Monitoring ATM usage

You work for a large bank with hundreds of ATMs, each with thousands of users, and would like a view into a wide variety of statistics that reveal insights into ATM usage. Of particular interest are amounts of deposits and withdrawals for a given time period, locations of major ATM activity, and time series views of the duration of each transaction.

Data required

**Business service data** for ATM transactions

- 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.

► ATM average withdrawal and deposit amounts

To see how your ATMs are performing, two good KPIs are average deposit and average withdrawal amounts for a given period of time. If the average withdrawal is too large compared to the average deposit, your bank needs to investigate why as the reasons may vary from IT issues, fraud, or currency movements.

```
| sourcetype=<ATM transaction data>  
| eval _time=strptime(_time, "%Y/%m/%d %H:%M:%S")  
| presort 10000 -auto(_time)  
| sort - _time  
| where action="withdrawal"  
| stats avg(amount) AS average_withdrawal  
| eval average_withdrawal=tostring(round(average_withdrawal, 2),"commas")  
| appendcols [ |sourcetype=<ATM transaction data> | eval _time=strptime(_time, "%Y/%m/%d %H:%M:%S")  
| sort - _time | where action="deposit" | stats avg(amount) as average_deposit | eval average_deposit=tostring(round(average_deposit, 2),"commas") ]
```

Running the search for deposits using the **appendcols** command outputs all results into one report.

► ATM withdrawal top users

Getting the top users who withdraw money allows a bank to monitor them. This first search provides a list of top users and can be used to create a pie chart to compare their activity.

```
| sourcetype=<ATM transaction data source>  
| eval _time=strptime(_time, "%Y/%m/%d %H:%M:%S")
```

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.
This search also provides the top 10 users by withdrawal amounts sorted in descending order, but the sparkline gives a visual of activity trends for each. The main thing to monitor is lockstep activity or sudden upswing in activity for a longer time span for the search.

| sourcetype=<ATM transaction data source> | eval _time=strptime("_time","%Y/%m/%d %H:%M:%S") | sort - _time | where (action == "withdrawal") | stats sparkline sum(amount) AS totalWithdrawal BY user | sort - totalWithdrawal | head 10 | eval totalWithdrawal=tostring(round(totalWithdrawal,2),"commas")

► ATM deposit and withdrawal maps and trellis charts

The count of actions at ATM location seen visually on a map tells you at a glance which ATMs are most active and least active. This helps you see if ATMs may be down or need further capacity. It also indicates how the business is doing.

- This sample search uses a "withdrawal" action, which you can replace with "deposit" when needed.
- This sample search uses a lookup with a location field to get the required fields. If you have public IP addresses for these locations in your data, you can use the iplocation command to get the longitude and latitude instead.

| sourcetype=<ATM transaction data source> | eval _time=strptime("_time","%Y/%m/%d %H:%M:%S") | sort - _time | where (action == "withdrawal") | lookup ATM_place location OUTPUT latitude longitude | geostats count latfield=latitude longfield=longitude

By having users' ATM activities shown side-by-side, analysts can understand typical behaviors. Trellis charts give you side-by-side comparisons of how your top users are using your ATM over given time periods. This information helps you monitor your top users' activities and look for any unusual behavior like lockstep usage. Run the search and save the format or your search as Trellis.

This sample search uses a "withdrawal" action, which you can replace with "deposit" when needed.

| sourcetype=<ATM transaction data source> | eval _time=strptime("_time","%Y/%m/%d %H:%M:%S") | sort - _time | where (action == "withdrawal") | timechart span=10m fixedrange=F avg(amount) BY user useother=f
Visualizations of ATM usage

ATM durations at locations over time with a Timeline visualization

Knowing the duration of an ATM transaction over time shown by location shows you how busy a location is. Comparing all locations in one diagram can give a business the KPI it needs to understand the health of the ATMs. If a few locations show no usage, investigate why. Run the search and then save the report as a Timeline visualization.

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

```
|sourcetype=<ATM transaction data source>
|eval _time=strptime(_time, "%Y/%m/%d %H:%M:%S")
|sort - _time
|transaction user,location maxspan=5m
|table _time location duration
```

ATM fine-grained location usage over time with a Horizon visualization

ATM location usage shown across time is a KPI worth knowing. Unlike using a sparkline, seeing this data in a Horizon diagram gives a visual on increases and decreases in usage counts over time in a color coded manner. If a particular location has a high delta, it may be worth knowing. Run the search and then save the report as a Horizon visualization.

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

```
|sourcetype=<ATM transaction data source>
|eval _time=strptime(_time, "%Y/%m/%d %H:%M:%S")
|sort - _time
|timechart span=10m fixedrange=F count BY location useother=f
```

ATM withdrawals by user and location with a Sankey visualization

Withdrawals grouped by user and location for top ATM withdrawal amounts is a KPI worth knowing. Seeing this data in a Sankey diagram gives a visual on relative sizes to help you find unusual amounts, such as one user dominating the rest. 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=<ATM transaction data source>
|eval _time=strptime(_time, "%Y/%m/%d %H:%M:%S")
|sort - _time
|where action="withdrawal"
|stats count sum(amount) AS sum BY user,location
|sort - sum
```
Next steps

Use the results of these searches to evaluate service and capacity, monitor for suspicious activity, and make business recommendations. 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:

- Wire transfer statistics
- Retail banking transactions
- Credit card statistics

You might also be interested in monitoring your ATMs 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