Machine Learning and Data Science Hands-On

splunk>

Forward-Looking Statements

This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

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. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

splunk>

Please introduce yourself!

- Name
- Company/organisation
- Role
- Are you currently using Splunk?
- What are you interested in using Splunk for?

REGISTRATION 5 MINS

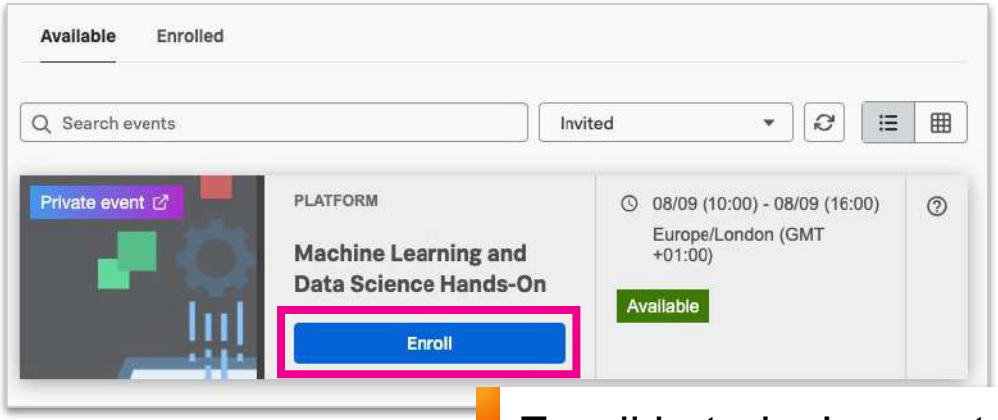
Enroll in Today's Workshop

Tasks

1. Get a splunk.com account if you don't have one yet: https://splk.it/SignUp
2. Enroll in the Splunk Show workshop event: https://show.splunk.com/event/<eventID>
3. Download the hands-on lab guide: https://splk.it/MLDS-Lab-Guide

   Contains step-by-step instructions for all of today's exercises!
4. Download a copy of today's slide deck: https://splk.it/MLDS-Attendee

Goal

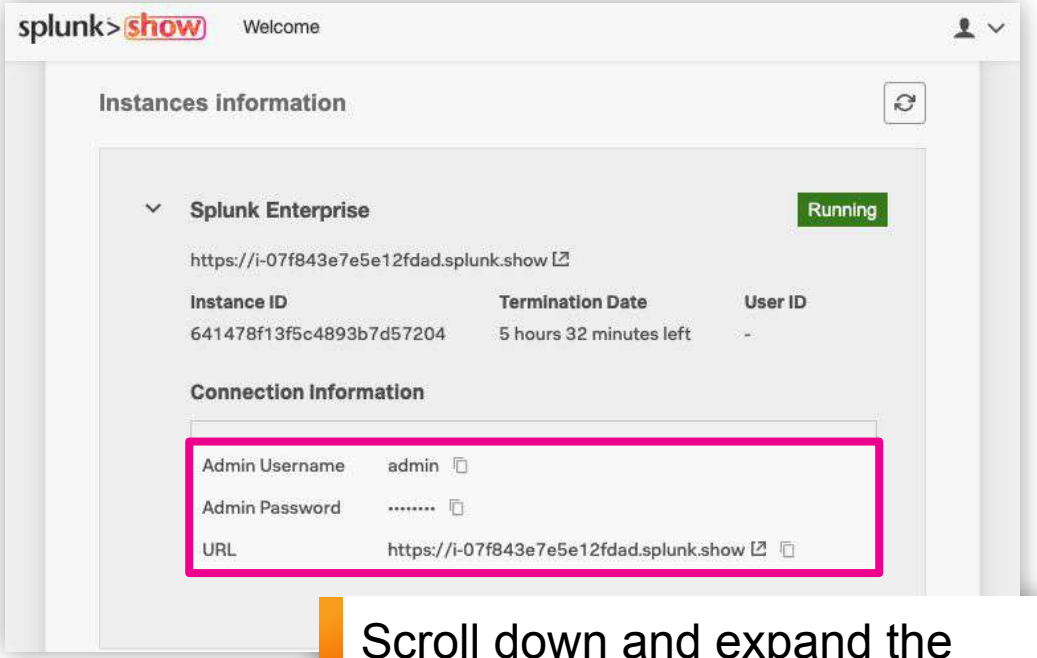


Enroll in today's event

splunk>

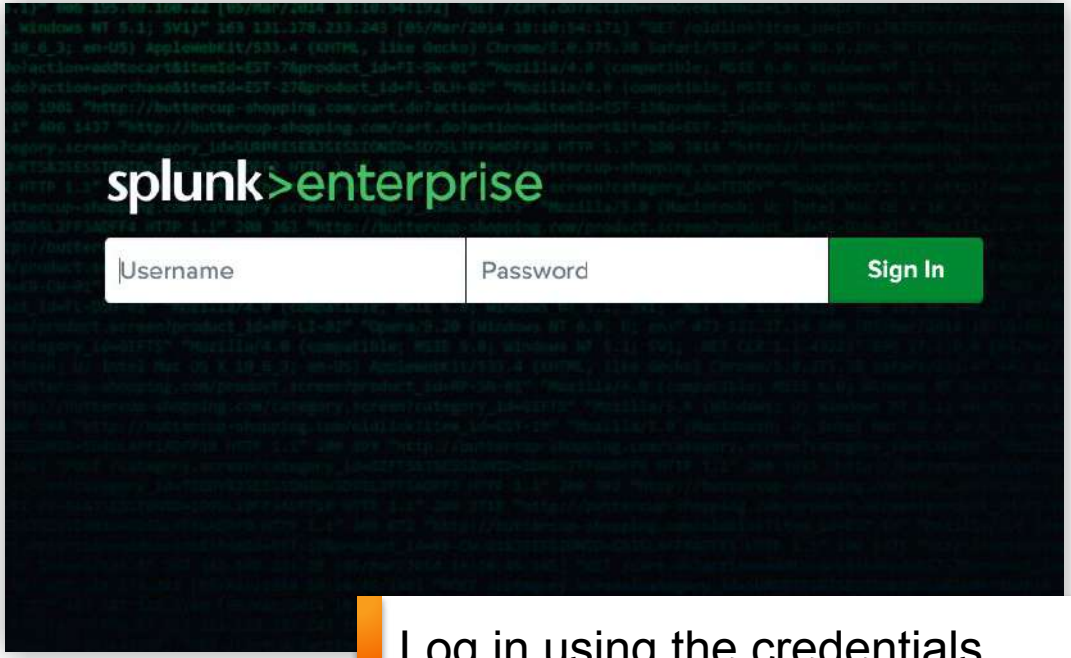
Log in to Splunk

Locate your instance URL and credentials in the Splunk Show event https://show.splunk.com



Scroll down and expand the **Instances information** section to view your login details

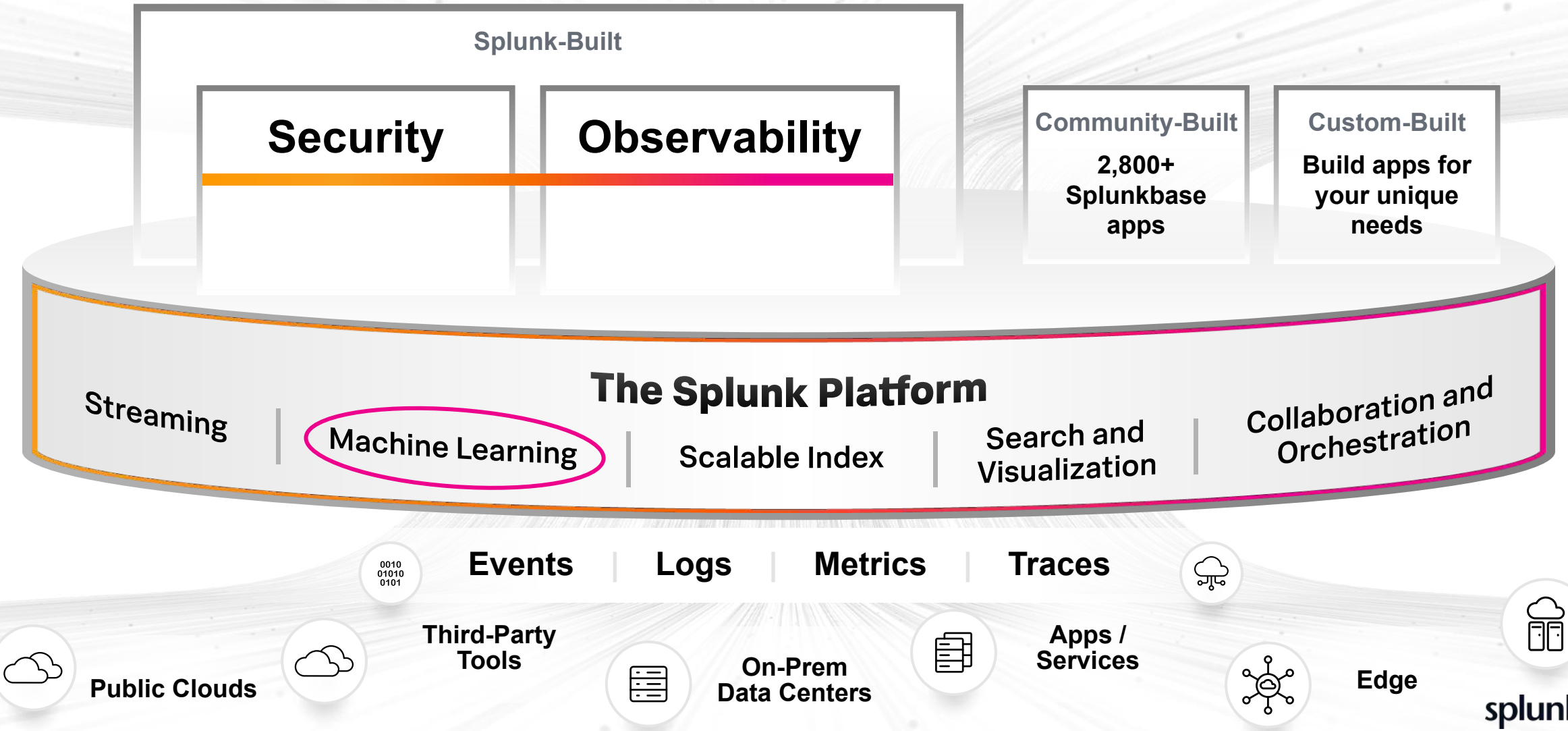
Log in to your Splunk instance



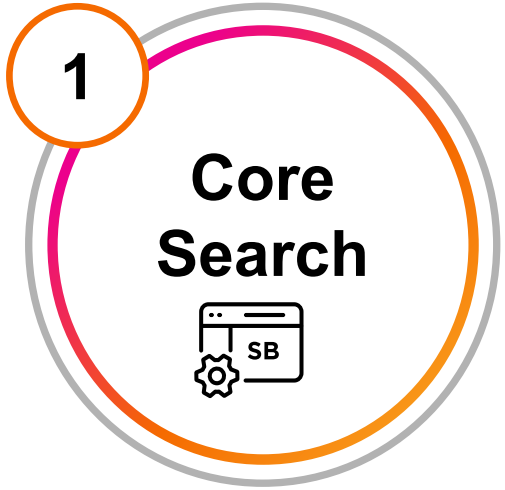
Log in using the credentials from Splunk Show

splunk>

The Unified Security and Observability Platform

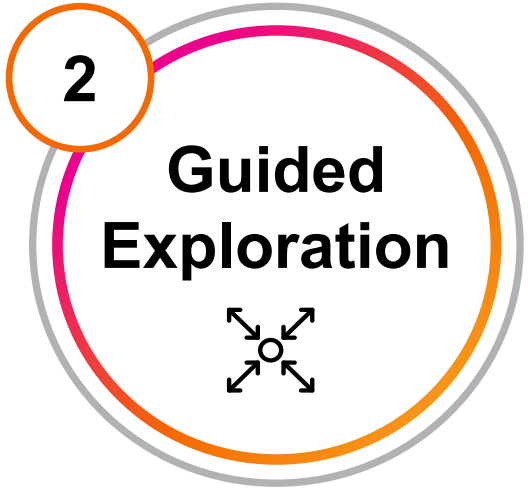


Diverse Capabilities Across the Splunk Portfolio



Embedded

Included in the powerful search capabilities of our products, plus our apps extend the core search language with ML commands

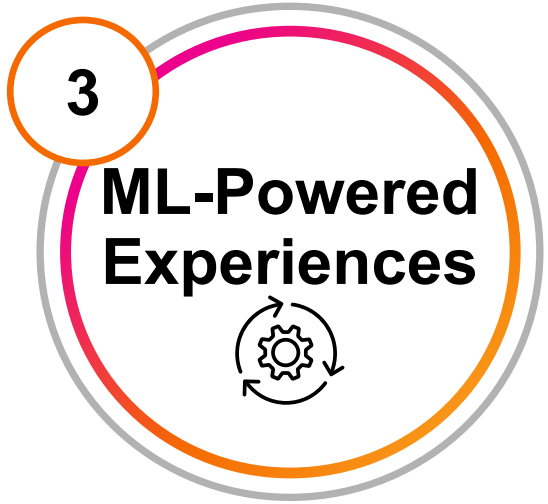


MLTK

Guided exploration for Splunk Citizen Data Scientists

Assistive Intelligence Apps

Beta ML content customized for some of the most frequent Splunk use cases



ITSI Service Insights

Predicting outages in IT Service Intelligence (ITSI) relies on ML

Enterprise Security

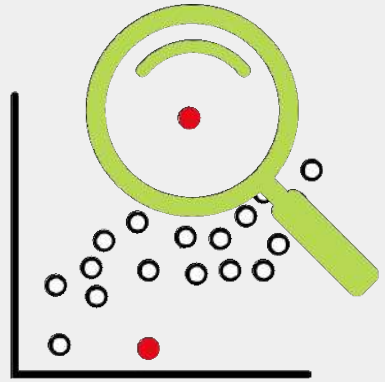
ML powers many of the detections in Enterprise Security (ES)

splunk>

Common Challenges

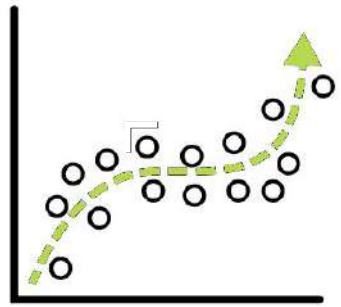
What sorts of problems do we most commonly encounter?

Anomaly Detection



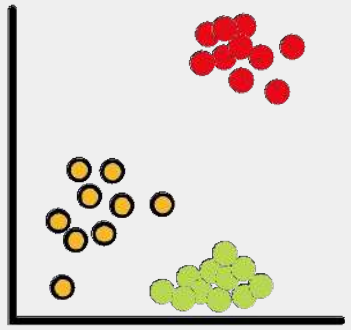
- Deviation from past behavior
- Deviation from peers
- Unusual change in features

Predictive Analytics



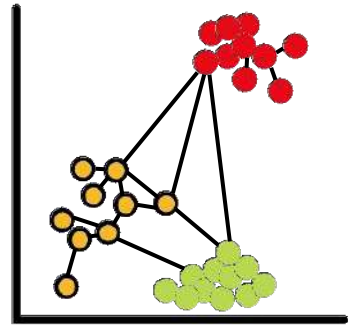
- Predict health score
- Predicting events
- Trend forecasting
- Early warning of failure

Clustering



- Identify peer groups
- Event correlation
- Reduce alert noise
- Behavioral analytics

Graph Analytics



- Most influential nodes
- Link analysis
- Community detection
- Impact analysis

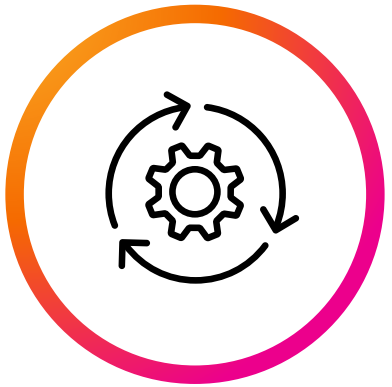
How Customers Realize Value with Advanced Analytics

3 examples from Security & Fraud to Operations to Business

Security & Fraud

Investigative Analytics for Fraud Detection, Data Science based Threat Hunting, advanced custom ML Detections

IT Operations



Large Telco Customer scales out Prophet based Forecasting Models for 100,000s of Devices

Business Analytics

Predict error patterns in automotive manufacturing from vehicle configuration with a deep neural network

splunk>

Latest Threat Research and Detections

JA3

Exploration of JA3 Embedding Space

DGA

Detect DGA domains using pretrained model in DSDL

PROC

Detect suspicious process names using a pretrained model in DSDL

DNS TXT

Detect suspicious DNS TXT records using pretrained model in DSDL

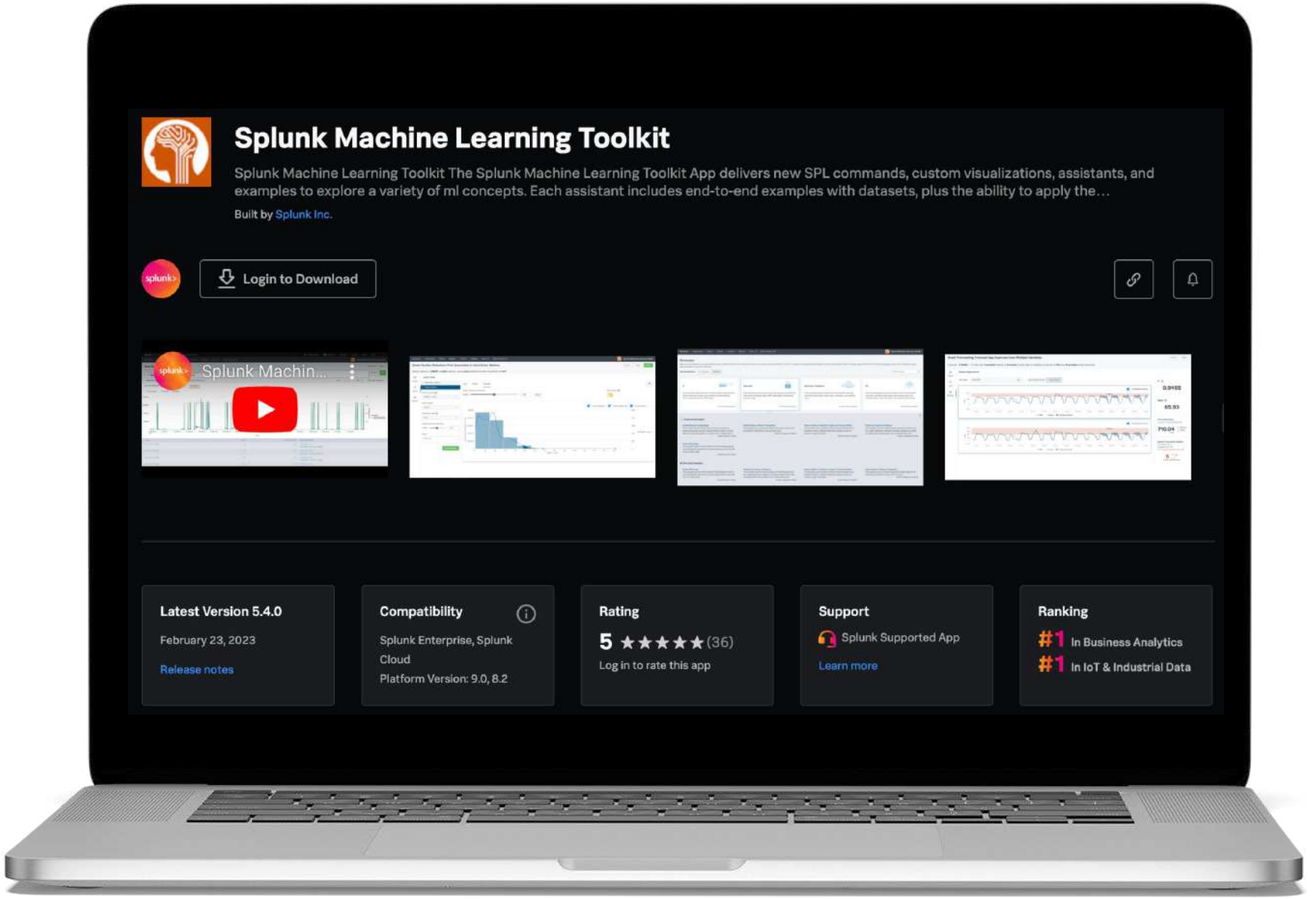
splunk>

What is the Splunk Machine Learning Toolkit (MLTK)?

splunk>

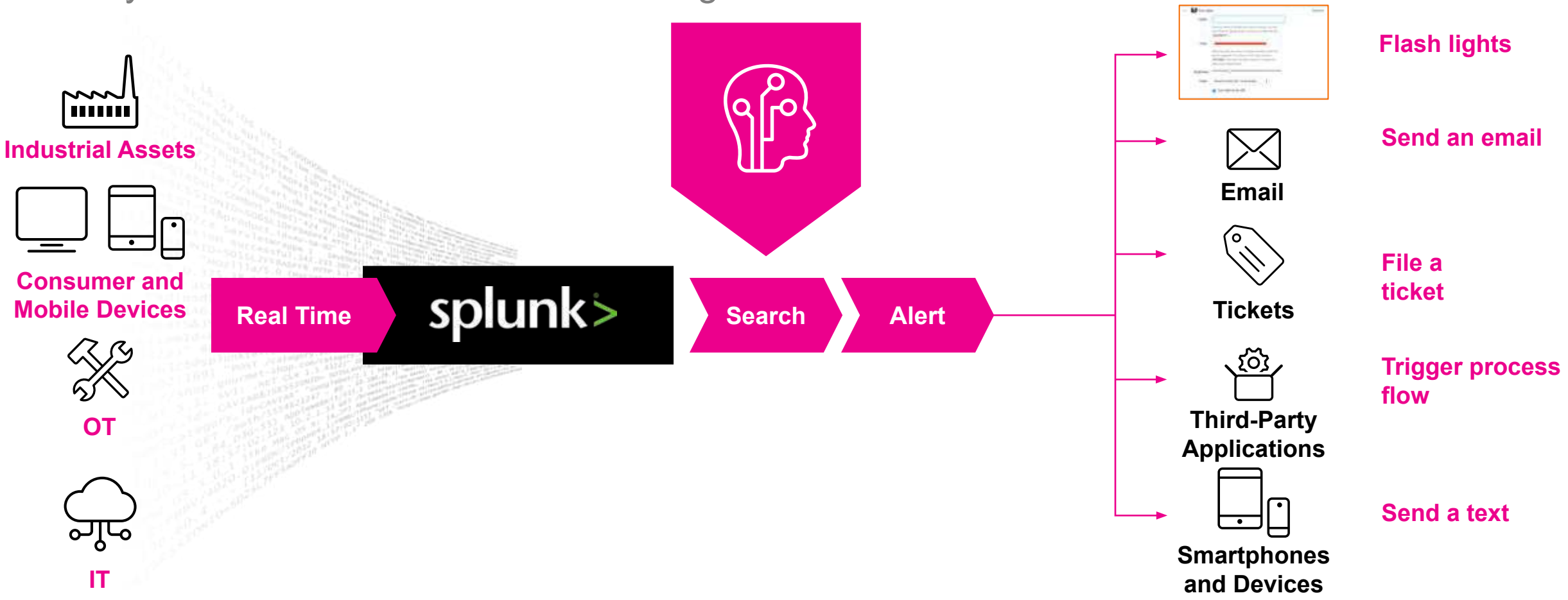
MLTK

One of the most downloaded Splunkbase apps



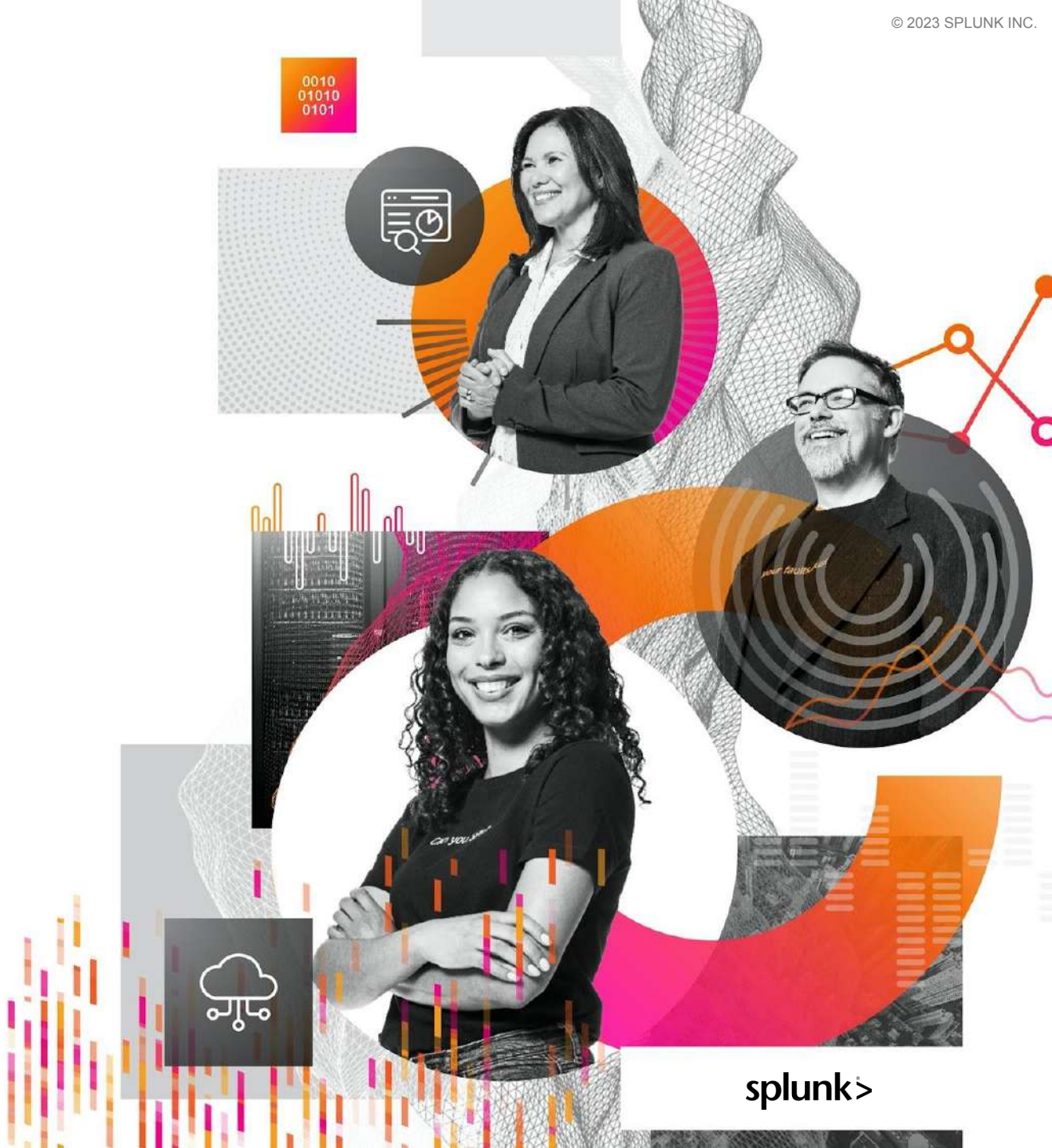
What does the MLTK provide?

Every search can use Machine Learning



splunk>

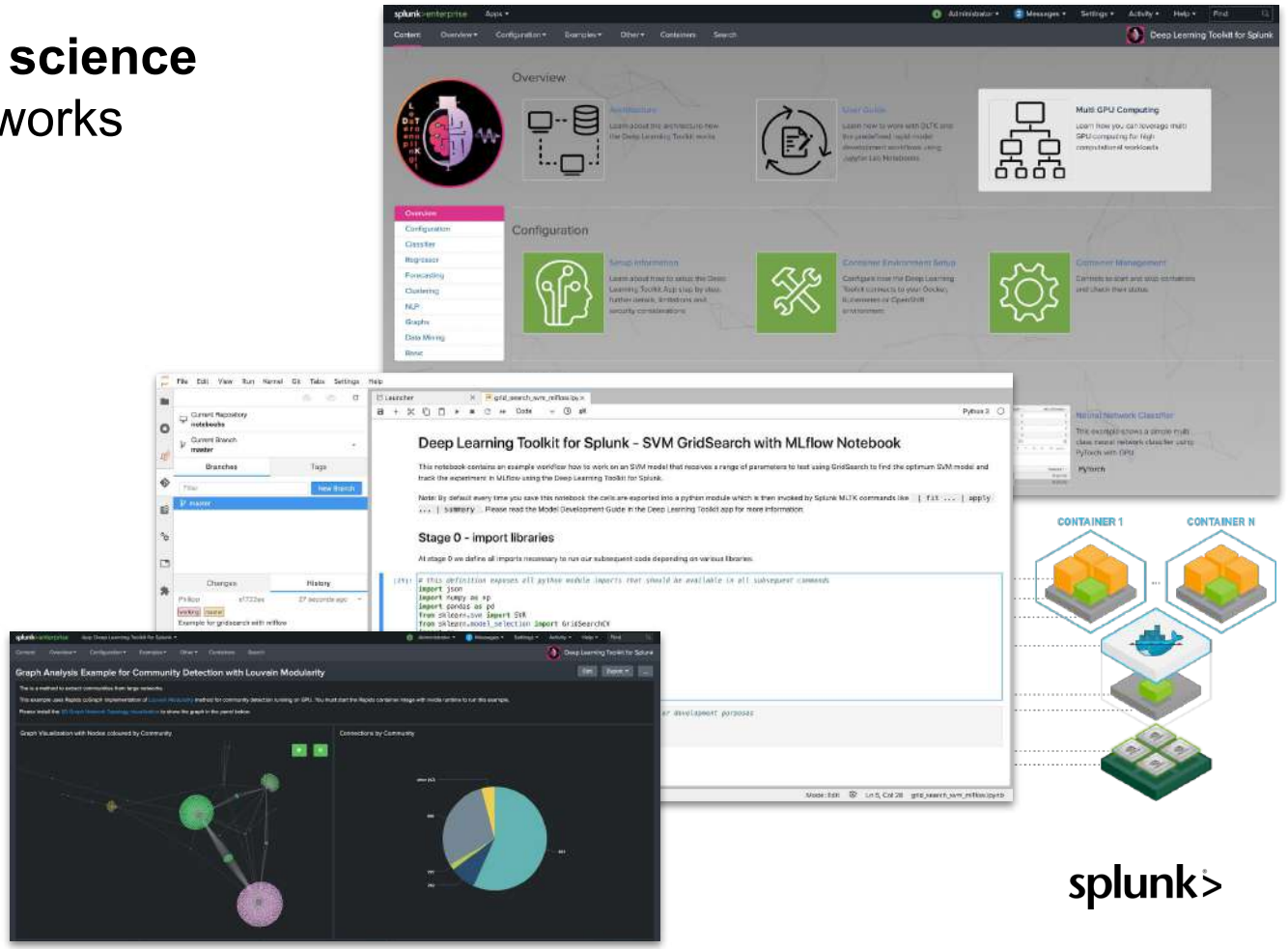
Introducing the Splunk App for Data Science and Deep Learning



Splunk App for Data Science and Deep Learning (DSDL)

Download and install for free: https://splunkbase.splunk.com/app/4607/

- **Freely available app for advanced data science projects** using any open source AI frameworks
- **Speed up** your data science projects with **GPU accelerated containers**
- **Seamlessly integrate & operationalize** your use cases with Splunk® Enterprise
- **Open source** for customization: https://github.com/splunk/splunk-mltk-container-docker

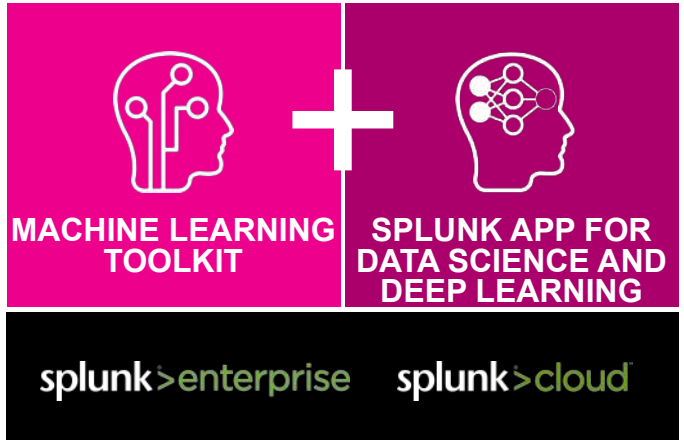


DSDL goes hand-in-hand with MLTK

Best of both worlds that help customers to extend their Splunk platform with ML

Compliments

- DSDL does not replace MLTK but complements it with additional capabilities



Builds

- DSDL builds on MLTK's API and shares the same familiar SPL syntax of commands like `fit`, `apply` and `summary` as MLTK does
- These commands can be used to operationalize advanced machine learning and deep learning workloads with Splunk

Extends

- DSDL extends MLTK's functionality by connecting to containerized external ML services customers manage for following key advantages:
  - **Access** Jupyter Notebook for data scientists to build custom models
  - **Ability** to use any state of the art python open source libraries such as TensorFlow, PyTorch, SpaCy, DASK, Rapids, Spark and more
  - **Ability** to run on GPU infrastructure for accelerated computing
  - **Offload** heavy ML workloads from splunk search heads to elastically scalable container environments such as Docker, Kubernetes or OpenShift
  - **Allow** customers to address very advanced modelling use cases that are not possible to address with MLTK

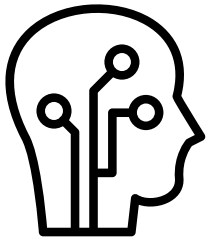
splunk>

Hands-On Workshop

Fun challenges to explore ML!

splunk>

The Splunk Platform and Machine Learning



Key Takeaways

- How to use MLTK and DSDL to embed intelligence in enterprise operations
- Focus on what you want to detect, then analyze your data to see if ML can help with the detection
- MLTK will help you with how the detection works
- The Splunk platform and MLTK provide a free path for you to leverage ML in your everyday use cases!

Additional Resources

Where can you find more information

MLTK

Download it now from Splunkbase!

DSDL

Download it now from Splunkbase!

Getting Started

- View some of our webinars
- Check out our YouTube playlist
- Check out the blog on MLTK 5.4 release
- Try out some of our starter blogs, such as Cyclical Statistical Forecasts and Anomalies, part 1
- Try our new MLTK Deep Dives

Increasing Complexity

- Try part 4 or 6 of the Cyclical Statistical Forecasts and Anomalies series
- Brush up on how MLTK works with our comprehensive documentation
- Get familiar with today's Workshop Guide

More Advanced

- The Analytics and Data Science course
- Try out part 5 of the cyclical statistical forecasts and anomalies series
- Try the ML-SPL API

splunk>

Thank You