Detecting credit card fraud

Applicability

- Product: Splunk Enterprise or Splunk Cloud Platform
- Function: Monitoring, alerting, reporting
- Data: Business service data of customer information
- A CSV or KV lookup file of categorized spending by customer

Scenario

You work for a credit card provider and need to monitor consumer transactions to prevent fraud. You are aware of various indicators of credit card fraud, and you need to analyze transactions as they occur to monitor for these indicators and surface them as suspicious through regular reporting. The Splunk platform can help increase your operational intelligence and efficiency within the financial services industry. Since the Splunk platform collects and indexes machine data in near real time, most of the searches provided here can be run in near real time, giving you a business advantage over other solutions.

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.

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.

Detect large and rapid credit card spending

A common sign of fraud is when a card is used to make a lot of purchases in a short time span, especially when the purchases are for large dollar amounts.

```
| sourcetype=<business service data>
| eval _time=strptime(_time,"%Y/%m/%d %H:%M:%S")
| sort _time
| streamstats earliest(_time) AS time earliest time latest(_time) AS latest_time time_window=1m count(action) AS num_transactions sum(amount) AS total_spent BY customer
| where ((total_spent > 5000) AND (num_transactions >= 5))
| eval latest_time=strftime(latest_time,"%Y/%m/%d %H:%M:%S"), total_spent=round(tostring(total_spent),"commas")
```
Detect outlier credit card spending by category

A common sign of fraud is when a customer starts spending large amounts of money in categories they don’t usually shop in. For example, if a customer never uses their card for travel but suddenly buys a $2,000 airplane ticket, you would be concerned.

```
| sourcetype=<business service data>
| eval _time=strptime('_time',"%Y/%m/%d %H:%M:%S")
| sort - _time
| lookup <name of lookup file of categorized spending>
| streamstats window=1 list(category) AS category BY customer
| where (amount > 1000)
| makemv delim="|" categories
| eval match=if(match(categories,category),1,0)
| where (match == 0)
| eval amount=tostring(round(amount,2),"commas")
| table customer, _time, amount, categories, category, action
```

Detect outlier credit card spending by value

A common sign of fraud with a stolen card is rarely using a card and suddenly spending a large amount.

```
| sourcetype=<customer information data source>
| eval _time=strptime('_time',"%Y/%m/%d %H:%M:%S")
| sort - _time
| stats sum(amount) AS total_spent first(_time) AS time first(previous_tx_date) AS previous_date BY customer
| where (('_time' > relative_time(strptime(previous_date,\"%m/%d/%Y %H:%M:%S\"),\"+6mon\")) AND (total_spent > 3000))
| eval total_spent=tostring(round(total_spent,2),"commas")
```

Detect an excessive number of credit card transactions in a short period

A common sign of fraud with a stolen card is a large number of transactions in a short time period.

```
| sourcetype=<customer information data source>
| eval _time=strptime('_time',"%Y/%m/%d %H:%M:%S")
| sort - _time
| streamstats earliest(_time) AS time latest(_time) AS latest_time time_window=1m count(action) AS num_transactions BY customer
| where (num_transactions >= 10)
| eval latest_time=strftime(latest_time,\"%Y-%m-%d %H:%M:%S\")
| dedup customer
```

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.
Detect credit card test purchases

A common sign of fraud is when a credit card is used to make a small purchase, immediately followed by a large purchase.

| source=<customer information data source>
| eval _time=strptime('_time',"%Y/%m/%d %H:%M:%S")
| sort _time
| streamstats earliest(amount) AS first_amount latest(amount) AS last_amount earliest(_time) AS _time latest(_time) AS latest_time time_window=1m count(action) AS num_transactions by customer
| where (((first_amount < 20) AND (last_amount > 3000)) AND (num_transactions >= 2))
| eval first_amount=tostring(round(first_amount,2),"commas"), last_amount=tostring(round(last_amount,2),"commas"), latest_time=strftime(latest_time,"%Y/%m/%d %H:%M:%S")
| table customer, _time, latest_time, num_transactions, first_amount, last_amount

Results

Analysts can investigate possible fraudulent activity and take the appropriate steps to notify the customer. This often includes alerting the customer right away to prevent further fraud since the activity could be conducted on a bot or a stolen credit card.

Additional resources

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:

- Banking fraud
- ATM fraud
- Wire transfer fraud

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

- .Conf Talk: 40 ways to use Splunk in financial services
- Blog: Detecting credit card fraud using SMLE
- .Conf Talk: Fighting fraud at Mastercard, thousands of times every second
- Tech Talk: Getting started to be PCI compliant

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 or 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.