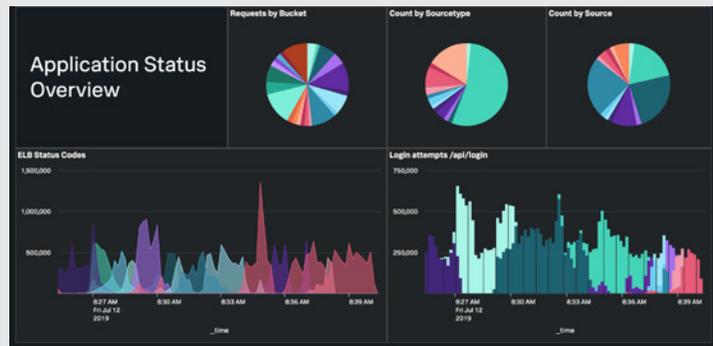# SPLUNK® INVESTIGATE

Investigation and action across any data source – start collaborating with your team in minutes

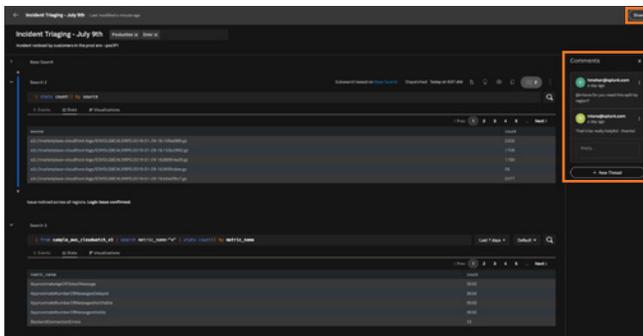## How Splunk Investigate Works:

- **Collaboration is built into the entire solution** with the ability to share dashboards, write searches as a team, and annotate all aspects of data investigation in a unified, centralized workspace.

- With **SQL-like search language and an ML-based search assistant**, searching is accurate and efficient

- Create visibility across apps, systems, and stacks by adding and editing **any data source** with Splunk Investigate's guided assistance

- Dashboards come with a **drag-and-drop editing experience**, support for absolute layouts and a wide range of visualizations to make it faster and easier than ever to tell a story with your data.

Splunk Investigate provides DevOps teams with visibility and trouble-shooting capabilities across any data source, from apps to infrastructure. Splunk's ability to offer powerful search and collaboration means teams can spend less time switching across different apps and tools, and more time getting code into production. Add data in various formats - structured and unstructured, and from multiple data sources - all in one place helps accelerate Mean Time To Detection (MTTD) and Mean Time To Resolution (MTTR).

Dev teams want to see if their code is working, understand response time and error rates, and quickly discover incidents. They don't want to monitor and investigate in silos, spend time maintaining tools or learn yet another query language. Splunk Investigate delivers one place to ingest and correlate data from any location or source and fast tracks answering any question, without wasting time on maintenance.

Built with Splunk Cloud Services, Splunk Investigate is a cloud native application that requires no download, hardware or software - everyone can access the solution with just an internet connection.

Collaborate and Investigate

Collaboration capabilities are built into every aspect of Splunk Investigate with the ability to share searches and dashboards, make comments and create one-source-of-truth for post incident reviews. Make investigations easier with post-processing and iterative search as well as support for re-using searches, search fragments, text, dashboards and more.
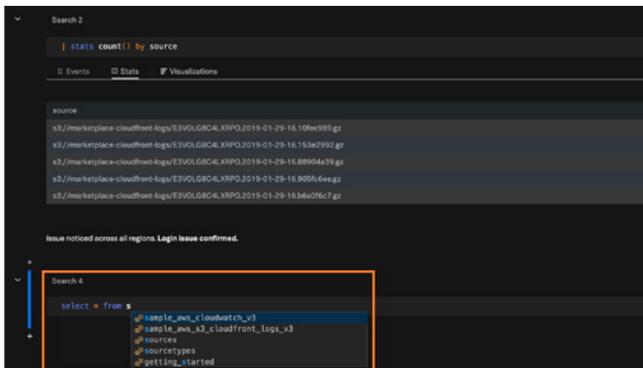

No need to learn yet another query language

Splunk Investigate uses a SQL-like query language and simplifies search execution with an ML-enabled search assistant. You can also drive search efficiency by reusing search-string, importing your favorite searches, and more.
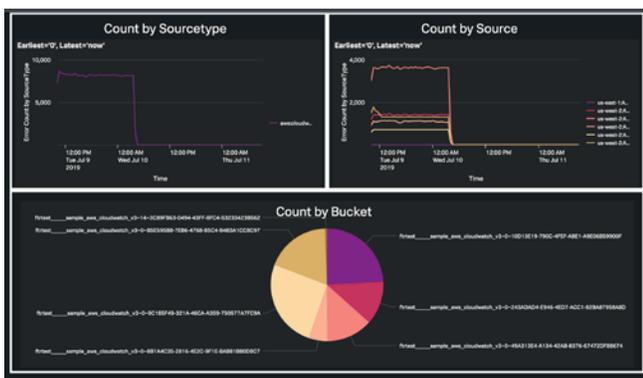
Dashboards and Visualization

Use dashboards to tell & share a compelling story with your data. The drag-and-drop editor makes it easy to get started adding and configuring visualizations as well as enhancing the consumer experience through interactive elements like inputs and automatic search refresh.
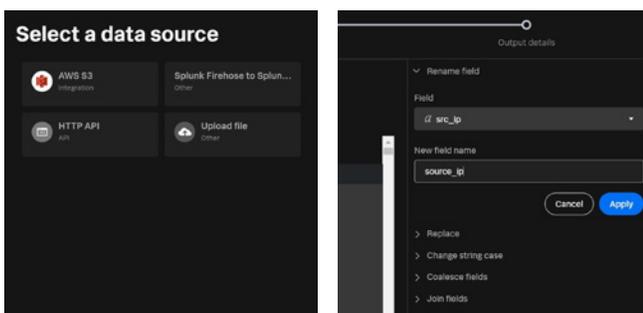
Quickly ingest data and add context

Splunk Investigate simplifies ingesting data by guiding you through connecting to external data sources and enabling you to augment and edit your data before indexing it. To provide additional context for your team, you can add descriptions and contextualize your data.

Join our Splunk Investigation Beta program today – Create your own account and instance to start your collaborative investigation in minutes. **Get Splunk Investigate.**

splunk>   **Learn more:** www.splunk.com/asksales   **www.splunk.com**