Machine Learning @ Splunk 2019

The Splunk Machine Learning Toolkit in Action

Iman Makaremi & Harsh Keswani
Machine Learning PM | Splunk
Iman Makaremi
Product Manager, ML & AI, Splunk

Harsh Keswani
Product Manager, ML & AI, Splunk
Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans 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 may differ materially. 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, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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 functionalities described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Turn Data Into Doing, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk Inc. All rights reserved.
Agenda

.conf Talk Analysis
ML at Splunk
MLTK in Action
What’s New?
Talk Data Analysis

MLTK Impact in 2019 .conf Talks
Talks per Sessions Track

- Foundations/Platform: 39.2%
- Security, Compliance: 23.5%
- Internet of Things: 19.6%
- IT Operations: 13.7%
- Business Analytics: 3.9%
MLTK Talks Per Product Category

- Splunk Enterprise
  - Security: 13.9%
  - IT Service Intelligence: 12.5%
- Splunk Cloud: 6.9%
- Splunk for Industrial IoT: 2.8%
- Splunk Enterprise: 58.3%
Talks Per ML Use Case

- Outlier Detection: 50.0%
- Recommendation: 4.3%
- Other: 8.7%
- Forecasting: 8.7%
- Clustering: 13.0%
- Classification: 10.9%
- Other: 8.7%
machine learning
anomaly detection
use splunk
machine learning toolkit
predictive maintenance
remote work
use case
real world
machine learning

anomaly detection

user experience
MLTK?!
What?

Splunk has a Machine Learning Toolkit App!

- What is Splunkbase
- What is the App
- Where can I go to learn more
Machine Learning Process

Collect Data

Deploy

Evaluate

Clean / Transform

Explore / Visualize

Model
Machine Learning Process with Splunk
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.

- **Access and explore data**
- **Select and fit an algorithm to generate a model**
- **Apply and validate models to derive insights**
- **Surface insights to consumers to solve problems**

**Operationalize**
MLTK Delivers Easy-to-Use Outcome Assistants

Clear Workflow

Easily Readable Summary

Interactive Customizations

Visualizations

Easy Automation to put ML into Production
What is the ML Advisory Program?

Complimentary support of Splunk data science resources to help build a ML use case resulting in a public reference

- Early access to new and enhanced Machine Learning features
- Opportunity to shape the development of the product
- Complimentary assistance in operationalizing a production quality ML model
ML Advisory Customers

- T-Mobile
- Siemens
- Intel
- StubHub
- TransUnion
- Ministry of Israel
- Honda
- BMW
MLTK in Action
Talks Per ML Use Case

- **Outlier Detection**: 50.0%
- **Recommendation**: 4.3%
- **Classification**: 10.9%
- **Clustering**: 13.0%
- **Forecasting**: 8.7%
- **Other**: 8.7%
Outlier Detection
Anomaly Detection
Threat Detection
Fraud Detection
Intrusion Detection
Threat Hunting
Outage Prediction
Identifying service-impacting events across the deployed enterprise applications.

---

FN1366 - Enhanced Anomaly Detection: Join T-Mobile and Splunk as we Deep Dive an Enterprise-IT Operational Use Case

Wednesday, October 23, 01:45 PM - 02:30 PM
Iman Makaremi, Principal Product Manager – Machine Learning and AI, Splunk
Scott Garcia, MTS - Member Technical Staff, T-Mobile
Automatic monitoring of performance KPIs and anomaly discovery within minutes.

IT1171 - Accelerate your ability to sniff out application exceptions and detect outliers in performance KPIs

Tuesday, October 22, 04:15 PM - 05:00 PM
Eurus Kim, Staff ML Architect, Splunk
PJ Pokhrel, Performance Engineer, Stubhub
Steve Veio, Performance OPS Manager, StubHub
Insurance Fraud Detection

SEC1904 - The Duck Test: Leverage Machine Learning to Remediate Fraud in Huge Datasets

Thursday, October 24, 01:00 PM - 01:45 PM
Matthew Harper, Director, Cyber Crime Prevention, Aflac
Datacenter security monitoring for hacker detection.


Thursday, October 24, 11:45 AM - 12:30 PM

Oliver Kollenberg, Security Consultant, Siemens AG
Philipp Drieger, Staff Machine Learning Architect, Splunk
MLTK Offers

1. Numeric Outlier Detection Assistant
2. Smart Outlier Detection Assistant
3. Custom ML
Numeric Outlier Detection Assistant
Smart Outlier Detection Assistant
Smart Outlier Detection Assistant
Custom ML

• Custom ML Outlier Detection Blog (link)

• Add Custom ML Alg (link)
Forecasting
Predict future outages by forecasting congestion rates of cell towers.

IT1722 - Predict Real World Outage using Splunk MLTK

Wednesday, October 23, 12:30 PM - 01:15 PM

Vijay Veggalam, Member of Technical Staff, T-Mobile
Gintaras Gaigalas, Sr. RF Engineer, T-Mobile
Eliminate out-of-disk outages by forecasting disk usage and creating what-if scenarios.

FN1137 - Forecasting Disk Usage with Machine Learning – So easy, even a cave-person can do it!

Tuesday, October 22, 01:45 PM - 02:30 PM
Steve Koelpin, Splunk Advisor, TransUnion
Alicia Dale, Site Reliability Engineer, TransUnion
MLTK Offers

1. Time Series Forecasting Assistant
2. Smart Forecasting Assistant
3. Custom ML
Time Series Forecasting Assistant
Smart Forecasting Assistant
Clustering
Predict future outages by forecasting congestion rates of cell towers.

IT1722 - Predict Real World Outage using Splunk MLTK

Wednesday, October 23, 12:30 PM - 01:15 PM
Vijay Veggalam, Member of Technical Staff, T-Mobile
Gintaras Gaigalas, Sr. RF Engineer, T-Mobile
Insurance Fraud Detection

SEC1904 - The Duck Test: Leverage Machine Learning to Remediate Fraud in Huge Datasets

Thursday, October 24, 01:00 PM - 01:45 PM
Matthew Harper, Director, Cyber Crime Prevention, Aflac
MLTK Offers

1. Cluster Numeric Events Assistant
2. Custom ML
Cluster Numeric Events Assistant
What’s New?
What’s New?

MLTK 5.0
New smart assistants for forecasting and outlier detection, new algorithms, UI refresh, more examples

PSC 2.0
Upgrade to Python 3.7 for MLTK 5.0 and later versions. Networkx Library Support

Large Scale Splunk ML PoC
Visit us in the Innovation Booth to know more!

ML on Splunk Cloud Platform
ML-SPL on new Splunk Cloud Platform (SCP), ML-APIs on SCP

TF 2.0 and PyTorch Support
MLTK Container now supports TensorFlow 2.0 and PyTorch (Only PS Offering).
How to Reach Us?
Reach out to us for feedback and suggestions

mlprogram@splunk.com
Thank You!

Go to the .conf19 mobile app to RATE THIS SESSION