The Core Power of Splunk

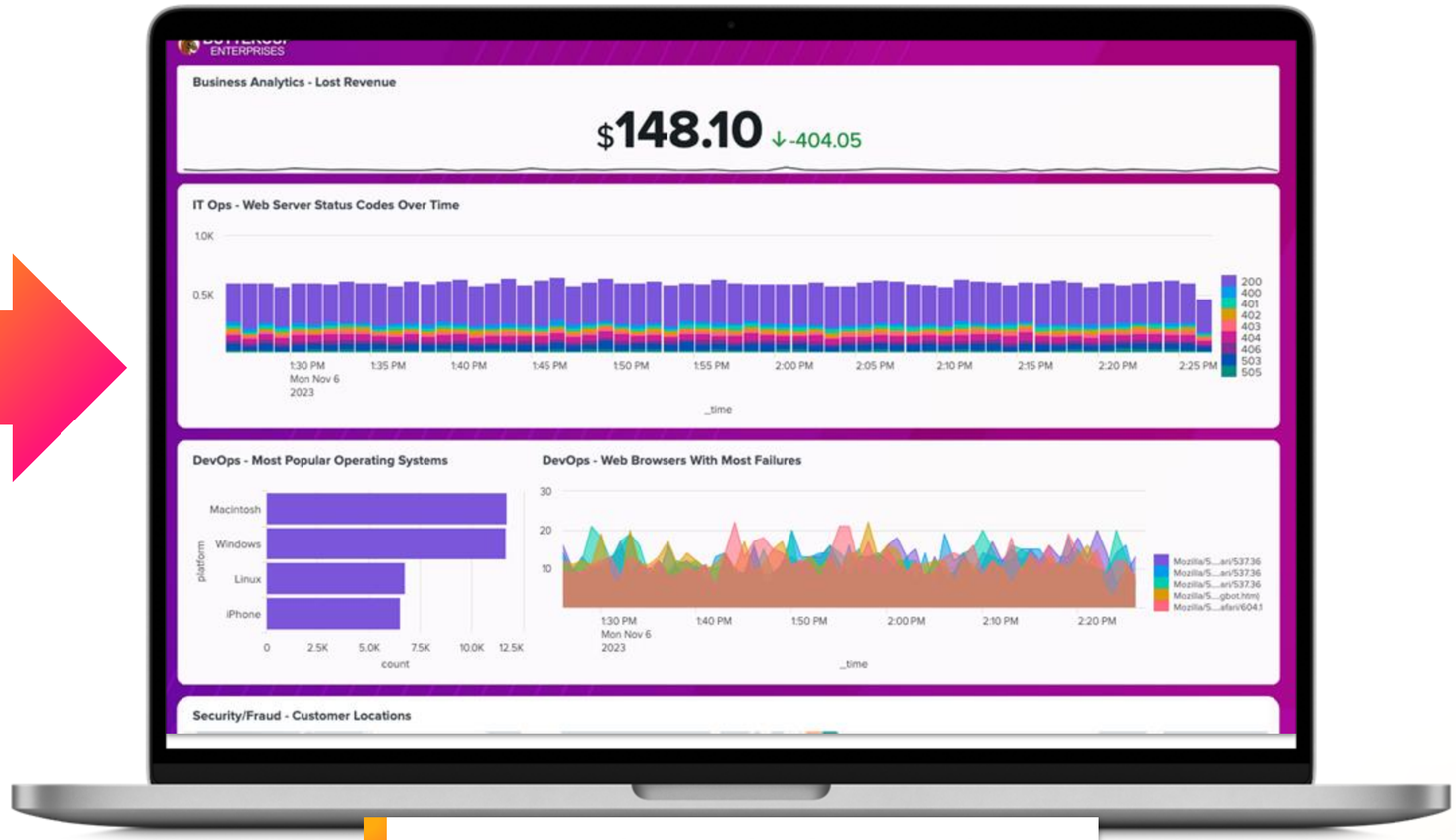
One platform to gather your data, ask it questions, and get the answers you need

Jake Miller – Sr. Solutions Engineer

October 2nd, 2025

The Power of Splunk

Go from messy machine data…



…to a dynamic, interactive dashboard!

Machine Data is ~~Complex~~ Valuable!

```
10.2.1.35 64.66.0.20 - - [21/Dec/2015 16:21:51:326103]
"GET /product.screen?product_id=CC-P3-BELKIN-
SILBLKIPH5&JSESSIONID=SD5SL6FF1ADFF9 HTTP 1.1" 503 865
"http://shop.splunktel.com/product.screen?product_id=CC
-P3-BELKIN-BLK_BTOOTH_HFREE" "Mozilla/5.0 (Linux; U;
Android 2.3.5;   FR-fr; SAMSUNG-SGH-I927
Build/GINGERBREAD) AppleWebKit/533.1 (KHTML, like
Gecko) Version/4.0 Mobile Safari/533.1" 3875
```

Security Use Case Data Lens

IP of client

URL Resource requested

```
10.3.1.35 64.66.0.20 - - [21/Dec/2015 16:21:51:326103]
GET /product.screen?product_id=CC-P3-BELKIN-
SILVERKIPH5&JSESSIONID=SD5SL6FF1ADFF9 HTTP 1.1" 503 865
"http://shop.splunktel.com/product.screen?product_id=CC
-P3-BELKIN-BLK_BTOOTH_HFREE" "Mozilla/5.0 (Linux; U;
Android 2.3.5;   FR-fr; SAMSUNG-SGH-I927
Build/GINGERBREAD) AppleWebKit/533.1 (KHTML, like
Gecko) Version/4.0 Mobile Safari/533.1" 3875
```

Dustin

DevOps Use Case Data Lens

```
10.2.1.35 64.66.0.20 - - [21/Dec/2015 16:21:51:326103]
"GET /product.screen?product_id=CC-P3-BELKIN-
H5&JSESSIONID=SD5SL6FF1ADFF9 HTTP 1.1" 503 865
 nt   //shop.splunktel.com/product.screen?product_id=CC
-P3-B LKIN-BLK_BTOOTH_HFREE" "Mozilla/5.0 (Linux; U;
Android 2.3.5;   FR-fr; SAMSUNG-SGH-I927
Build/GINGERBREAD) AppleWebKit/533.1   HTML, like
Gecko) Version/4.0 Mobile Safari/53
```

Platform

Handset model

Tony

IT Operations Use Case Data Lens

IP of web server

IP of client

```
10.2.1.35 64.66.0.20 - - [21/Dec/2015 16:21:51:326103]
"GET /product.screen?product_id=CC-P3-BELKIN-
SILBLKIPH5&JSESSIONID=SD5SL6FF1ADFF9 HTTP 1.1" 503 865
"http://shop.splunk.com/product.screen?product_id=CC
ELKIN-BLK_BTC... "Mozilla/5.0 (Linux; U;
Android 2.3.5;  FR-fr; SAMSUNG-SGH-I92
Build/GINGERBREAD) AppleWebKit/533.1 (KHTML, like
Gecko) Version/4.0 Mobile Safari/533.1" 3875
```

Status code

Page requested

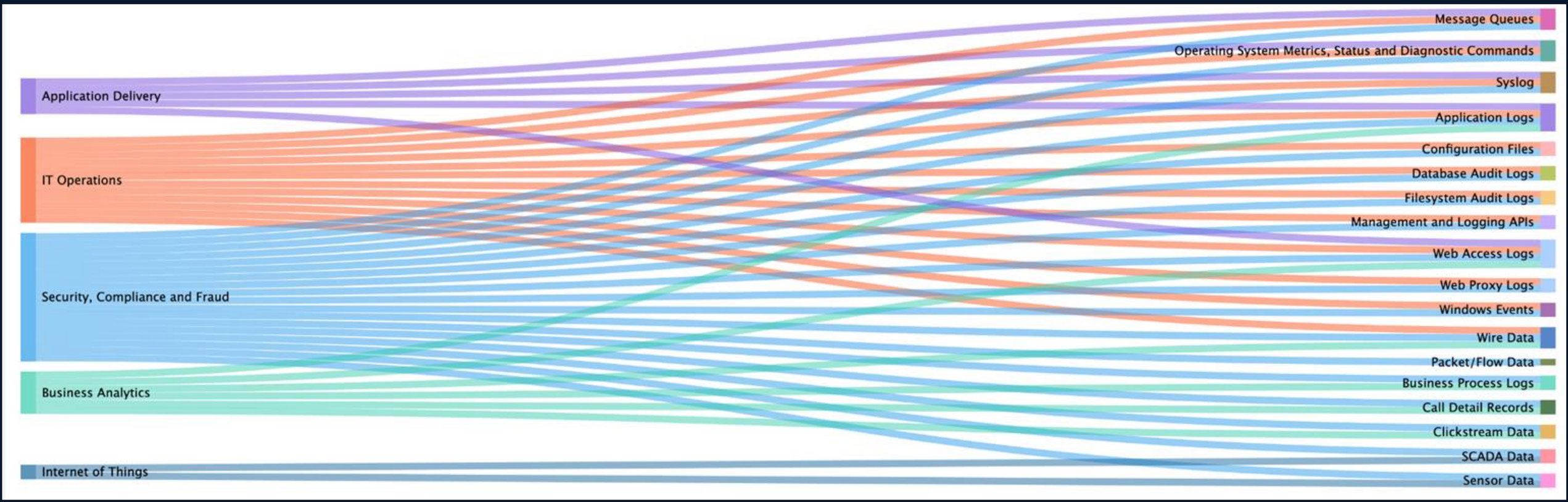
ID of web session

Browser

Nicole

Size of objects returned to client

We can map all the raw data into these key use cases.



Today's Scenario

1. We will be in the role of a Splunk Admin

As a Splunk Admin, we will be answering questions from our Security, DevOps, and ITOps teams.

2. We work for Buttercup Enterprises

Buttercup Enterprises earns revenue by selling products on its online web store.

The data we will be using for all three teams is the same web log data we were just reviewing.

3. Questions from the team are as follows:

Security - Where are clients accessing our website from?

DevOps – What are the top platforms customers use to access our website?

ITOps – When do customers experience checkout failures and what are all the HTTP status codes encountered on our website?

Demo

Training & Certification

https://splunk.com/training

- **Online education classes**
  Instructor-led and self-paced eLearning
- **Certification tracks for different roles**
  User, Power User, Admin, Architect and Developer
- **Splunk Education Rewards**
  Complete training and receive points that you can redeem for Splunk swag!
- **Free education!**
  Single-subject eLearning courses to kick start your Splunk learning