How to Extend Splunk with an AI Assistant for Pattern Recognition

Greg Olsen, PhD

SVP of Products, Falkonry

Disclaimer

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 the 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.

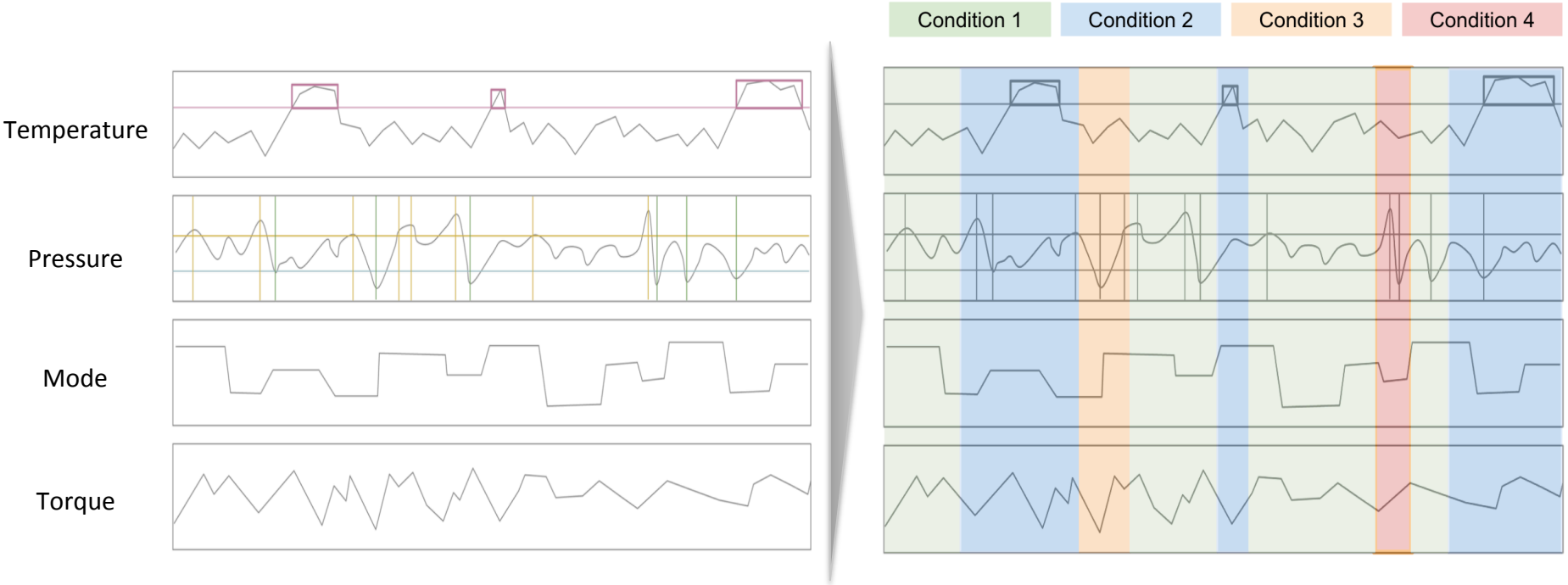
Agenda

- Why are time series data patterns interesting?
- Can pattern recognition be easy?
- What does Splunk + pattern recognition look like?

Time Series Data Patterns

splunk>

From Data to Conditions

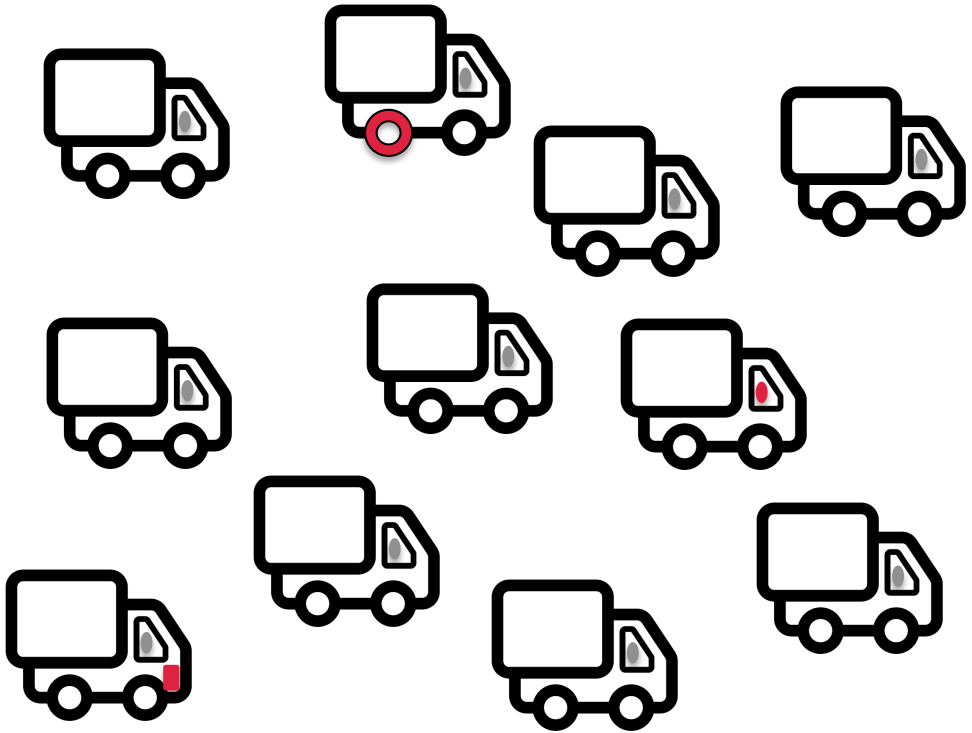


Fleets

Time Series Data

- x,y,z acceleration
- turn angle
- accelerator
- braking
- driver heart rate

Fleets



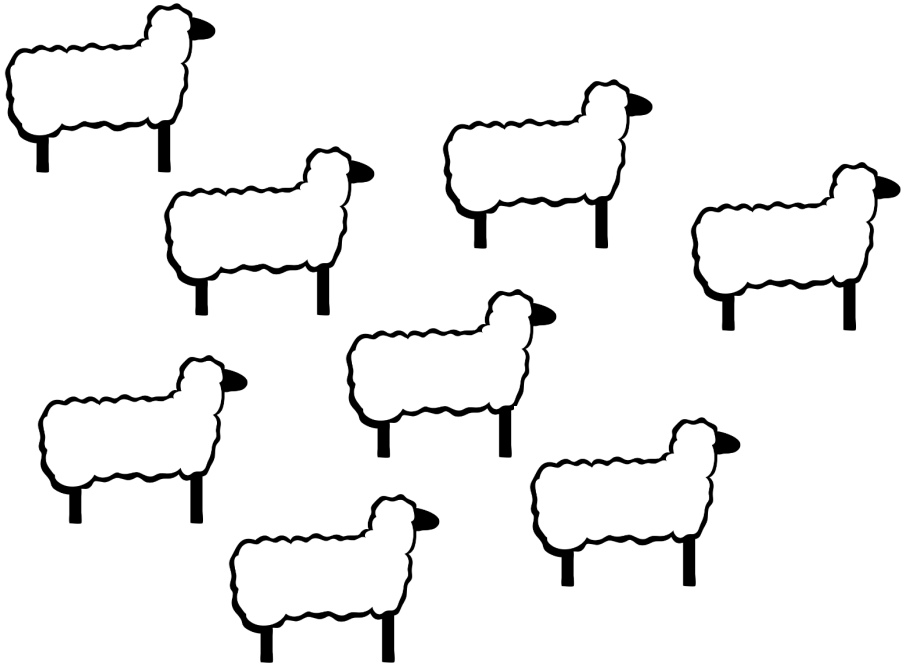
Time Series Data

- x,y,z acceleration
- turn angle
- accelerator
- braking
- driver heart rate

Conditions

- Impaired driver
- Tire problem
- Engine problem

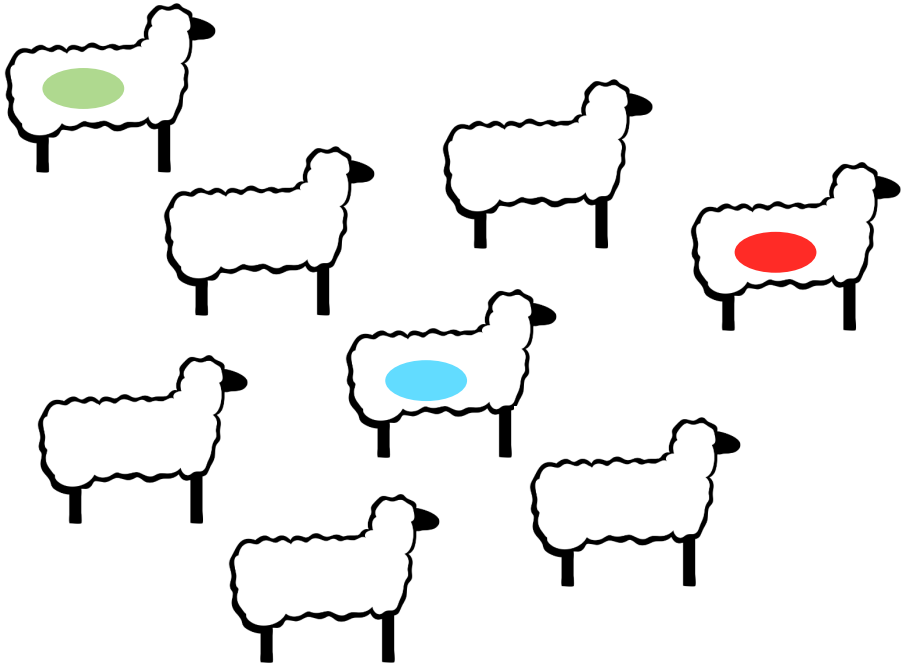
Livestock



Time Series Data

- x,y,z location
- body temperature
- heart rate

Livestock



Time Series Data

- x,y,z location
- body temperature
- heart rate

Conditions

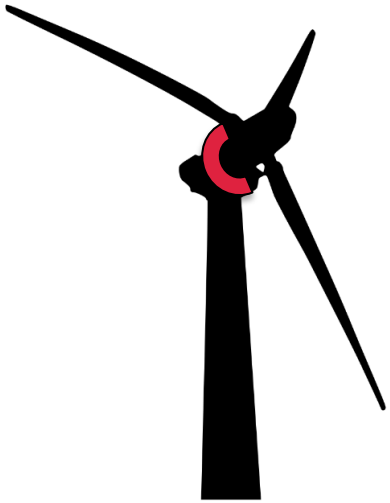
- illness
- fertility window
- pregnancy

Machine

Time Series Data

- x,y,z acceleration
- rpm
- power
- wind velocity

Machine



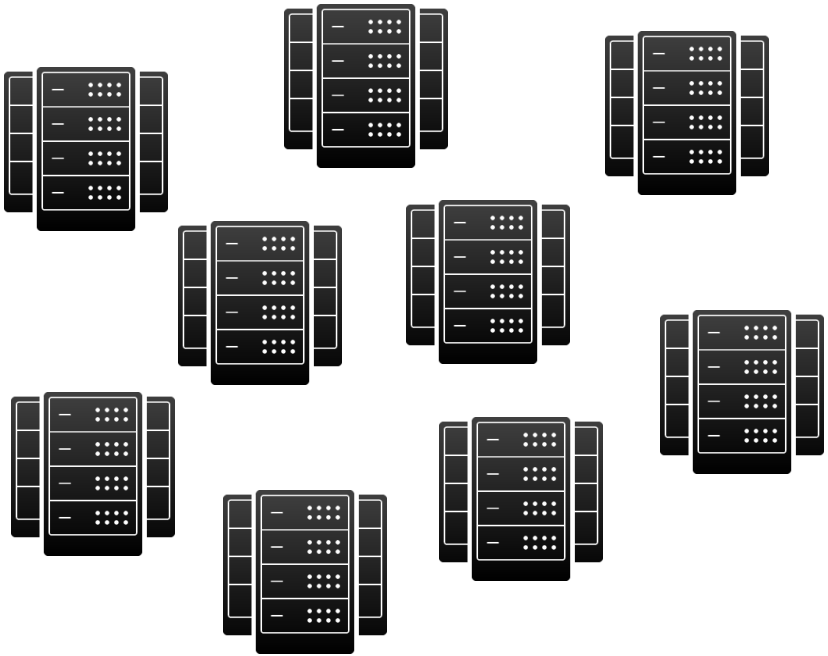
Time Series Data

- x,y,z acceleration
- rpm
- power
- wind velocity

Conditions

- Bearing problem
- Structural problem

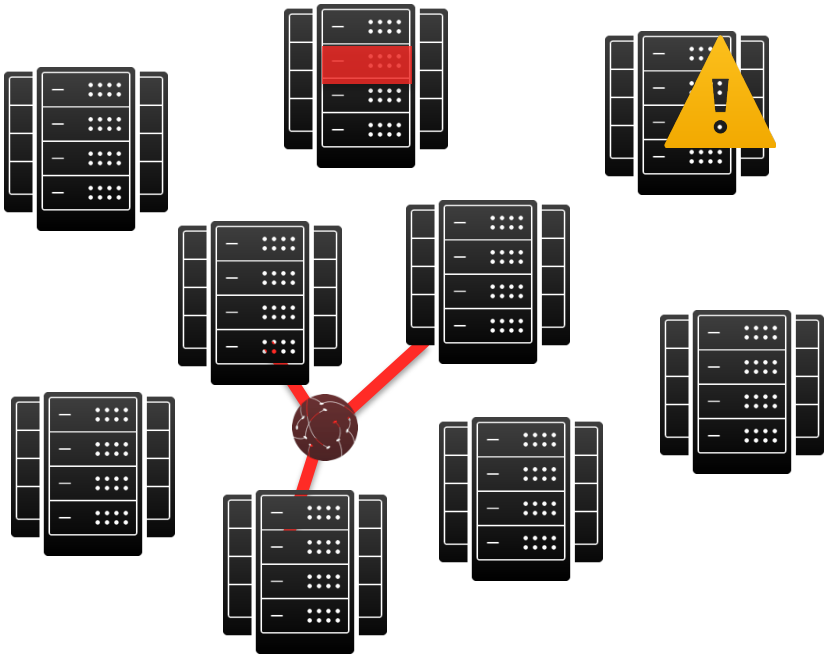
Data Centers



Time Series Data

- I/O stats
- temperature
- acoustic data
- activity metrics

Data Centers



Time Series Data

- I/O stats
- temperature
- acoustic data
- activity metrics

Conditions

- Hardware problem
- Network problem
- Upgrade problem

Users

Time Series Data

- logons
- http requests
- building entries
- attachment events

Users

Time Series Data

- logons
- http requests
- building entries
- attachment events

Conditions

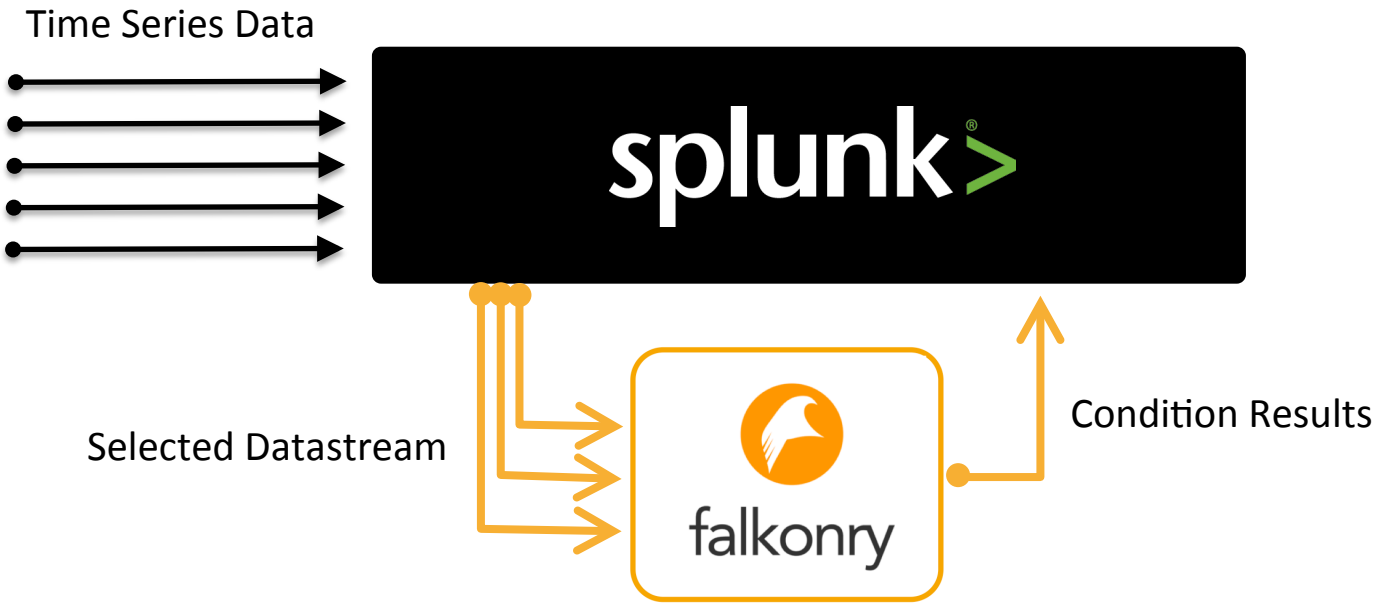
- Threat risk

An AI Assistant for Condition Recognition

.conf2016

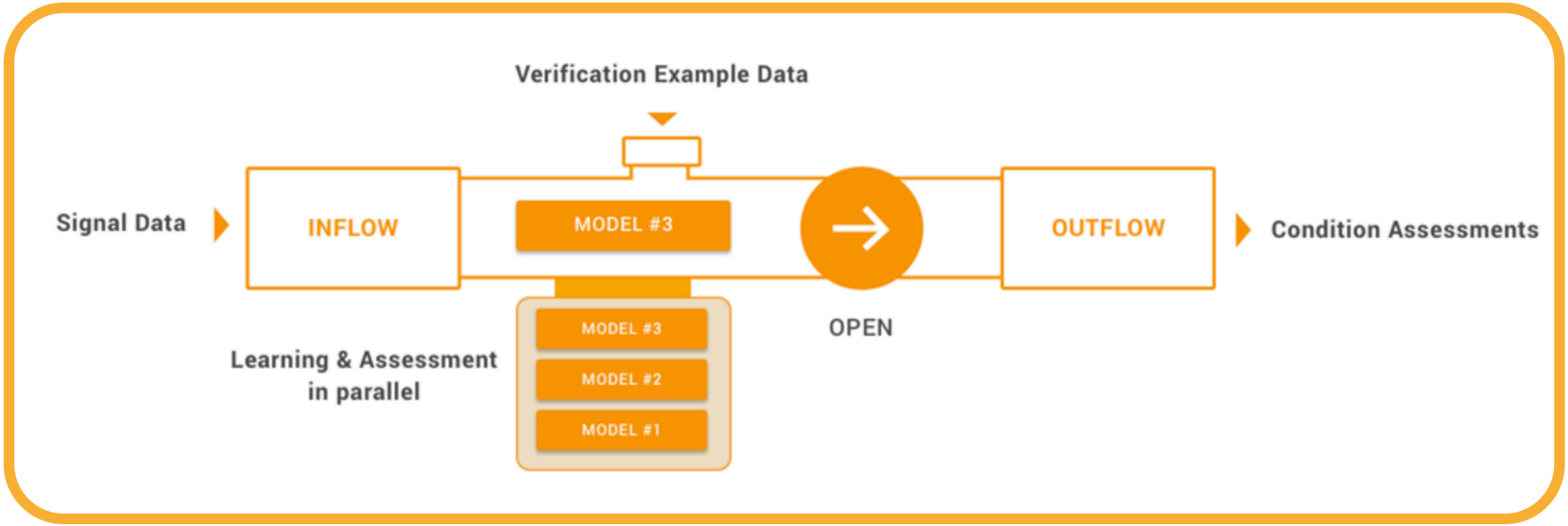
splunk>

Falkonry & Splunk

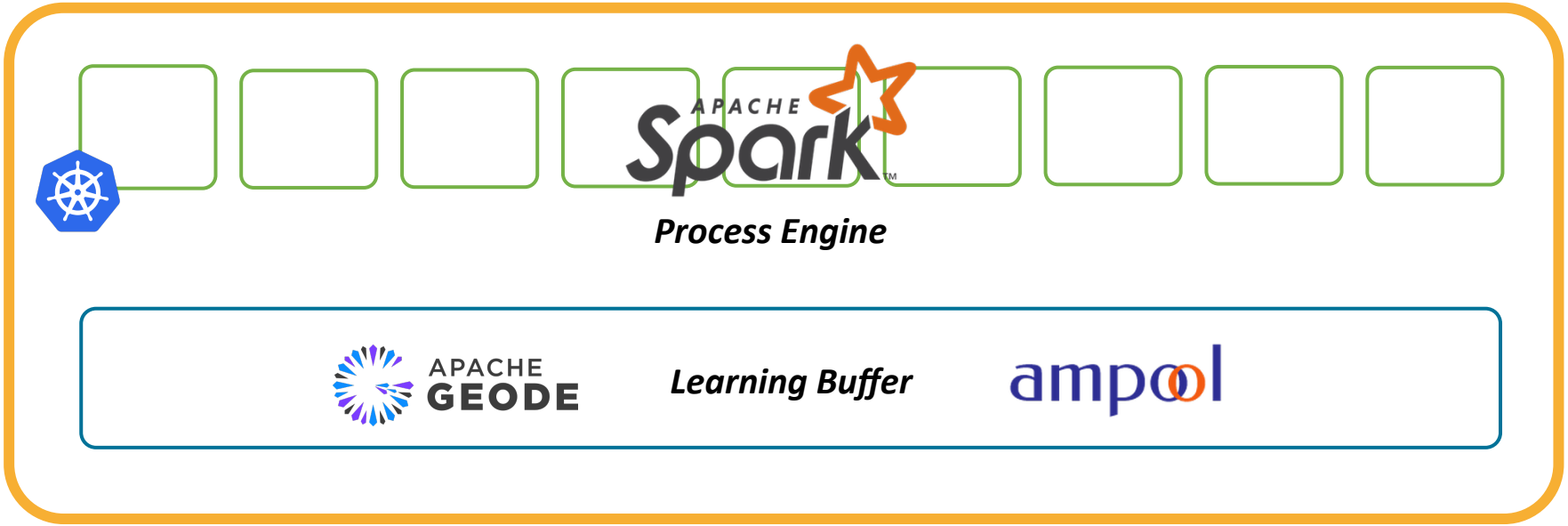


Inside the Assistant

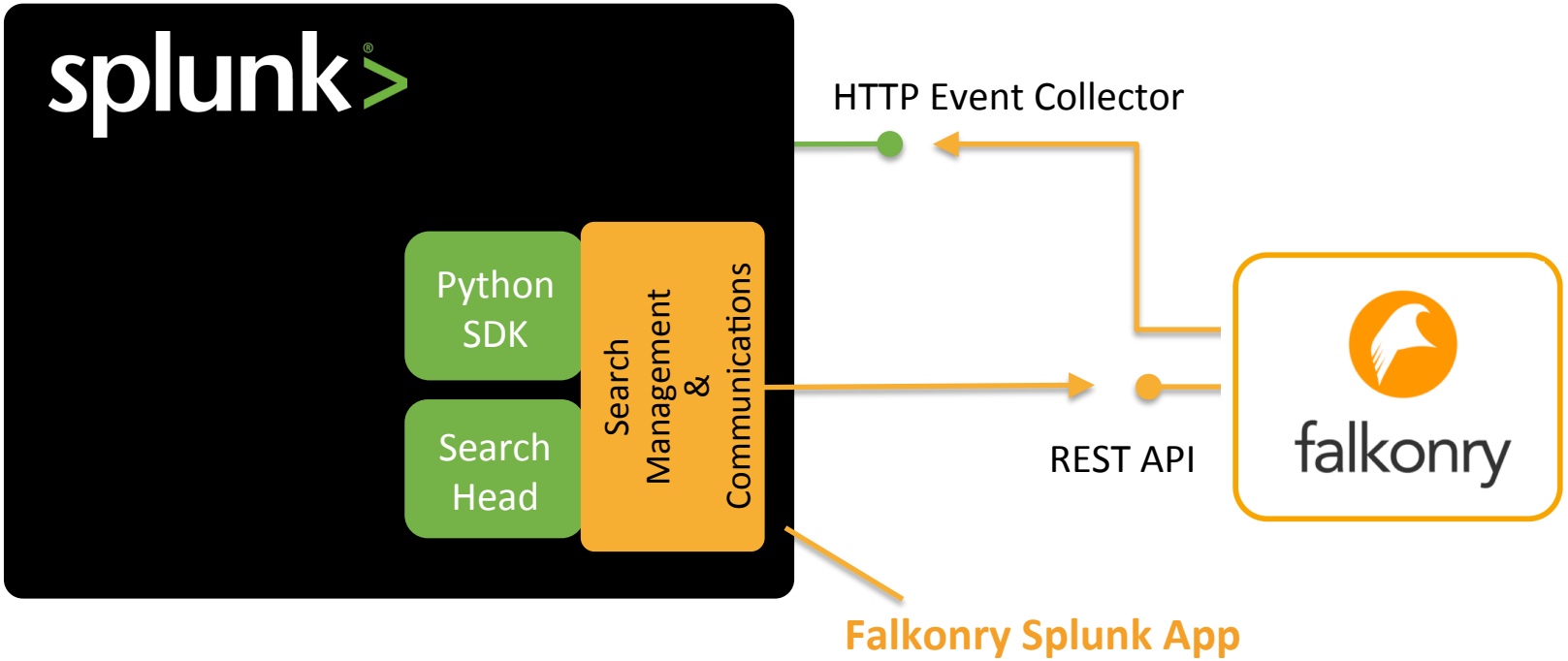
Inside the Assistant



Inside the Assistant



Splunk-Falkonry Connection



Deployment Options

falkonry

Virtual Appliance

Customer Cloud

A Falkonry-enhanced Splunk Application
Demonstration

Summary

- Time series pattern recognition is an enormous need
- Adding pattern recognition to Splunk is easy
- Splunk+Falkonry is a great platform for condition-aware applications

THANK YOU

falkonry

greg.olsen@falkonry.com

.conf2016

splunk>