel>

<title>Success rate of order creation per minute</title>

<chart>

<title>Success rate of order creation per minute</title>

<search>

<query>index="order\_creation" | spath responseCode | search responseCode != 0 | timechart span=1m count(eval(match(responseCode,"20\*"))) as count\_success count(eval(match(responseCode,"40\*") or match(responseCode,"50\*"))) as count\_failure | where count\_success &gt; 0 or count\_failure &gt; 0 | eval time=strftime(\_time,"%Y-%m-%dT%H:%M:00") | stats sum(count\_success) as count\_success sum(count\_failure) as count\_failure by time | eval success\_percent = round((count\_success/(count\_success+count\_failure))\*100,2)</query>

<earliest>$field1.earliest$</earliest>

<latest>$field1.latest$</latest>

<sampleRatio>1</sampleRatio>

</search>

<option name="charting.axisLabelsX.majorLabelStyle.overflowMode">ellipsisNone</option>

<option name="charting.axisLabelsX.majorLabelStyle.rotation">0</option>

<option name="charting.axisTitleX.visibility">visible</option>

<option name="charting.axisTitleY.visibility">visible</option>

<option name="charting.axisTitleY2.visibility">visible</option>

<option name="charting.axisX.abbreviation">none</option>

<option name="charting.axisX.scale">linear</option>

<option name="charting.axisY.abbreviation">none</option>

<option name="charting.axisY.scale">linear</option>

<option name="charting.axisY2.abbreviation">none</option>

<option name="charting.axisY2.enabled">0</option>

<option name="charting.axisY2.scale">inherit</option>

<option name="charting.chart">column</option>

<option name="charting.chart.bubbleMaximumSize">50</option>

<option name="charting.chart.bubbleMinimumSize">10</option>

<option name="charting.chart.bubbleSizeBy">area</option>

<option name="charting.chart.nullValueMode">gaps</option>

<option name="charting.chart.showDataLabels">none</option>

<option name="charting.chart.sliceCollapsingThreshold">0.01</option>

<option name="charting.chart.stackMode">default</option>

<option name="charting.chart.style">shiny</option>

<option name="charting.drilldown">none</option>

<option name="charting.layout.splitSeries">0</option>

<option name="charting.layout.splitSeries.allowIndependentYRanges">0</option>

<option name="charting.legend.labelStyle.overflowMode">ellipsisMiddle</option>

<option name="charting.legend.mode">standard</option>

<option name="charting.legend.placement">right</option>

<option name="charting.lineWidth">2</option>

<option name="refresh.display">progressbar</option>

<option name="trellis.enabled">0</option>

<option name="trellis.scales.shared">1</option>

<option name="trellis.size">medium</option>

</chart>

</panel>

</row>

<row>

<panel>

<title>Success rate of order creation per minute</title>

<table>

<title>Success rate per minute for order creation</title>

<search>

<query>index="order\_creation" | spath responseCode | search responseCode != 0 | timechart span=1m count(eval(match(responseCode,"20\*"))) as count\_success count(eval(match(responseCode,"40\*") or match(responseCode,"50\*"))) as count\_failure | where count\_success &gt; 0 or count\_failure &gt; 0 | eval time=strftime(\_time,"%Y-%m-%dT%H:%M:00") | stats sum(count\_success) as count\_success sum(count\_failure) as count\_failure by time | eval success\_percent = round((count\_success/(count\_success+count\_failure))\*100,2)</query>

<earliest>$field1.earliest$</earliest>

<latest>$field1.latest$</latest>

<sampleRatio>1</sampleRatio>

</search>

<option name="dataOverlayMode">none</option>

<option name="drilldown">none</option>

<option name="percentagesRow">false</option>

<option name="refresh.display">progressbar</option>

<option name="rowNumbers">false</option>

<option name="totalsRow">false</option>

<option name="wrap">true</option>

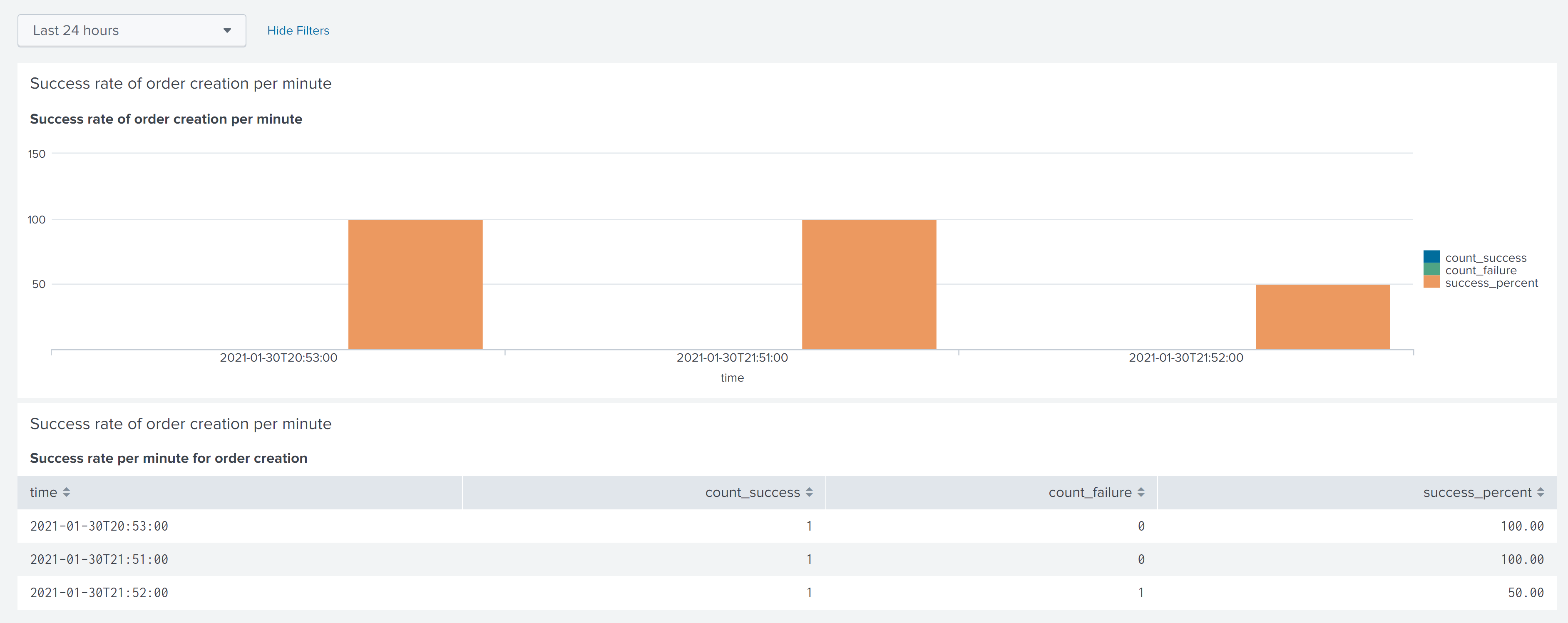
</table>

</panel>

</row>

</form>

Again, we have date picker and two panels. The upper panel has the dashboard, and the lower panel has the report. The dashboard and report change with the date picker.



Thus, the implementation of alerts, dashboards and reports is complete.