



See What's New With Splunk Business Flow

Lizzy Li
Product Manager | Splunk

splunk>

.conf19

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. © 2019 Splunk Inc. All rights reserved.

Imagine:

You work for an **online retail** company

It's **Black Friday/Cyber Monday** weekend

It's **your job** to ensure the surge in orders processes successfully

Are you able to answer:

“Are customers **dropping off** before purchasing?”

“What do incomplete purchases have **in common**?”

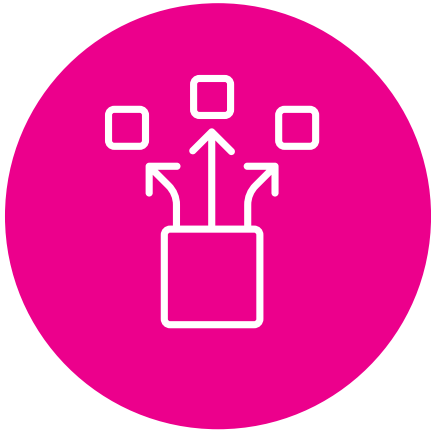
“Are orders being **processed successfully**?”

“Where are the **delays** during order processing?”

“Is there an increase in **cancelled orders**?”

“Is something in our process causing **errors** in customer orders?”

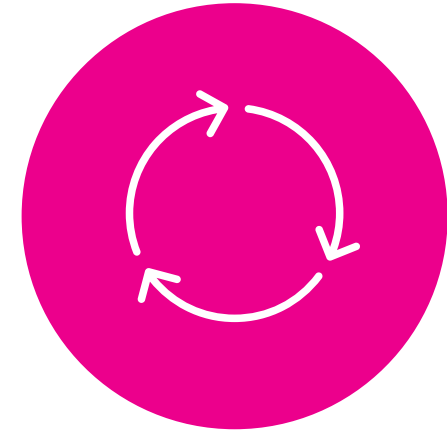
Gaining Transparency Into Complex, High Volume Processes is Challenging



Data spans disparate
systems, difficult to
collect



Processes lack real-time
visibility, slow feedback
loop



Processes are fluid,
need to constantly
update and model data

What if Your Data Could Tell You...



If processes are
actually operating
as expected



Which processes
are incomplete
or delayed

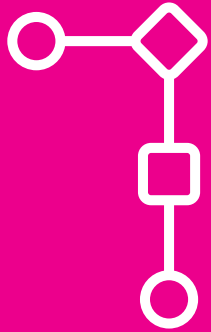


How conversion
rates and
performance differ
between cohorts



If processes are
deviating out of
conformance

Introducing Splunk Business Flow



End-to-end process
discovery through
event stitching



Investigate
drill-down with
exploration interface



Side-by-side
A/B comparison
of process flows



Conformance
checking and
deviation notifications

SPLUNK BUSINESS FLOW

splunk>enterprise

splunk>cloud™

Key Concepts & Terminology

- ▶ **Flow Model**

the definition of a business process (e.g. Customer Activation, Order to Fulfillment); includes SPL and field names to stitch together timestamped events

- ▶ **Flow**

a saved view of a Flow Model; includes filters, metrics, conversion funnels, A/B comparisons, and more

- ▶ **Journey**

a specific instance of a multi-event flow where related events have been grouped into an ordered sequence



New Search

Save As

Close

```
index=sbf1 source=equitytrading.csv
| search ("TradeID"="L*")
| fields "_time" "Step" "TradeID" "Amount" "ClientID" "CounterPartyID" "Limit Price" "Order Type" "Purchase Price" "Remaining"
  "Symbol" "Time" "TradeID" "TraderID" "Volume"
| sort + _time
```

Date time range



✓ 530 events (1/3/19 9:15:59.000 AM to 1/3/19 9:16:18.000 AM) No Event Sampling

Job



Smart Mode

Events

Patterns

Statistics (530)

Visualization

20 Per Page

Format

Preview

< Prev

1

2

3

4

5

6

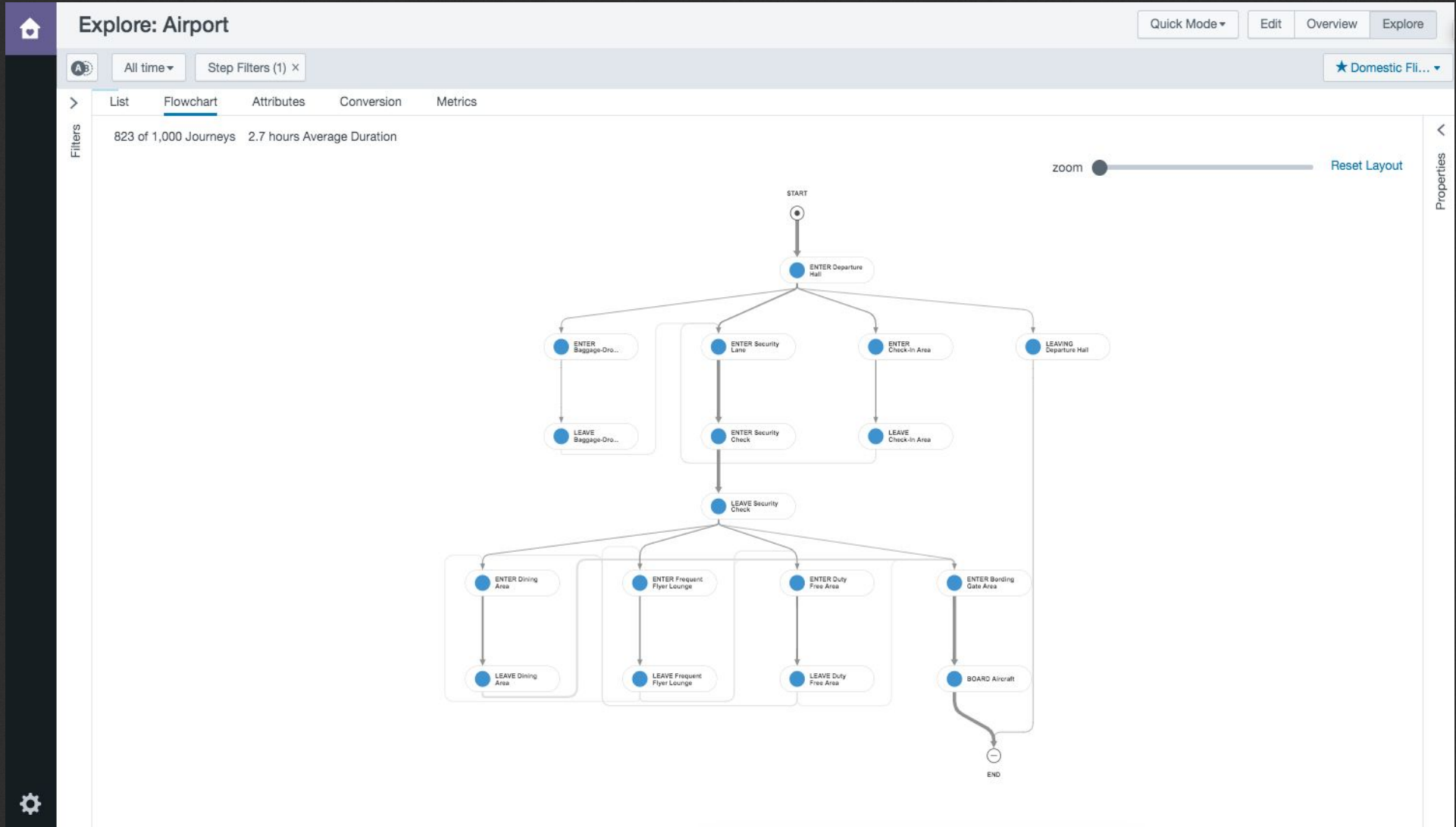
7

8

...

Next >

	Step	TradeID	Amount	ClientID	CounterPartyID	Limit Price	Order Type	Purchase Price	Remaining	Symbol	Time	TraderID
01-03 09:15:59	Unfilled Order	L99235366		HSGDK103104		170	Limit Order		1750	FB	01/03/2019 09:15:59	TRDR144
01-03 09:15:59	Order Expiry	L9762228		HSGDK103739		175	Limit Order		2650	AAPL	01/03/2019 09:15:59	TRDR123
01-03 09:15:59	Sell	L97591482		HSGDK101085		25	Limit Order		400	QLIK	01/03/2019 09:15:59	TRDR140
01-03 09:15:59	Unfilled Order	L97113498		HSGDK102315		170	Limit Order		3950	FB	01/03/2019 09:15:59	TRDR110
01-03 09:15:59	Sell	L94454954		HSGDK103913		170	Limit Order		1200	FB	01/03/2019 09:15:59	TRDR116



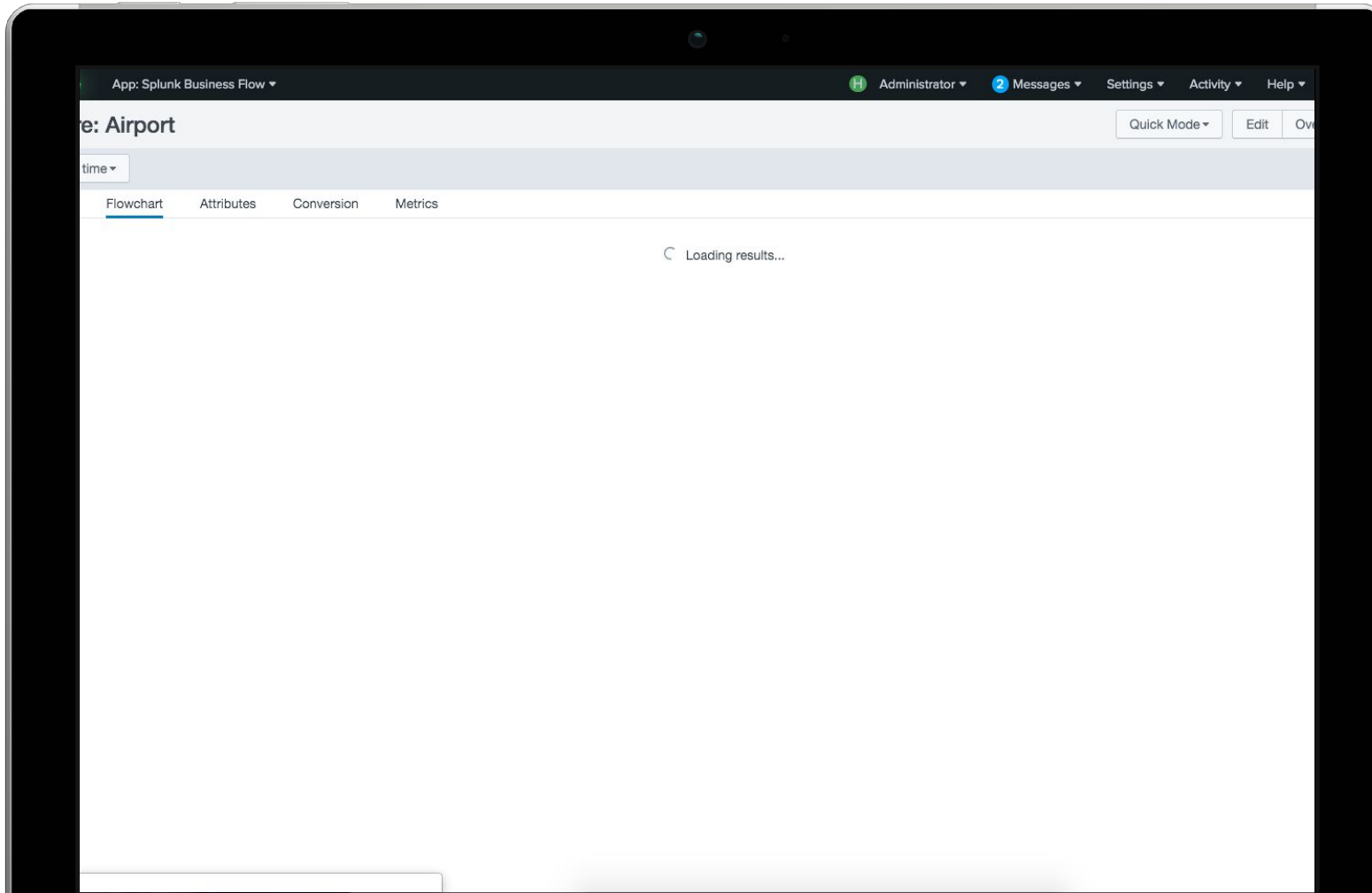
Cloud Accelerated Flow Models

Beta program



When data sets are really, really big

Journey visualization becomes computationally intensive



It becomes computationally intensive to:

- ▶ Stitch millions of events into journeys
- ▶ View events over months or years
- ▶ Constantly filter to slice and dice data

Introducing Cloud Accelerated Flow Models

With SBF

- ▶ For most use cases (100,000s of events)
- ▶ SBF today provides instant, interactive investigation
- ▶ Executes search and event stitching on demand

With SBF + CAFM

- ▶ For computationally intensive use cases (millions of events)
- ▶ CAFM enables preprocessing
- ▶ Accelerates journey visualization through columnar data storage

Sign up for the beta in three easy steps



Contact your rep
about SBF's beta
performance feature



Sign up for the beta:
<http://bit.ly/2kjBoXm>



The fun begins

Notifications



Back at your job at the online retailer, can you tell me when:

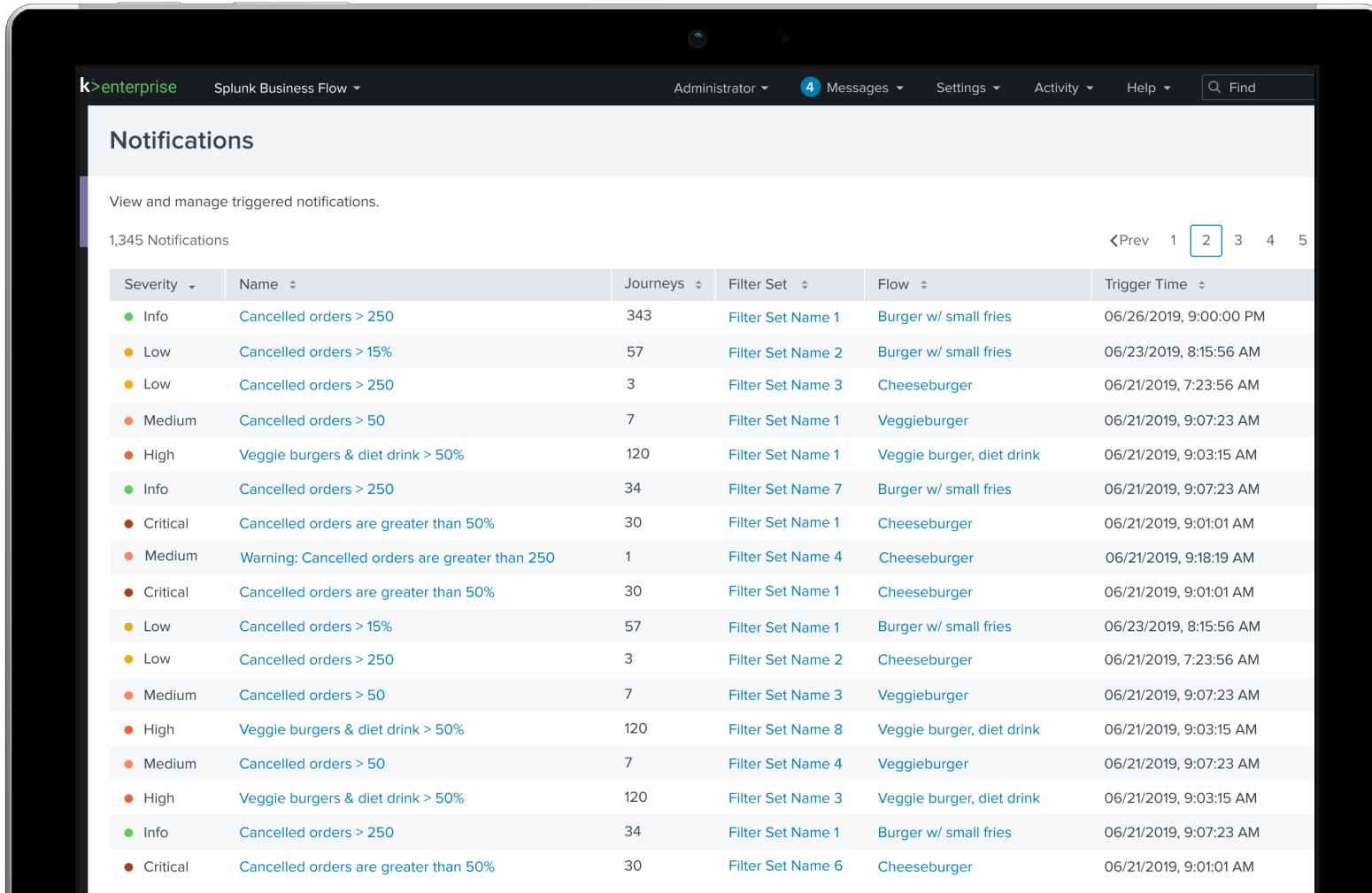
“The **shopping cart abandonment rate** exceeds 30%?”

“The average order processing time **takes longer** than 2 minutes?”

“**Cancelled orders** exceeds 15% of orders placed?”

Notifications

Be notified when your processes meet certain conditions



The screenshot shows the Splunk Business Flow interface. The top navigation bar includes the Splunk logo, 'Splunk Business Flow', and user roles like 'Administrator'. A 'Messages' tab is active, showing 4 messages. The main section is titled 'Notifications' and contains a table of triggered notifications. The table has columns for Severity, Name, Journeys, Filter Set, Flow, and Trigger Time. The first row shows an 'Info' severity notification for 'Cancelled orders > 250' with 343 journeys, triggered on 06/26/2019 at 9:00:00 PM. The table is paginated, showing 1,345 notifications in total.

Severity	Name	Journeys	Filter Set	Flow	Trigger Time
Info	Cancelled orders > 250	343	Filter Set Name 1	Burger w/ small fries	06/26/2019, 9:00:00 PM
Low	Cancelled orders > 15%	57	Filter Set Name 2	Burger w/ small fries	06/23/2019, 8:15:56 AM
Low	Cancelled orders > 250	3	Filter Set Name 3	Cheeseburger	06/21/2019, 7:23:56 AM
Medium	Cancelled orders > 50	7	Filter Set Name 1	Veggieburger	06/21/2019, 9:07:23 AM
High	Veggie burgers & diet drink > 50%	120	Filter Set Name 1	Veggie burger, diet drink	06/21/2019, 9:03:15 AM
Info	Cancelled orders > 250	34	Filter Set Name 7	Burger w/ small fries	06/21/2019, 9:07:23 AM
Critical	Cancelled orders are greater than 50%	30	Filter Set Name 1	Cheeseburger	06/21/2019, 9:01:01 AM
Medium	Warning: Cancelled orders are greater than 250	1	Filter Set Name 4	Cheeseburger	06/21/2019, 9:18:19 AM
Critical	Cancelled orders are greater than 50%	30	Filter Set Name 1	Cheeseburger	06/21/2019, 9:01:01 AM
Low	Cancelled orders > 15%	57	Filter Set Name 1	Burger w/ small fries	06/23/2019, 8:15:56 AM
Low	Cancelled orders > 250	3	Filter Set Name 2	Cheeseburger	06/21/2019, 7:23:56 AM
Medium	Cancelled orders > 50	7	Filter Set Name 3	Veggieburger	06/21/2019, 9:07:23 AM
High	Veggie burgers & diet drink > 50%	120	Filter Set Name 8	Veggie burger, diet drink	06/21/2019, 9:03:15 AM
Medium	Cancelled orders > 50	7	Filter Set Name 4	Veggieburger	06/21/2019, 9:07:23 AM
High	Veggie burgers & diet drink > 50%	120	Filter Set Name 3	Veggie burger, diet drink	06/21/2019, 9:03:15 AM
Info	Cancelled orders > 250	34	Filter Set Name 1	Burger w/ small fries	06/21/2019, 9:07:23 AM
Critical	Cancelled orders are greater than 50%	30	Filter Set Name 6	Cheeseburger	06/21/2019, 9:01:01 AM

- ▶ Define conditions with filter sets
- ▶ Specify journey count threshold and severity
- ▶ View notifications and drill into journeys

Learn More About Splunk Business Flow

BA2642 Technical Overview: How we used Splunk Business Flow at Splunk

BA1191 Driving More Sales at Deutsche Bahn: DB Systel's Journey Mapping With Splunk Business Flow

BA2138 Technical Workshop: Business Analytics with Splunk Business Flow



**Thank
You!**

Go to the .conf19 mobile app to

**RATE THIS
SESSION**