

splunk® > .conf2017

Predictive, Proactive, and Collaborative ML with IT Service Intelligence

Not a Science Project – Creating actionable events through Analytics

Nate Smalley | Staff SE

Andrew Stein | Analytical Architect

Sept 26, 2017 | Washington, DC

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.

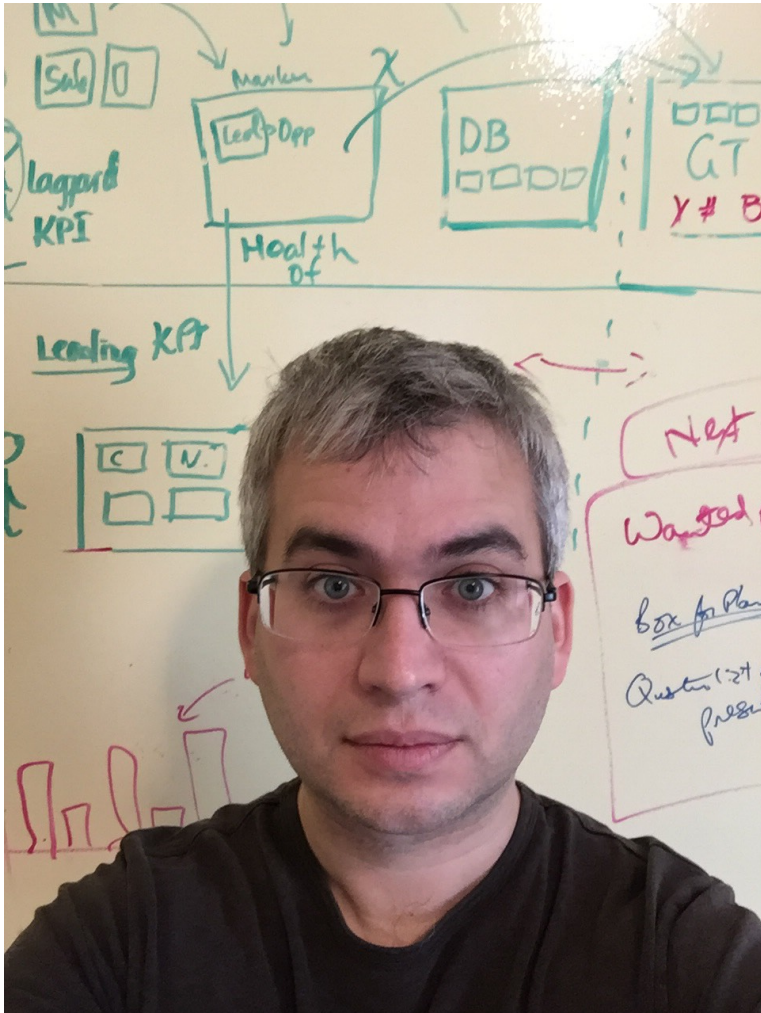
Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.

Nate Smalley



- ▶ IT Operations Technologist (Reformed Security Guy)
- ▶ Former Technical Director of Security & Monitoring Tools Team – Apollo Group (University of Phoenix)
- ▶ Currently Splunk Staff Sales Engineer supporting Large Businesses in FinServ & Manufacturing
- ▶ Enjoy Long walks across SNMP and Candle light dinners while fighting Operational Outages

Andrew Stein



- ▶ Splunk Global Analytical Architect
- ▶ 17 years creating mathimatically modeled solutions
- ▶ I spend 80 percent of time spent preparing data and 20 percent of time complaining about the need to prepare data.

Problem Statement

Operations Teams need more time between an alert and a failure that has Availability impacting ramifications. The introduction of Machine Learning is a have to have in order to predict these failures. These notable events must be able to pushed and collaborated on by via teams in various tools.



Indicators Matter

ITSI

Indicators

- ▶ Key Performance Indicators that is
 - Defined - **metrics** that are used to evaluate the overall status of a service.
- ▶ Leading Indicators – Drivers of a Result
- ▶ Lagging Indicators – Outcome of the Result
- ▶ Example Scenario
 - DB Runs out of Space
 - KPI Storage value = 100% <- Leading Indicator
 - KPI User Response time value = 2000+ secs <- Lagging Indicator

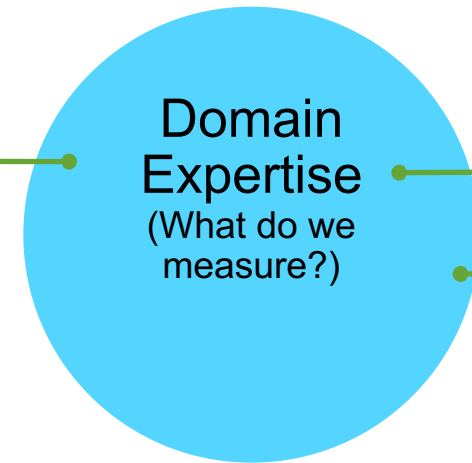
KPI's so what?

- ▶ Understanding the historical break out of Leading vs Lagging KPI's and the association to Services is critical in understanding how to predict a good outcome vs bad outcome.

- ▶ Understanding these key parts from the Service Experts is critical:

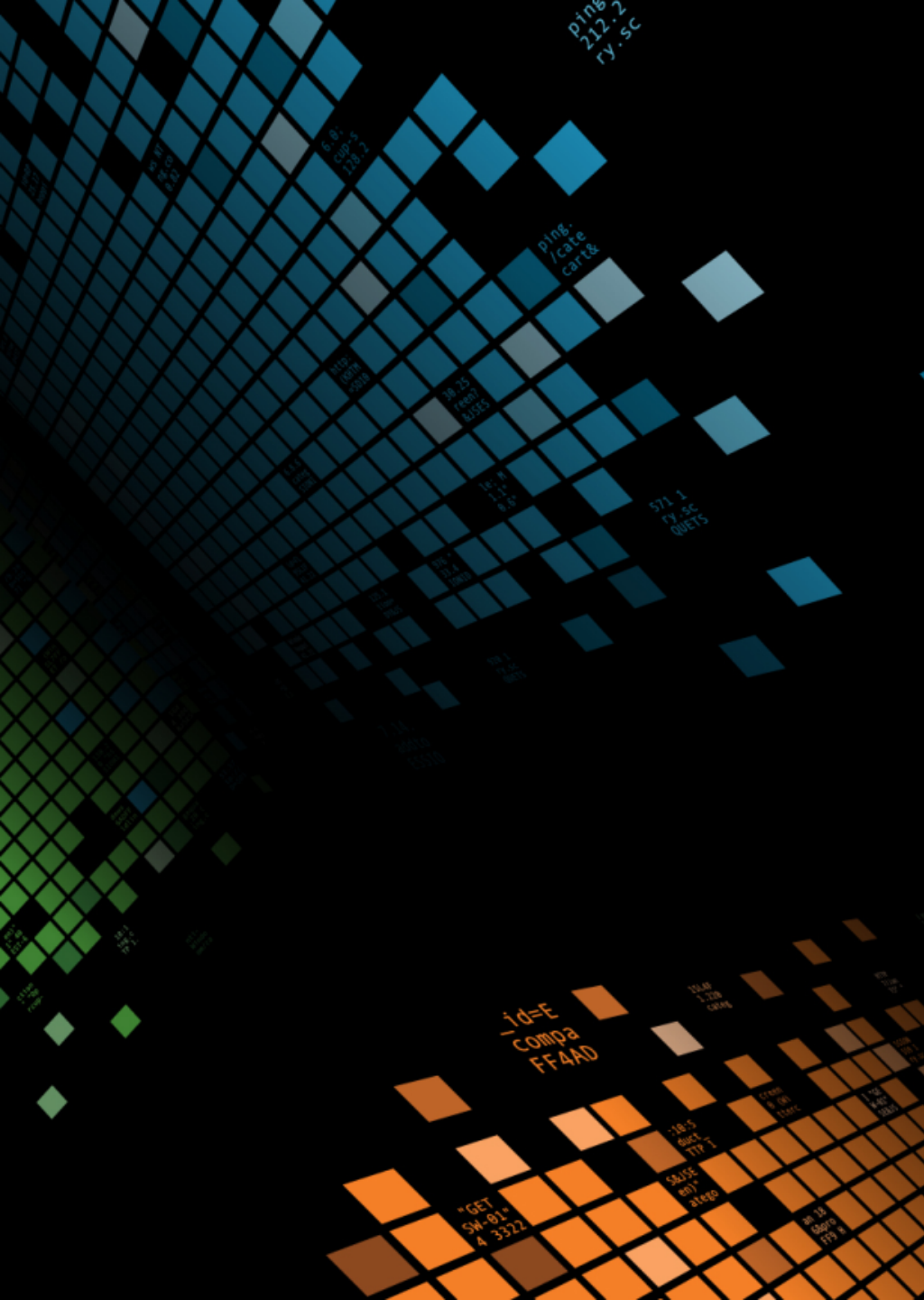
- Business Priority
- Use Case Data Needed
- The “RIGHT” KPI's to measure
- What decision happens when a Bad outcome Occurs

Set business/ops priorities



Identify use cases

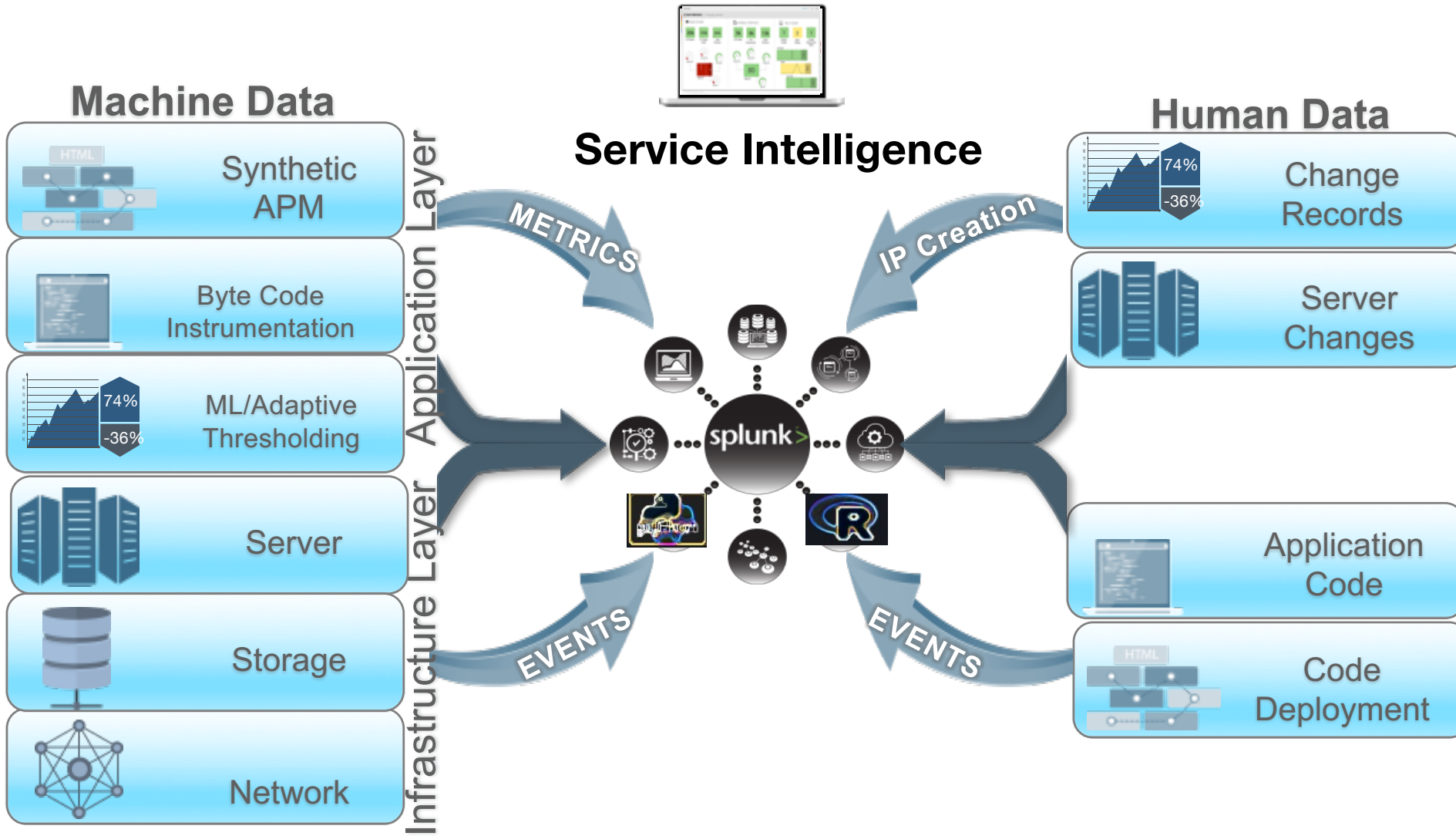
Drive decisions



Data Where to Get it

I need it STAT

Where Does Data Come From?



130.60.4 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5SLAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-5W-03" Moz/1.12.0
128.241.220.82 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5SLAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=K0-CB-01" Moz/1.12.0
ows NT 5.1; SV1: .NET CLR 1.1.4322" 468 125.17 14 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SLAFF10ADFF10 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01" Comp/1.1.0
itemId=EST-16&product_id=RP-LI-02" 468 125.17 14 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01" Comp/1.1.0
action=purchase&itemId=EST-268product_id=K0-CB-01" Moz/1.12.0
buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01" Comp/1.1.0

What Do I do with it Now?

- ▶ Use IT Service Intelligence
- ▶ Dynamic Service Structure
 - Provide Flexible Dependency Service mapping for interactions at Scale
- ▶ Build Key Performance Indicators
 - Leverage a Platform to build out KPI's
 - Ensure repeatability amongst Services for Consistency
 - Aggregation and Per Entity KPI Values
- ▶ Ease the burden of Cleaning Data (Schema at search time?)

“Data scientists spend 60% of their time on cleaning and organizing data. Collecting data sets comes second at 19% of their time, meaning data scientists spend around 80% of their time on preparing and managing data for analysis.”



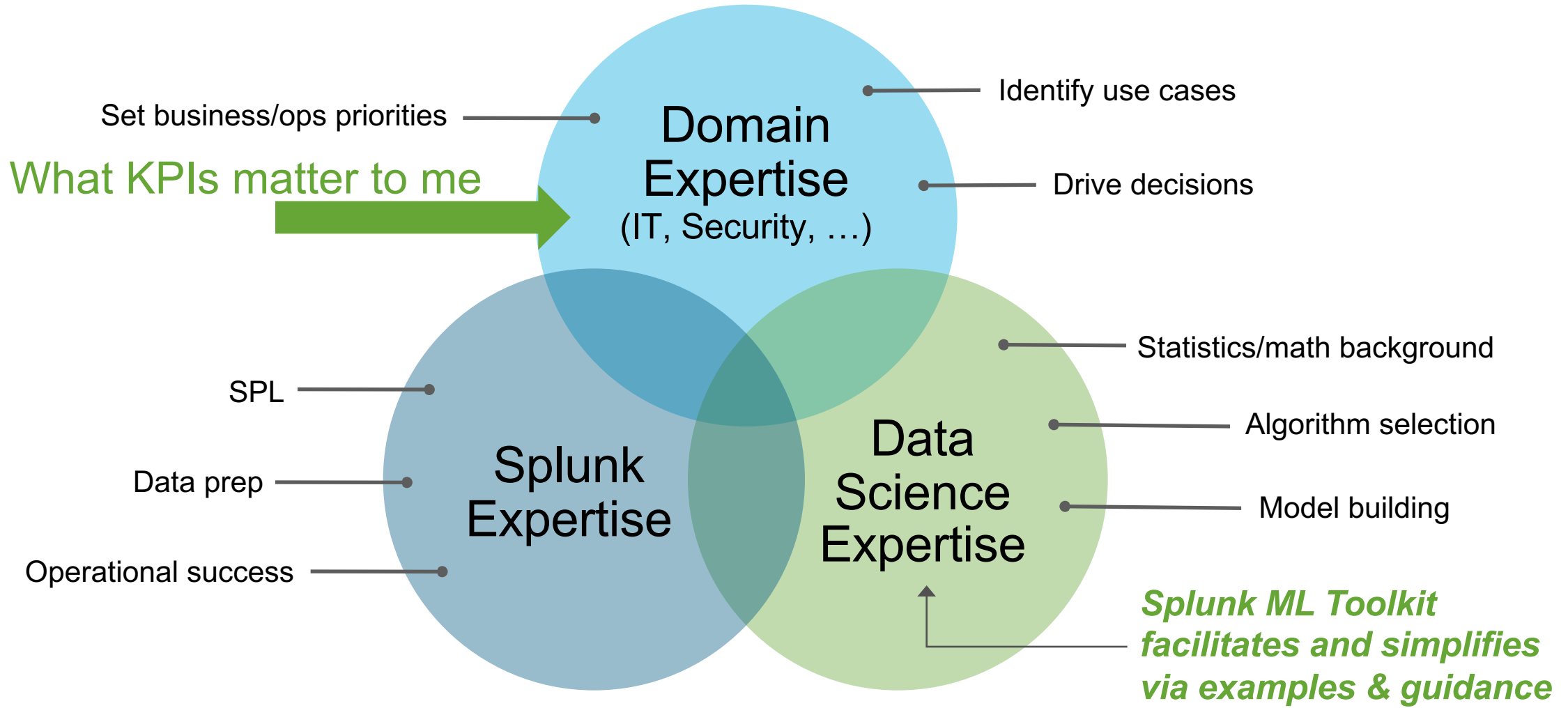
Real Use Case Example

Lets Get the data

We Need Machine Learning

Do you want to watch it or let it go?

Custom Machine Learning – Success Formula



```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-00"
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3"
10.0.0.0 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-00"
10.0.0.0 - - [07/Jan 18:10:55:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-00"
  
```

Overview of ML at Splunk



CORE PLATFORM
SEARCH



PACKAGED PREMIUM
SOLUTIONS



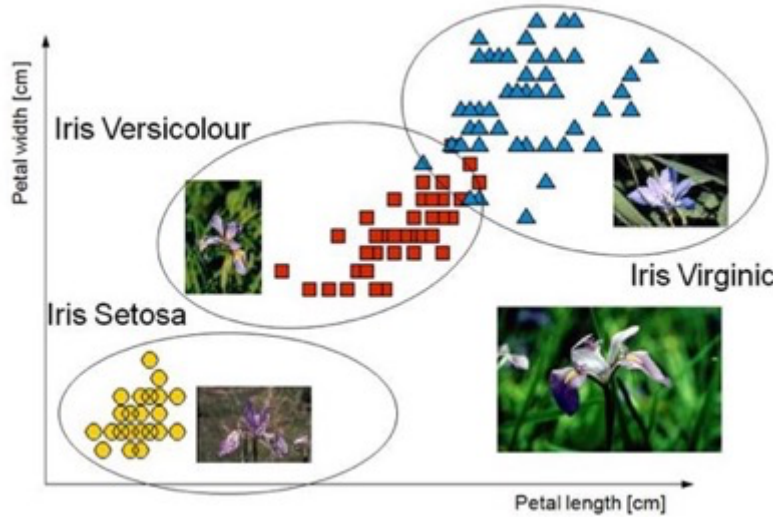
MACHINE LEARNING
TOOLKIT

splunk> Platform for Operational Intelligence

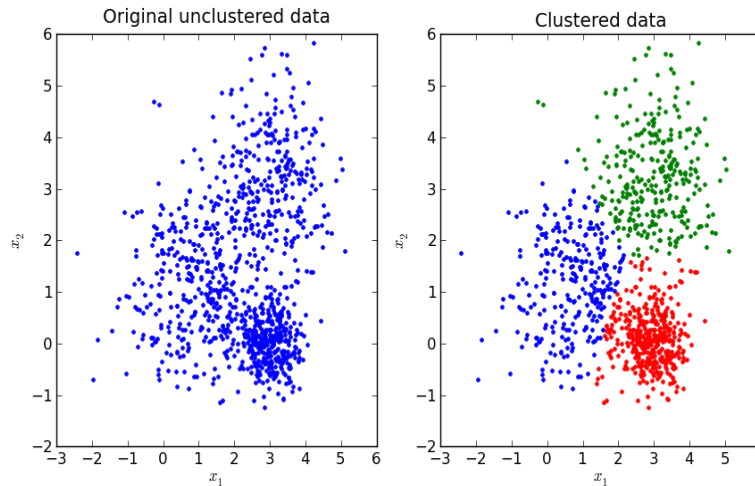
```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS"
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3"
10.55.187 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3"
10.55.188 - - [07/Jan 18:10:55:188] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3"
10.55.189 - - [07/Jan 18:10:55:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3"
10.55.190 - - [07/Jan 18:10:55:190] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3"
10.55.191 - - [07/Jan 18:10:55:191] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3"
10.55.192 - - [07/Jan 18:10:55:192] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3"
10.55.193 - - [07/Jan 18:10:55:193] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3"
10.55.194 - - [07/Jan 18:10:55:194] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3"
10.55.195 - - [07/Jan 18:10:55:195] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3"
10.55.196 - - [07/Jan 18:10:55:196] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3"
10.55.197 - - [07/Jan 18:10:55:197] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3"
10.55.198 - - [07/Jan 18:10:55:198] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3"
10.55.199 - - [07/Jan 18:10:55:199] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3"
10.55.200 - - [07/Jan 18:10:55:200] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3"
```


Three Types Of Machine Learning

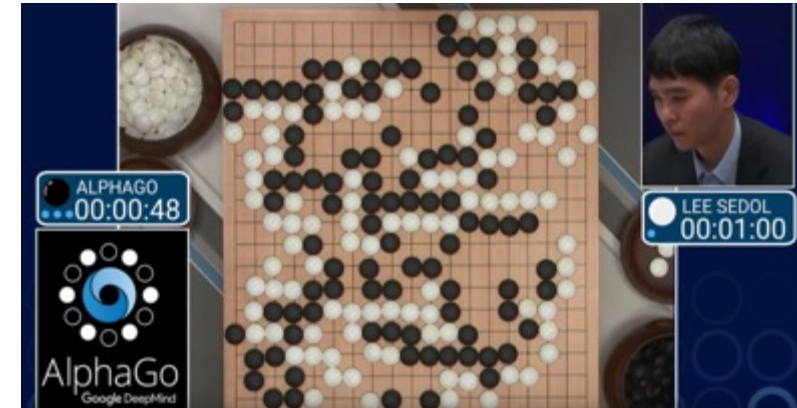
Supervised Learning:



Unsupervised Learning:



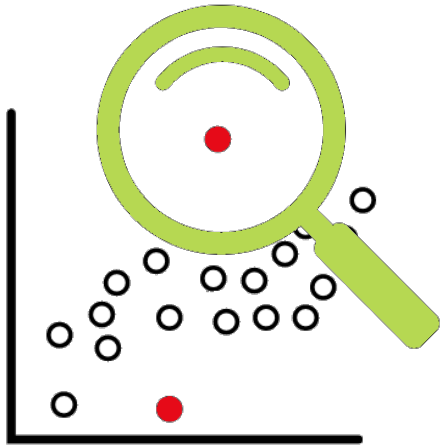
Reinforcement Learning:



130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product_id=KQ-CW-01"
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3"
10.0.0.1 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3"
10.0.0.1 - - [07/Jan 18:10:55:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3"
10.0.0.1 - - [07/Jan 18:10:55:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3"
10.0.0.1 - - [07/Jan 18:10:55:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3"

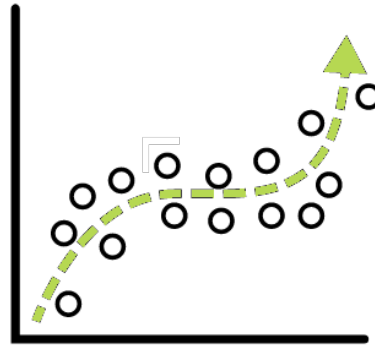
Splunk Customers Have ML Problems

Anomaly detection



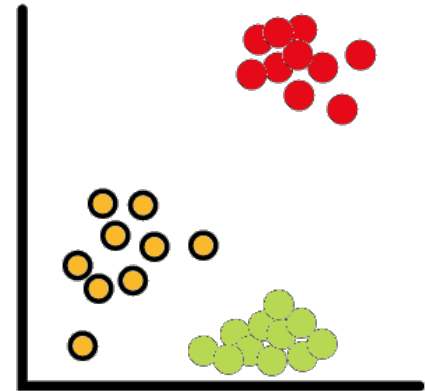
Deviation from past behavior
 Deviation from peers
 (aka Multivariate AD or Cohesive AD)
 Unusual change in features
ITSI MAD Anomaly Detection

Predictive Analytics

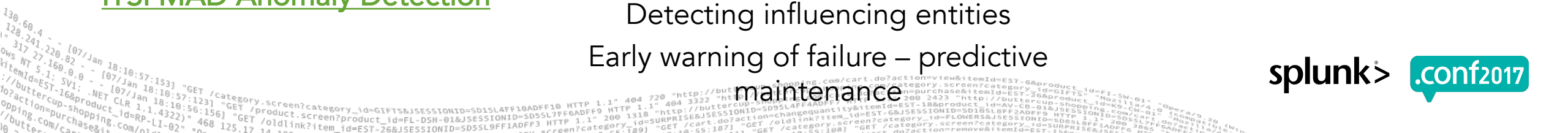


Predict Service Health Score
 Predicting Churn
 Predicting Events
 Trend Forecasting
 Detecting influencing entities
 Early warning of failure – predictive maintenance

Clustering



Identify peer groups
 Event Correlation
 Reduce alert noise
ITSI Event Analytics



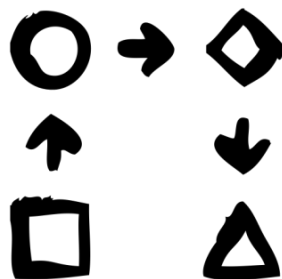
Splunk Machine Learning Toolkit



Created by Arthur Shian from Noun Project

Algorithms

25+ standard algorithms available prepackaged with the toolkit



Created by Ralf Schmitzer from Noun Project

Assistants

Guide model building, testing, & deployment for common objectives



Created by Antony from Noun Project

Showcase

Interactive examples for over 25 typical IT, security, business, IoT use cases



New commands to fit, test and operationalize model



Python for Scientific Computing Library
300+ open source algorithms available for use



Mlib integration



Real Use Case Example

Lets Use ML to get Predictive



Event Analytics

BUILT IN - IT Service Intelligence Machine Learning

IT Service Intelligence Event Analytics

- ▶ **Notable Events are key**
 - We created a notable for Web Store Service – Called webstore_health_alert
 - Lets see how Splunk can cluster this with other events to show other Notable Events that are attributed

- ▶ **Smart Mode is actually Smart**
 - It use clustering to group events remember unsupervised ML at the beginning

The screenshot shows the Splunk Service Analyzer interface with a modal dialog titled "Select the fields to be analyzed". The dialog provides a summary of selected fields for event similarity analysis. Below is a table of the selected fields:

| Field | Type | # of Values | Event Coverage |
|-----------------|----------|-------------|---------------------|
| NetObject | Category | 7 | 4.08 % |
| Title | Category | 9 | 4.08 % |
| account_id | Category | 2 | 45.73 % |
| activity_due | Category | 642 | 6.84 % |
| alert | Category | 3 | 4.12 % |
| alert_color | Category | 3 | 7.489999999999999 % |
| alert_level | Category | 3 | 7.489999999999999 % |
| alert_severity | Category | 3 | 7.489999999999999 % |
| alert_value | Category | 11 | 7.53 % |
| alertriggertime | Text | | |

The dialog also includes a "Re-run Analysis" button, a time range of "Last 24 hours", and a "Done" button.

The Diamonds in the Rough

Clustering Events into actionable alerts

- ▶ Take 1000's or 100's of 1000's of alerts and connect them
- ▶ Use ML prediction to improve correlation
- ▶ Boil the events down to reasonable count of Actionable Events

The screenshot displays the 'Notable Events Review' interface in Splunk. At the top, there are navigation tabs: Service Analyzer, Notable Events Review, Glass Tables, Deep Dives, Multi KPI Alerts, Search, Configure, and Product Tour. The main area shows 11685 events for the last 24 hours. A bar chart visualizes event counts, with a peak around 6:00 PM on Sun Sep 17. Below the chart is a table of event titles, including 'Database Events: status: Default Policy', 'Database Events: status: Grouping Factors', and 'Nagios Service Check: cl'. A configuration panel is overlaid on the table, allowing users to adjust event similarity factors and split events into groups. The configuration panel includes sliders for 'Textual Similarity' and 'Categorical Similarity', and options to 'Split events by field' and 'Break group'. A warning message at the bottom states: 'Cannot save ACE policy until group generation has been completed'.

Real Use Case Example

Predictive Analytics in Real-time

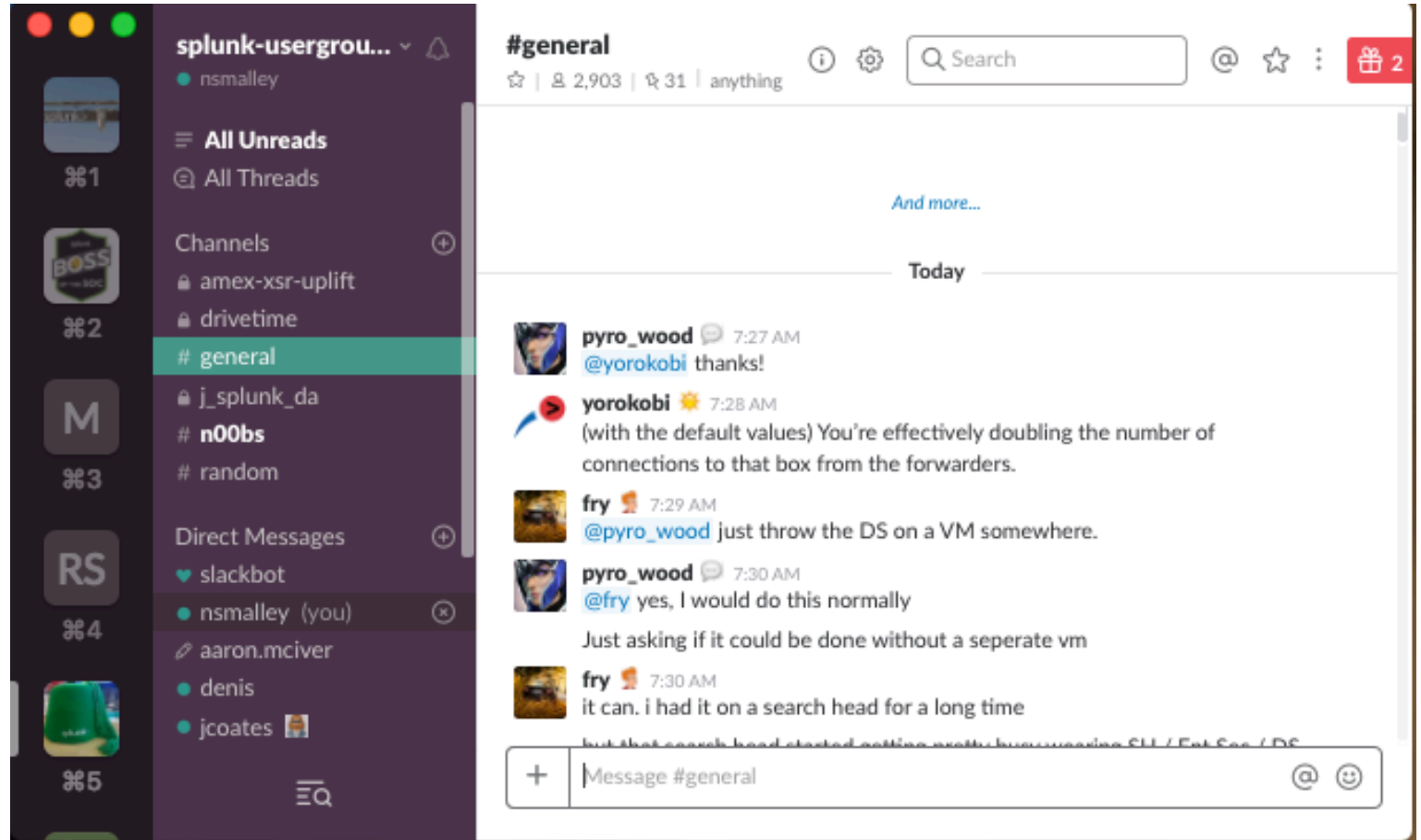
Lets Get Others Involved

ChatOps - Anyone Slack?

Slack

▶ Slack

- Instant Message
- Easy Channel Setup
- Fast time to create incident working groups
- Other Products just as easy HipChat, Skype etc...



The screenshot shows a Slack interface for a workspace named "splunk-usergrou...". The left sidebar lists channels and direct messages. The main area shows a conversation in the #general channel.

Channels: amex-xsr-uplift, drivetime, # general (selected), j_splunk_da, # n00bs, # random

Direct Messages: slackbot, nsmalley (you), aaron.mciver, denis, jcoates

Messages in #general:

- pyro_wood: @yorokobi thanks!
- yorokobi: (with the default values) You're effectively doubling the number of connections to that box from the forwarders.
- fry: @pyro_wood just throw the DS on a VM somewhere.
- pyro_wood: @fry yes, I would do this normally
- pyro_wood: Just asking if it could be done without a seperate vm
- fry: it can. i had it on a search head for a long time

ChatOps = Splunk & Slack

► Slack Setup

- Install the Alert Action
- <https://splunkbase.splunk.com/app/2878/>
- For Core Searches – Configure as alert action in Alerts
- For ITSI
 - Enable Slack in `notable_event_actions.conf`
- Lets add it to our Policy
- Configure -> Notable Event Aggregation Policy -> Create New

Create New Policy

Filtering Criteria

Create filtering criterion to group notable events

Include the events if

owner matches Splunk Bot

+ Add Rule (AND)

+ Add Rule (OR)

Create New Policy

Action Rules

Create action rules upon this group

If this group existed for 10, then on all events in this group

If this group existed for 10 In Seconds

Then slack Configure on all events in this group

+ Add Rule

Splunk APP 9:00 AM ☆

Digital Errors Detected

07-19-2017 08:59:22 AM c2b:nginx-access GET /api/v1/mr/accounts/#####/obligations?limit=#####&startDate=##### 500 Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko 0.009

Click here for full results: https://itsi-republicservices.splunkcloud.com/app/itsi/@go?sid=scheduler_andpbHNvbjEwQHJlCfHVibGjlc2VydmljZXMuY29t_itsi__RMD57952f7c075dc27be_at_1500480000_36881

Real Use Case Example

Predictive Analytics in Real-time

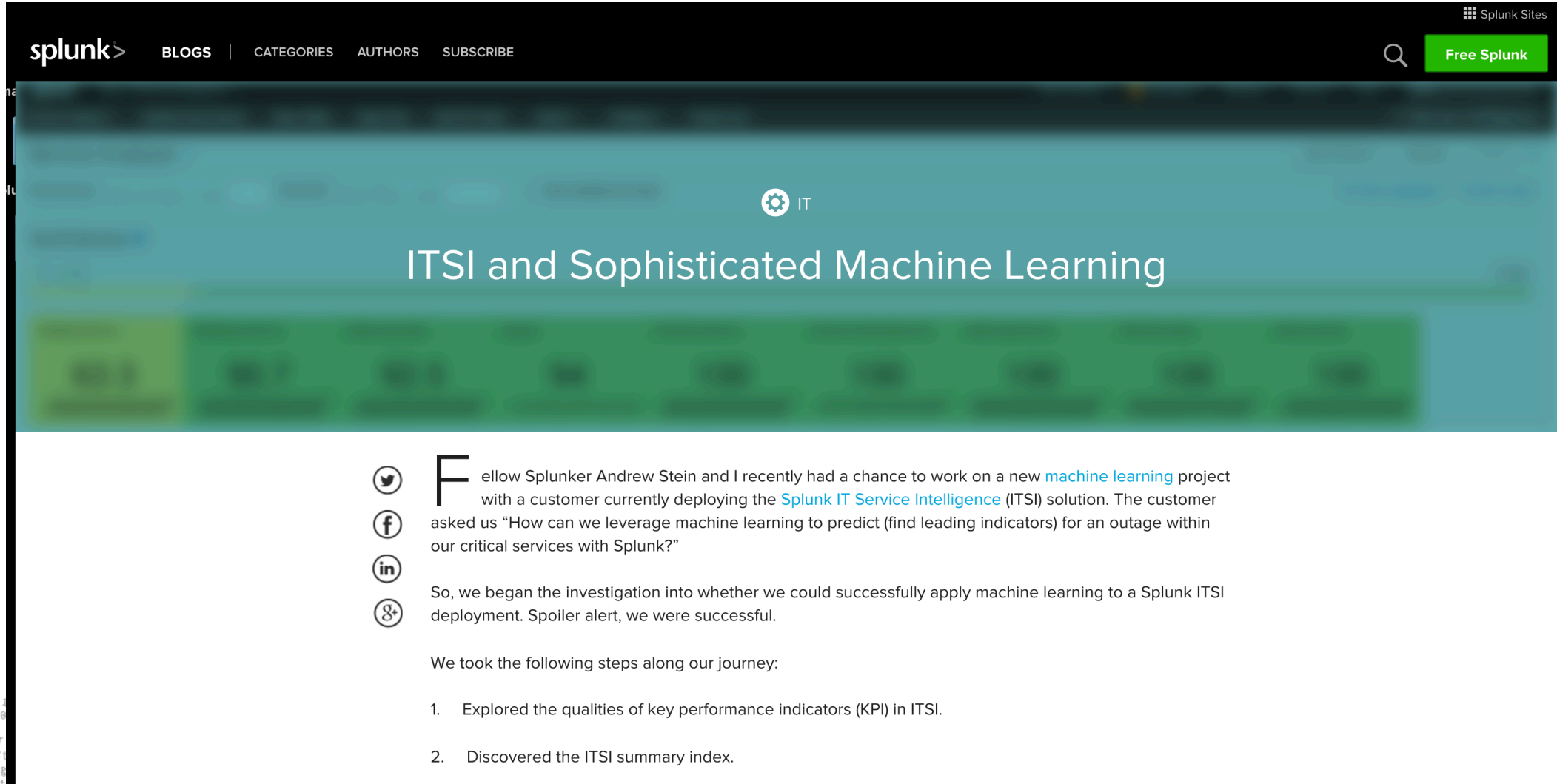
Wrap Up

- ▶ ITSI allows for Rapid Service, KPI, Entity creation and alerting
- ▶ Machine Learning through MLTK provides a repeatable ability to Predict Service Health
- ▶ IT Service Intelligence Event Analytics enables teams to cluster Notable events together to have 1 Actionable Alert
- ▶ Splunk IT Service Intelligence provides extendable capabilities to provide immediate notification to Chat Groups, Ticketing system and other communication platforms to improve the Mean Time to Remediate Availability Impacting Situations



I fell asleep. Where else can I read about this?

<https://www.splunk.com/blog/2017/08/28/itsi-and-sophisticated-machine-learning.html>



The screenshot shows the Splunk website interface. At the top, there is a navigation bar with the Splunk logo, links for 'BLOGS', 'CATEGORIES', 'AUTHORS', and 'SUBSCRIBE', a search icon, and a 'Free Splunk' button. The main content area features a large teal header with the title 'ITSI and Sophisticated Machine Learning' and a gear icon with 'IT' next to it. Below the header, there are social media sharing icons for Twitter, Facebook, LinkedIn, and Google+. The main text begins with a large 'F' and discusses a machine learning project with a customer using Splunk IT Service Intelligence (ITSI). It mentions the goal of predicting outages and the successful application of machine learning to a Splunk ITSI deployment. The text concludes with a spoiler alert and a list of two steps taken during the investigation.

splunk > BLOGS | CATEGORIES | AUTHORS | SUBSCRIBE

Splunk Sites

Free Splunk

IT

ITSI and Sophisticated Machine Learning

Follow Splunker Andrew Stein and I recently had a chance to work on a new [machine learning](#) project with a customer currently deploying the [Splunk IT Service Intelligence \(ITSI\)](#) solution. The customer asked us “How can we leverage machine learning to predict (find leading indicators) for an outage within our critical services with Splunk?”

So, we began the investigation into whether we could successfully apply machine learning to a Splunk ITSI deployment. Spoiler alert, we were successful.

We took the following steps along our journey:

1. Explored the qualities of key performance indicators (KPI) in ITSI.
2. Discovered the ITSI summary index.

130.60.4 - - [07/Jan
128.241.220.82 - - [0
ows NT 5.1; SV1: .NET
kItemId=EST-16&product
io?action=purchase&i
opping.com/cas
/butte

.conf2017

Go see these Talks!

This is where the subtitle goes

▶ David Vueve

- Splunk Ninja Skills
- 190+ slides of SPL and guidance.

▶ Xander and (fred?)

- Deep dive into MLTK
- MLTK API for importing algorithms

▶ Phillip Drieger

- DGA Analysis
- End to End MLTK example

▶ Making ML Solutions

- Deep dive into ML process
- Customer use cases explored

Questions?

Please Feel Free

Want to Learn More About ITSI at .conf2017?

Tuesday
September
26th, 2017

- ▶ **Ready, Set, Go! Learn From Others - The First 30 Day Experiences of ITSI Customers:** Tuesday, September 26th, 2017 12:05 PM- 12:50 PM Room Salon C
- ▶ **Splunk ITSI Overview:** Tuesday, September 26th, 2017 1:10 PM-1:55 PM Room 147 AB
- ▶ **PWC: End-to-End Customer Experience:** Tuesday, September 26th, 2017 2:15 PM-3:00 PM Room 143ABC
- ▶ **RSI: Operational Intelligence: How to go From Engineering to Operationalizing IT Service Intelligence Where the Rubber Meets the Road:** Tuesday, September 26th, 2017 2:15 PM-3:00 PM Room147AB
- ▶ **Cardinal Health: Ensuring Customer Satisfaction Through End-To-End Business Process Monitoring Using Splunk ITSI:** Tuesday, September 26th, 2017 3:30 PM-4:15 PM Room143ABC
- ▶ **ITSI in the Wild - Why Micron Chose ITSI and Lessons Learned From Real World Experiences:** Tuesday, September 26th, 2017 4:35 PM- 5:20 PM Room Salon C

Wednesday
September
27th, 2017

- ▶ **Event Management is Dead. Time Series Events are the Means to the End, not the End Itself. See How Event Analytics is Revolutionizing IT:** Wednesday, September 27th, 2017 11:00 AM-11:45 AM Ballroom C
- ▶ **Triggering Alerting (xMatters) and Automated Recovery Actions from ITSI:** Wednesday, September 27th, 2017 1:10 PM- 1:55 PM Room Salon C
- ▶ **Leidos - Our Journey to ITSI:** Wednesday, September 27th, 2017 2:15 PM-3:00 PM Room147AB
- ▶ **How Rabobank's Monitoring Team Got a Seat at the Business Table by Securing Sustainability on Competitive Business Services Build on Splunk's ITSI:** Wednesday, September 27th, 2:15-3:00pm Room 147AB
- ▶ **Here Comes the Renaissance: Digital Transformation of the IT Management Approach:** Wednesday, September 27th, 2017 3:30 PM-4:15 PM Room Salon C

Thursday
September
28th, 2017

- ▶ **The ITSI 'Top 20' KPI's:** Thursday, September 28th, 2017 10:30 AM-11:15 AM Room Salon C
- ▶ **Automation of Event Correlation and Clustering with Machine Learning Algorithms – An ITSI Tool:** Thursday, September 28th, 2017 11:35 AM- 12:20 PM Room Salon C
- ▶ **Event Management is Dead. Time Series Events are the Means to the End, not the End Itself. See How Event Analytics is Revolutionizing IT:** Thursday, September 28th 11:35 AM - 12:20 PM in Ballroom B
- ▶ **IT Service Intelligence for When Your Service Spans Your Mainframe and Distributed ITSI:** Thursday, September 28th, 2017 1:20 PM-2:05 PM Room Salon C

Hidden Gems

- ▶ Remember that the MLTK will see any numeric field as a number, not as an entity, so if we want to use date_hour (a number between 0 and 23) we need to change the value into a string (|eval date_hour_string= date_hour ."."_"_t" for example
- ▶ Remember we are predicting the future, so we need to move the target of our regression through time.
- ▶ Remember that your data retention policy means you will lose past data at some point – consider making two models, one with partial_fit and one without and comparing the results.

```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-03" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.0.0.0
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.0.0.0
317 27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.0.0.0
10 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&product_id=KQ-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.0.0.0

```