Splunk Machine Learning Toolkit (MLTK) app Cheat Sheet

In the proud tradition of CliffNotes, SparkNotes, and Bookrags, allow us to give you the answers to the test!

Check out this handy cheat sheet of resources to get started with the MLTK app >

splunk>

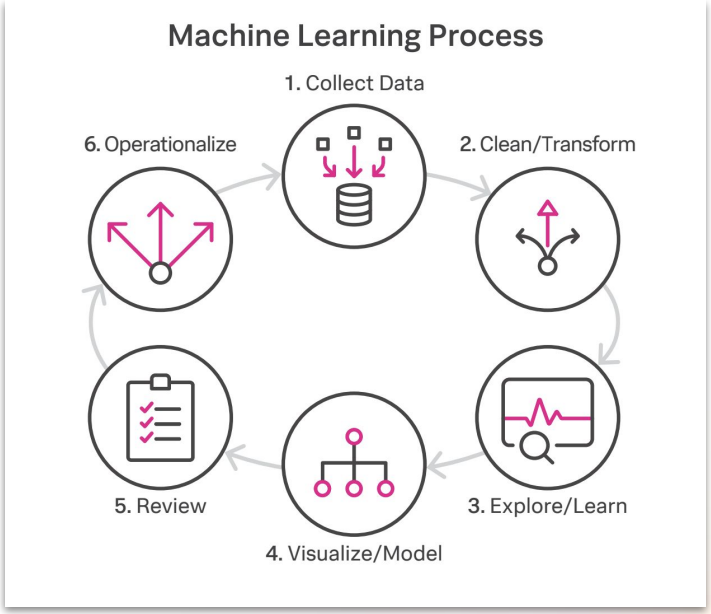
Machine Learning Toolkit 5.4

Free Splunkbase app to operationalize ML use cases within Splunk search

Designed for Splunk users at all levels

- **Supports ML-powered Splunk searches** by applying techniques like anomaly detection and predictions within search to power dashboards & insights
- **Low-code experience** to guide model building, testing, and deployment
- **Extensible out of the box** with 80+ built-in scikit-learn algorithms, and API support to plug in new runtimes

Product Brief | **Download app on Splunkbase >**



New 5.4 updates:

- Ability to upload externally pre-trained ONNX models with a simple UI, then use the model with your Splunk data with no modification to your existing workflows
- Extended user anomaly detection capabilities with a new algorithm for multivariate outlier detection

Splunk Enterprise 9.1, Splunk Cloud Platform

How to get started

MLTK Deep Dives

Get started with MLTK by using deep dives, which provide **end-to-end walkthrough guides** for how to implement specific use cases against your own data in Splunk. These offer a more **prescriptive introduction** into using ML at Splunk and will help you implement the ML search commands that ship with MLTK (learn more).

Deep Dives

- Detect user access anomalies
- Detect outliers in error message rates
- Detect outliers in server response time
- Detect network traffic anomalies
- Create a data ingest anomaly detection dashboard using ML-SPL commands

Showcase Examples

Use the MLTK Showcase to **explore machine learning concepts**. Each end-to-end example is comprised of a pre-populated use case for the Machine Learning Toolkit and each of the guided modeling Assistants.

Showcase Examples

- Smart Prediction
- Predict Numeric Fields
- Predict Categorical Fields
- Smart Outlier Detection
- Detect Numeric Outliers
- Detect Categorical Outliers
- Smart Forecasting
- Forecast Time Series
- Smart Clustering

Smart Assistants

Smart Assistants in the MLTK app offer a **guided workflow** through which you can create new Experiments. They let you **automatically apply ML models** to common use cases and frequently observed data challenges for Splunk users.

Quickly move from fitting a model on historic data to applying a model on real-time data and taking action **with little to no SPL knowledge.**

Each assistant includes end-to-end examples with datasets, plus the ability to apply the visualizations and SPL commands to your own data. Learn more >

Smart Assistants available now


Smart Forecasting Assistant


Smart Outlier Detection Assistant


Smart Clustering Assistant


Smart Prediction Assistant

splunk>

Additional MLTK Resources

- MLTK Documentation
    - Understand the Fit and Apply Commands
- Quick reference guide of ML search commands
- Machine Learning YouTube video playlist
- MLTK Answers on Community

Blogs

- Getting Started with ML at Splunk
- Machine Learning Guide: Choosing the Right Workflow