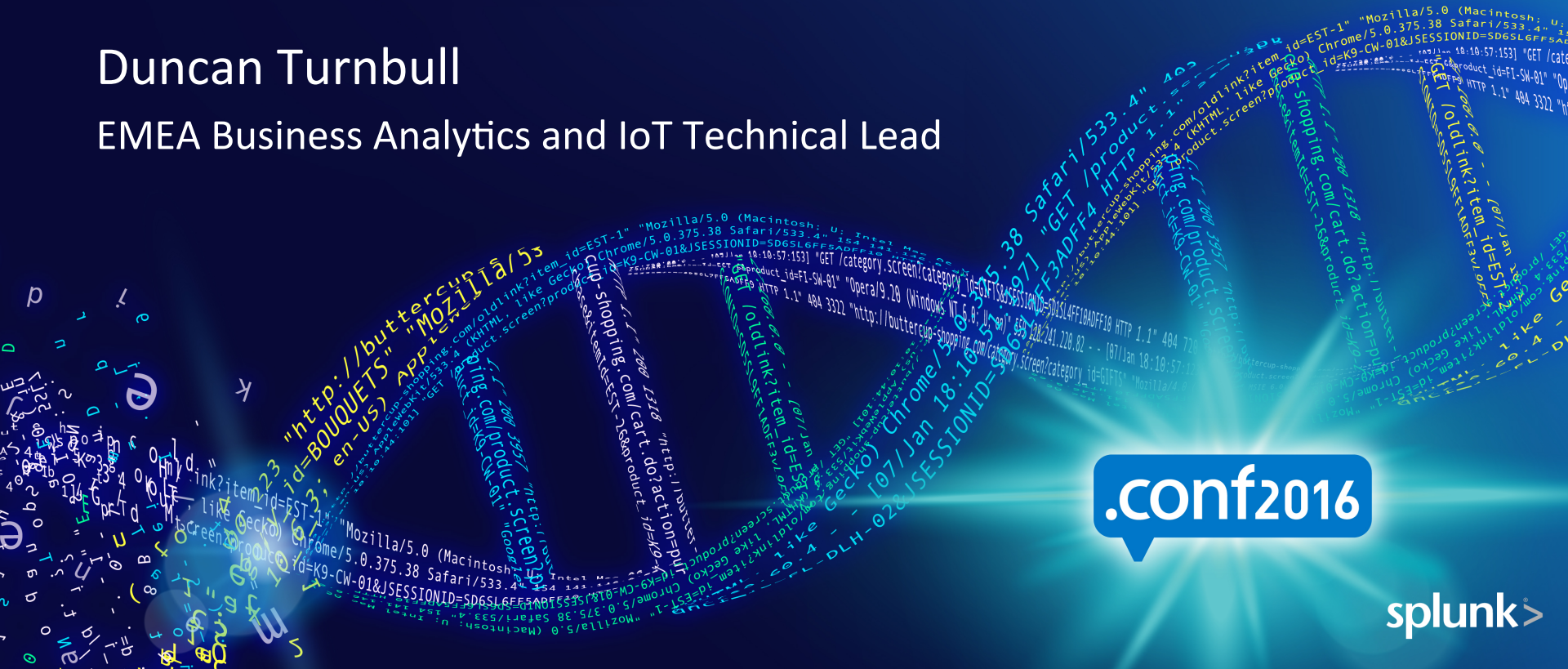
Tracking Trading With Splunk

Duncan Turnbull

EMEA Business Analytics and IoT Technical Lead



FIX

What Is FIX?

- Financial Information eXchange protocol
- Standard for communication between financial software
- Comes in two varieties:
  - FIX (^A seperated fields)
  - FIXML (XML formatted)

Why Do This?

- **Operations : Reduce Time To Investigate**
  - Tracking down all the steps of a trade is difficult
  - Doubly so when you have many identifiers
  - Even harder when it looks like 35=D
  - Automatically detect anomalies at scale to see problems
- **Analytics : Better understand customers**
  - How often do they trade?
  - Is their volume with us increasing or decreasing?
  - What's new and interesting for this customer?
  - Automatically detect anomalies at scale to see customer behavior

How Do We Get It?

- For FIXML, bring in the XML data and use spath or KV_MODE=xml or INDEXED_EXTRACTIONS=xml
- Often logged in application logs or files
- Otherwise usually from a message bus (use JMS Messaging Modular Input)
- For FIX, decode using the Financial Information eXchange (FIX) Log Parsing App from Splunkbase

What Else Can We Use?

- Interactive Trading Applications
  - Often have a FIX component
  - Contain other useful information, such as user interactions
- Pricing Engines
- Market Data
  - Metrics
  - Logging
- Messaging

- Accounting / Settlement

Decoding FIX Messages

- The Financial Information eXchange (FIX) Log Parsing App provides a translatefix command
- Pipe into your search to translate your messages
- Translates both keys and some values
  - 35=D becomes MsgType=New Order – Single
- Optionally use summary indexing, or wire into the JMS modular input to decode all messages all the time

Searching FIX Messages

- Either search with the undecoded message
- Or search with decoded after the pipe
- Or both (e.g. for a price, then verify in the correct field)
- Or encode your search terms by running through translatefix backwards
  - When decoding watch out for special cases – a search for Logon wouldn't go backwards, but a search for MsgType=Logon would

Joining Trades Or Message Flows Together

- FIX often will have multiple identifiers depending on the types of messages
- Many messages have an expected response
  - E.g. a New Order could be followed by an Execution Report
- Different types of messages have different identifiers
  - A Quote would have a QuoteEntryID
  - A New Order would reference the QuoteEntryID as a QuoteID
  - An Execution Report and a New Order would have a Customer Order ID

Detecting Trade Anomalies

- Use Splunk's anomalydetction command
- Build state lookups (see lookup talk) of:
  - Expected messages and responses
  - Expected failure reasons and historic rates
- Compare now versus the past to find anomalies
- Build rules for specific behavior (e.g. failed Market Data)
- Issue alerts for volume spikes, pricing and latency anomalies

Monitor The Whole Trade Workflow

- Use ITSI KPIs to measure:
  - Volume
  - Error rate
  - Latency
  - Queue Depth
- Track expected flows between stages
  - Each trade has a lifecycle
  - Did it meet all steps?
  - Did it meet all timelines / SLAs?

Putting Together The Pieces

- For end users we need prebuilt workflows to empower self service
- Use dashboards to present overviews by:
  - Security / Currency Pair / Equity
  - Trader / Desk
  - Counterparty / Customer
- Allow drilldown to individual trades
  - Also allow finding trades by any identifier
- Summarize systems and steps
  - With ITSI glass tables
  - With the Timeline ModViz

Customer Success : UK Financial Institution

- Monitoring common FIX platforms for FX
- Many internal and external clients
- Tracking queue depth and performance
- Also detecting anomalies
  - Technical anomalies : failures to subscribe
  - Rare/New currency pairs for customers : upsell and cross-sell opportunities

- And more use cases to come!

What Now?

Related breakout sessions and activities…

- **Superspeeding Transaction Monitoring with the kvtransaction Command**
- **Extending SPL with Custom Search Commands and the Splunk SDK for Python**
- **Monitor Your Business Transactions with Splunk to Gain Real-Time Insights Into Your Business Performance**
- **From DevOps to BizOps**
- **How to Use Splunk to Detect and Defeat Fraud, Theft and Abuse**

THANK YOU

splunk>