identifies, resolves, and reviews incidents using Splunk>Investigate

Amr Saad
Engineering Manager | Splunk

Matthew Erbs
Senior Software Engineer | Splunk

Heather Hunsinger
Senior Software Engineer | Splunk

Who are We?

Splunkbase Engineering

Amr Saad
Engineering Manager | Splunk

Matthew Erbs
Senior Software Engineer | Splunk

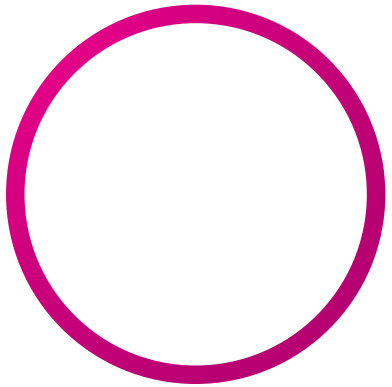
Heather Hunsinger
Senior Software Engineer | Splunk

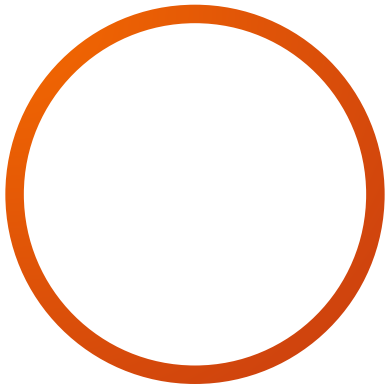
Forward-Looking Statements

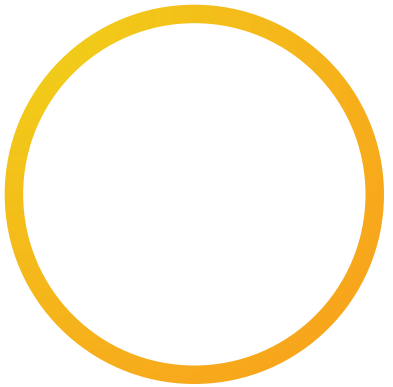
During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. 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.

Goals of the Talk







Agenda

Matthew Erbs
Senior Software Engineer
Splunk

Amr Saad
Engineering Manager
Splunk

Heather Hunsinger
Senior Software Engineer
Splunk

splunk> turn data into doing

Matthew Erbs
Senior Software Engineer
Splunk

Amr Saad
Engineering Manager
Splunk

Heather Hunsinger
Senior Software Engineer
Splunk

A Day in the Life of Amr...

What is Splunkbase?

https://splunkbase.splunk.com

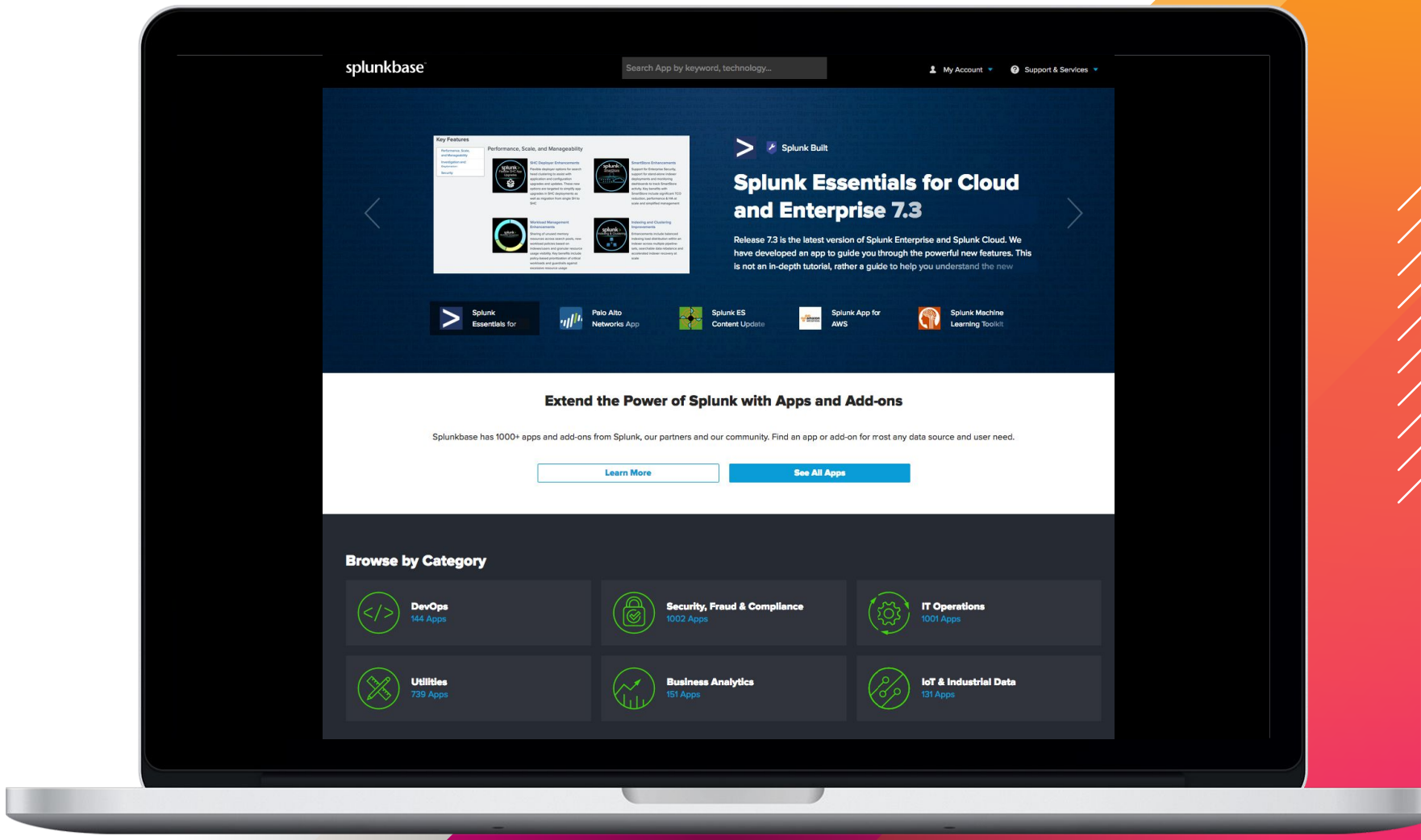
© 2019 SPLUNK INC.

Splunk App Distribution Platform

Apps by Splunk and 3rd Party Devs

APIs for App Install from within Splunk

Users can extend the power of Splunk



Splunkbase Stats

Apps

Users

Daily Downloads

New Apps Last 4 months

A Day in the Life of Matt...

Architecture

Our Splunk Journey

Splunk Enterprise

Splunk Cloud

Splunk Investigate

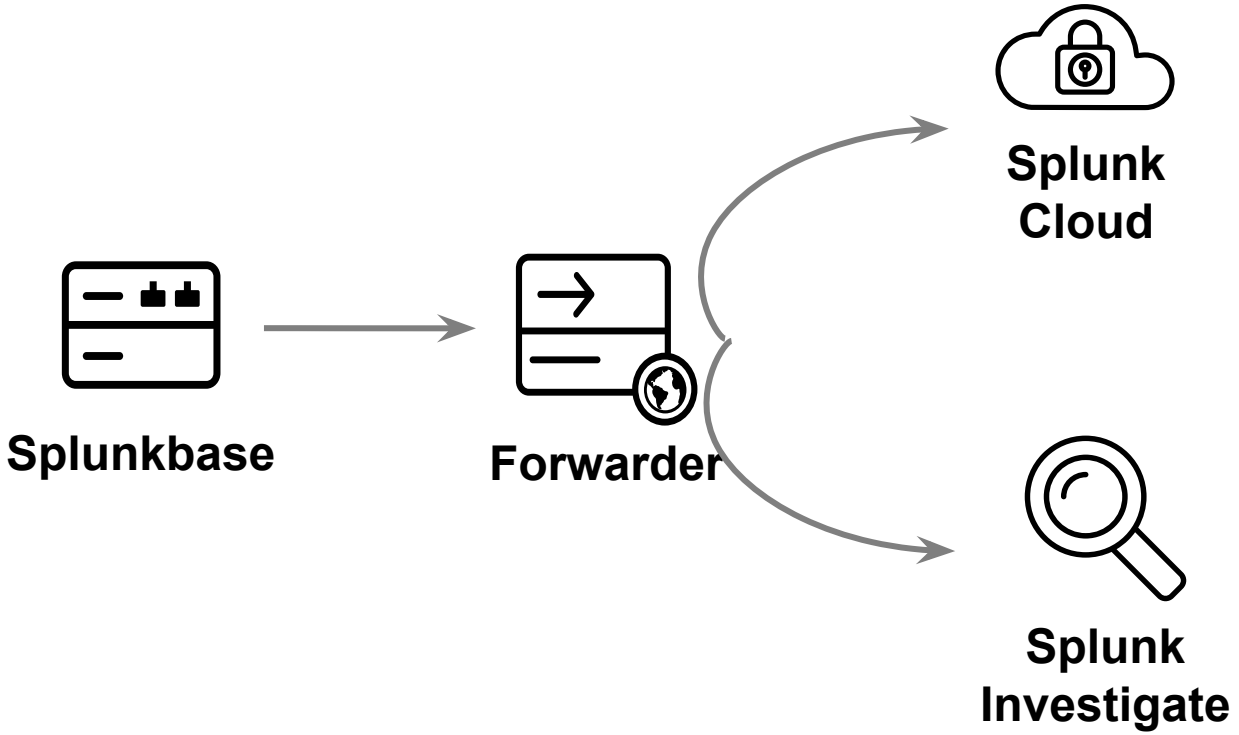
What is Splunk>Investigate?

splunk> .conf19

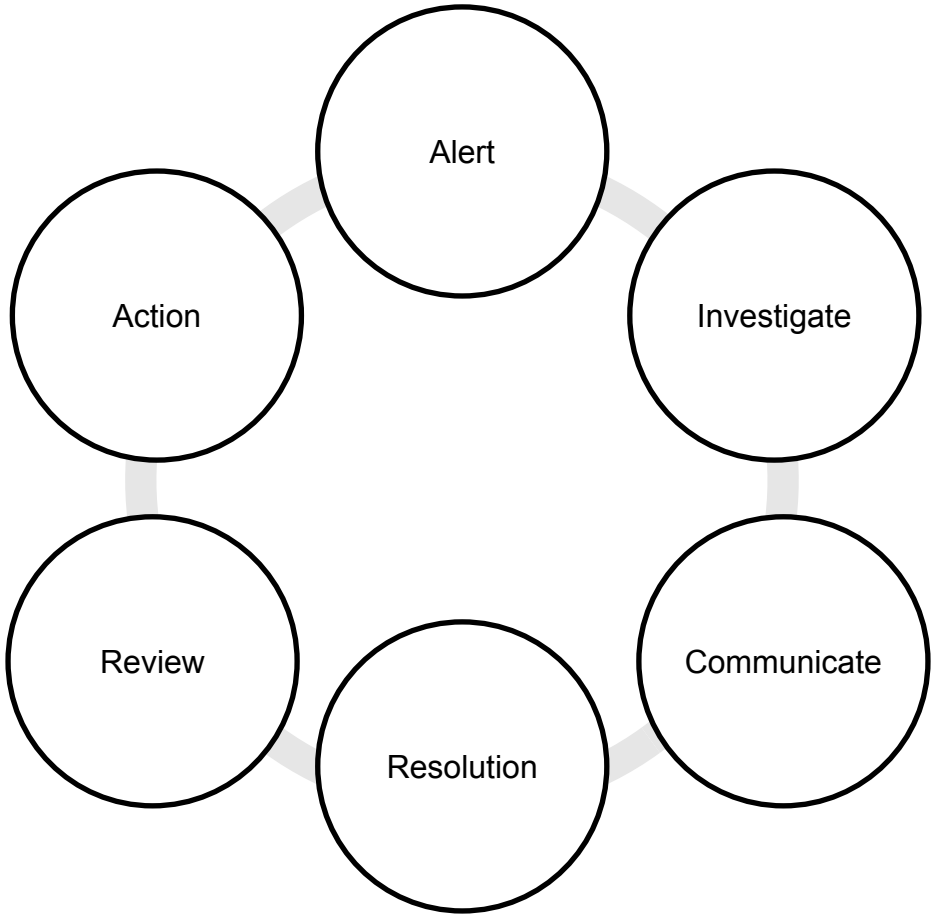
"Splunk Investigate is a new **cloud-based application** focused on **reducing time to incident resolution, improving collaboration** and helping teams **conduct effective postmortems.**"

Splunkbase & Splunk Investigate

- Why?
- How?
- Who?



Splunkbase Process



Incident Challenges

Increased Time To Remediation

Lack of access and re-use of incident findings means time is lost

Higher Developer to Incident Ratio

Multiple Dev./SRE's are working on the same incident

Increased Time To Resolution

Multiple tools + context switching means time is lost

Multiple Repeat Incidents

Ineffective retrospectives and post mortems

Splunk Investigate – Core Capabilities

Collaborative Investigative Interface

Smart Knowledge Object Library

Visual Storytelling with Dashboards

Add and Process Data Seamlessly

Scalable Cloud Infrastructure

Splunk Investigate – Accelerate Remediation and Resolution

Multiple Data Sources

Real Time Streaming

Single place to collect + process data

Default connectors: AWS-S3, Cloudwatch, Kinesis

Local Universal Forwarder

Modern Infrastructure

Multi-tenant based architecture

Continuous deployment velocity

Kubernetes based orchestration – scale dynamically

Use-Cases

- ✔ **Remediation**
- ✔ **Resolution**
- ✔ **Retrospective**

Business Outcomes

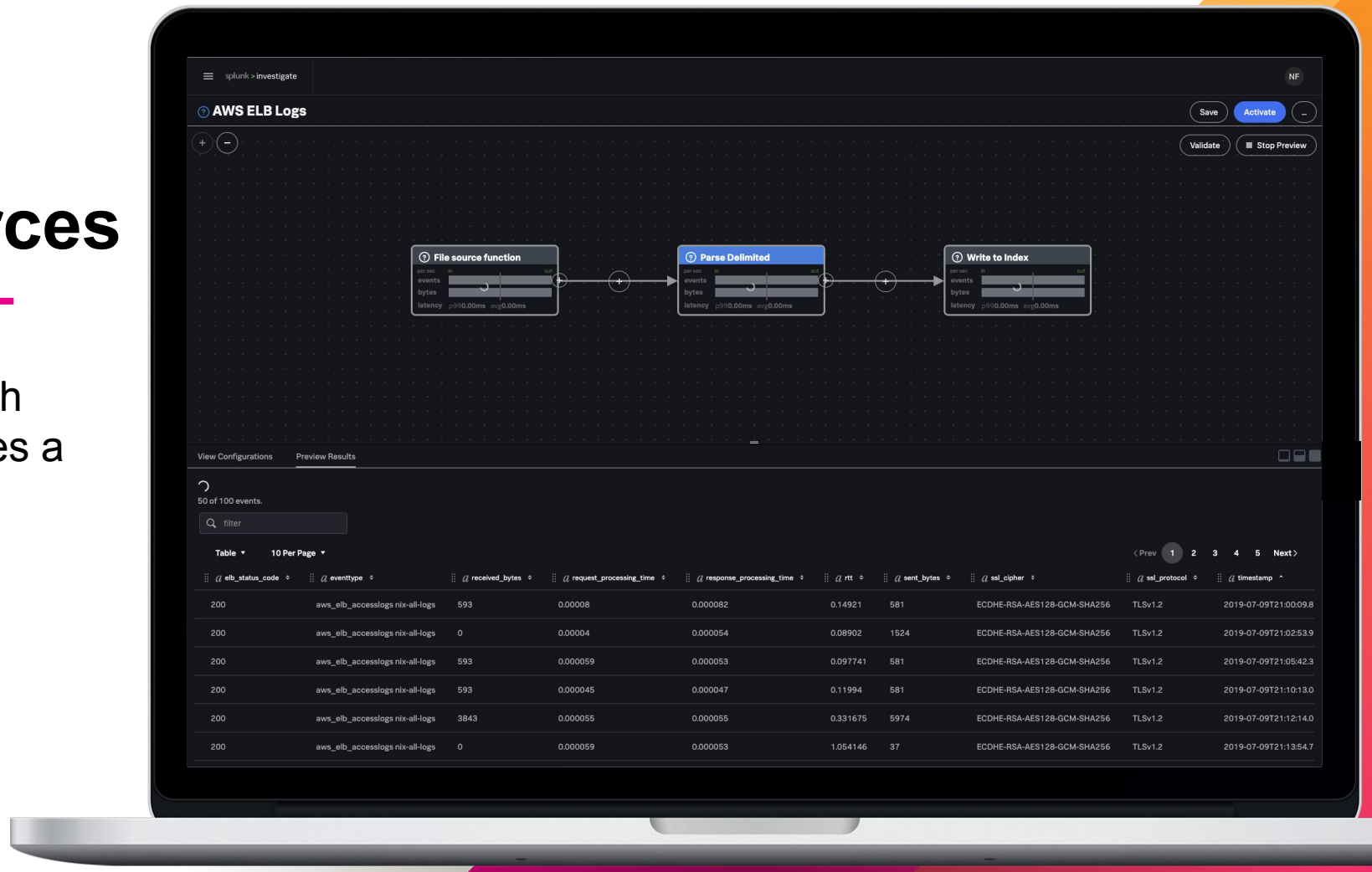
- Accelerate Mitigation
- Expedite Resolution
- No repeat incidents

Across Disparate Teams…

- Developers
- SREs
- Product Mgmt.
- Engineering Execs.

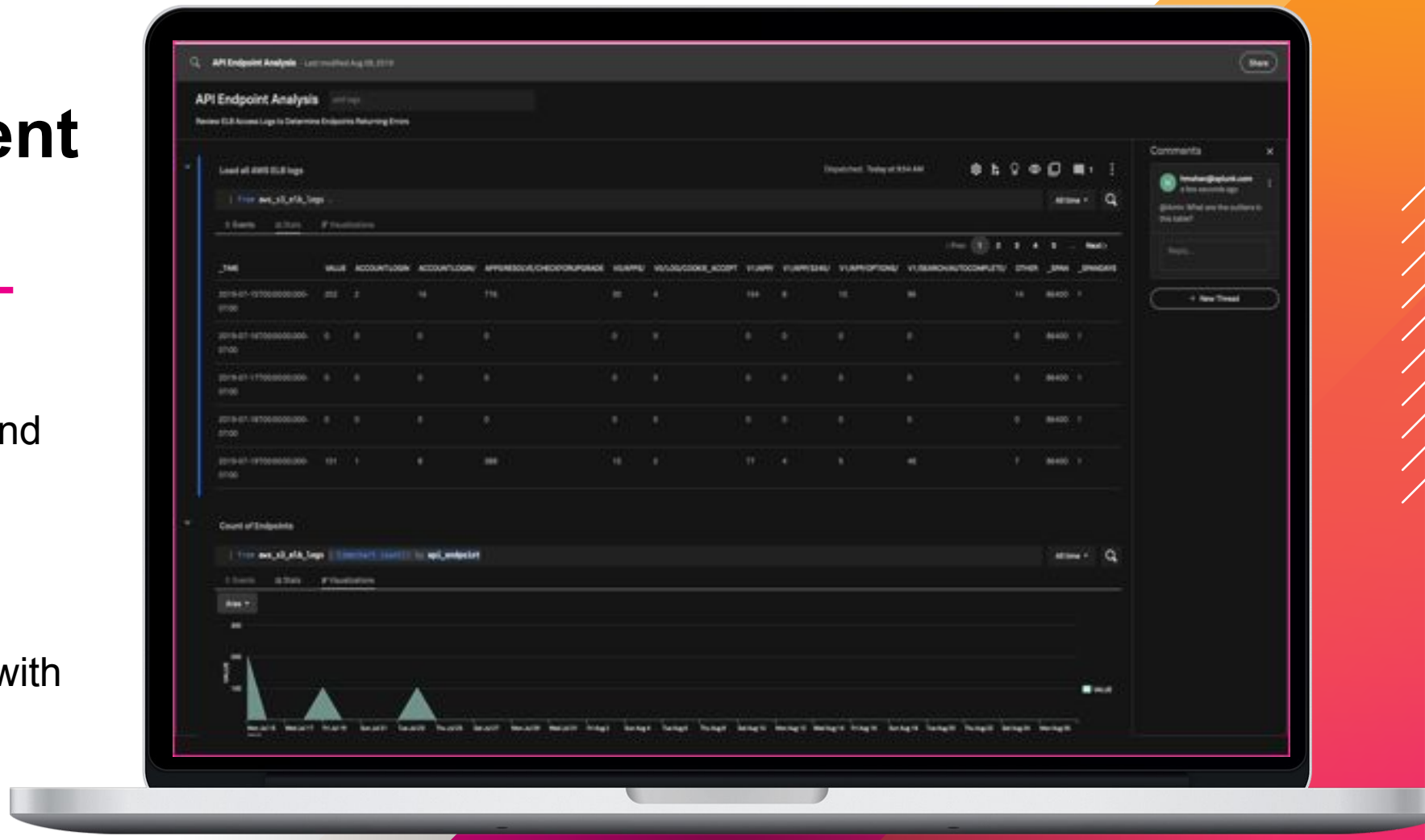
Investigation and Insights Across Multiple Data Sources

- Real-time data integration with streaming capabilities provides a single place to collect and process-then deliver insights
- Default data connectors for common sources – universal forwarder for additional optionality



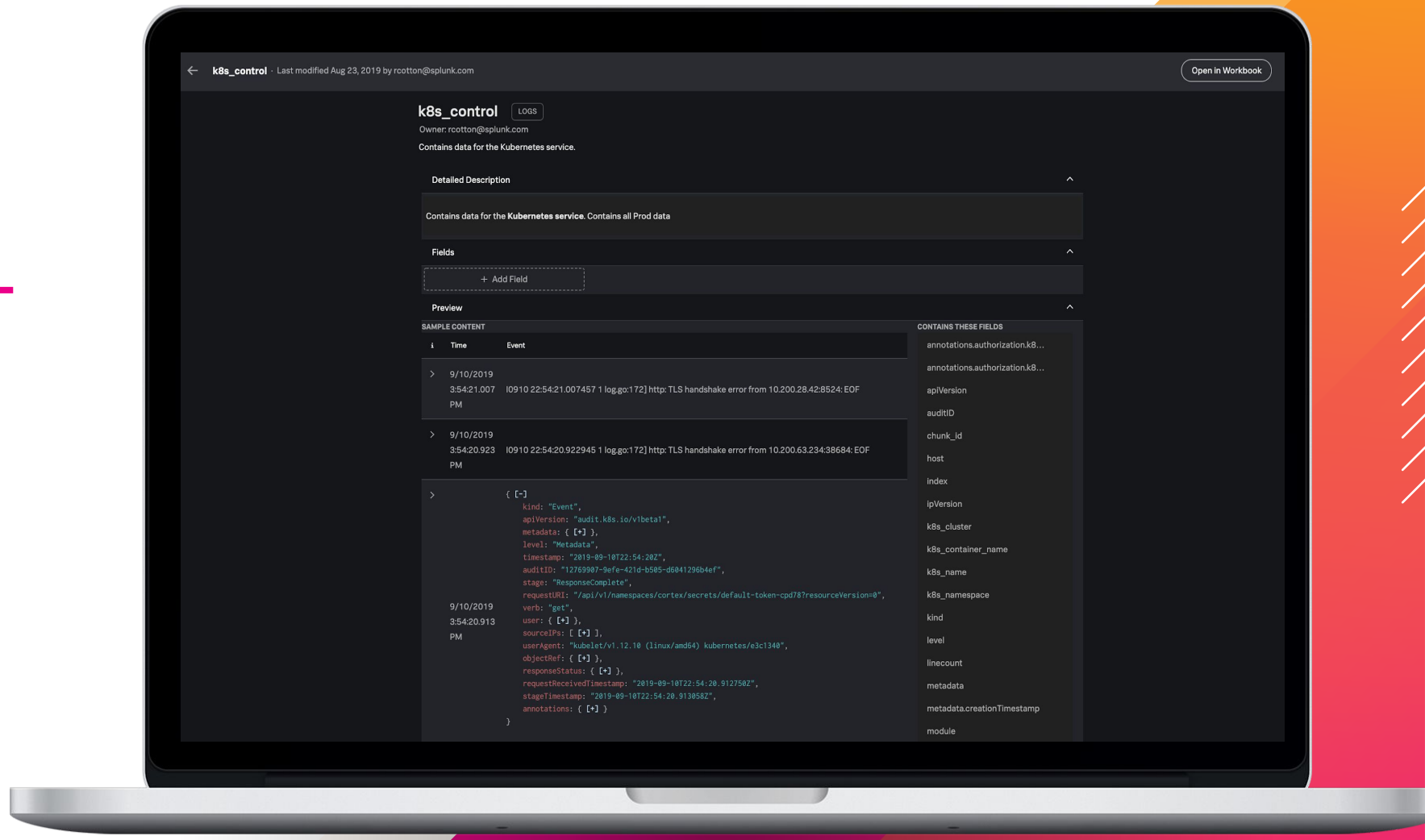
Collaborative Interface for Incident Investigation

- Run multiple searches, add markup text, import images and dashboards for complete visibility
- SQL-based query language provides incremental coding with inline annotations



Ensure No Repeat-incidents

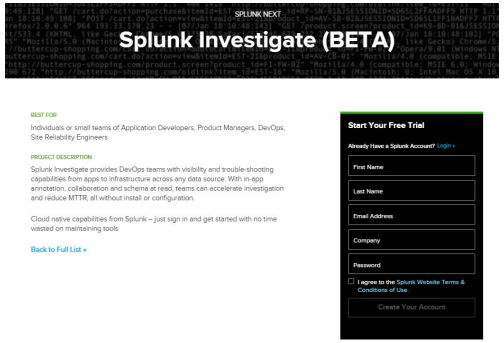
- Knowledge object library that leverages all stored team knowledge around queries, data-sets and dashboards
- Efficient and actionable Post Incident Reviews with easy access to outage events and anomalies as they really happened



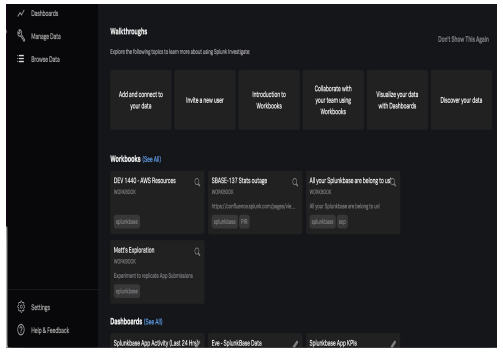
A Day in the Life of Heather...

Demo

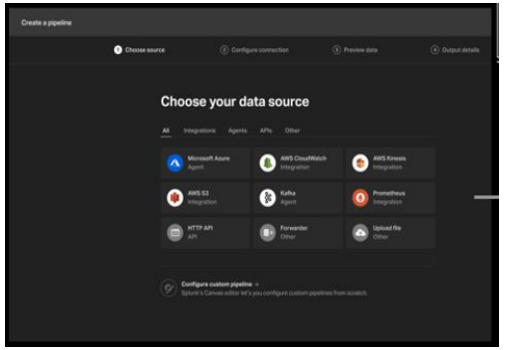
Getting Started in 3 Steps…



Sign-up for a free-trial on our webpage



Create and name your own tenant so your team can collaborate



Upload your own data or use ours – Start Investigating!

Get answers to any question by joining our Splunk User Community Slack Group!

splunk> .conf19

Key Takeaways

1. Splunk Investigate is a lightweight tool for engineering teams

2. Remote collaboration is a seamless process

Q&A

Heather Hunsinger | Splunk

Amr Saad | Splunk

Matthew Erbs | Splunk

splunk> .conf19

.conf19

splunk>

Thank You !

Go to the .conf19 mobile app to

RATE THIS SESSION