splunk> .conf2017

Catching Rogue Traders

How a multinational bank used Splunk to catch rogue traders in financial markets

Aleksey Eremenko | Vincent Leycuras

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

About Us

- **Aleksey Eremenko (Lex)**
  - Background for financial markets & data science
  - Markets Surveillance
  - Think of me as a secret agent

- **Vincent Leycuras**
  - Background in financial markets
  - Eager to fix the divide between Technologists and the rest of the world
  - Splunk convert since 2015

Why We Do What We Do

- **UBS Rogue Trader Scandal**
- In early September 2011, the Swiss bank UBS announced that it had **lost around 2.3 billion dollars**, as a result of unauthorized trading performed by a director of the bank's Global Synthetic Equities Trading team in London.

- **Societe Generale Rogue Trader**
- SocGen revealed that in January 2008 that a rogue trader had **lost the bank £3.7bn**. The trader, had been taking unauthorised positions on stock futures. The trader had previously worked in compliance, and bank bosses suggested he was adept at hiding his losses and bypassing checks.

- **Baring's Bank Goes Bust**
- Leeson did make Barings vast sums. In 1993, he made £10m - 10% of the bank's profits for that year. But in 1995, the discovery of a secret file - Error Account 88888 - showed that Leeson had gambled away **£827m in Barings's name** and the city's oldest merchant bank, and banker to the Queen, went bust.

splunk> .conf2017

“Why is it so hard to catch rogue traders?”

Rogue Trader Tactics & Behaviors

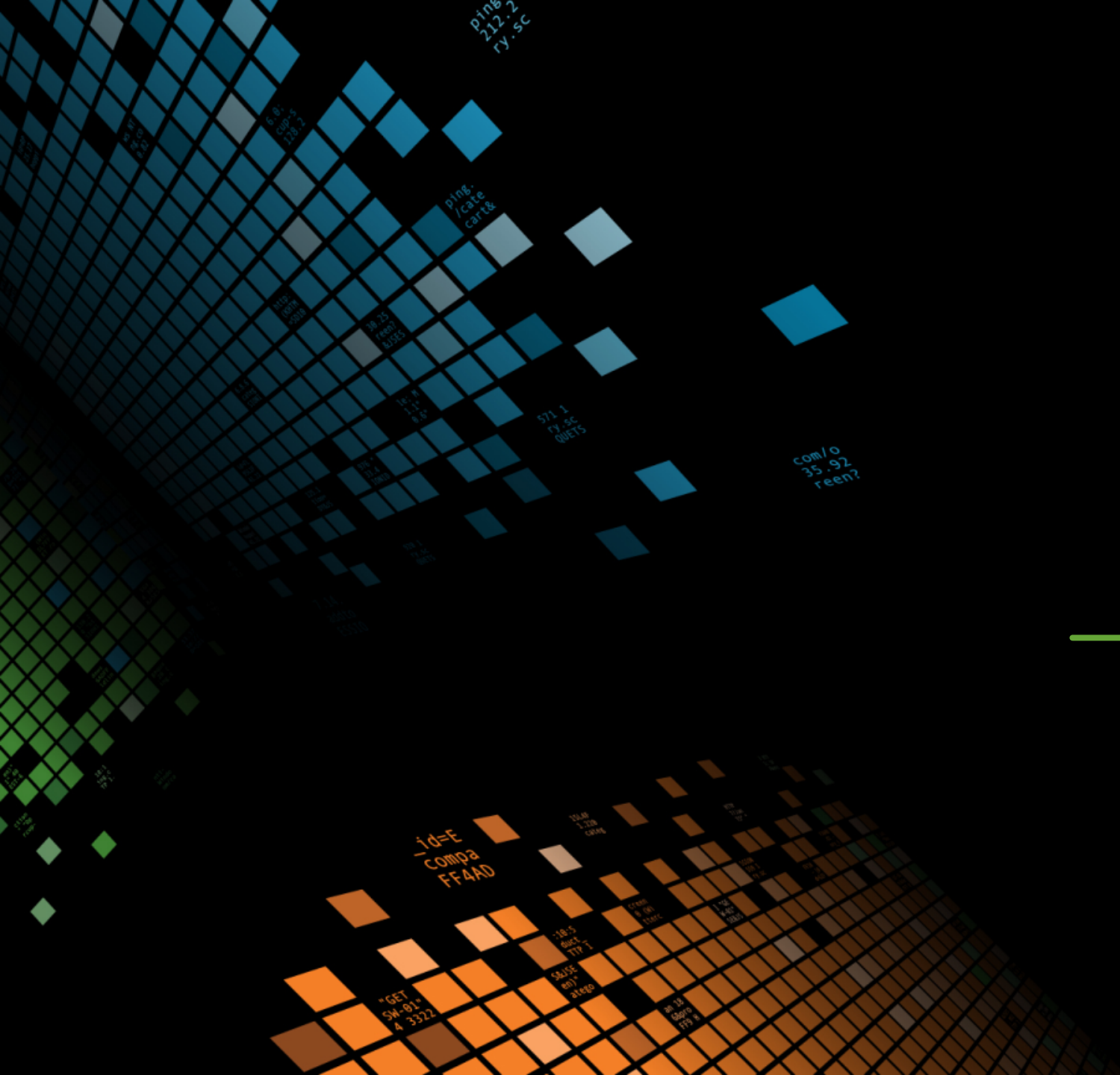
1. Get a job on a trading desk
2. Trade things your bosses don't understand
3. Trade away from the home office
4. Know the back office systems
5. Trade with other people's accounts
6. If you lose money, double down
7. Cross your fingers
8. Enlist your colleagues
9. Confess and point fingers

Need to correlate many non-traditional data sources across multiple systems

splunk> .conf2017

The Banking Technology Challenge

- Legacy banking infrastructure
- Systems were not designed to accept the granularity of data requirements of today
- Siloed systems & data sources

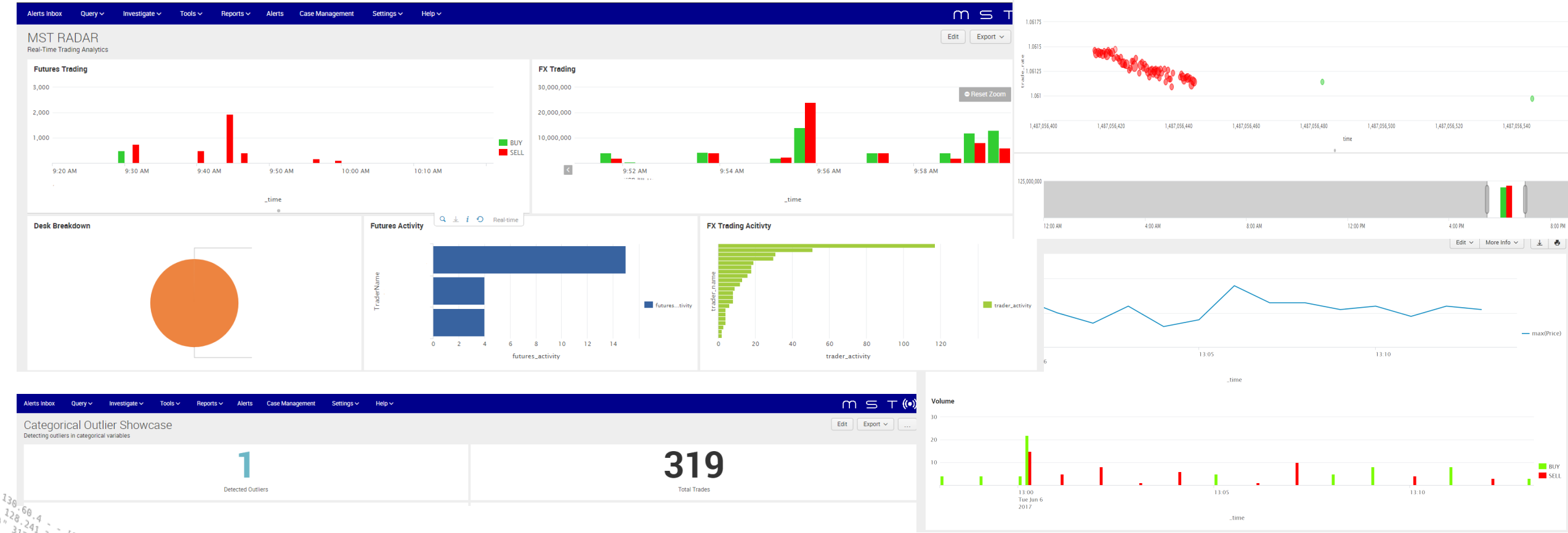


Enter Splunk!

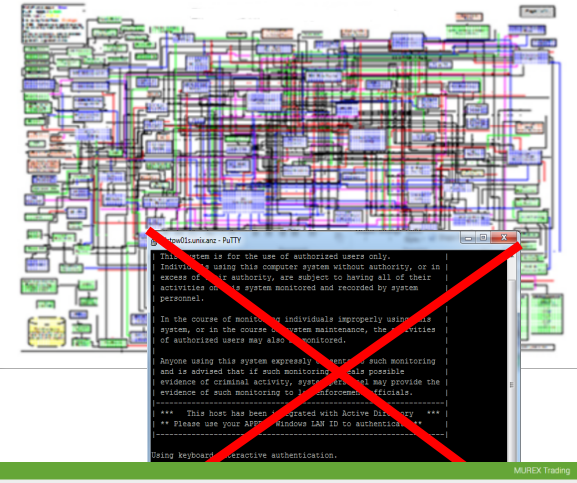
splunk> .conf2017

Our Splunk Story

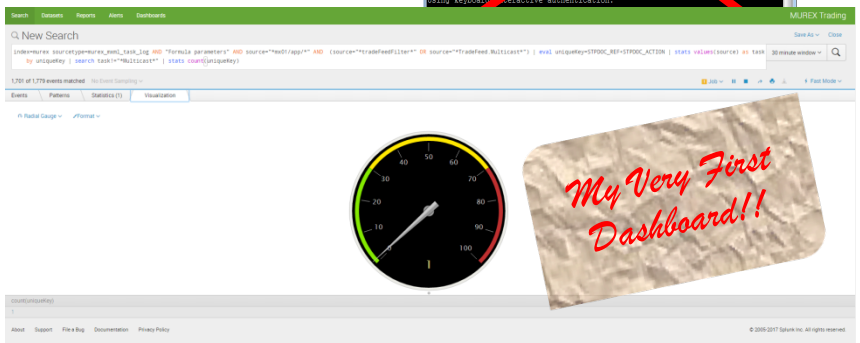
- Developed an app to conduct real-time financial markets monitoring, analytics, reporting & investigations.



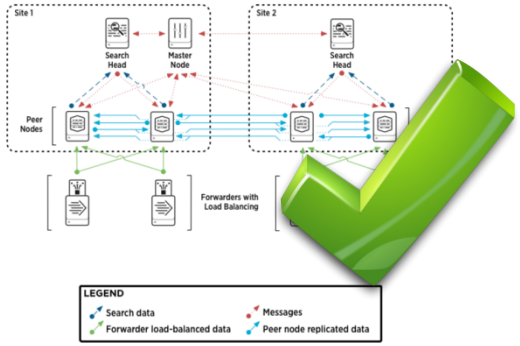
Where It All Started



- **Technology needed better systems monitoring capability – the brief was:**
- Ability to monitor flows across systems, not just the systems
- Reuse/recycle legacy tools/scripts/daemons, avoid throw away
- Remove the need for direct server access, especially for non-support staff



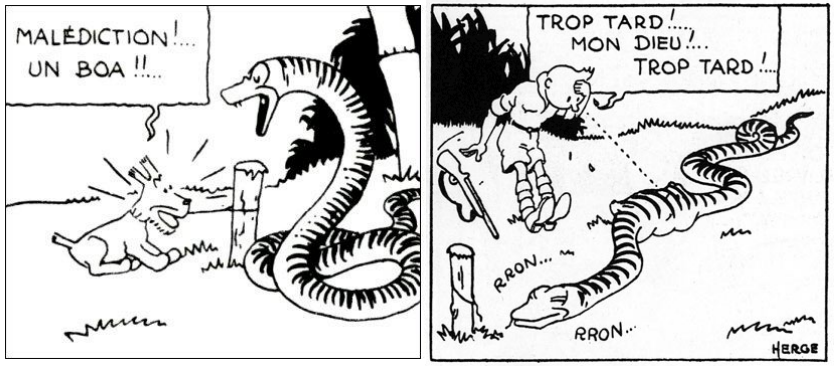
- **Discovered Splunk almost by accident:**
- A project team had sneaked it in for their own needs
- Just enough license headroom to add another system *(mine!!)*
- *V*ery little exposure, so plenty of opportunity to investigate *(i.e., muck around)*



- **Let the platform grow organically *(for a while…)***
- More systems were added with virtually 0 marginal cost
- Funding eventually came to build it properly
- All key systems are now on-boarded, the journey really begins NOW

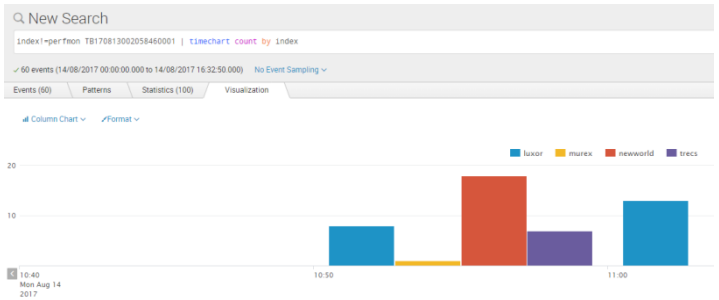
splunk> .conf2017

Climbing The Value-Add Ladder



- **From System Monitoring…**
- Financial systems are fault-tolerant, true system failures are rare…
- … But integration is extremely hard to get right
- ➔ ***Splunk allows us to measure cross-system efficiency***

- **… To Operational Intelligence**
- Integration patterns are asynchronous, this can cause choke points and chain reactions…
- … Often caused by an upstream system
- ➔ ***Splunk allows us to detect early symptoms and contain the risk of outage***



- **… To Trade Surveillance**
- Splunk captures all the trade booking steps down to the millisecond
- Which allows for indisputable timelines…
- ➔ ***… That can be tested against known suspicious patterns***

splunk> .conf2017

Alerts Inbox

Current number of alerts, trend over selected timerange and list of alerts

Timerange: Date time range | Submit | Hide Filters

Edit | Export | ...

Alerts Inbox

Operational	Benchmarks	Sales Practices	Rogue Trading	Market Manipulation
0 → 0	0 → 0	0 → 0	2 ↘ -4	1 ↘ -9

Recent Alerts

Owner: All | Alert: All | Category: All | Subcategory: All | Tags: All, [Untagged] | Status: All open | Incident ID: *

Title: | Impact: All | Urgency: All | Priority: All | Freeform Filter:

i	_time	owner	status_description	title	category	Desk	Location	tags	OutsideHours	priority
>	2017-05-05 02:15:19.900	mstinbox	New	Front Running - FX	Rogue Trading	FX	New York	[Untagged]	false	medium
>	2017-05-05 02:15:04.839	mstinbox	New	Front Running - FX	Rogue Trading	FX	New York	[Untagged]	false	medium
>	2017-05-05 00:25:08.255	mstinbox	New	Spoofing - Futures	Market Manipulation	Commodities	London	[Untagged]	true	medium
>	2017-05-04 18:25:33.345	mstinbox	New	Spoofing - Futures	Market Manipulation	Commodities	Australia London	[Untagged]	false	medium
>	2017-05-04 18:25:28.727	mstinbox	New	Spoofing - Futures	Market Manipulation	Commodities	Australia	[Untagged]	false	medium
>	2017-05-04 18:25:23.179	mstinbox	New	Spoofing - Futures	Market Manipulation	Commodities	Australia	[Untagged]	false	medium
>	2017-05-04 18:25:18.555	mstinbox	New	Spoofing - Futures	Market Manipulation	Commodities	Australia	[Untagged]	false	medium
>	2017-05-04 18:25:09.959	mstinbox	New	Spoofing - Futures	Market Manipulation	Commodities	Australia	[Untagged]	false	medium
>	2017-05-04 14:25:18.719	mstinbox	New	Spoofing - Futures	Market Manipulation	Commodities	Australia	[Untagged]	false	medium
v	2017-05-04 14:25:13.590	mstinbox	New	Spoofing - Futures	Market Manipulation	Commodities	Australia	[Untagged]	false	medium

Details

incident_id=be0f2f66-56ed-4598-a2f3-52bb54d798fe impact=medium urgency=medium

History

_time	user	action	details	comment

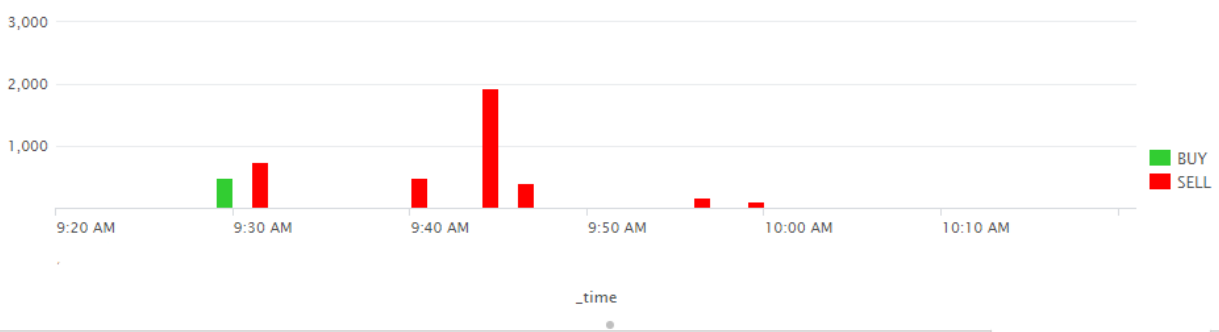
MST RADAR

Real-Time Trading Analytics

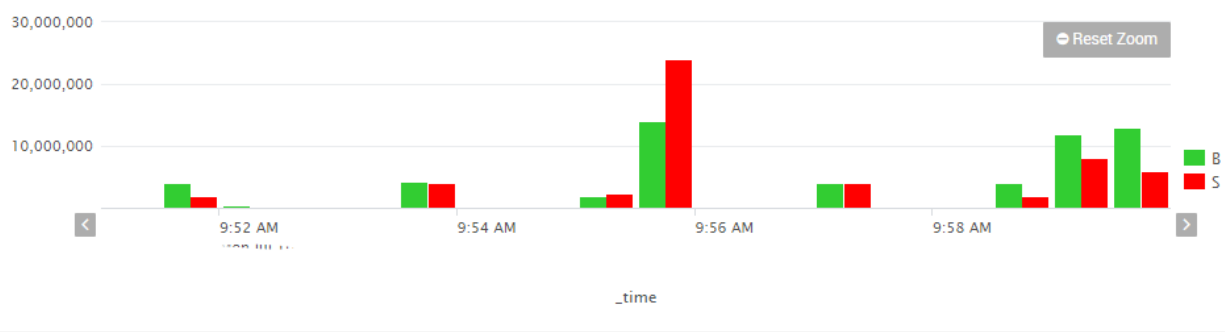
Edit | Export | ...

Markets Radar

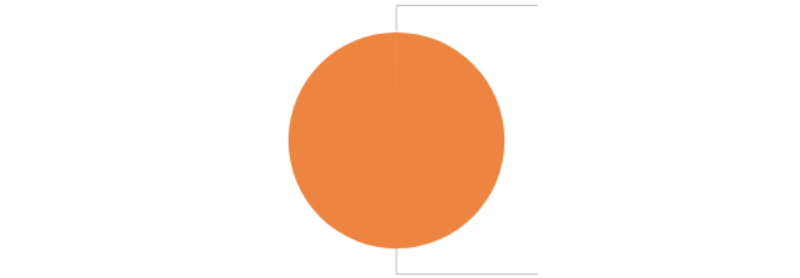
Futures Trading



FX Trading

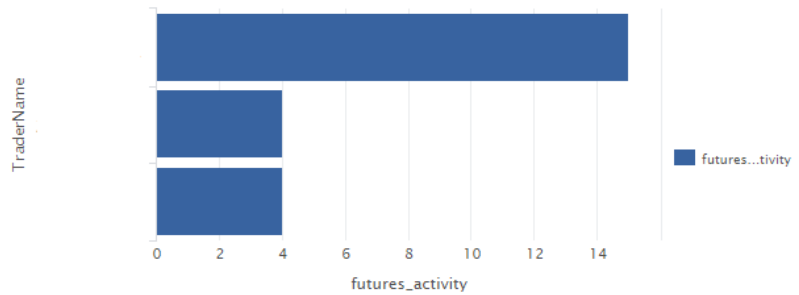


Desk Breakdown

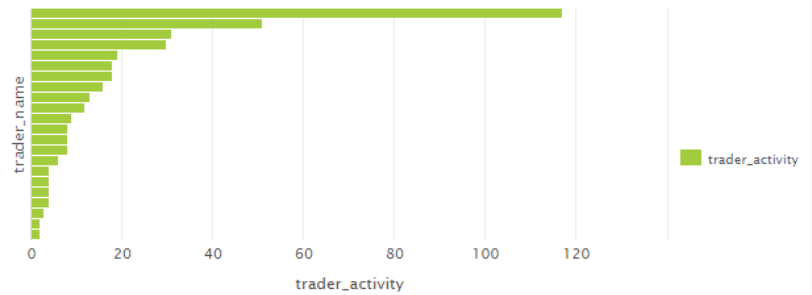


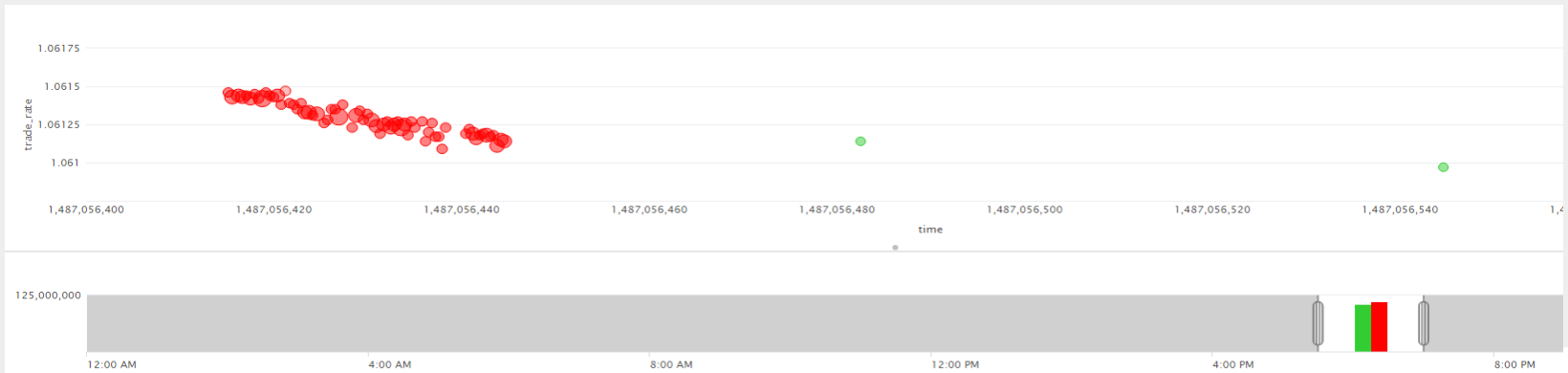
Futures Activity

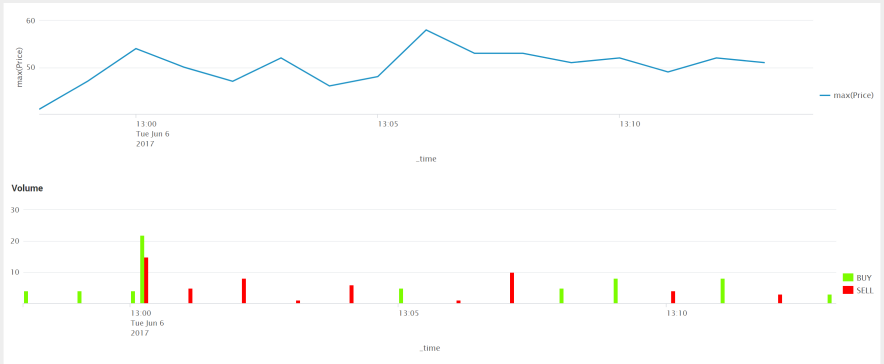
Real-time



FX Trading Acitivty







splunk> .conf2017

Trend Reporting & Drilldown Analytics

Chart Selector

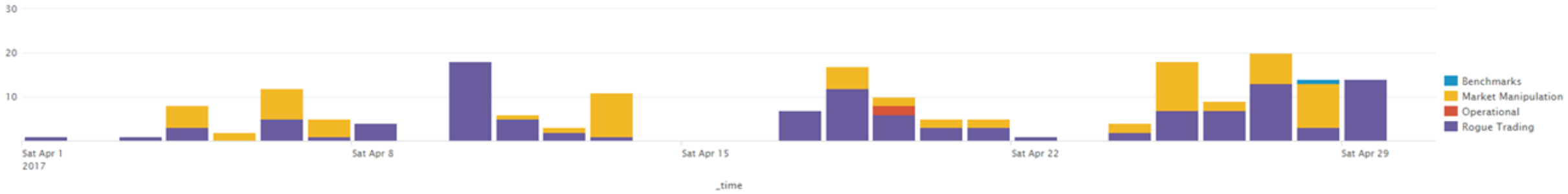
Split by Series

Total with Average

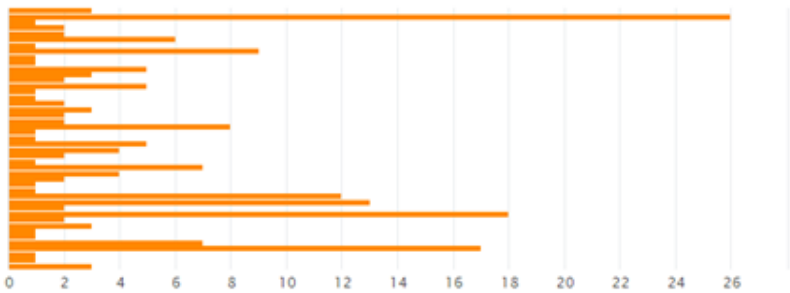
Split by: Category

Alert: All

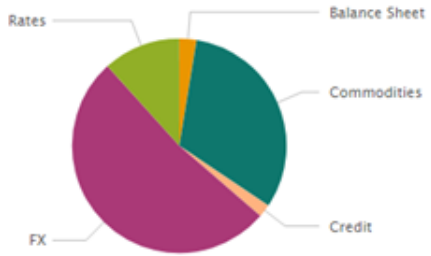
Timerange: Previous month



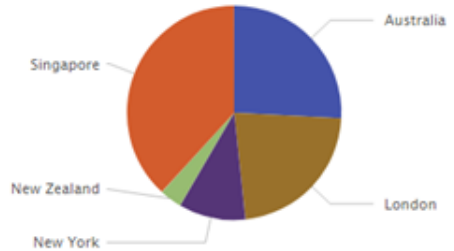
Alerts by Trader



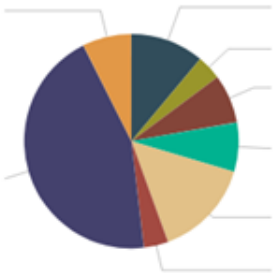
Alerts by Desk



Alerts by Location

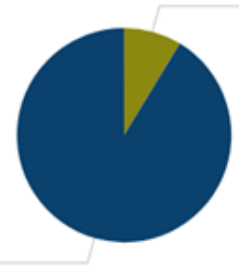


Alerts by Trader



Total Number of Alerts

Alerts by Type



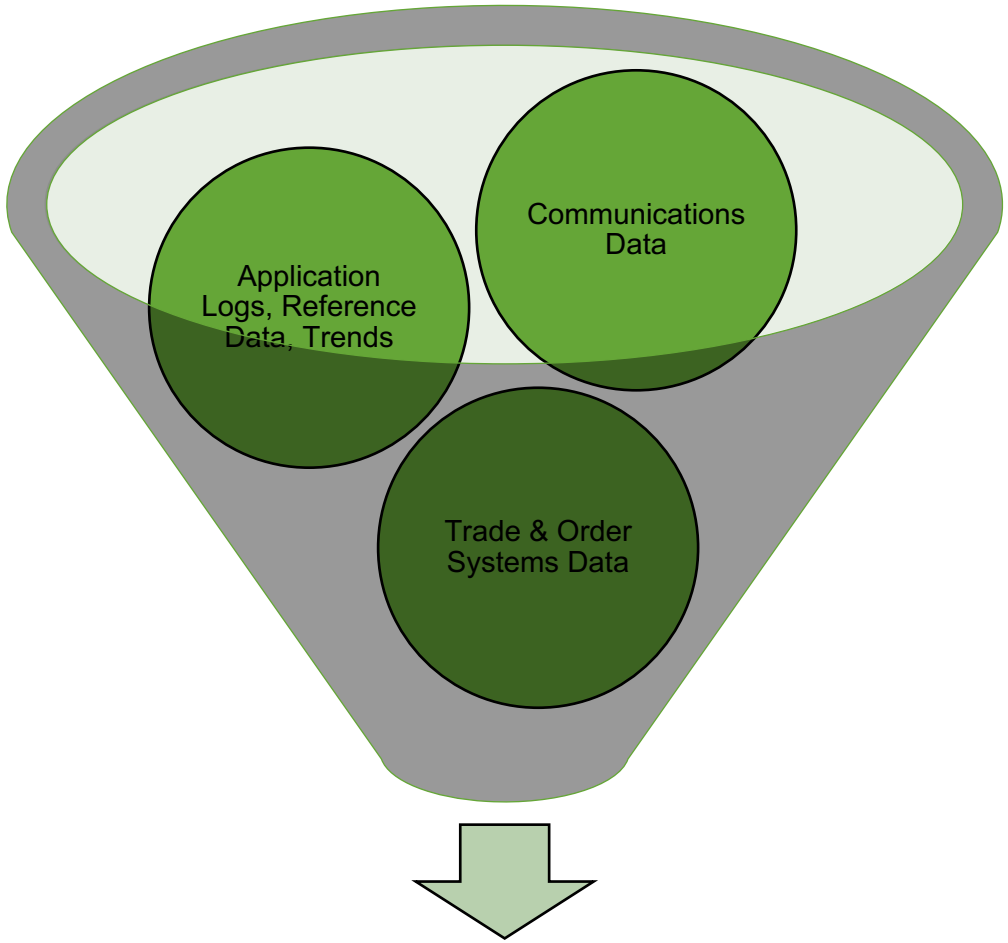
splunk> .conf2017

“But what about #machinelearning?”

Machine Learning

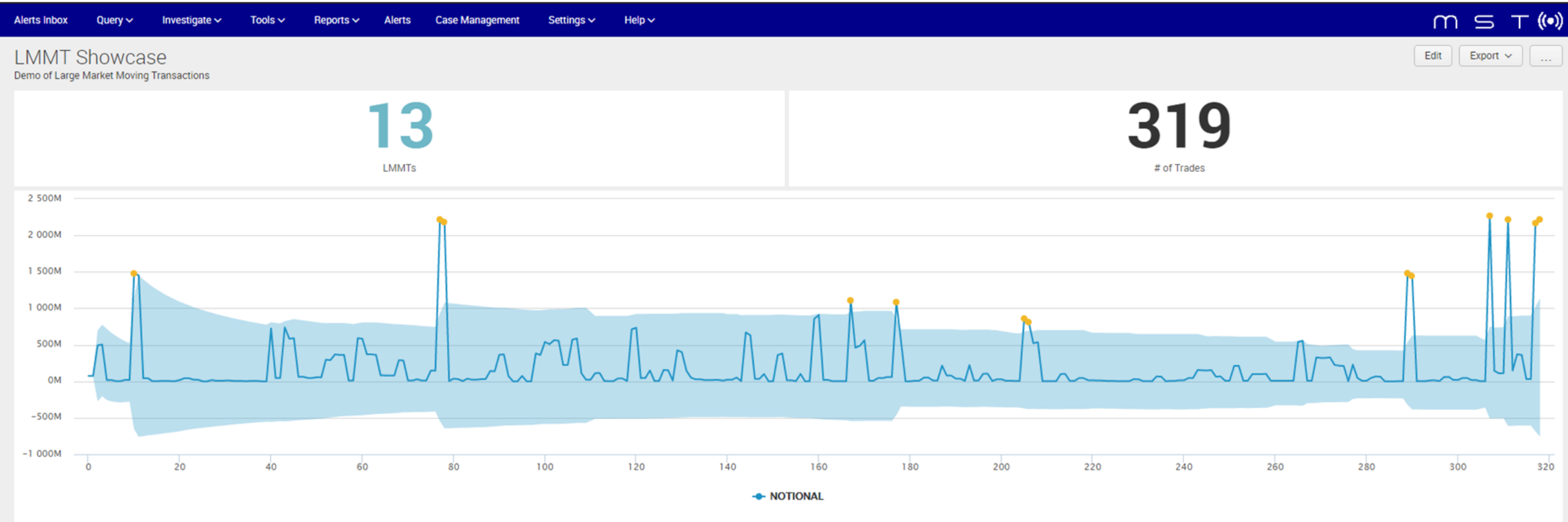
Our Approach

- Correlate data sources across 50+ metrics for individuals, product types, regions
- Identify patterns & behaviours with classification models
- Train classification model
- **Detect Rogue Traders!**

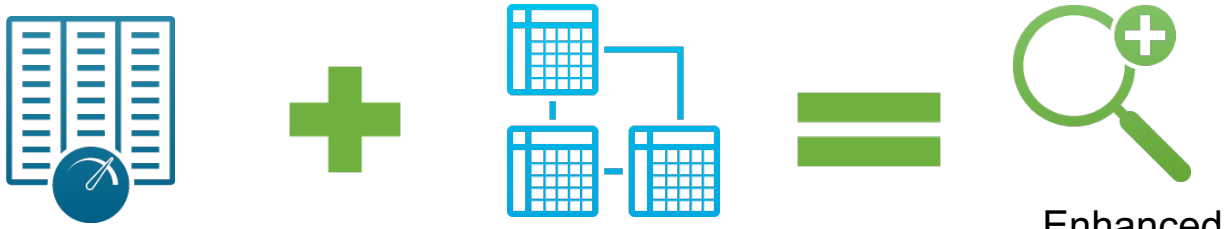


ML Classification Models

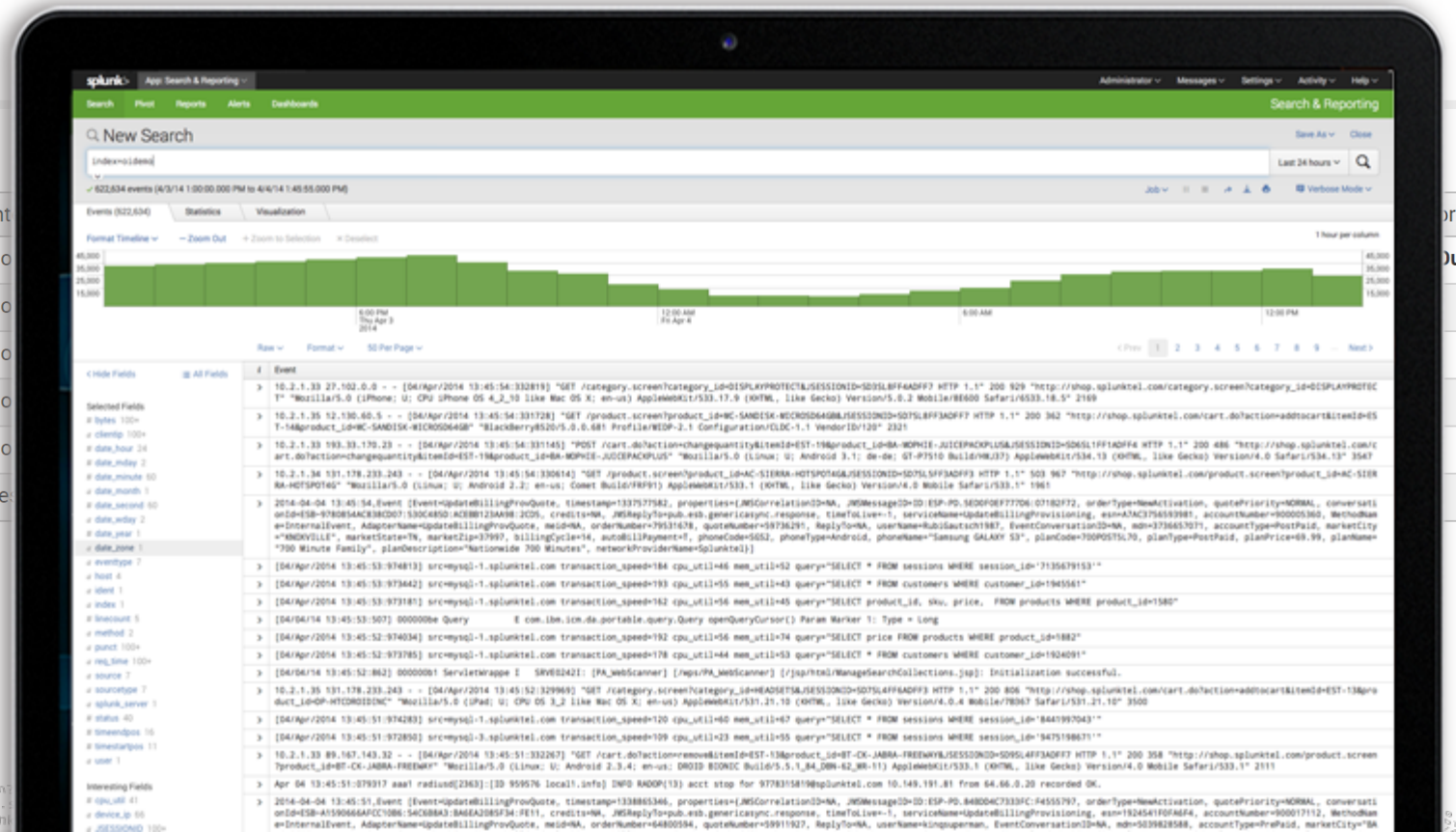
Adaptive Limit Anomaly Detection



Use ML Alongside Prescriptive Rules



Machine Learning + Prescriptive Rules = Enhanced Detection



Data and Outliers

Higher_Risk_Trading	Int	robable_cause	isOutlier
High	No	utsideHoursTrading	⚠ 1
Medium	No		✓ 0
Low	No		✓ 0
Low	No		✓ 0
Medium	No		✓ 0
Medium	Ye		✓ 0

splunk> .conf2017

The Splunk Value Evolution

What is going to happen?

Machine Learning, Predictive Analytics & Forecasting

What's happening now?

Real-Time Dashboards, Radar

Why did it happen?

Visualization Tools, Scorecards

What happened?

Reports, Query and Search Tools

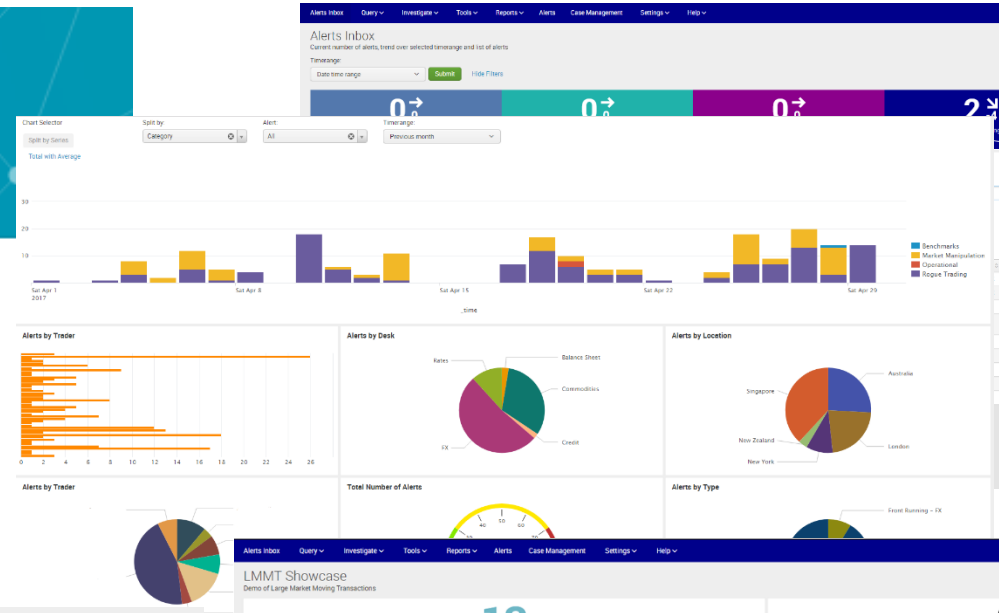
splunk> .conf2017

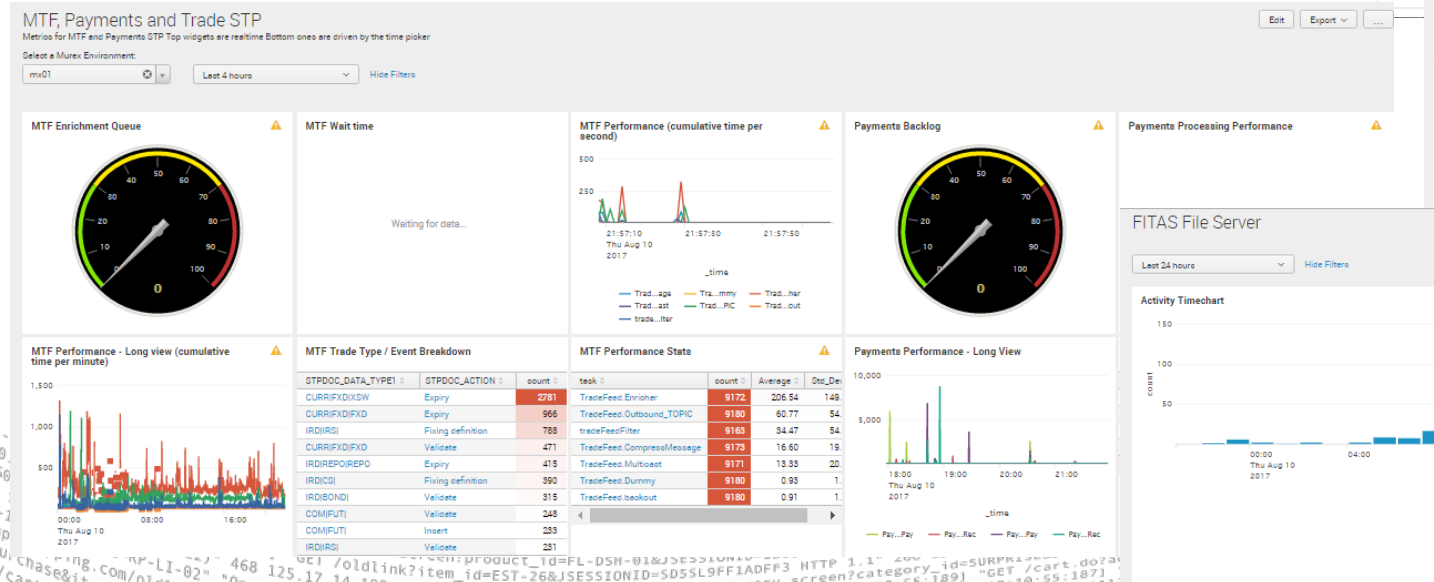
Add Us On LinkedIn!

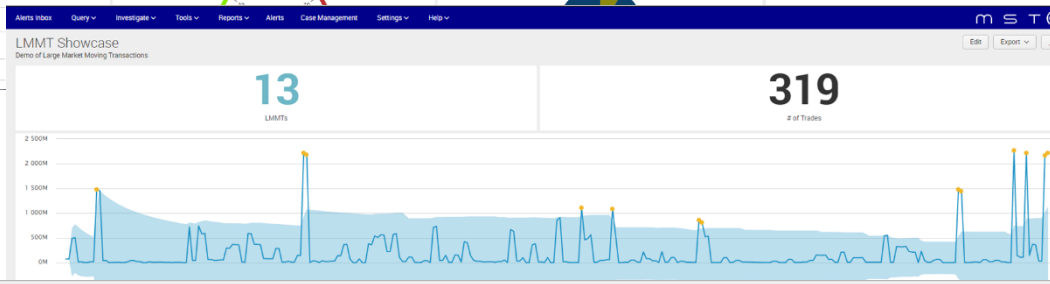
Aleksey Eremenko

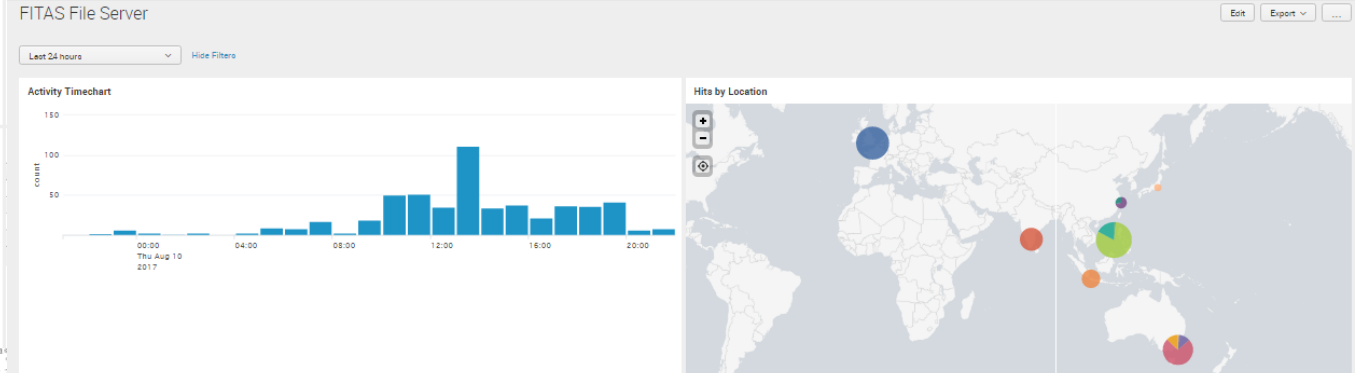
Markets Surveillance Manager

Vincent Leycuras









Thank You

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