Using Splunk for Retail Banking Cross Channel Fraud Analysis, Detection and Investigation

Commercial Bank Of Dubai

Rory Blake | Splunk Professional Services Staff Consultant
Rinaldo Ribeiro | Head of IT Risk & GRC, Risk Management

28th September 2017 | Washington, DC
Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.
Agenda
Agenda
subtitle

▶ Introductions
▶ About CBD
▶ CBD & Splunk
▶ Use Case
▶ Splunk Architecture
▶ Data Models
▶ Investigation Dashboards
▶ Alerts
▶ What’s Next
Introductions

Section subtitle goes here
Rory Blake

Splunk Professional Services Staff Consultant

- UK Based – Covering EMEA
- Nearly 6 Years Delivering Splunk PS
- 16 Countries
- 4 US States
- Product, Strategy & Technical Content
- Bat Signal Accounts
- 10 Years in Financial Services
- 2 Years Fraud Strategy
About CBD

Section subtitle goes here
About Us

The bank which leads the way to greater financial freedom and social prosperity

- Est. 1969
- 26 Branches
- 150 ATMs
- Retail and commercial banking products
- Conventional and Islamic Banking
- Total assets: AED 71 billion (£ 15 billion)
Banking designed around you
Smart, simple, always with you.

- No minimum balance required
- Real-time smart notifications
- 100% mobile
- Instant and easy to use
- Debit card hand-delivered in 24 hours
- 100s of FREE amazing discounts

UAE’s first digital bank is here.
Your bank now fits in your phone

Love the moment
Fraud In The Gulf

- Gulf region saw the highest rise in fraud incidents globally*
- 90% of executives said their company has suffered a cyber incident over past 12 months

* 2016/17 Kroll Annual Global Fraud and Risk Report
Platform Objectives

- Behavioural Analytics
- Near Real Time Proactive Detection & Prevention
- Entity & Group Profiling
- Holistic Cross Channel View
- Anomaly Detection
Splunk & CBD
Journey Timeline

<table>
<thead>
<tr>
<th>Evaluation</th>
<th>First Deployment</th>
<th>Skills Development</th>
<th>Architecture Expansion</th>
<th>New Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>Enterprise Security</td>
<td>Staff Training Investment</td>
<td>Indexer Clustering</td>
<td>Fraud Monitoring Deployment</td>
</tr>
<tr>
<td>2013</td>
<td>2014</td>
<td>2016</td>
<td>2017</td>
<td></td>
</tr>
</tbody>
</table>
Splunking Fraud At CBD

Section subtitle goes here
Project Drivers

- Constantly Evolving Threat Landscape
- Increase in Cyber Crime / Fraud Activity in the GCC and UAE
- No Existing Multi-Channel Fraud Detection Platform
- Cross Channel Fraud Detection Rules
- Near Real Time Proactive Responses
- Cumbersome Investigation Processes
- 360 Degree View of Cross Channel Customer Interactions
Banking Channels

- Credit Cards
- Debit Cards
- Digital
- Telephone & SMS
- SWIFT
Risk Platform Integration

- Device Fingerprinting
- Behavioral Profiling
- Entity Linking
- Transaction Risk Score
- Device Payment Statistics

- Data Enrichment
Data Sources
Card Transactions

Debit Cards
- Internal Platform
- DBX Connections

Credit Cards
- 3rd Party Platform Provider
- MSMQ -> DBX

Enrichment
- ATM GPS Coordinates
- Merchant Details
- Customer Demographics
Splunk Architecture
Data Models

Data Models For Fraud Detection
Data Models

Why?

▶ Cross Channel Searches became complicated very quickly
▶ Inconsistent enrichment across channels
▶ Cross channel field names inconsistencies
▶ Search performance optimization
▶ Investigation streamlining
▶ Performance issues on complex dashboards
# Data Models

## Custom Retail Banking Models

<table>
<thead>
<tr>
<th>Data Model</th>
<th>Channels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Transactions</td>
<td>Credit Cards</td>
</tr>
<tr>
<td></td>
<td>Debit Cards</td>
</tr>
<tr>
<td></td>
<td>Authorizations</td>
</tr>
<tr>
<td></td>
<td>SWIFT Payments</td>
</tr>
<tr>
<td>&lt;Risk Platform&gt;</td>
<td>Internet Banking</td>
</tr>
<tr>
<td></td>
<td>Mobile Banking</td>
</tr>
<tr>
<td>Customer Activity</td>
<td>Internet Banking</td>
</tr>
<tr>
<td></td>
<td>Mobile Banking</td>
</tr>
<tr>
<td></td>
<td>Telephone Banking</td>
</tr>
<tr>
<td>SMS</td>
<td>Outbound Communication</td>
</tr>
</tbody>
</table>
Custom Data Models
Specific To Retail Banking Fraud
Data Models
Holistic Views: An Example

| pivot Financial_Transactions All_Transactions count(All_Transactions) AS "Count of All Transaction" SPLITROW rim_no AS rim_no SPLITROW _time AS _time PERIOD hour SPLITTCOL channel SPLITTCOL status FILTER monetary_transaction = true ROWSUMMARY 0 COLSUMMARY 0 NUMCOLS 100 SHOWOTHER 1 |addtotals fieldname=total_approved "*approved" | addtotals fieldname=total_declined "*declined" | search total_declined > 2 total_approved > 2
Investigation Dashboards for Analysts

Data Models For Fraud Detection
Cross Channel Analysis
Analyst Investigation Dashboard
Mobile Banking Activity
Mobile Device & Session Investigation
Internet Banking Authentication

Analyst Investigation of Authentication & Registration
Card Transaction Geography

Card Transaction Location Analysis
Fraud Alerting
Alert: International Transaction Declines
What’s Next?
What’s Next
Looking Forward - What’s next

- Graphs are everywhere. Using graph databases for improved fraud detections
- Explore interconnectivity of data
- Explore ways to improve visualization
- Machine learning?
Key Takeaways
This is where the subtitle goes

1. Understand your own data, focus on use cases
2. It must be actionable. Careful data onboarding
3. Consider the need for Splunk professional service while building required skill sets internally
Thank You

Don't forget to rate this session in the .conf2017 mobile app