Monitoring wire transfers

Wire transfer statistics can help analytics teams gain a deeper insight into their flow of funds. These statistics include a mapping of sources and destinations for transfers to see where the majority of funds are flowing. They also include the largest amounts of transfers being made and outlier transfer.

Data required

Business service data for wire transfer transactions

Procedures

- 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.

**Wire transfer actions**

Wire transfers result in a number of action results, such as authorized, cancelled, denied, or in error. By seeing a distribution of these actions across time, you are in a better position to judge how the business is performing. View the results of this search in a column to compare a count of each result.

```
|sourcetype=<wire transfer transaction data source>
| sort -_time
| stats count BY action
| sort - count
```

You can also use the timechart command to see how the distribution of results progresses across a time range, in this example, 15 minute increments.

```
|sourcetype=<wire transfer transaction data source>
| eval _time=strptime("_time","%Y/%m/%d %H:%M:%S")
| sort _time
| timechart span=15m fixedrange=F count BY action
```

**Wire transfer errors**

When a wire transfer attempt is made resulting in an error condition, it causes a bad customer experience. You want to proactively watch for these conditions so you can investigate root cause sooner.
Wire transfer max amounts

Seeing the largest amounts being transferred over a time range with a customer name helps a bank identify customers with large accounts who are emptying some of their balance. You want to report on the top 10 largest amounts of money being transferred at a given time.

Wire transfer amount outliers

Users who have transferred amounts larger than the general population of users may be worth monitoring. By locating outliers in the amount that is being transferred, a bank can monitor which customers have the largest average transfers.

Top transfer origins and destinations over time

By seeing over time the top client and destinations where transfers originate and where they are going, you can gather a picture of your business, as well as how many transfers are initiated and received. This helps you track your top customers.

This sample search uses "clientIP", which you can replace with "destIP" when needed.
| timechart span=15m fixedrange=F count BY clientIP usenull=f limit=10

You can also view this information on a map for a better picture of origins and destinations.

- This sample search uses "clientIP" for iplocation and geostats, which you can replace with "destIP" when needed.
- This sample search assumes you have public IP addresses for these locations in your data, so that you can use the iplocation command to get the longitude and latitude instead. If you do not, you need to use a lookup with a location fields.

| sourcetype=<wire transfer transaction data source> | eval _time=strptime(_time,"%Y/%m/%d %H:%M:%S") | sort _time | search action="authorized" | iplocation clientIP | geostats count BY clientIP

---

**Linking origins and destinations of wire transfers with a Sankey visualization**

Visualizing the number of times a clientIP is linked to a location destination can help you identify trends. This may help in future planning and fraud use cases. For instance, if a destination is a source for another transfer, why is that? These are the types of questions this search can help raise. Run the search and then save the report as a Sankey visualization.

- You must have the Splunk Sankey Diagram - Custom Visualization app from Splunkbase installed on your Splunk instance to complete the visualization.

| sourcetype=<wire transfer transaction data source> | eval _time=strptime(_time,"%Y/%m/%d %H:%M:%S") | sort _time | search action="authorized" | stats count BY clientIP,destIP

---

**Next steps**

Use the results of these searches to evaluate service and improve the wire transfer experience for customers. You can also monitor unusual transactions to see whether they are one-time occurrences or regular activities. Such information can help you serve your customers better or understand when customers are at a risk of leaving your bank. When taking action on these results, be sure to follow any industry policies and regulations that are required for compliance.

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 monitoring and reporting solutions for financial services:

- ATM usage statistics
- Retail banking transactions
• Credit card statistics

You might also be interested in monitoring wire transfers for potentially fraudulent activity.

Finally, these additional Splunk resources might help you understand and implement this use case:

• Conf Talk: 40 ways to use Splunk in financial services