

What's new in Machine Learning across the Splunk Portfolio

Manish Sainani | Director, Product Management

Bob Pratt | Sr. Director, Product Management

September 2017

Forward-Looking Statements

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 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.

Splunk, Splunk>, Listen to Your Data, 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. © 2017 Splunk Inc. All rights reserved.

Agenda

- ▶ Machine Learning Overview
- ▶ Splunk Machine Learning Toolkit (MLTK) Overview
- ▶ What's New in Machine Learning Toolkit?
- ▶ What's new in IT Service Intelligence ML?
- ▶ Splunk User Behavior Analytics (UBA) Overview
- ▶ What's new in UBA 4.0?

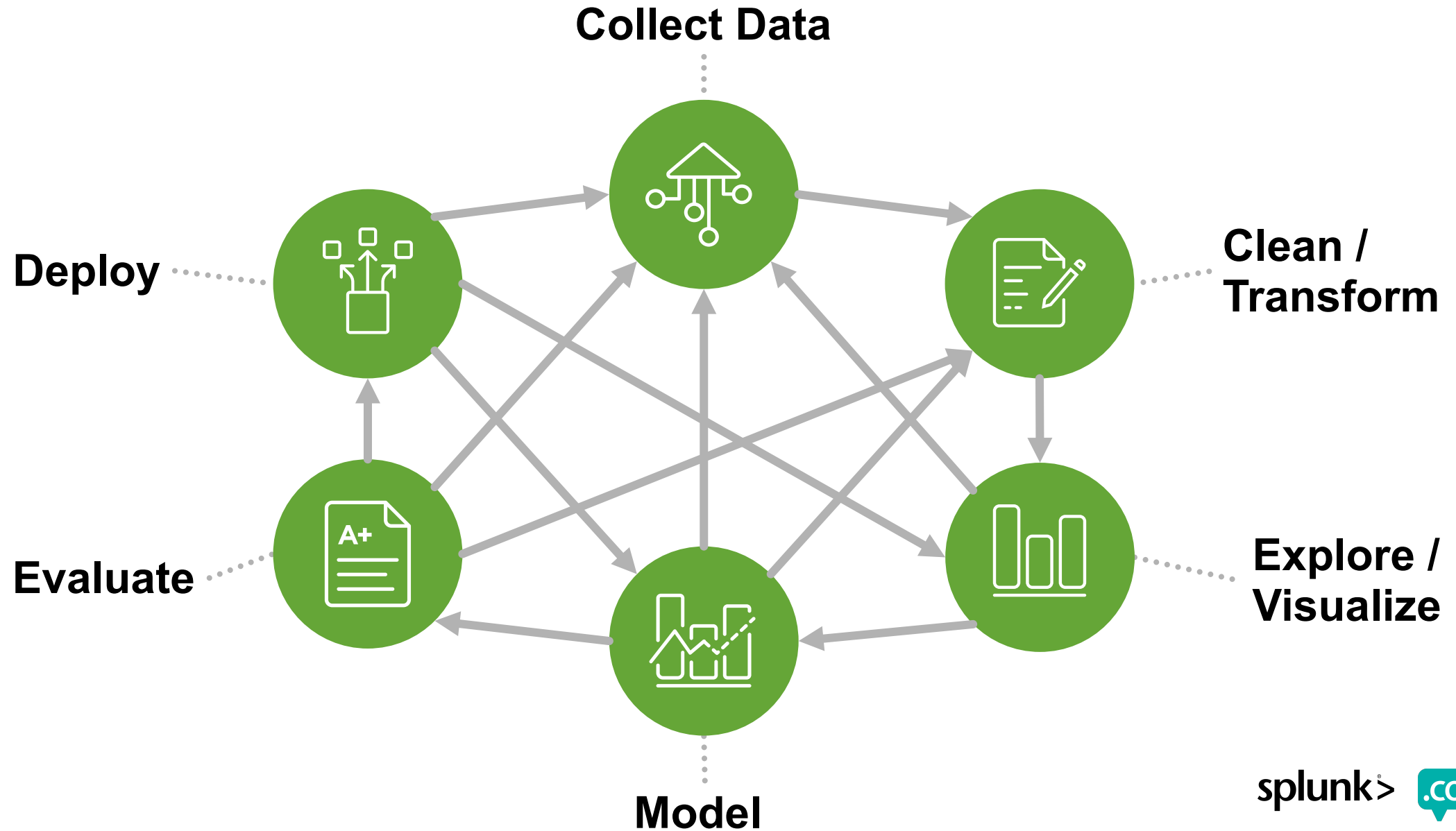
Machine Learning Overview

Machine Learning

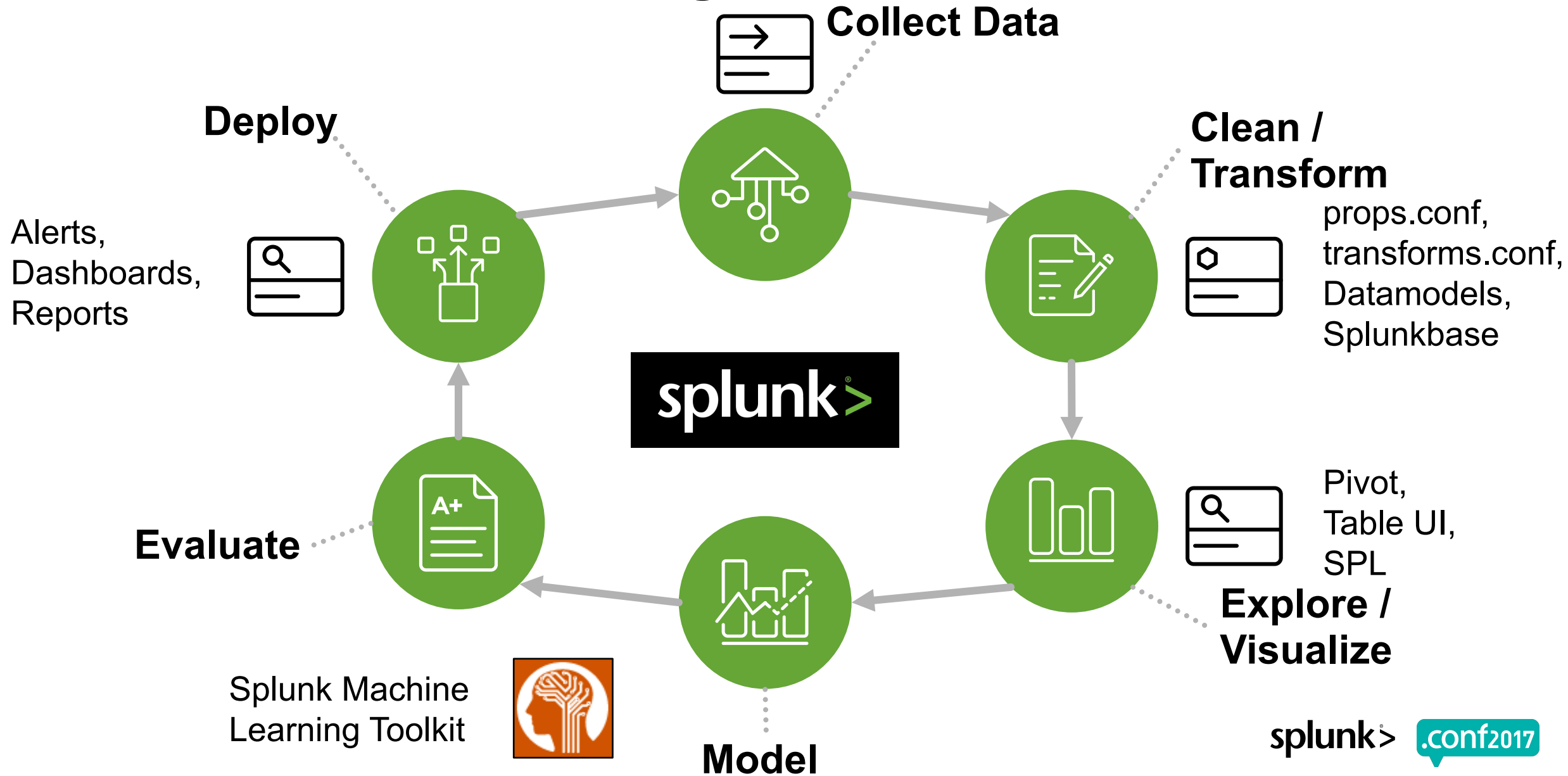
- ▶ A process for generalizing from examples
- ▶ Examples
 - $A, B, \dots \rightarrow \#$ (regression)
 - $A, B, \dots \rightarrow a$ (classification)
 - $X_{\text{past}} \rightarrow X_{\text{future}}$ (forecasting)
 - like with like (clustering)
 - $|X_{\text{predicted}} - X_{\text{actual}}| \gg 0$ (anomaly detection)



Machine Learning Process



Machine Learning Process with Splunk



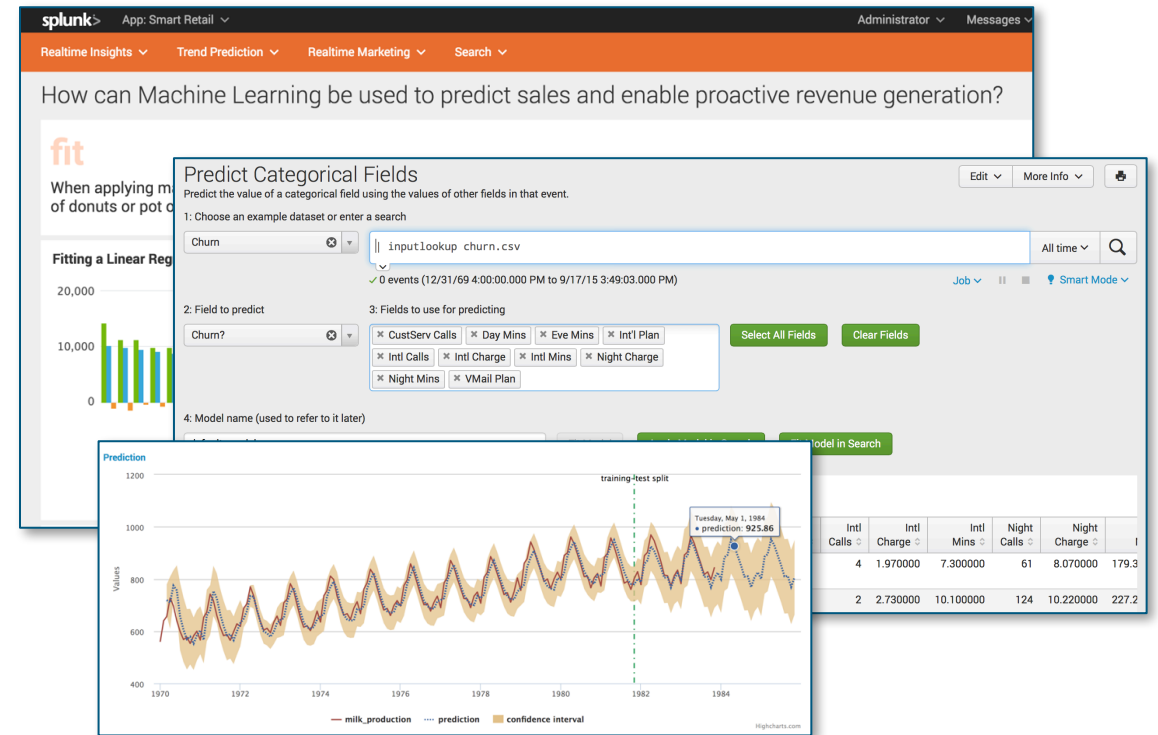
Splunk Machine Learning Toolkit

platform extensions and guided modeling dashboards

Splunk Machine Learning Toolkit

extends Splunk with new tools and guided modeling

- ▶ **Assistants:** Guide model building, testing, & deployment for common tasks
- ▶ **Showcase:** 25+ interactive examples from IT, security, business, and IoT
- ▶ **Algorithms:** 30 standard algorithms plus an extensibility API
- ▶ **SPL ML Commands:** New commands to fit, test, and operationalize models
- ▶ **Python for Scientific Computing Library:** 300+ open-source algorithms





Minimizing cell tower degradation and downtime with improved issue detection sensitivity



Speeding website problem resolution by automatically ranking actions for support engineers



Ensuring mobile device security by detecting anomalies in ID authentication



Preventing fraud by Identifying malicious accounts and suspicious activities



Improving uptime and lowering costs by predicting/preventing cell tower failures and optimizing repair truck rolls

What's New in MLTK?

since last .conf

What's New

(since .conf 2016)

- ▶ **Detect Numeric Outliers improvements**
- ▶ **Preprocessing / Data Prep**
- ▶ **Model Management**
- ▶ **ML-SPL extensibility API**
- ▶ **Spark Support (private limited beta)**
- ▶ **New algorithms:**
 - ARIMA supported in Forecasting Time Series Assistant
 - ACF & PACF
 - Gradient Boosting Classifier & Regressor
- ▶ **Load Existing Settings is per-user**
- ▶ **Downsampled Line Chart supports drilldown**

Detect Numeric Outliers

split-by support

?

Print

Detect Numeric Outliers

Find values that differ significantly from previous values.

Detect Outliers

Load Existing Settings

Enter a search

| inputlookup supermarket.csv | head 1000

All time

Q

✓ 1,000 results (12/31/69 4:00:00.000 PM to 8/11/17 4:26:57.000 PM)

Field to analyze

Threshold method

Threshold multiplier

☐ Sliding window (# of values)

Fields to split by

×

shop_id

quantity

Standard Deviation

5

0

☒ Include current point

Detect Outliers

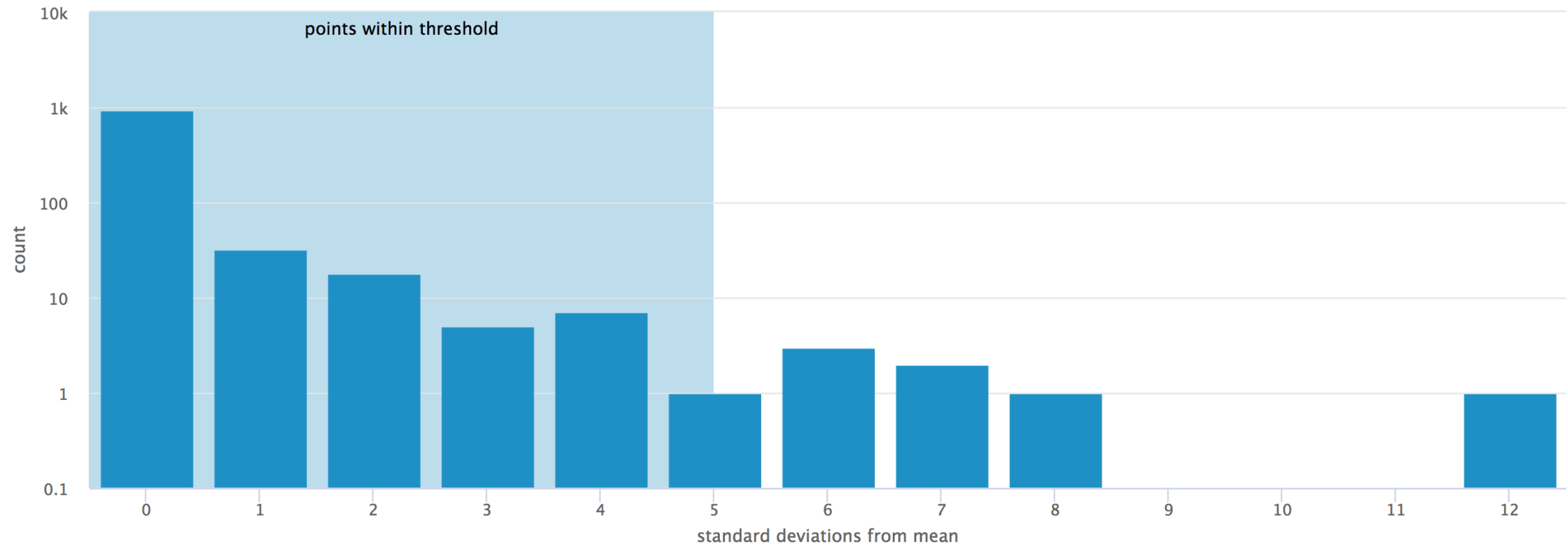
Open in Search

Show SPL

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D5SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-03" "Opera/9.80.2011.4.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D5SL7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.14 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D5SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-03" "Opera/9.80.2011.4.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D5SL7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.14 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)"
```

Detect Numeric Outliers

data distribution viz

Data Distribution [🔗](#)[Open in Search](#)[Show SPL](#)

Preprocessing

build a pipeline of data prep

- In Predict Numeric, Predict Categorical, and Cluster Numeric assistants

Preprocessing Steps

▼ StandardScaler

Preprocess method

StandardScaler

Fields to preprocess

business_acres property_tax_rate
distance_to_employment_center

Standardize Fields

☒ with respect to mean ☒ with respect to standard deviation

Apply

▼ PCA

Preprocess method

PCA

Fields to preprocess

✕ highway_accessibility_index ✕ distance_to_employment_center
✕ pupil_teacher_ratio ✕ crime_rate

K (# of Components)

2

Apply

130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-03" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_4; rv:55.0) Gecko/20100101 Firefox/55.0"
128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D5SL7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_4; rv:55.0) Gecko/20100101 Firefox/55.0"
ows NT 5.1; SV1; .NET CLR 1.1.4322" 468 125.17 14.1.1.1 "GET /oldlink?item_id=EST-26&SESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_4; rv:55.0) Gecko/20100101 Firefox/55.0"
item_id=EST-16&product_id=RP-LI-02" 404 720 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_4; rv:55.0) Gecko/20100101 Firefox/55.0"
action=purchase&itemId=EST-16&product_id=RP-LI-02" 404 720 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_4; rv:55.0) Gecko/20100101 Firefox/55.0"
buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02" 404 720 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_4; rv:55.0) Gecko/20100101 Firefox/55.0"

Model Management

(coming to MLTK 3.0)

- Provides Role Based Access Control to models
- Assign permissions to models to control who has what level of access
- Manage models via a rich UI interface

Edit Permissions

Model Title

Buttercup Store Purchases

Model ID

Buttercup_Store_Purchases

Owner

admin

App

Machine Learning

Allow access for

Owner

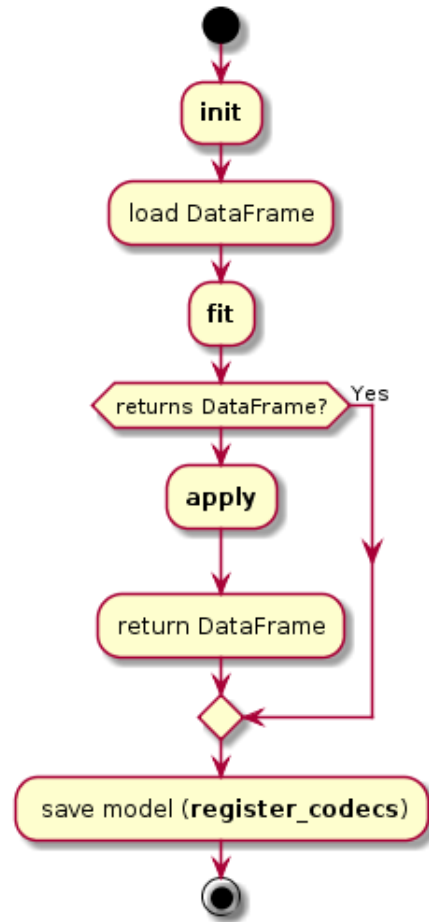
App

All Apps

Role	Read	Write
Everyone	<input type="checkbox"/>	<input type="checkbox"/>
admin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
can_delete	<input type="checkbox"/>	<input type="checkbox"/>
poweruser	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Splunk-System-Role	<input type="checkbox"/>	<input type="checkbox"/>
user	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

featuring: primo documentation

- ▶ Make more algos available to **fit** / **apply**
 - 300+ in PSC
 - Custom algorithms
- ▶ Expose new or different parameters
- ▶ Docs include examples
 - Correlation Matrix
 - Agglomerative Clustering
 - Support Vector Regressor
 - Savitzky-Golay Filter
- ▶ Use in your apps / dashboards / etc.!



private beta open now

Machine Learning Customer Success



Network Optimization
Detect & Prevent Equipment Failure



Security / Fraud Prevention



Prevent Cell Tower Failure
Optimize Repair Operations



Prioritize Website Issues
and Predict Root Cause



Entertainment
Company

Predict Gaming Outages
Fraud Prevention



Machine Learning Consulting Services



Analytics App built on ML Toolkit

What's new in ITSI ML ?

Event Co-relation and Clustering for Event Data

- ▶ Uses the Splunk “Reverse Pyramid Clustering” Algorithm to reduce noise in IT event data
- ▶ The algorithm extracts categorical and textual similarity from events and uses them in combination with a Service context to correlate events.
- ▶ Provides a UI based configuration editor that allows users to tweak parameters and tune configuration without a data scientist
- ▶ Not a black box – explainability is built right in. All event groups created by the algorithm provide an explanation as to why events were grouped together.

Splunk User Behavior Analytics

Machine Learning-based Threat Detection

Splunk User Behavior Analytics

An out-of-the-box solution that helps organizations find



Anomalous Behavior



Risky Users



Unknown Threats

with the use of **machine learning**

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=S01SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=S03SL7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CB-01"
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=S05SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=S01SL8FF3ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-4&product_id=K9-CB-01"
125.17 14.14.14.14 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=FLOWERS&JSESSIONID=S03SL7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CB-01"
125.17 14.14.14.14 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=FLOWERS&JSESSIONID=S03SL7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CB-01"
125.17 14.14.14.14 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=FLOWERS&JSESSIONID=S03SL7FF6ADFF0 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CB-01"

Splunk User Behavioral Analytics Pillars

Five Foundational Pillars



Real-Time & Big
Data Architecture



Behavior Baseline
& Modelling



Unsupervised
Machine Learning



Anomaly
Detection



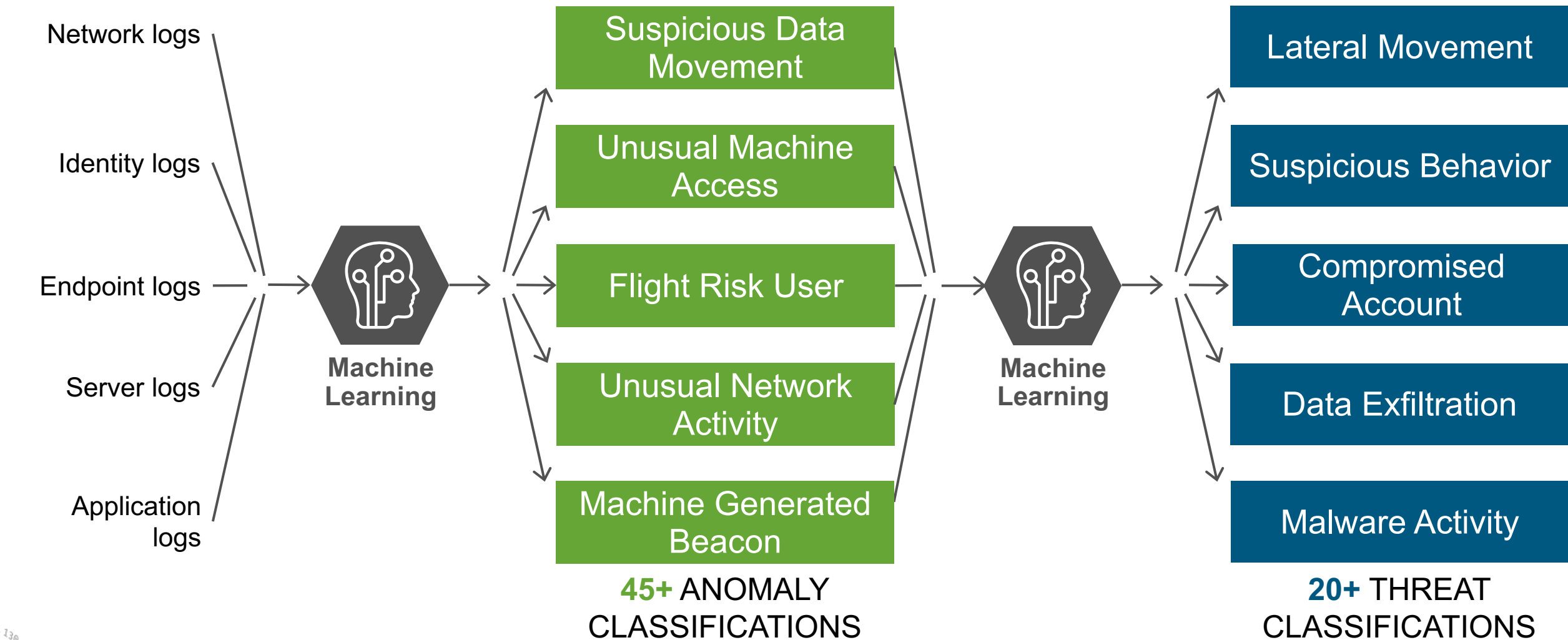
Threat
Detection



Splunk User Behavior
Analytics™

splunk> Platform for Machine Data

How Does Splunk UBA Work?



```
130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-03" "Mozilla/5.0" "Opera/9.80 (Win
128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D35L7FF6ADFF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/5.0" "Opera/9.80 (Win
317 27.160.0.0 - - [07/Jun 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/5.0" "Opera/9.80 (Win
item_id=EST-26&SESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/5.0" "Opera/9.80 (Win
toaction=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/5.0" "Opera/9.80 (Win
opping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Mozilla/5.0" "Opera/9.80 (Win
```

How does UBA integrate with Splunk Enterprise and ES?

Human-driven

- Rules
- Correlations
- Statistics

Splunk Enterprise Investigate

Known Threats

Splunk ES

Detect, Investigate & Respond

ML-driven

- Machine Learning
- Behavior Analysis
- Risk-level Scoring

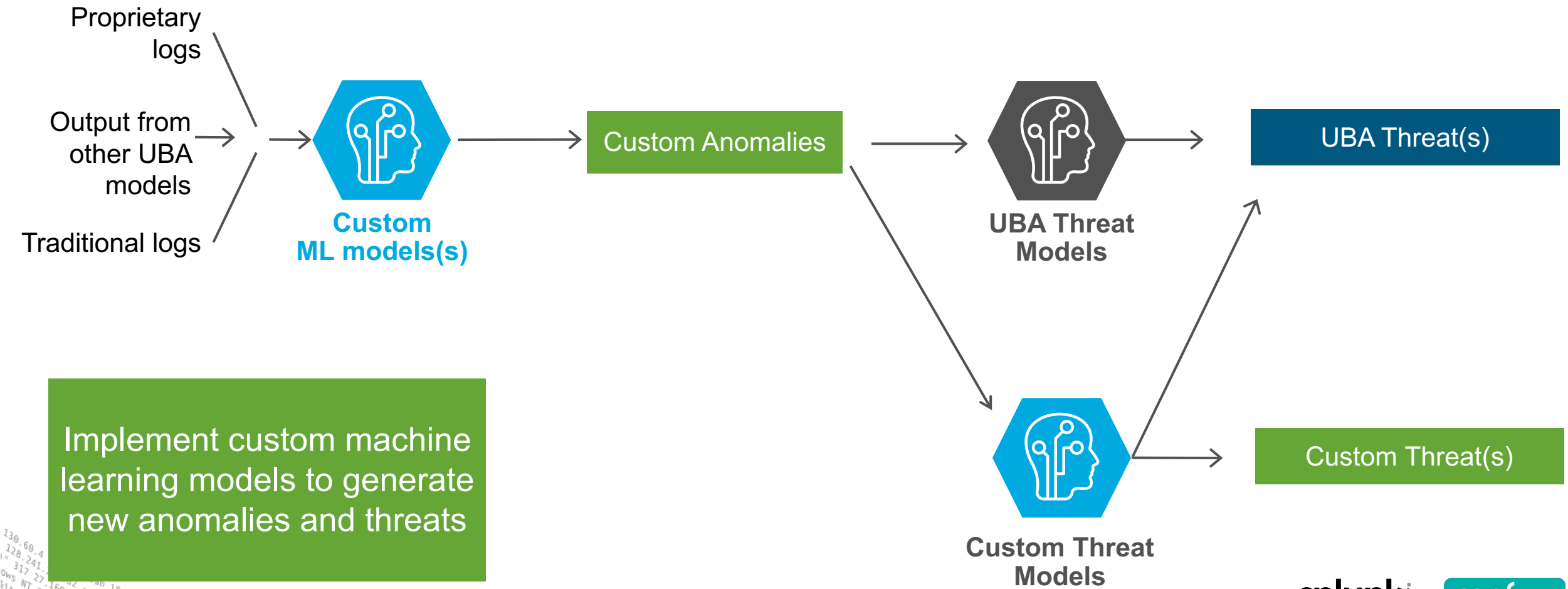
Splunk UBA Detect

Unknown Threats

What's New in UBA 4.0?

Announced here at .conf

UBA SDK – now available



PII Masking – also shipping now

PII Masking

☐ Disable PII Masking
☒ Enable PII Masking

Password ?

Confirm Password ?

Unmask Time * ?

[Cancel](#)
[OK](#)

Obfuscate user details during investigation or hunting

splunk> User Behavior Analytics

[Explore](#)
[Analytics](#)
[Config](#)

[Home](#) / [Users Table](#) / [_qhANLwzWnfnbszU5wy6v3u](#)

_qhANLwzWnfnbszU5wy6v3u

6

Last Update

Mar 28, 2017 7:07 AM

Watchlists

★

Account

Security Staff (_qnXudmt10u)

User Facts

THREATS	ANOMALIES	EVENTS	FAILED LOGINS	TOTAL SESSIONS	ANOMALOUS SESSIONS
2	38	962K	1	0	0

<div>EMPLOYEE ID</div> <div>_qnXudmt10u</div>	<div>OU</div> <div>IS Information Security</div>	<div>TITLE</div> <div>Cons Sec Risk Controls Eng</div>	<div>PHONE</div> <div>__am0atmTado5KsnXydk</div>
<div>CITY</div>	<div>STATE</div>	<div>ZIP CODE</div>	<div>COUNTRY</div>

Q&A

Manish Sainani | Director, Product Management

Bob Pratt | Sr. Director, Product Management