

splunk> .conf2017

# Automation of Event Correlation and Clustering With Built-In Machine Learning Algorithms in Splunk IT Service Intelligence (ITSI)

Ross Lazerowitz | Product Manager, ITSI

Vineetha Bettaiah | Data Scientist, ITSI

09/08/2017 | 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.

# You Need an Approach That...

Provides easy and seamless access to all data of any type and volume

1 Delivers **service context** to prioritize investigation



2 Understands **time-based behavior** based on historical patterns



Splunk IT Service Intelligence™

3 Helps you find what's broken quickly with human-scale actionable alerts



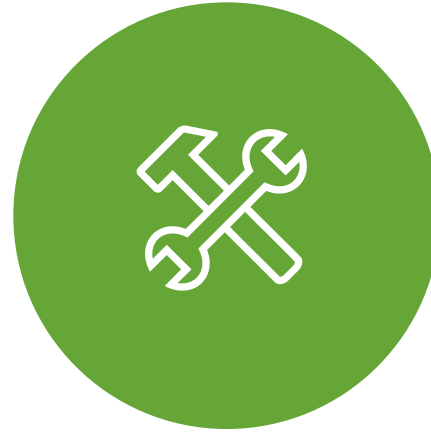
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=FI-SW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product\_id=FL-DSH-01&JSESSIONID=SD35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://shopping.com/cart.do?action=purchase&itemId=EST-268product\_id=KQ-CU-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /category.screen?category\_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=FI-SW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product\_id=FL-DSH-01&JSESSIONID=SD35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://shopping.com/cart.do?action=purchase&itemId=EST-268product\_id=KQ-CU-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /category.screen?category\_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product\_id=FI-SW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product\_id=FL-DSH-01&JSESSIONID=SD35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://shopping.com/cart.do?action=purchase&itemId=EST-268product\_id=KQ-CU-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14

# The Three Pillars of Monitoring Data

ITSI needs to be able to handle all of this in order to be “The Backbone of IT Monitoring”



Logs



Metrics



Events

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-5W-03" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6; rv:53.0) Gecko/20100801 Firefox/53.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF9 HTTP 1.1" 404 3322 "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_6; rv:53.0) Gecko/20100801 Firefox/53.0"
317.27.160.0 - - [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" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6; rv:53.0) Gecko/20100801 Firefox/53.0"
125.17.14.189 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-10&product_id=K9-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6; rv:53.0) Gecko/20100801 Firefox/53.0"
125.17.14.189 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-10&product_id=K9-CW-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6; rv:53.0) Gecko/20100801 Firefox/53.0"
```

# The Three Pillars of Monitoring Data

ITSI needs to be able to handle all of this in order to be “The Backbone of IT Monitoring”



Logs



Metrics



Events

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&JSESSIONID=5D15L9FF1ADFF10 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=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product\_id=K9-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 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product\_id=RP-LI-02"  
125.17 14.1.1.189] "GET /category.screen?category\_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product\_id=RP-LI-02"  
189] "GET /category.screen?category\_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product\_id=RP-LI-02"  
189] "GET /category.screen?category\_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product\_id=RP-LI-02"

# What the Heck is an (IT) Event Anyway?

- ▶ For the purposes of this talk when we say “Event” we are referring to Events in the IT sense not the Splunk sense.
- ▶ Self descriptive message that tells a user that something happened.
- ▶ Usually contain some sort of title, severity, and description.
- ▶ Used to determine in the moment health.
- ▶ Often very noisy.
- ▶ Think alarm data coming out of tools like Nagios, Solarwinds, APM, Netcool, etc.

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "00000000-0000-0000-0000-000000000000"
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://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)" "00000000-0000-0000-0000-000000000000"
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 HTTP 1.1" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "00000000-0000-0000-0000-000000000000"
10.0.0.0 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-14" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "00000000-0000-0000-0000-000000000000"
```

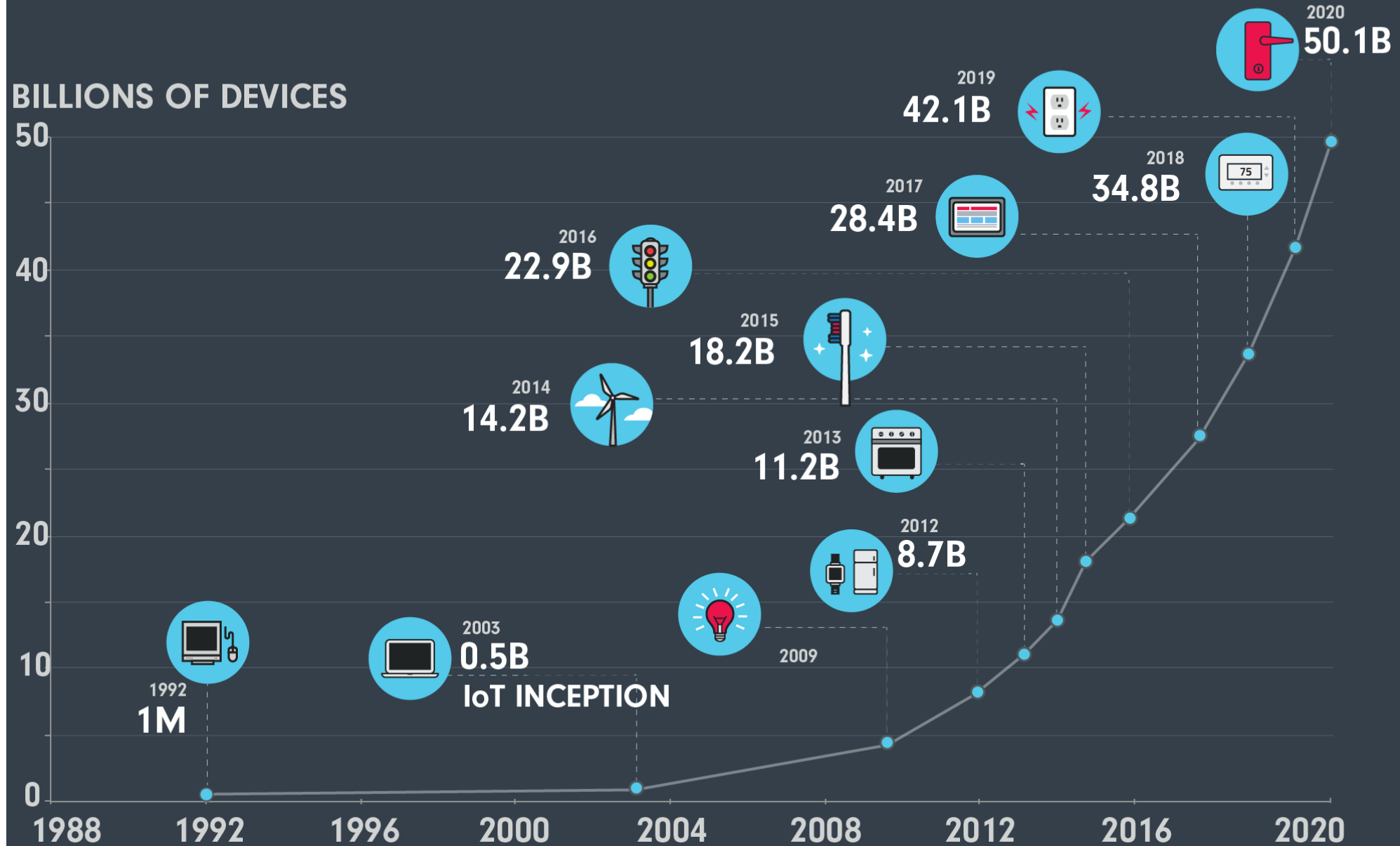
# Example Event

## Nagios Health Check

```
1502642822 src_host="splunk_sh-01" omd_site="SJC"  
perfddata="SERVICEPERFDATA" name="check_dhcp" severity="OK" attempt="1"  
statetype="HARD" executiontime="0.000" latency="0.000" reason="OK: Received 1  
DHCPOFFER(s), max lease time = 600 sec." result="OK"
```

# GROWTH IN THE INTERNET OF THINGS

THE NUMBER OF CONNECTED DEVICES WILL EXCEED **50 BILLION** BY 2020



Source: Cisco

From NCTA: <https://www.ncta.com/positions/internet-of-things>





# The Road to ITSI Event Analytics

## ITSI 2.1

ITSI supports Notable Events.



## .conf 2017

ITSI releases Smart Mode. ITSI can now use machine learning to reduce noise in events.

## .conf 2016

ITSI releases the Policy Engine. Users can curate policies that reduce the noise in events and take automated action.

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-01"  
 128.241.220.82 - [07/Jan 18:10:57:123] "GET /product.category\_id=FL-DSH-01&JSESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://shopping.com/cart.do?action=purchase&itemId=EST-268product\_id=KQ-CW-01"  
 317.27.160.0 - [07/Jan 18:10:56:156] "GET /oldlink?item\_id=EST-26&JSESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product\_id=AV-CB-01&JSESSIONID=5D5L9FF1ADFF3"  
 10.2.1.1:5V1 - [07/Jan 18:10:56:156] "GET /oldlink?item\_id=EST-26&JSESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product\_id=AV-CB-01&JSESSIONID=5D5L9FF1ADFF3"  
 10.2.1.1:5V1 - [07/Jan 18:10:56:156] "GET /category.screen?category\_id=FLOWERS&JSESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product\_id=AV-CB-01&JSESSIONID=5D5L9FF1ADFF3"  
 10.2.1.1:5V1 - [07/Jan 18:10:56:156] "GET /category.screen?category\_id=FLOWERS&JSESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product\_id=AV-CB-01&JSESSIONID=5D5L9FF1ADFF3"

# Splunk ITSI for Event Analytics

## Simplify Your Operations With Artificial Intelligence and Service Context

### Service Context

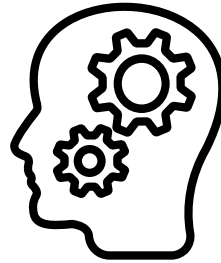


Find and fix the most important issues

Contextualize and prioritize

Reduce time-to-resolution on business-critical services

### Artificial Intelligence



Transform IT operations with machine learning

Separate valuable signal in noise

Enable IT with intelligence for data-driven decisions

### Scalable Platform



Get a full view of your IT environment

Respond collaboratively and simplify operations

Share customized insights across the enterprise to enable business-centric IT



# Under the hood

---

Vineetha Bettaiah

# Objective

To identify all ideal groups of similar events

- ▶ Input – Set of events
- ▶ Features – Each event has a number of attribute fields (topological, numerical, text, etc)
- ▶ Output – List of ideal groups with characteristic metadata of each group

Group 1  
Metadata

name = "check\_dhcp"  
severity = "OK"  
reason = "OK: Received 1 DHCPOFFER(s)"

Group 2  
Metadata

src\_host="splunk\_sh-01"  
statetype="HARD"

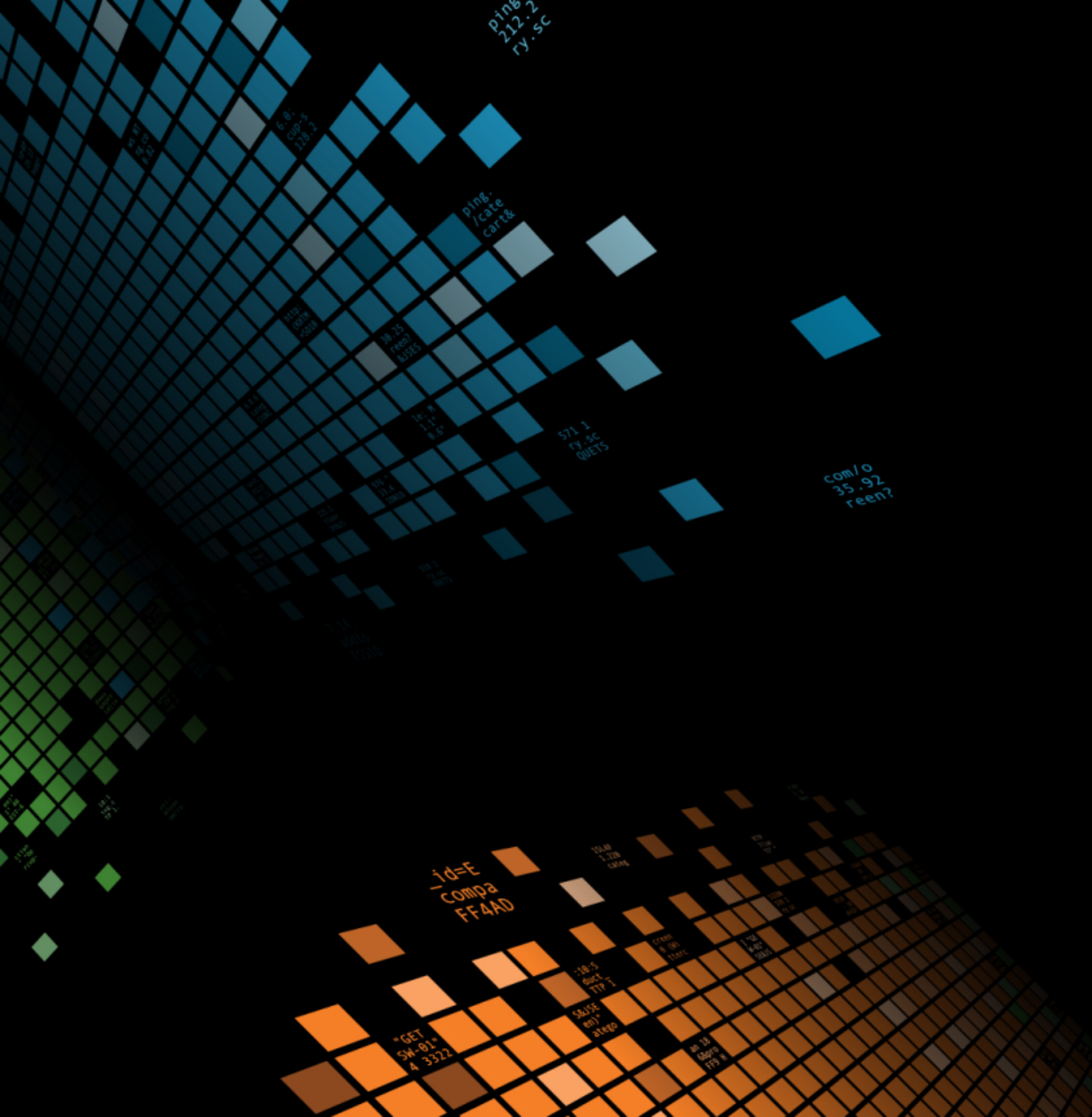
# This is not easy

Big O is not your friend

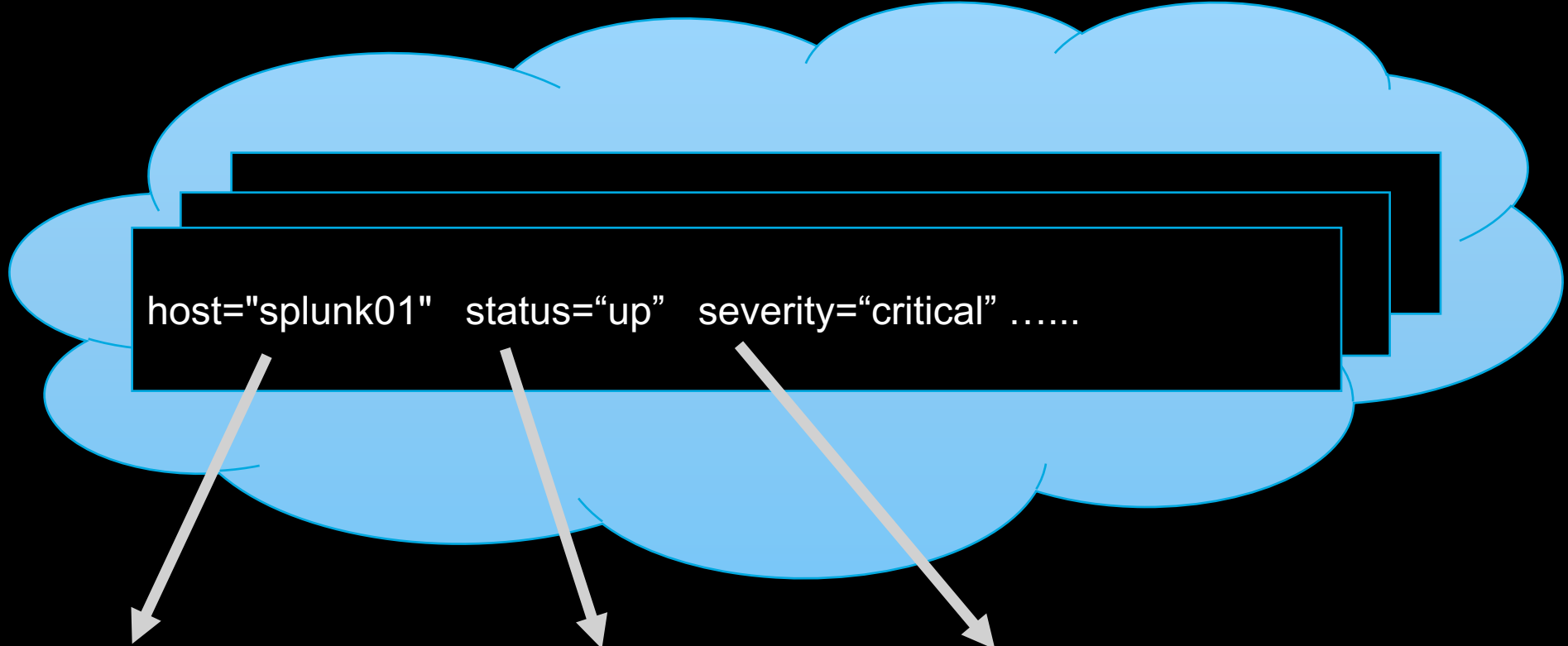
- ▶ The computational complexity is exponential
  - Number of event feature fields = 78
  - Number of possible feature values = 4
  - Number of possible groupings =  $2^{80}$
- ▶ An event can belong to many groups
- ▶ Brute force is not a practical approach for real time data

# Approach and Algorithm

---



# Step 1- Feature Extraction



```
host="splunk01" status="up" severity="critical" .....
```

```
host={splunk01, splunk02, ...}status={up, down} severity={low, medium, critical} .....
```

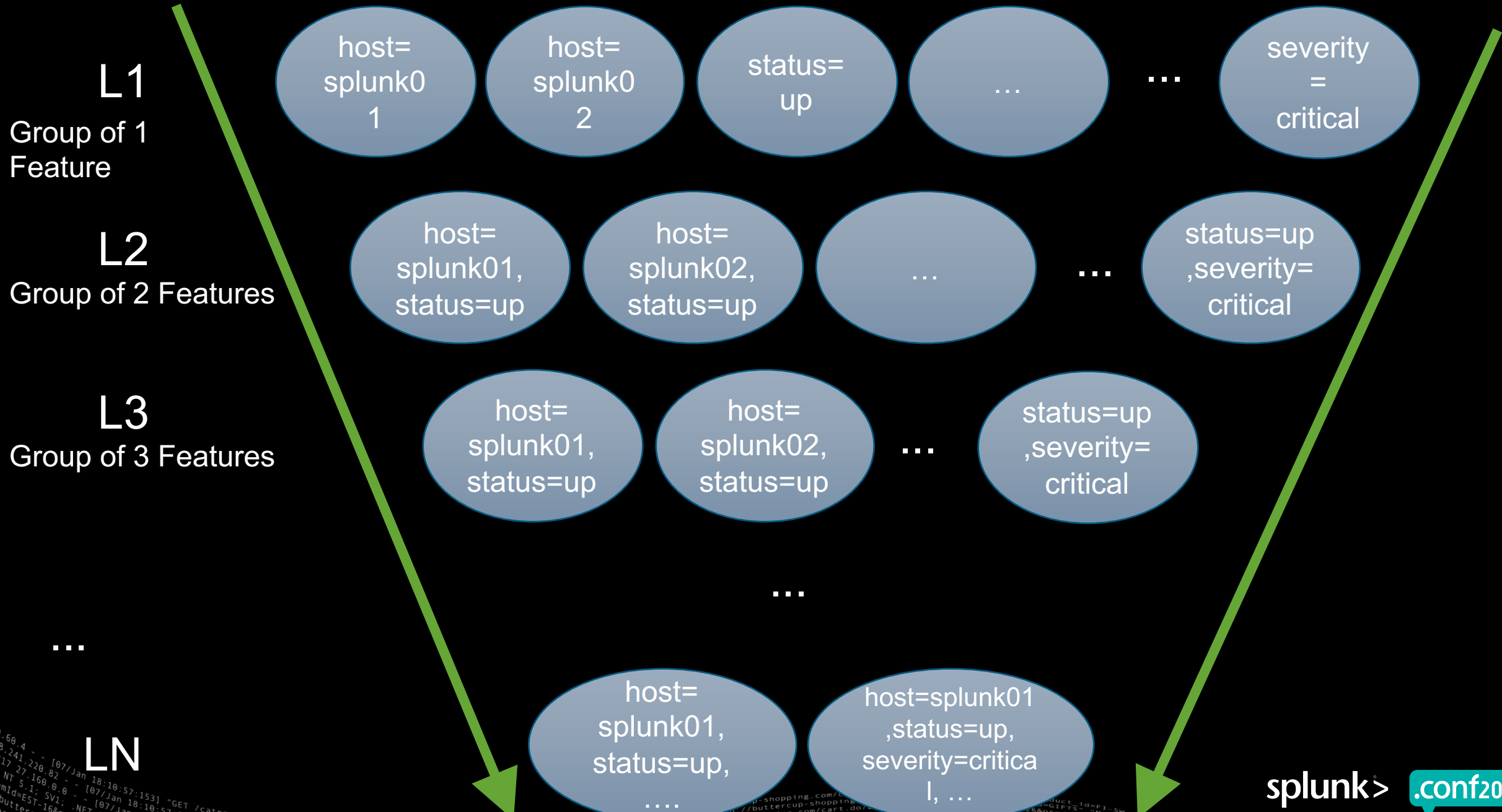


```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD15L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" Opera/9.80...  
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/category.screen?category_id=GIFTS" Mozilla/4.0...  
ows NT 5.1; SV1: - - [07/Jan 18:10:56:150] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-6&product_id=FL-SW-01" Opera/9.80...  
: //buttercup-shopping.com/product_id=RP-LI-02" 468 125.17.14.101 "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-6&product_id=FL-SW-01" Opera/9.80...  
: //buttercup-shopping.com/product_id=RP-LI-02" 468 125.17.14.101 "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-6&product_id=FL-SW-01" Opera/9.80...  
: //buttercup-shopping.com/product_id=RP-LI-02" 468 125.17.14.101 "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD10SL9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/category.screen?category_id=FLOWERS&JSESSIONID=SD55L7FF6ADFF9 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-6&product_id=FL-SW-01" Opera/9.80...
```

# Step 2 – Reverse Pyramid Clustering

---





# Step 3 – Backtracking

---









# Splunk Demo

---

Presented by Buttercup Splunker

# The principles behind a successful ML feature

This is where the subtitle goes

## Explainability

The feature should be able to clearly explain to the analyst any inferences made.

## Configurability

The feature should be easy to configure and tune by users of different technical abilities.

## Extensibility

The feature should be extensible so that it can be quickly iterated upon.

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category\_id=GIFTS&SESSIONID=5D55L9FF1ADFF3 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&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product\_id=KQ-CW-01"  
10.0.0.1 - - [07/Jan 18:10:56:156] "GET /oldlink?item\_id=EST-26&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product\_id=AV-CB-01&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-189" "GET /category.screen?category\_id=FLOWERS&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268&product\_id=KQ-CW-01"



# The ITSI way

This is where the subtitle goes

## Explainability

Every group that is discovered includes a human readable explanation of how it came to be.

## Configurability

ITSI provides a UI that lets non-Data Scientists tune the algorithm's parameters.

## Extensibility

Smart Mode is built on top of a Machine Learning Engine, on which additional “Factors” will be added over time.

```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D5$L9FFIADFF3 HTTP 1.1" 404 322 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D5$L9FFIADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D5$L9FFIADFF3 HTTP 1.1"
137.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D5$L9FFIADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D5$L9FFIADFF3 HTTP 1.1"
137.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D5$L9FFIADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D5$L9FFIADFF3 HTTP 1.1"
137.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D5$L9FFIADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D5$L9FFIADFF3 HTTP 1.1"
137.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D5$L9FFIADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D5$L9FFIADFF3 HTTP 1.1"
137.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D5$L9FFIADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D5$L9FFIADFF3 HTTP 1.1"
137.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D5$L9FFIADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D5$L9FFIADFF3 HTTP 1.1"
137.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D5$L9FFIADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D5$L9FFIADFF3 HTTP 1.1"
137.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D5$L9FFIADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D5$L9FFIADFF3 HTTP 1.1"
```

# Q&A

---

Participant name | Role

Participant name | Role