

# BA1529

## Splunk Business Flow + Splunk Connect for Kubernetes = Happy Containers

Tom Martin  
Staff Practitioner | Splunk

Matt Modestino  
Staff Practitioner | Splunk

**Session ID:**

BA1529

**Session Title:**

BA1529 - Splunk Business Flow + Splunk Connect for Kubernetes = Happy Containers

**Session Abstract:**

Splunk Business Flow.



**Tom Martin**  
Staff Practitioner | Splunk



**Matt Modestino**  
Staff Practitioner | Splunk

# Forward-Looking Statements



During the course of this presentation, we may make forward-looking statements regarding future events or plans 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 may differ materially. 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, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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 functionalities described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Turn Data Into Doing, 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.

# Today's Agenda

////////////////////

**.conf19**

Las Vegas, Nevada

October 21-24

- 1) **Splunk for Kubernetes (SCK)**
- 2) **SCK Demo**
- 3) **Splunk Business Flow (SBF)**
- 4) **SBF with SCK data Demo**
- 5) **Q&A**

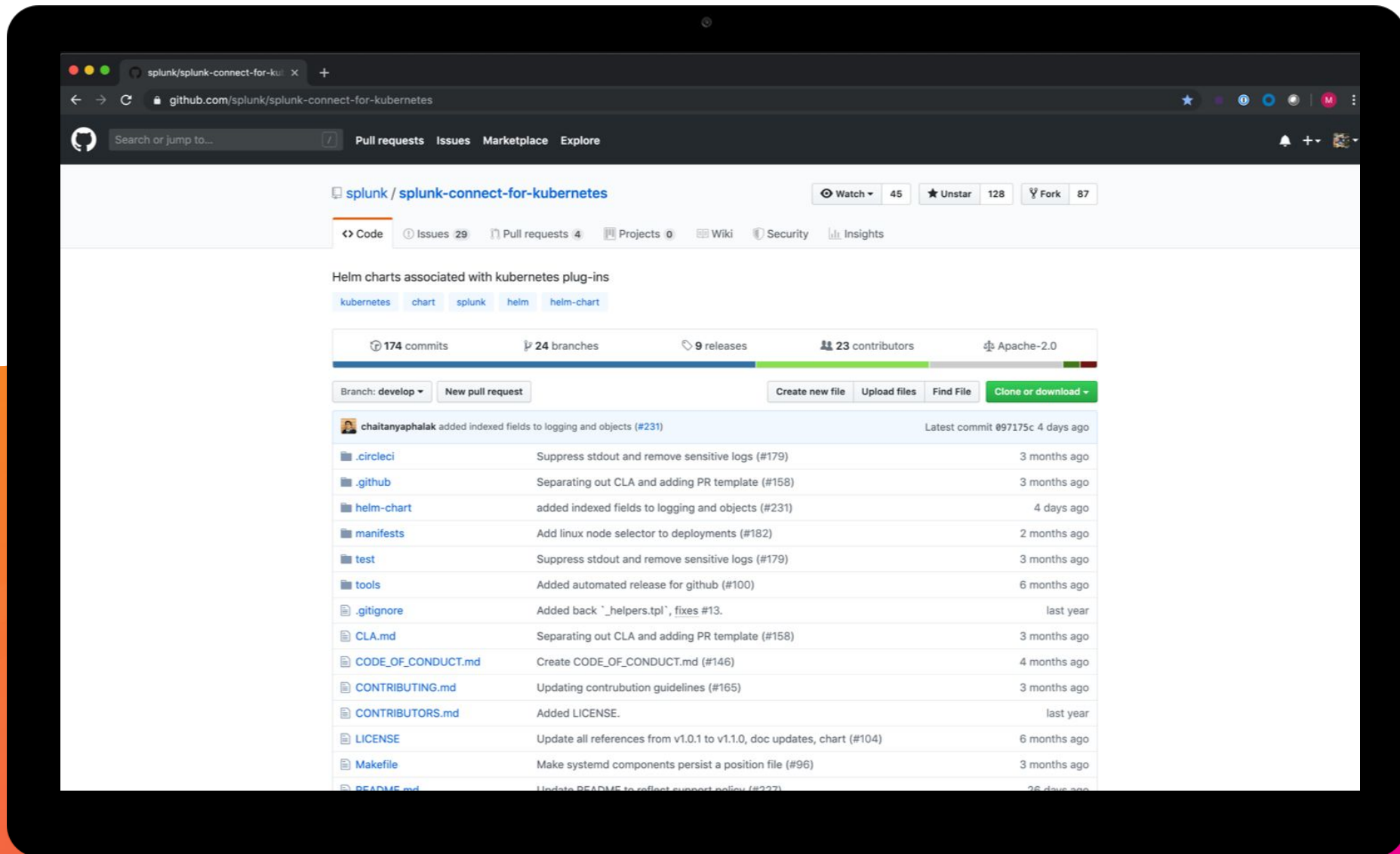




# Splunk Connect for Kubernetes

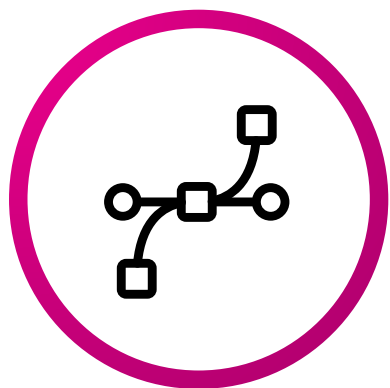
---

Kubernetes Data Collection by Splunk  
& the Opensource Community!



# Splunk Connect for Kubernetes

## Kubernetes Data Sources



Splunk Kubernetes  
Logging



Splunk Kubernetes  
Metrics



Splunk Kubernetes  
Objects



# Splunk Kubernetes Logging

Application & OpenShift Cluster Logging



kubernetes

Docker/CRI-O Logs

Journald

Kubernetes API Audit Logs

Custom Log Sources



fluentd

in\_tail

systemd

jq\_transformer

fluentd-hec

splunk®>

HTTP Event Collector

Event Index

# Splunk Kubernetes Objects

OpenShift Metadata Collection



Kubernetes API



kubernetes\_objects  
jq\_transformer  
fluentd-hec



HTTP Event Collector  
Event Index

# Splunk Kubernetes Metrics

OpenShift Platform Metrics



Kubernetes API  
Kubelet



kubernetes\_metrics  
kubernetes\_metrics\_aggregat  
or  
record\_modifier  
fluentd-hec



HTTP Event Collector  
Metrics Index

# Splunk Connect for Kubernetes

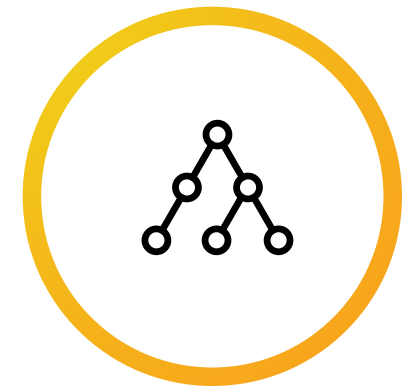
Business Flow Use



Kubernetes API Audit



Kubernetes Events API



Microservice Logging

# Demo



The screenshot shows a web browser window with the URL `i-02782275744fca325.ec2.splunkit.io:8000/en-US/app/splunk_app_infrastructure/configure`. The page title is "Configure Integrations" for the "Splunk App for Infrastructure". The left sidebar lists integration options: Linux/Unix, AWS, Windows, OSX, Kubernetes, and OpenShift (which is selected). The main content area for OpenShift includes instructions to monitor the deployment and two numbered steps:

- 1 Prepare for deployment**

Install the [Helm client](#) and [OpenShift Container Platform CLI](#) on a local machine you'll use to set up data collection.

The script runs the `helm template` command to render manifests locally. The script does not attempt to install Tiller on your cluster to deploy manifests.

**Download Config Only** ☒ This option generates manifests but does not deploy them. If you enable this option, you have to manually deploy the manifests.
- 2 Specify configuration options**

**Data to be collected** ☒ 2 Objects [Customize Objects](#)

**Monitoring machine**   
Specify the FQDN or IP address of the system you want to send data to. Do not enter a hostname.

**HEC token**   
Enter the HEC token you configured to send data to the app. The HEC token's sourcetype must be `em_metrics`. [Global HEC settings must have tokens enabled.](#)

**HEC port**   
Enter the HEC port of the system you want to send metrics data to. The recommended port is 8088.

**Cluster name**



# Splunk Business Flow

---

What is Process Mining?

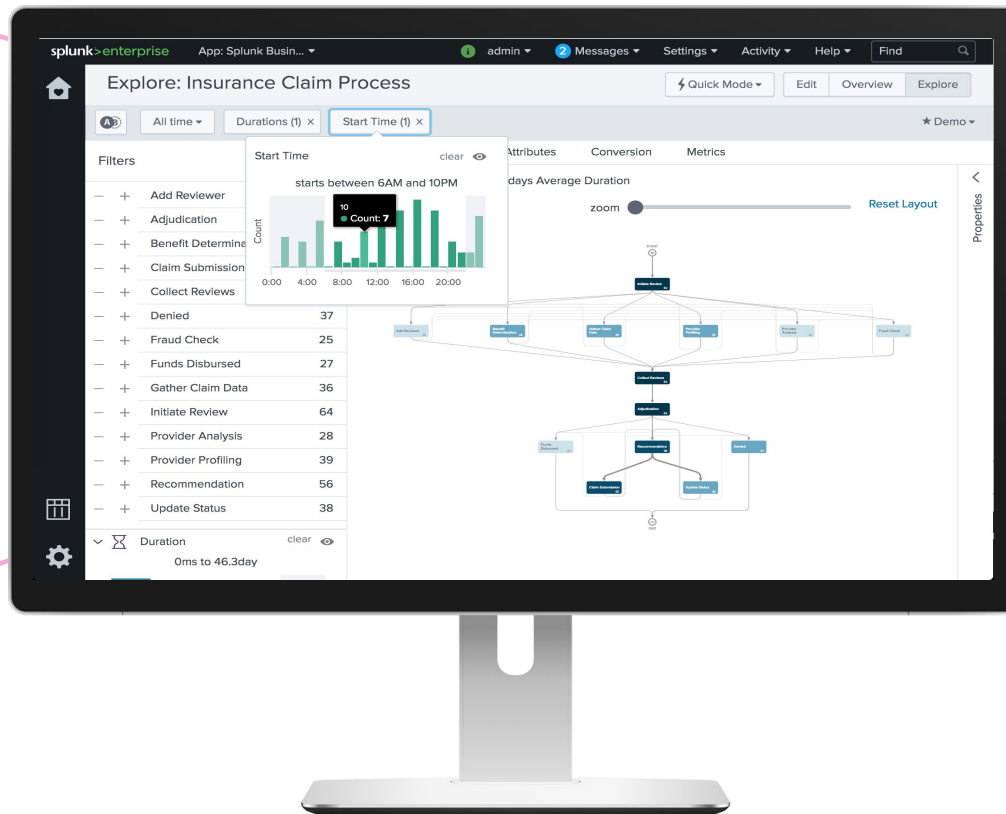
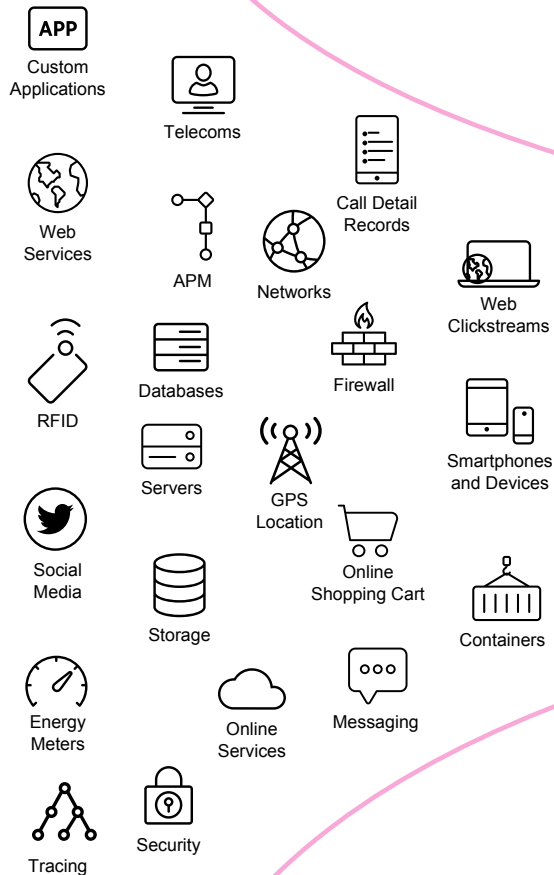
<http://www.processmining.org/>

# Splunk Business Flow enables process mining using your existing data in Splunk!



because your data can tell stories...

# Splunk Can Mine Your Existing Data to Better Understand Your Business



Faster cycle times  
of critical business  
processes

Higher conversion  
rates of critical  
customer experiences

More consistent  
achievement of  
service delivery

# 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™

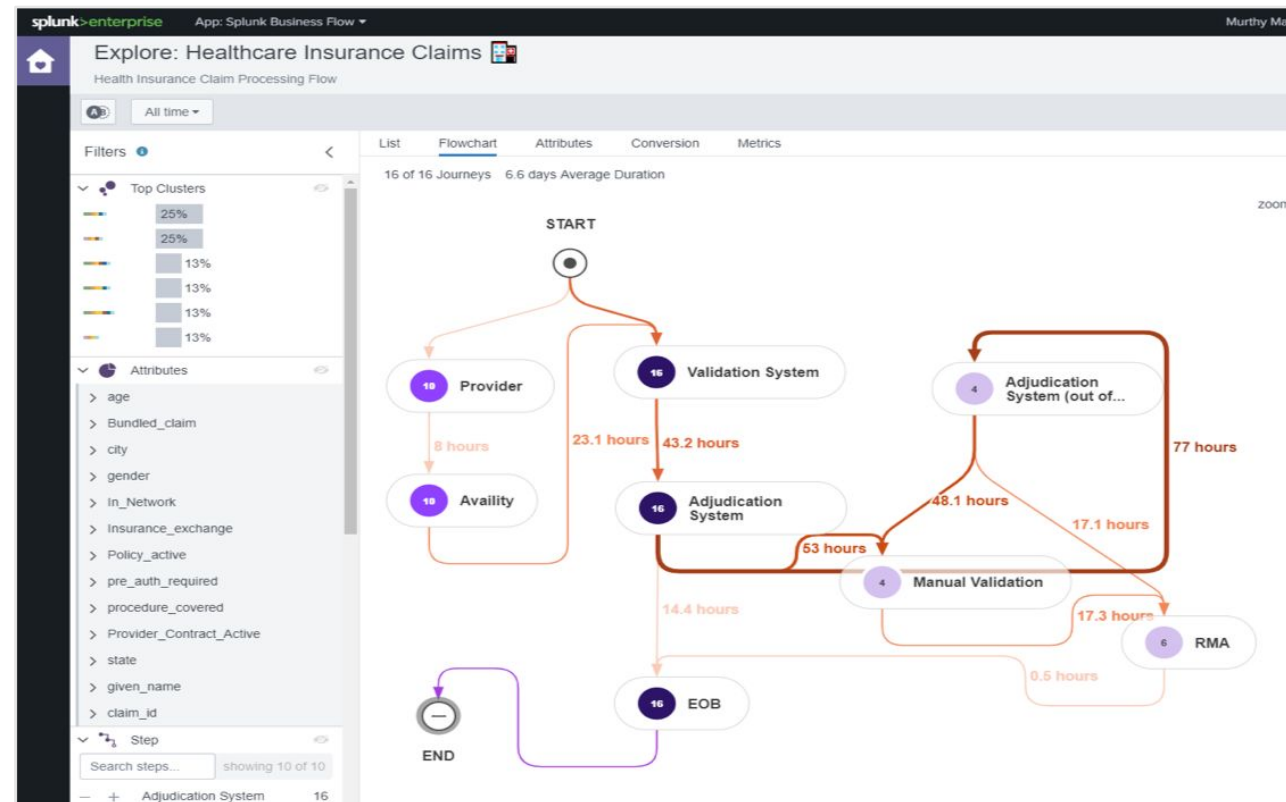


# Splunk Business Flow

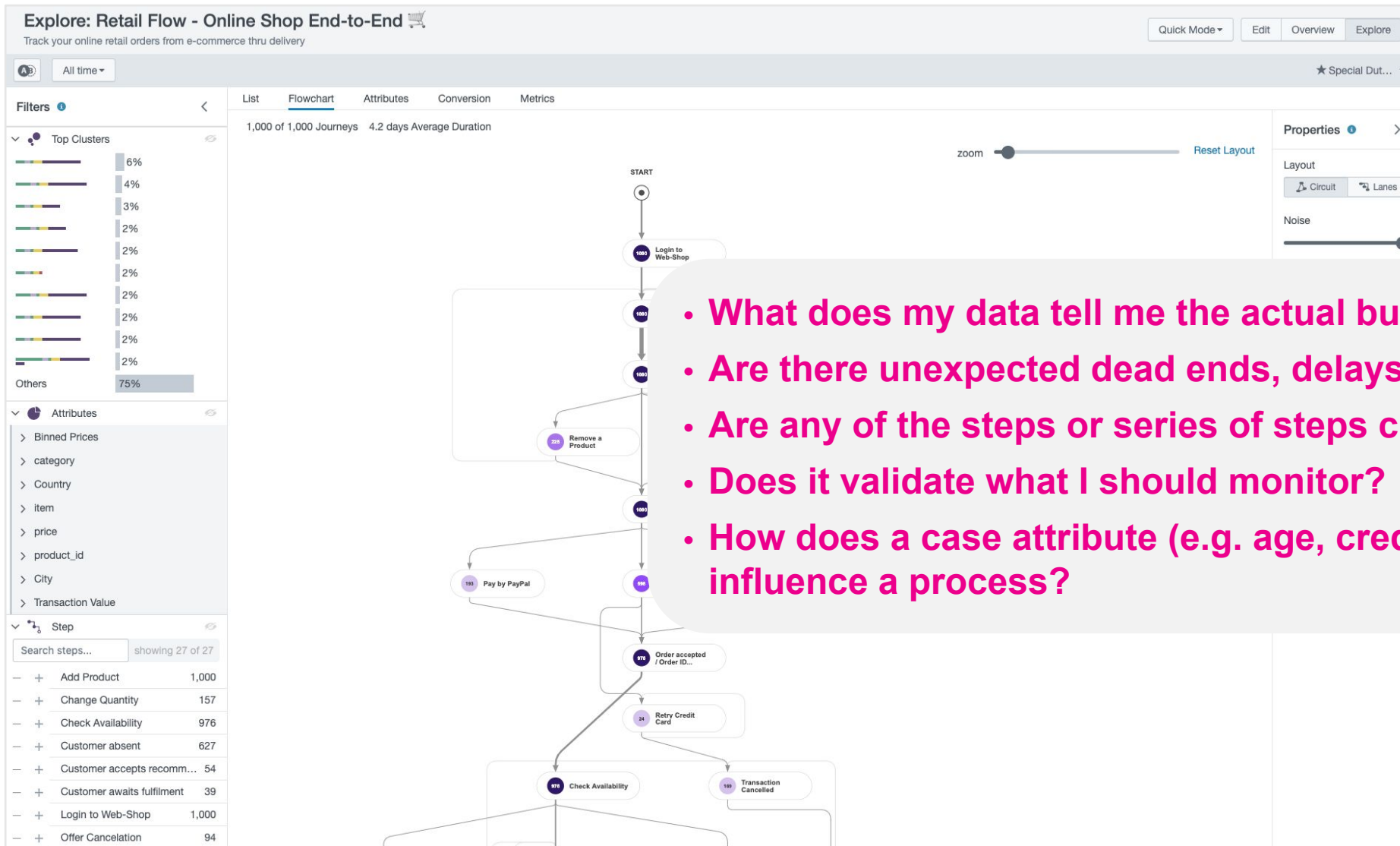
Splunk Business Flow is a fast, flexible, and intuitive process mining solution for interactive discovery, investigation, and conformance checking of any business process

## Premium application on top of Splunk platform

- Quickly discover and identify anomalous pathways in any existing end-to-end business processes
- Easily explore the impact of planned changes and investigate the root causes of unplanned, incomplete or delayed processes
- Determine conformance of actual processes against reference processes and performance thresholds (new for October 2019!)



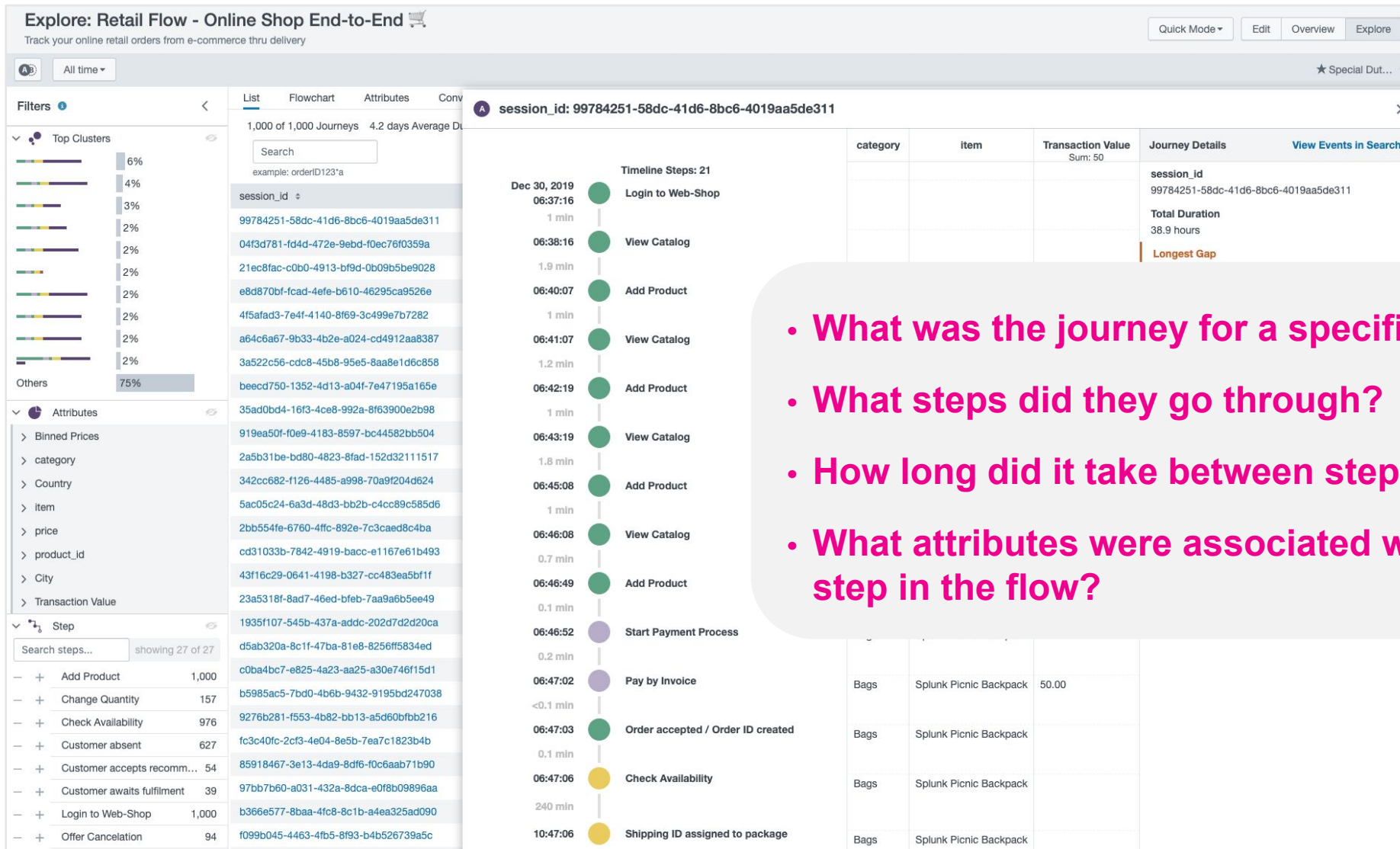
# Process Discovery



## Flowchart Tab

- What does my data tell me the actual business process is?
- Are there unexpected dead ends, delays, loops, variances?
- Are any of the steps or series of steps creating a bottleneck?
- Does it validate what I should monitor?
- How does a case attribute (e.g. age, credit score, geography) influence a process?

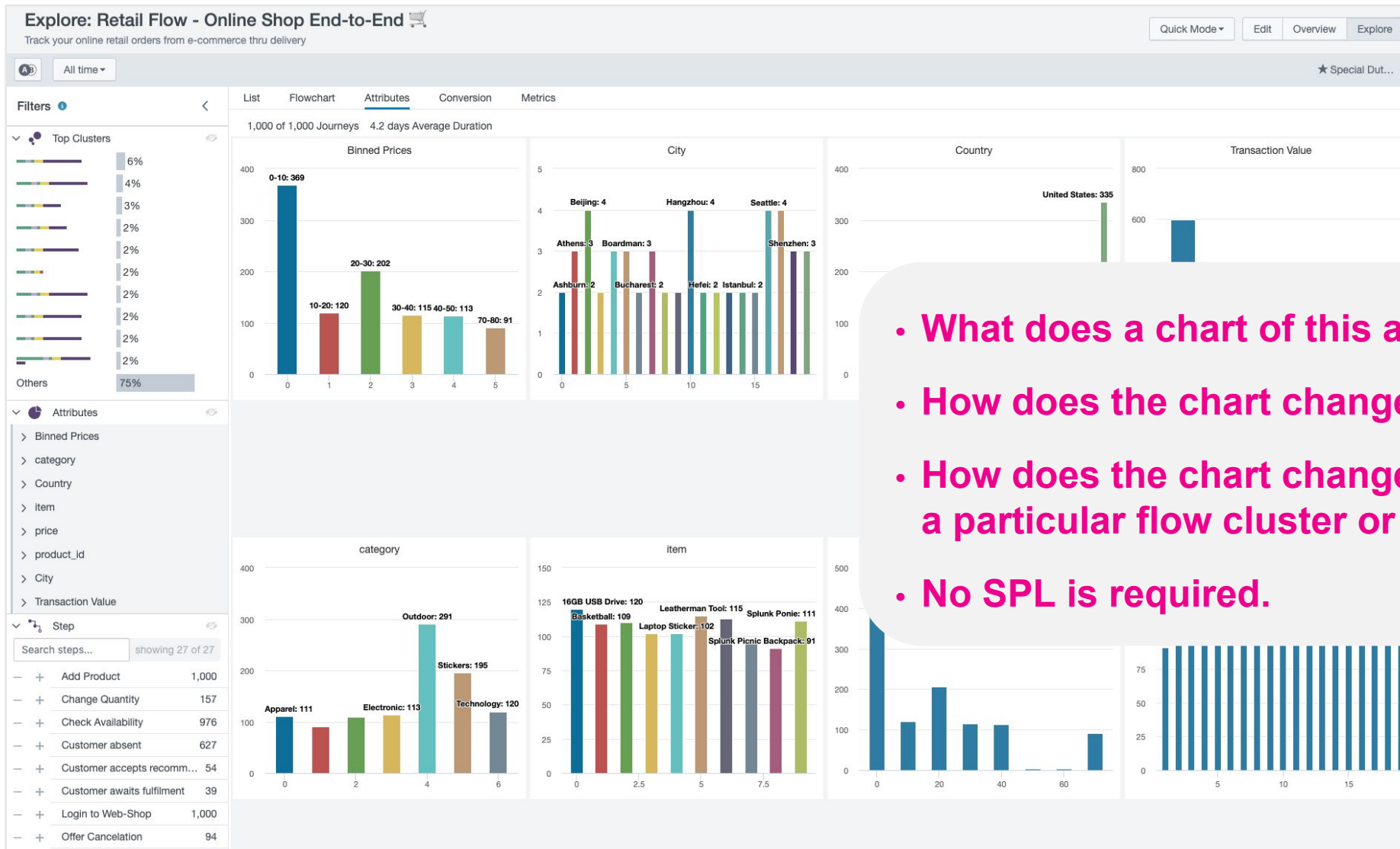
# Investigation & Troubleshooting



## List Tab

- What was the journey for a specific case or customer?
- What steps did they go through?
- How long did it take between steps?
- What attributes were associated with this case at each step in the flow?

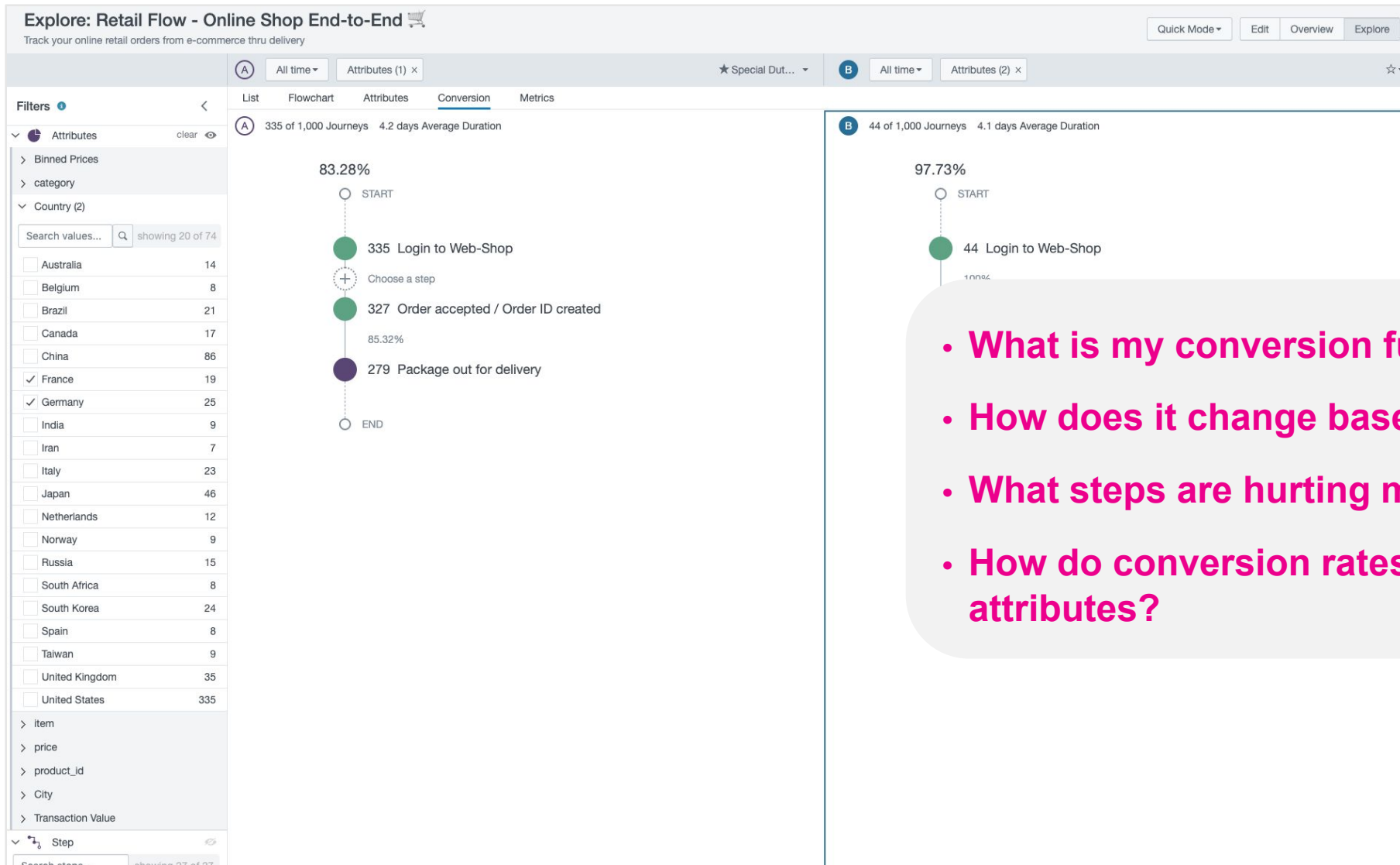
# Segmentation and Analysis



## Attributes Tab

- What does a chart of this attribute look like?
- How does the chart change if I filter the data?
- How does the chart change if I filter the data by a particular flow cluster or series of steps?
- No SPL is required.

# Conversions, Churn & Comparisons



## Conversion Tab

- What is my conversion funnel?
- How does it change based on the mix of steps?
- What steps are hurting my conversion rates?
- How do conversion rates vary based on different attributes?



# Infrastructure Journeys



Analyzing the Kubernetes  
Object Lifecycles

# Visualize and Observe Kubernetes Object Lifecycles and Developer Usage of the Kubernetes API



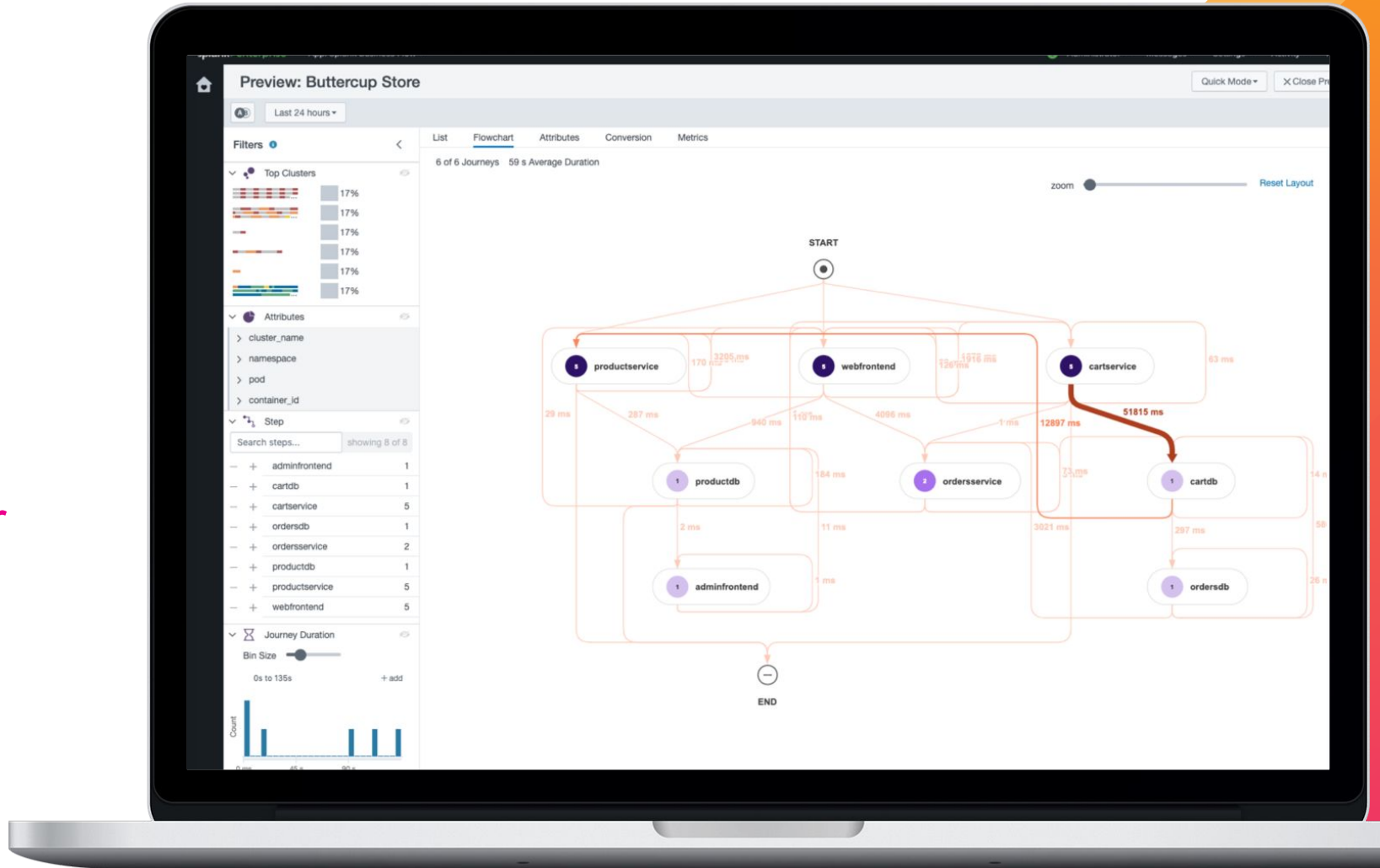
# Analyzing User Journeys Using Application Logging



Analyzing user journeys using Application Logging

## Visualize & Observe your user journeys present in Application Logging

## Visualize & Observe your user journeys present in Application Logging







# Demo: SBF for k8s

---

A study of Kubernetes Clusters



# SCK + SBF

Making sense of your  
Kubernetes world

1. SCK to capture
  - Audit Events
  - Object Events
  - Application Log Events
2. SBF to visualize
  - Changes / Updates
  - Infrastructure
  - Applications



# Q&A

---



splunk>

# Thank

# You



Go to the .conf19 mobile app to

**RATE THIS SESSION**

