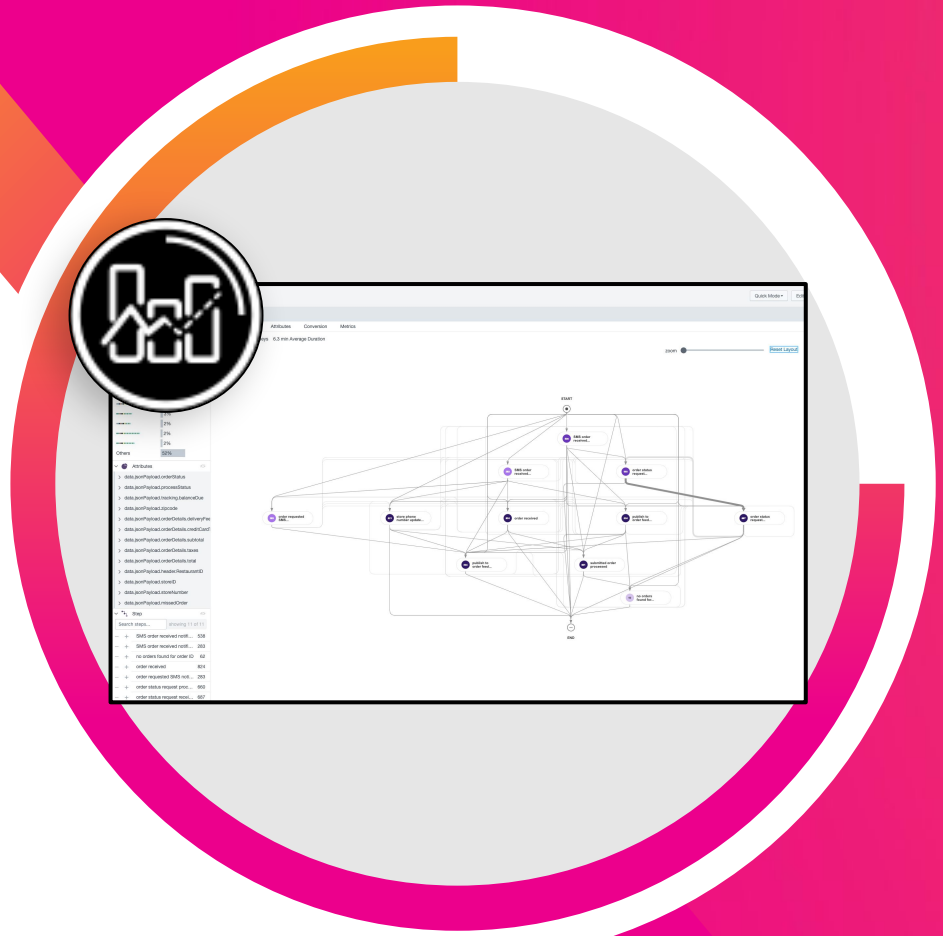


BA1529

Splunk Business Flow + Splunk Connect for Kubernetes = Happy Containers

Tom Martin
Staff Practitioner | Splunk

Matt Modestino
Staff Practitioner | Splunk

splunk> .conf19

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

splunk> .conf19

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.

Today's Agenda

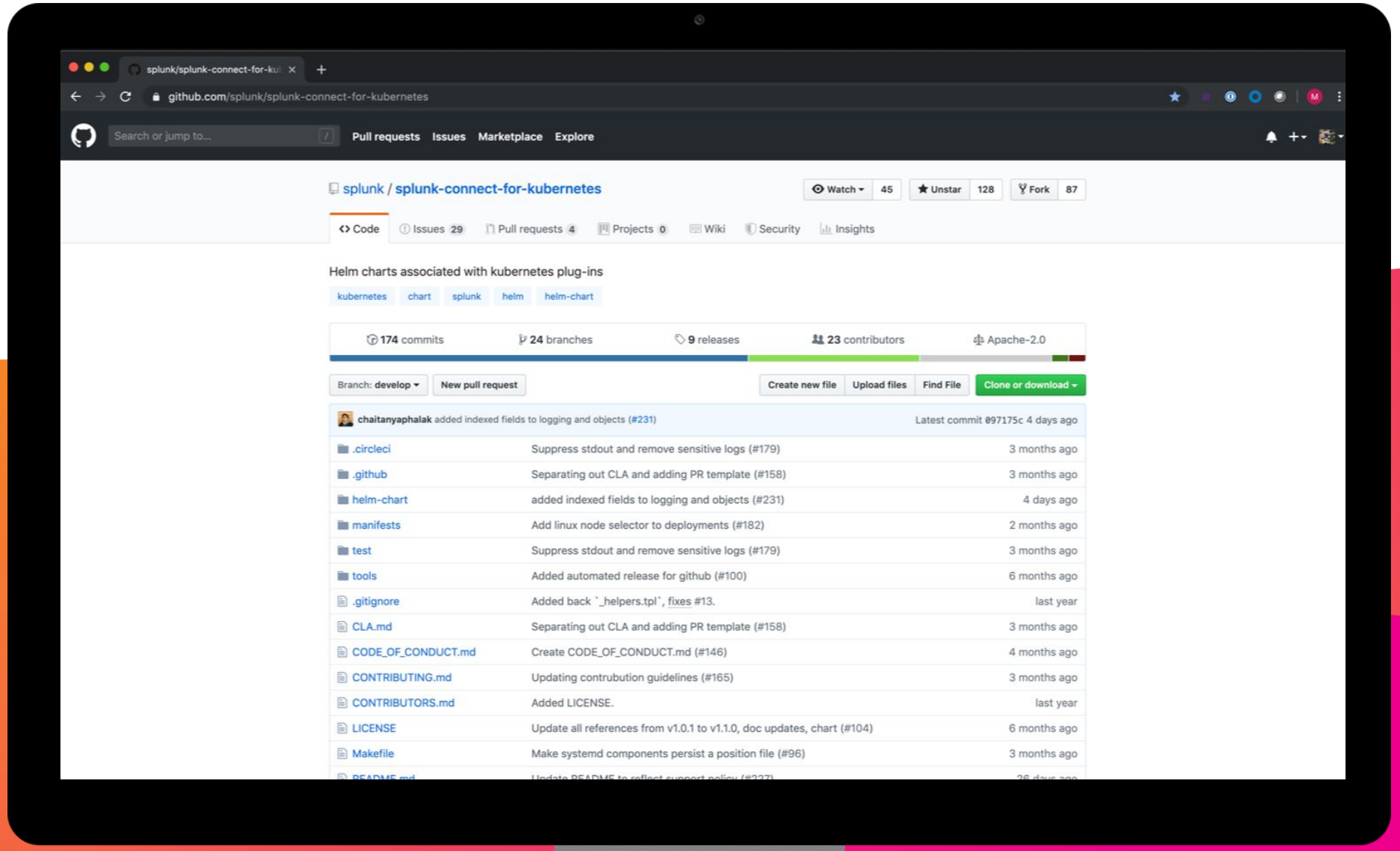
.conf19
Las Vegas, Nevada
October 21-24

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!

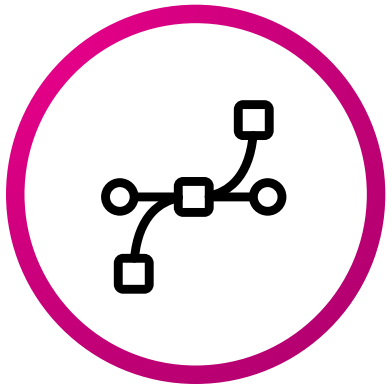
splunk> .conf19



splunk> .conf19

Splunk Connect for Kubernetes

Kubernetes Data Sources



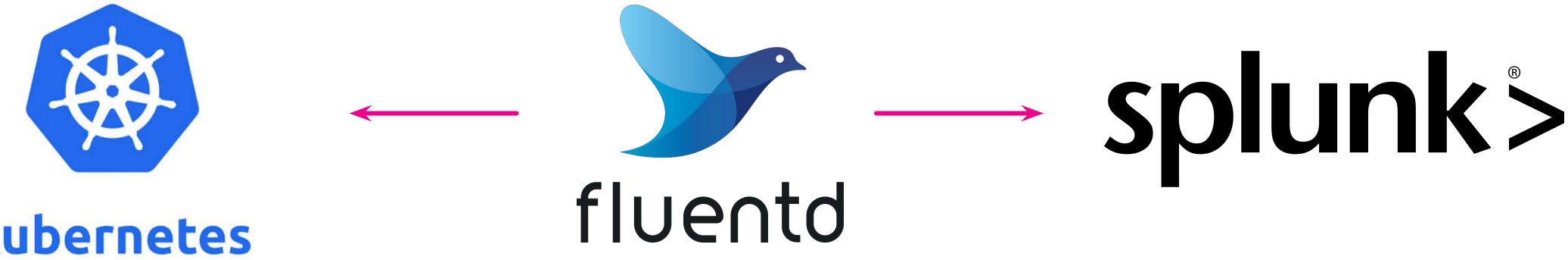
Splunk Kubernetes Logging

Splunk Kubernetes Metrics

Splunk Kubernetes Objects

Splunk Kubernetes Logging

Application & OpenShift Cluster Logging



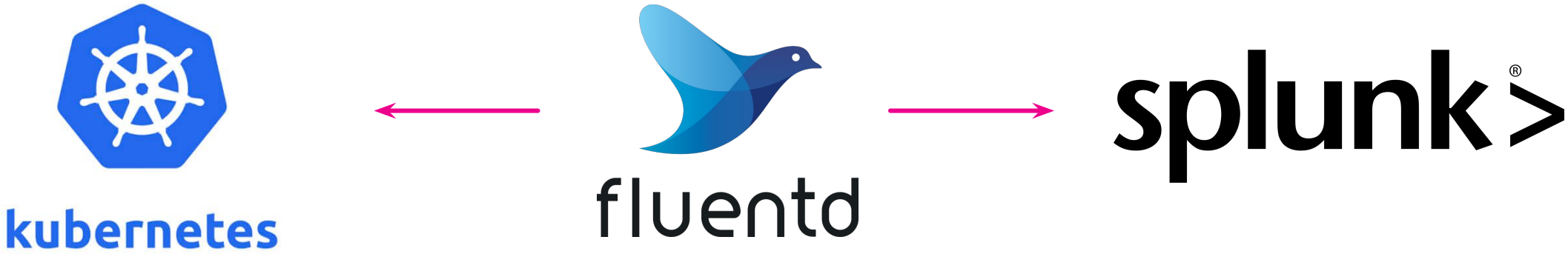
Docker/CRI-O Logs
Journald
Kubernetes API Audit Logs
Custom Log Sources

in_tail
systemd
jq_transformer
fluentd-hec

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_aggregator

record_modifier

fluentd-hec

HTTP Event Collector

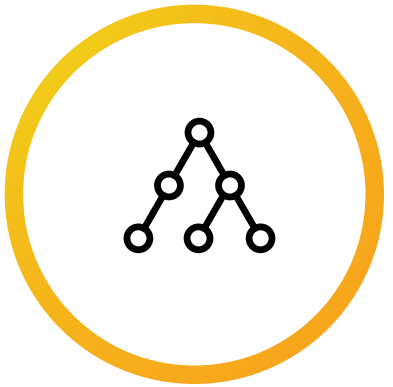
Metrics Index

Splunk Connect for Kubernetes

Business Flow Use

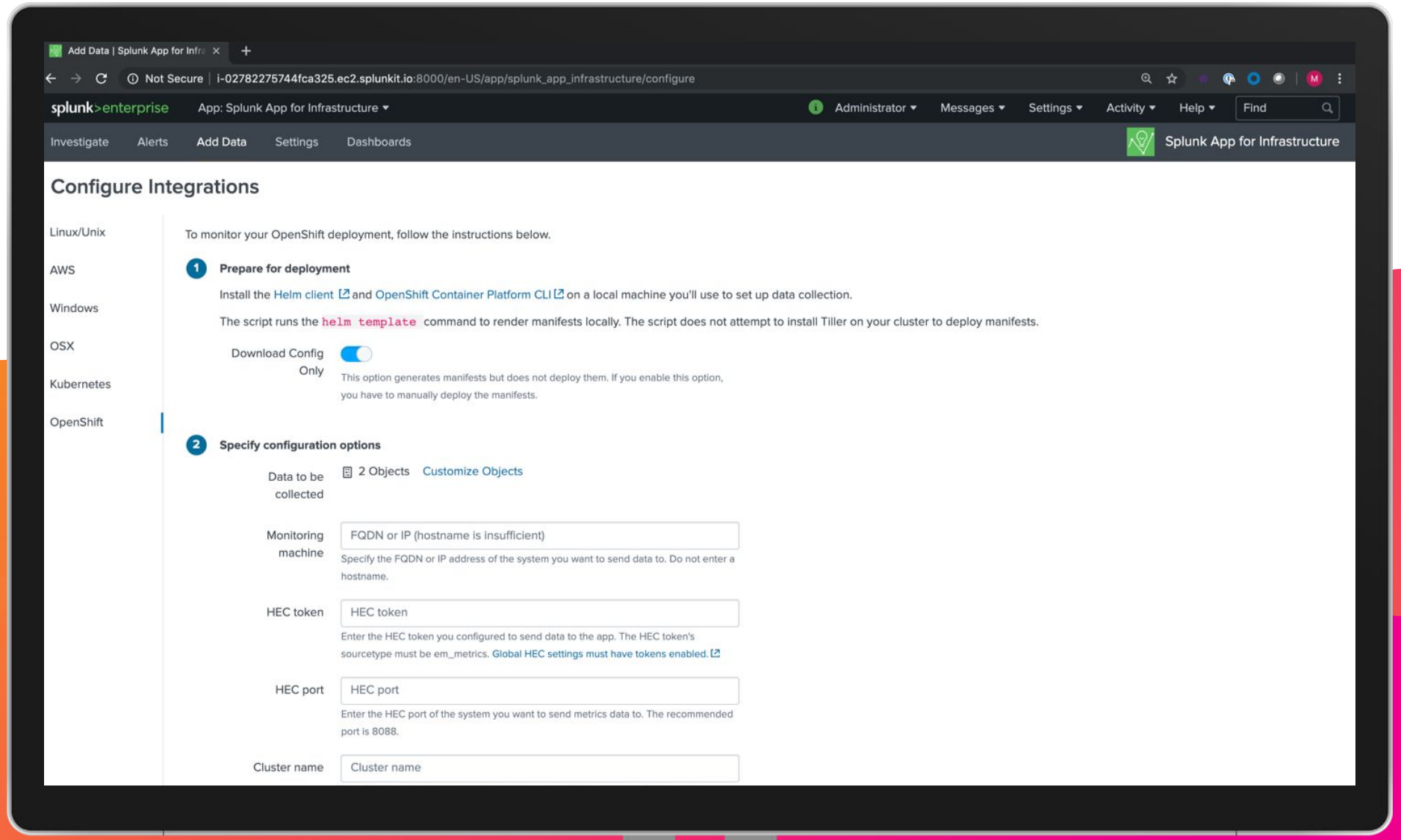
Kubernetes API Audit

Kubernetes Events API



Microservice Logging

Demo



Splunk Business Flow

What is Process Mining?

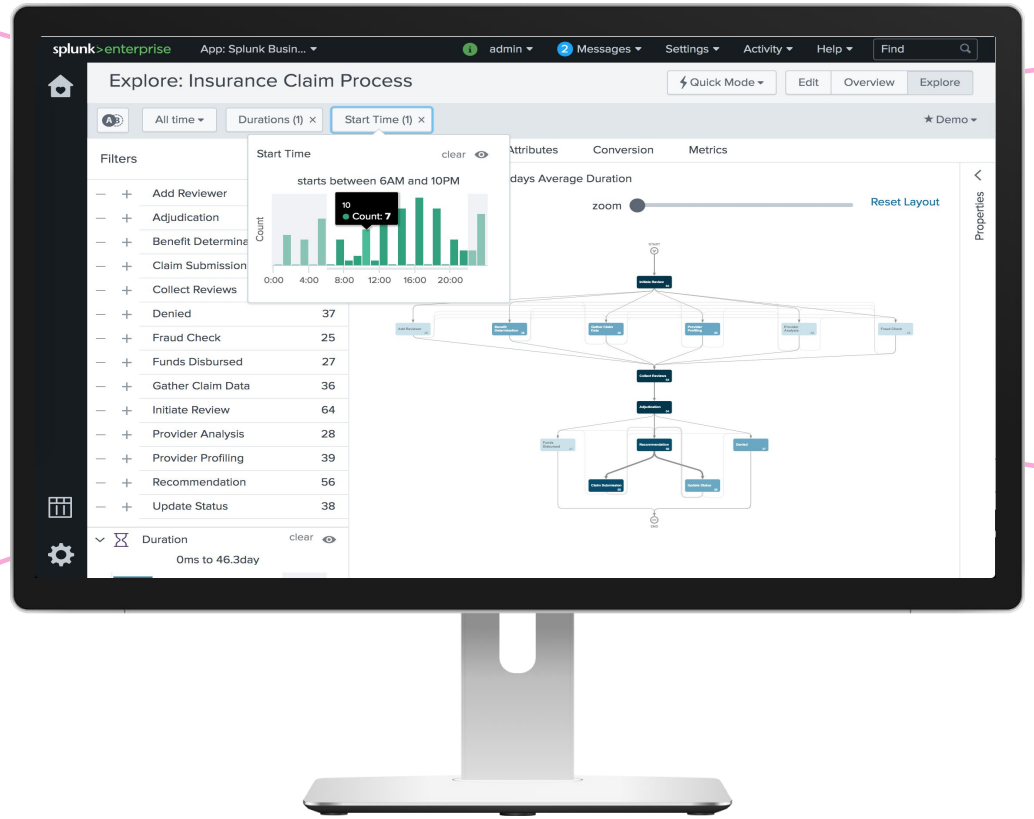
http://www.processmining.org/

splunk> .conf19

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> .conf19

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

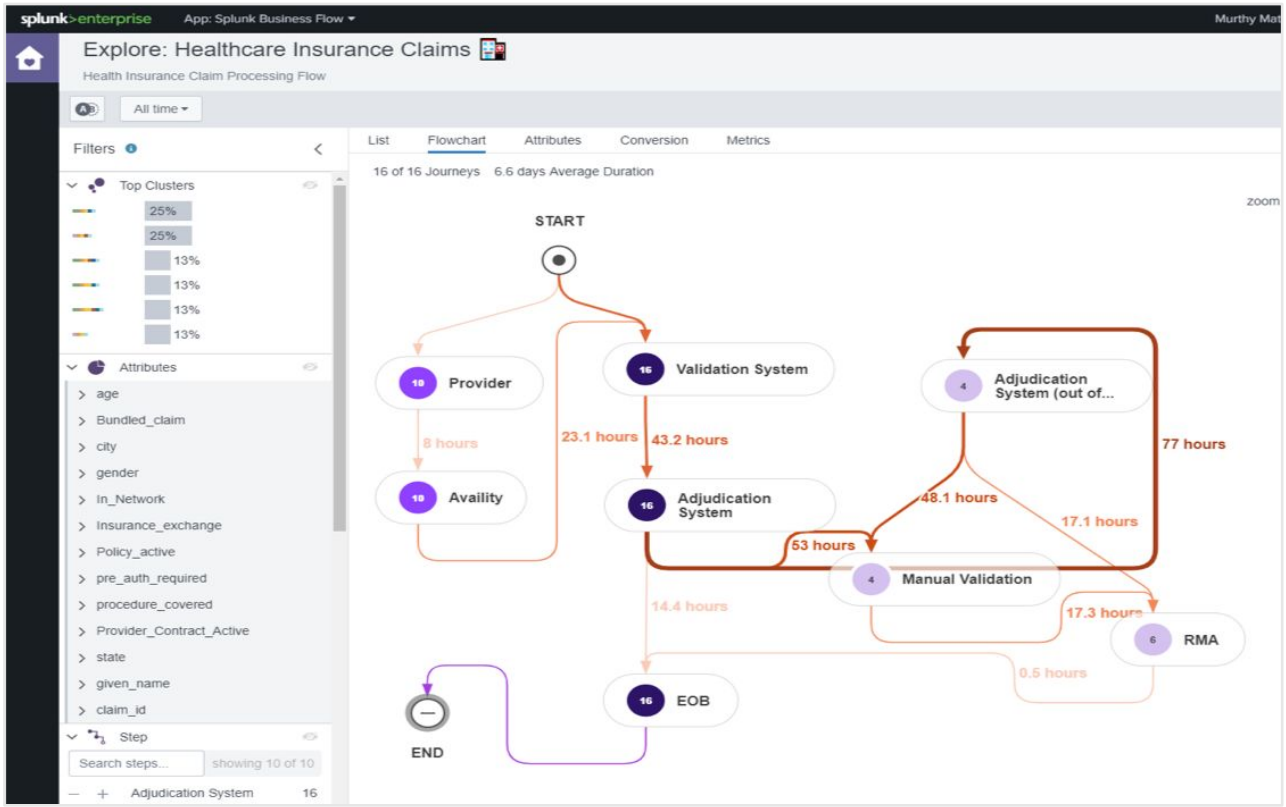
splunk>enterprise splunk>cloud

Splunk Business Flow

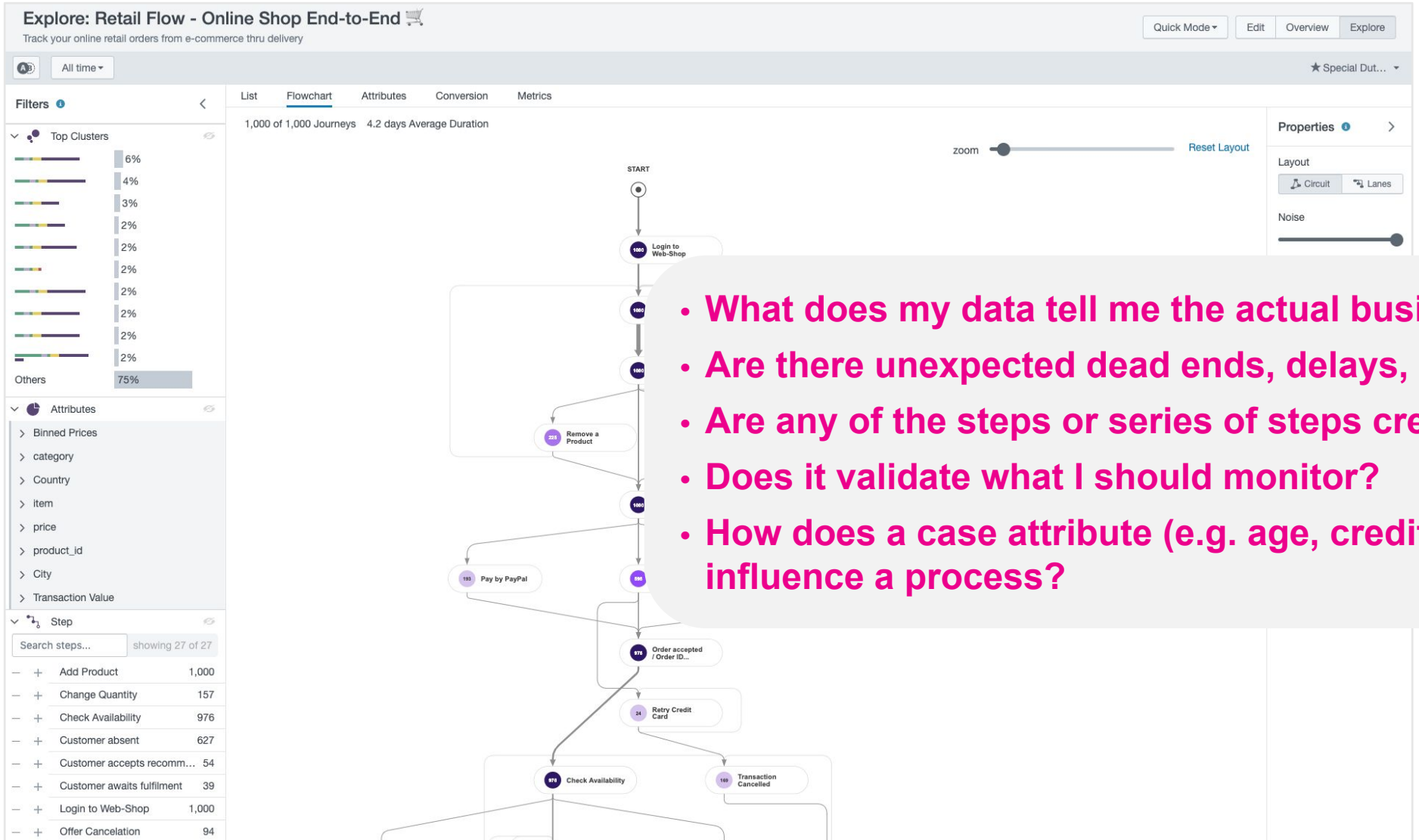
Splunk Business Flow is a fast, flexible, and intuitive process mining solution for interactive discovery, investigation, and conformance checking of any business process

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

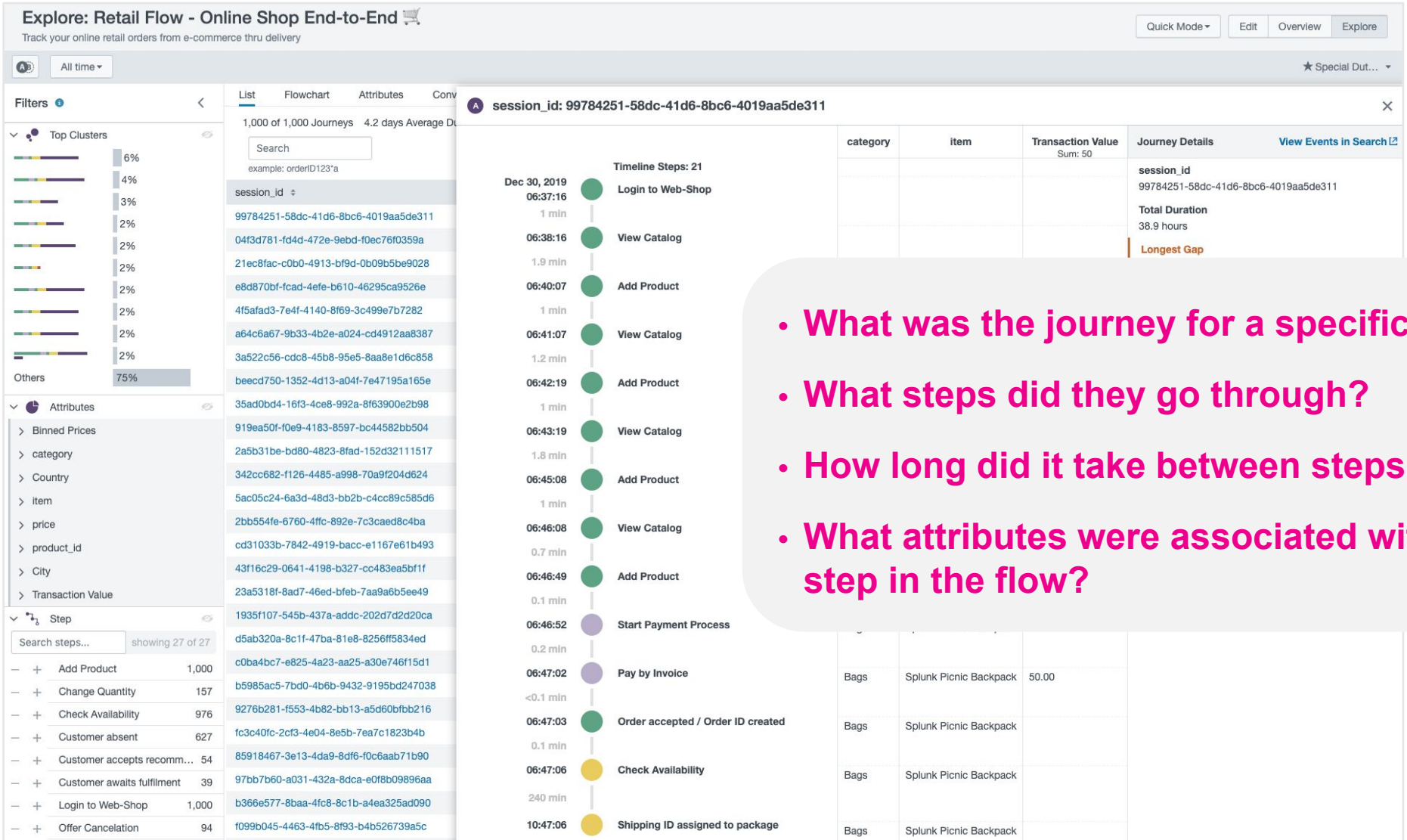


Flowchart Tab

- 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?

splunk> .conf19

Investigation & Troubleshooting

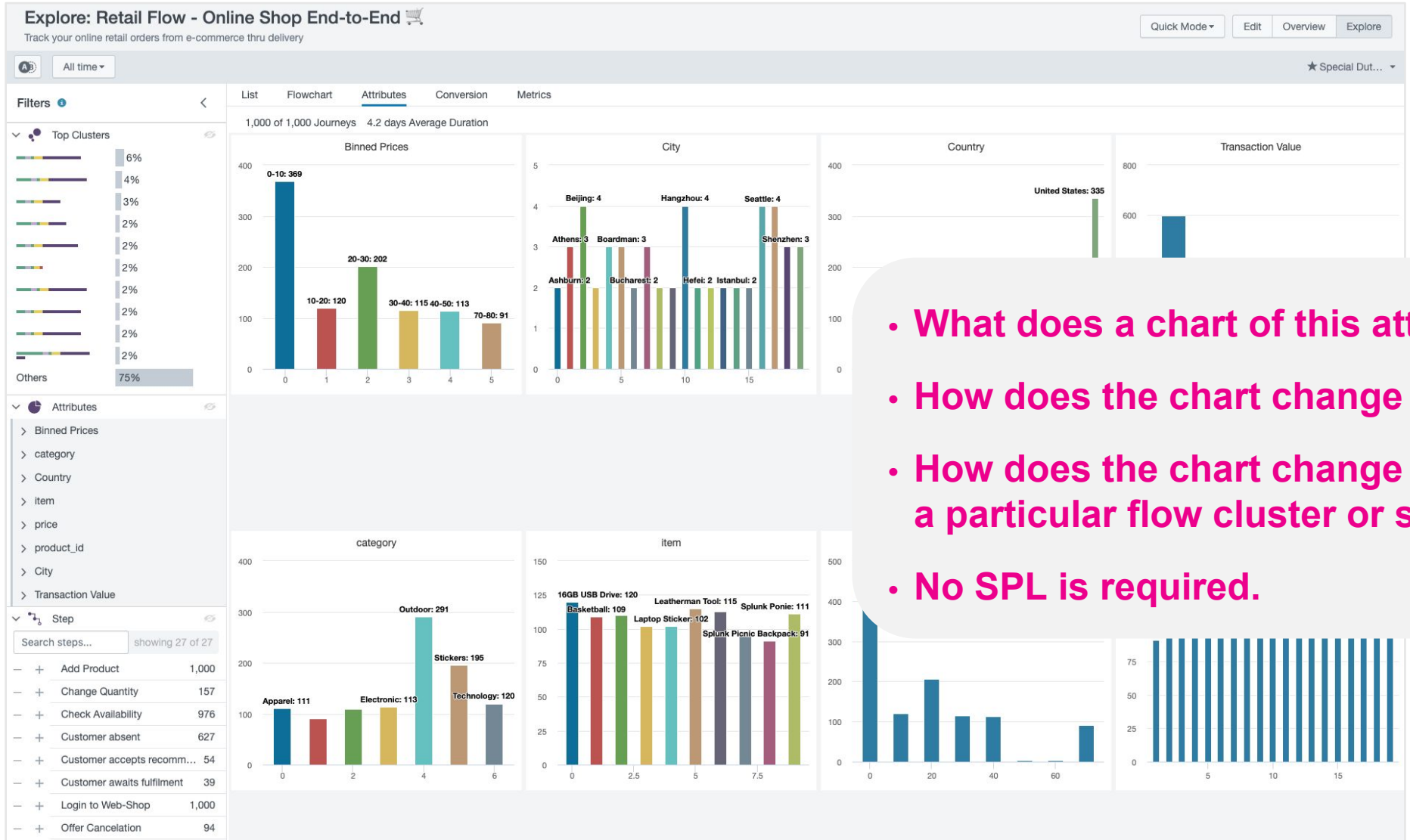


List Tab

- 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?

splunk> .conf19

Segmentation and Analysis

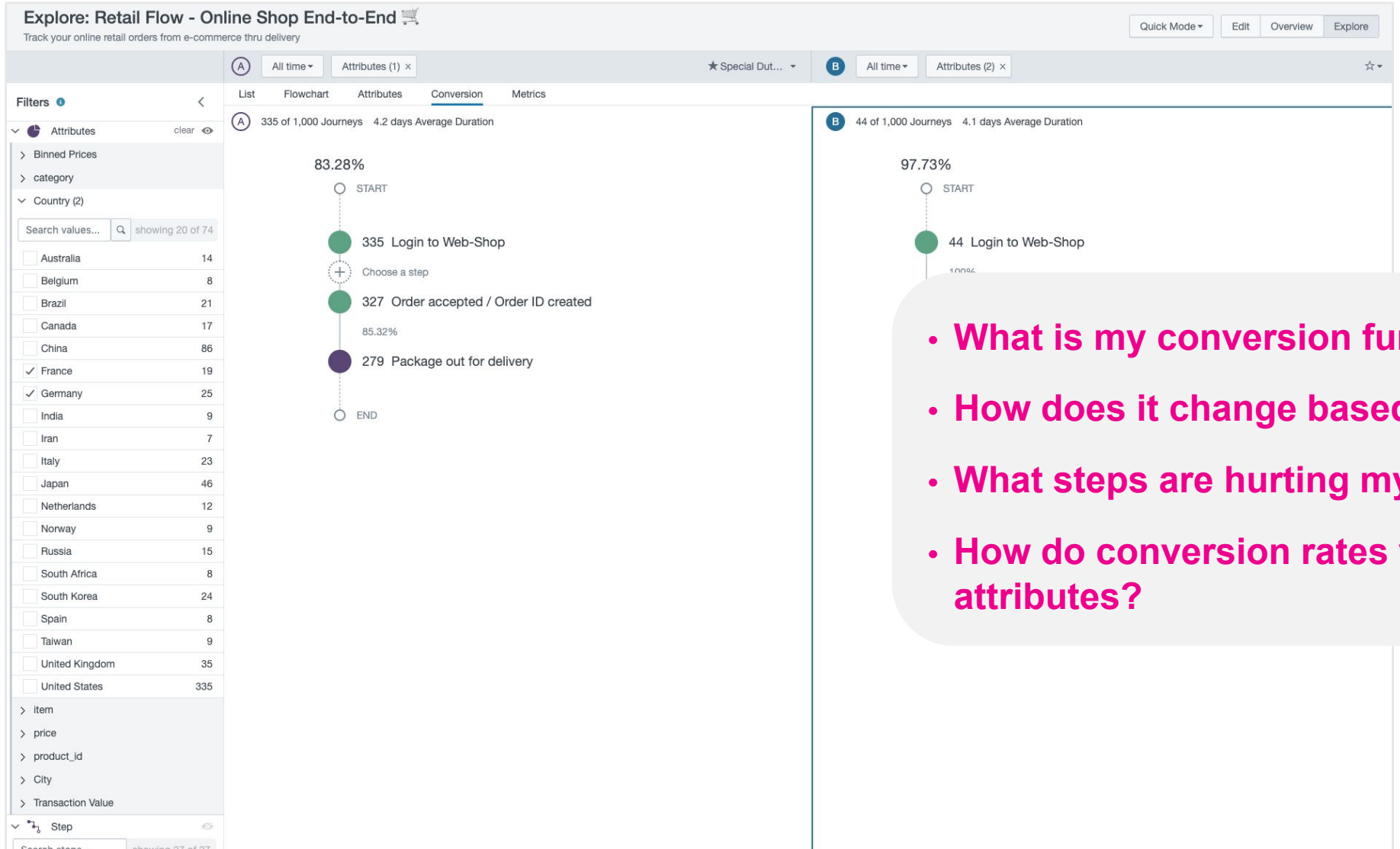


Attributes Tab

- 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.

splunk> .conf19

Conversions, Churn & Comparisons



Conversion Tab

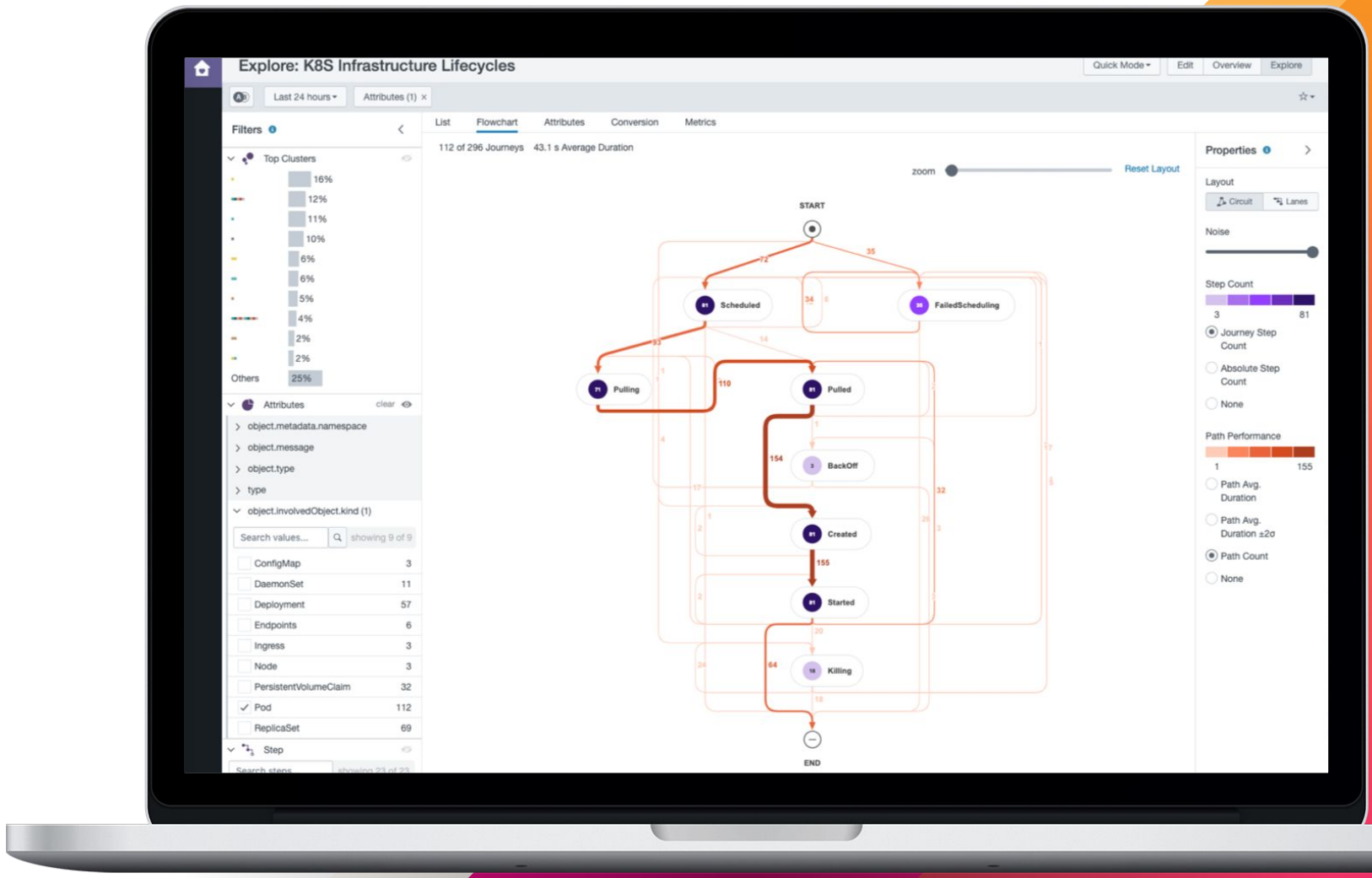
- What is my conversion funnel?
- How does it change based on the mix of steps?
- What steps are hurting my conversion rates?
- How do conversion rates vary based on different attributes?

Infrastructure Journeys

Analyzing the Kubernetes Object Lifecycles

The Business of k8s Pods

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



splunk> .conf19

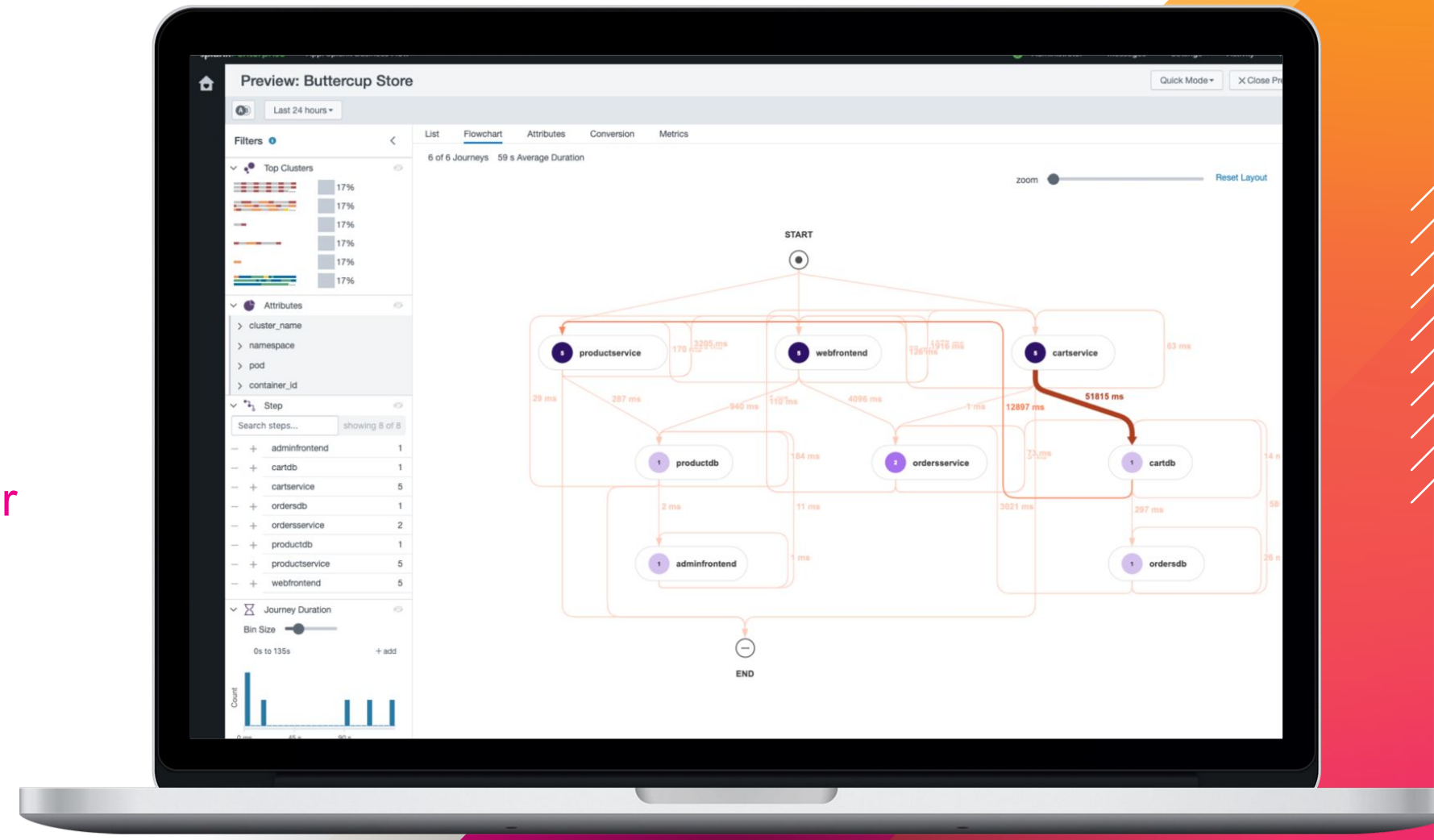
Analyzing User Journeys Using Application Logging

Analyzing user journeys using Application Logging

splunk> .conf19

Your App's Journeys!

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> .conf19

.conf19

splunk>

Thank You !

Go to the .conf19 mobile app to

RATE THIS SESSION