# Building A Smarter Strategy For Alarms With Splunk Machine Learning Tookit!


Jason Rombough

TELUS, Technology Strategy

Matthew Modestino

Splunk> Advisory Engineer


.conf2016

splunk>

# Disclaimer

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 the 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.

# Meet The Presenters

**TELUS - Manager, Technology Strategy**
(2015 – Present)
OSS/BSS & GIS – TELUS MBNE

**TELUS - Manager, Network Integrity**
(2010 – 2015)
Tier – III Network & Service Assurance

**Splunk> - Advisory Engineer**
(2016 - Present)
Customer Success Manager

**TELUS - Design Specialist, Network Integrity**
(2012 – 2016)
Network & Service Assurance
Splunk> Technical Champion

# TELUS At A Glance

TELUS
the future is friendly®

| | |
|---|---|
| Wireless Subs | **8.5 million** |
| LTE Penetration | **>85% of data traffic goes over LTE** |
| Smartphones | **82% penetration** |
| Canadian Population | **35+ million** |
| Area | **10M Km²** |
| Annual Revenue | **$12.5 billion** |
| Wireless Revenue | **$7 billion** |
| Wireless ARPU | **$63.74 CAD** |

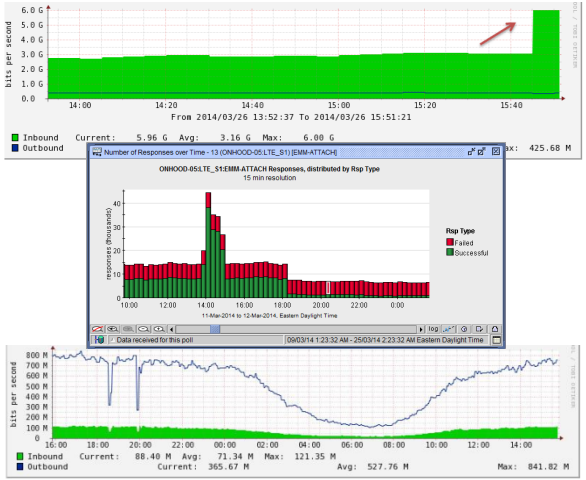
TELUS is Canada's fastest-growing national telecommunications company, with $12.6 billion of annual revenue and 12.5 million subscriber connections. TELUS provides a wide range of communications products and services, including wireless, data, Internet protocol (IP), voice, television, entertainment and video, and is Canada's largest healthcare IT provider.




splunk> .conf2016

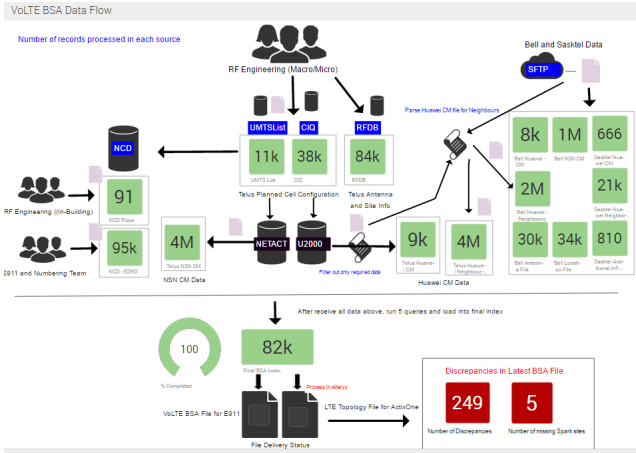
# An Ops Intel Journey…

## March, 2014




## Sept 2015


## July 2016



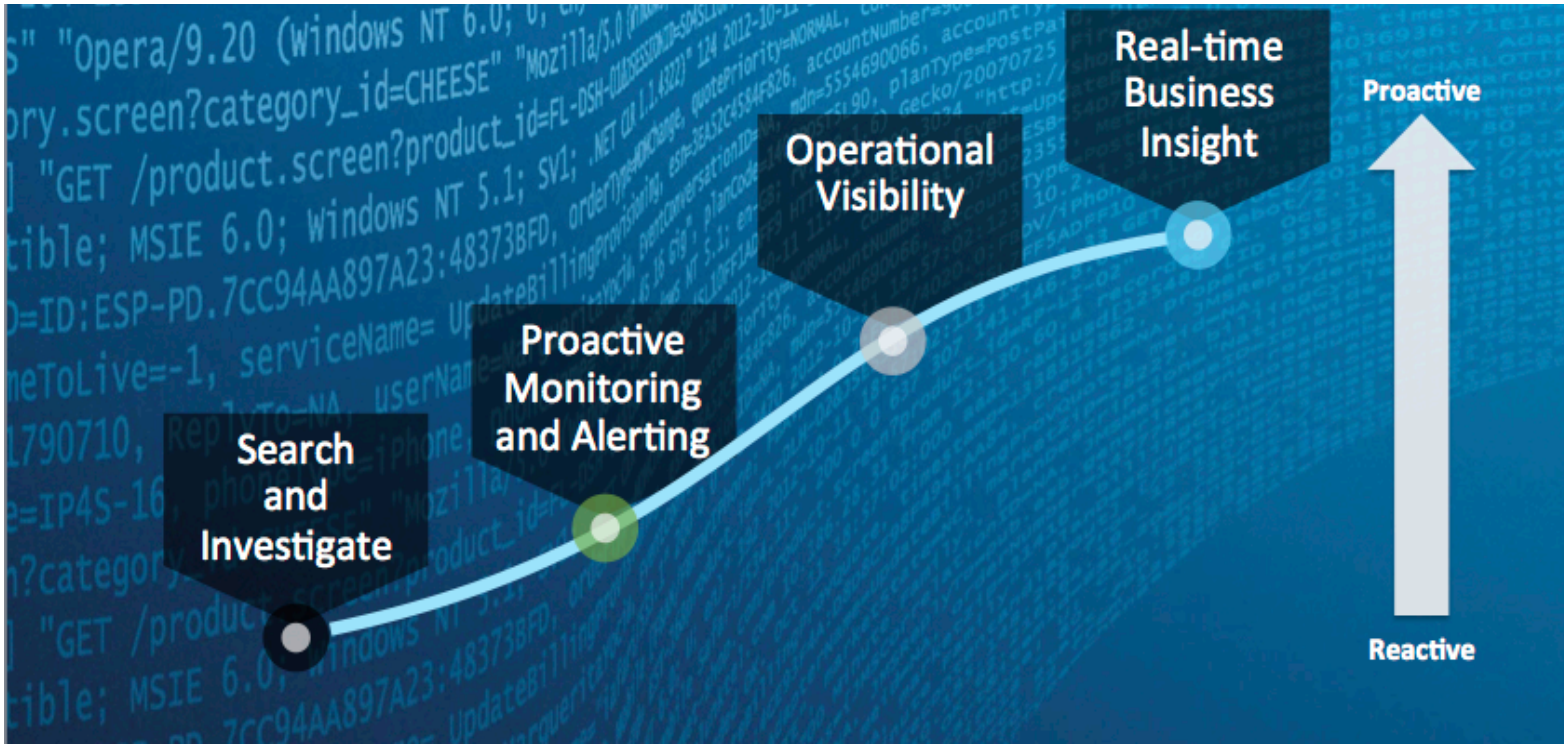

**Graph Wars**

**Enriched Viz**

**Glass Tables**

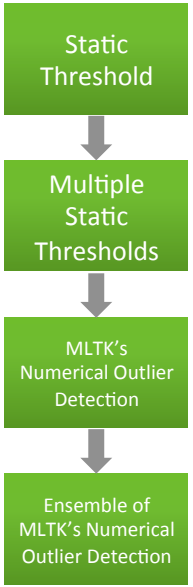
*Proactive Pursuit of OI4*

# Phases Of Operational Intelligence



# Quest for Operational & Business Intelligence

## Building Monitoring Tools Process




✗ Too restrictive for dynamically changing data

✗ Too many rules to be set for too many KPIs

✓ Catches most of outlier without knowing the data range

✗ Misses subtle outliers

✓ Catches subtle outliers too

## Machine Learning Workflow

1. **Get** data
2. **Split** data (set aside some to train the model, some to test its performance)
3. **Fit** the model on some of the data (training data)
4. **Apply** the model on data the model hasn't seen (test data)
5. **Evaluate** the performance of the model on the test data
6. **Adjust** the model based on sources of error
7. **Repeat** as needed until the margin of error is low enough

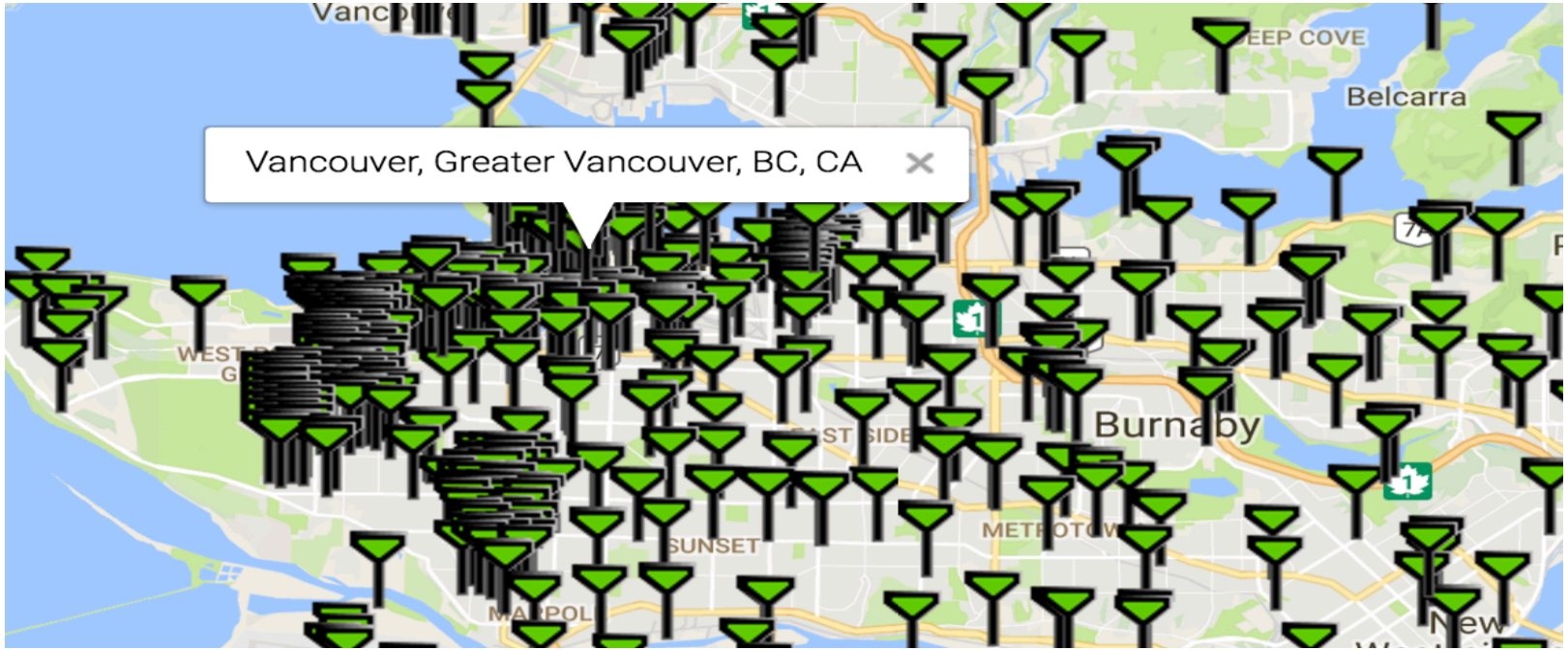
B U I L D

8. **Use** the model on real world business questions

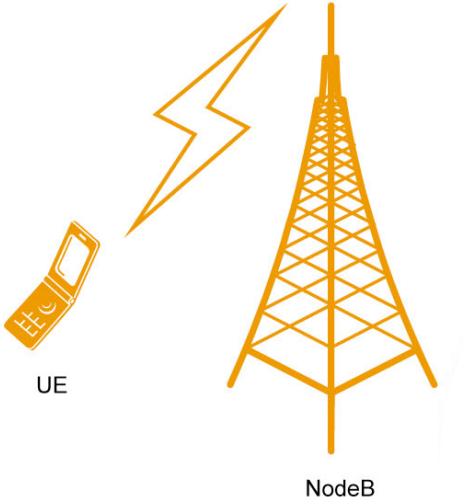
# Use Case #1:
# Wireless Network Operation Profiling

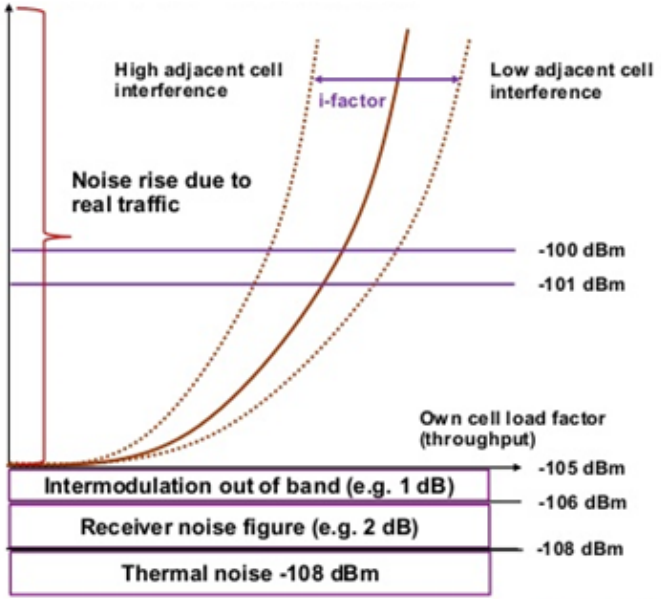
## “The Trick Is To See The Forest For The Trees“

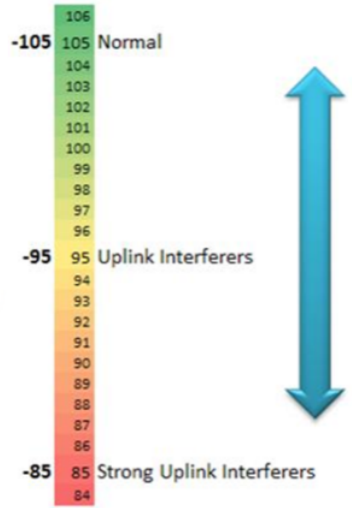
# Mobility 3GPP RAN KPI



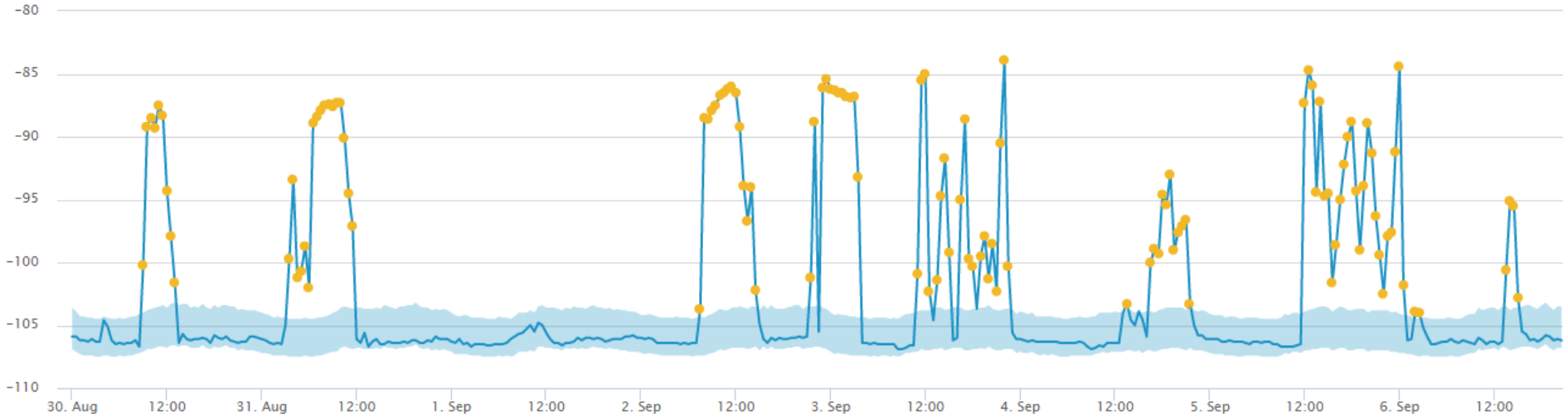
# Radio Access Network Interference



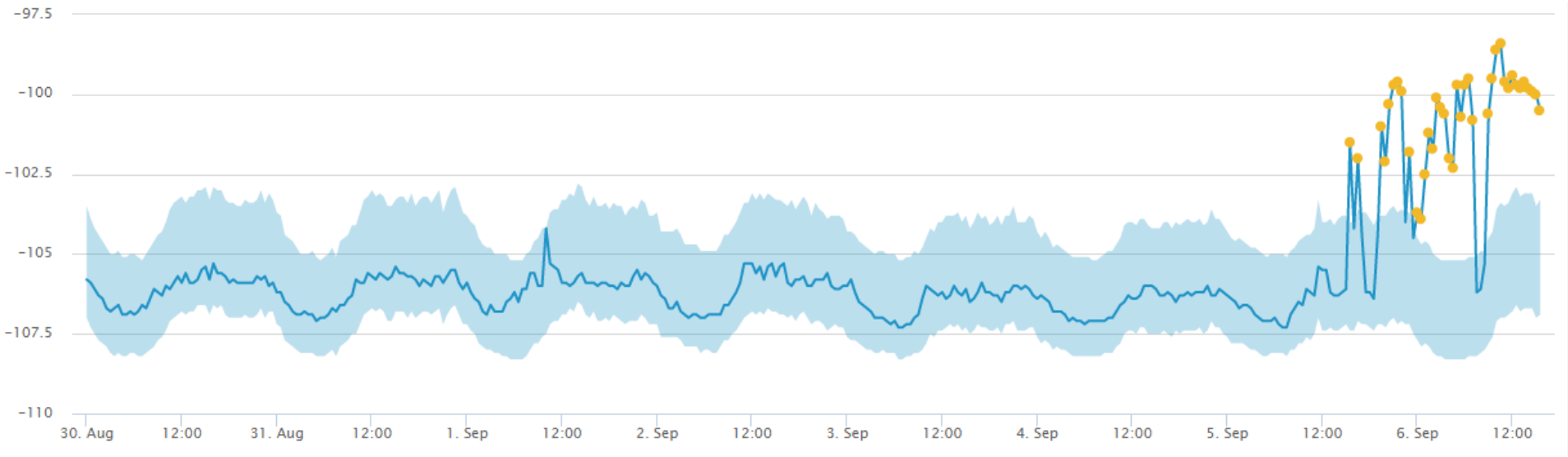



# Example #1



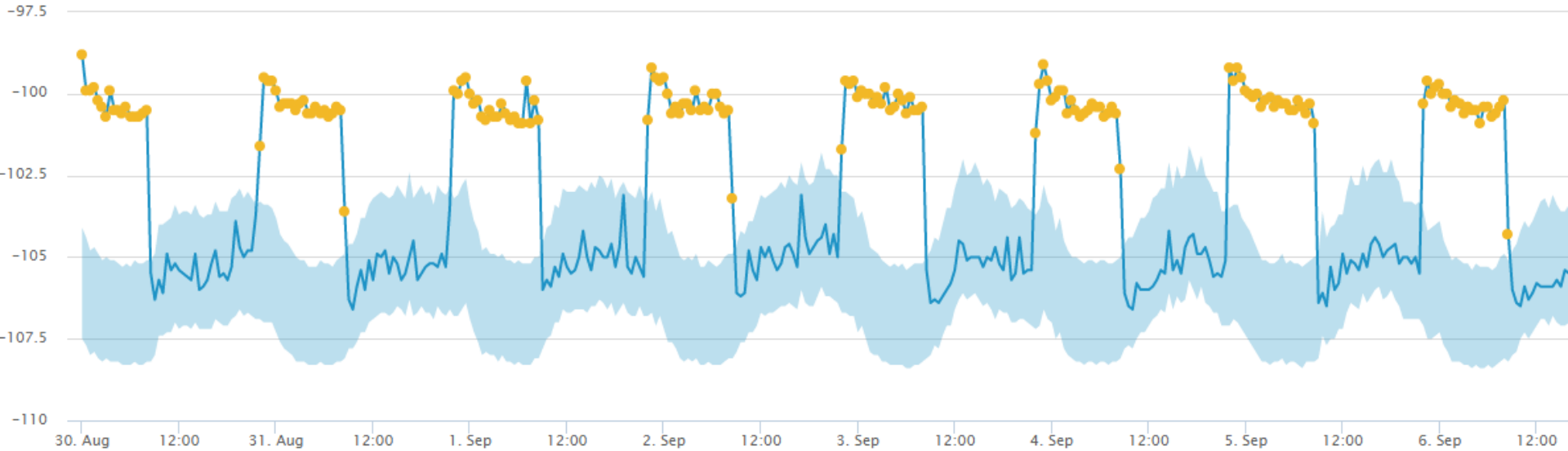

- Outlier detected for abnormal interference pattern.
- Not every cell has the same issue but many cell neighbors experience a similar pattern

# Example #2



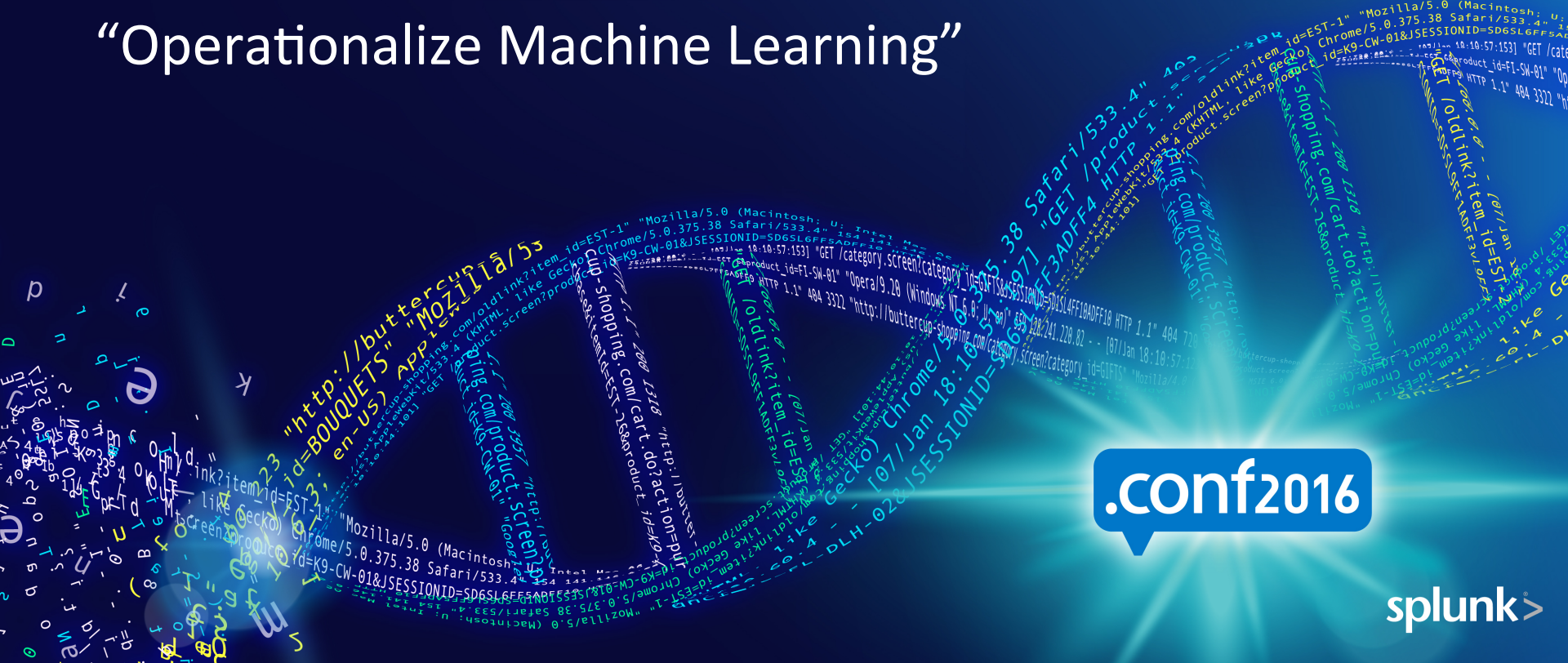

- Recent spike in interference alerts team members to begin investigations.
- MLTK assist the information overload problem through machine correlation vs manual correlation

# Example #3



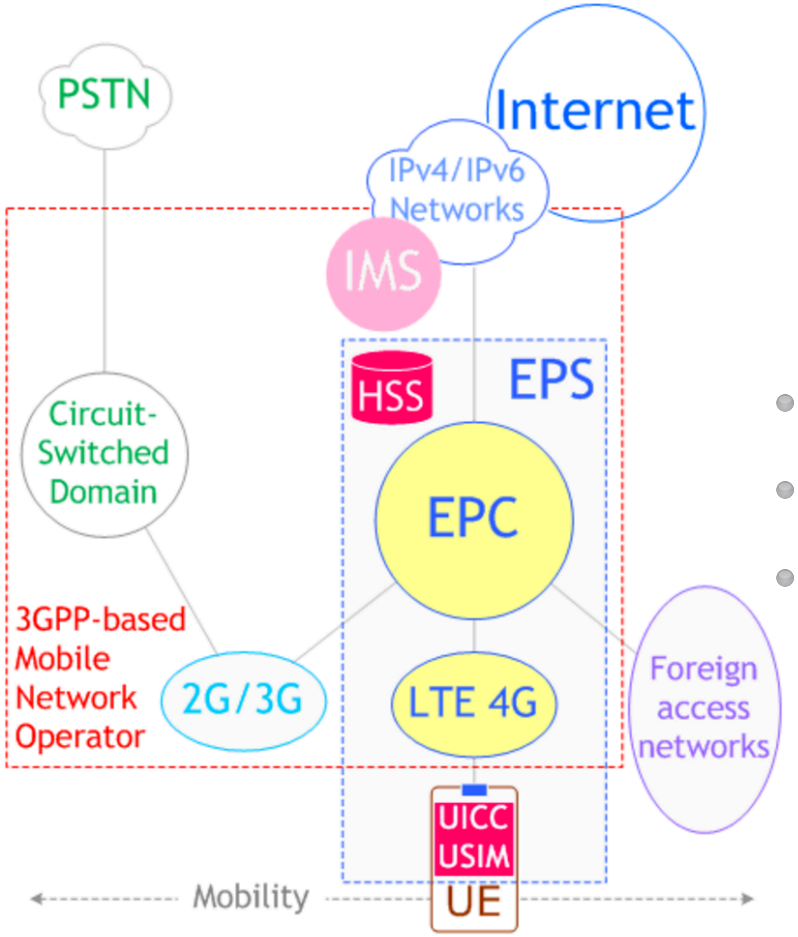

- Outlier detected for potential faulty tower light
- The tower light turns on only at night and Nav Canada controls the blinking interval.

# Use Case #2:
# Outlier Detection On 3GPP Core KPI
## “Operationalize Machine Learning”



.conf2016

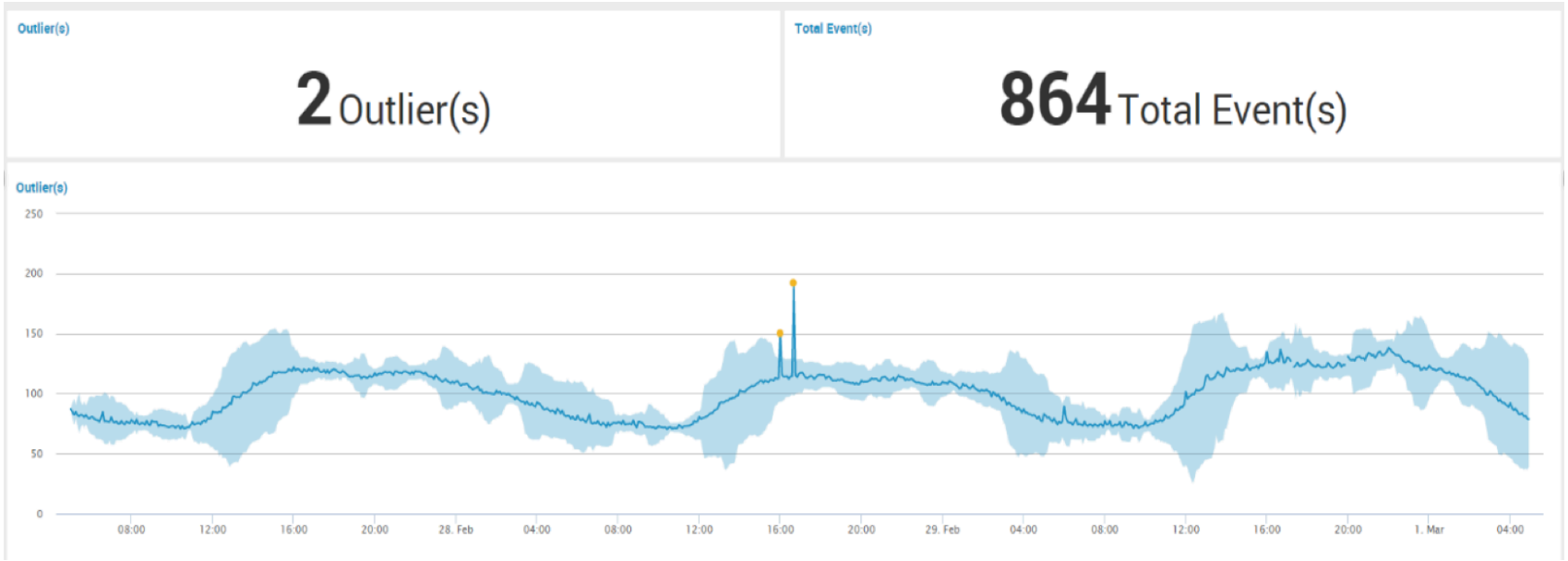
splunk>



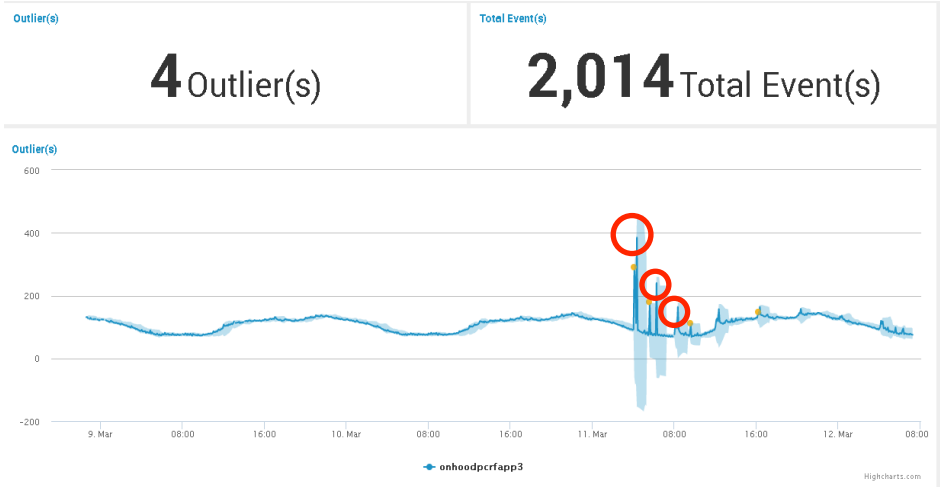

# Mobility 3GPP Core KPI

- Connection Details on 3GPP Core as KPI
- Real-time Network Behaviour
- Performance Degradation Monitoring

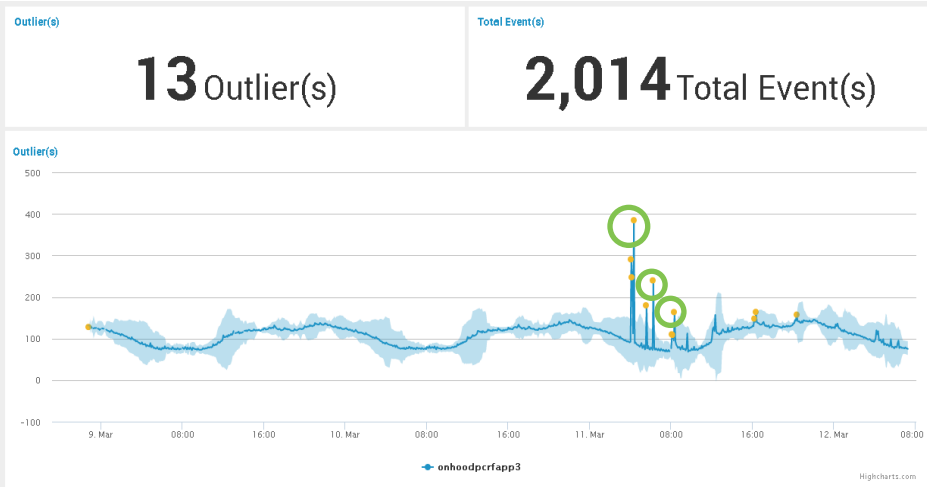
# Numerical Outlier Detection In Machine Learning Toolkit



# Iterating Over Different Threshold Methods




Standard Deviation




Absolute Median Deviation

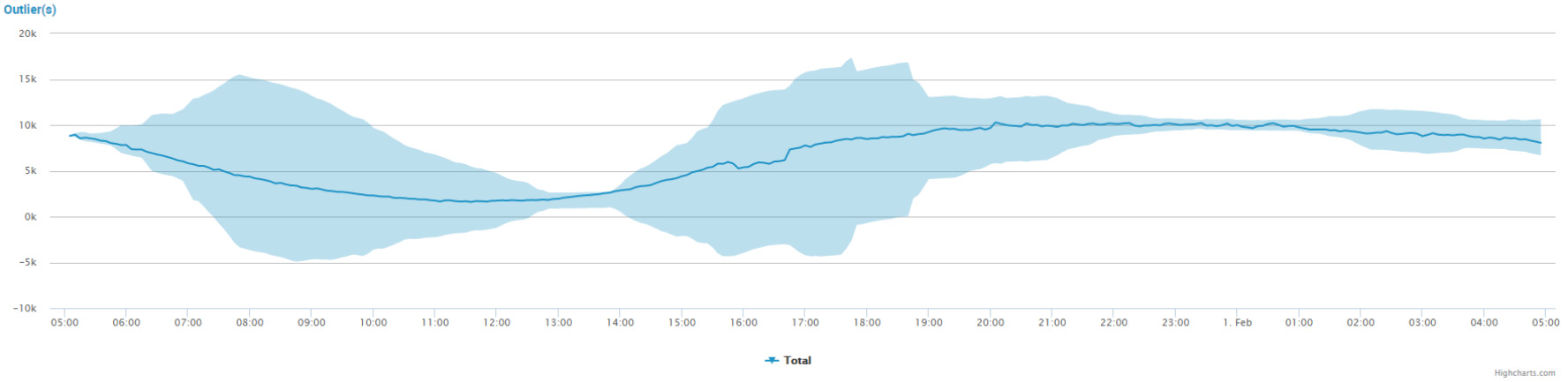
# Missed Outlier!

Outlier(s)

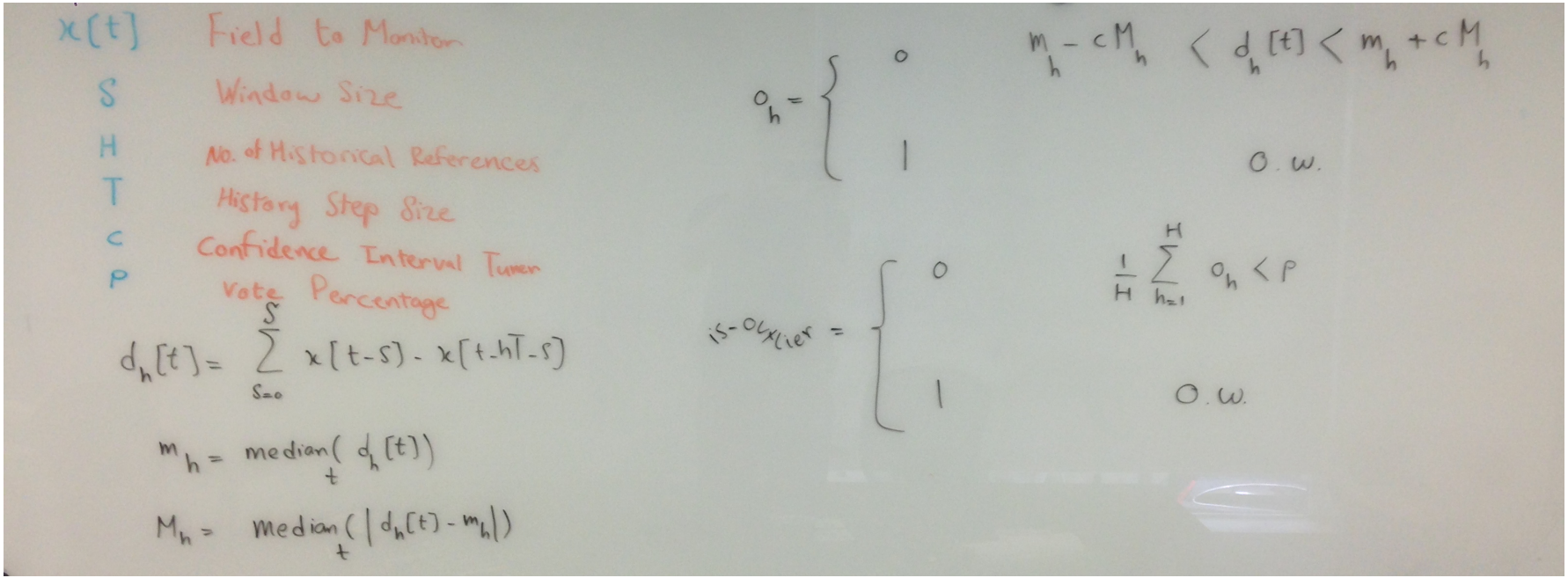
**0** Outlier(s)

Total Event(s)

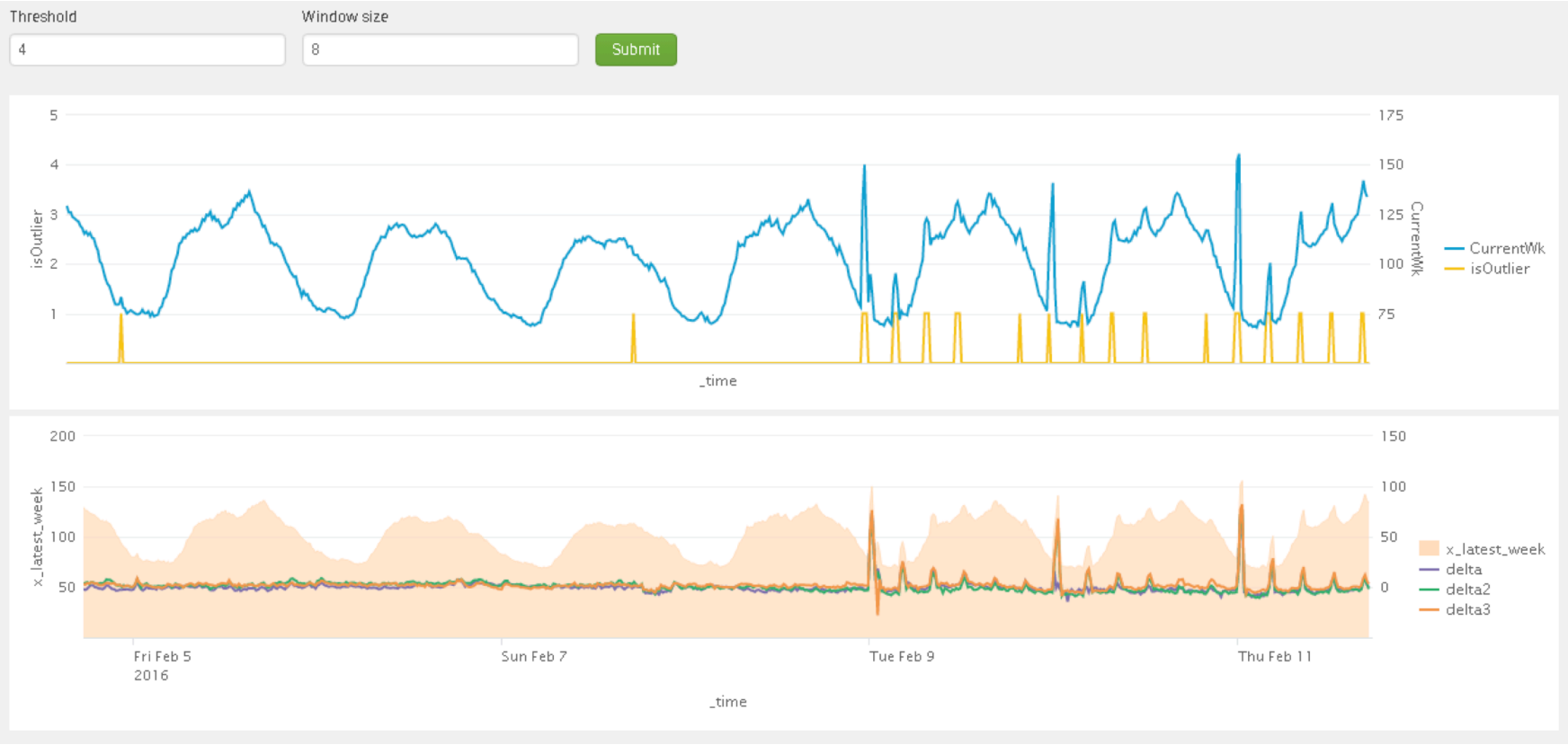
**288** Total Event(s)



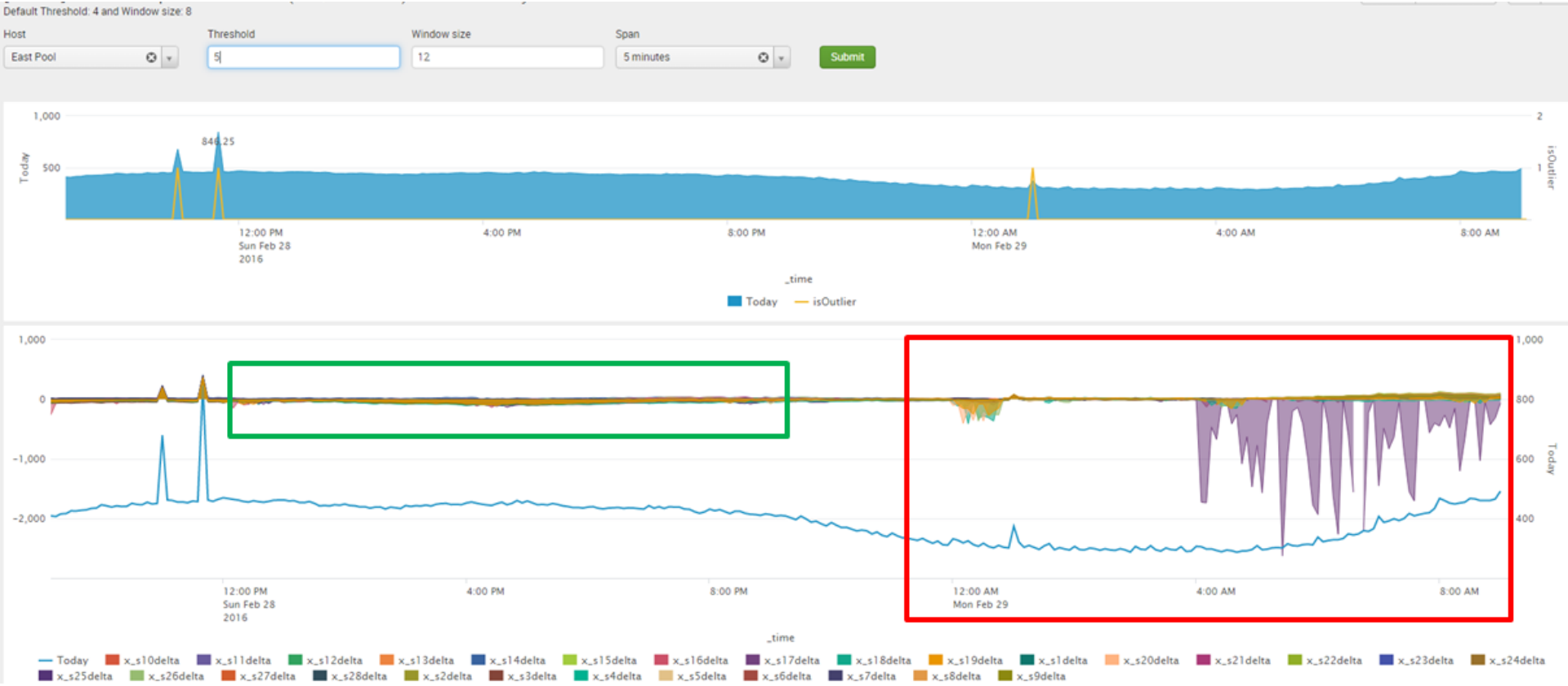
# Customized Outlier Detection



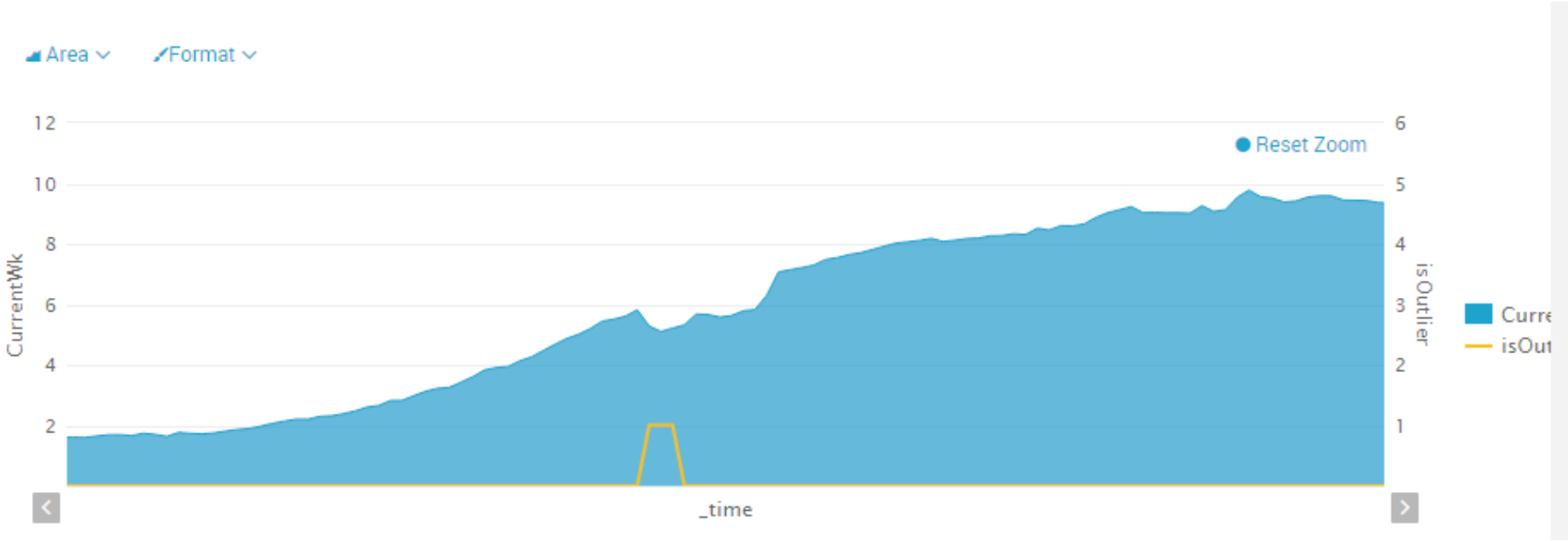
# Evaluate!



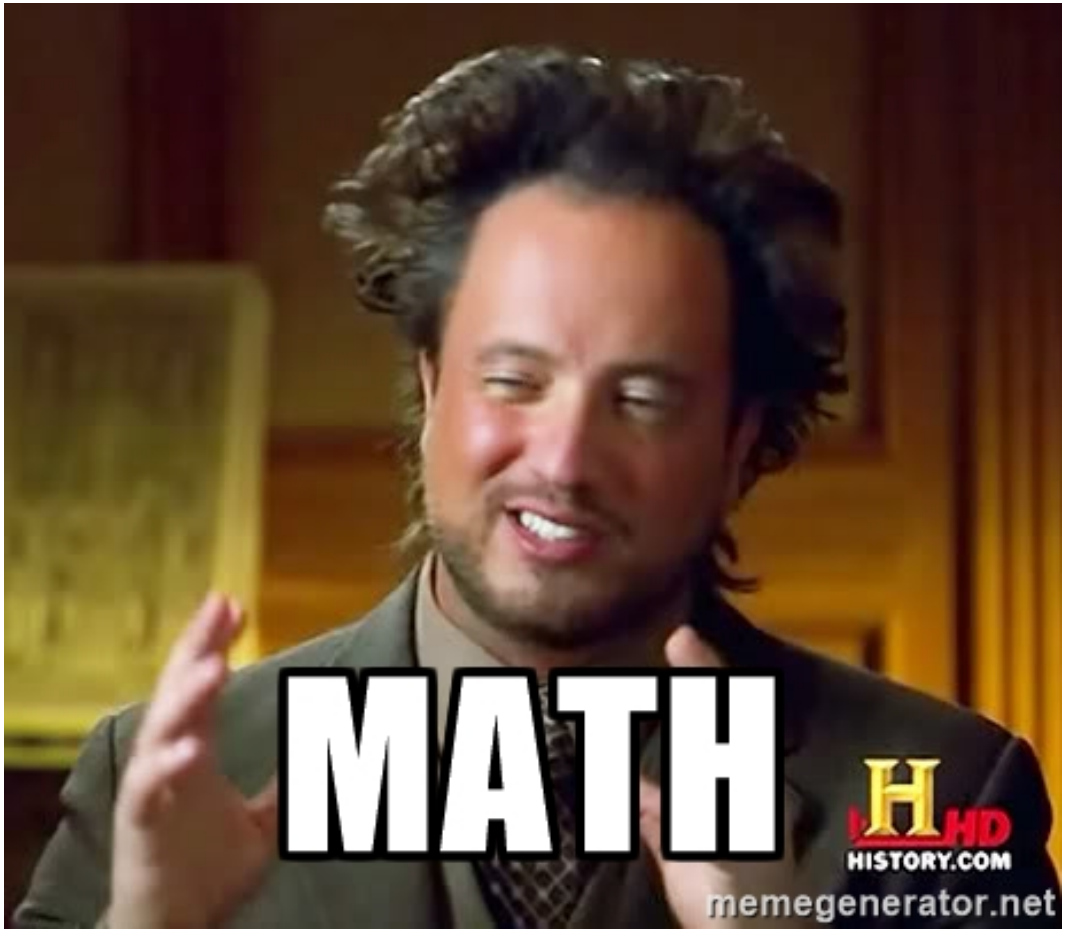
# Current Vs Historic And Delta Calculation



# DETECTED!



# Conclusion
## “Feed the Models!”



# Conclusion

- Future of IT -> Leveraging Machine Learning
- Machine Learning Toolkit (MLTK) Helped:
  - Modelling Complex System's Behaviour
  - Right Algorithm
  - Custom Visualization
  - Quick Validation
  - Generating SPL
- OI4

# THANK YOU


splunk>