Do more with your Data: Splunk Machine Learning

September | 2019

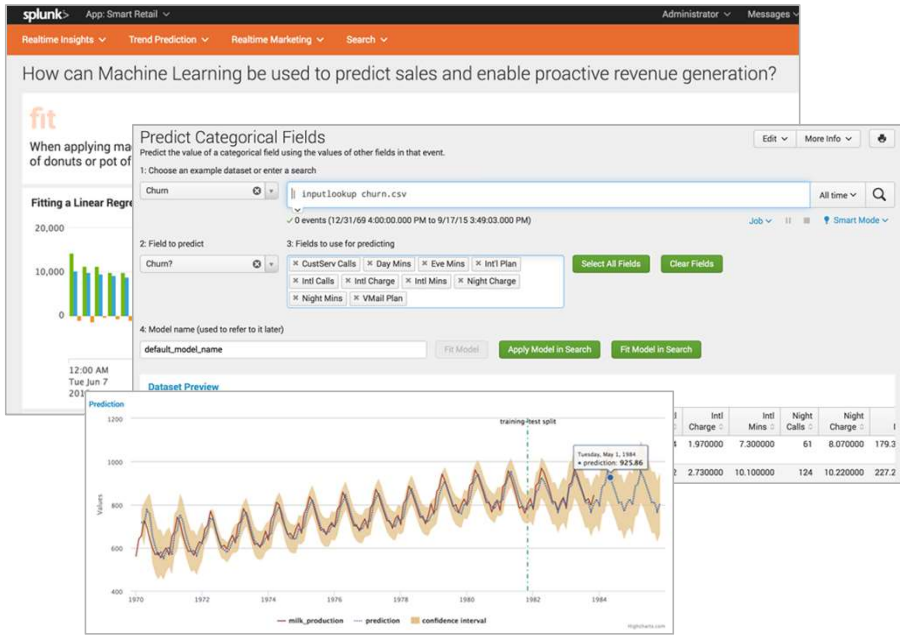
IndyPy User Group

David Muegge

Splunk Machine Learning Toolkit (MLTK)

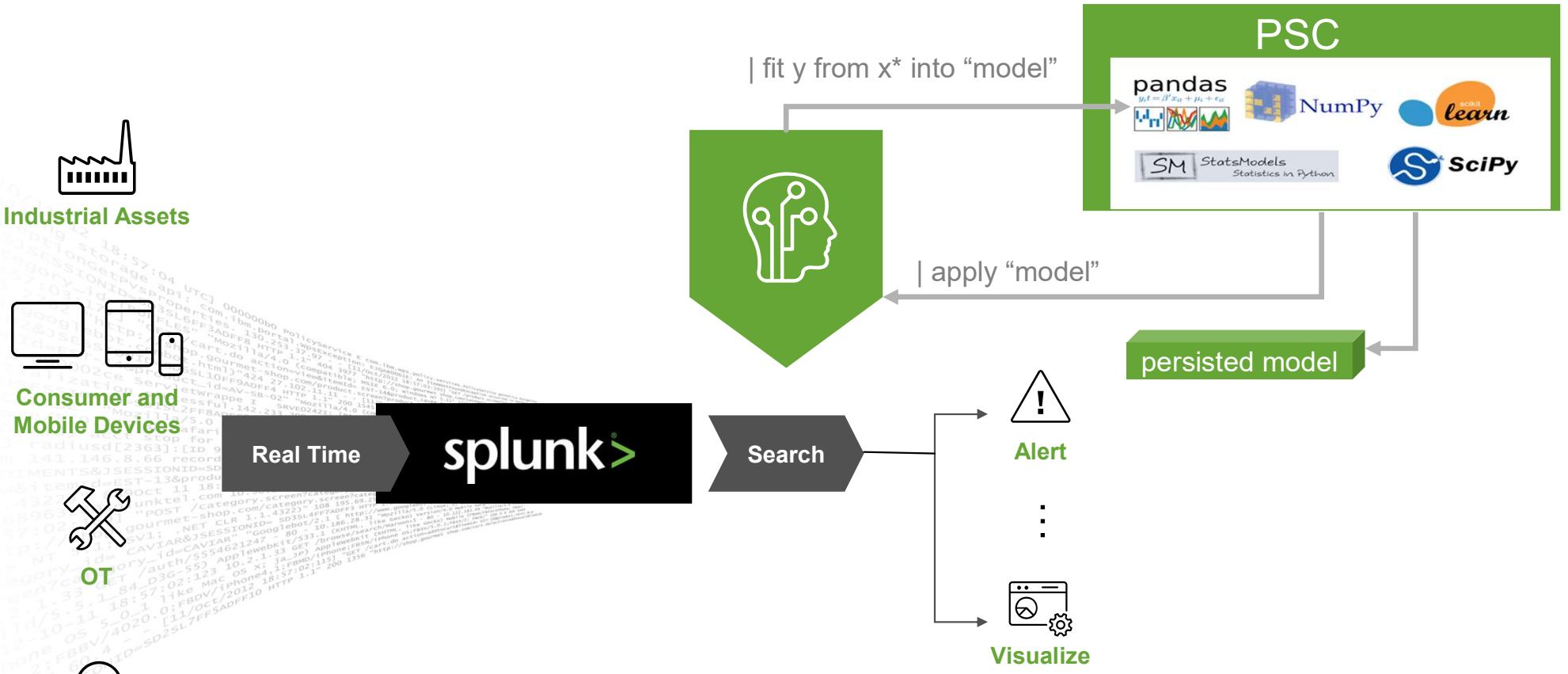
Build custom analytics for any use case on the Splunk data platform

- **Experiments and Assistants:** Guided model building, testing, and deployment for common objectives
- **Showcases:** Interactive examples for typical IT, security, business, and IoT use cases
- **Algorithms:** 80+ standard algorithms out of the box (supervised and unsupervised)
- **ML Commands:** New SPL commands to fit, test, score and operationalize models
- **ML-SPL API:** Extensibility to easily import any algorithm (proprietary / open source)
- **Python for Scientific Computing Library:** Access to 300+ open source algorithms
- **Apache Spark MLLib:** Support large scale model training via Spark Add-on for MLTK (LAR)
- **Tensorflow Container:** Supports NN and GPU accelerated ML
- **Github Community:** Share or import algorithms

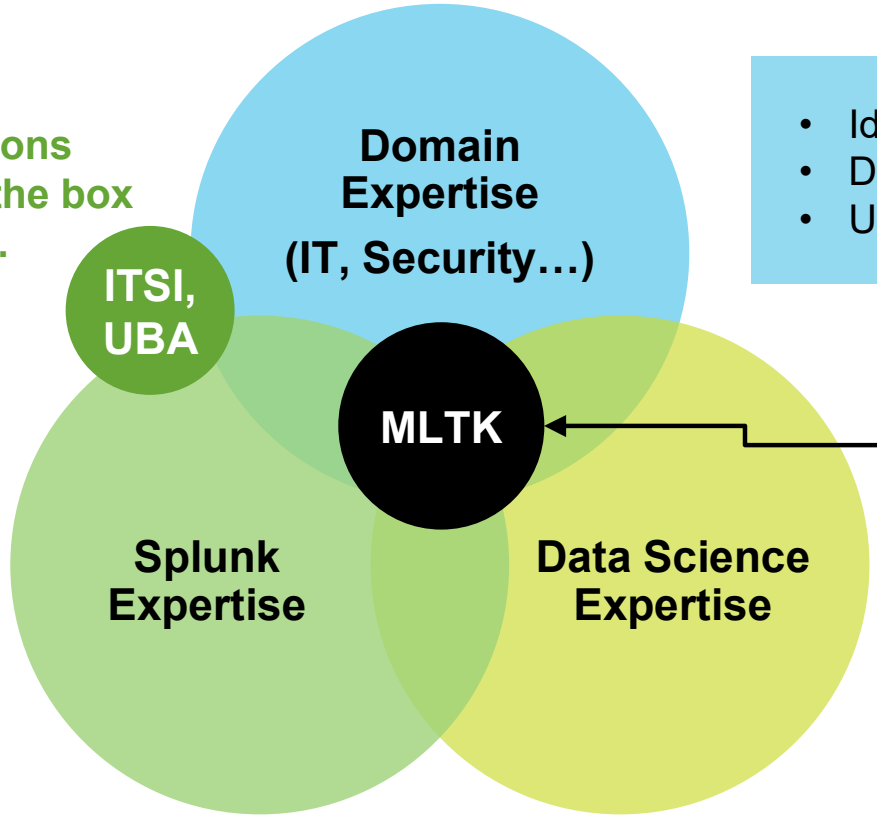


128.241.220.82 [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://butter-
cup-shopping.com/category.screen?category_id=GIFTS" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 317 27.160.0.0 [07/Jan 18:10:56:156] "
GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=pur-
chase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.100 8[786fa 18:10:56:147]

MLTK - Python for Scientific Computing



Skill Areas for Machine Learning at Splunk



Premium solutions provide out of the box ML capabilities.

- Identify use cases
- Drive decisions
- Understanding of business impact

- Searching
- Reporting
- Alerting
- Workflow

Splunk ML Toolkit facilitates and simplifies via examples & guidance

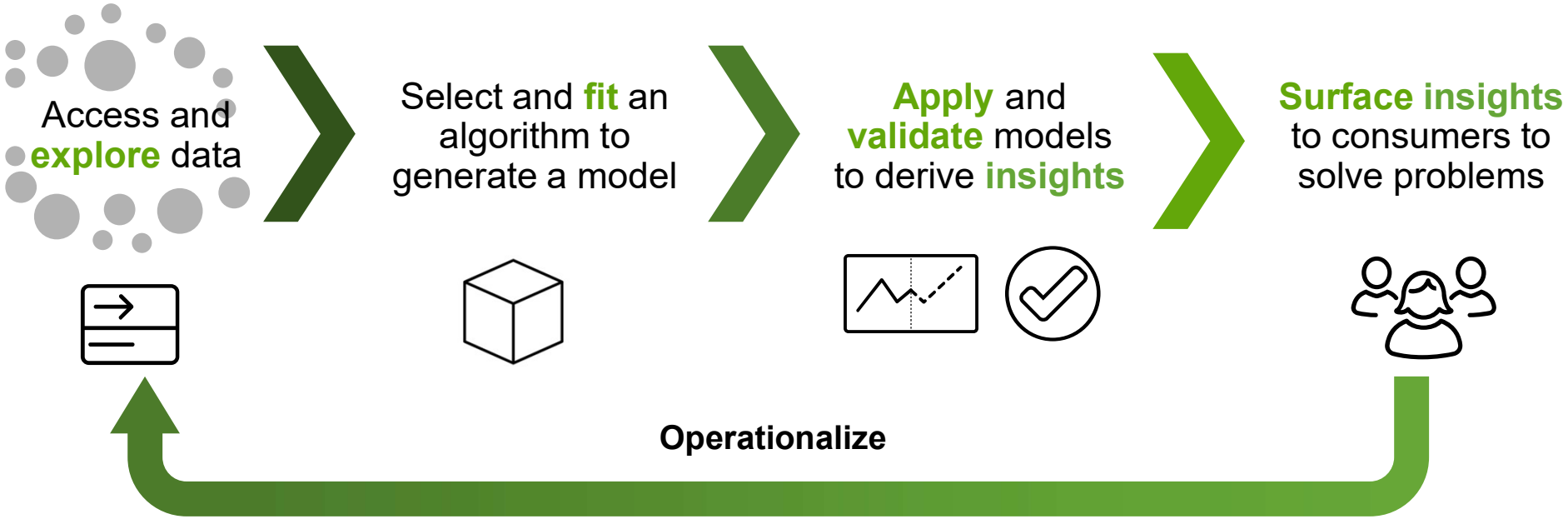
- Statistics/math background
- Algorithm selection
- Model building

128.241.220.82 [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://butter-
cup-shopping.com/category.screen?category_id=GIFTS" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 317 27.160.0.0 [07/Jan 18:10:56:156] "
GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=pur-
chase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.100 0[786fa 18:10:56:147]

Splunk helps answer questions with AI and ML

Identify a Problem: <Stuff in the world> requires big time and money investment.

Build a Solution: Build ML model to forecast <possible incidents>, act preemptively and continuously learn.



128.241.220.82 [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://butter-
cup-shopping.com/category.screen?category_id=GIFTS" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 317 27.160.0.0 [07/Jan 18:10:56:156] "
GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=pur-
chase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17.14.100 0[786fa 18:10:56:147]

Demo

Splunk MLTK creates value for a range of users

A powerful data science tool to raise meaningful insights to business consumers

Data Scientists build sophisticated machine learning models to generate insights for business consumers

Citizen Data Scientists rely on guided assistants to apply machine learning to their questions

Developers build on top of Splunk with Machine Learning as one tool to solve problems, answer questions, and surface insights

Business users, executives, and other applications consume insights raised in dashboards and visualizations to take action

Resources

- MLTK User Documentation - https://docs.splunk.com/Documentation/MLApp/4.2.0/User/About
- MLTK API Documentation - https://docs.splunk.com/Documentation/MLApp/4.2.0/API/Introduction
- Splunk Machine Learning Blog - https://www.splunk.com/blog/category/machine-learning.html
- Splunk Machine Learning YouTube Playlist - https://www.youtube.com/playlist?list=PLxkFdMSHYh3Q1jwpgJJ0ZSnRzZIx2c_KM
- Splunk Algorithm Repository - https://github.com/splunk/mltk-algo-contrib
- Splunk .conf Online - https://conf.splunk.com/watch/conf-online.html?#/

Thank You.