Art of Reality -ITSI and the MLTK or There is No Spoon

Nate Smalley, Senior SE Manager
Arvind Swaminathan, Product Manager for ITSI Machine Learning
Andrew Stein, Splunk Principal PM for Machine Learning

May 2018 | Version 1.0

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.

Nate Smalley

- IT Operations Technologist
- Former Technical Director of Security & Monitoring Tools Team – Apollo Group (University of Phoenix)
- Currently Splunk Engineering Manager
- Enjoy Long walks across SNMP and Candle light dinners while fighting Operational Outages

Arvind Swaminathan

- Product Manager with ITSI in charge of the Machine Learning features (and few non-ML)
- Released the Health Score Prediction, KPI Forecast and Probable cause analysis PA features in ITSI out of the box
- Currently working on releasing more out of the box PA in ITSI

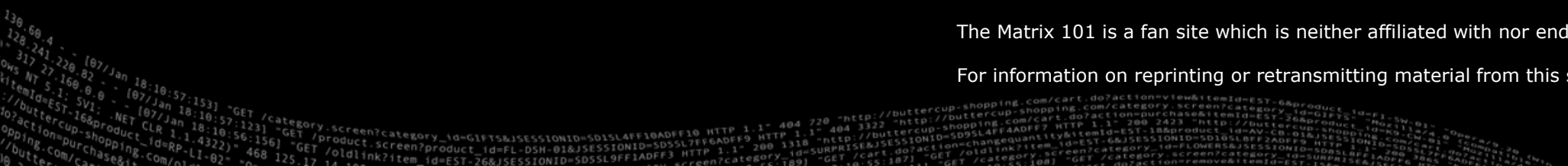
Andrew Stein

- Splunk Principal Product Manager – Machine Learning
- 18 years creating mathematically modeled solutions as a data scientist.
- I spend 80 percent of time spent preparing data and 20 percent of time complaining about the need to prepare data.

Agenda

Are You in the Right Room?

- Saturday Afternoon Phone Calls
- Out of the Box in ITSI: The Blue Pill
- Custom ML in ITSI: The Red Pill



splunk> .conf18

Saturday Afternoon Phone Calls

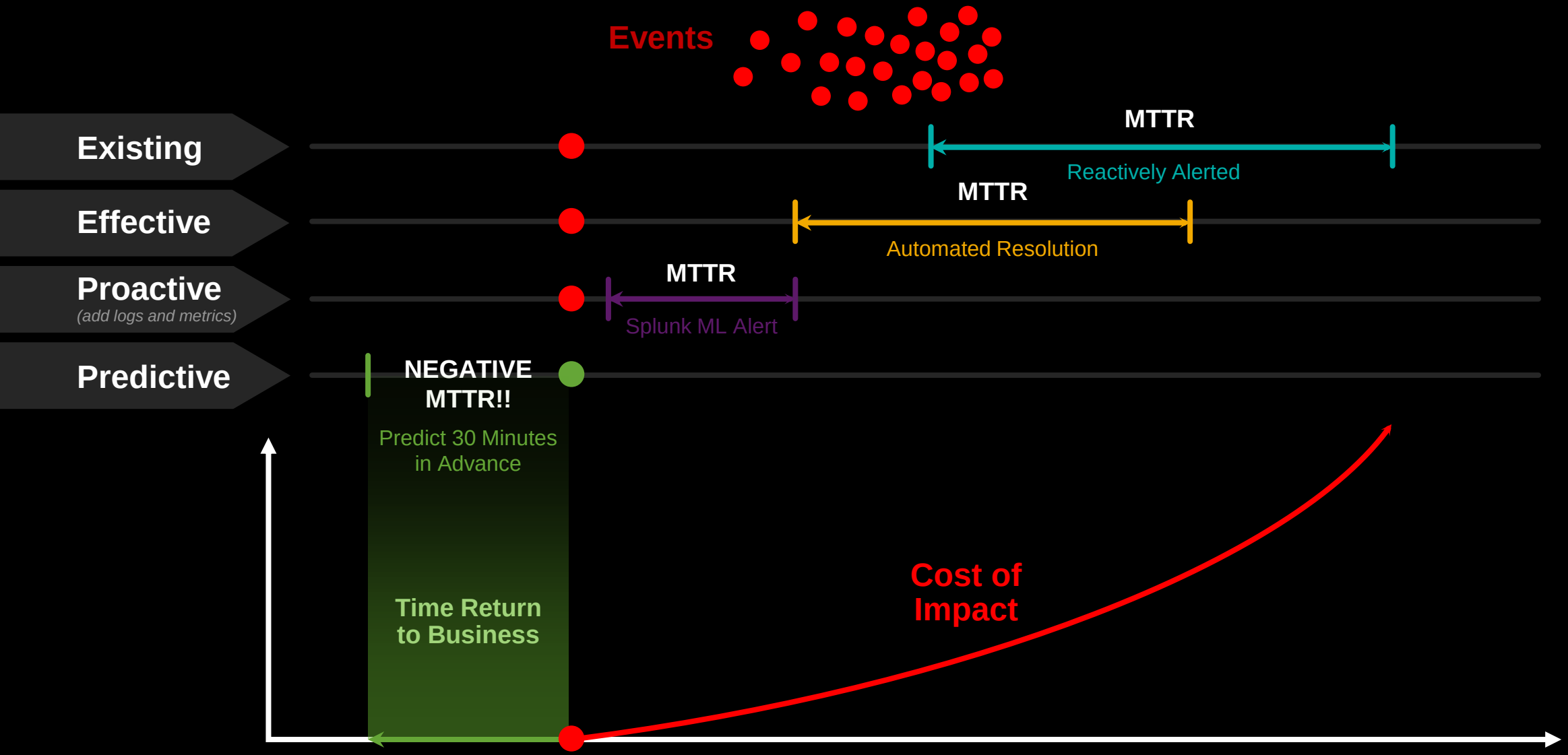
This is a Fun Saturday for Splunkers

splunk> .conf18

When the Phone Rings…

Do You Answer?

Why Use Machine Learning?



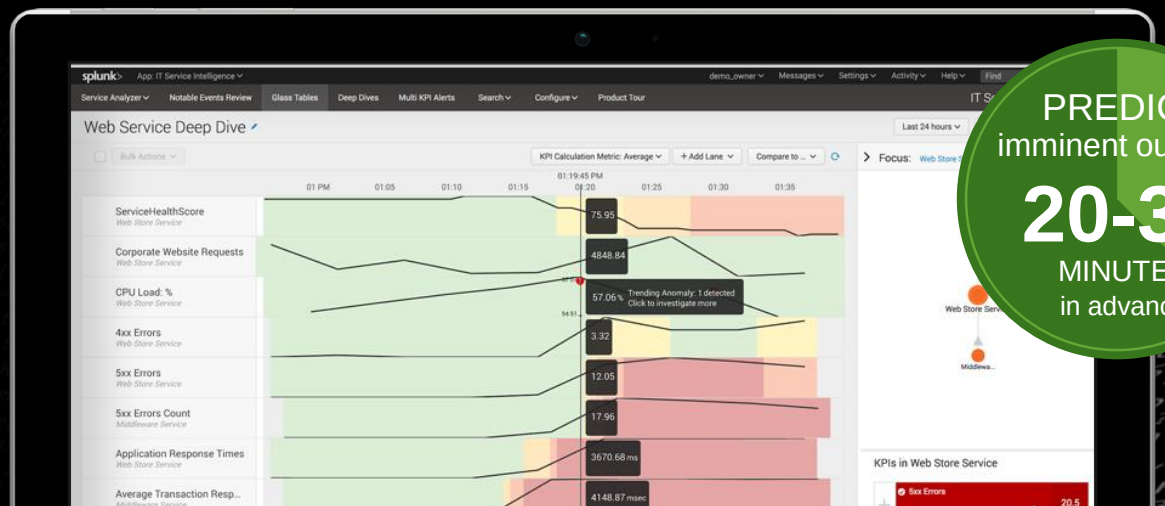
Splunk IT Service Intelligence (ITSI)

Predictive analytics for real-time insights, simplified operations and root-cause isolation

Predict and Prevent Outages
while reducing event noise & MTTR

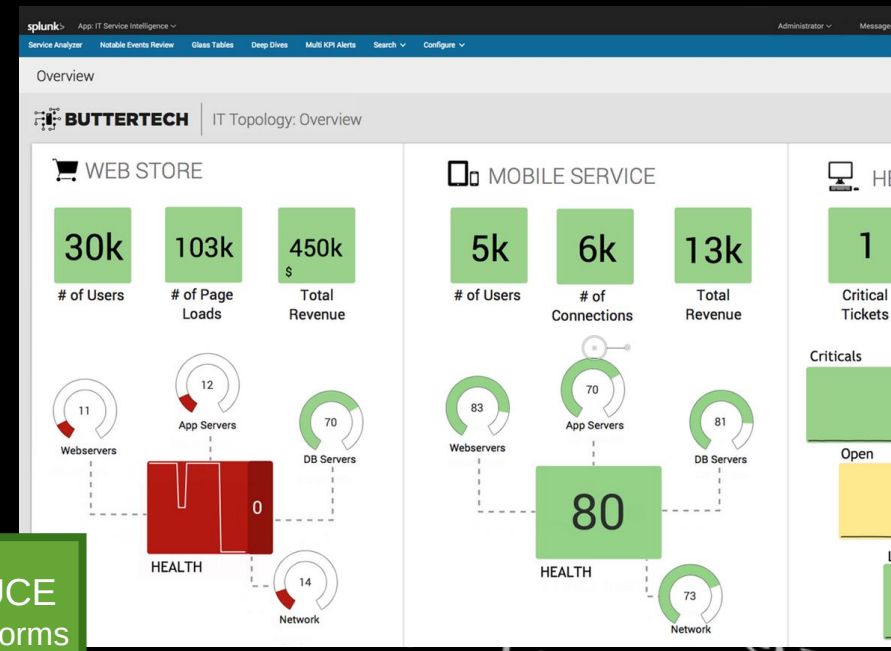
Create a 360-degree View
of real-time insights across all business & IT services

Trust the Splunk Platform
for scalability and versatility with artificial intelligence (AI) at its core

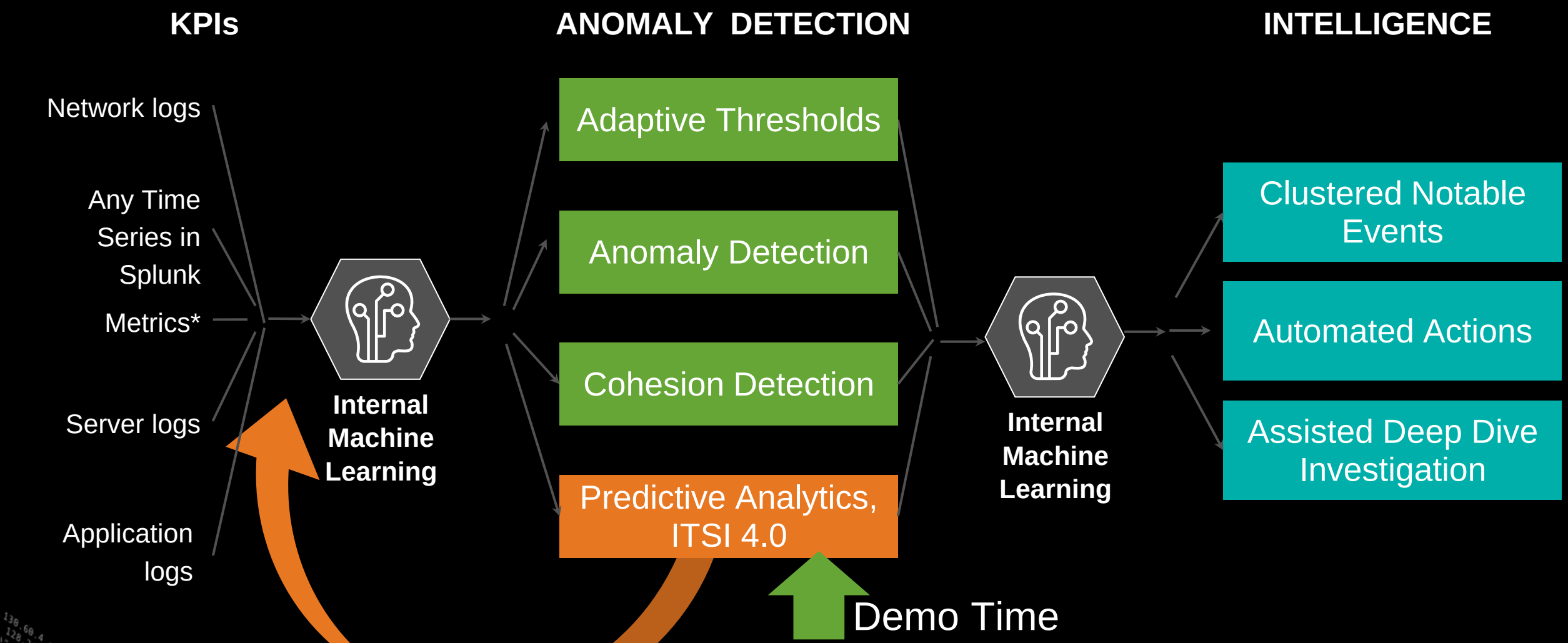


PREDICT
imminent outages
20-30
MINUTES
in advance

REDUCE
event storms
& noise by
+95%



Machine Learning in ITSI



Out of the Box!

You Take the BLUE PILL
The Story Ends, You Wake Up in Your Bed and Believe Whatever You Want to Believe

Out of the Box

The Blue Pill: ITSI 4.0

Predict Imminent Service Degradation 30 Minutes in Advance

Find the Probable Root Cause of Service Degradation Using KPI Prediction

See the KPI's Predicted Root Cause for the Next 30 Minutes

Splunk Demo

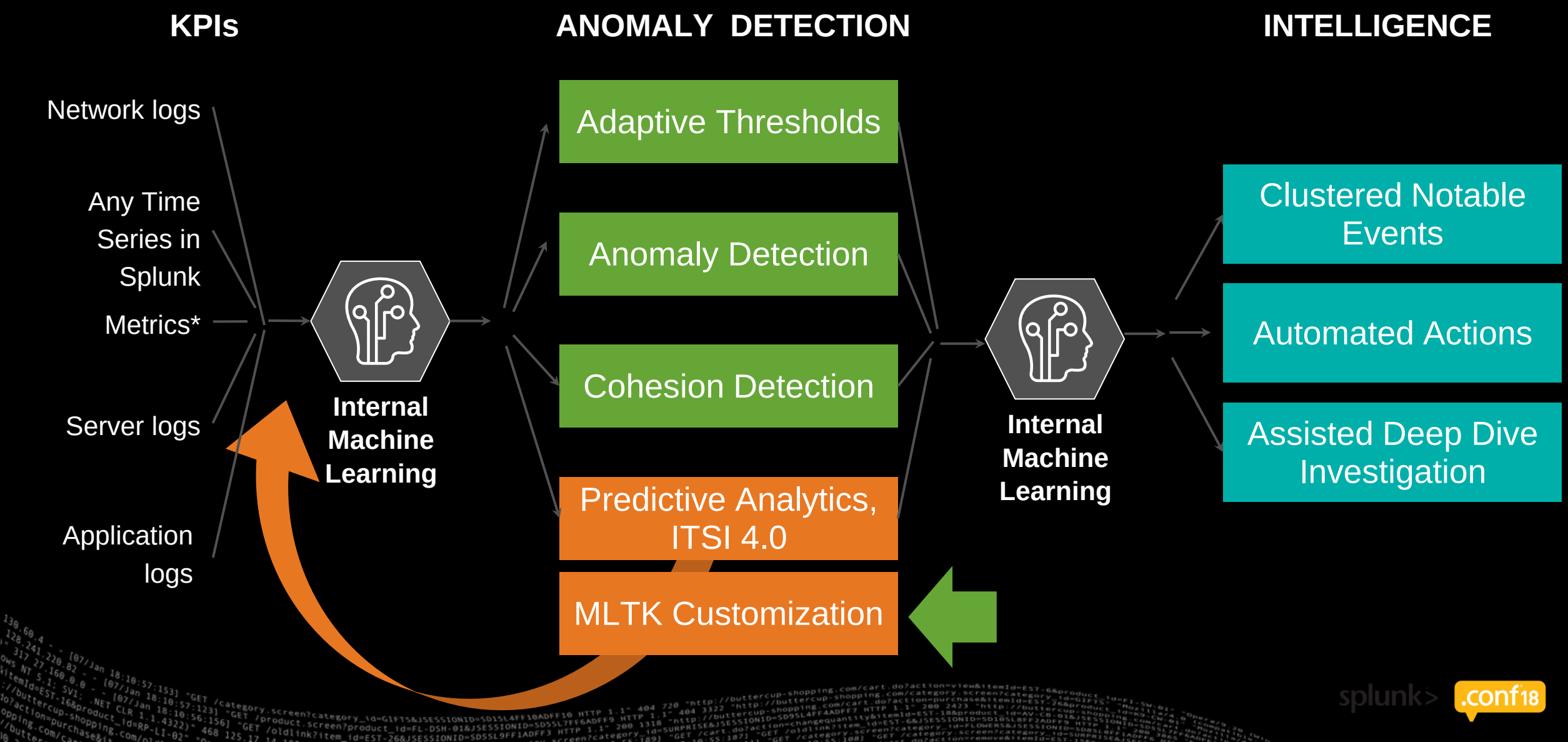
Presented by Arvind Swaminathan

splunk> .conf18

Real World Complications

You Take the RED PILL
You Stay in Wonderland and I Show You How Deep the Rabbit Hole Goes

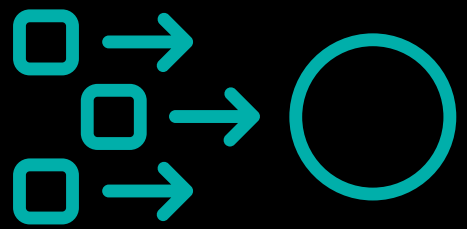
Machine Learning in ITSI



“We Can Never See Past Choices We Don’t Understand”

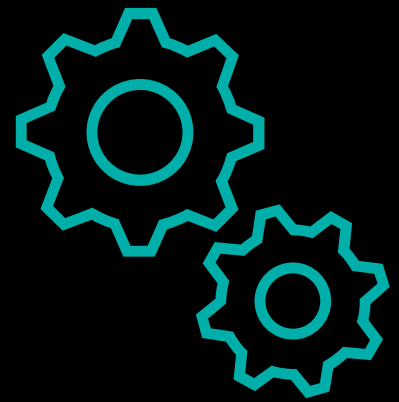
Where We Left Off in This Trilogy…

Get a bunch of data consistently moving through time in ITSI’s Service Health Scores and KPIs



Use a bit of time shifting SPL to move the Service Health Score so you can predict the future

Build a model and operationalize with ITSI



Don’t Fear the Math!

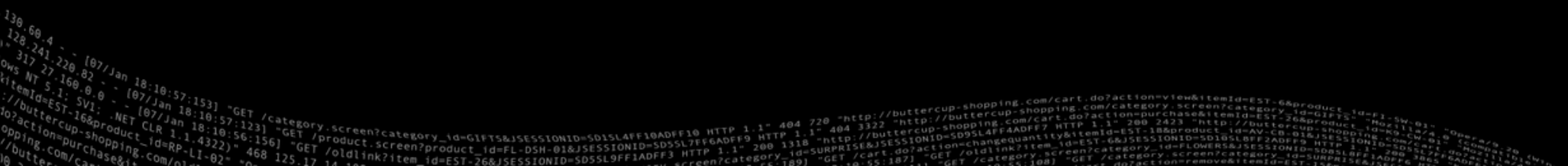
Customer Asks and Unintended Side Effects

Top Customer Asks

- Popular Fields
  - Introducing Business Rules
    - Example: Holidays!
- External Data Sources as Features
  - Anything in the Search Bar is fair game!
  - Remember to build other Services in ITSI to keep it all clean!

Unintended Side Effects: Beware!

- Removing outliers from the Service Health Score is NOT always a great idea
  - You want variance from the past so you can better understand the future
  - You do this through finding anomalies and label them as anomalies, remove, or replace the values with new ‘normal’ values



Don’t Like to Predict the Numbers? Then Predict the State!

Leverage ITSI’s ’Intelligence’

Change Your Target from Numeric to State Value and Use a Classifier

Now Your Prediction is the State

Best Practices

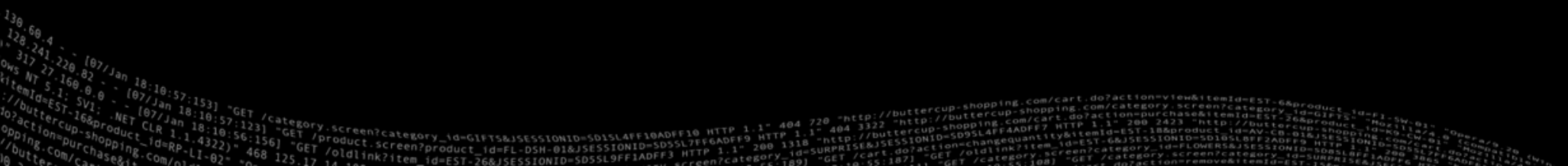
The Endless Time Travel Paradox

Rule #1

- When you are building your future prediction model by shifting data through time, you must take care to only use the shifted value as the target

Rule #2

- All exceptions to Rule #1 are basically wrong.
- If you add a KPI to ITSI or field to any Splunk search that is from the future as a FEATURE to a future prediction model , you will get amazing results. **And your model will fail from paradox.**



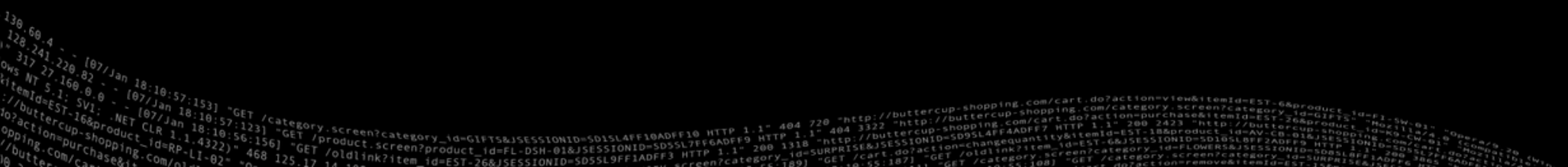
Don’t Fear the Math

“I am totally against the use of |reverse!”

- Assuming you want to shift 7 days , and every row is a day

```
| streamstats window=7 current=f first(*) as *FromNow
| rename ValueFromNow AS ValueFromTheFuture
| rename *FromNow AS *
| eval _time=strptime(_time,"%Y-%m-%d")+(24*60*60*7)
```

- That last line is a doozy. We are shifting 24 hours * 60 minutes * 60 seconds * 7 days. In ITSI this will more commonly be
  - `| eval _time=strptime(_time,"%Y-%m-%d")+(60*5)`



Why Didn't You Just Use the |predict command?

English Kind of Sucks….

predict | prɪ'dɪkt |

verb *[with object]*

say or estimate that (a specified thing) will happen in the future or will be a consequence of something: *it is too early to predict a result* | *[with clause] : he predicts that the trend will continue* | (as adjective **predicted**) *: the predicted growth in road traffic.*

forecast | 'fɔːkɑːst |

verb (past and past participle **forecast** or **forecasted**) *[with object]*

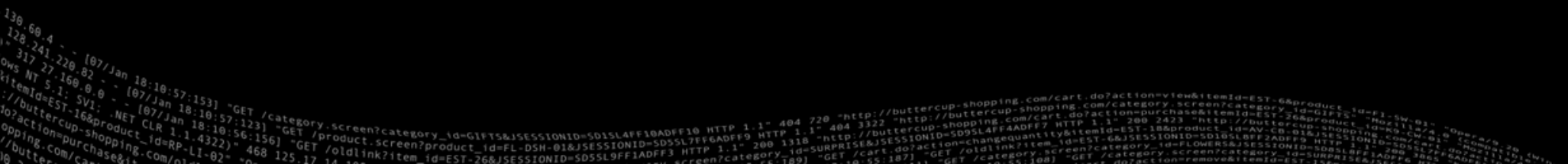
predict or estimate (a future event or trend): *rain is forecast for Scotland* | *[with object and infinitive] : coal consumption in Europe is forecast to increase.*

| predict command is a forecast!

| predict command is a forecast!

| predict command is a forecast!

| predict command is a forecast!



splunk> .conf18

ITSI PA / MLTK Predict Numeric Field vs. a Forecast

predict | prɪ'dɪkt |

verb *[with object]*

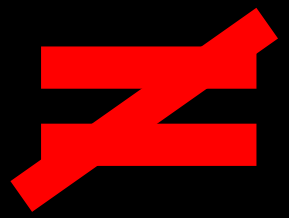
say or estimate that (a specified thing) will happen in the future or will be a consequence of something: *it is too early to predict a result* | *[with clause] : he predicts that the trend will continue* | (as adjective **predicted**) *: the predicted growth in road traffic.*

forecast | 'fɔːkɑːst |

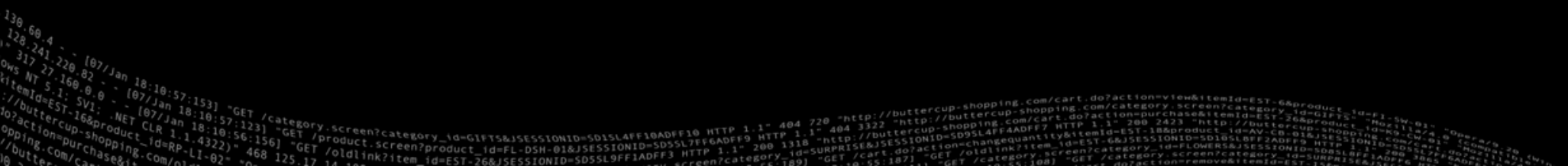
verb (past and past participle **forecast** or **forecasted**) *[with object]*

predict or estimate (a future event or trend): *rain is forecast for Scotland* | *[with object and infinitive] : coal consumption in Europe is forecast to increase.*

The Splunk stock is influenced by interest rates, global economic conditions, road map, CFO's blood pressure, density of CEO's beard, AND seasonality…



The Splunk stock is cyclical, and every July stock price in the future will look like the July stock in the past +/- trending.



splunk> .conf18

ITSI PA / MLTK Predict Numeric Field vs. a Forecast

predict | prɪ'dɪkt |

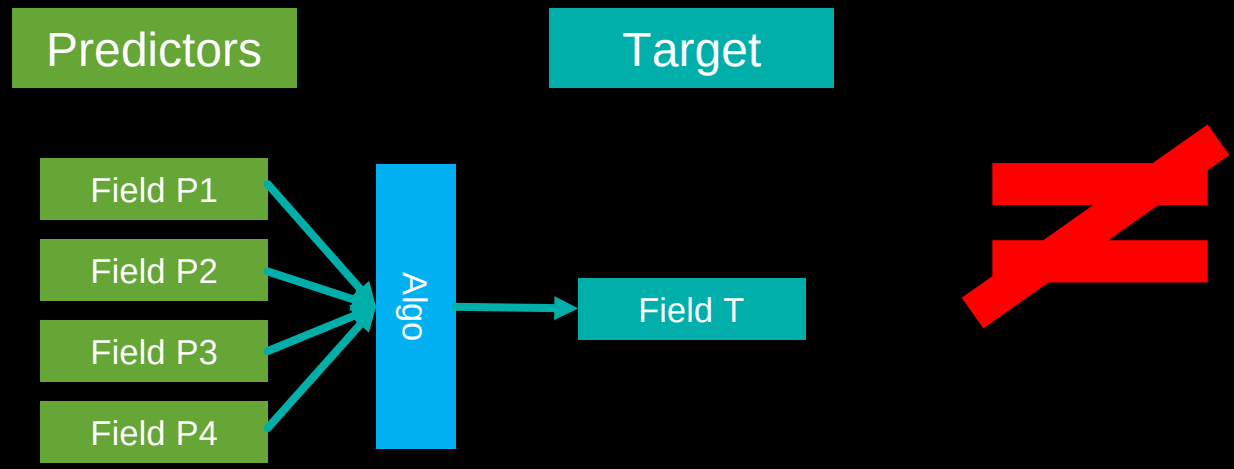
verb *[with object]*

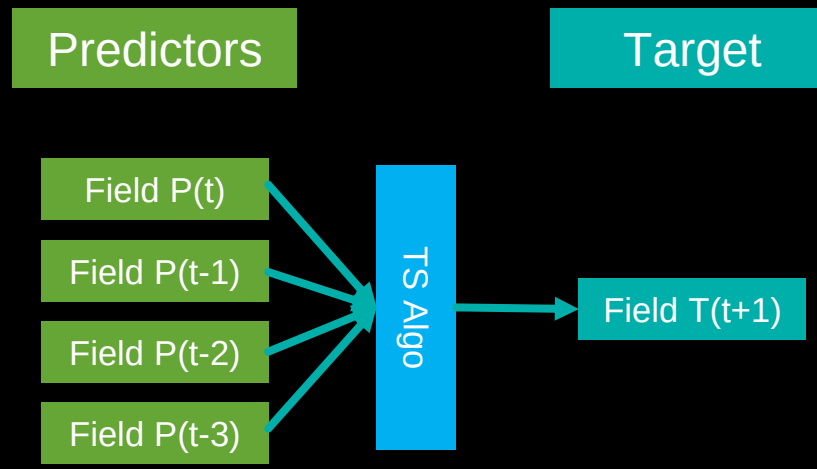
say or estimate that (a specified thing) will happen in the future or will be a consequence of something: *it is too early to predict a result* | *[with clause] : he predicts that the trend will continue* | (as adjective **predicted**) *: the predicted growth in road traffic.*

forecast | 'fɔːkɑːst |

verb (past and past participle **forecast** or **forecasted**) *[with object]*

predict or estimate (a future event or trend): *rain is forecast for Scotland* | *[with object and infinitive] : coal consumption in Europe is forecast to increase.*





splunk> .conf18

Transunion and Time Traveling Delorean

Session IT1396

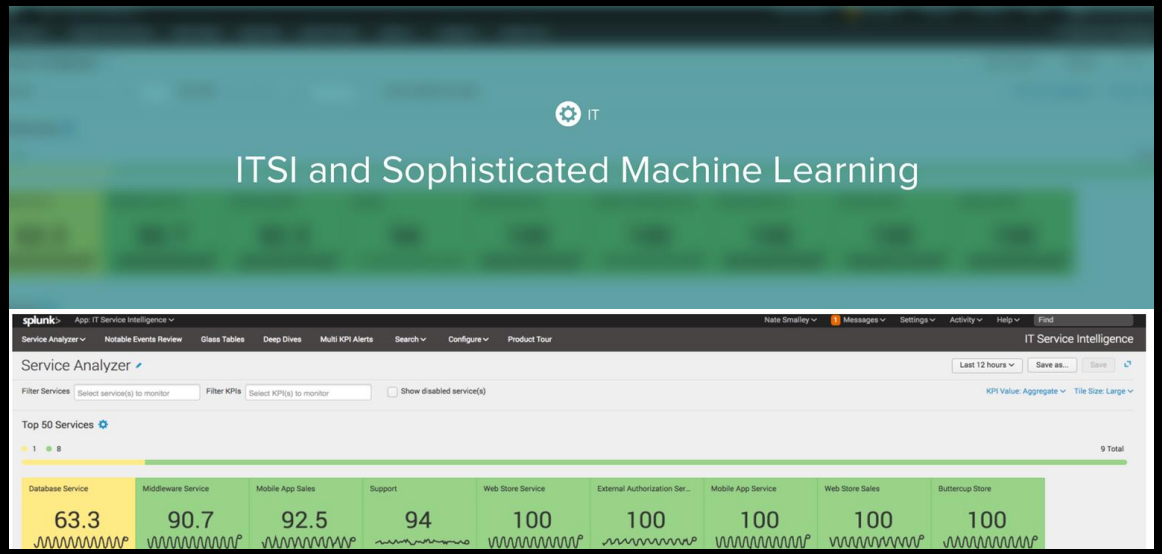
Wednesday, October 3rd, 2018
3:15 PM-4:00 PM

Resources

How-To Blogs at Your Disposal

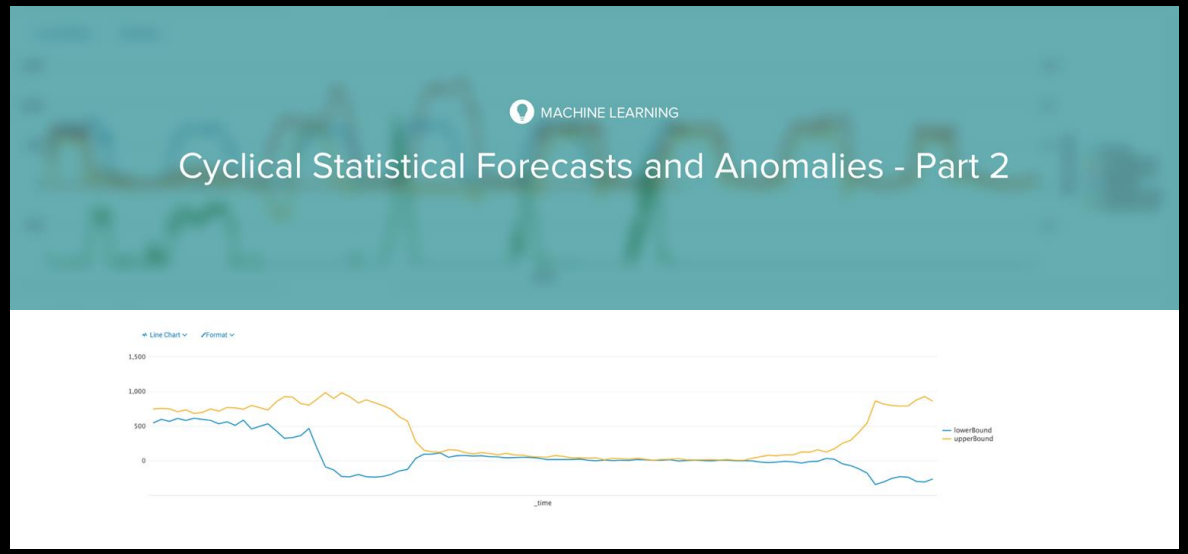
Predict

- ITSI and Sophisticated Machine Learning



Forecast

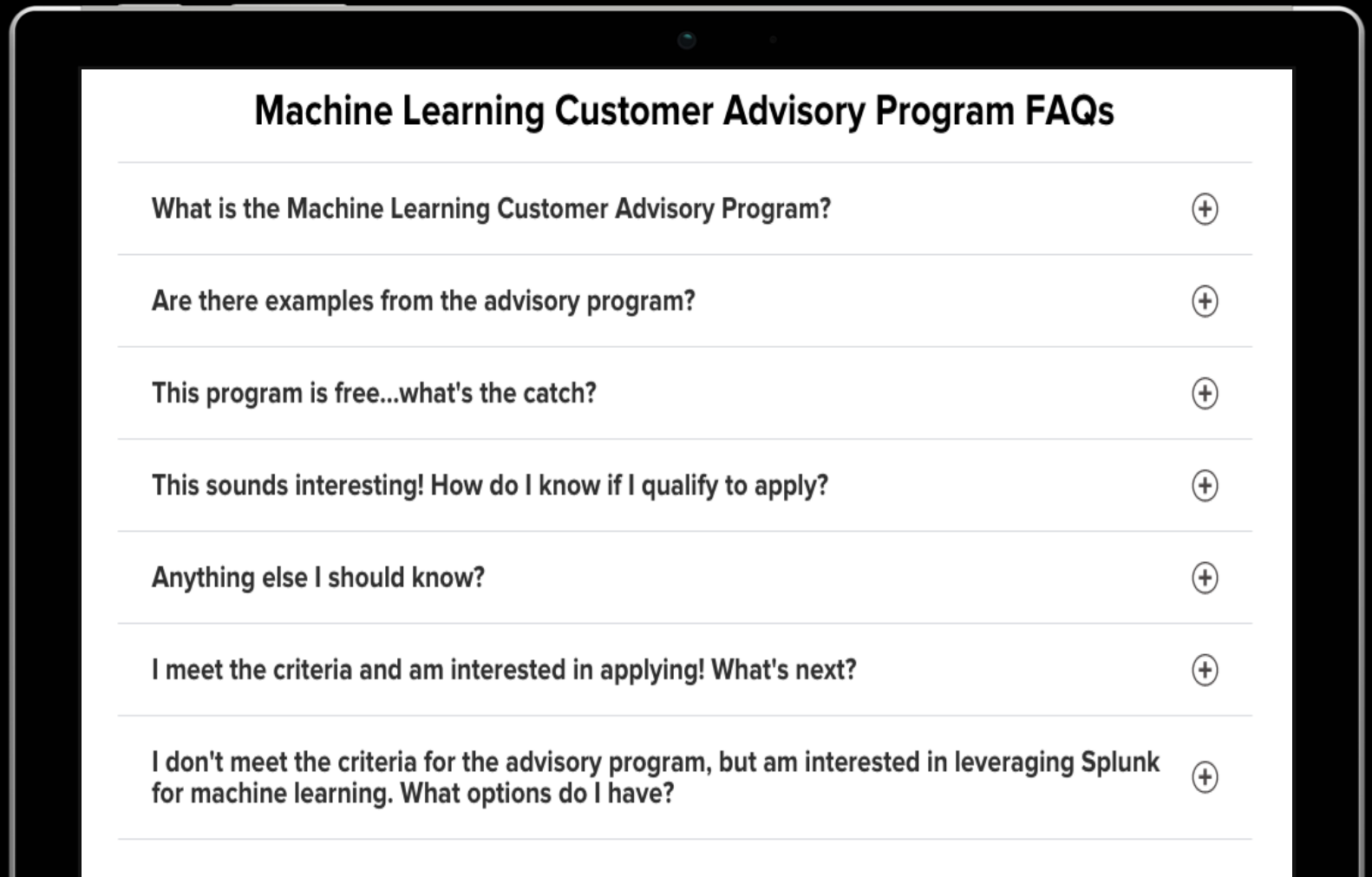
- Statistical Anomalies and Forecasts (Parts 1,2,3)



splunk> .conf18

What is the ML Advisory Program?

Partners a Splunk Data Science Resource to Help Operationalize a ML Use Case



- Early access to new and enhanced MLTK features
- Opportunities to shape the development of the product
- Assistance in operationalizing a production quality ML model

splunk> .conf18

Thank You!

Questions?

splunk> .conf18