Splunk 4 Rookies Workshop

October 19th

We will start at 10:00AM CT

Forward-Looking Statements

This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

A discussion of factors that may affect future results is contained in our most recent annual report on Form 10-K and subsequent quarterly reports on Form 10-Q, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov, including descriptions of the risk factors that may impact us and the forward-looking statements made in this presentation. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

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. We undertake no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

Your Splunk Account Team

Hermia Johnson
Account Manager
Account Owner, sales advocate. Provides program management oversight.

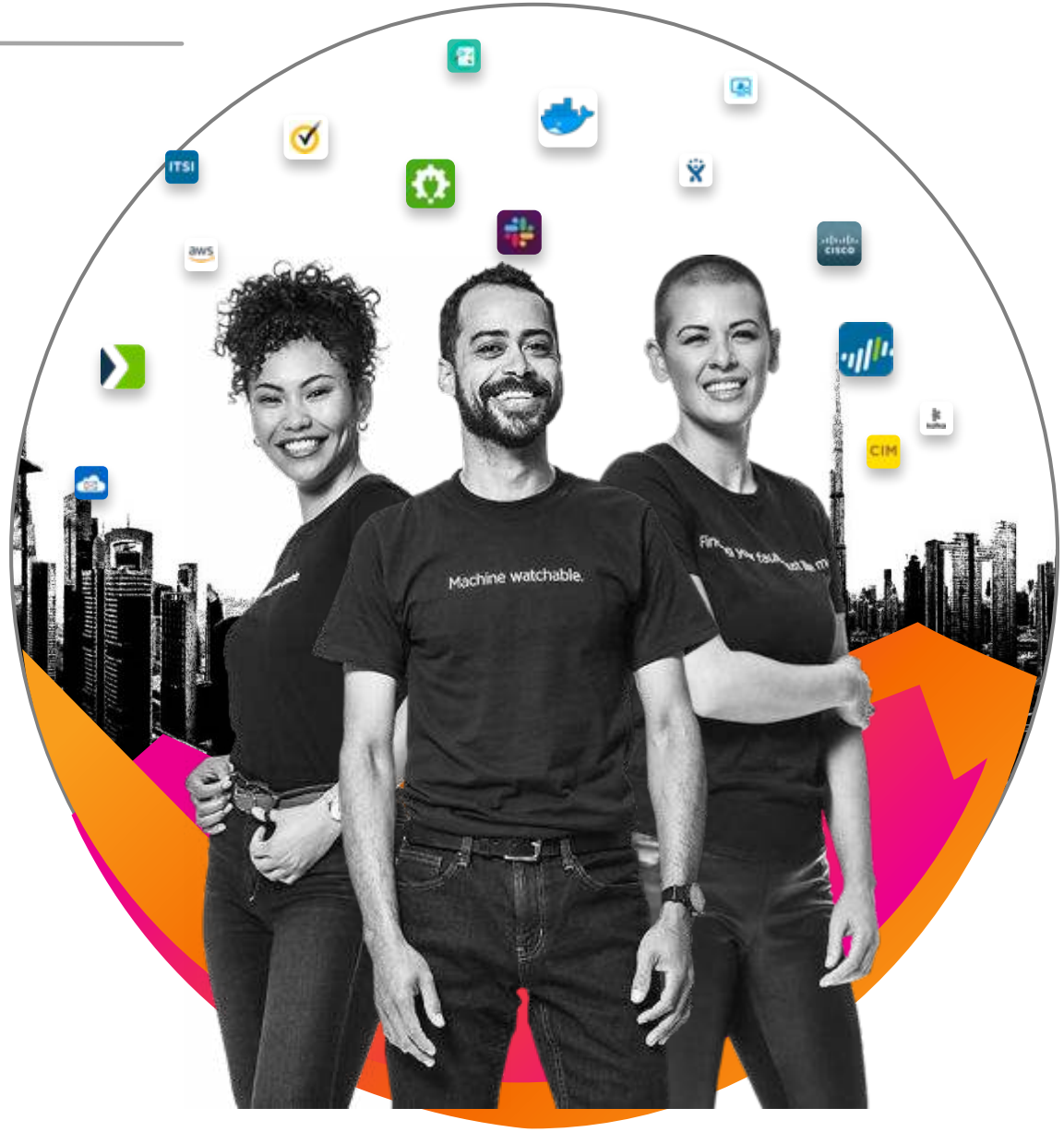
John Gonzales
Solutions Engineer
Technical Best Practice, Compute, Storage, and Network, Skillsets.

Matt Cavanaugh
Account Manager
Account Owner, sales advocate. Provides program management oversight.

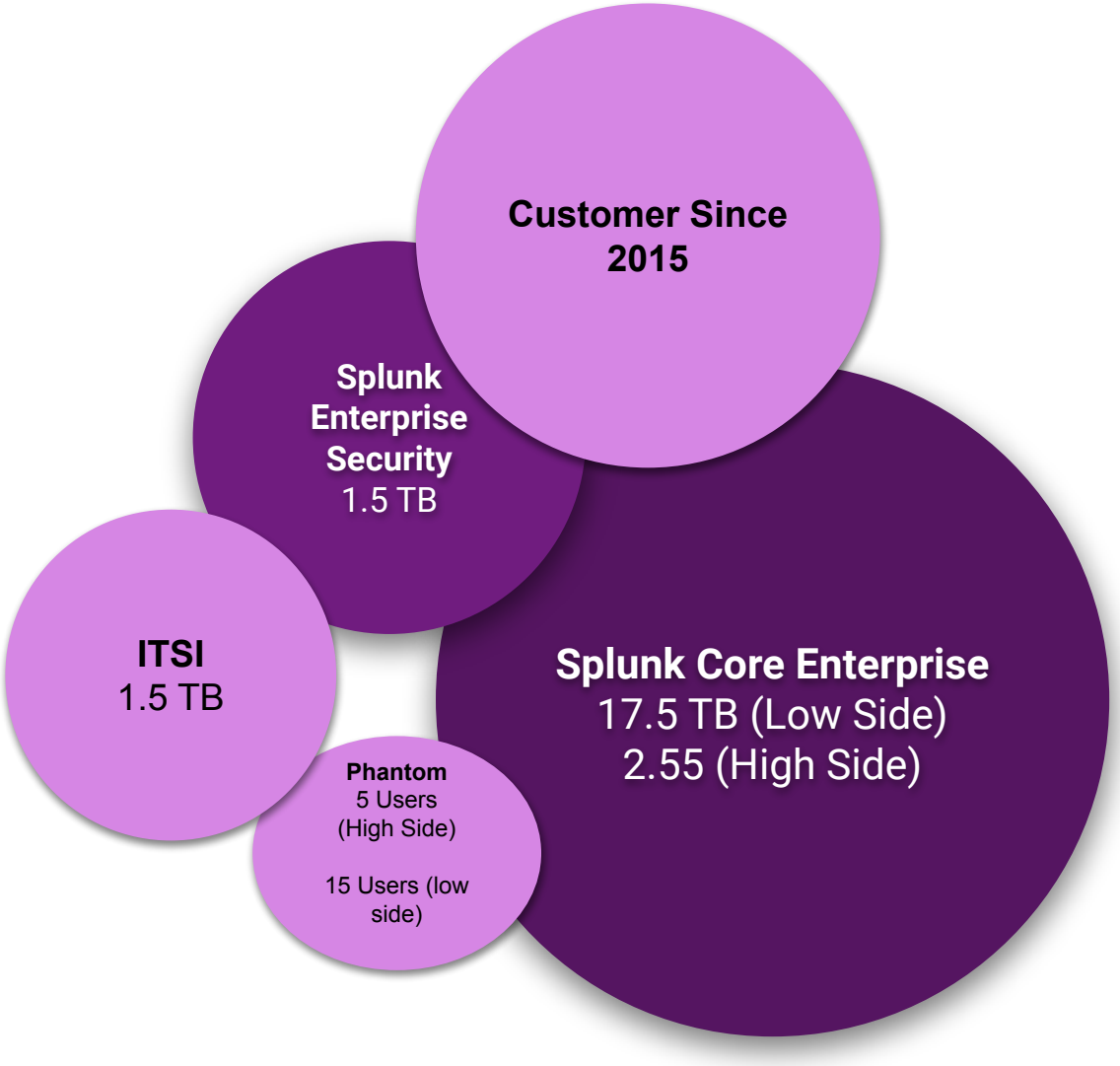
Amanda O'Neill
Customer Success Manager
Success planning aligned to strategic objectives, enablement & best practices.

Eric Jensen
Professional Services
Development, Consulting / Expert Services, Customer Education, Custom End-User Training.

Connor Westbrook
Inside Sales Rep
Inside Account Owner



LMCO Splunk Product: Overview



Prof. Services

Enterprise FTE

Edu & Support

On Demand Credits
Dedicated TSAM
Specialized Training Plan

Customer Success

Tier 1 CSM

LMCO Internal Splunk Site

https://tiny.lmco.com/entsplunk

Presenter Intro

Hunter Pavlovich

Solutions Engineer

Amin Hamidi

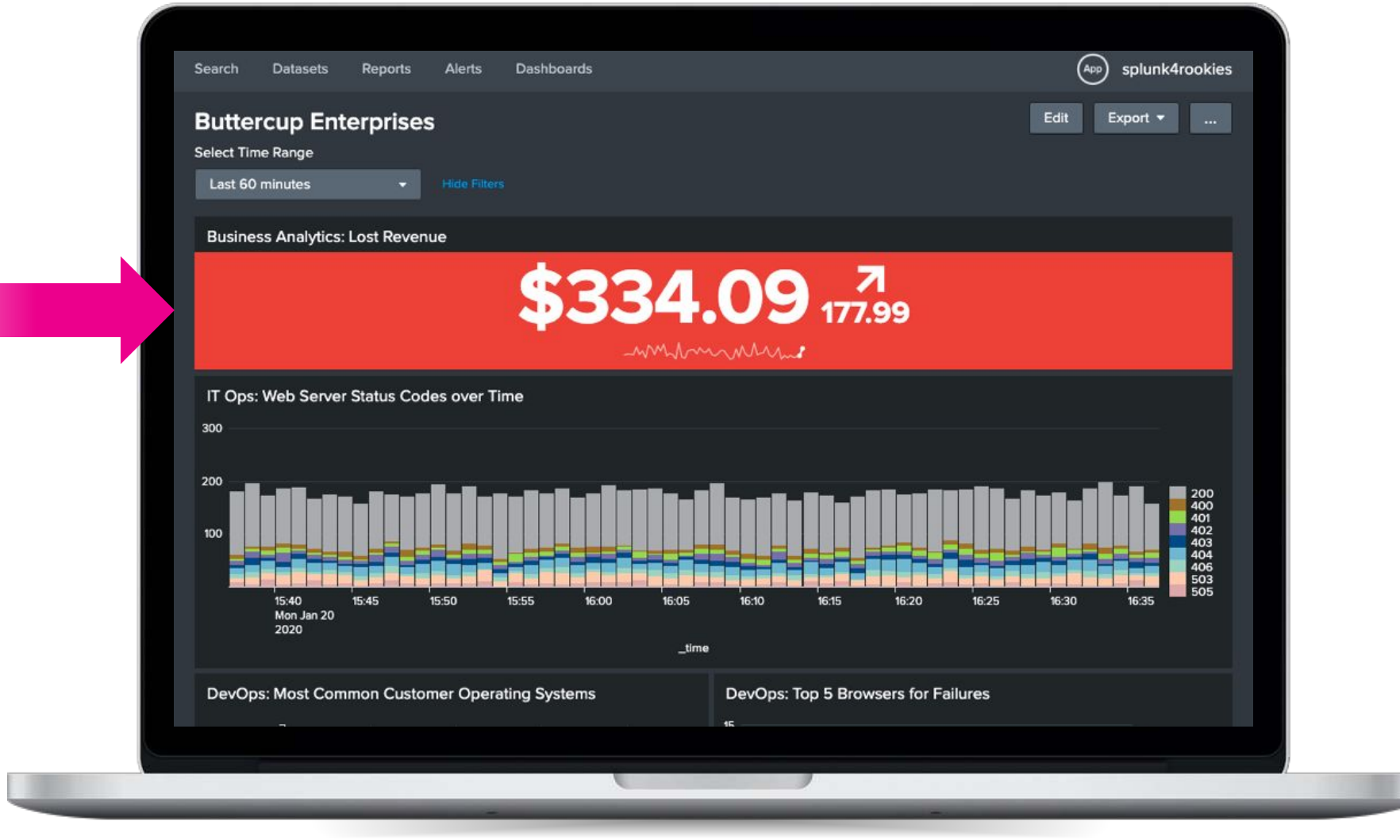
Solutions Engineer

Yang Lowe

Solutions Engineer

Agenda for Today's Workshop

- ✔ The value of data
- ✔ Splunk's investigative approach to data
- ✔ Creating a Splunk app
- ✔ Adding data
- ✔ Searching and reporting
- ✔ Extracting a new field (schema-on-the-fly!)
- ✔ Create a dynamic dashboard for multiple use cases



Task 1 > Register and Create Your Environment

Lab Guide | Page 3

splunk> turn data into doing

Register and Create Your Environment

Lab Guide | Page 3

Register:

http://splunk4rookies.com/10203/self_register

- Keep registration tab open so you do not lose the link to your instance!
- Today's slide deck and lab guide were emailed to all attendees, but please let us know if you still need these materials

Your link will take a few minutes to spin up so please be patient!

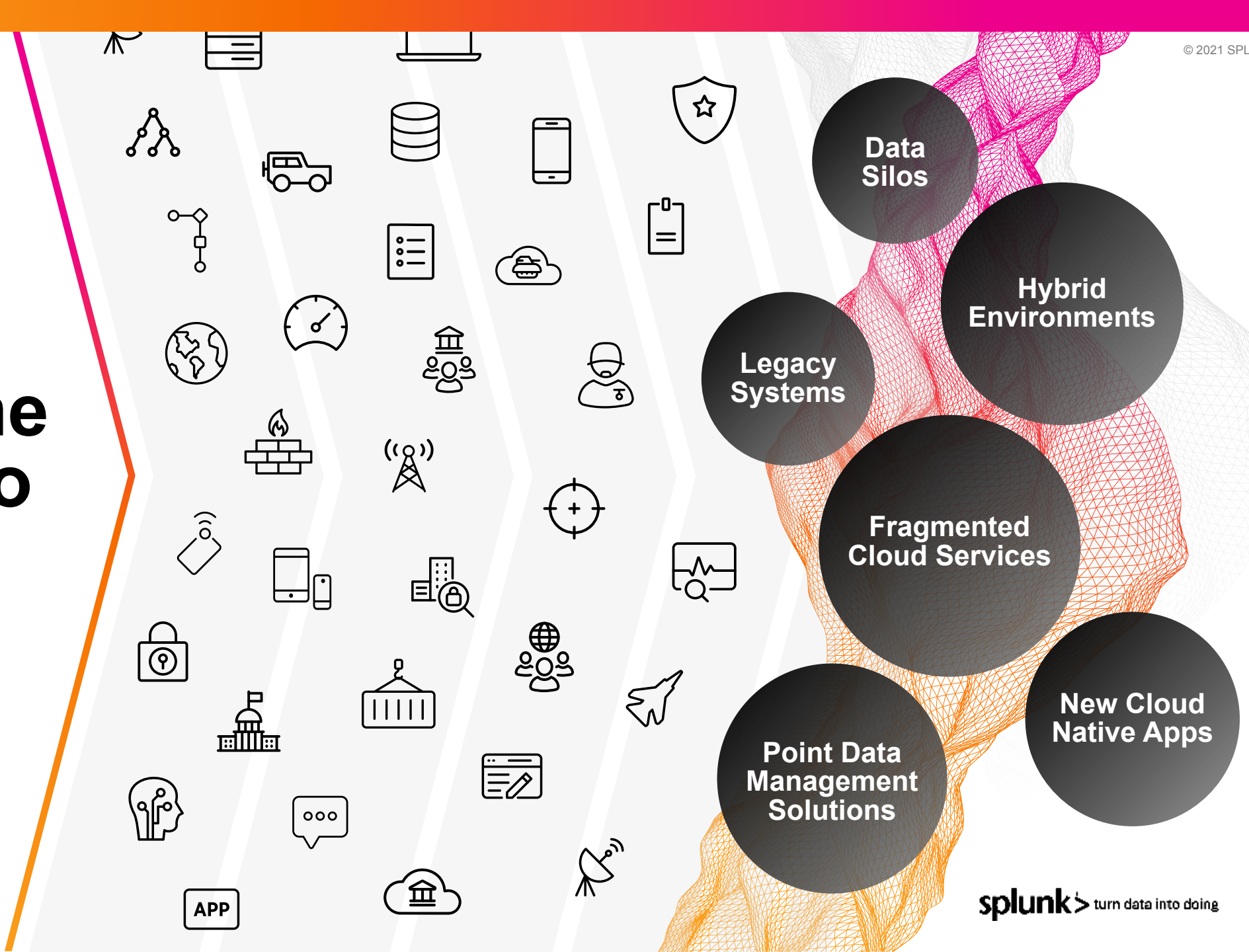
Every Company Has a Universe of Real-time Data

Creating More Opportunities and Threats than Ever Before

- Inventory RFID'S
- Assembly Robots
- Databases
- Business Apps
- Warehouse Utilization Systems
- Control Units
- New Technology
- New Data Streams
- Networks
- New Devices

splunk> turn data into doing

Turning Real-time Data Into Action is Hard



splunk> turn data into doing

splunk>

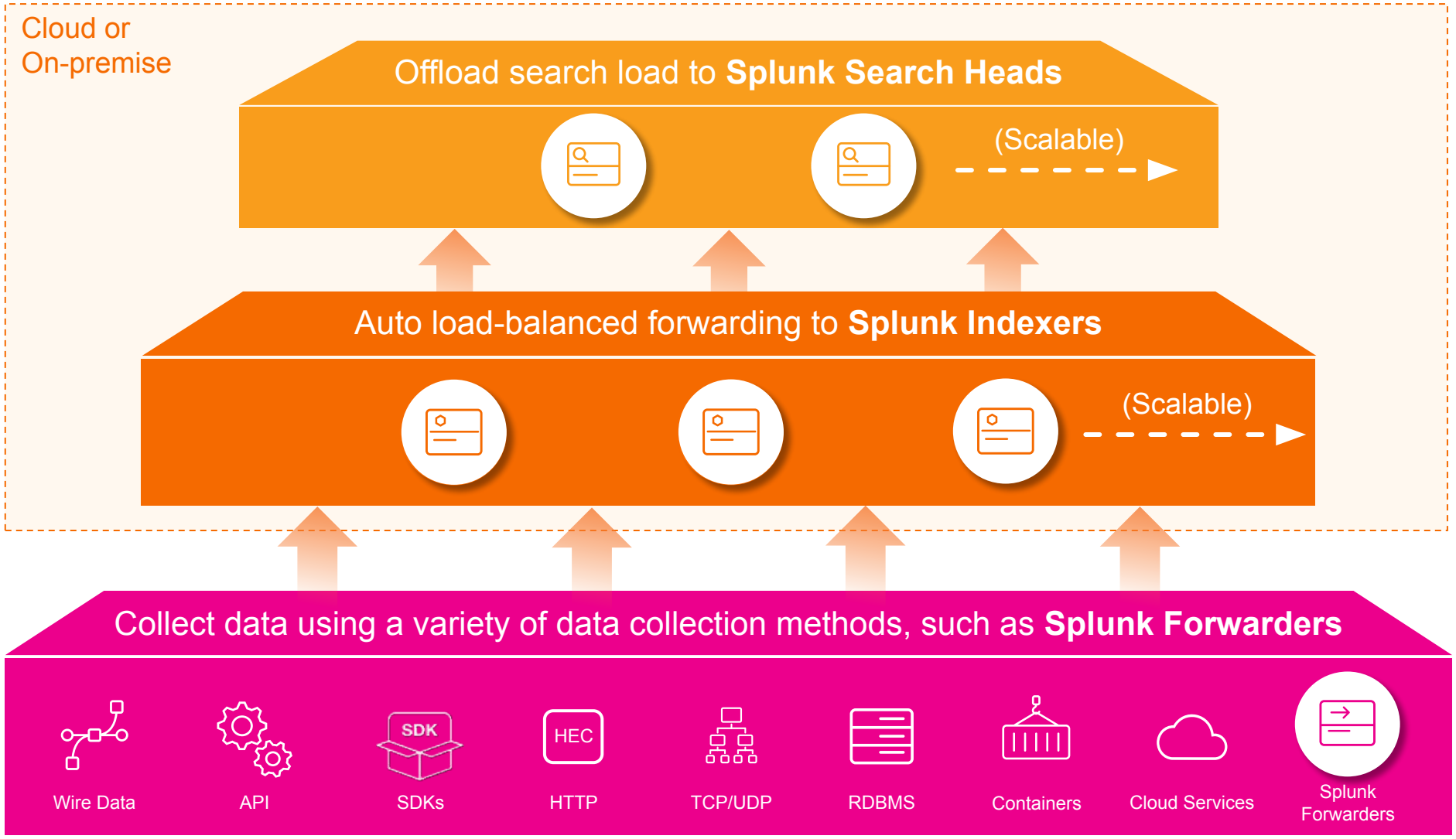
The Data-to-Everything Platform

- IT
- Security
- DevOps
- Business Operations

splunk> turn data into doing

Scales to Petabytes Per Day

Enterprise-Class Scale, Resilience and Interoperability



> Distribute Searches to Indexers
> Can be clustered (active-active)

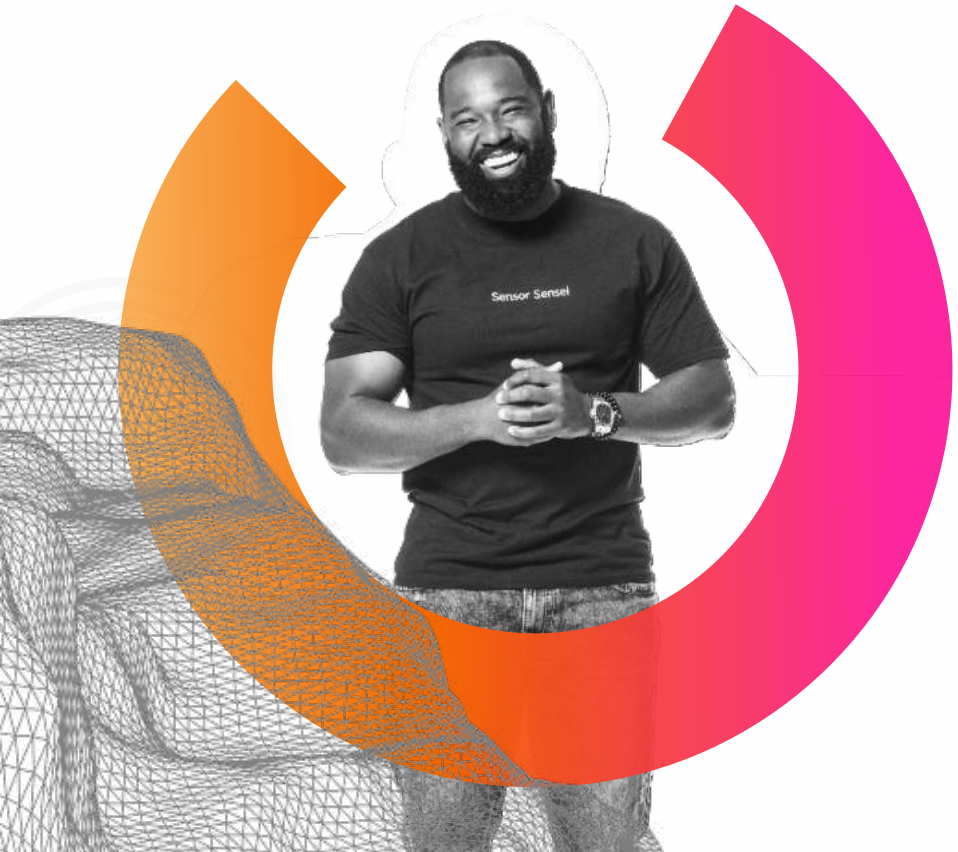
> Receive and store raw data
> Data is analysed and indexed
> Can be clustered (active-active)

> Collect/monitor and forward data to Indexers
> Collection options for a variety of data sources

splunk> turn data into doing

splunk>

The Data-to-Everything Platform



Act

Investigate

Monitor

Analyze

Any **Structure**

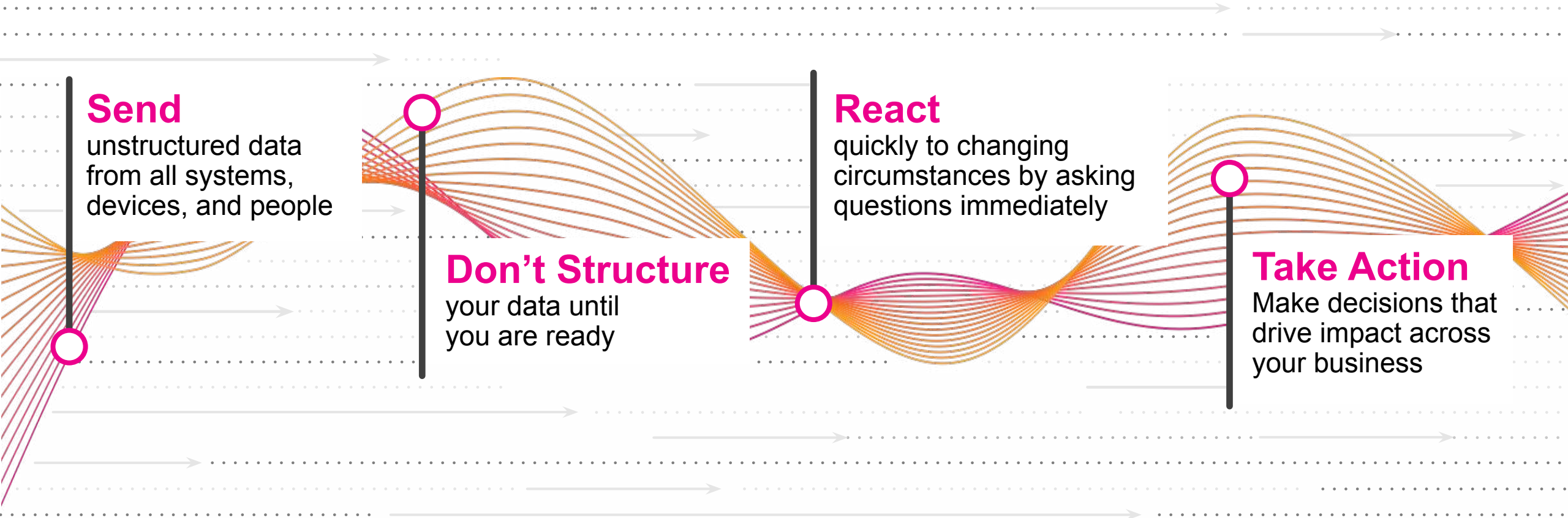
Any **Source**

Any **Time Scale**

splunk> turn data into doing

Spot Risk and Opportunity in Your Complex Data

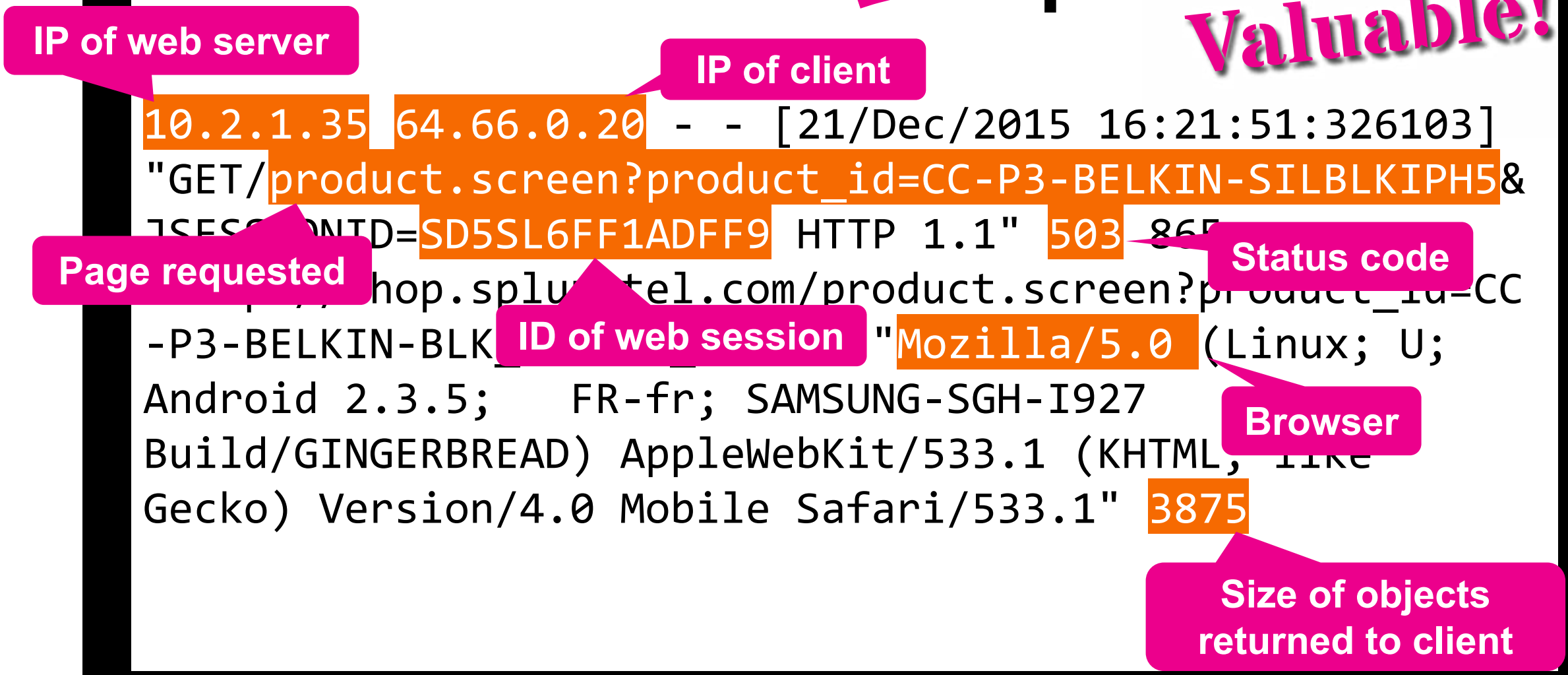
We solved one of the biggest challenges in data with our investigative approach



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
```

Machine Data is ~~Complex~~ Valuable!

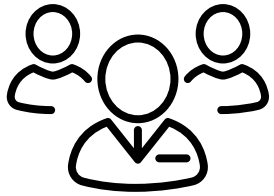


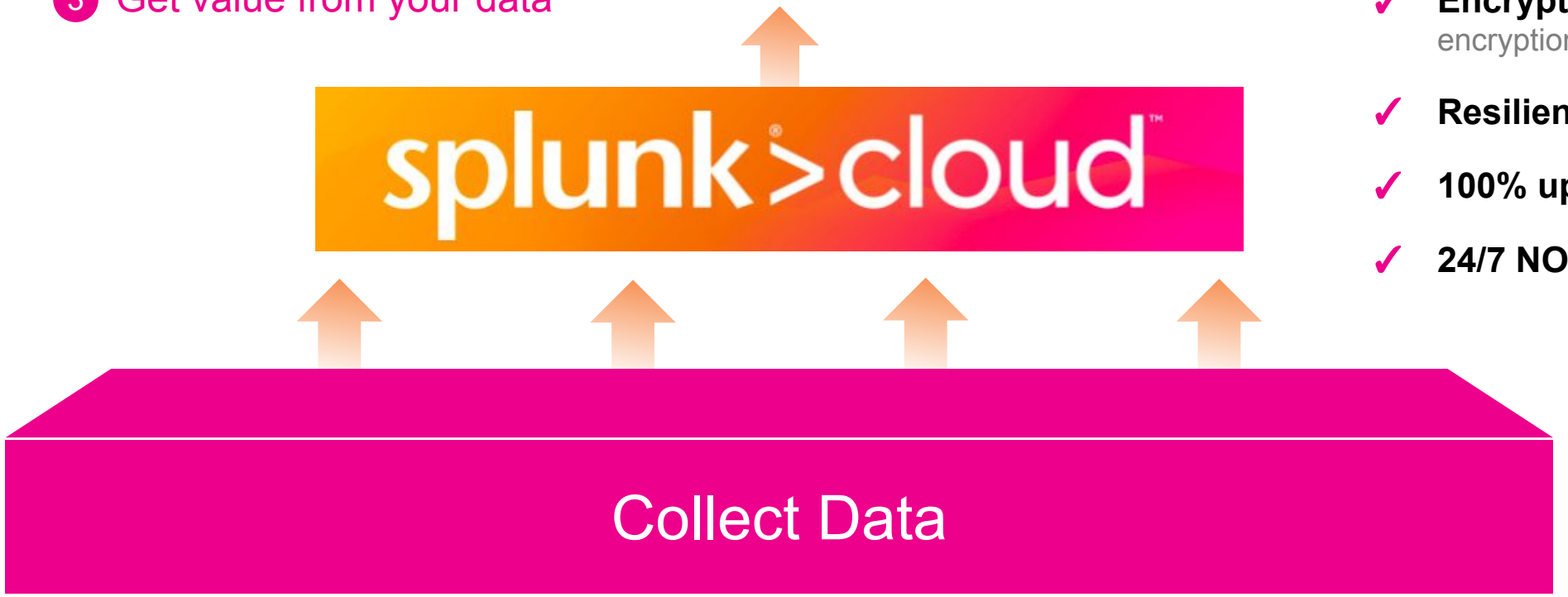
Splunk as a Service

Fastest time to value, minimum infrastructure, maximum value

Three simple steps:

1. Onboard data
2. Onboard users
3. Get value from your data



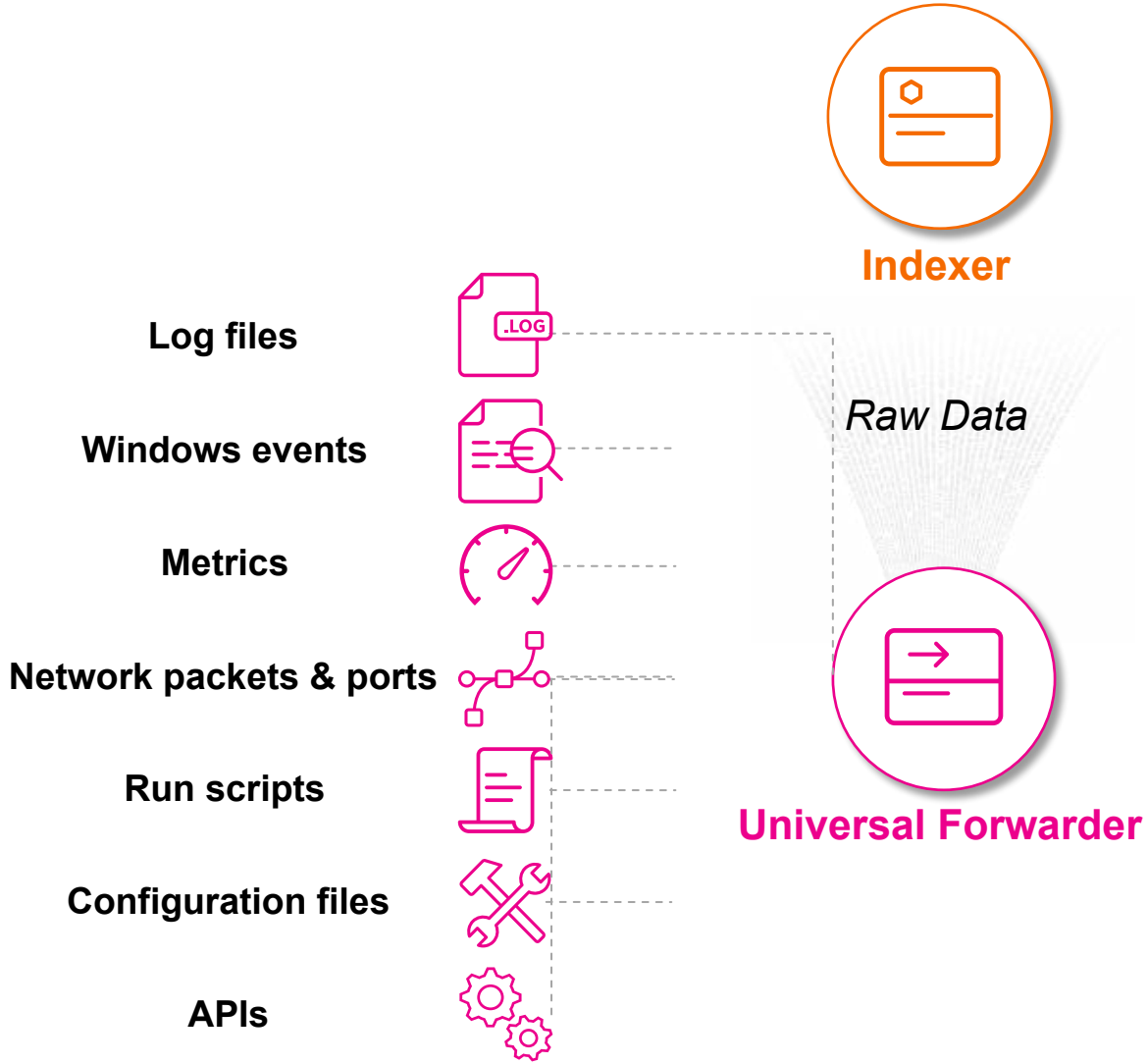


- ✓ **Software as a service (SaaS)**
- ✓ **Secure** - ISO27001, SOC2 Type 2, PCI, HIPAA, FedRAMP
- ✓ **Encryption-in-transit** - optional encryption-at-rest
- ✓ **Resilient infrastructure**
- ✓ **100% uptime guarantee**
- ✓ **24/7 NOC/SOC support team**

> **Splunk Cloud Service Description:** https://bit.ly/SplunkCloudServDesc

What is a Universal Forwarder?

- Reliable collection of data from remote locations
- Includes methods for collecting from a variety of data sources
- Simple, but packed with lots of goodness:
  - ✓ Buffering / guaranteed delivery
  - ✓ Encryption
  - ✓ Compression
  - ✓ Load balancing
  - ✓ And more!
- Very small footprint
- Just forwards data – no parsing beforehand!



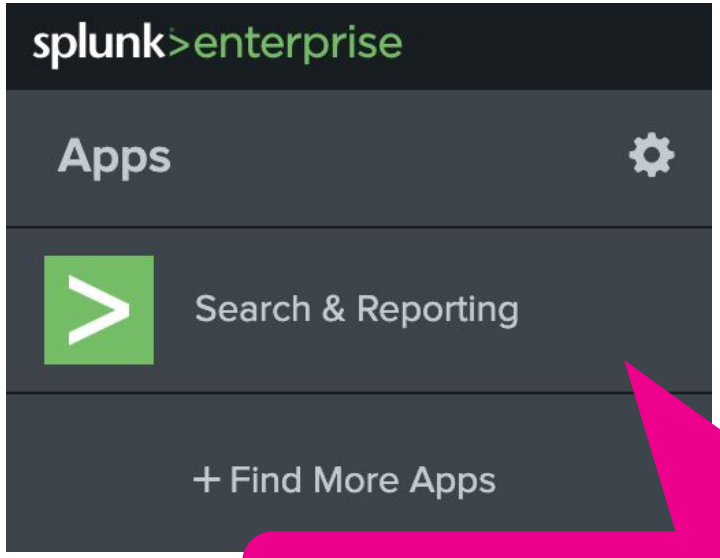
Today's Environment

Pre-loaded sample data

Combined Indexer & Search Head

Log in to Splunk

Username: admin
Password: changeme



Default generic "app" for searching your data

Q & A | Break

splunk> turn data into doing

Task 2 > Create an App and Add Data to Splunk

Lab Guide | Page 5

splunk> turn data into doing

Apps and Add-ons

- Built either by Splunk, our technology partners or members of our user community
- Prebuilt packages that help to enhance and extend the Splunk platform
- Provide content and capabilities – such as reports, dashboards and integrations – for a specific technology, purpose or use case, with the flexibility to customise for your own needs
- Over 2000 free apps and add-ons available from https://splunkbase.splunk.com/

Apps

✔ Content designed to bring fast time-to-value from your data in Splunk, including pre-built dashboards, reports, alerts, visualisations and workflows

Add-ons

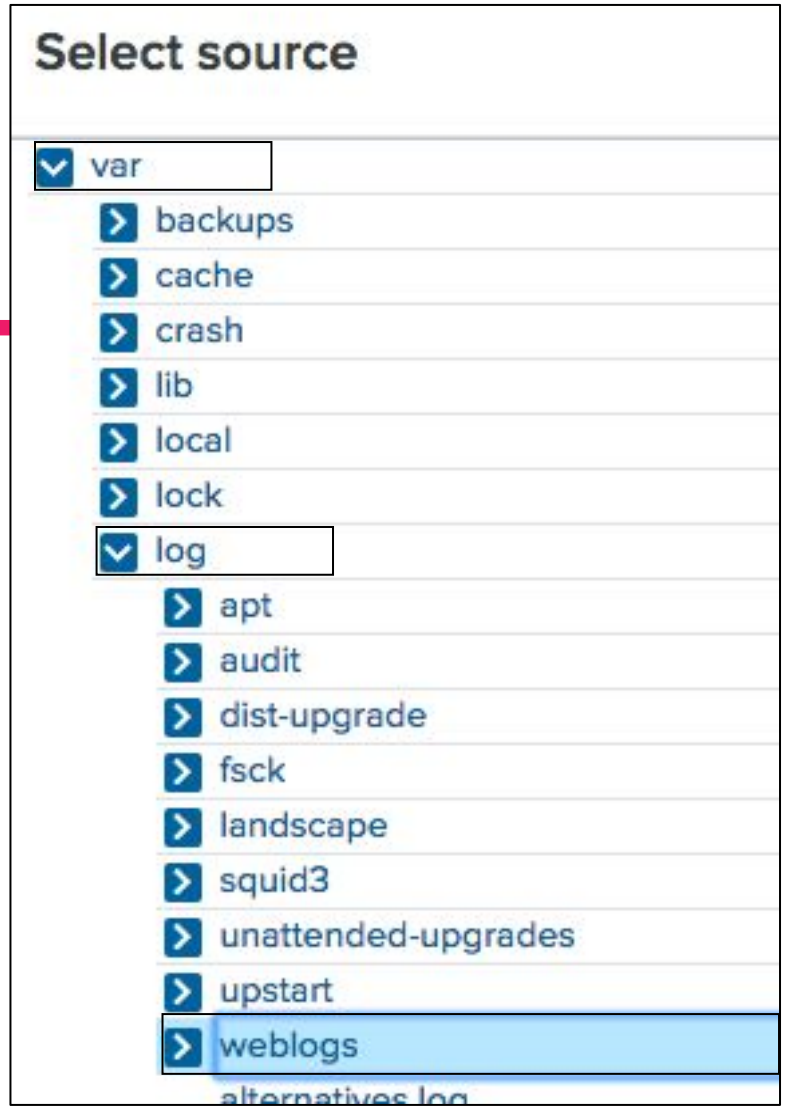
✔ Provide specific capabilities to Splunk, such as getting data in, mapping data, or providing saved searches and macros

Task 2 > Create an App and Add Data to Splunk

Objectives

1. Create a new app
2. Monitor a directory: /var/log/weblogs
3. Select a source type: access_combined
4. View your data in Splunk

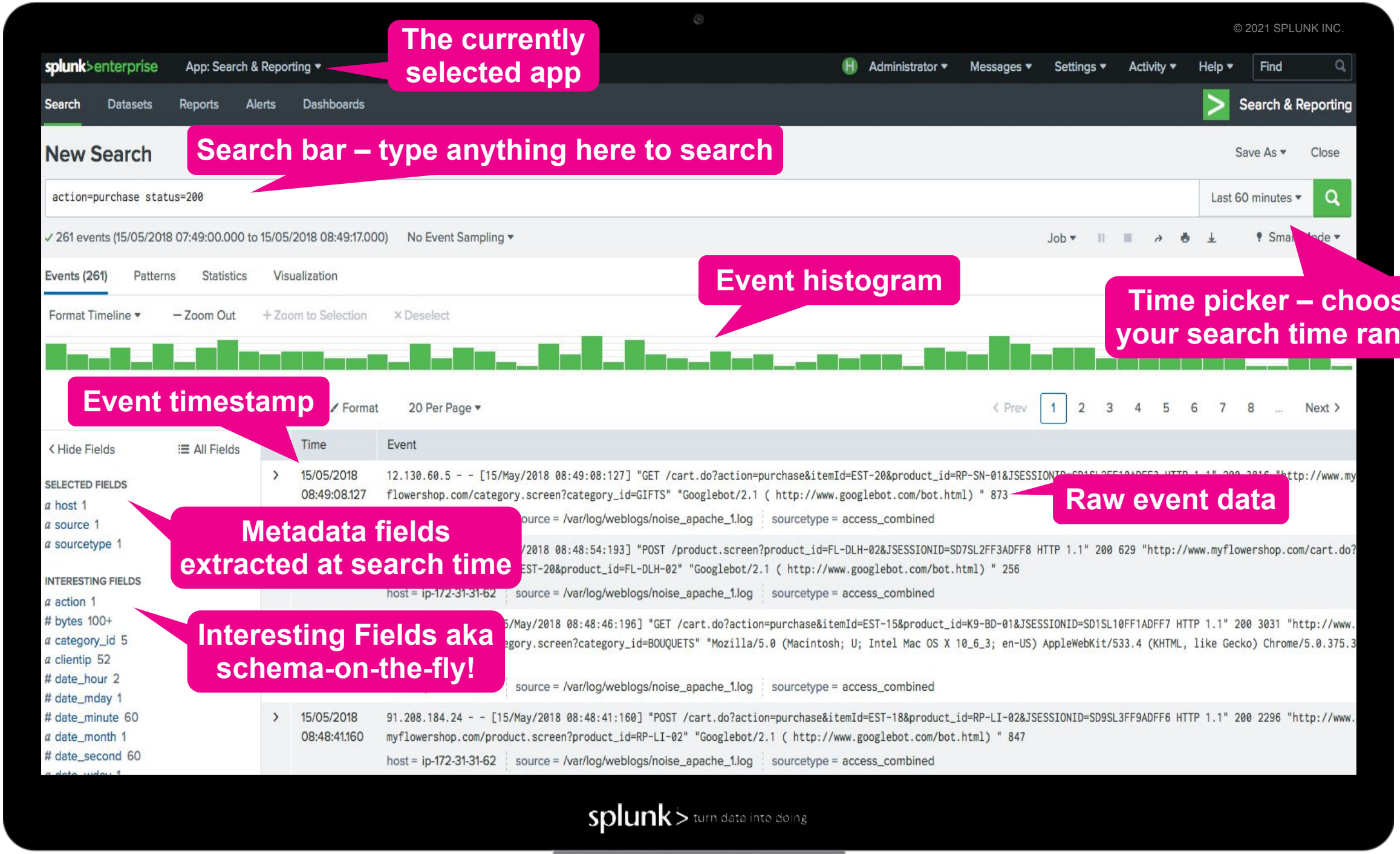
Goal



Task 2 > Create an App and Add Data to Splunk Break

Lab Guide | Pages 5-11

splunk> turn data into doing



splunk> turn data into doing

Start Searching in Splunk

Lab Guide | Page 12

- `503 purchase`
  Finds all events that contain the words “503” and “purchase”
- `503 p*`
  Finds all events containing “503” and words beginning with “p”
- `503 (purchase OR addtocart)`
  Boolean operators (`AND`/`OR`/`NOT`) - must be UPPERCASE!
- `status=503 action=purchase`
  Use *fieldname* = *value* to return accurate results

Challenge Task

Lab Guide | Page 13

Solution Page 31

How can we find events with a status of 200 that are NOT purchase events?

```
status=200 NOT action=purchase
```

```
status=200 action!=purchase
```

Splunk's 'Search Processing Language' (SPL)

Search terms

Commands

```
action=purchase | stats count by status | rename count as "number of events"
```

Pipe character: Output of left is input to right

Functions

e.g. `action=purchase`

`| stats count by status`

status	count
200	641
400	42
404	51
406	44
503	95

`| rename count as "number of events"`

status	number of events
200	641
400	42
404	51
406	44
503	95

Want to know more? Check out:

> **Splunk Quick Reference Guide:** http://bit.ly/S4R-QuickRef

> **Splunk Docs:** https://docs.splunk.com

Search Overview

- **Keywords:** Search for a single word (e.g., error) or group of words (e.g., error password)
- **Booleans:** NOT, OR, AND; AND is implied; MUST be uppercase; can use ()'s to force precedence sourcetype=vendor_sales OR (sourcetype=access_combined action=purchase)
- **Phrases:** "web error" (different than web AND error)
- **Field Searches:** status=404, user=admin
- **Wildcard(*):** status=40* matches 40, 40a, 404, etc; starting keywords with a wildcard is a very inefficient
- **Comparisons:** =,!=,<=,>=,<,> status>399, user!=admin

Organization Overview

- **table**: returns table containing only specified fields in the result set
- **rename**: renames a field in results
- **fields**: includes or excludes specified fields
- **dedup**: removes duplicates from results
- **sort**: sorts results by specified field
- **lookup**: adds field values from external sources (e.g., csv files)

Transforming Commands Overview

- **Transforming Commands**
  - Massage raw data into a data table
  - ”Transforms” specifies cell values for each event into a numerical values that you can use for statistical purposes
  - Is required to ”transform” search results into visualizations
- **Transforming Commands include:**
  - top
  - rare
  - **chart**
  - **timechart**
  - **stats**
  - geostats

eval Command Overview

- **eval allows you to calculate and manipulate field values in your report**
  - *eval fieldname1 = expression1 [, fieldname2 = expression2…]*
- **Support a variety of functions (some of them can be referenced in the quick guide)**
- **Results of eval written to either new or existing field you specify**
  - If the destination field exists, the values of the field are replaced by the results of eval
  - Indexed data is not modified, and no new data is written into the index
  - Field Values are treated in a case-sensitive manner

Today's Scenario: Buttercup Enterprises

Your Company

- Buttercup Enterprises is a large national online retailer operating in the US, which sells a variety of books, clothing and other gifts through its online webstore
- Buttercup Enterprises have recently invested in Splunk and now they want to start making use of it across the business

Your Role

- You are one of the chosen few: a Splunk power user!
- Your responsibility is to provide information to users throughout the company
- You gather data and statistics, and report on:
  - **Security**
  - **IT Operations**
  - **Development**
  - **Business intelligence**

What Does the Business Want to See?

One dashboard | Four panels > One for each team

- **IT Operations team | Task 3:** Investigate successful vs unsuccessful web server requests over time
- **DevOps team | Task 4:** Show the most common customer operating systems and which web browsers are experiencing the most failures
- **Sales/Business Analytics teams | Task 5:** Show lost revenue from the Buttercup Enterprises website
- **Security/Fraud teams | Task 6:** Show website activity by geographic location

splunk> turn data into doing

Task 3 >
IT Operations team

Investigate successful vs unsuccessful web server requests over time

Lab Guide | Page 14

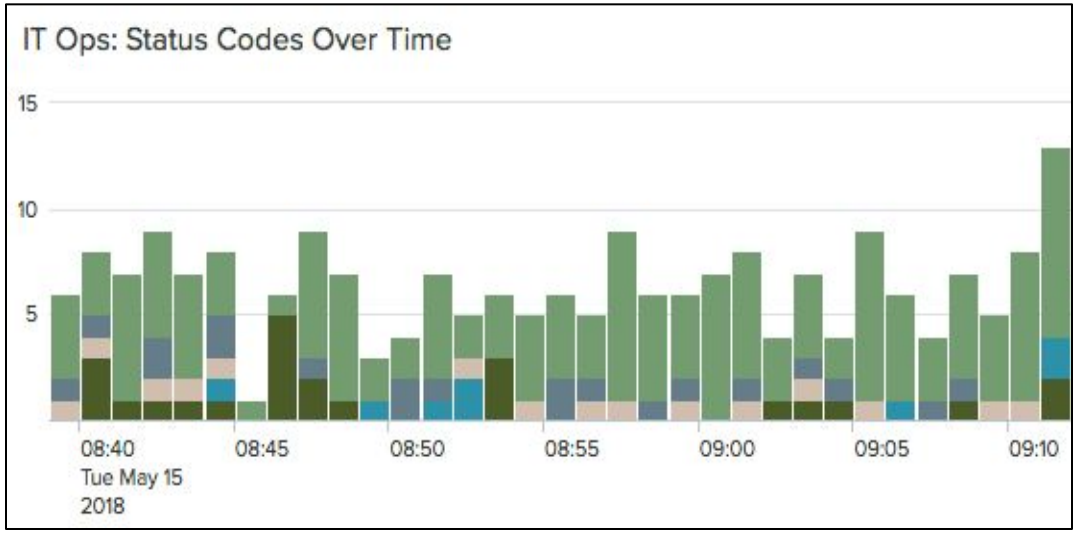
splunk> turn data into doing

Task 3 > IT Operations team

Objectives

1. Show all website purchase failures on over time
2. Use a stacked column chart visualization
3. Add your chart to a new dashboard

Goal



Task 3 > IT Operations team Break

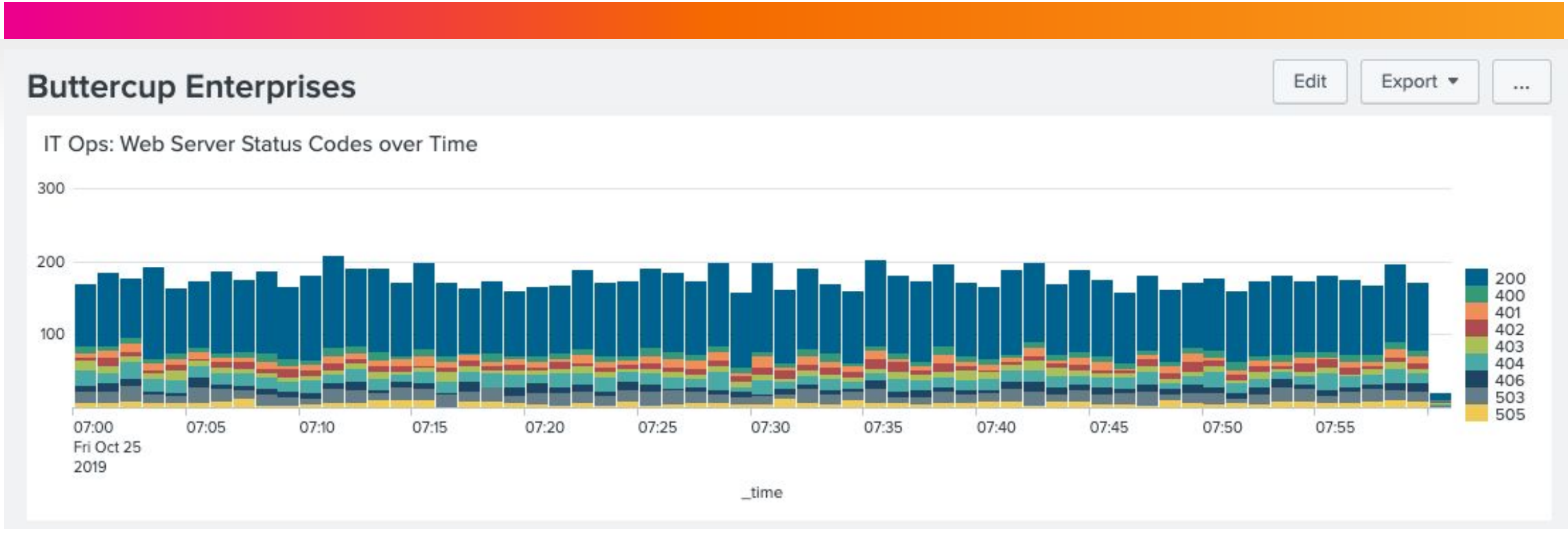
Lab Guide | Pages 14-16

splunk> turn data into doing

Your Dashboard so far...

Solution:

```
sourcetype=access_combined | timechart count by status
```



Task 4 >
DevOps team

Show the most common customer operating systems and which web browsers are experiencing the most failures

Lab Guide | Page 17

splunk> turn data into doing™

Task 4 > DevOps team

Objectives

1. Extract a new field: platform
2. Show the top values of the most common customer operating systems using a bar chart
3. Show the top 5 web browsers (or ‘useragents’) that are experiencing the most failures over time using an area chart
4. Add your charts to your existing dashboard

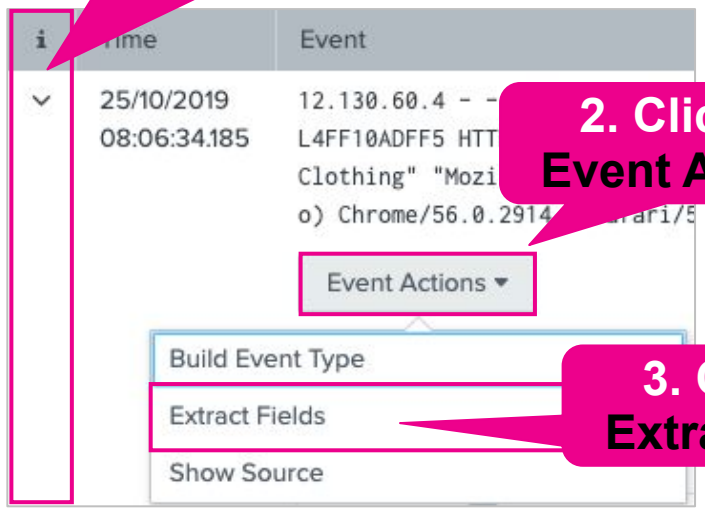
Goals

splunk> turn data into doing

Extracting a New Field

Lab Guide | Page 17

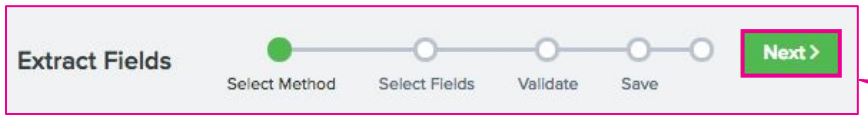
1. Click on the arrow to expand an event



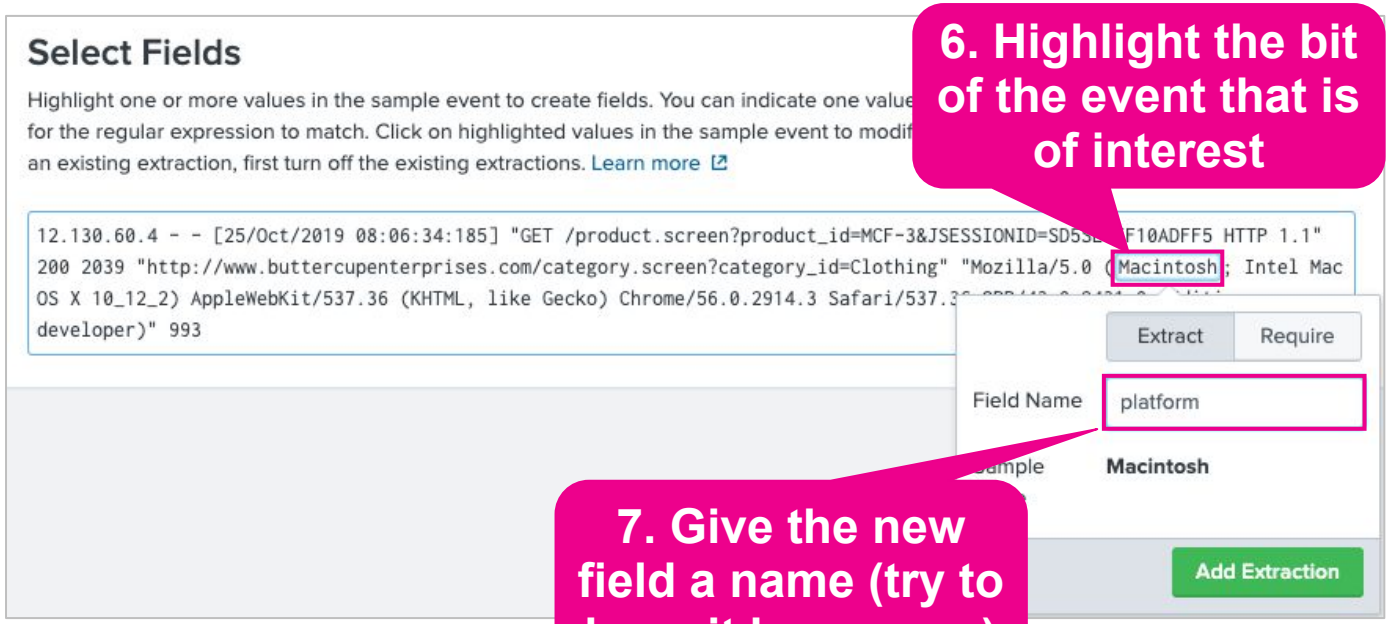
2. Click on Event Actions

3. Click on Extract Fields

4. Click on Regular Expression



5. Click on **Next**



6. Highlight the bit of the event that is of interest

7. Give the new field a name (try to keep it lowercase)

splunk> turn data into doing

Task 4 > DevOps team

Page 19 | Show the most common customer operating systems

Search

Search for all web server events

```
sourcetype="access_combined"
```

We can see operating system information in our events and after extracting a new field, we can now report on it!

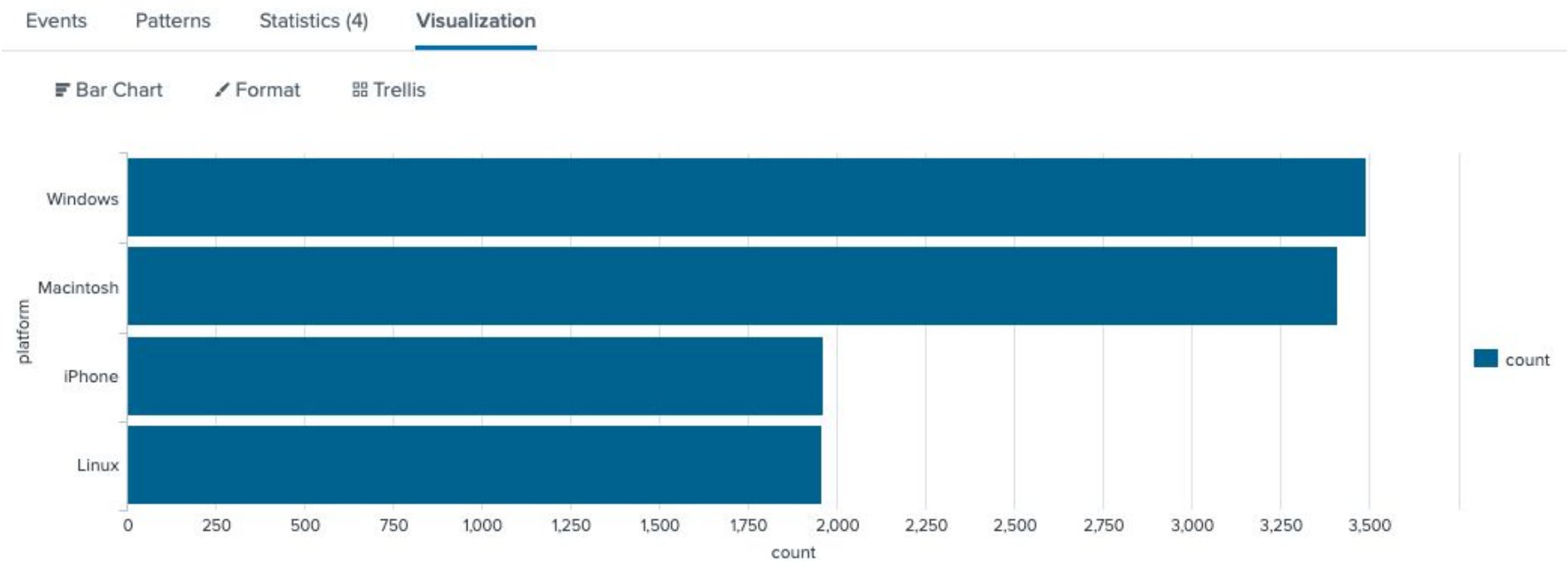
i	Time	Event
>	25/10/2019 08:06:34.185	12.130.60.4 - - [25/Oct/2019 08:06:34:185] "GET /product.screen?product_id=MCF-3&JSESSIONID=SD5SL4FF10ADFF5 HTTP 1.1" 200 2039 "http://www.buttercupenterprises.com/category.screen?category_id=Clothing" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2914.3 Safari/537.36 OPR/43.0.2431.0 (Edition developer)" 993 host = myserver | source = /var/log/weblogs/noise_apache_2.log | sourcetype = access_combined

Task 4 > DevOps team

Page 19 | Show the most common customer operating systems

Solution:

```
sourcetype=access_combined | top limit=5 platform
```



Task 4 > DevOps Team Break

Lab Guide | Pages 17-21

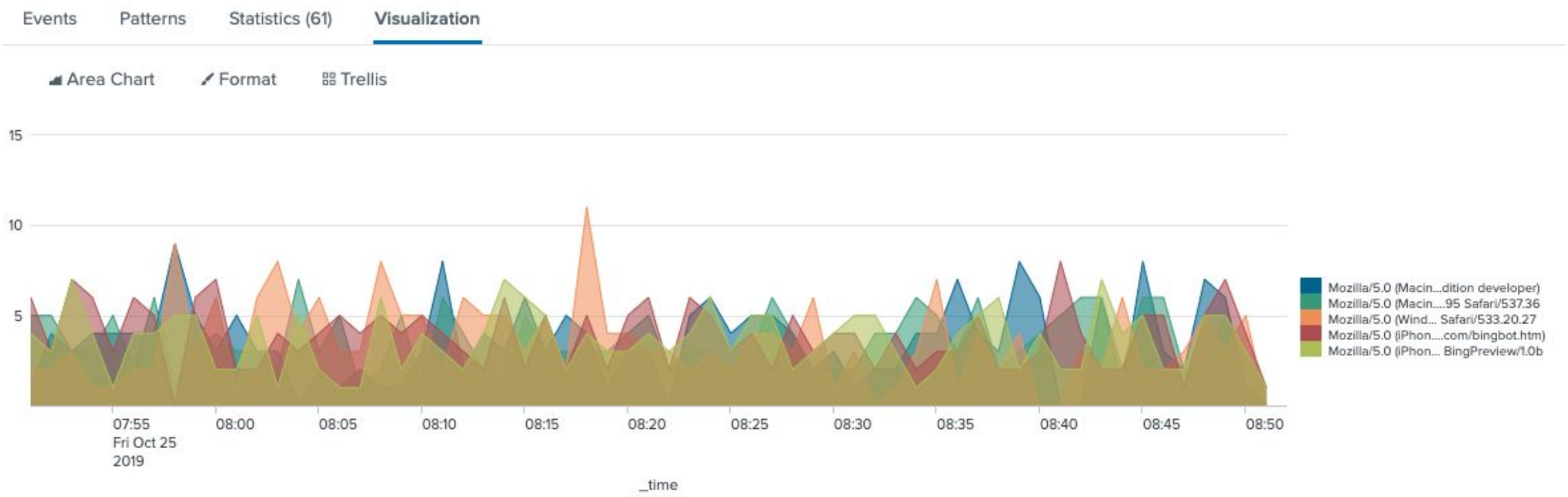
splunk> turn data into doing

Task 4 > DevOps team

Page 20 | Show which web browsers are experiencing the most failures

Solution:

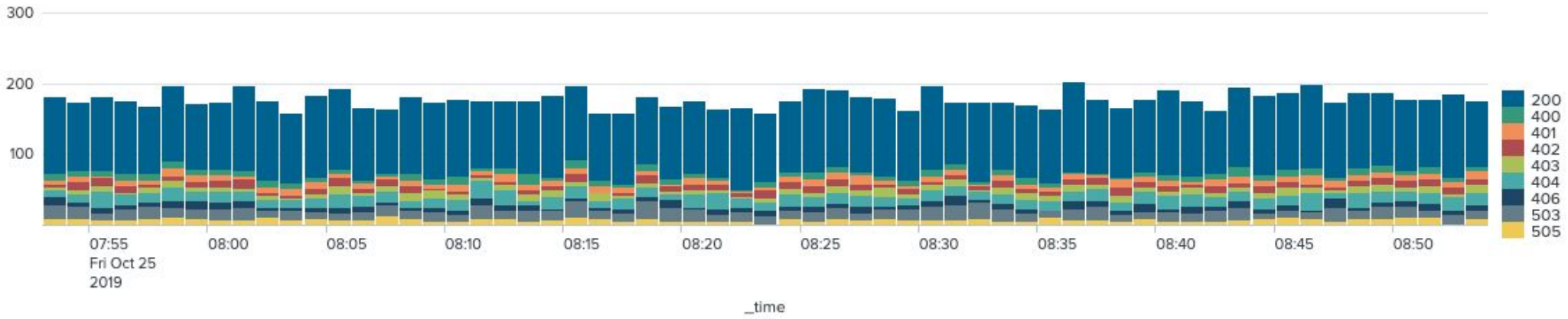
```
status>=400 | timechart count by useragent limit=5 useother=f
```



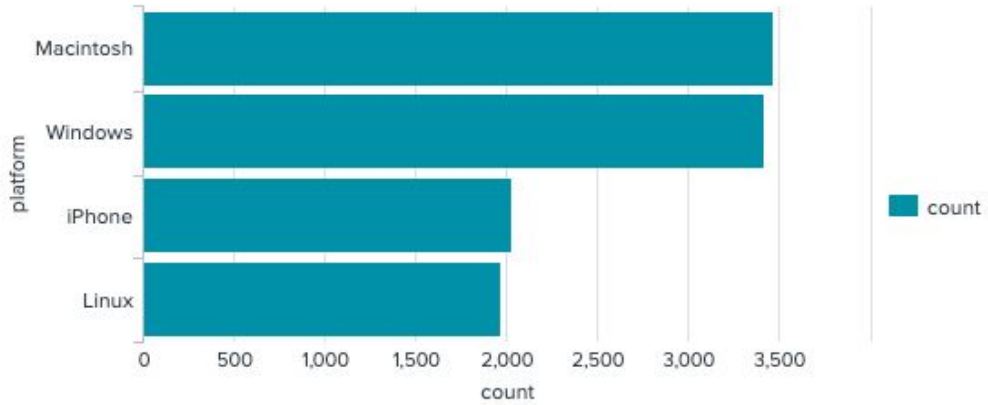
Buttercup Enterprises

Edit Export ...

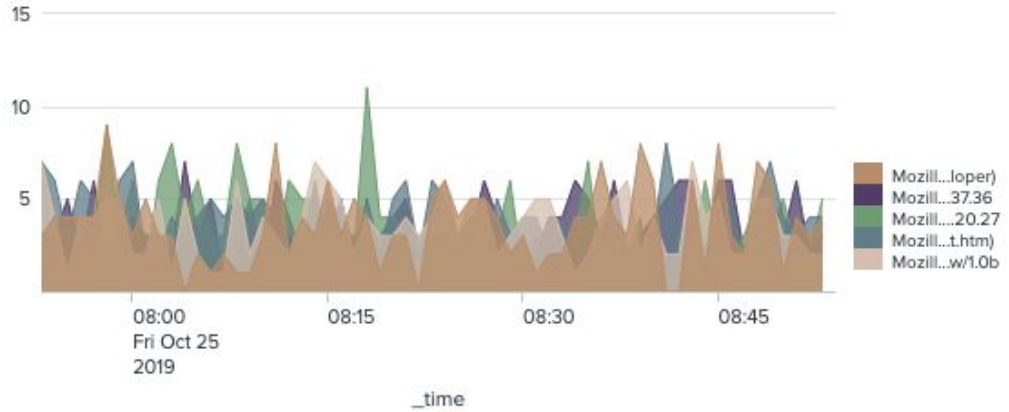
IT Ops: Web Server Status Codes over Time



DevOps: Most Common Customer Operating Systems



DevOps: Top 5 Browsers for Failures



Task 5 > Sales/Business Analytics teams

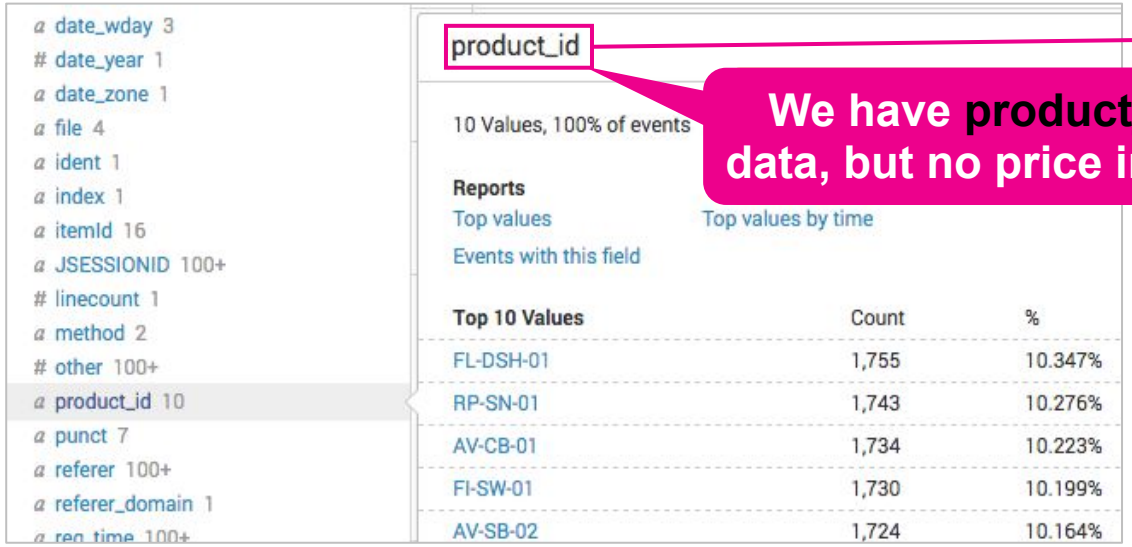
Show lost revenue from the website

Lab Guide | Page 22

splunk> turn data into doing

Task 5 > Sales/Business Analytics teams

Fields extracted from events by Splunk



We have **product_id** in our data, but no price information!

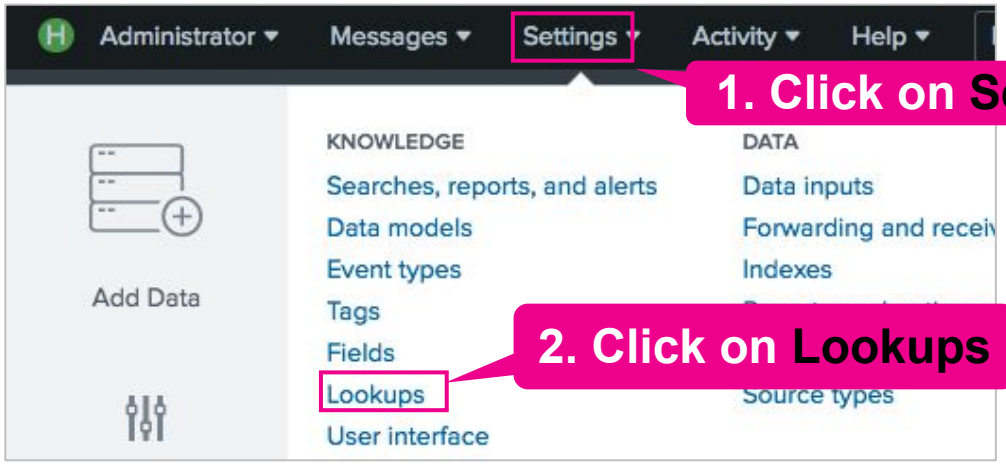
External CSV file

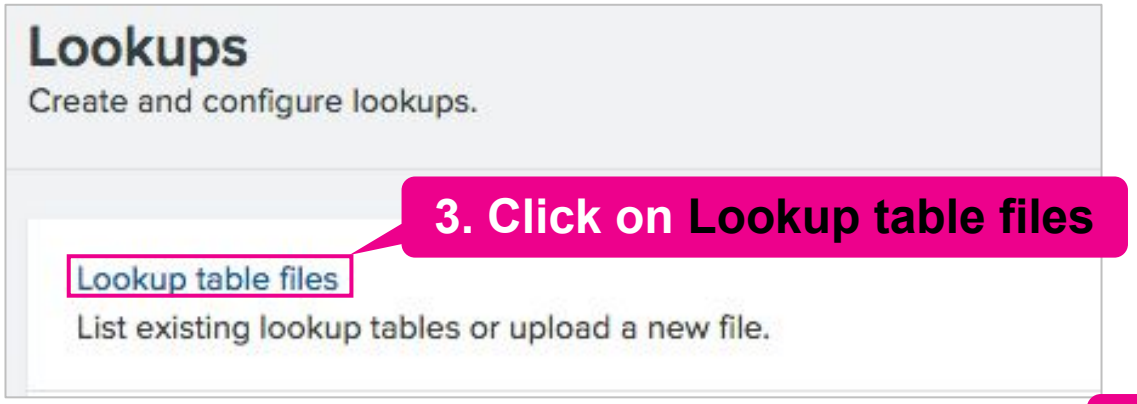
```
category,product_id,product_name,product_price
,BS-2,Batguy Slippers,25.7
CB-5,Mad Comics- Batg
CB-6,Mad Comics- Bron
Books,MCF-3,Mad Comics- Flym
Books,ZSG-2,Zombie Survival Guide,15.21
Clothing,CM-1,Costume- ManHawk,97.5
Gifts,DFS-2,Double Fudge Sundae,22.75
Gifts,PP-5,Pony Potpourri,9.99
Clothing,BW-3,Batguy Watch,9.99
```

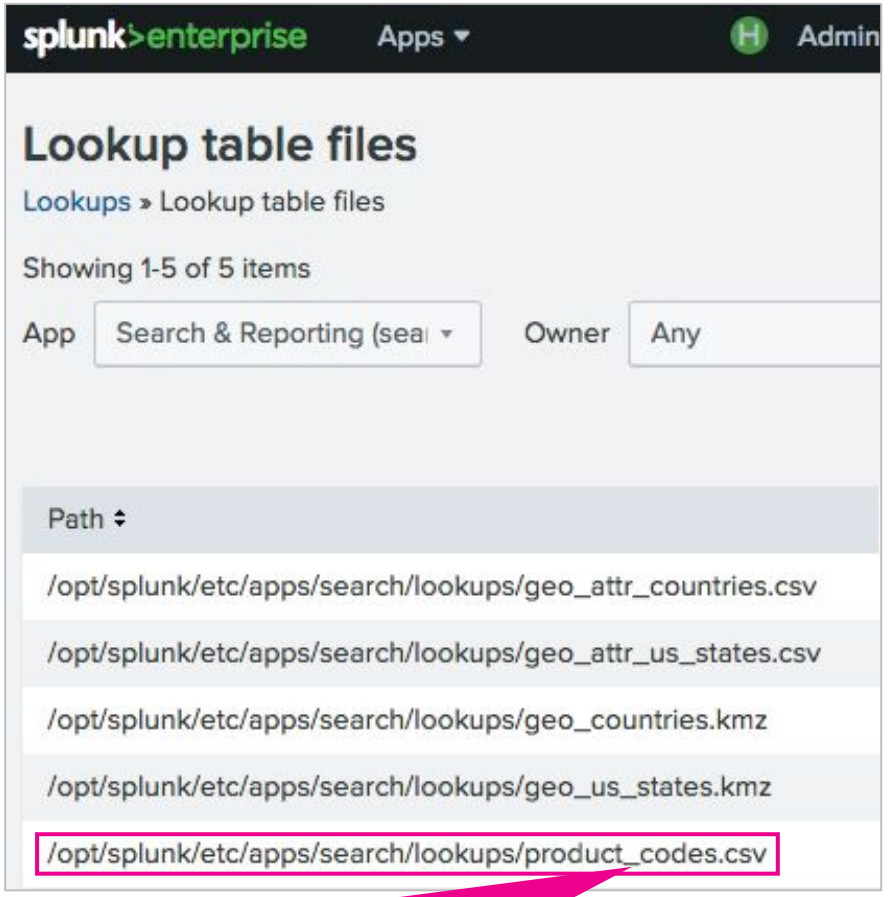
This is the information we need!

Verify Lookup File Exists

A lookup file has already been uploaded for you!







Enriching Data with the lookup Command

Usage:

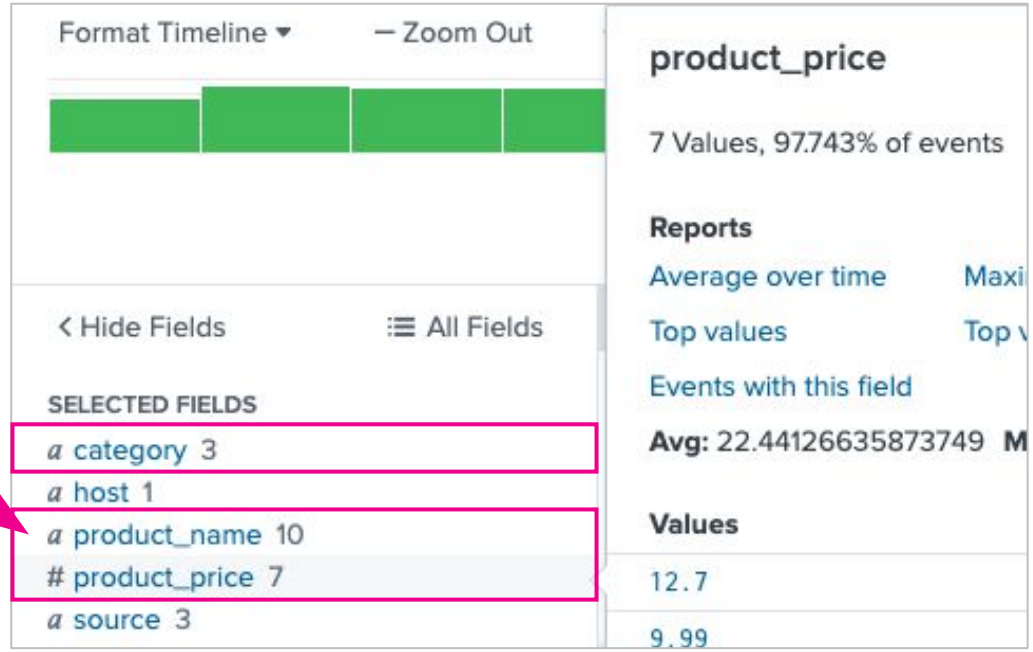
```
<your search> | lookup product_codes.csv product_id
```

Splunk command to enrich data on-the-fly

The name of the lookup file uploaded to Splunk

The field to join on - product_id is the field name both in the Splunk data and the lookup file

The lookup command retrieves the category, product_name and product_price fields from the lookup file



Task 5 > Sales/Business Analytics teams

Objectives

1. Use the lookup command to enrich the events with price data from our lookup file
2. Show lost website revenue using a Single Value visualization
3. Add your visualization to your existing dashboard

Goal

Task 5 > Sales/Business Analytics teams Break

Lab Guide | Pages 22-24

splunk> turn data into doing

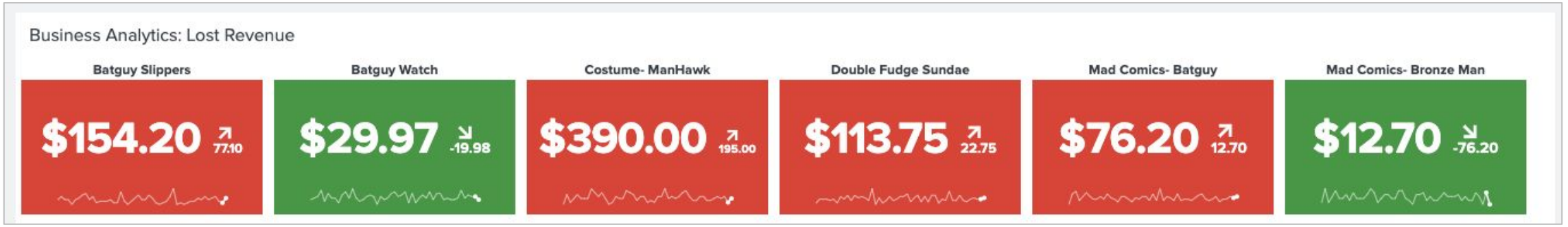
Task 5 > Challenge Task

Page 24 | Add a Single Value visualization to show the lost revenue from the company website

Challenge Task Solution:

```
action=purchase status>=400 | lookup product_codes.csv product_id | timechart sum(product_price)
```


```
...| timechart sum(product_price) by product_name
```



Task 6 > Security/Fraud teams

Show website activity by geographic location

Lab Guide | Page 25

splunk> turn data into doing

Obtaining Location Information with the `iplocation` and `geostats` Commands

Usage:

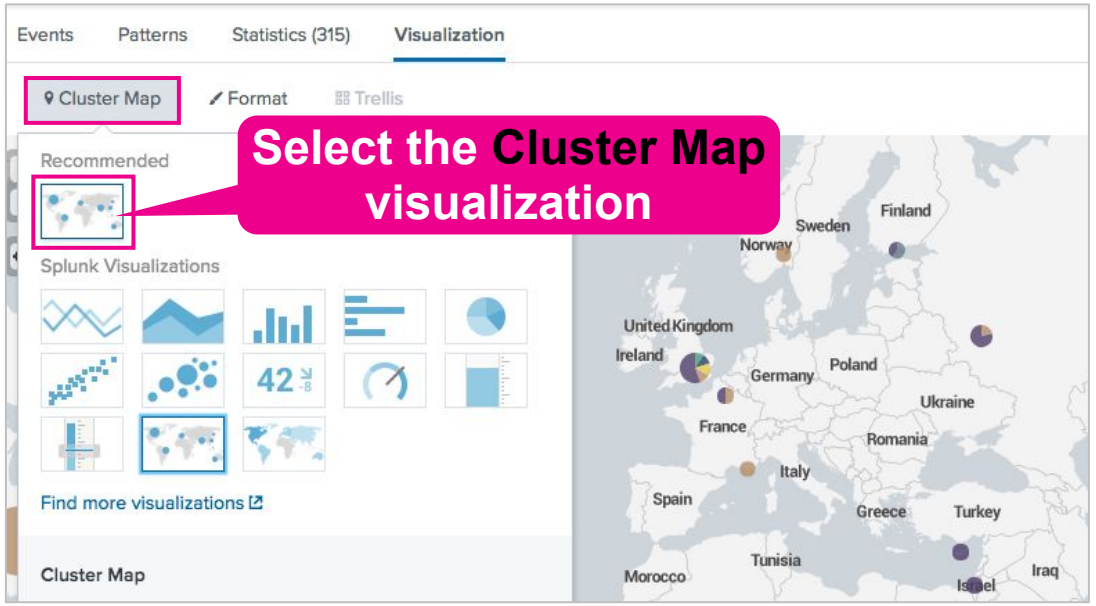
```
<your search> | iplocation clientip | geostats count by <field>
```

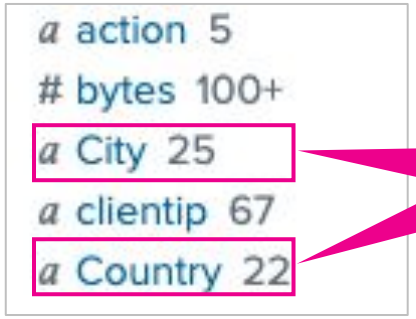
Enriches IP data on-the-fly with location data

The name of a field in your data that contains IP addresses

Generates the 'tiles' that will be rendered on the map when visualised

Split your results by a specific field for a more detailed analysis





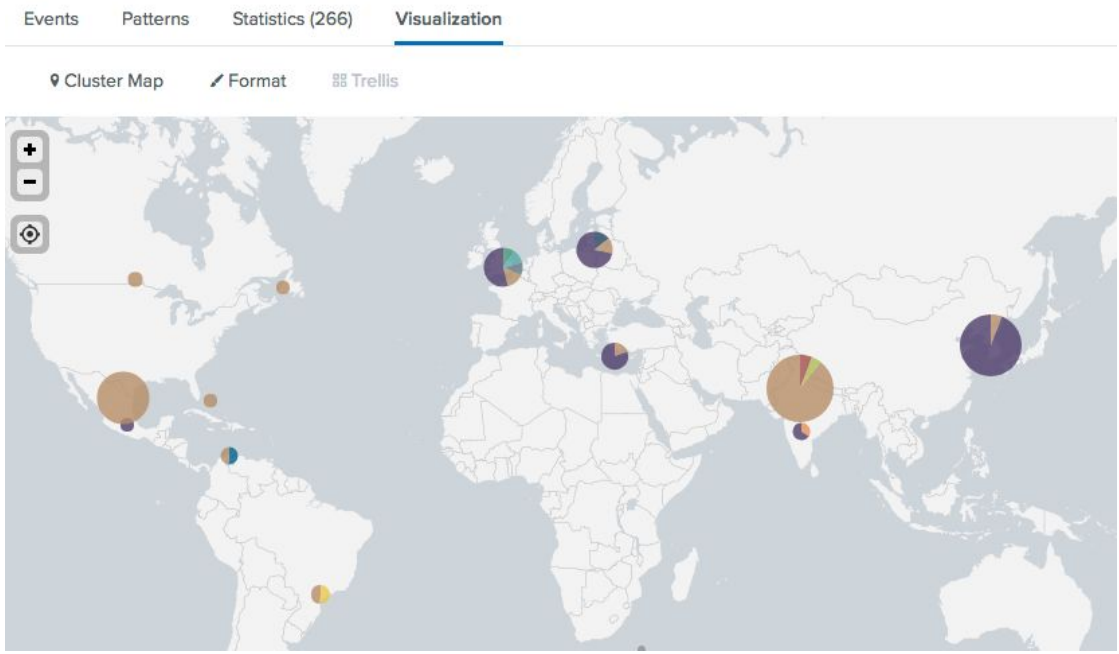
The iplocation command produces additional fields containing geographic data

Task 6 > Security/Fraud teams

Objectives

1. Use the iplocation command to enrich the events with location data
2. Create a world map showing the geographic location of all website activity down to the city level
3. Add your visualization to your existing dashboard

Goal



Task 6 > Security/Fraud teams Break

Lab Guide | Pages 25-26

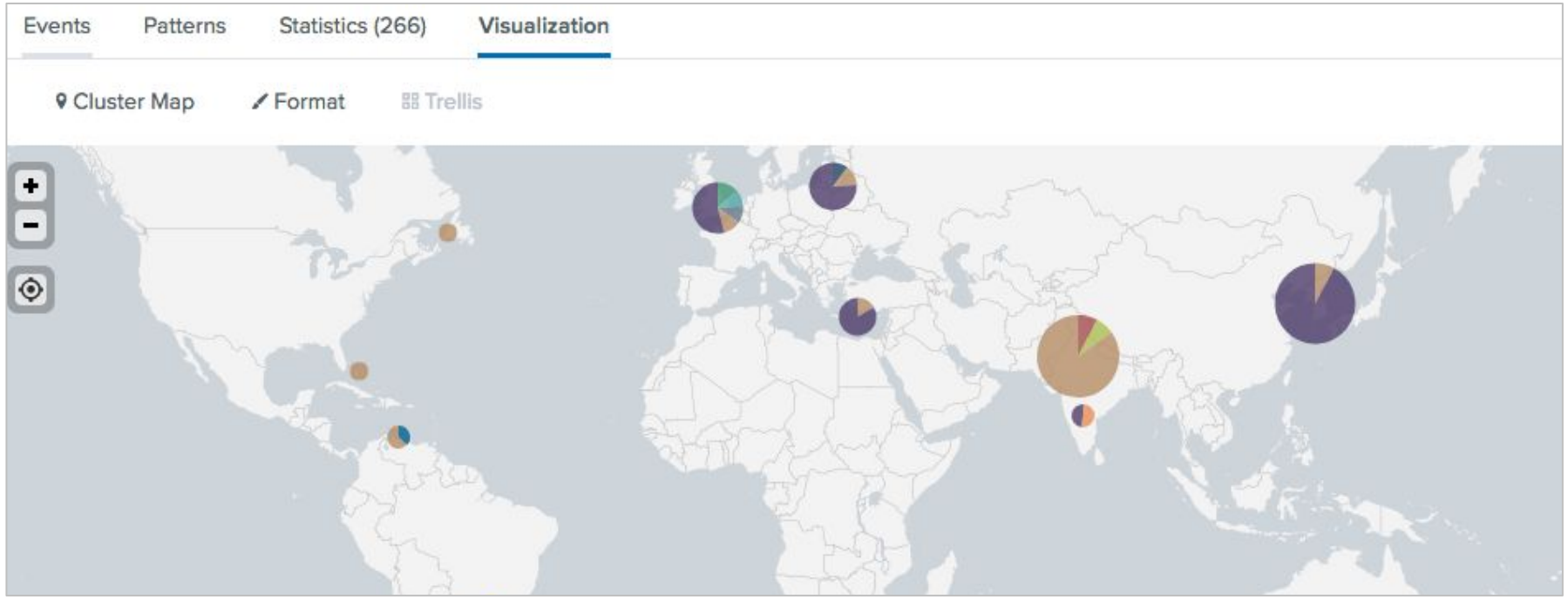
splunk> turn data into doing

Task 6 > Security/Fraud teams

Page 25 | Show website activity by geographic location

Solution:

```
sourcetype=access_combined | iplocation clientip | geostats count by City globallimit=0
```

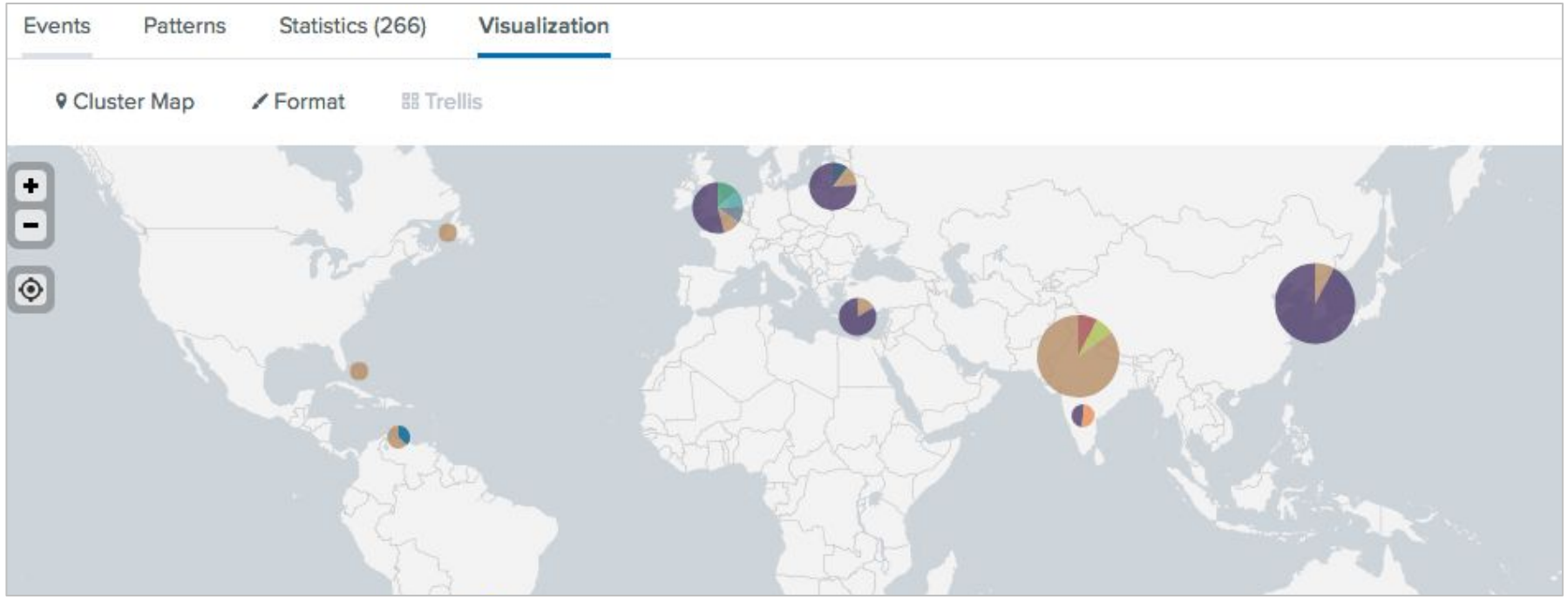


Task 6 > Challenge Task

Page 26 | Remove events coming from “United States” from the Cluster Map

Solution | Page 33:

```
sourcetype=access_combined | iplocation clientip | search Country!=“United States” |
geostats count by City
```



Task 7 > Enhance Your Dashboard

Lab Guide | Pages 27

splunk> turn data into doing®

Task 7 > Enhance Your Dashboard

Objectives

1. Add a shared time range picker to your dashboard and set all panels to use the new time range picker
2. Switch your dashboard to dark mode!

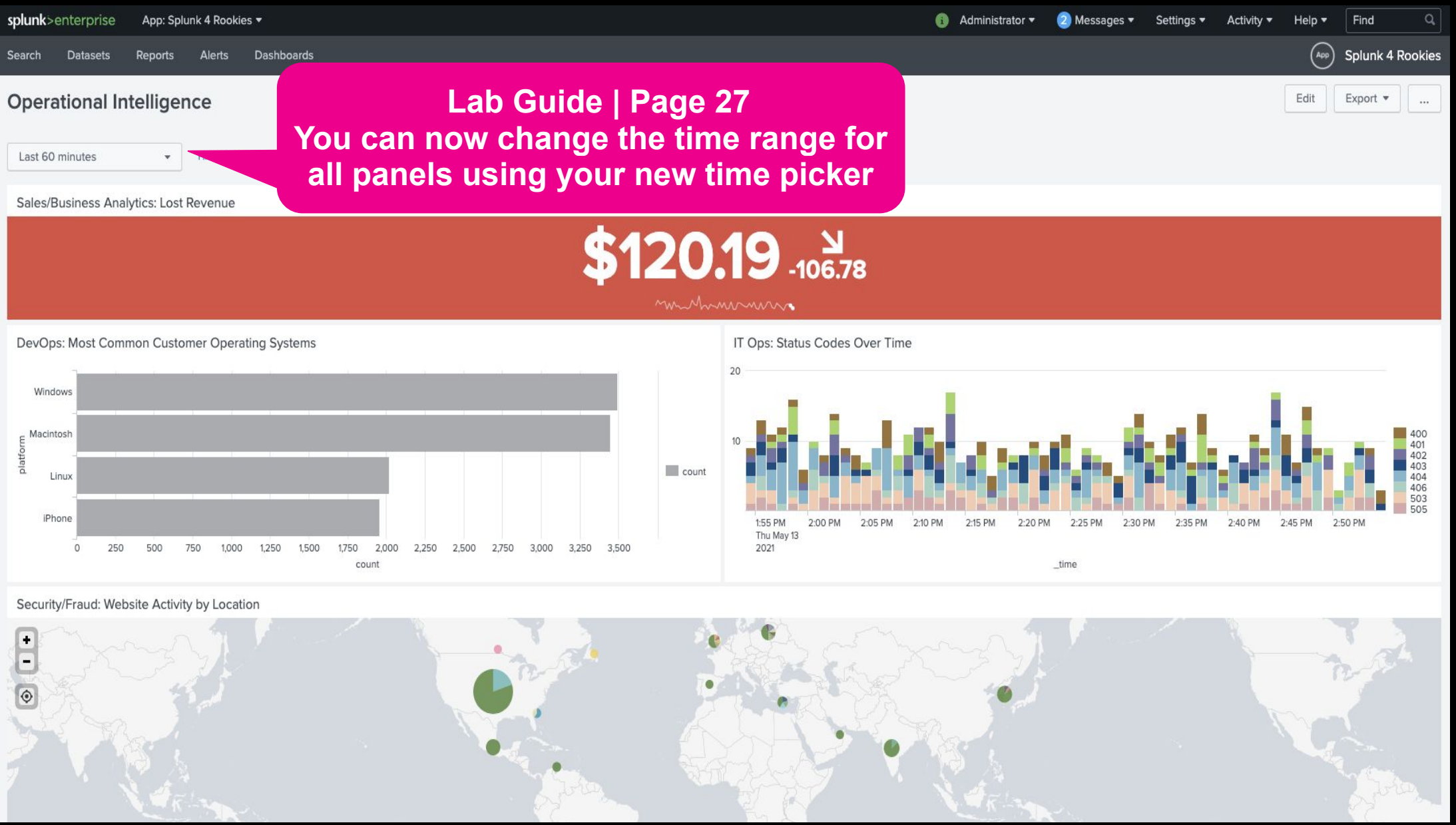
Goal

Task 7 > Enhance Your Dashboard Break

Lab Guide | Pages 27-30

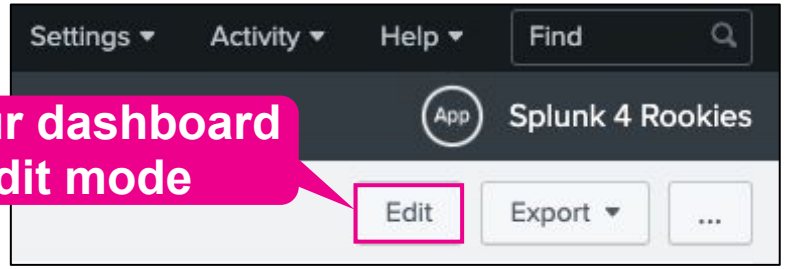
splunk> turn data into doing

Lab Guide | Page 27
You can now change the time range for all panels using your new time picker



Switch the dashboard to Dark Mode

Lab Guide | Page 30



1. Put your dashboard into edit mode

2. Toggle Dark Theme on

3. Save your dashboard and refresh the page to view your new dark dashboard!

splunk> turn data into doing

Congratulations | You Finished!

How did you do?

Splunk Resources

splunk> turn data into doing™

Splunk Connected Experiences

Get actionable alerts, respond to notifications, view mobile-friendly dashboards, interact with augmented reality Splunk visualizations, and display dashboards on a TV

Splunk Mobile
Extend Splunk dashboards and alerts to mobile devices

Splunk Mobile for Apple Watch
Empower consumption and action on information via Apple Watch

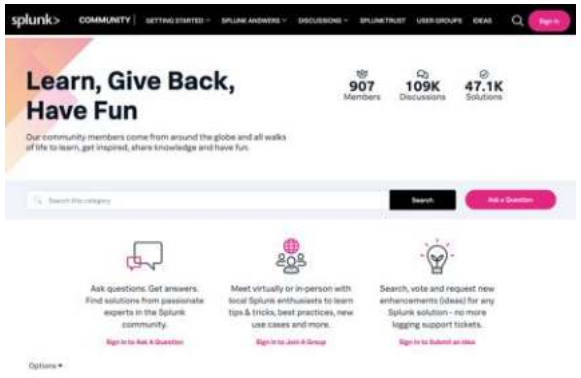
Splunk AR
Scan QR codes or NFC tags for on-demand insights via Augmented Reality

Splunk TV
Display Splunk dashboards on an Apple TV

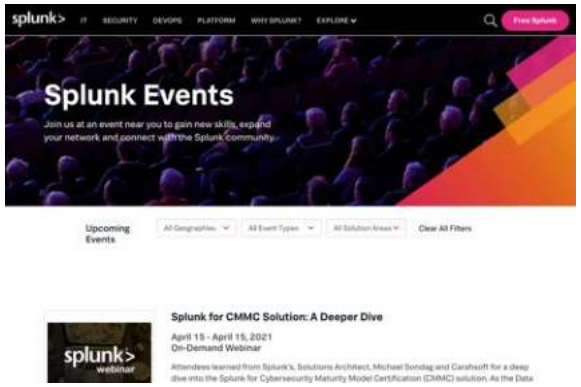
splunk> turn data into doing

Splunk's Thriving Community

Splunk Community

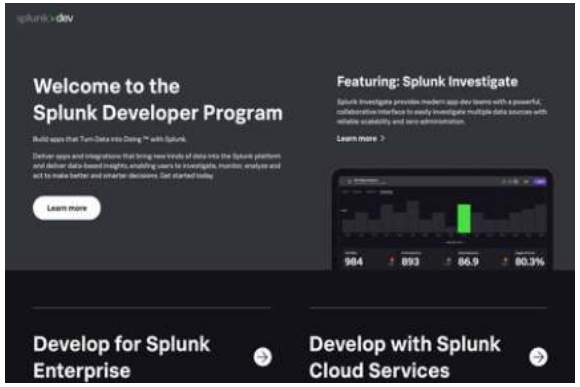


Splunk Events

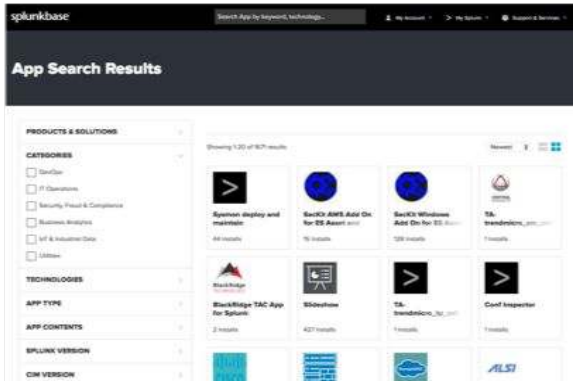


Documentation

Developer Resources

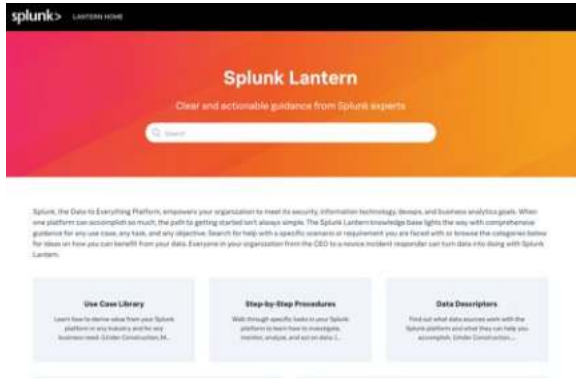


Splunkbase



Education

Splunk Lantern

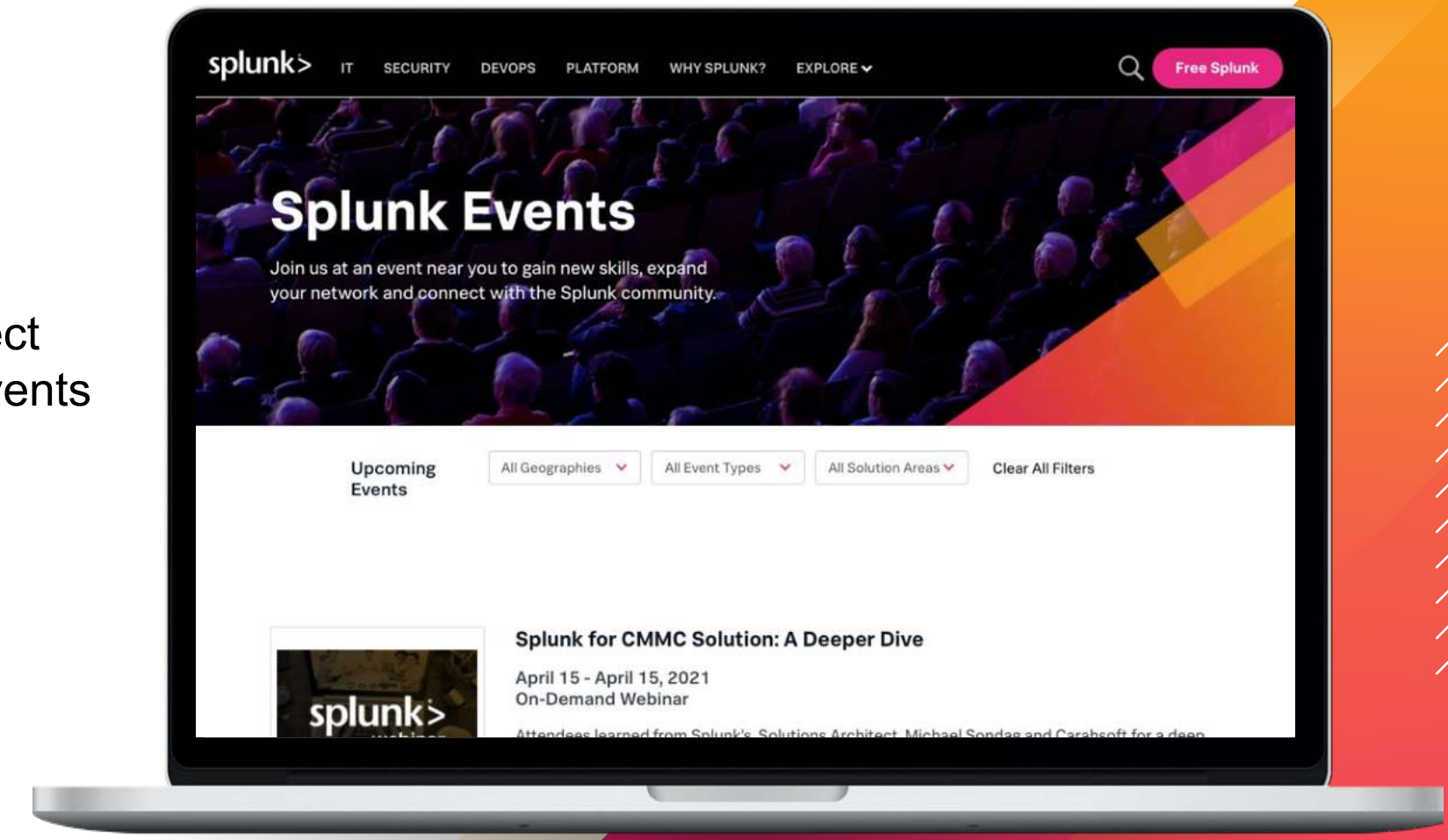


splunk> turn data into doing

Splunk Events

https://events.splunk.com

- Expand your network and connect with the Splunk community at events near you



.conf20

https://conf.splunk.com

- Join us online on 20-21 October for two days of innovation!
- Dozens of educational sessions and numerous opportunities to learn new skills

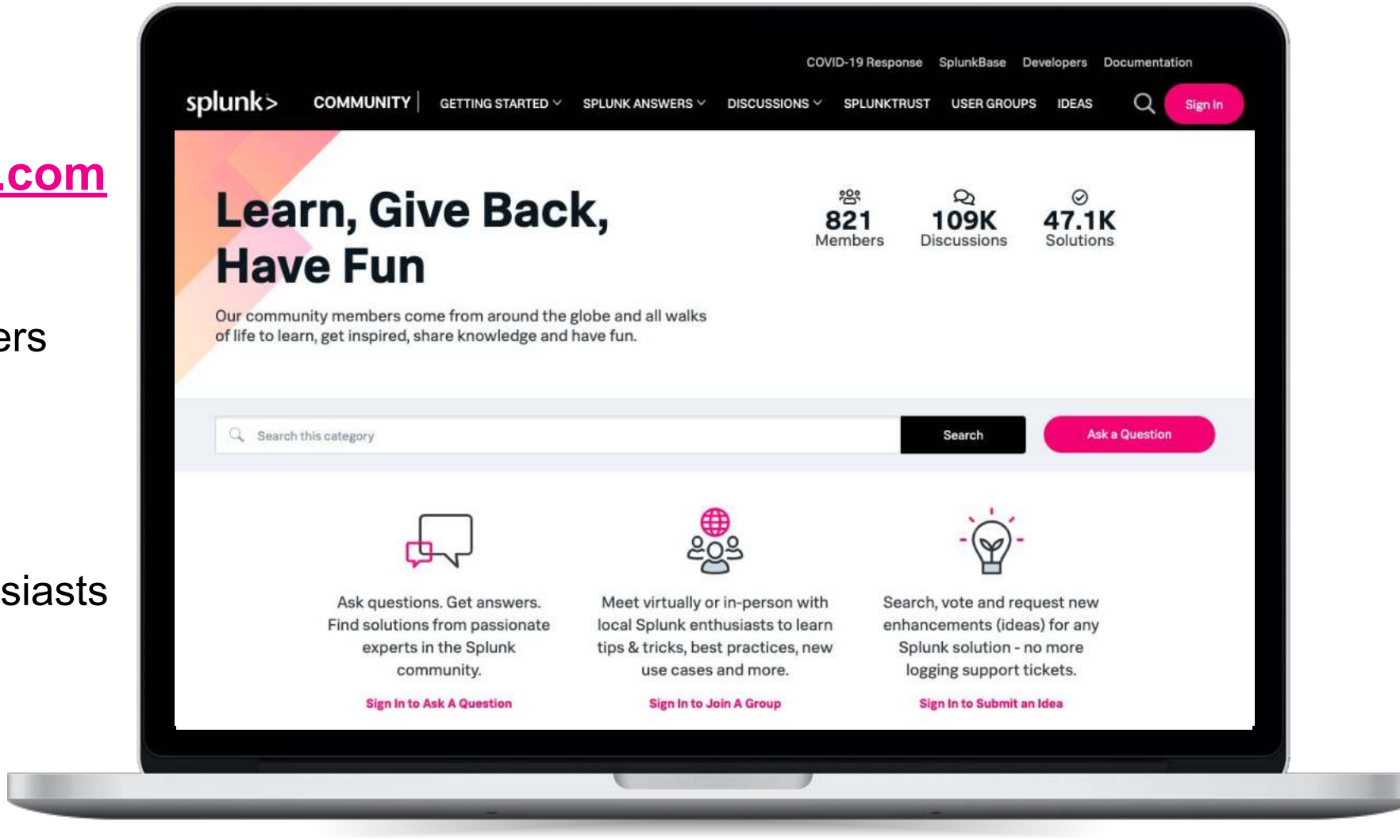
Splunk Community

https://community.splunk.com

- **Splunk Answers**
  Ask questions and get answers from the passionate Splunk community!

- **Splunk User Groups**
  Meet with local Splunk enthusiasts to learn tips and tricks

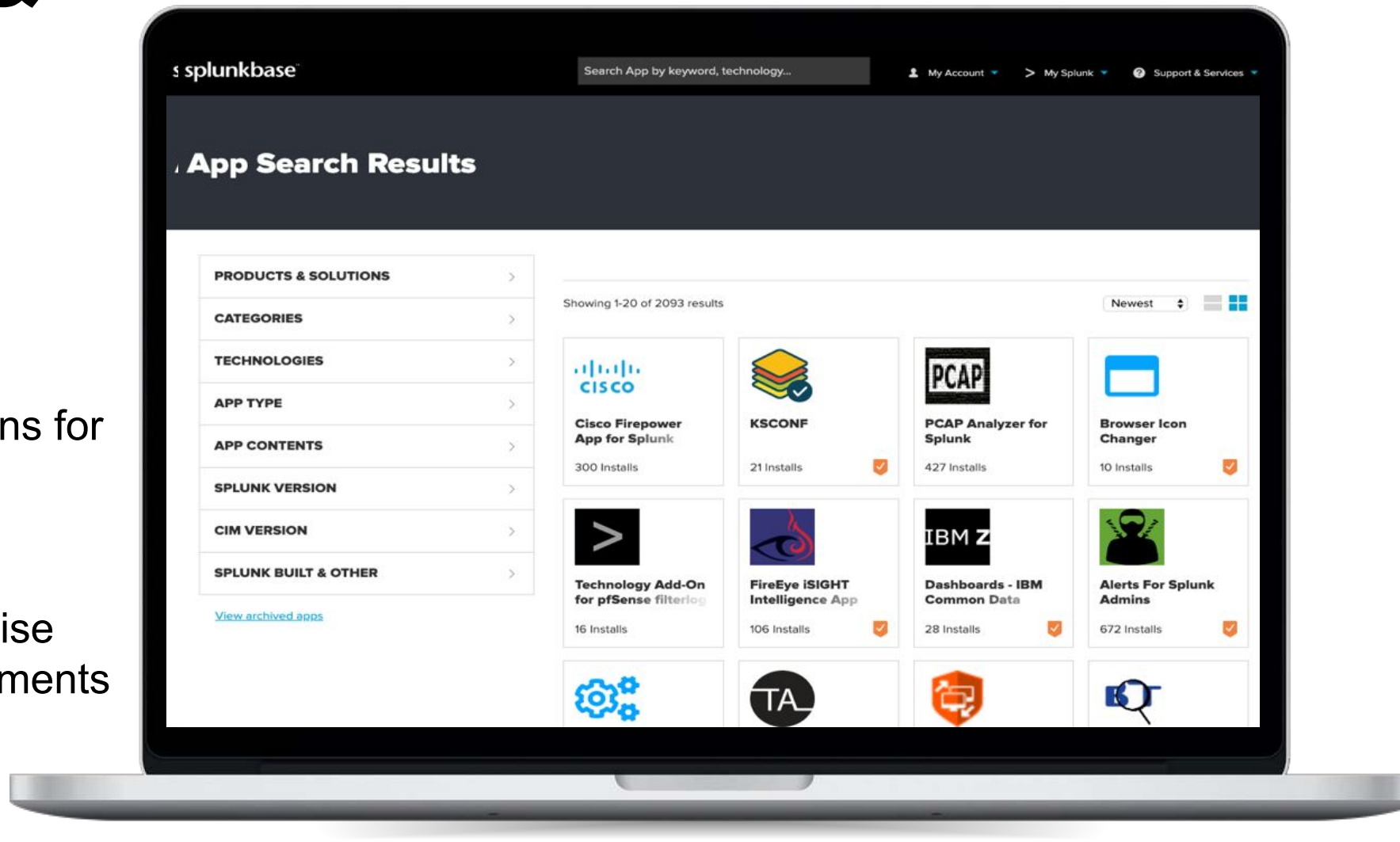
- **Splunk Ideas**
  Search, vote and request new product enhancements



Splunk Apps & Add-ons

https://splunkbase.com

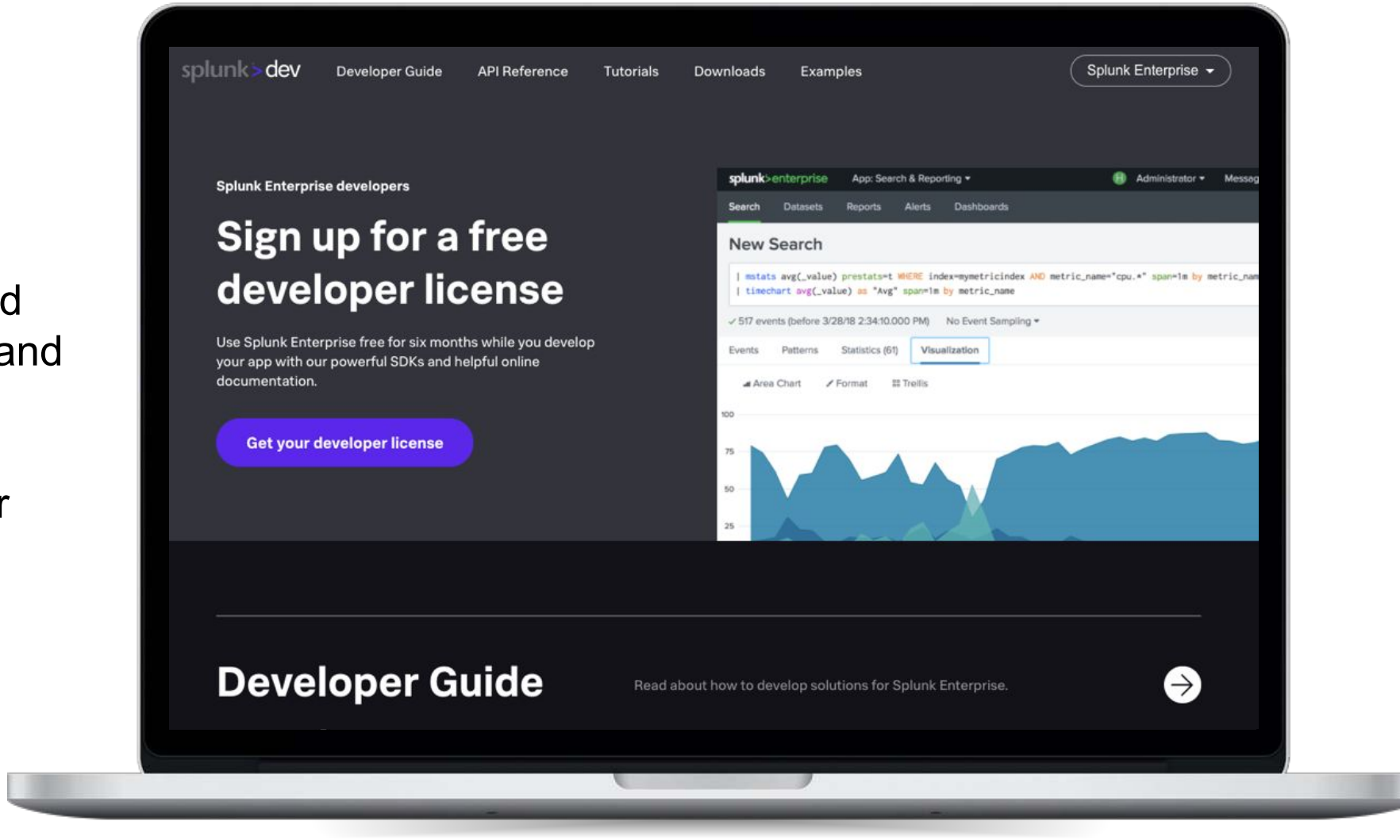
- 2000+ apps and add-ons
- Pre-built searches, reports, visualizations and integrations for specific use cases and technologies
- Download apps and customise them based on your requirements
- Fast time to value from your data
- Build and contribute your own apps!



Developer Resources

http://dev.splunk.com

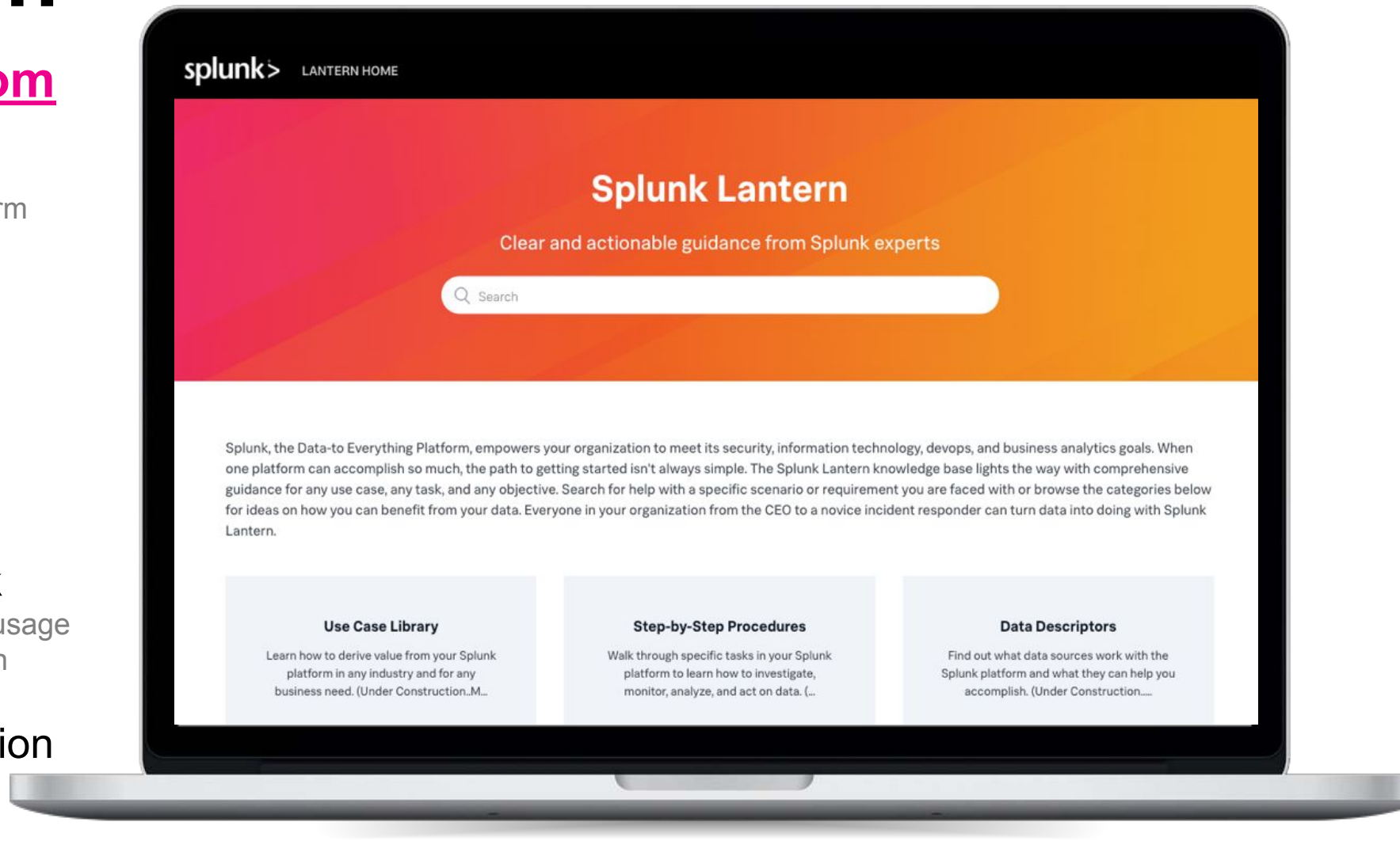
- Check out our REST API and suite of SDKs to customise and extend the power of Splunk
- Splunk integration with other applications and systems
- Resources for building Splunk apps
- Splunk Investigate



Splunk Lantern

https://lantern.splunk.com

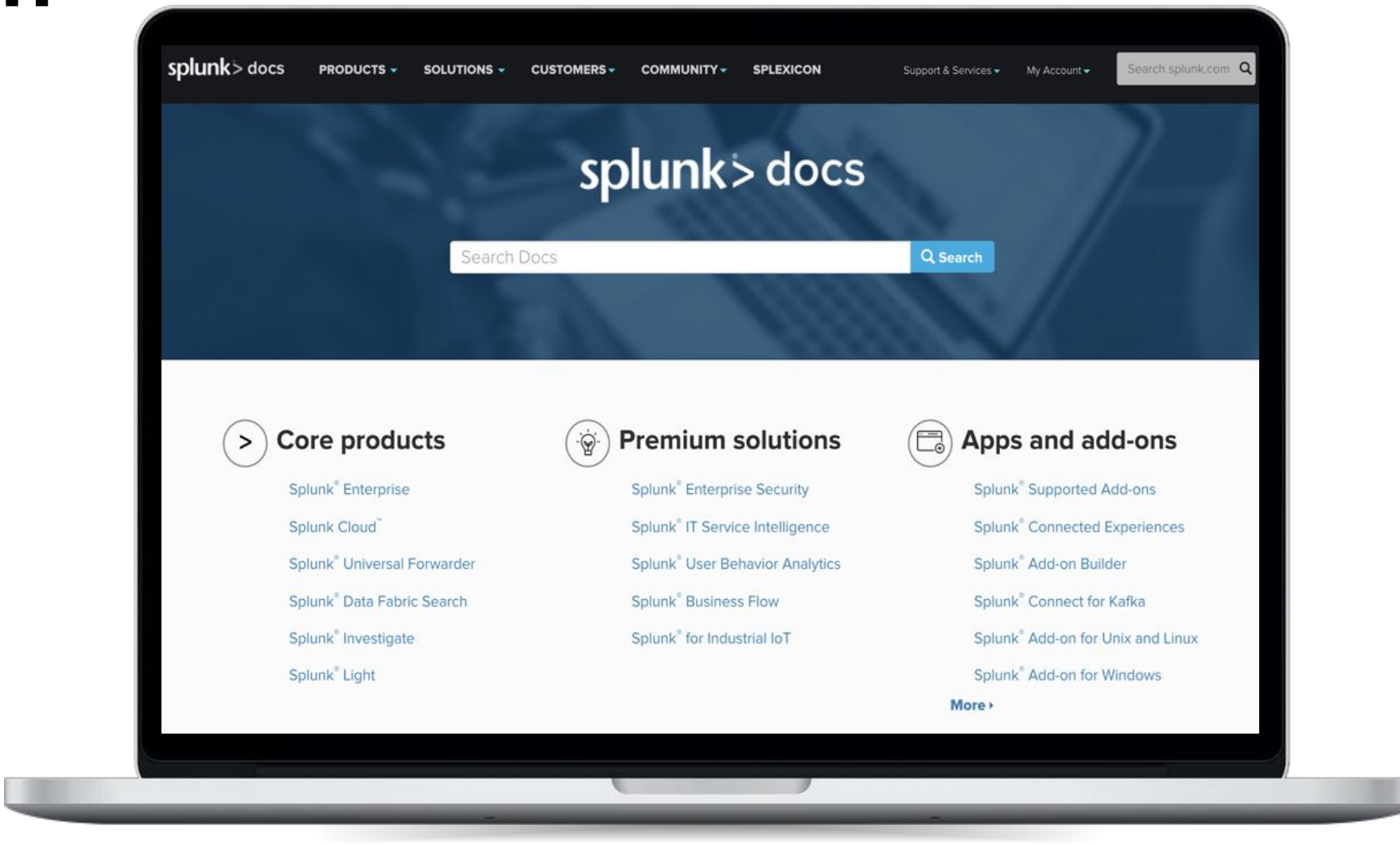
- Use case library
  Get more value from your Splunk platform
- Step-by-step procedures
  Investigate, monitor, analyse and act
- Data descriptors
  Map use cases to data sources to reach your goals
- Splunk Success Framework
  Structure your Splunk deployment and usage to realise value across your organisation
- Splunk Platform Administration
  Keep your Splunk deployment running smoothly



Documentation

https://docs.splunk.com

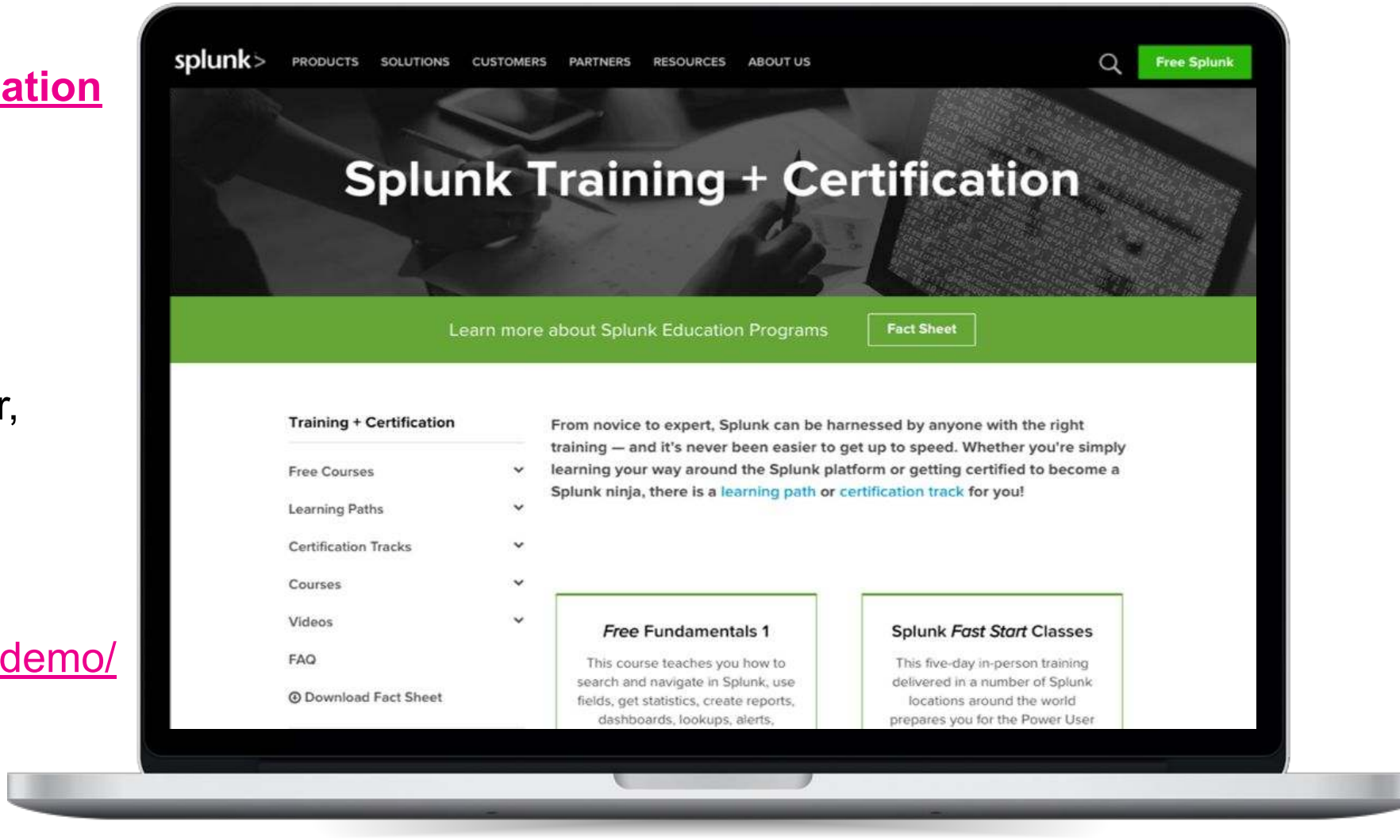
- Splunk reference
  Learn the commands!
- Tutorials
  Check out the search tutorial that even includes sample data to play with!
- Use cases
- References
- Procedures/guides
  Installing, upgrading
- And more!



Education

https://www.splunk.com/education

- Check out our online education classes
- Certification tracks for different roles, including User, Power User, Admin, Architect and Developer!
- Course examples: https://www.splunk.training/edemo/
- Free education! FREE: Online Splunk Fundamentals 1 course



The New Fundamentals of Splunk Education

Start your learning journey with **free training** and one of our **foundational learning paths.**

FREE SELF-PACED ELEARNING

These **free** foundational courses are recommended for all learners.

1. What is Splunk?
2. Intro to Splunk
3. Using Splunk

4. Choose your learning path. **Search Experts** write advanced searches, perform forensics and analytics, may staff a help desk for search-related assistance, and create dashboards and alerts. **Knowledge Managers** perform data interpretation, classification, and enrichment, build data models, manage knowledge objects, and configure summary-based reports and data model acceleration.

Search Expert

Scheduling Reports and Alerts	free eLearning
Visualizations	free eLearning
Working with Time	1 credit
Statistical Processing	1 credit
Comparing Values	1 credit
Result Modification	1 credit
Leveraging Lookups and Subsearches	1 credit
Correlation Analysis	1 credit
Search Under the Hood	free eLearning
Multivalue Fields	1 credit
Search Optimization	1 credit

Knowledge Manager

Introduction to Knowledge Objects	free eLearning
Creating Knowledge Objects	1 credit
Creating Field Extractions	1 credit
Enriching Data with Lookups	1 credit
Data Models	1 credit
Introduction to Dashboards	free eLearning
Dynamic Dashboards	1 credit
Using Choropleth	1 credit
Search Optimization	1 credit

Note: The courses in these learning paths are shown in recommended order, but can be mixed and matched between paths or completed in partial order. These courses are each 3 hours in duration and have replaced the Fundamentals 1-3 series, as well as Creating Dashboards and Advanced Searching & Reporting. If you began your learning journey with these legacy courses, please click here for your recommended next steps.

splunk> turn data into doing

****NOTE all Single Course Classes are FREE to Veterans!**

Thank You