Monitoring payment responses

You work for a retail bank. Processing payments is a core function that banks like yours provide to customers. You need to be able to identify the status and response time of each payment and determine whether service level agreements are being achieved.

Data required

**Business service data** for payment processing

Procedure

- Splunk recommends that customers look into using data models, report acceleration, or summary indexing when searching across hundreds of GBs of events in a single search. The searches provided here are a good starting point, but depending on your data, search time range, and other factors, more can be done to ensure that they scale appropriately.
- Some commands, parameters, and field names in the searches below may need to be adjusted to match your environment. In addition, to optimize the searches shown below, you should specify an index and a time range when appropriate.

► Payment responses

Payments requests that have no response indicate an error condition and, more important, cause customer dissatisfaction. You need a search to be able to quickly identify and report on this problem.

```
|sourcetype=<payment processing data>
|sort _time
|stats values(action) AS action values(customer) AS customer values(amount) AS amount  count BY sessionID
|where count=1
|eval amount=tostring(round(amount, 2),"commas")
```

Need more help with this search? Click [here](#).

Knowing which responses took the longest in terms of duration to process is important to meet SLAs. Payments that take too long to process may be subject to fines and cause customer dissatisfaction.

```
|sourcetype=<payment processing data>
|eval _time=strptime(_time, "%Y/%m/%d %H:%M:%S")
|sort _time
|stats count values(customer) AS customer values(amount) AS amount  values(_time) AS _time first(epoch) AS first last(epoch) AS last BY sessionID
|where count>1
```

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.
Counts of payment requests and responses over time shows how your systems are performing. Tracking this statistic allows you to gather insights on treating your best customers to better service.

Payment SLAs

A key KPI in the financial industry is how many transactions met SLAs and did not meet SLAs for duration/response time. Payments that take too long to process may be subject to fines and cause customer dissatisfaction. Seeing the affected monetary values for such payments can help drive an organization to take action.
Customers with the most processed payments

This search shows customers who have the most payments cleared. By knowing who are the top users getting responses, you can gather insights on treating your best customers to better service.

```
| sourcetype=<call detail records>  
| eval _time = start  
| lookup <cdr disposition mapping file> disposition  
| search disposition="ANSWERED" OR disposition="BUSY"  
| rex field=src "(?<srcCountry>\d+)(?=\d{10})"  
| rex field=dst "(?<dstCountry>\d+)(?=\d{10})"  
| lookup <country code to name mapping file> phoneCode AS dstCountry OUTPUTNEW countryName AS dstCountryName ISO2 AS dstCountryCode  
| fields src dst dstCountryName duration  
| stats count list(dst) AS dst list(dstCountryName) AS dstCountryName BY duration src  
| rename duration AS "Call Duration" src AS "Caller" dst AS "Called Number" dstCountryName AS "Destination Country"  
| sort - "Call Duration"  
```

Average completed payment duration over time

Average payment duration over time shows how your systems are performing. Tracking this statistic allows you to gather insights on treating your best customers to better service.

```
| sourcetype=<payment processing data>  
| eval _time=strptime(_time, "%Y/%m/%d %H:%M:%S")  
| sort _time  
| stats count values(_time) AS _time first(epoch) AS first last(epoch) AS last BY sessionID  
| where count>1  
| eval duration=last-first  
| timechart avg(duration) span=5m fixedrange=F  
```

Next steps

Add the results of these searches to dashboards so you can monitor activity. Investigate requests and response times that do not meet your SLAs. You can also use the results to report on key performance indicators, improve your payment response application, and make decisions on how to improve customer service.

The Splunk Essentials for the Financial Services Industry app helps you automate the searches provided in this article. The app also provides more insight on how they can be applied in your environment, how they work, the difficulty level, and what data can be valuable to run them successfully. In addition, the Splunk Essentials for the Financial Services Industry app provides a number of other fraud detection solutions for financial services.
Finally, these additional Splunk resources might help you understand and implement this use case:

- .Conf Talk: 40 ways to use Splunk in financial services
- Webinar: AIB: Monitoring payments with real time insights using Splunk and ITSI