splunk> .conf2017

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

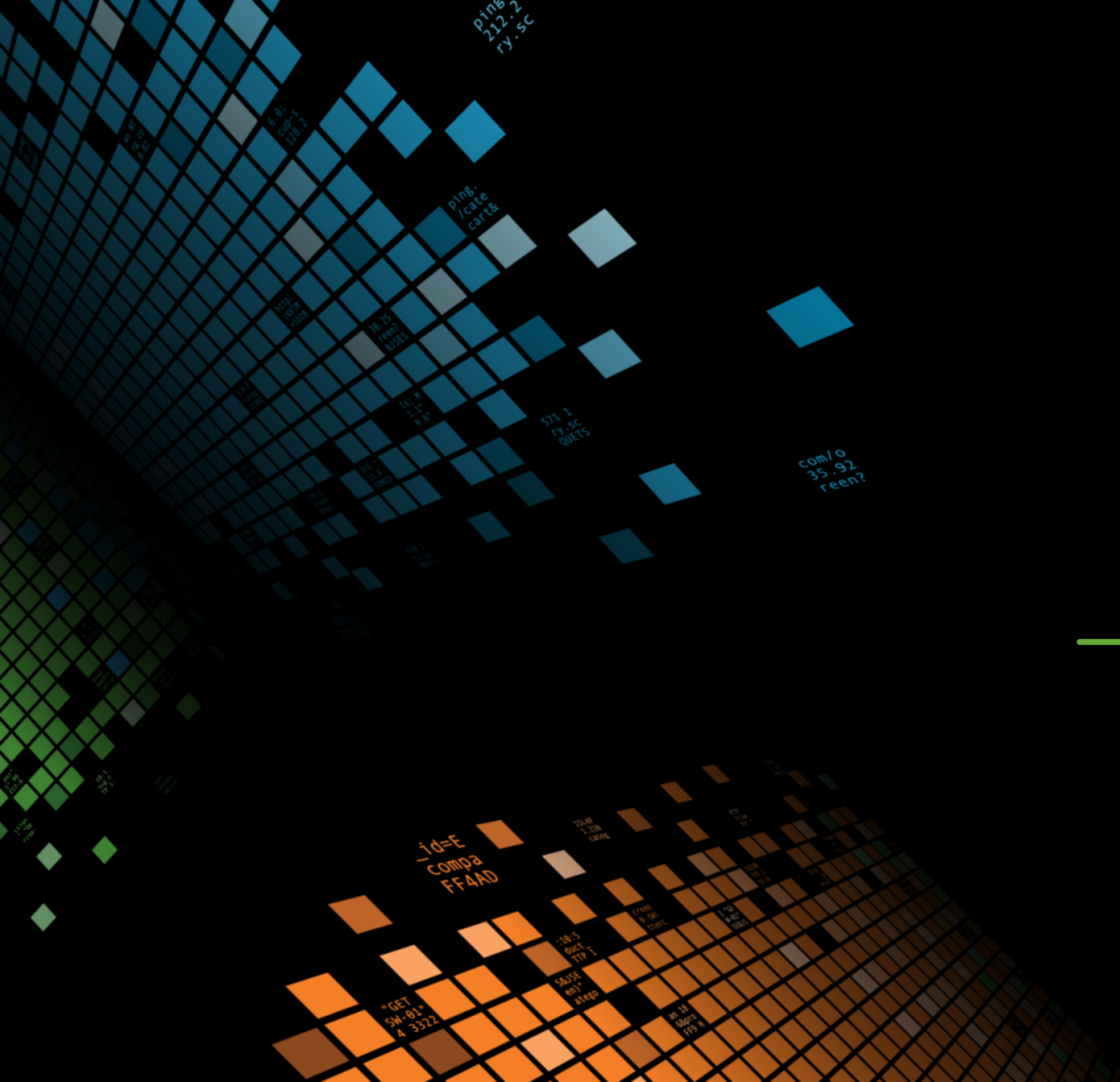
28th September 2017 | Washington, DC

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> .conf2017



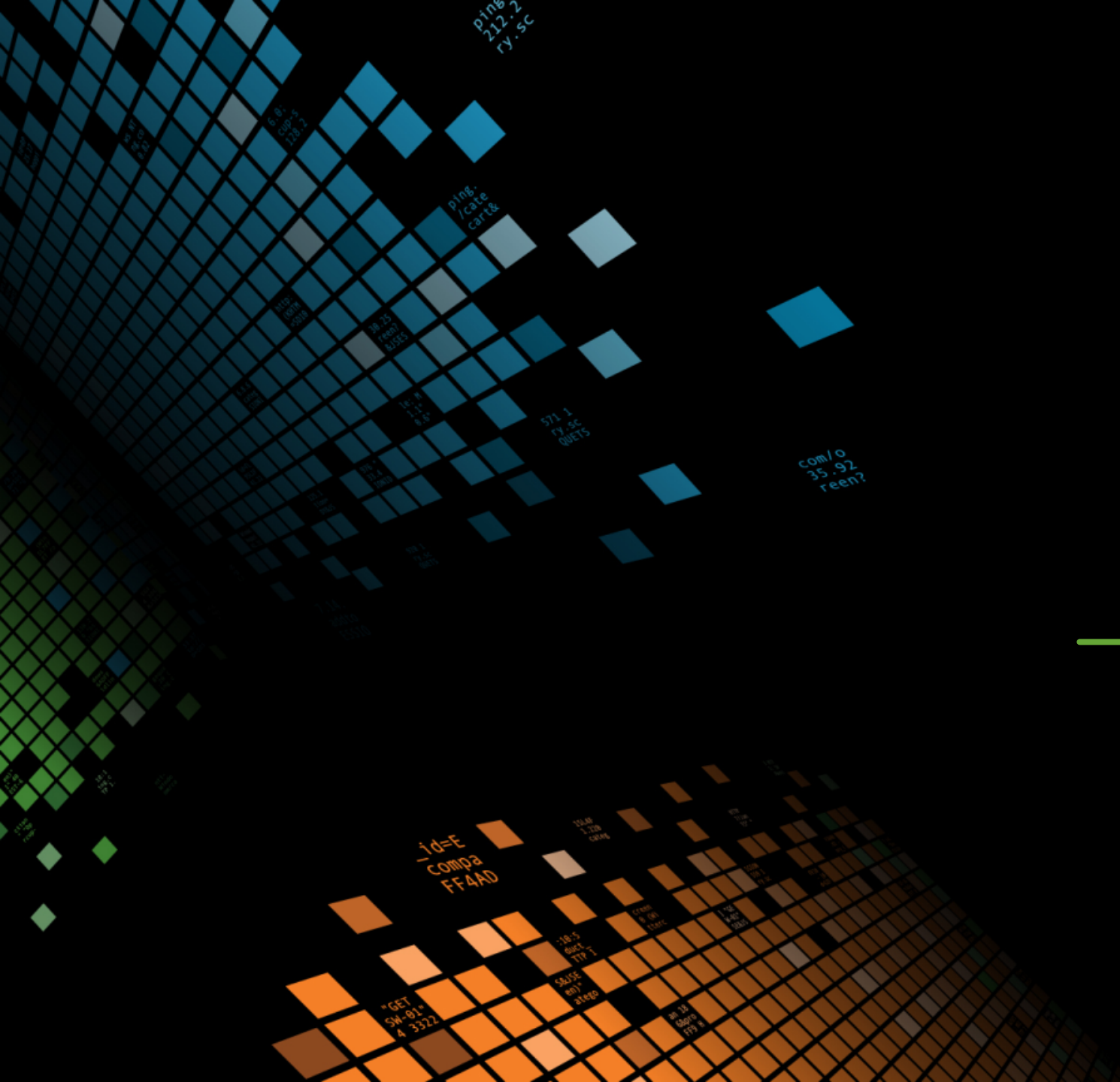
Agenda

Agenda

subtitle

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

splunk> .conf2017



Introductions

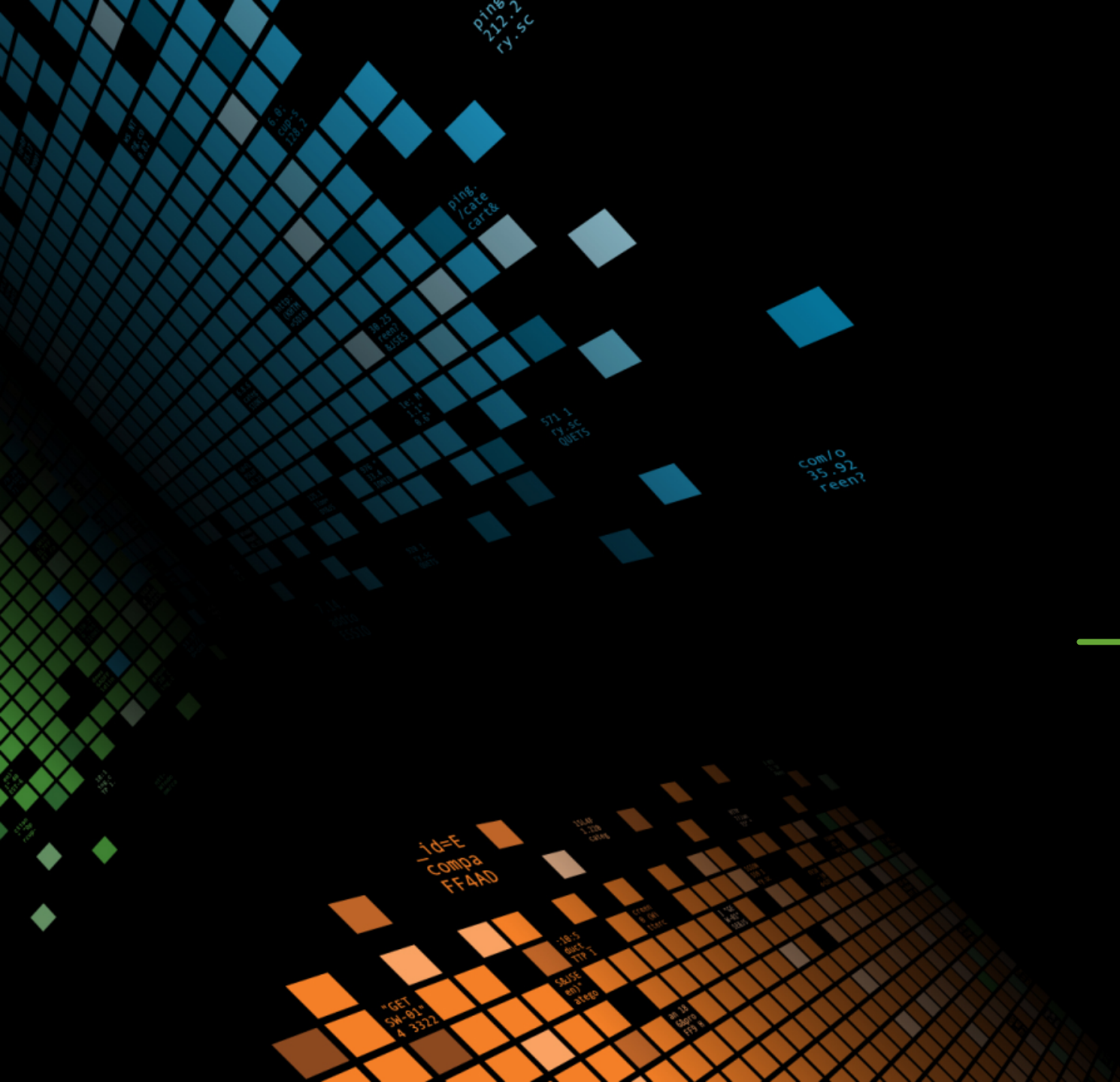
Section subtitle goes here

splunk> .conf2017

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

splunk> .conf2017

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)

CBD NOW

Who Are We? | Smart Banking | Special Offers | Accounts & Cards | Join NOW

Banking designed around you

Smart, simple, always with you.

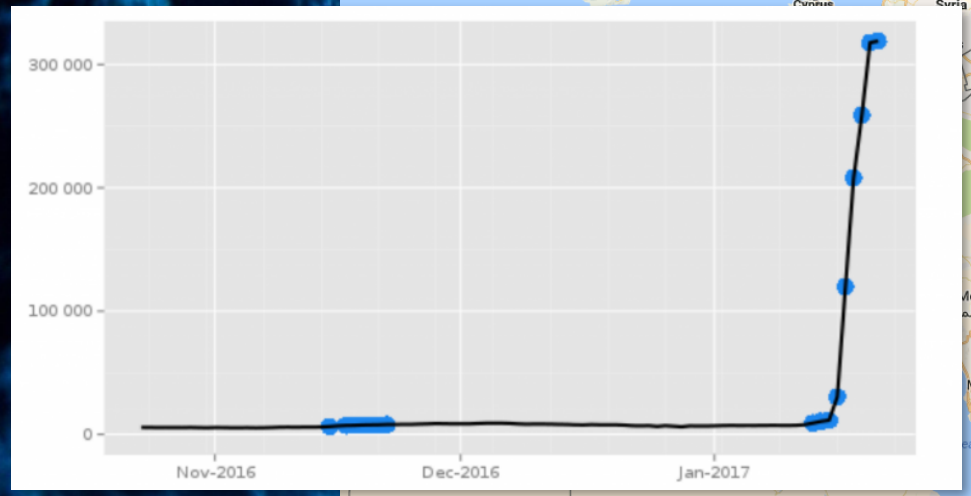
- No minimum balance required
- Real-time smart notifications
- 100% mobile
- Instant and easy to use
- Debit card hand-delivered in 24 hours
- 100s of FREE amazing discounts

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

splunk> .conf2017

Platform Objectives

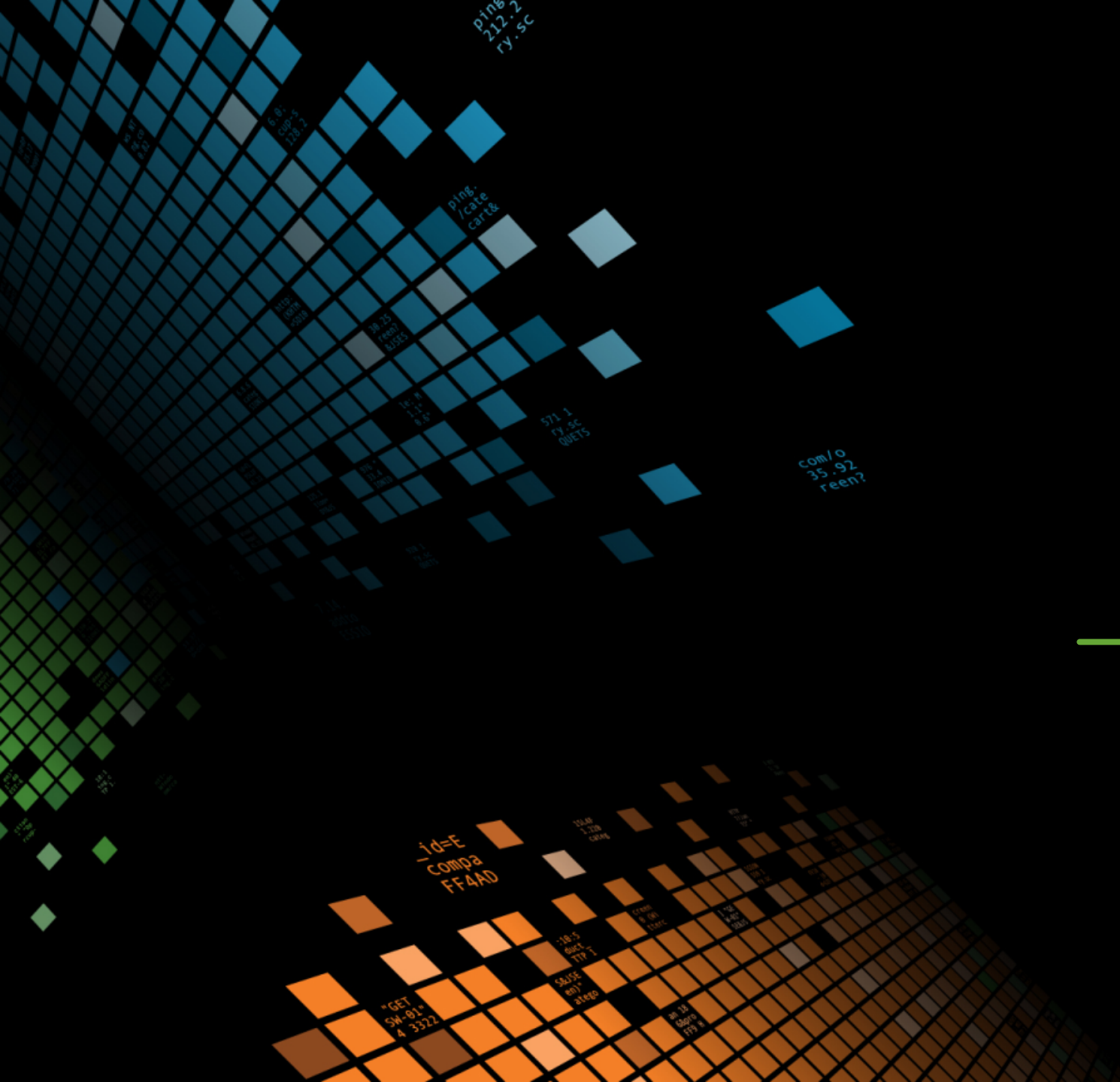
Behavioural Analytics

Near Real Time Proactive Detection & Prevention

Entity & Group Profiling

Holistic Cross Channel View

Anomaly Detection



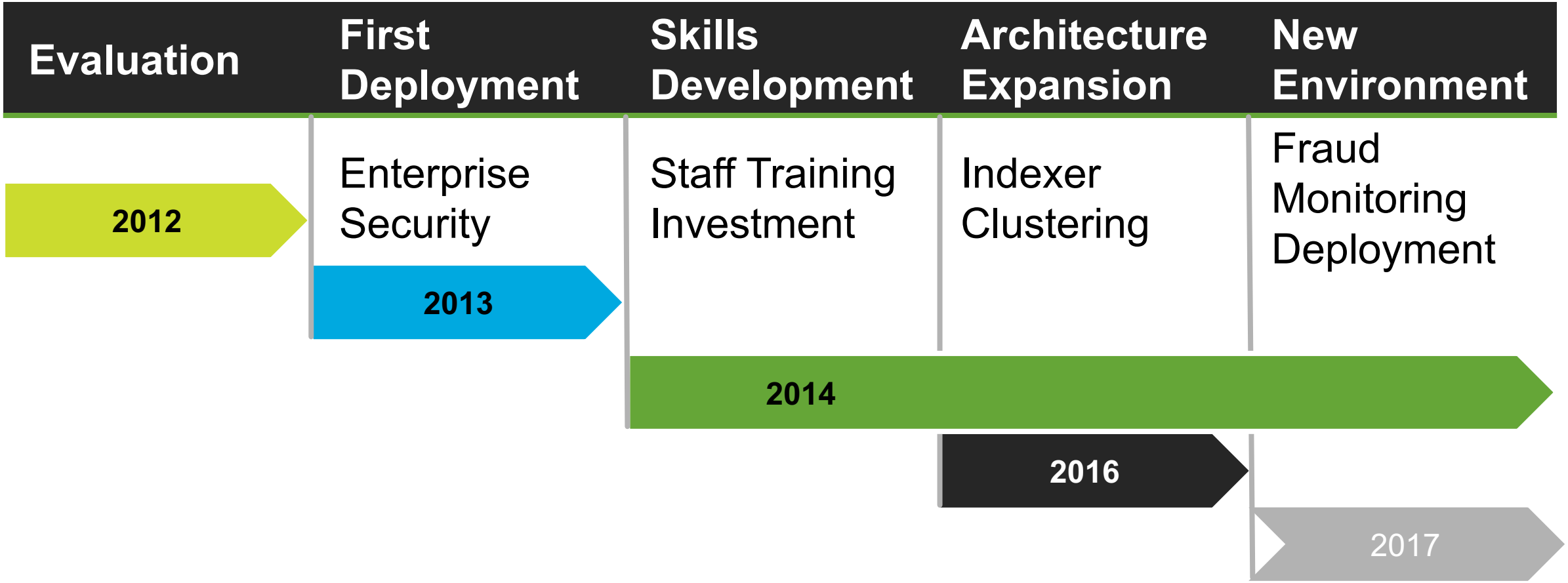
Splunk & CBD

Section subtitle goes here

splunk> .conf2017

Splunk & CBD

Journey Timeline



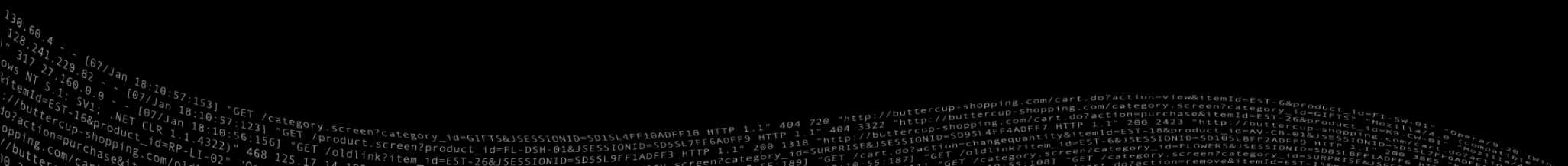
Splunking Fraud At CBD

Section subtitle goes here

splunk> .conf2017

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



splunk> .conf2017

Banking Channels

Credit Cards

Debit Cards

Digital

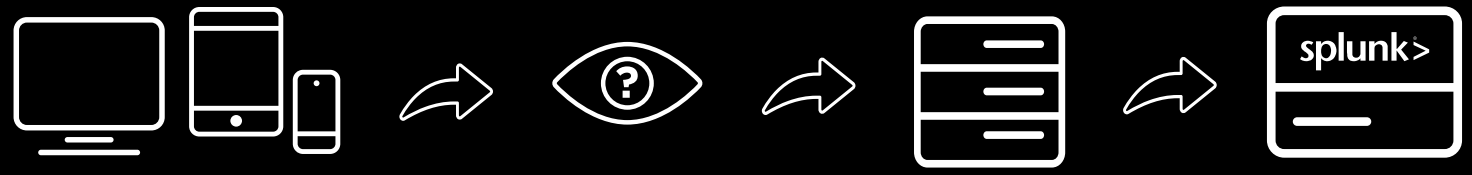
Telephone & SMS

SWIFT

splunk>

splunk> .conf2017

Risk Platform Integration



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

- Data Enrichment

Data Sources

Card Transactions

Enrichment

ATM GPS Coordinates
Merchant Details
Customer
Demographics

Debit Cards

Internal Platform
DBX Connections

Credit Cards

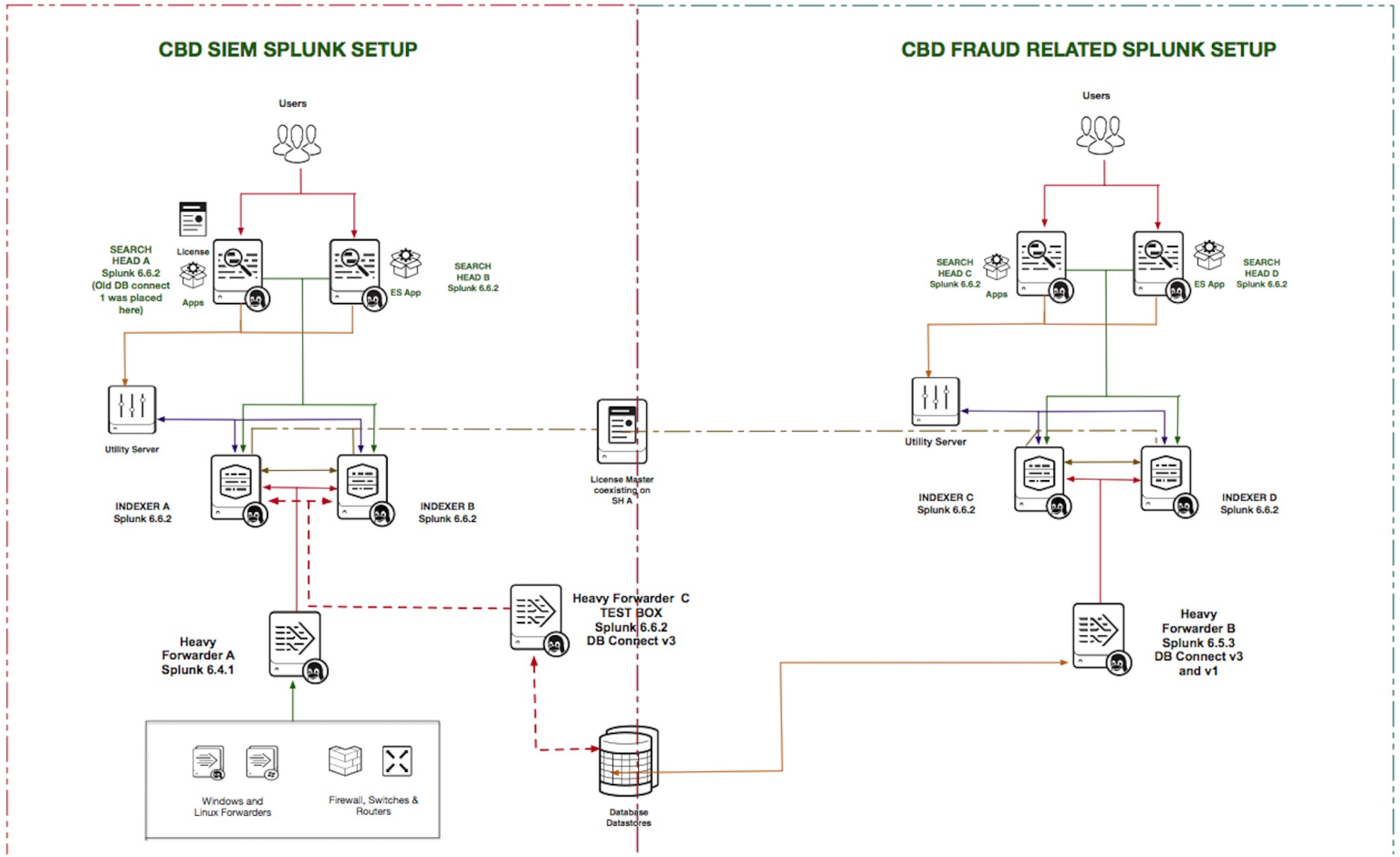
3rd Party Platform
Provider
MSMQ -> DBX

Splunk Architecture

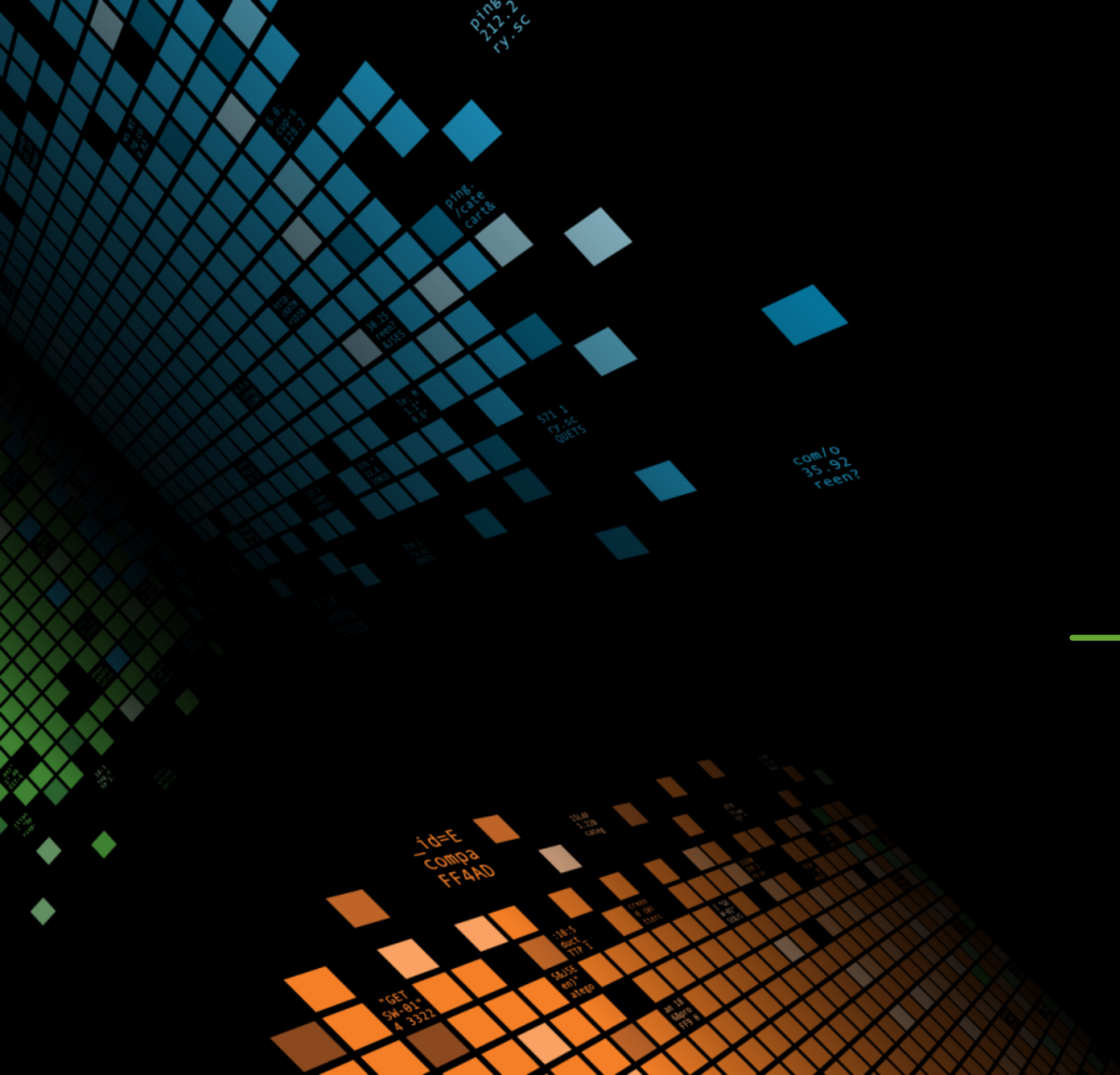
splunk> .conf2017

High Level Architecture

Splunk Infrasturcture



splunk> .conf2017



Data Models

Data Models For Fraud Detection

splunk> .conf2017

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

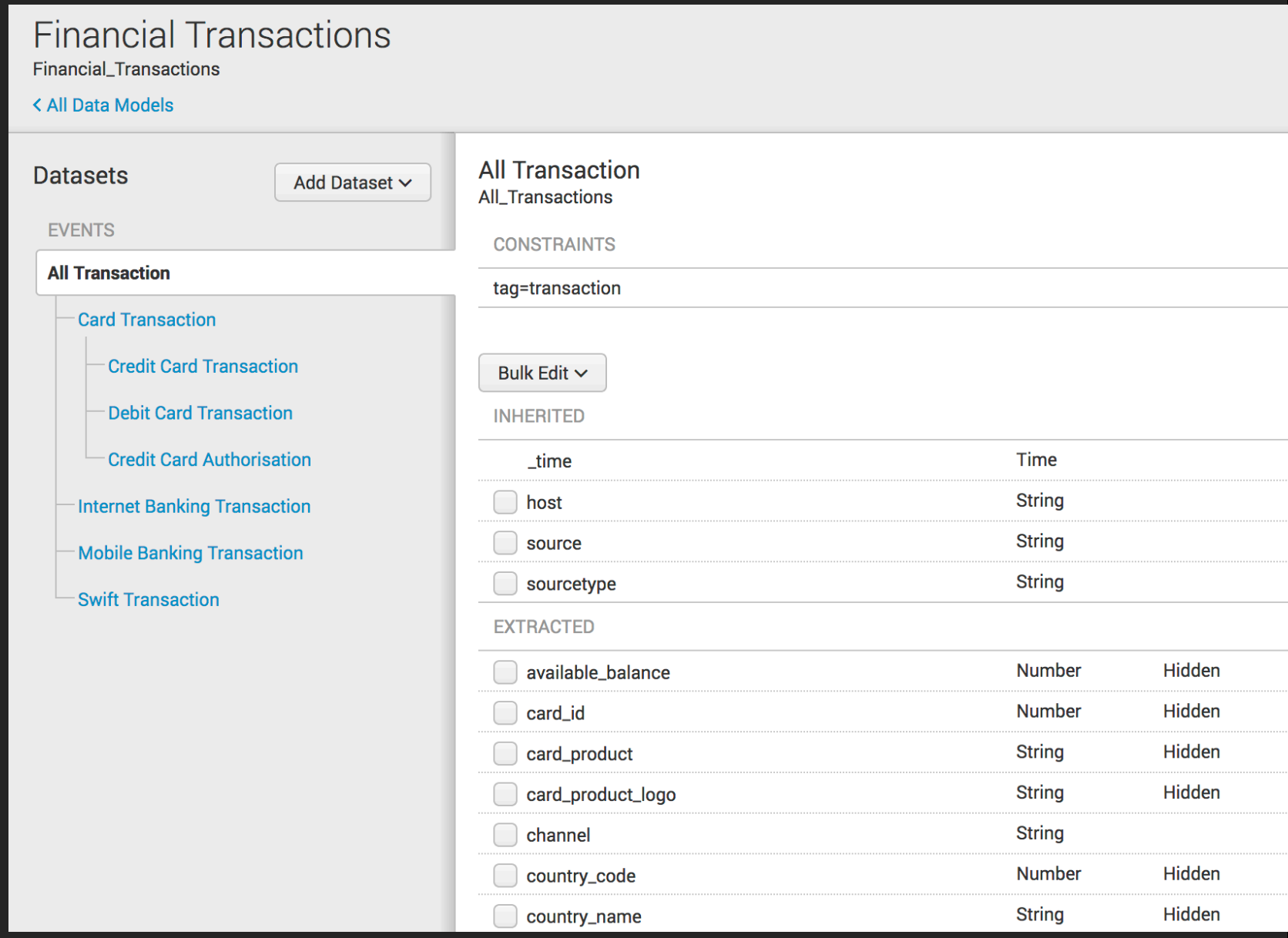
Data Models

Custom Retail Banking Models

Data Model	Channels
Financial Transactions	Credit Cards Debit Cards Authorizations SWIFT Payments
<Risk Platform>	Internet Banking Mobile Banking
Customer Activity	Internet Banking Mobile Banking Telephone Banking
SMS	Outbound Communication

Custom Data Models

Specific To Retail Banking Fraud



splunk> .conf2017

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 SPLITCOL channel SPLITCOL 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
```

rim_no	_time	credit_card ::: approved	credit_card ::: declined	debit_card ::: approved	debit_card ::: declined	internet_banking ::: approved	mobile_banking ::: approved	swift ::: approved	swift ::: declined	total_approved	total_declined
d0aaf39f31aed7d7bec1137e15d335b6	2017-09-19 09:00	0	3	0	0	8	0	0	0	8	3
7e34103d20ea96e0304389a74c44b50d	2017-09-14 06:00	0	5	0	0	5	0	0	0	5	5
33f68b5283ce15ed81bb906444473742	2017-09-16 02:00	0	3	0	0	0	3	0	0	3	3
456388d7767a9aaa38a8e5e8792f9cca	2017-09-16 12:00	1	6	0	0	0	6	0	0	7	6
2cae033644ec69257036df2ab6663350	2017-09-17 20:00	1	3	0	0	0	3	0	0	4	3
f698a9fa48ef482cc78042eb0626f86b	2017-09-18 16:00	0	3	0	0	4	0	0	0	4	3
4f72b078285a1746963be396111691e3	2017-09-15 19:00	3	3	0	0	0	1	0	0	4	3
2e4bd93ee1d7b2f36d66d1d78bff65f3	2017-09-13 17:00	0	4	0	0	0	4	0	0	4	4

splunk> .conf2017

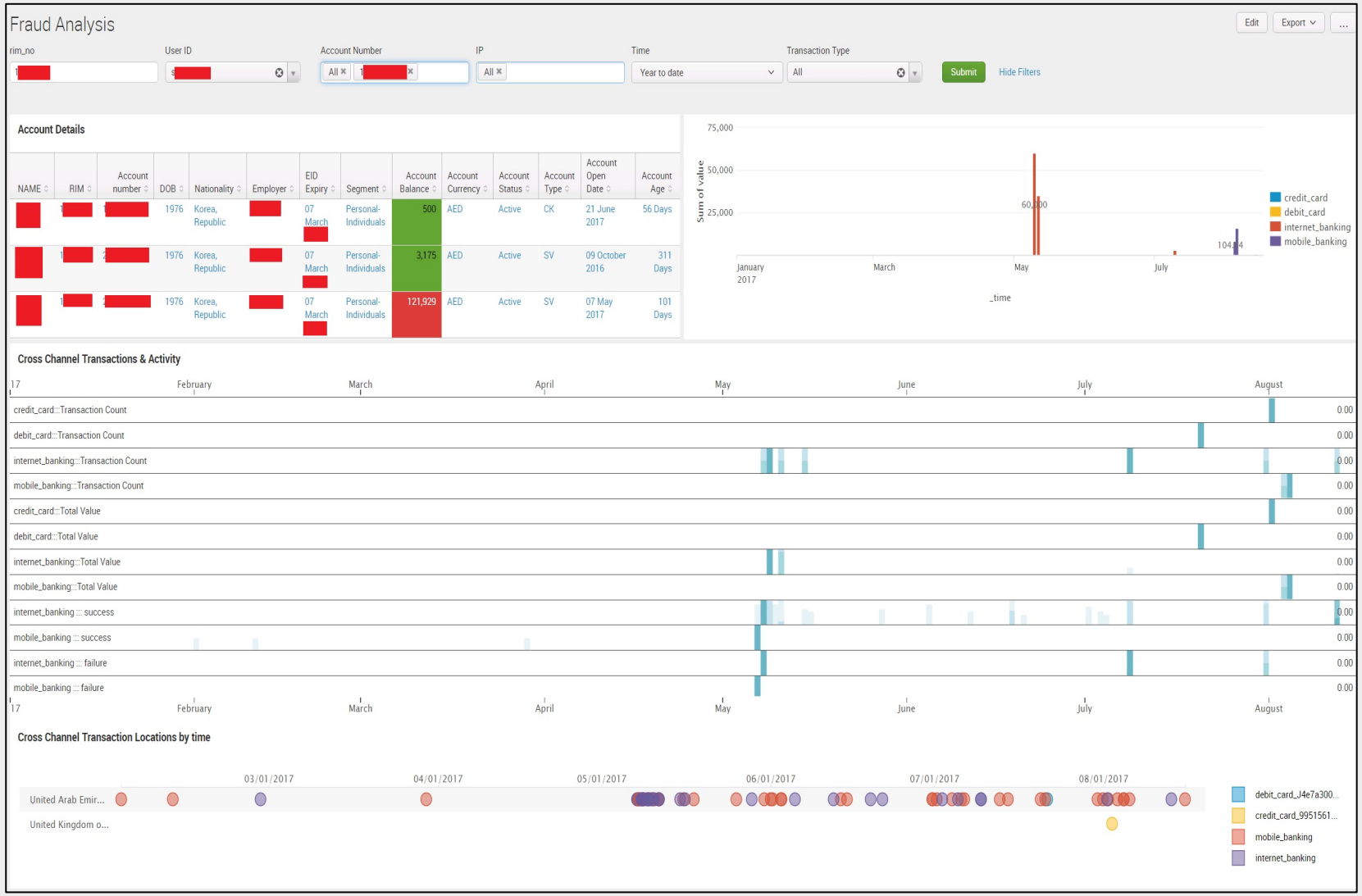
Investigation Dashboards for Analysts

Data Models For Fraud Detection

splunk> .conf2017

Cross Channel Analysis

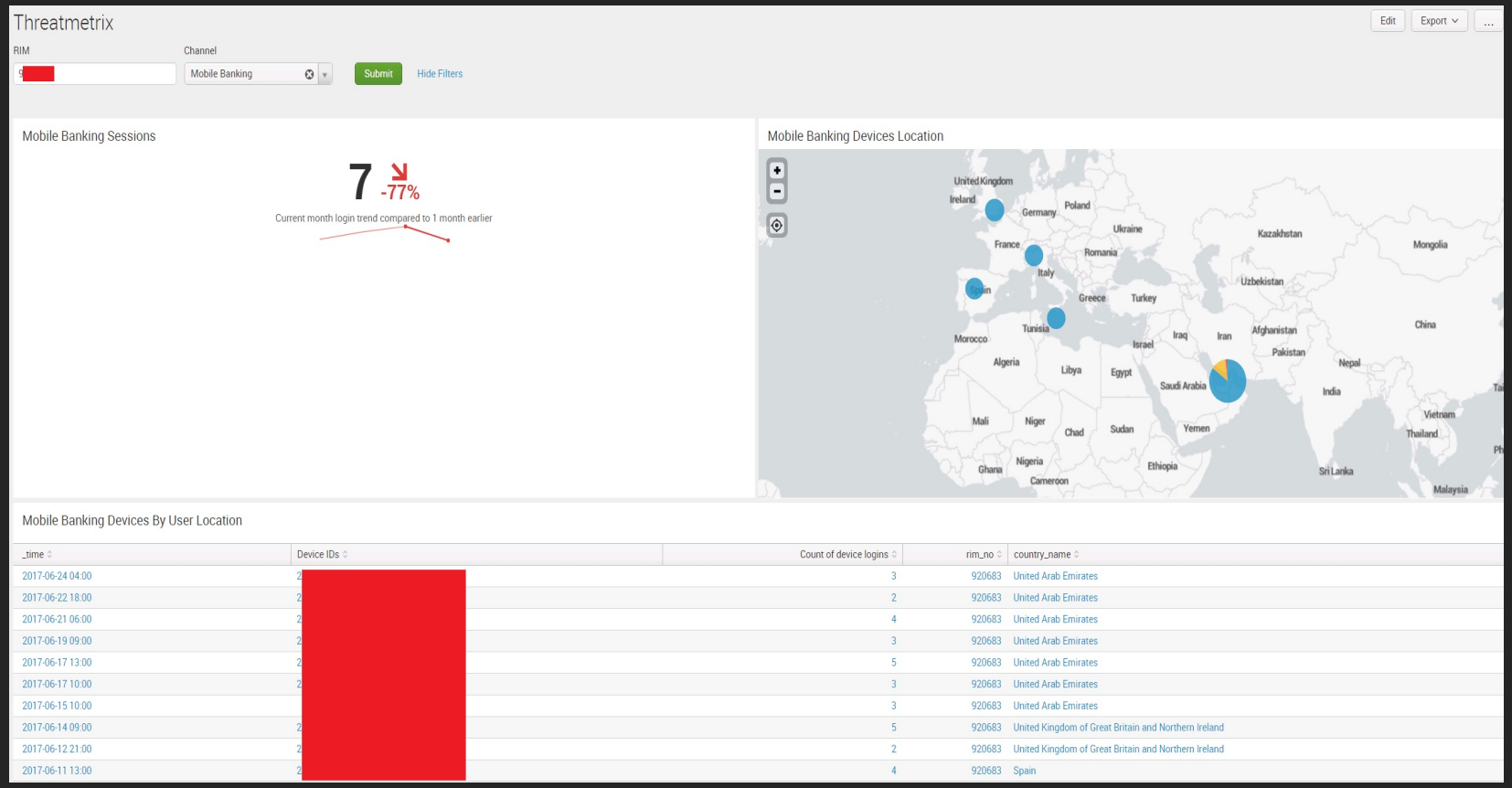
Analyst Investigation Dashboard



splunk> listen to your data®

Mobile Banking Activity

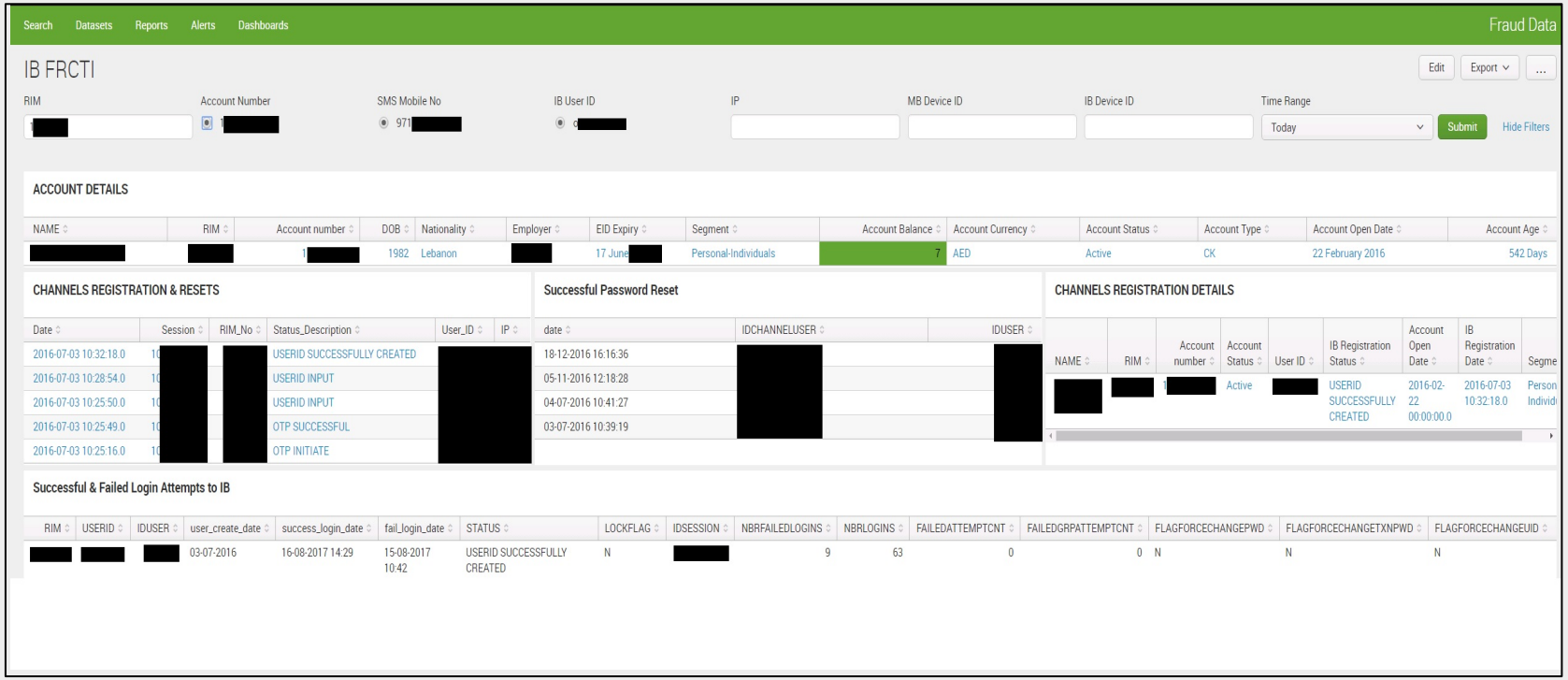
Mobile Device & Session Investigation



splunk> .conf2017

Internet Banking Authentication

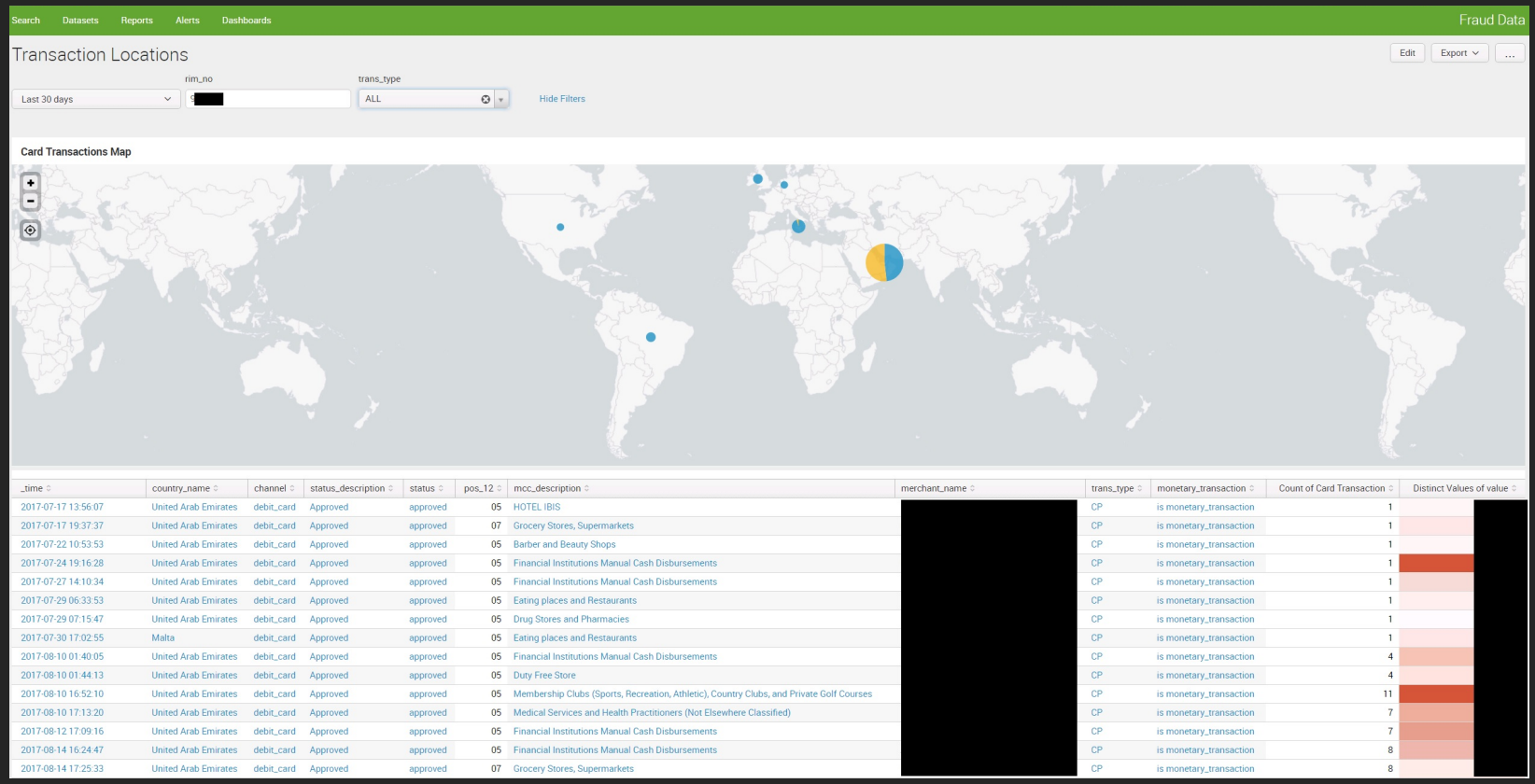
Analyst Investigation of Authentication & Registration



splunk> listen to your data®

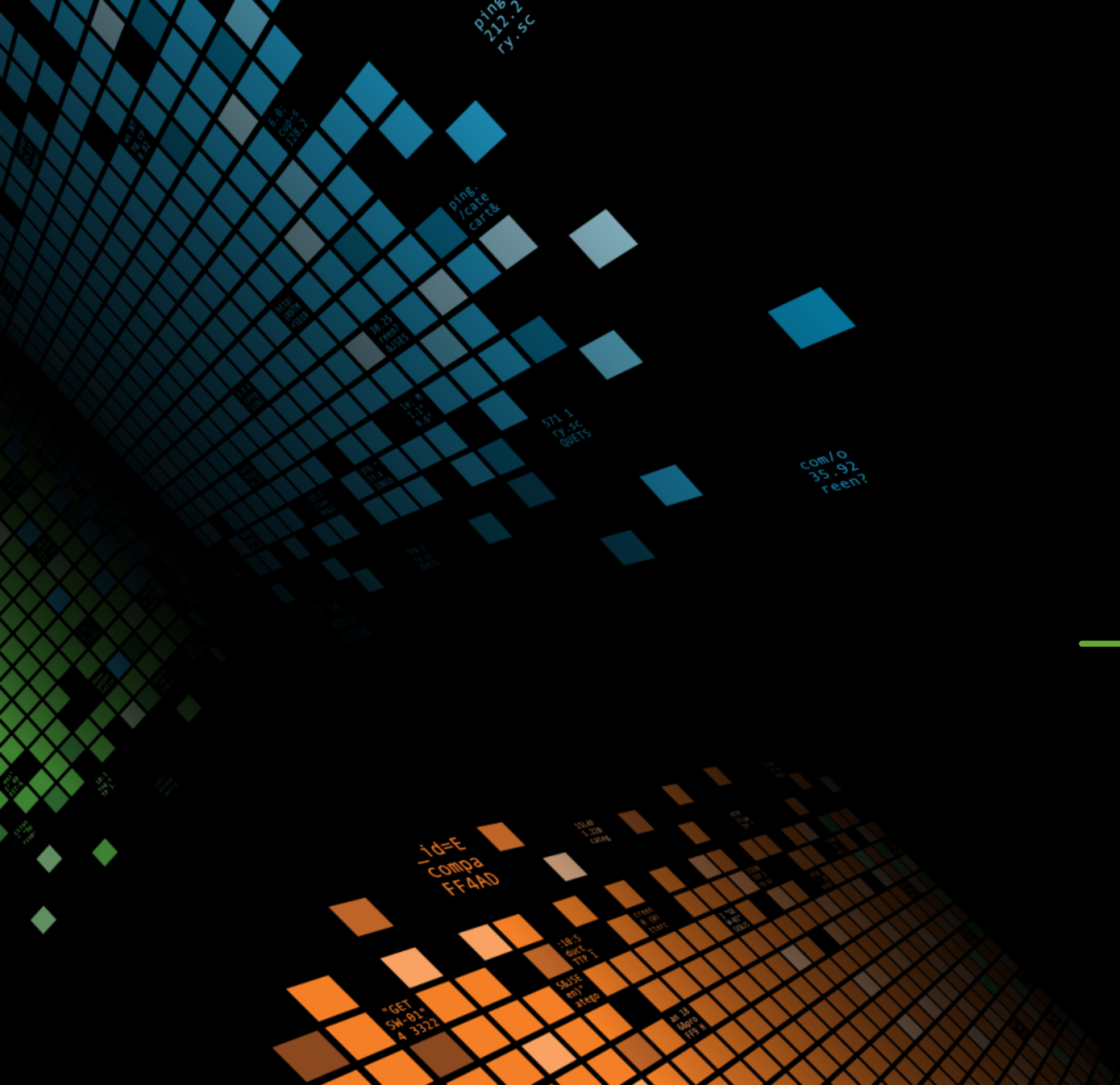
Card Transaction Geography

Card Transaction Location Analysis



_time	country_name	channel	status_description	status	pos_12	mcc_description	merchant_name	trans_type	monetary_transaction	Count of Card Transaction	Distinct Values of value
2017-07-17 13:56:07	United Arab Emirates	debit_card	Approved	approved	05	HOTEL IBIS	[redacted]	CP	is monetary_transaction	1	[redacted]
2017-07-17 19:37:37	United Arab Emirates	debit_card	Approved	approved	07	Grocery Stores, Supermarkets		CP	is monetary_transaction	1	
2017-07-22 10:53:53	United Arab Emirates	debit_card	Approved	approved	05	Barber and Beauty Shops		CP	is monetary_transaction	1	
2017-07-24 19:16:28	United Arab Emirates	debit_card	Approved	approved	05	Financial Institutions Manual Cash Disbursements		CP	is monetary_transaction	1	
2017-07-27 14:10:34	United Arab Emirates	debit_card	Approved	approved	05	Financial Institutions Manual Cash Disbursements		CP	is monetary_transaction	1	
2017-07-29 06:33:53	United Arab Emirates	debit_card	Approved	approved	05	Eating places and Restaurants		CP	is monetary_transaction	1	
2017-07-29 07:15:47	United Arab Emirates	debit_card	Approved	approved	05	Drug Stores and Pharmacies		CP	is monetary_transaction	1	
2017-07-30 17:02:55	Malta	debit_card	Approved	approved	05	Eating places and Restaurants		CP	is monetary_transaction	1	
2017-08-10 01:40:05	United Arab Emirates	debit_card	Approved	approved	05	Financial Institutions Manual Cash Disbursements		CP	is monetary_transaction	4	
2017-08-10 01:44:13	United Arab Emirates	debit_card	Approved	approved	05	Duty Free Store		CP	is monetary_transaction	4	
2017-08-10 16:52:10	United Arab Emirates	debit_card	Approved	approved	05	Membership Clubs (Sports, Recreation, Athletic), Country Clubs, and Private Golf Courses		CP	is monetary_transaction	11	
2017-08-10 17:13:20	United Arab Emirates	debit_card	Approved	approved	05	Medical Services and Health Practitioners (Not Elsewhere Classified)		CP	is monetary_transaction	7	
2017-08-12 17:09:16	United Arab Emirates	debit_card	Approved	approved	05	Financial Institutions Manual Cash Disbursements		CP	is monetary_transaction	7	
2017-08-14 16:24:47	United Arab Emirates	debit_card	Approved	approved	05	Financial Institutions Manual Cash Disbursements		CP	is monetary_transaction	8	
2017-08-14 17:25:33	United Arab Emirates	debit_card	Approved	approved	07	Grocery Stores, Supermarkets		CP	is monetary_transaction	8	

splunk> .conf2017



Fraud Alerting

splunk> .conf2017

Alert: International Transaction Declines

BIN_ATTACK_INTL_ATTEMPTS

```
sourcetype=cc:auth DeclineReason=1
| lookup decline_reason.csv DeclineReason OUTPUTNEW decline_reason_desc
| lookup cardmaster.csv CardId OUTPUTNEW CustNo Embname1 MaskdAccNo RIM
| rename MC_POS_CNTRY_CODE AS country-code, RIM as rim_no
| lookup country.csv country-code OUTPUTNEW country_name | search country_name!="United Arab Emirates"
| lookup sms_nos.csv rim_no OUTPUTNEW mob_no
| lookup mcc.csv mcc OUTPUTNEW mcc_description
| eval date=strftime(_time,"%d %B %Y")
| stats values(date) as Date, dc(country_name) as Country_Count, c(DeclineReason) as NumberOfAttempts, values(country_name) as Country, values(rim_no) as RIM_NO, values(CardId) as Card_ID, values(CustNo) as Cust_Number, values(MaskdAccNo) as Card_Number, values(Embname1) as Embossing_Name, values(mob_no) as Mobile_No, values
    (decline_reason_desc) as Auth_Reason, values(DeclineReason) as Response_Code, values(MC_POS_CNTRY_CODE) as Trans_Currency, values(TransAmt) as Trans_Amount, values(MCC) as Merchant_Category, values(mcc_description) as MCC_Desc, values(CRD_ACCPT_TERM_ID) as Terminal_ID, values(CRD_ACCPT_ID) as MID, values(POSENTRY) as
    Entry_Mode by MerchName1 | rename MerchName1 AS Merchant_Name
| search NumberOfAttempts>8
```

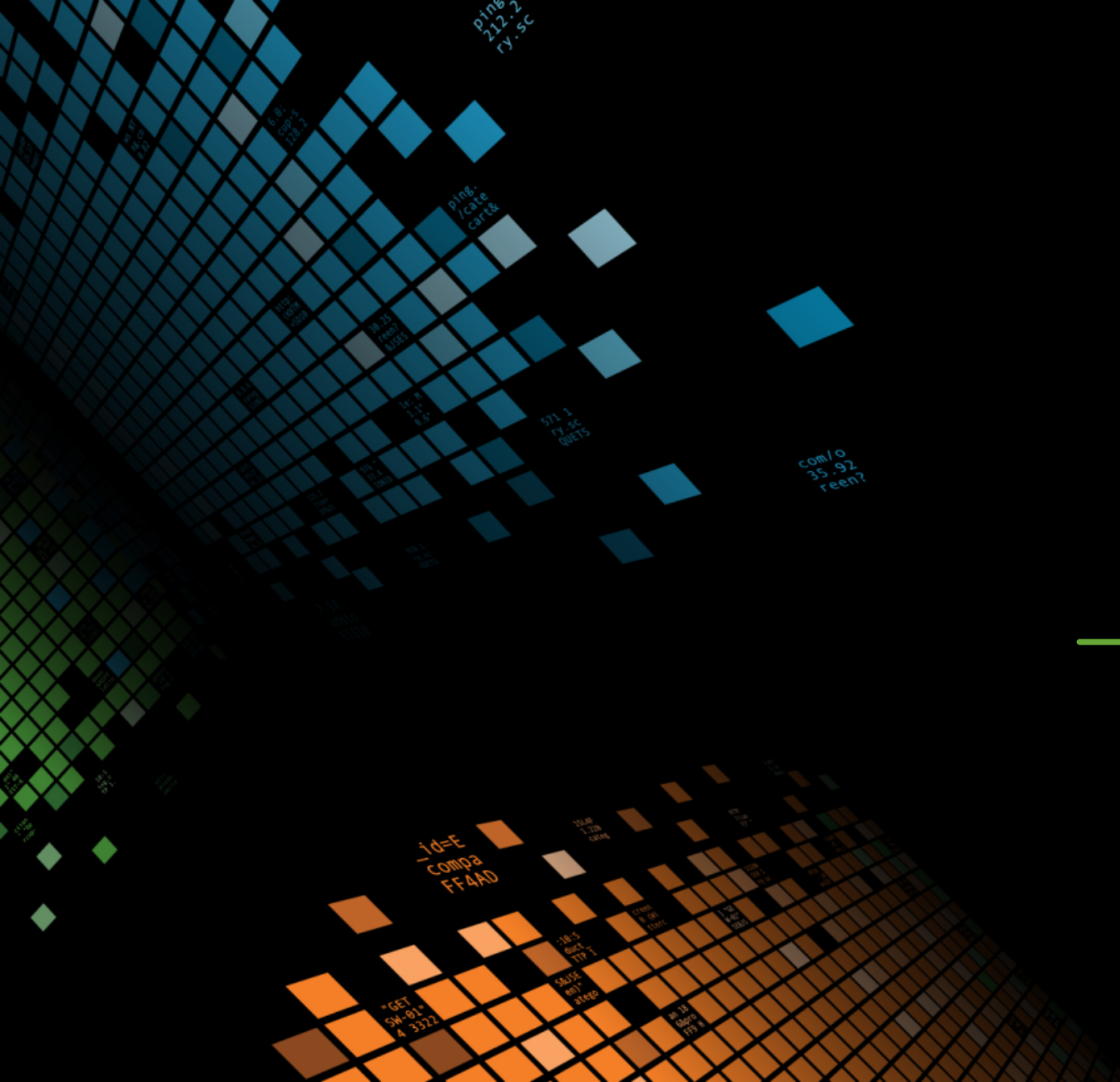
✓ 152 events (7/17/17 5:04:58.000 PM to 8/16/17 5:04:58.000 PM) No Event Sampling

Events (152) Patterns Statistics (3) Visualization

20 Per Page ✓ Format Preview

Merchant_Name	Date	Country_Count	NumberOfAttempts	Country	RIM_NO	Card_ID	Cust_Number	Card_Number	Embossing_Name	Mobile_No	Auth_Reason	Response_Code	Trans_Currency	Trans_Amount	Merchant_Category	MCC_Desc
[redacted]	06 August 2017 08 August 2017 11 August 2017 12 August 2017 19 July 2017 22 July 2017 23 July 2017 25 July 2017 27 July 2017 29 July 2017	2	24	United Kingdom of Great Britain and Northern Ireland United States of America	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		Invalid Account	1		0.82 0.86 2.87 2.89 3.23 3.64 3.67 3.79 4.00 4.17 4.25 4.38 4.51	5734 7399 7829	Business Services, Not Elsewhere Classified Computer Software Stores Motion Pictures and Video Tape Production and Distribution

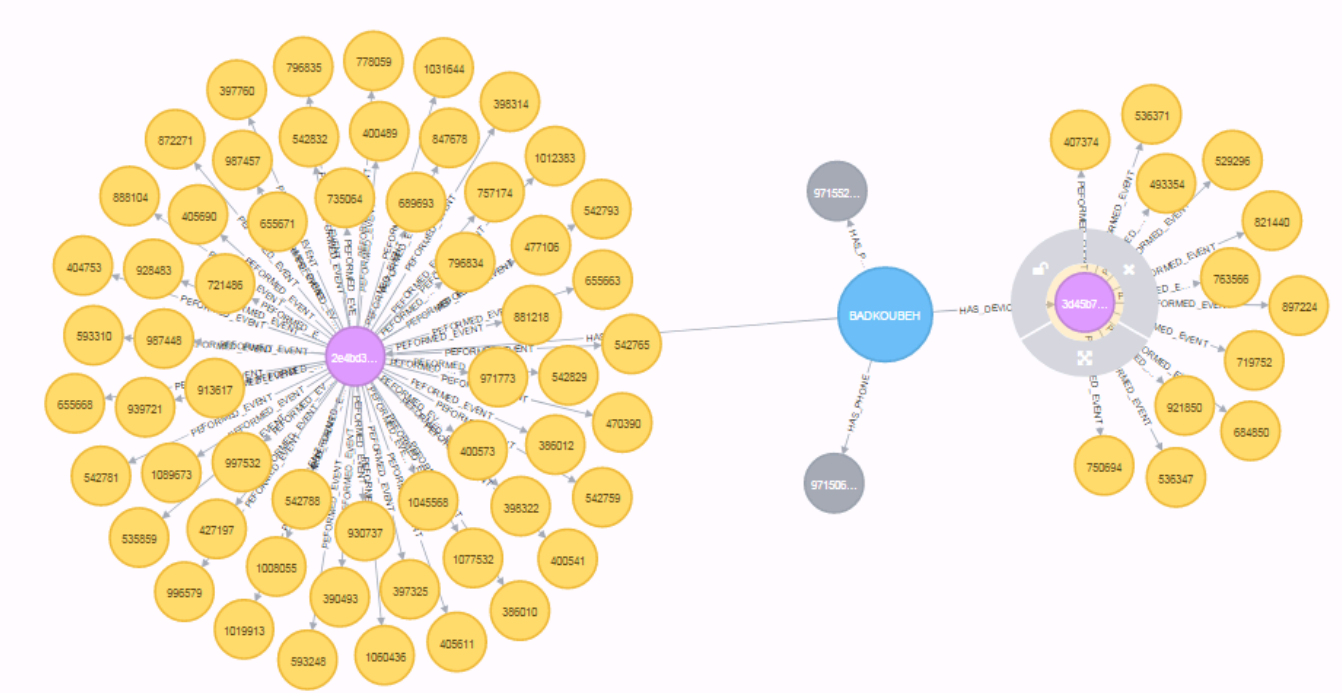
splunk> listen to your data®



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?

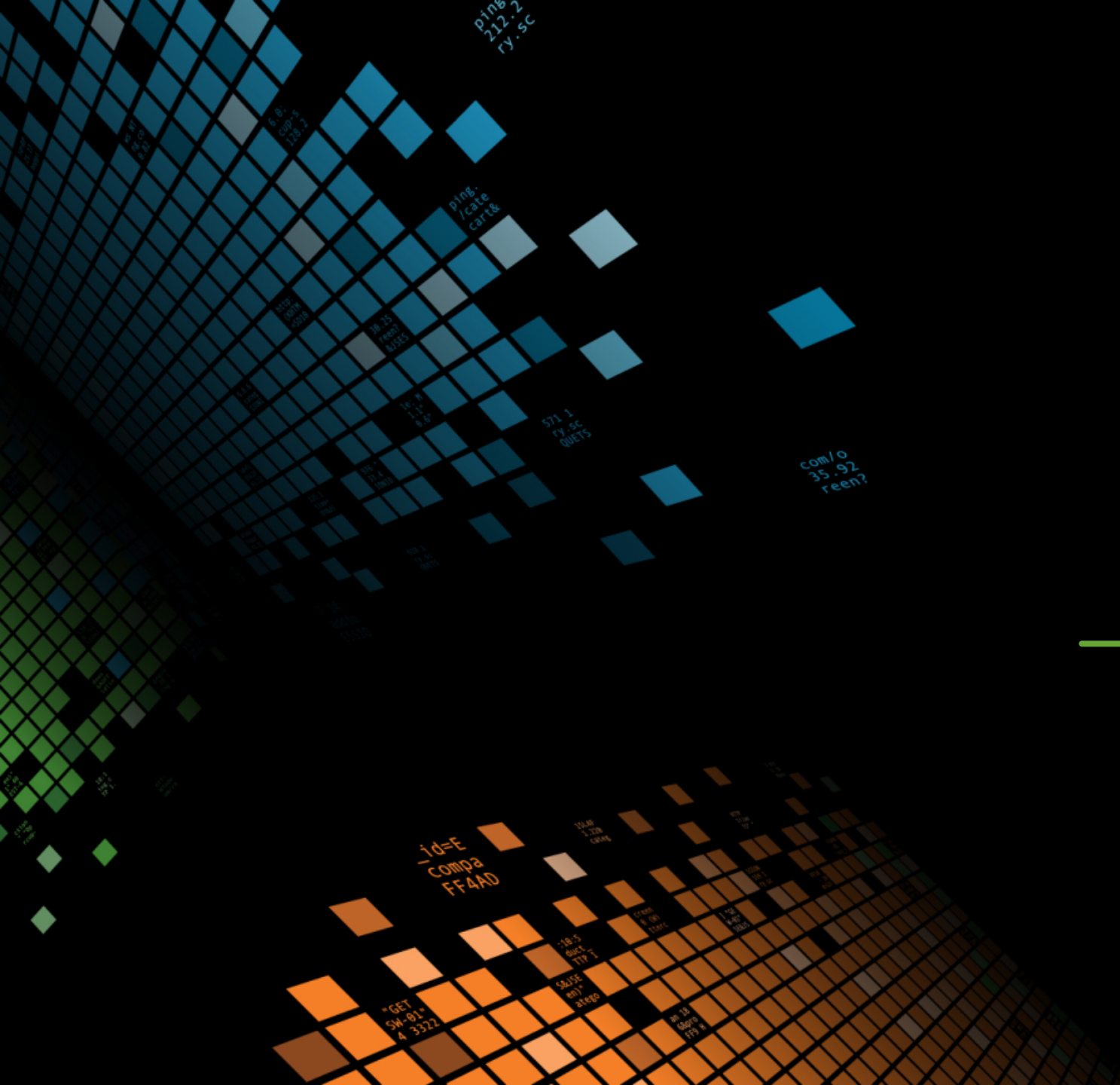
Key Takeaways

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



Q&A

Participant name | Role

Participant name | Role

splunk> .conf2017