

Splunk 4 Rookies

Randy Holloway
CISSP, MS / Staff Sales Engineer

splunk® turn data into doing™



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.

Splunk, Splunk>, Data-to-Everything, D2E and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2021 Splunk Inc. All rights reserved.

Agenda for Today's Workshop

- ✓ The value of data
- ✓ Various Splunk Concepts
- ✓ 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 dashboard for multiple use cases

splunk > turn data into doing™



#whoami

Randy Holloway

rholloway@splunk.com

Based in Houston, TX

24+ Years IT and Security Experience

15+ Years SIEM Experience

Previously with ArcSight

Splunk for ~5 years

Enjoys Michigan Football



\$whoami

- Scott Head
- PBST DOD CSE
- <3 Texas
- Fishing/Hunting
- Motorcycle racing

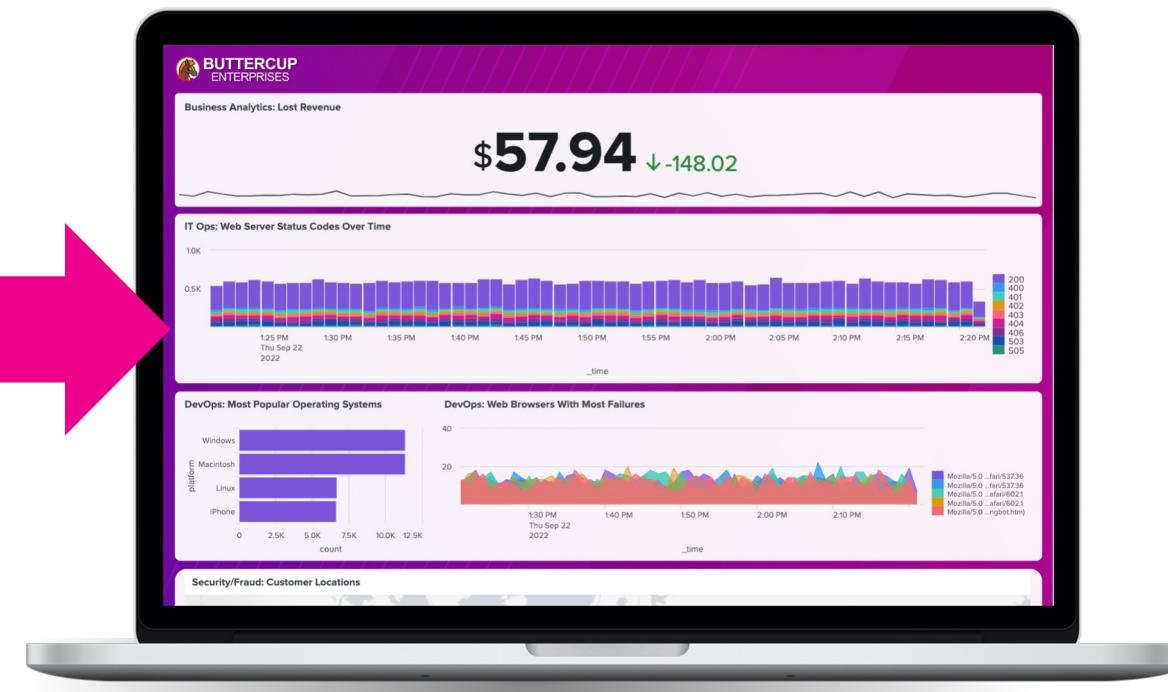
There's a Lot More to Splunk...

- > Clustering
- > Data Models
- > Alerting
- > Pivot
- > SDKs
- > APIs
- > DB Connect
- > Splunk Stream
- > Deployment Server
- > Data Stream Processor
- > Metrics
- > Advanced Searches
- > SOAR
- > Machine Learning (ML)
- > Custom Visualisations
- > HTTP Event Collector (HEC)
- > Data Filtering
- > Transformations
- > Architecture
- > Report Acceleration
- > Common Information Model (CIM)
- > Containers
- > Best Practices
- > And much more...



Visit <https://splunk.com/training> to learn more!

Objective for Today



splunk turn data into doing®

Access Class Material

Items of Interest can be found by going to this Google Drive:

1. This link will have your Lab Guide, Splunk Instance Details and more:
<https://tinyurl.com/splunkworkshops>
2. Follow the guidance of your instructor on accessing / noting which instance you will use for this workshop, along with getting access to the slides and lab guide.

Helpful Links

Splunk Quick Reference:

- <https://www.splunk.com/pdfs/solution-guides/splunk-quick-reference-guide.pdf>

Splunk Search Reference:

- <http://docs.splunk.com/Documentation/Splunk/latest/SearchReference/WhatsInThisManual>

Hunting with Splunk Blog Series:

- <https://www.splunk.com/blog/2017/07/06/hunting-with-splunk-the-basics.html>

Go Splunk (Good SPL Examples)

- <https://www.gosplunk.com>

Splunk in the Public Sector

© 2022 Splunk Inc.

Customers

- All 3 branches of US Govt.
- All 15 Cabinet-level Departments
- All 4 branches of US Military
- 25 largest civilian Depts. and Agencies (CDM)
- Defense ministries of (UK, Australia, New Zealand)
- Largest License **PB/day**

Engagements

- Founding member - U.S. Chamber of Commerce's Cybersecurity Leadership Council
- National Cybersecurity Center of Excellence at the NIST
- Engage policy community on key technology issues
- Splunk4Good

Investment

- Public Sector office in Tysons Corner, VA
- Continuing to grow our public sector team
- Sales, Professional Services, Solutions Expertise
- Key SI and GovCon partners
- .conf User Conference
- Free training for veterans



Different *lenses* into the same data

IT Ops Center



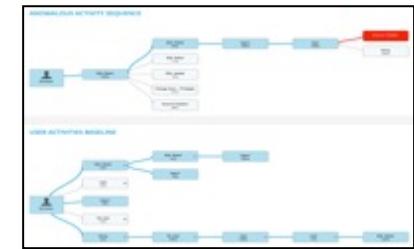
Security Ops Center



Compliance Ops Center



Mission Ops Center, etc...



Different People, Asking Different Questions, Of
the Same Data

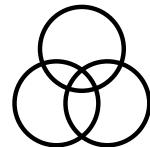
Data Reuse = Greater Data Leverage

Users only see what they should
Why Re-invent the Wheel?

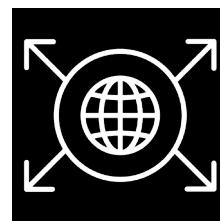
splunk> Machine Data Fabric

splunk> turn data into doing®

Why is this so hard?



Machine data is
real time, messy
and unpredictable



Requires
massive scale



You don't always
know which
questions to ask

Challenge: Adapt to Variety and Variability of Data

Other Guys

Schema at Write

SQL

ETL



Structured
RDBMS

Splunk

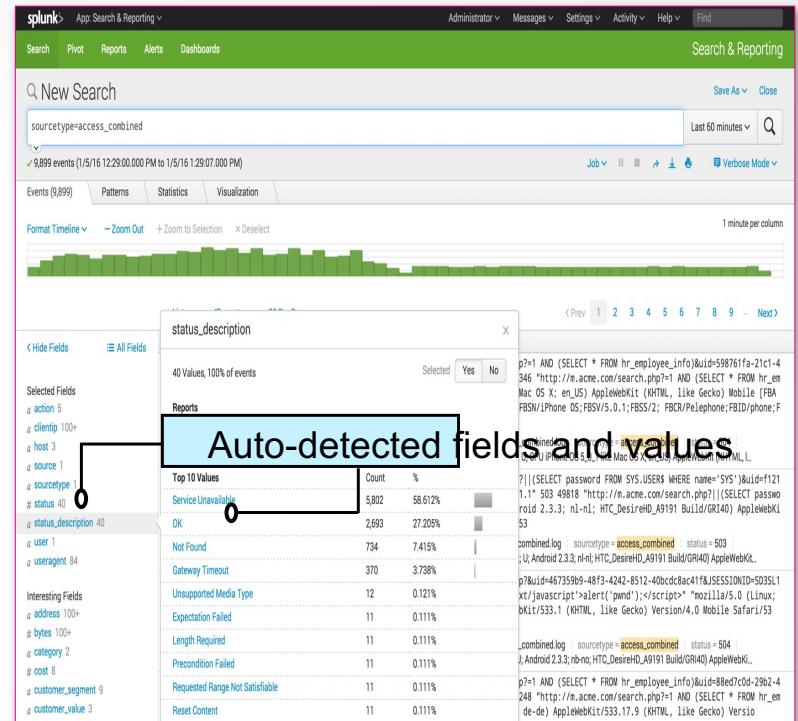
Schema at Read

Search

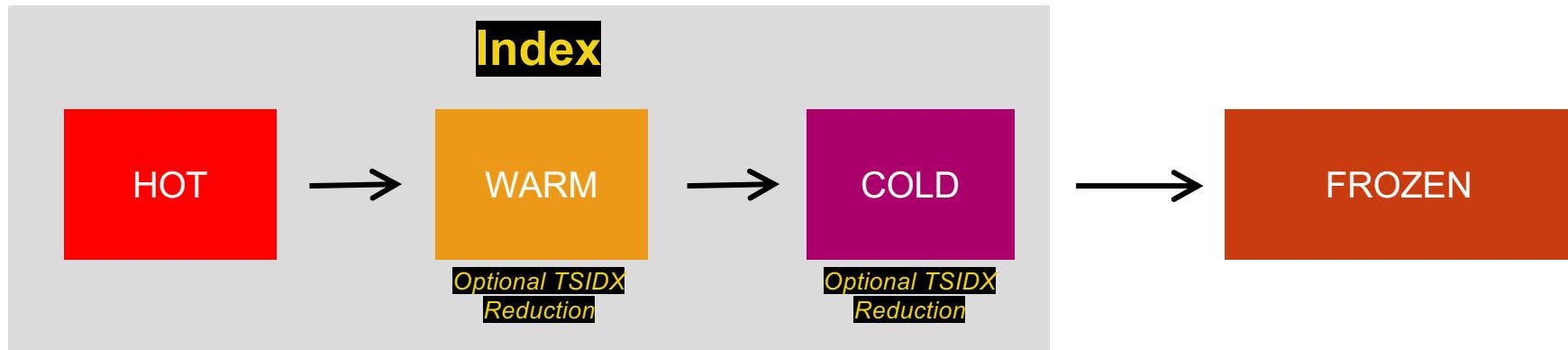
Universal
Indexing

Unstructured
Volume Velocity Variety

Schema at Read



How the Data is Stored and Aged in Splunk



- **Hot** – Newest buckets of data that are still open for write
- **Warm** – Recent data but closed for writing (read only)
- **Cold** – Oldest data, commonly on cheaper, slower storage
- **Frozen** – No longer searchable, commonly archived or deleted data (rarely see this anymore with the cost of storage going down and cloud space (e.g. s3))

Splunk Cloud Platform has achieved DoD IL5 Provisional Authorization



splunk® turn data into doing™

Why add the complexity of running enterprise software yourself?

Distinction between consuming SaaS and operating software on one's own cloud infrastructure

Splunk On-Premises and BYOL

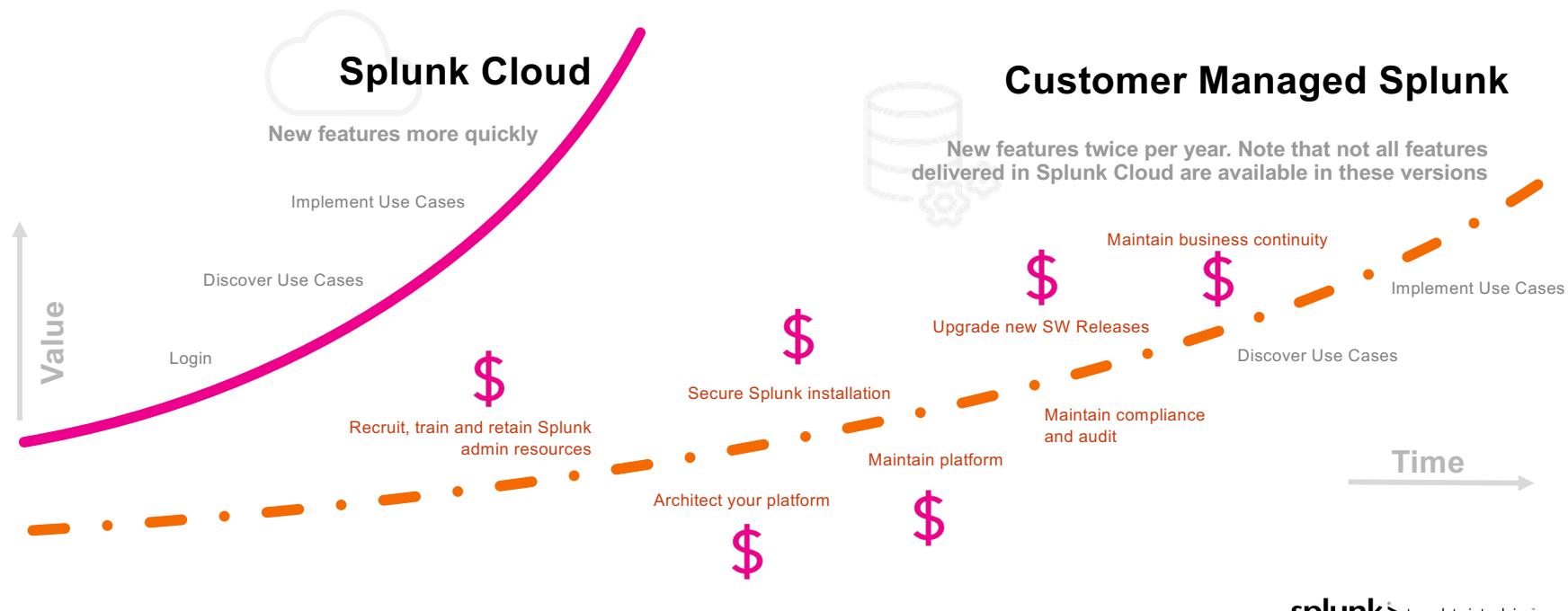
- Customer runs their own Splunk license on-prem or on IaaS (AWS, Azure, Google, other public/private cloud)
- Customer manages their infrastructure
- Customer is responsible for installation, setup, updates and upgrades
- Your IT team is responsible for a successful deployment
- Risk is predominantly absorbed by the customer

Splunk Cloud (SaaS)

- SaaS – Subscription-based cloud service
- Splunk manages and operates the underlying infrastructure and the software layer
- Customers manage forwarders and sends data to Splunk Cloud
- Platform is setup and **ready to go on purchase**
- **Removes the complexity** of managing infrastructure and enterprise software
- **Vendor takes on risk** for uptime, availability and performance of your solution

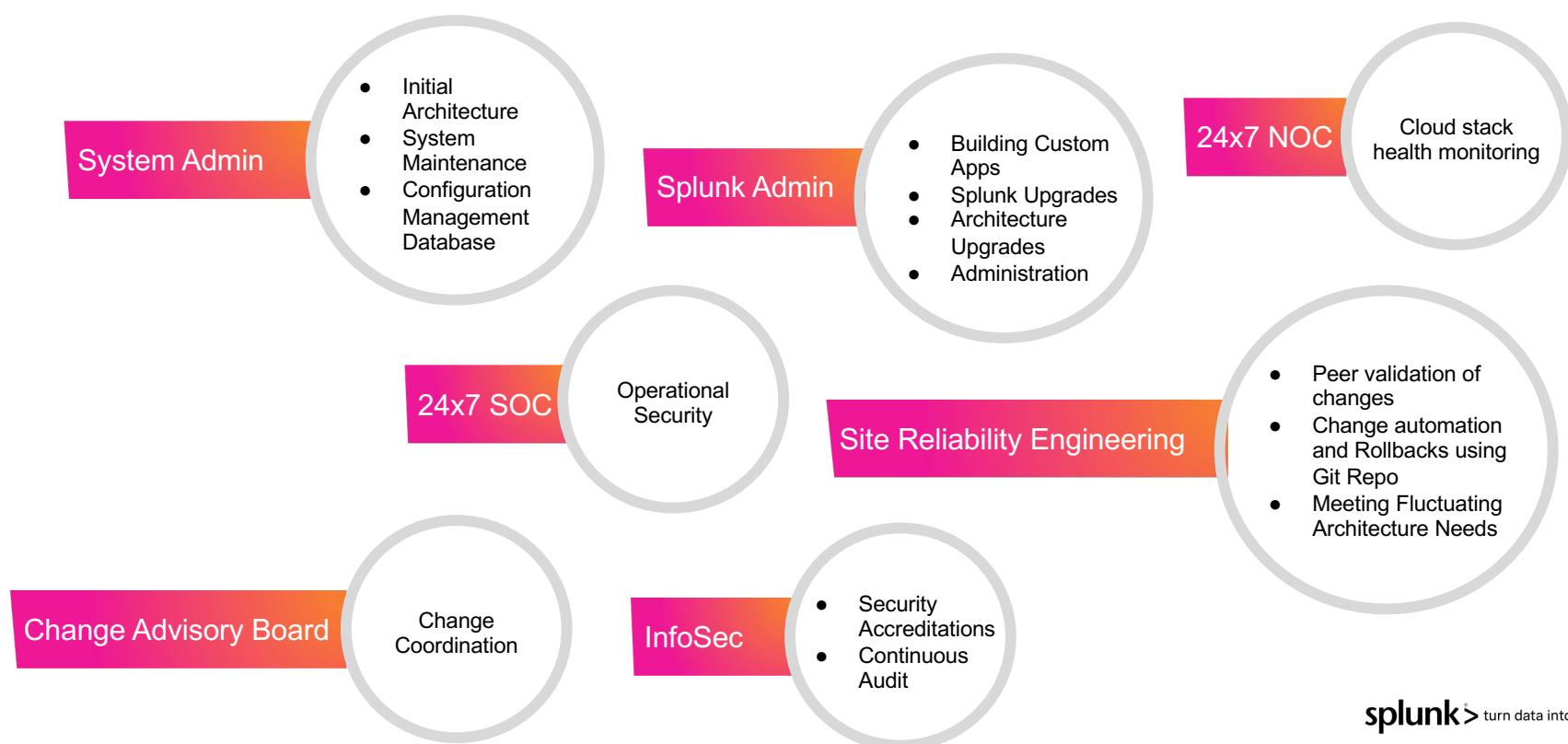
Get more value and get it faster

Different deployment options require different levels of engineering commitment, complexity handling and risk undertaking



splunk > turn data into doing®

Splunk takes care of Platform Management



Managing Splunk Is More Than Just Software

	Responsibility	Splunk Ent Deployed On-Premises	Splunk Cloud
Admin Tasks: One-time Setup	Purchase/rent HW	Customer	Splunk
	Rack and stack, cable, network all HW	Customer	Splunk
	Install Splunk	Customer	Splunk
	Install OS	Customer	Splunk
	Configure Splunk (create users, load apps, configure)	Customer	Splunk
	Configure indexes	Customer	Splunk
	Setup HA/clustering	Customer	Splunk
	Setup disaster and recovery	Customer	Splunk
	Configure forwarders	Customer	Joint
	Onboard data	Customer	Joint
	Integrate with LDAP/AD	Customer	Joint
	Scale up HW	Customer	Splunk
Admin Tasks: Ongoing	Install Splunk patches / upgrades	Customer	Splunk
	Install OS patches / upgrades	Customer	Splunk
	Monitor deployment / health checks	Customer	Splunk
	Manage forwarders	Customer	Customer
	Create users / roles	Customer	Customer
	Manage indexes	Customer	Customer
	Onboard additional data	Customer	Customer
	Load search head only apps	Customer	Both*
	Load distributed apps	Customer	Both*
	Load premium apps	Customer	Splunk
	Export data	Customer	Splunk
	Search, alerts, reports, dashboards	Customer	Customer
User Tasks			

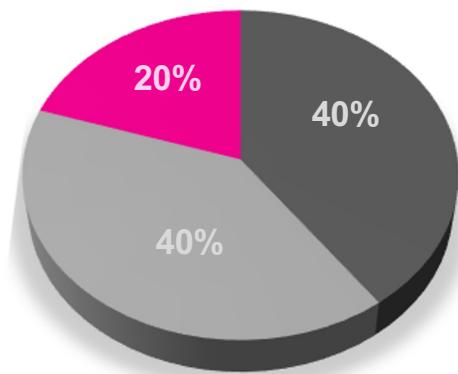
Managing a Splunk deployment involves 12 on-going admin tasks, 8 of which are conducted by Splunk for a Cloud based deployment



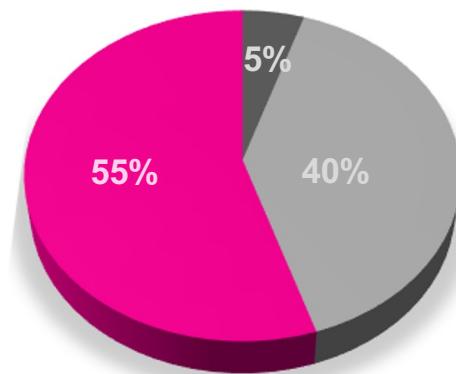
Reallocate your Time

To focus on higher value tasks directly tied to business outcomes

Customer Managed Splunk



Splunk Cloud SaaS



35%

Reduction in Time
on platform mgmt
(40% to 5%)

Increase in Time
on high value use case work
(20% to 55%)

■ **High Value** use case delivery,
adoption enablement, value realization

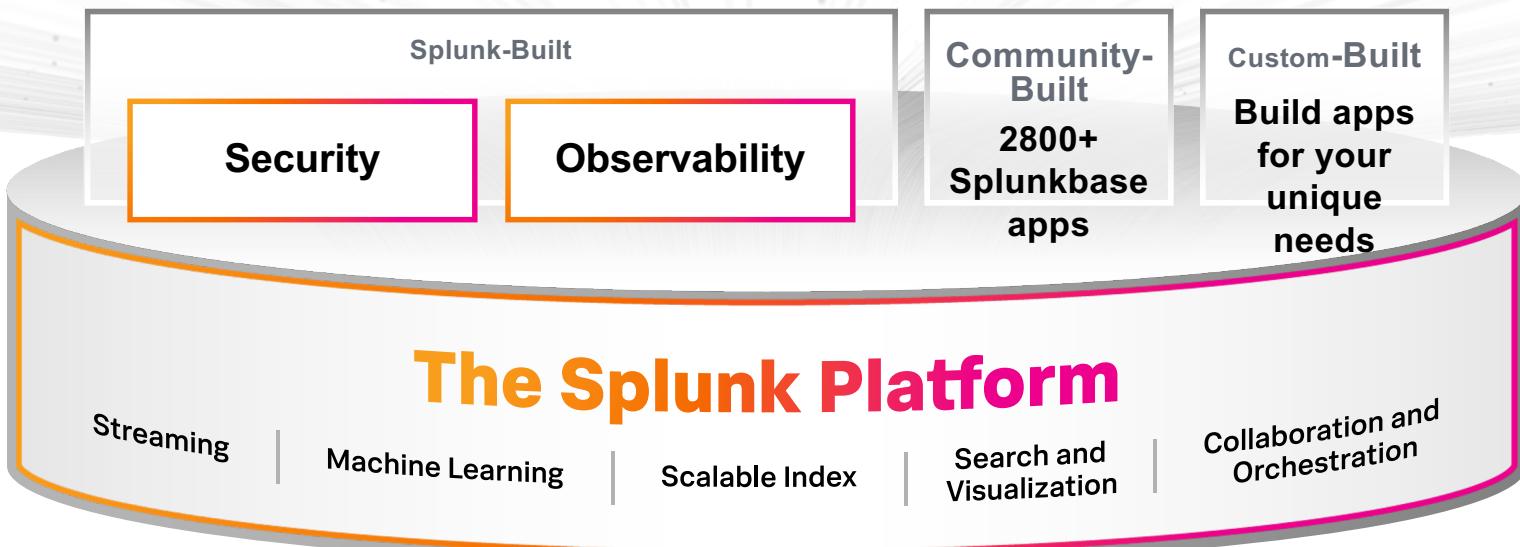
■ Data and user
onboarding

■ Platform
management

Note: metrics are based on 1000+ assessments with Splunk customers worldwide

splunk > turn data into doing®

Introducing Splunk



The Power of Splunk

Delivering unified security and observability

See

End-to-end visibility

No sampling or blindspots

Act

Investigate across massive data sets and take **action** fast

Extend

Extend the **platform** to use data to solve problems across the business

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

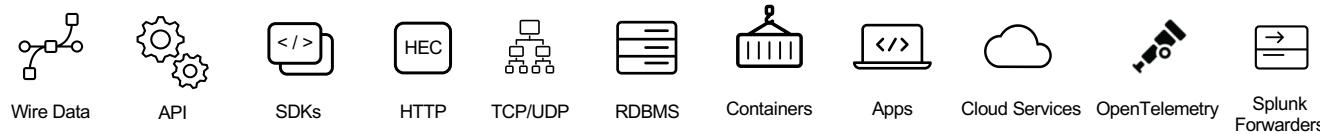


splunk>cloud™



- ✓ **Fastest time to value**
- ✓ **Software as a service** - AWS or GCP
- ✓ **Secure** - ISO 27001, SOC 2 Type II, PCI, HIPAA, FedRAMP (Moderate)
- ✓ **Encryption-in-transit** - plus optional encryption-at-rest
- ✓ **Resilient infrastructure**
- ✓ **100% uptime guarantee**
- ✓ **24/7 NOC/SOC support team**

Flexible options for data collection and forwarding

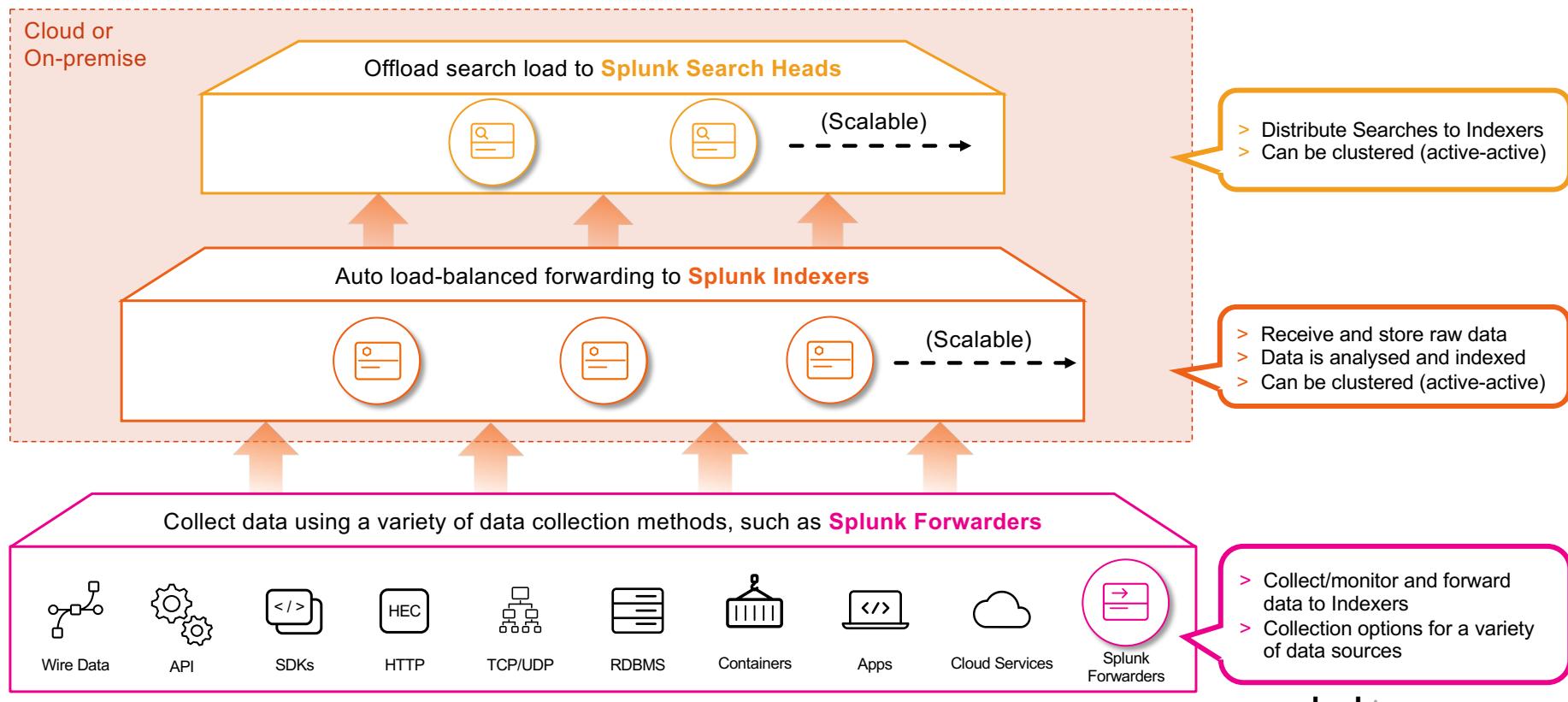


> Splunk Cloud Service Description: <https://splk.it/SplunkCloudServDesc>

splunk> turn data into doing®

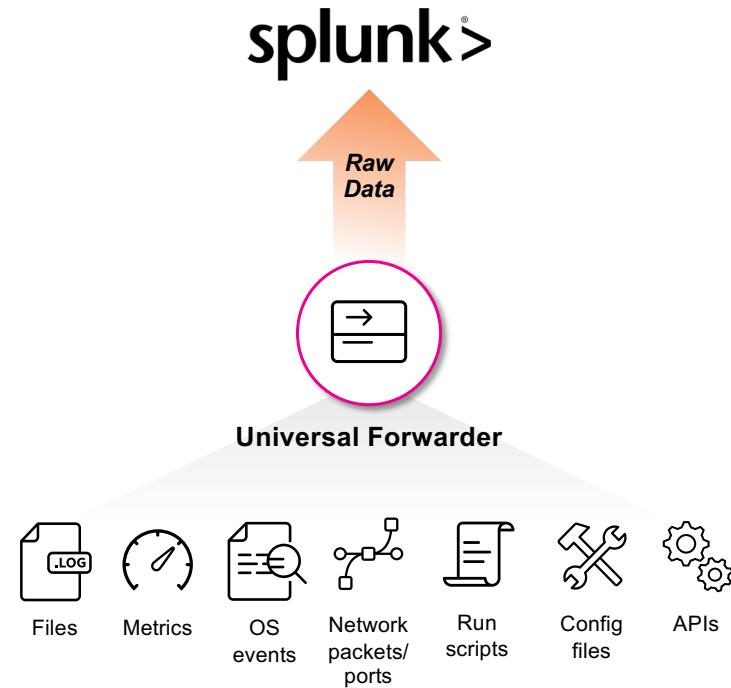
Scales to Petabytes Per Day

Enterprise-Class Scale, Resilience and Interoperability



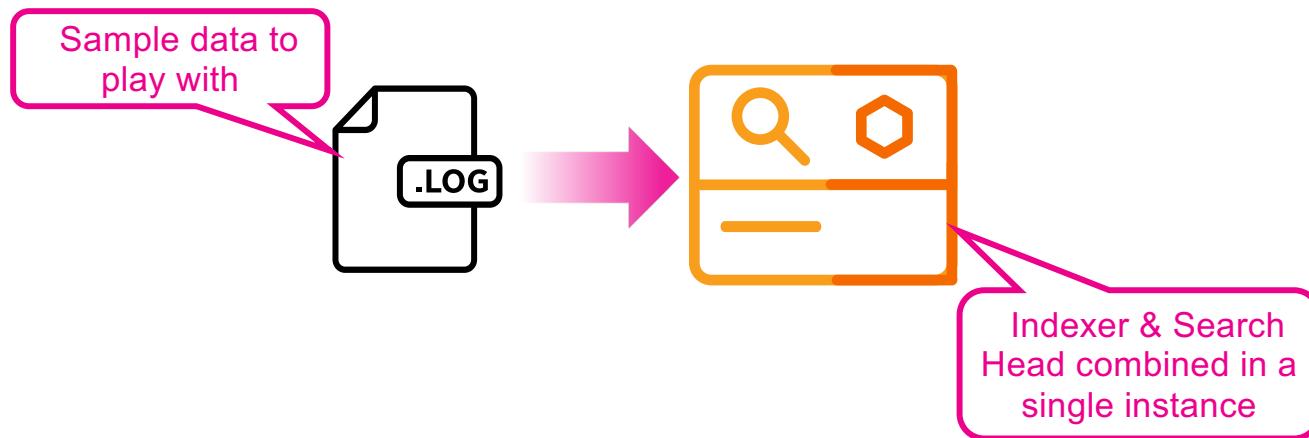
What is a Splunk Universal Forwarder?

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



splunk> turn data into doing®

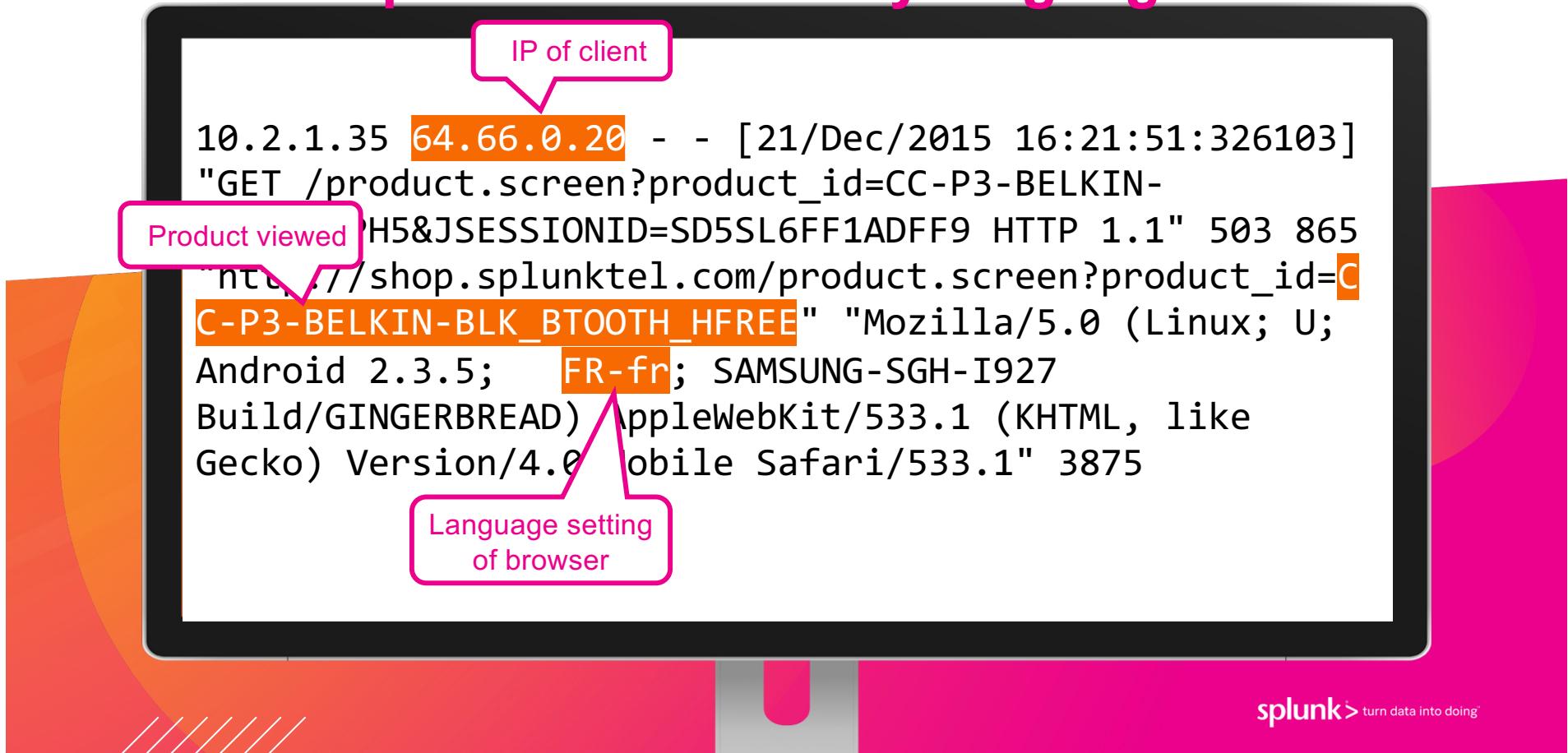
Today's Environment



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=C
C-P3-BELKIN-BLK_BT0OTH_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
```

Marketing Use Case: Show the top products viewed by language



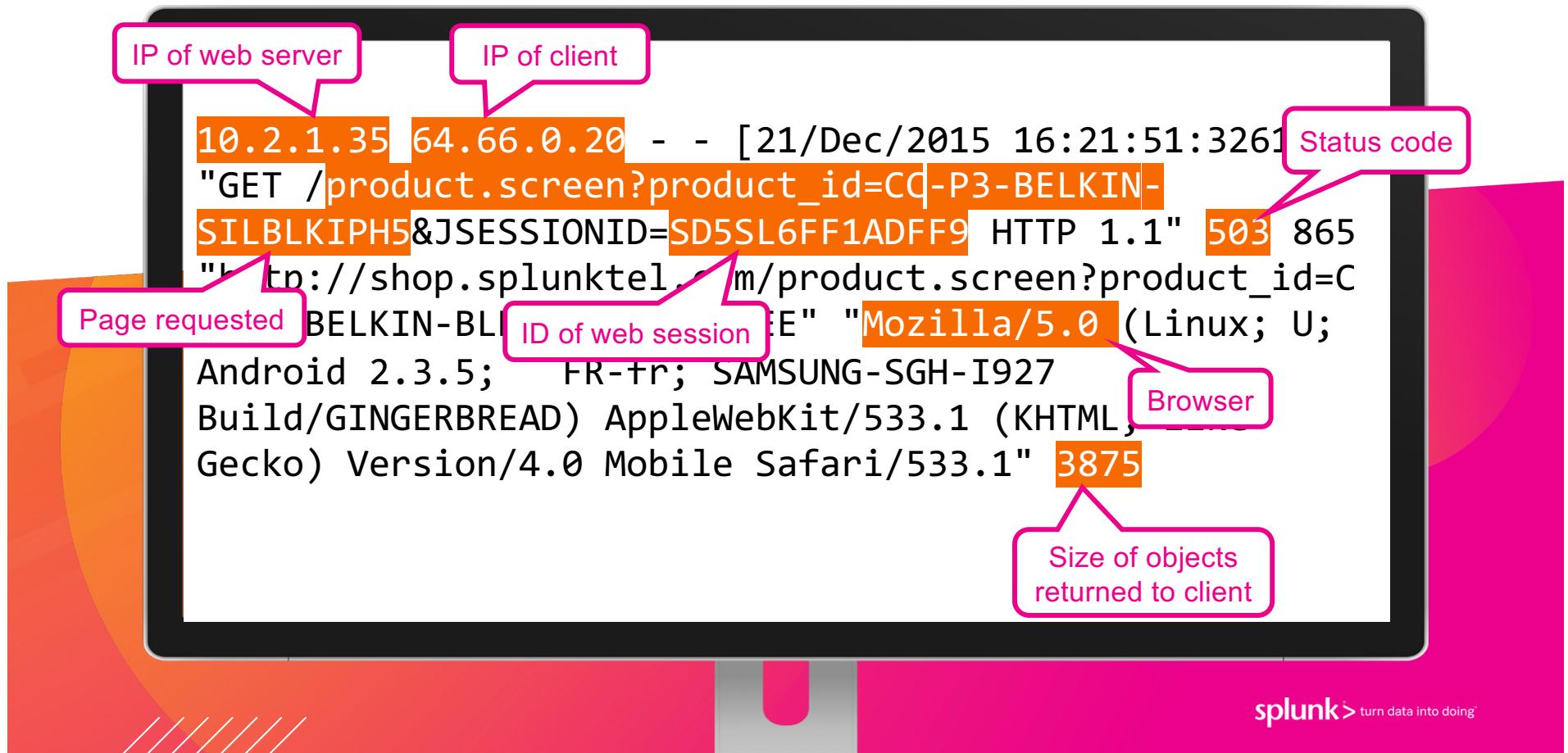
DevOps Use Case: Which mobile handsets should I test the most before releasing my new app?

```
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
shop.splunktel.com/product.screen?product_id=C
C-P3-BELKIN-BLK_BT0OTH_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"
```

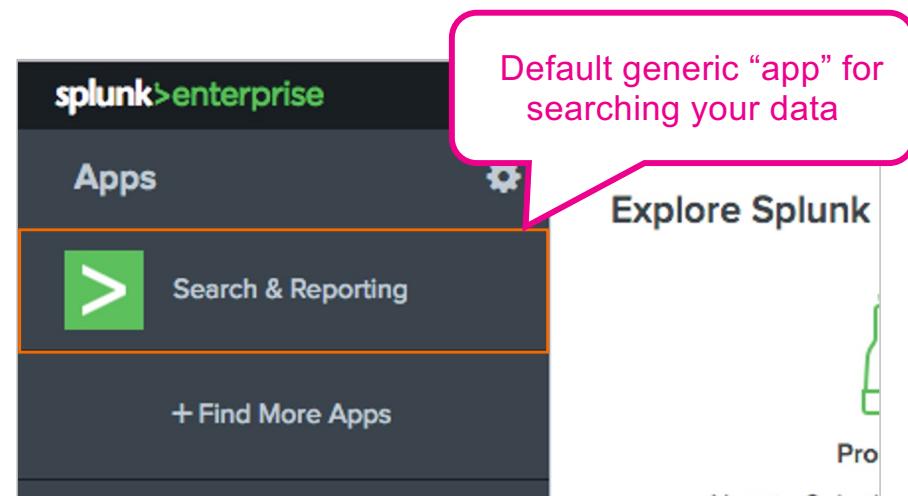
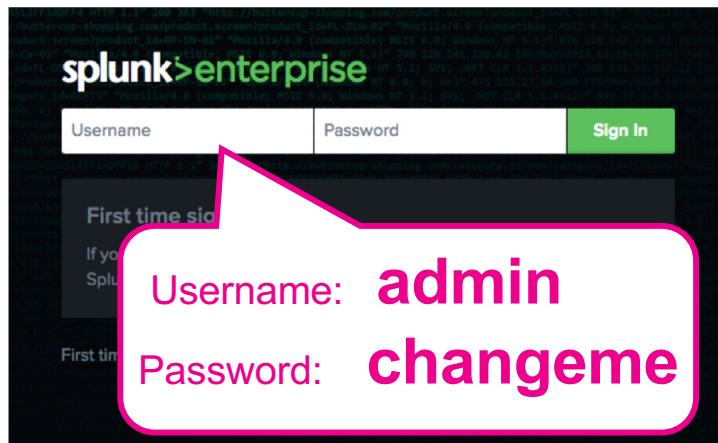
Platform

Handset model

IT Operations Use Case: Web pages with errors



Log in to Splunk



Start to use your lab guide!



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 customize for your own needs
- > Over 2100 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

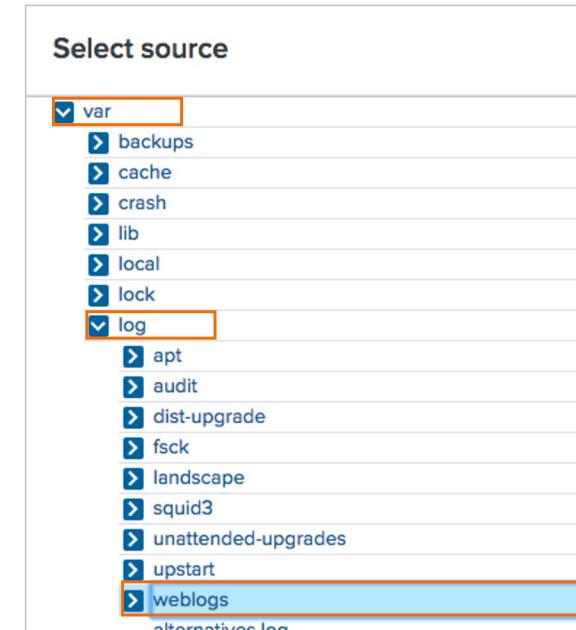
Provide specific capabilities to Splunk, such as **getting data in**, **mapping data**, or providing **saved searches** and **macros**



Lab Exercise 2: Create an App and Add Some Data

Tasks:

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



Reminder:

- > Download the lab guide for step-by-step instructions! <https://splk.it/S4R-Lab-Guide>

Open Your App and Explore!

The currently selected app

Search bar – type anything here to search

Time picker – choose your search time range

Event histogram

Event timestamp

Raw event data

Metadata fields extracted at search time (schema-on-the-fly!)

The screenshot illustrates the Splunk interface for exploring log data. At the top, the app 'Splunk 4 Rookies' is selected. The search bar contains the query 'action=purchase status=200', which has returned 261 events. The search results are displayed in a table with columns for Time, Event, and source. An event histogram is shown above the table, with a tooltip indicating '1 minute per column'. The left sidebar lists 'SELECTED FIELDS' (host, source, sourcetype) and 'INTERESTING FIELDS' (action, bytes, category_id, clientip, date_hour, date_minute, date_month, date_second, date_usec). A large callout box highlights the 'Event timestamp' in the search results table. Another callout box highlights the 'Raw event data' in the same table. A third callout box highlights the 'Metadata fields extracted at search time (schema-on-the-fly!)' in the sidebar. A fourth callout box highlights the 'Event histogram' above the table. A fifth callout box highlights the 'Time picker – choose your search time range' in the top right corner. The bottom right corner features the Splunk logo with the tagline 'turn data into doing'.

Start Exploring Your Data

Example searches:

503 purchase

← Find all events that contain the words “503” and “purchase”

503 pur*

← Find all events containing “503” and words beginning with “pur”

503 (purchase OR addtocart)

← Boolean operators (**AND/OR/NOT**) – must be UPPERCASE!

status=503 action=purchase

← Use **fieldname = value** to return accurate results



How would you find events with a status code of 200 that are NOT purchase events?

status=200 NOT action=purchase

status=200 action!=purchase

Splunk's Search Processing Language (SPL)



e.g. `action=purchase`

Time	Event
15/09/2022 09:12:53.163	12.138.68.5 - [15/Sep/2022:09:12:53:163] "GET /product.screen?product_id=HCB-5&SESSIONID=SD4SLPF7190Pfr HTTP/1.1" 401 3418 "http://www.buttercupenterprises.com/cart/doAction=purchase&item_id=EST-218product_id=HCB-5" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2959.8 Safari/537.36"
15/09/2022 09:12:48.194	128.241.228.82 - [15/Sep/2022:09:12:48:194] "GET /cart/doAction=purchase&item_id=EST-218product_id=Z50-2&SESSIONID=SD4SLPF7190Pfr HTTP/1.1" 404 2346 "http://www.buttercupenterprises.com/product.screen?product_id=Z50-2" "Mozilla/5.0 (iPhone; CPU iPhone OS 7_0 like Mac OS X) AppleWebKit/537.51.1 Version/7.0 Mobile/11A465 Safari/937.53 BingReview/1.0" 661
15/09/2022 09:12:42.194	141.148.8.66 - [15/Sep/2022:09:12:42:194] "POST /cart/doAction=purchase&item_id=EST-198product_id=HCB-5&SESSIONID=SD4SLPF7190Pfr HTTP/1.1" 503 3349 "http://www.buttercupenterprises.com/cart.doAction=purchase&item_id=EST-198product_id=HCB-5" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_1) AppleWebKit/537.36 Chrome/56.0.2914.3 Safari/537.36 OPR/43.0.2431.0 (Edition: developer)" 881
15/09/2022 09:12:42.176	281.3.128.132 - [15/Sep/2022:09:12:42:176] "POST /cart/doAction=purchase&item_id=EST-168product_id=HCB-3&SESSIONID=SD4SLPF7190Pfr HTTP/1.1" 200 3542 "http://www.buttercupenterprises.com/product.screen?product_id=HCB-3" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_1) AppleWebKit/537.36 Chrome/57.0.2959.8 Safari/537.36"

The diagram illustrates the execution flow of the SPL command:

- The search command `action=purchase` is processed by the `| stats count by status` command.
- The output of this command is then processed by the `| rename count as "number of events"` command.

status	count	status	number of events
200	850	200	850
400	81	400	81
401	76	401	76
402	50	402	50
403	57	403	57

Want to know more? Check out:

- > Splunk Quick Reference Guide: <https://splk.it/SplunkQuickRef>
- > Search manual: <https://splk.it/SplunkSearchManual>

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 insights to users throughout the company
- The teams you support include:
 - **IT Operations**
 - **DevOps**
 - **Business Analytics**
 - **Security/Fraud**



**BUTTERCUP
ENTERPRISES**

splunk > turn data into decisions

What Does the Business Want to See?

We need to create a dashboard with four views:



IT Operations team: Investigate successful vs unsuccessful web server requests over time



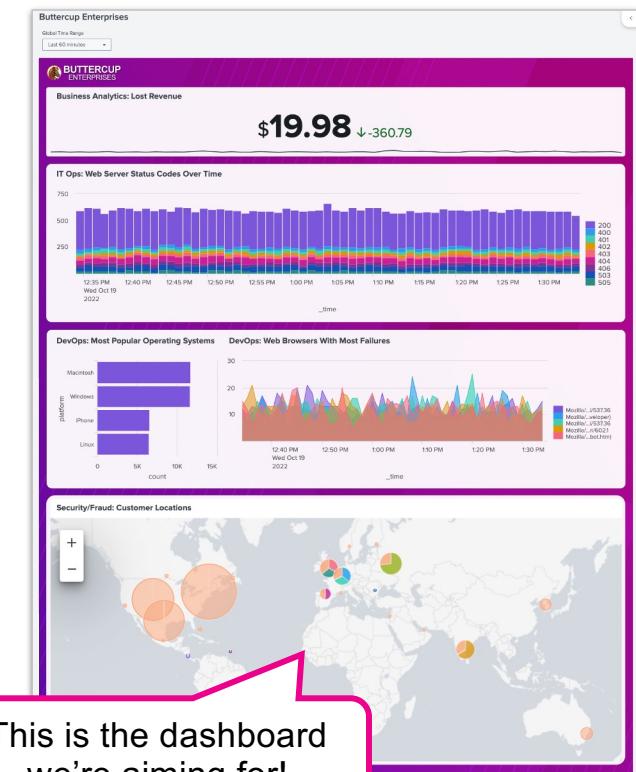
DevOps team: Show the most common customer operating systems and which web browsers are experiencing the most failures



Business Analytics team: Show lost revenue from the Buttercup Enterprises website



Security/Fraud team: Show website activity by geographic location





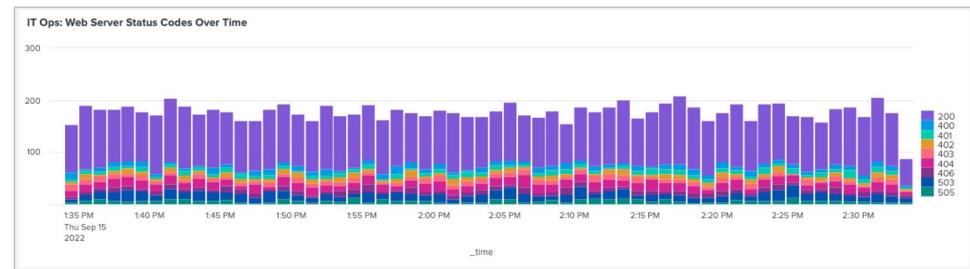
Lab Exercise 3: IT Operations Team

Investigate successful vs unsuccessful web server requests over time

Tasks:

1. Show successful vs unsuccessful web server requests over time
2. Use a stacked column chart visualisation
3. Add your chart to a new dashboard
4. Choose 'Dashboard Studio' and use 'Absolute' layout mode to allow for future dashboard customisation!

Goal:

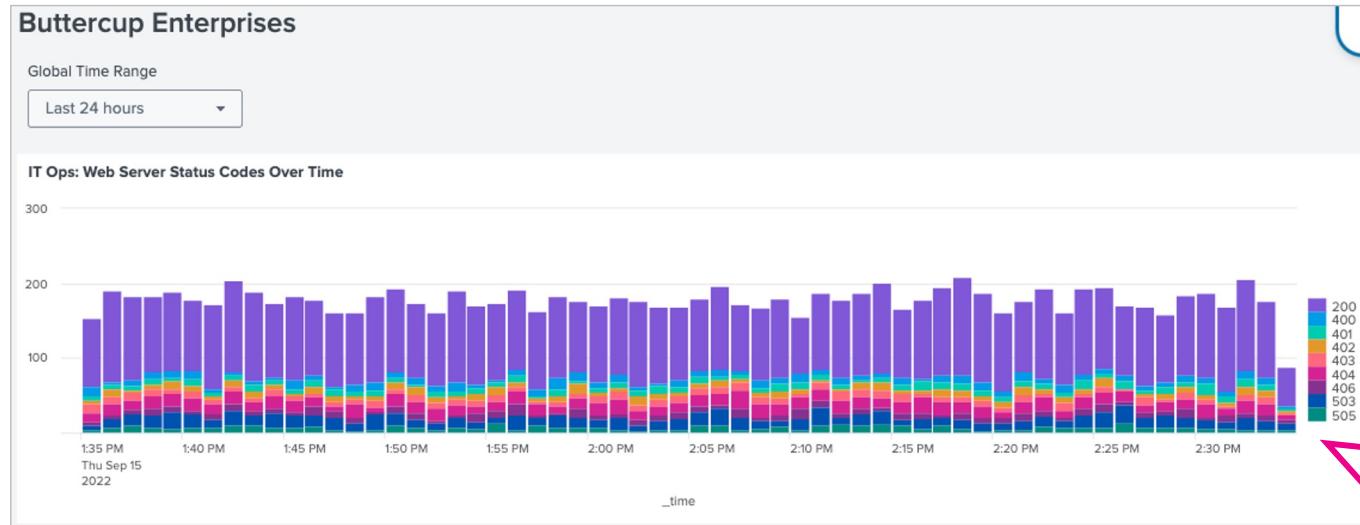




Your Dashboard so far...

Solution:

```
> sourcetype=access_combined | timechart count by status limit=10
```



Your dashboard should
hopefully look
something like this



DevOps Team

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

Step 1: Show the most common customer operating systems

Search

```
sourcetype="access_combined"
```

Search for all web server events

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=SD55L4FF10ADFF5 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/apache2/error.log sourcetype = access_combined

We can see operating system information in our events but we don't currently have a field we can use to report on

Extracting a New Field

1. Click on the arrow to expand an event

i timeline Event
25/10/2019 12.130.60.4 - - L4FF10ADFF5 HTTP 1.1
08:06:34.185 "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" "Macintosh" 993
Event Actions ▾
Build Event Type Extract Fields Show Source

2. Click on 'Event Actions'

3. Click on 'Extract Fields'

(.*?)

Regular Expression

Splunk Enterprise will extract fields using a Regular Expression.

4. Click on 'Regular Expression'



5. Click on 'Next'

Select Fields

Highlight one or more values in the sample event to create fields. You can indicate one value for the regular expression to match. Click on highlighted values in the sample event to modify an existing extraction, first turn off the existing extractions. [Learn more](#)

12.130.60.4 - - [25/Oct/2019 08:06:34:185] "GET /product.screen?product_id=MCF-3&JSESSIONID=SDS5-F10ADFF5 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" "Macintosh" 993

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

Field Name	platform
Sample Value	Macintosh
<input type="button" value="Extract"/> <input type="button" value="Require"/>	
<input type="button" value="Add Extraction"/>	

7. Give the new field a name (lowercase is recommended)



Lab Exercise 4: DevOps Team

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

Tasks:

1. Extract a new **platform** field
2. Show the top values using a bar chart visualisation
3. Create an area chart showing the top 5 web browsers that are experiencing the most failures over time
4. Add your charts to your existing dashboard

Goal:



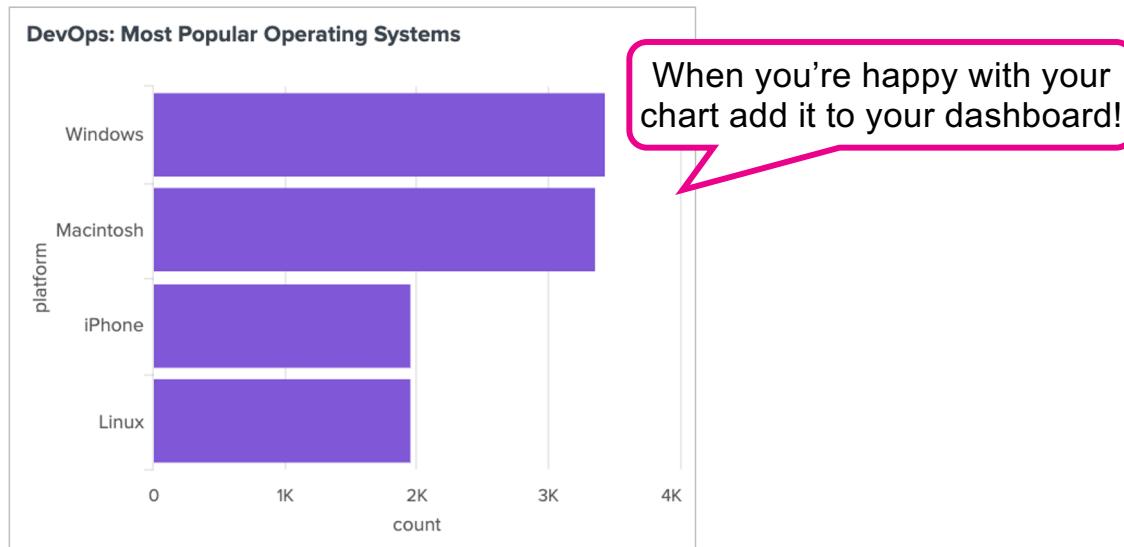


Lab Exercise 4: DevOps Team

Show the most common customer operating systems

Solution:

```
> sourcetype=access_combined | top limit=20 platform showperc=f
```



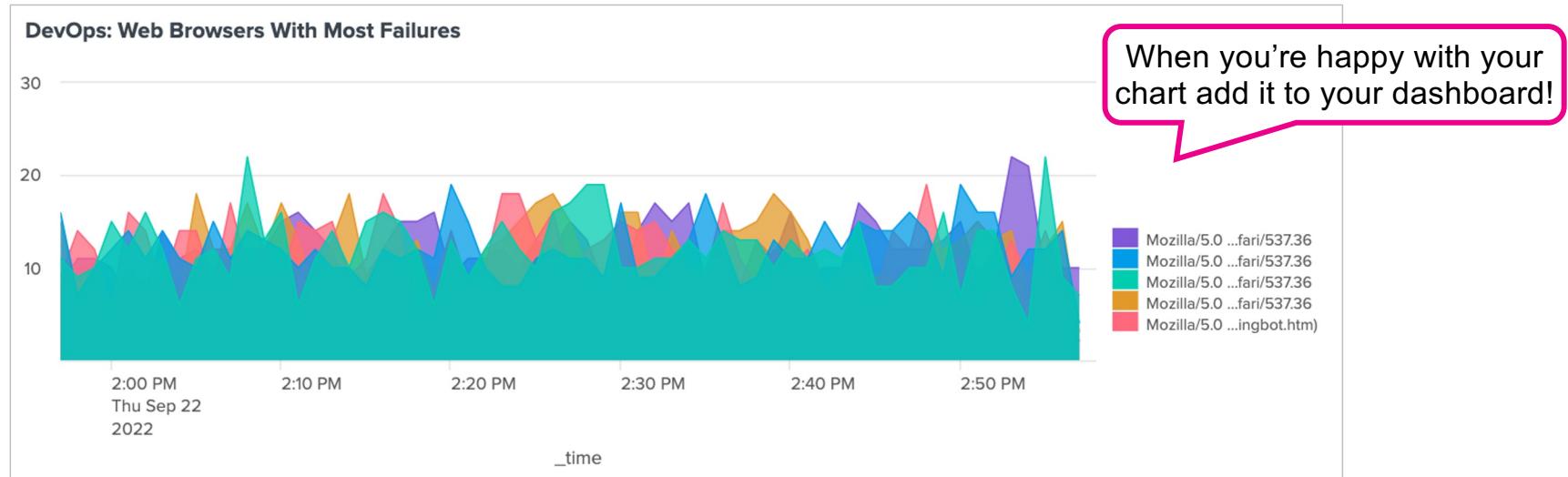


Lab Exercise 4: DevOps Team

Create a graph showing the top 5 web browsers that are experiencing the most failures over time

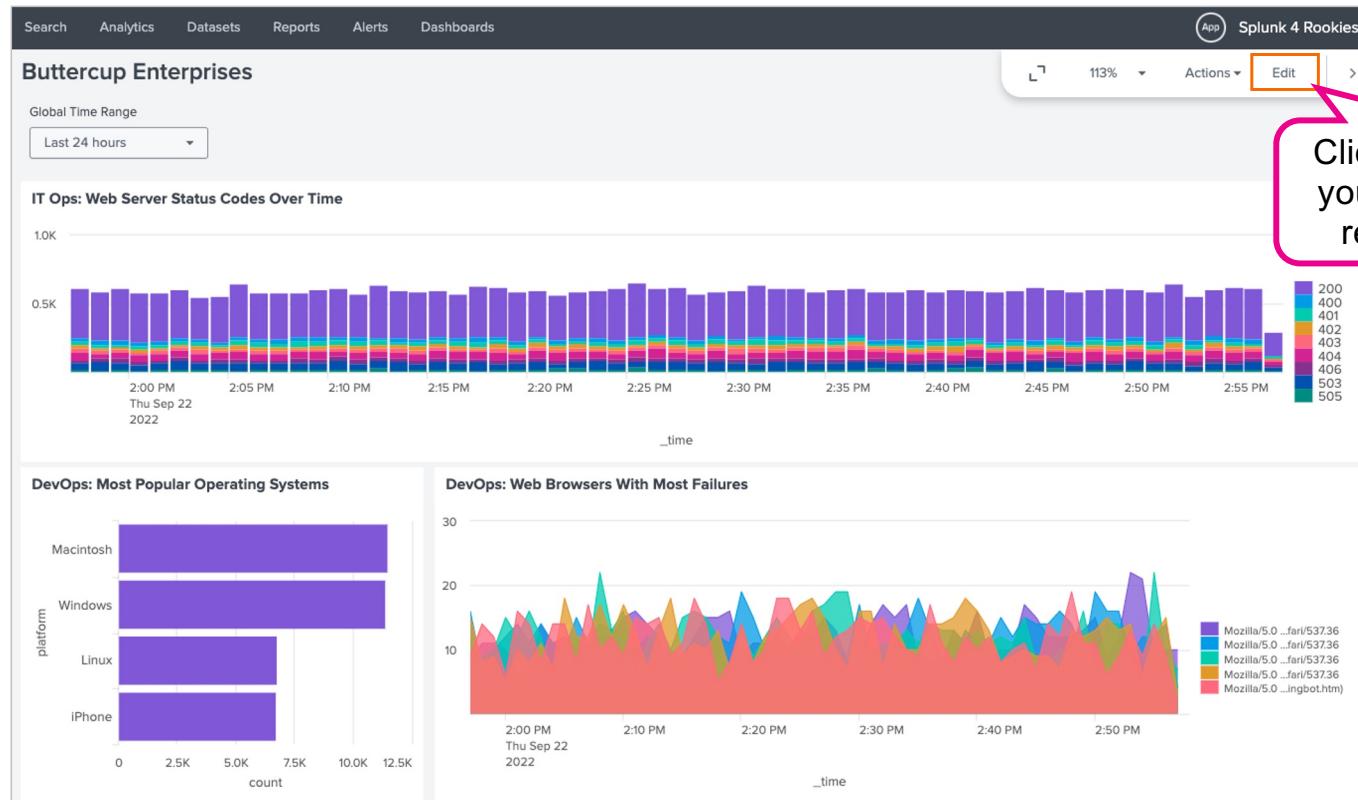
Solution:

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





Your Dashboard so far...



Working with statistics? Use `stats` and `timechart`

Usage:

```
<your search> | stats <function> <by clause>
```

```
<your search> | timechart <function> <by clause>
```

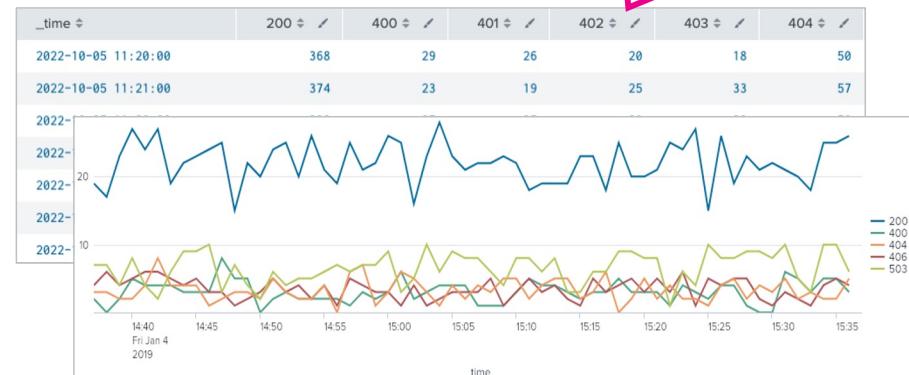
Examples:

> sourcetype=access_combined
| stats distinct_count(clientip) by status

status	distinct_count(clientip)
200	67
400	67
401	67
402	67

Calculates statistics based on fields in your events

> sourcetype=access_combined
| timechart count by status



Creates a time series chart with a corresponding table of statistics

Want to know more? Check out:

> Splunk Quick Reference Guide: <https://splk.it/SplunkQuickRef>

splunk turn data into doing®

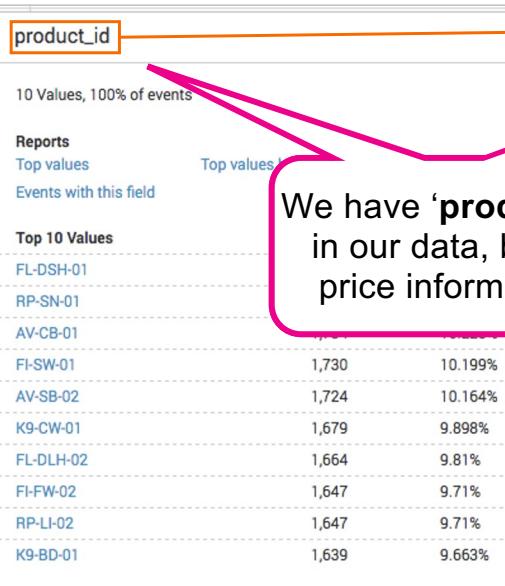


Business Analytics Team:

Show lost revenue from the website

Fields extracted from events by Splunk:

a date_wday 3
date_year 1
a date_zone 1
a file 4
a ident 1
a index 1
a itemid 16
a JSESSIONID 100+
linecount 1
a method 2
other 100+
a product_id 10
a punct 7
a referer 100+
a referer_domain 1
a req_time 100+
a splunk_server 1
status 5
timeendpos 8
timestamppos 8
a uri 100+
a uri_path 4
a uri_query 100+



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

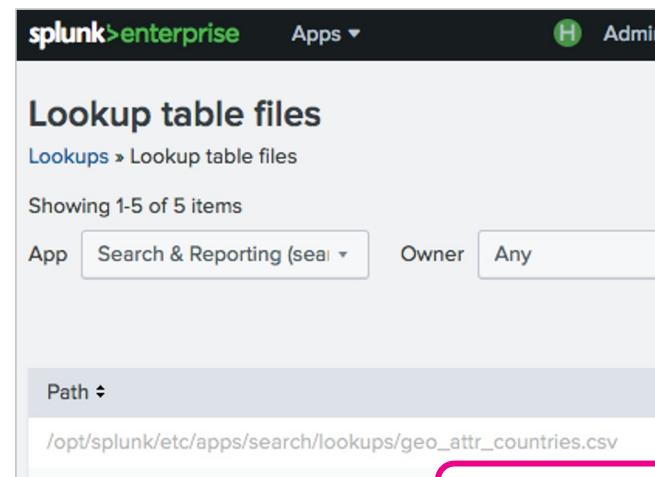
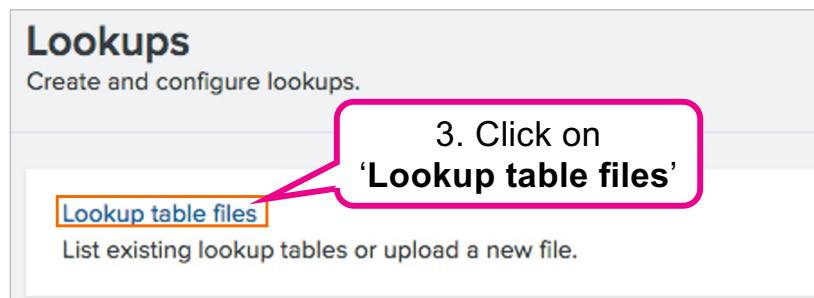
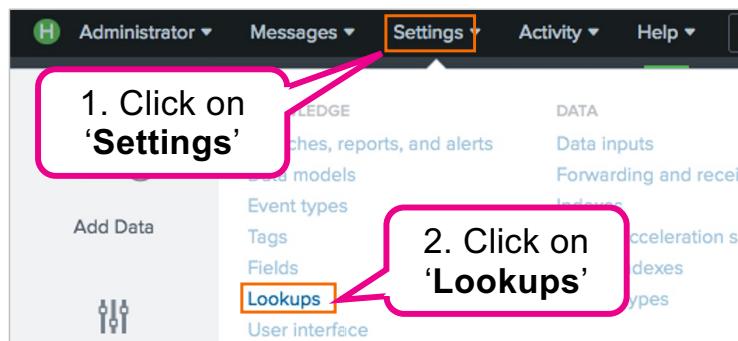
External CSV file:

category	product_id	product_name	product_price
Clothing	BS-2	Batguy Slippers	25.7
Books	MCB-5	Mad Comics- Batguy	12
Books	MCB-6	Mad Comics- Bronze	12
Books	MCF-3	Mad Comics- Flyman	12
Books	ZSG-2	Zombie Survival Guide	12
Costume	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
Gifts	WPSS-2	Waterproof Scratch and Sniff	4.99

This is the
information
we need!

Verify That the Lookup File Exists

- > A lookup file has already been uploaded for you!



Enriching Data with the `lookup` Command

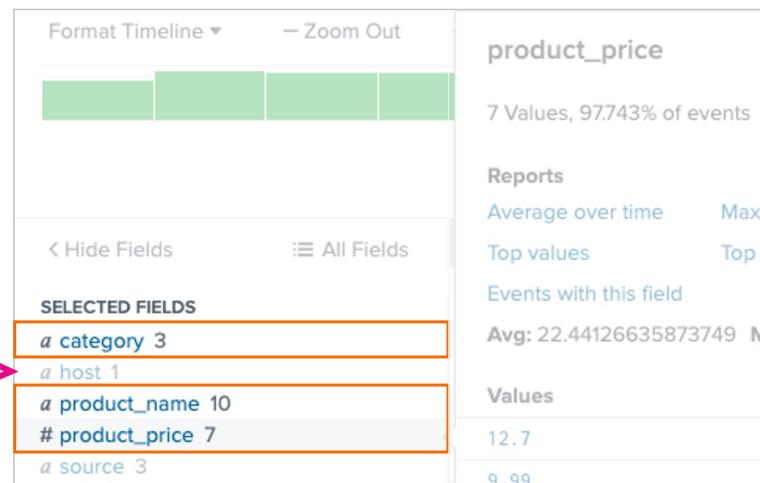
Usage:

```
<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 that exists in both the
Splunk data and the lookup file



The `lookup` command
retrieves additional fields
from the lookup file



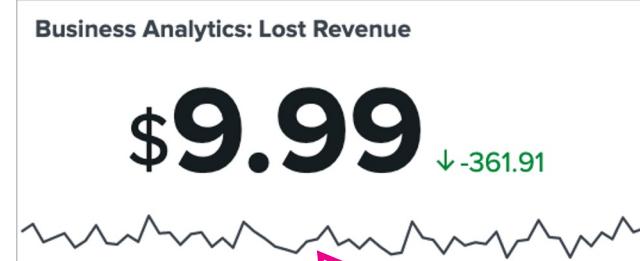
Lab Exercise 5: Business Analytics Team

Show lost revenue from the website

Tasks:

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 visualisation
3. Add your visualisation to your existing dashboard

Goal:



When you're happy with
your visualisation, add it to
your dashboard!

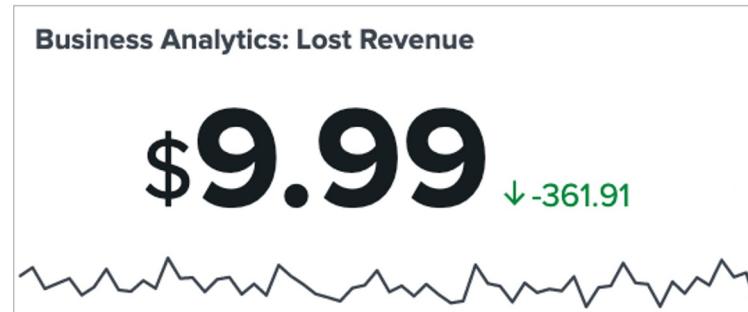


Lab Exercise 5: Business Analytics Team

Show lost revenue from the website

Solution:

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



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

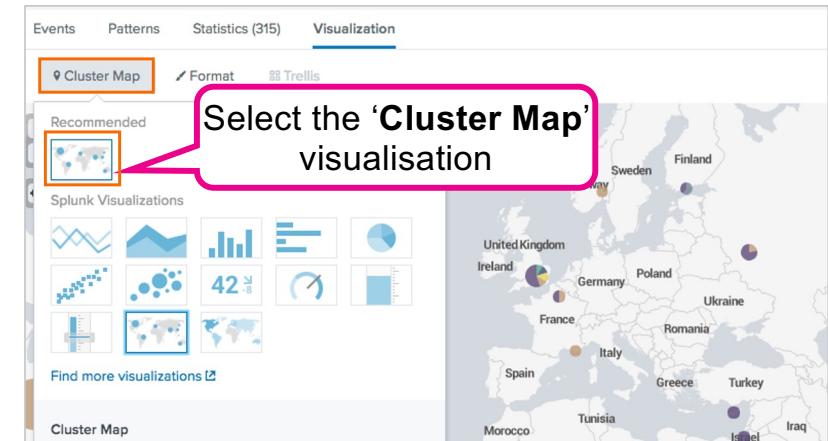
The name of a field in your data that contains IP addresses

Generates the ‘tiles’ that will be rendered on the map when visualised

Split your results by a specific field for more detailed analysis

a City 54
a Country 23
lat 56
lon 56
a Region 41

The `iplocation` command produces additional fields containing geographic data



splunk> turn data into doing®



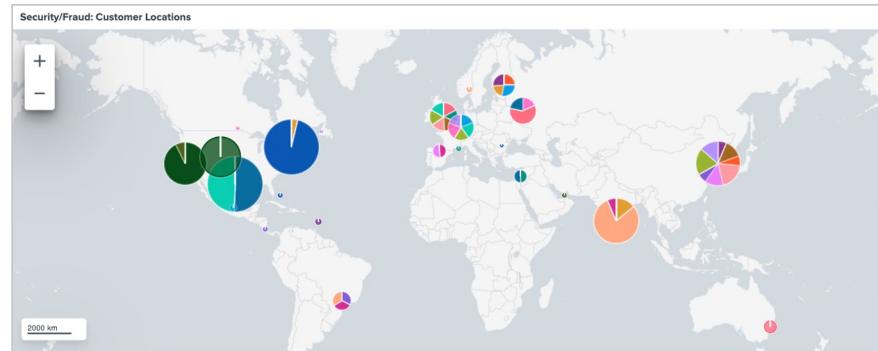
Lab Exercise 6: Security/Fraud Teams

Show website activity by geographic location

Tasks:

1. Use the [iplocation](#) command to enrich the events with location data
2. Generate a world map showing the geographic location of all website activity down to the city level
3. Add your visualisation to your existing dashboard

Goal:



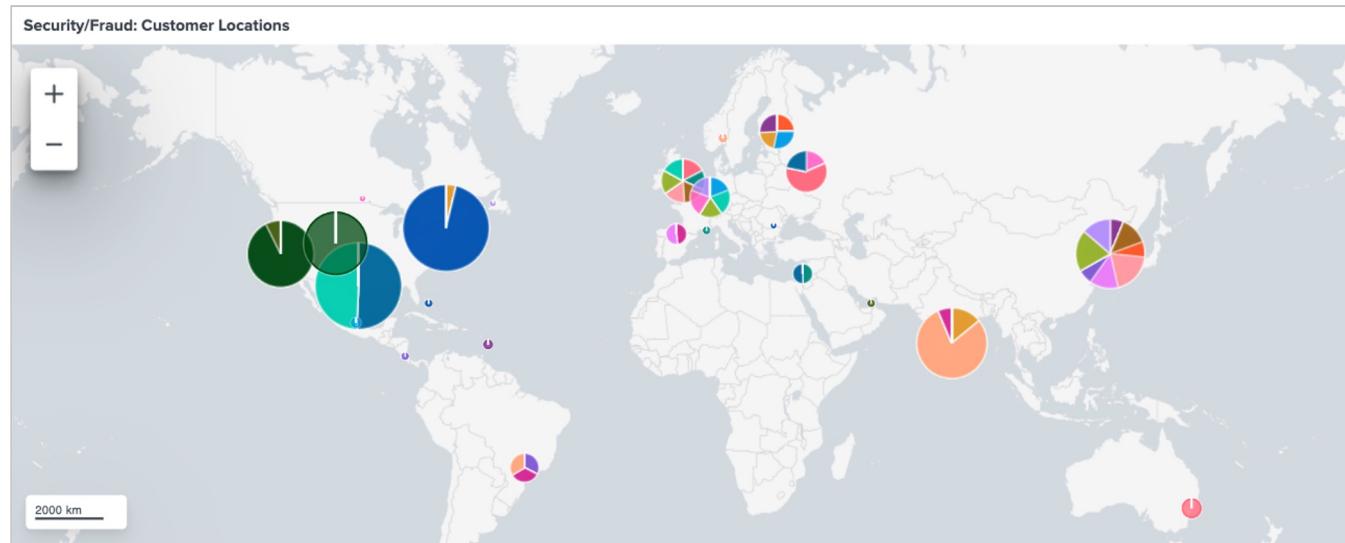


Lab Exercise 6: Security/Fraud Teams

Show website activity by geographic location

Solution:

```
> sourcetype=access_combined | iplocation clientip | geostats count by City
```





Create powerful, story-telling dashboards with Dashboard Studio

- ✓ Advanced visualisation tools
- ✓ Streamlined editing experience and fully customisable formats
- ✓ Flexible layouts (absolute and grid)
- ✓ Support for images, text boxes, shapes, lines and icons
- ✓ In-tact PDF export
- ✓ Support for custom SVG
- ✓ Support for dashboard level defaults

splunk > turn data into doing™

Customise Your Dashboard

The screenshot shows the Splunk interface for dashboard customization. On the left, a preview panel displays a chart with a wavy line and a bar chart below it. A pink callout box points to the 'Edit' button in the top right corner of this panel, with the text: 'Click on 'Edit' to put your dashboard into edit mode'. In the center, the main dashboard area contains several visualizations: a large number '263' with a green downward arrow, a bar chart titled 'IT Ops: Web Server Status Codes Over Time', a bar chart titled 'DevOps: Most Popular Operating Systems' showing Macintosh, Windows, Linux, and iPhone counts, and a line chart titled 'DevOps: Web Browsers With Most Failures'. Above these, a toolbar includes 'Gridlines' toggle, a percentage selector (71%), a 'Light' theme switch, a 'View' dropdown, and a prominent green 'Save' button. A pink callout box points to the toolbar with the text: 'Add new dashboard elements from the editing toolbar'. On the right, a configuration panel titled 'Splunk 4 Rookies' is open, containing sections for 'Configuration', 'Canvas' (with 'Display Mode' options like 'Actual Size' and 'Fit to Width'), 'Background Color' (#f2f4f5), 'Background Image' (with a note about uploaded files), 'Preferences' (with a 'Show Title & Description' toggle), and 'View Options' (with a 'Show Edit Button' toggle). A pink callout box points to this panel with the text: 'Customisation options from the contextual configuration panel'.

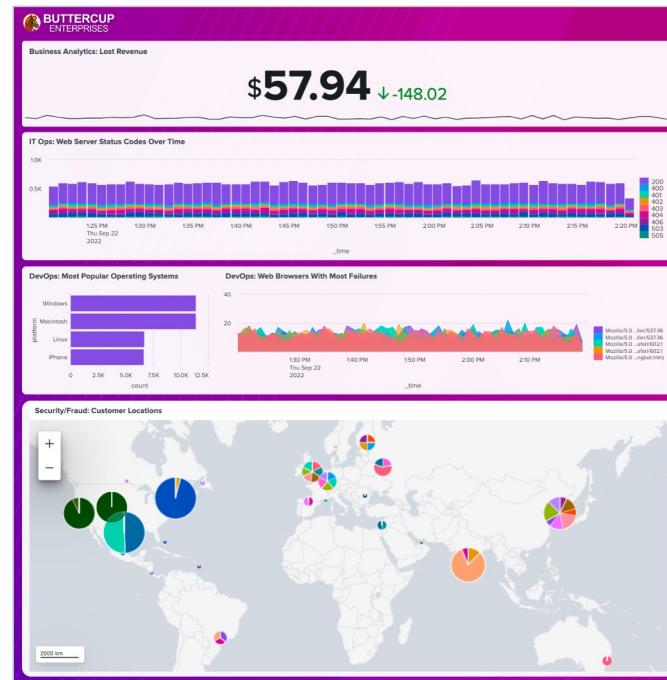


Lab Exercise 7: Customise Your Dashboard!

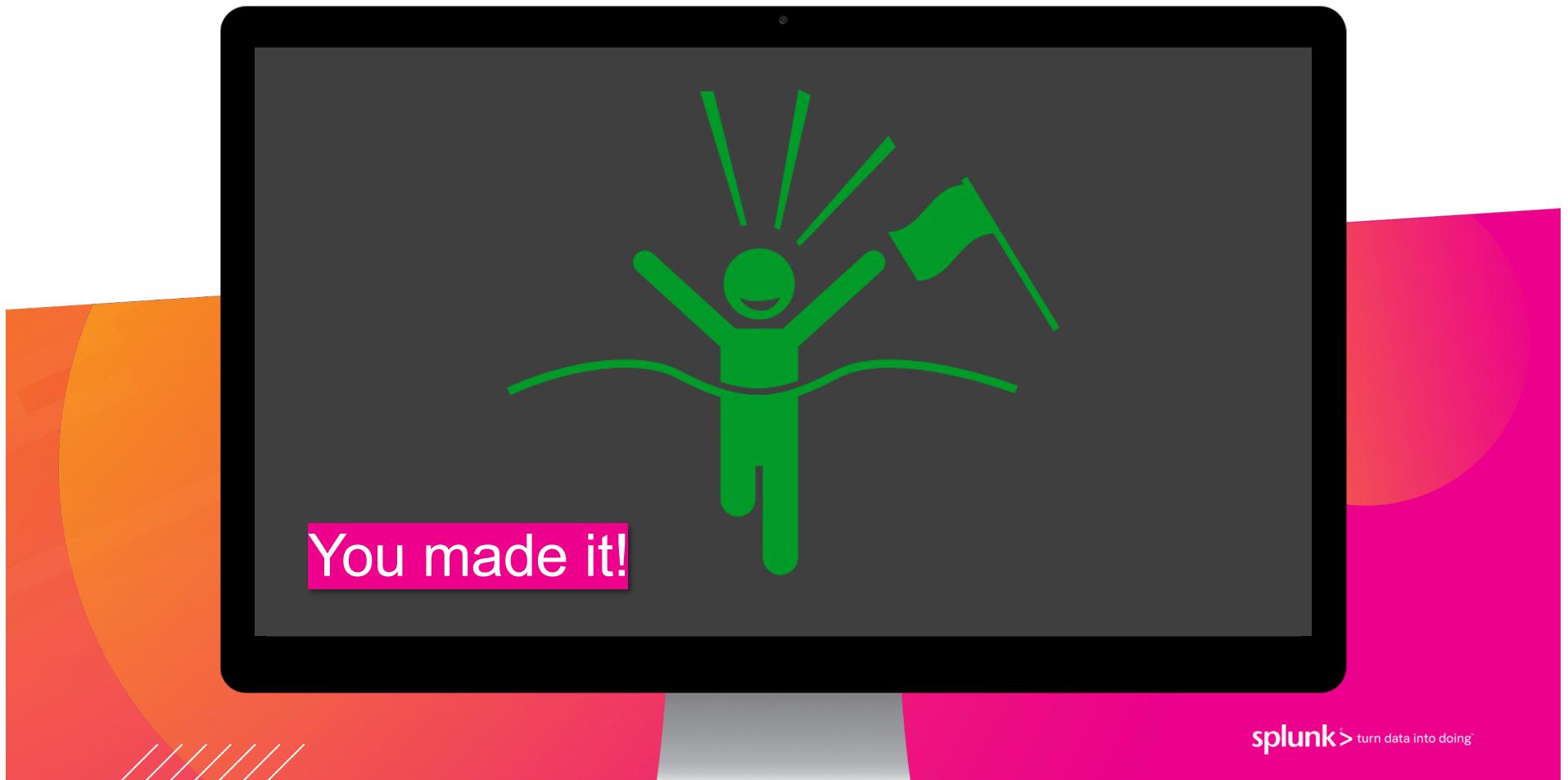
Tasks:

1. Add a custom background image provided by the Buttercup Enterprises Marketing team (<https://splk.it/ButtercupBackground>)
2. Resize your dashboard panels to fit within the boxes on the background image
3. Link your dashboard panels to the global time picker

Goal:

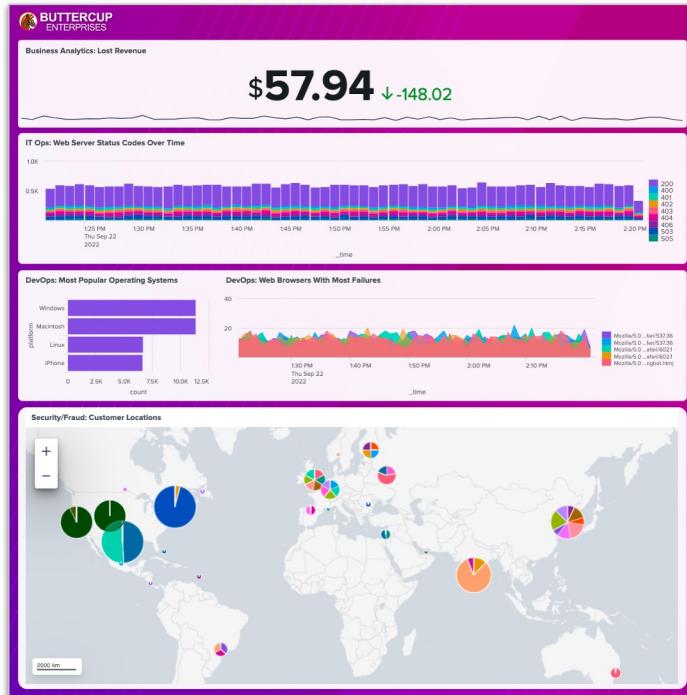


You Finished the Hands-on Exercises!

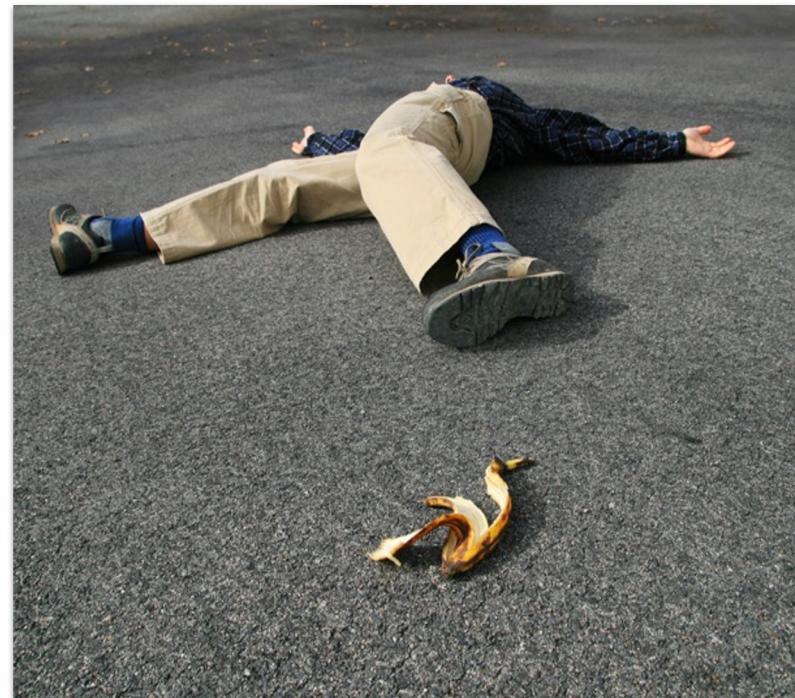


How Did You Do?

Did you end up like this?...



Or this?





Splunk Resources

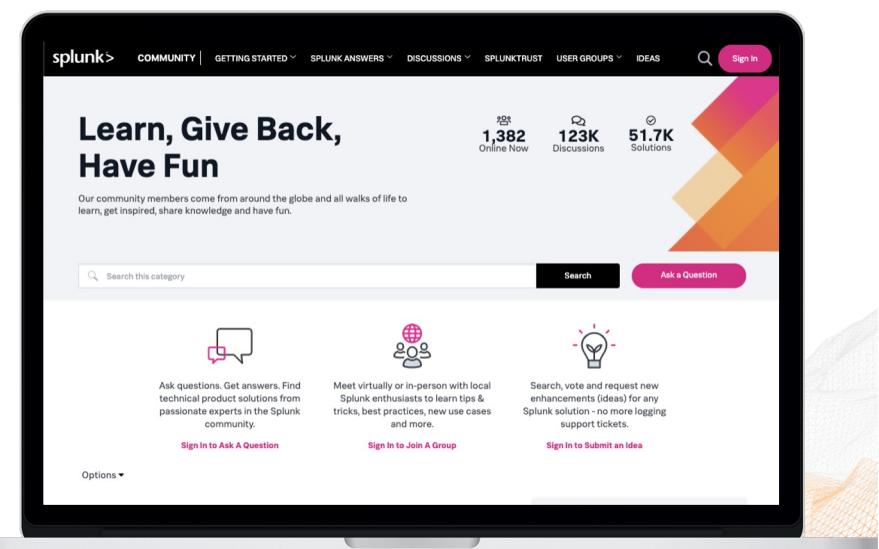
Where to go after today's workshop

splunk® turn data into doing™

Splunk Community

<https://community.splunk.com>

- > A free way to connect, learn, have fun, and find success with Splunk
- > Ask questions, get answers, and find solutions from passionate experts in the community
- > Meet in-person or virtually with like-minded enthusiasts, in your area or by interest
- > Search for, vote on, or submit your own ideas for new enhancements for any product or solution



splunk® turn data into doing™

Splunk Events

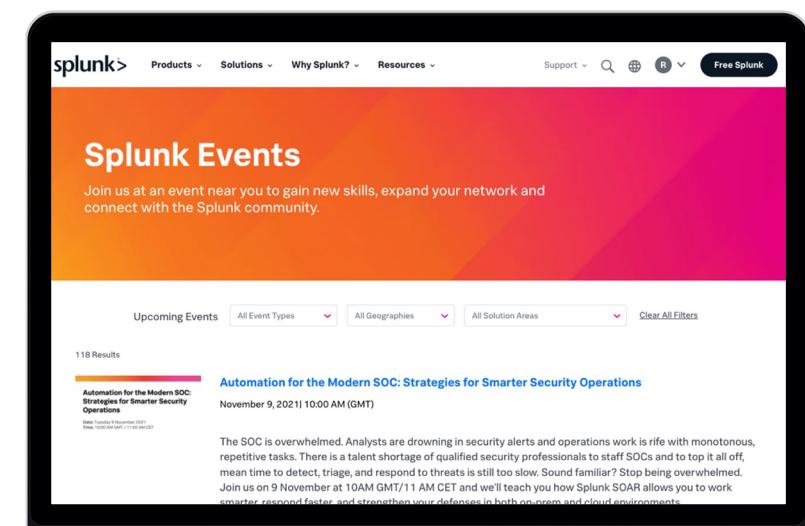
<https://events.splunk.com>

- > Expand your network and connect with the global and local Splunk community



<https://conf.splunk.com>

- > Join us at .conf23!
- > Hundreds of on-demand sessions from product updates to learning new Splunk skills!



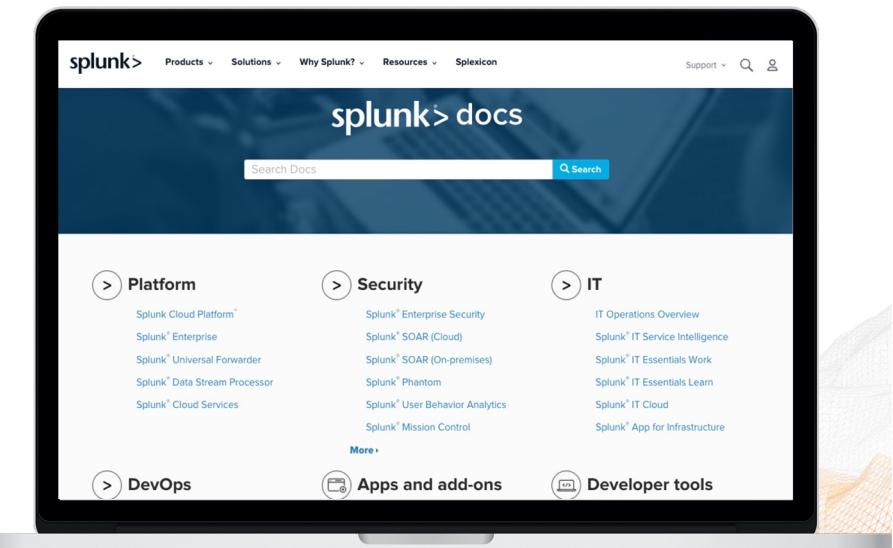
A screenshot of the Splunk Events website. The header features the Splunk logo and navigation links for Products, Solutions, Why Splunk?, Resources, Support, and a search bar. The main section is titled "Splunk Events" with the subtext "Join us at an event near you to gain new skills, expand your network and connect with the Splunk community." Below this is a search bar and filter options for "Upcoming Events", "All Event Types", "All Geographies", "All Solution Areas", and "Clear All Filters". The results section shows 118 results for the session "Automation for the Modern SOC: Strategies for Smarter Security Operations" on November 9, 2021, at 10:00 AM (GMT). A brief description of the session is provided.

splunk> turn data into doing®

Documentation

<https://docs.splunk.com>

- > Search reference for SPL
- > Step-by-step tutorials
Search: <https://splk.it/SplunkSearchTutorial>
Dashboard Studio: <https://splk.it/SplunkDashStudioTutorial>
- > Product references
- > Procedures/guides
- > And more!

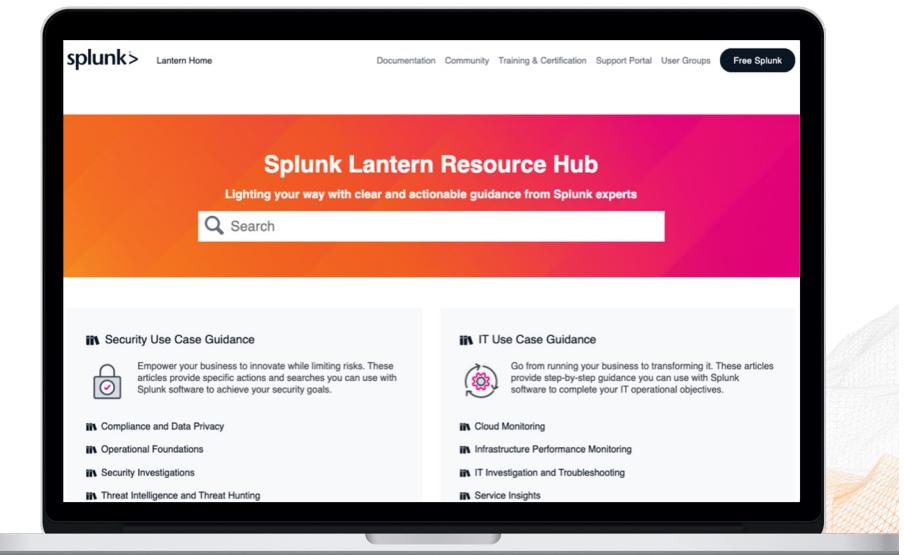


splunk> turn data into doing®

Splunk Lantern

<https://lantern.splunk.com>

- > Use case library
- > Step-by-step procedures
- > Map use cases to data sources
- > Splunk Success Framework to realise value across your organisation

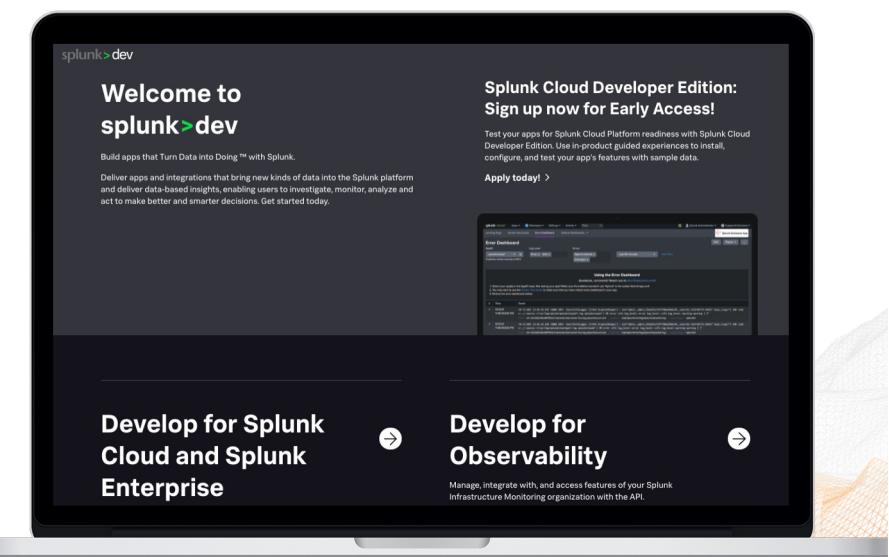


splunk> turn data into doing®

Developer Resources

<https://dev.splunk.com>

- > Developer Guide
- > API Reference
- > Tutorials
- > Downloads
APIs, libraries, tools
- > Code examples
- > Free Developer licence
- > Splunk Cloud Developer Edition
Test your apps for Splunk Cloud readiness

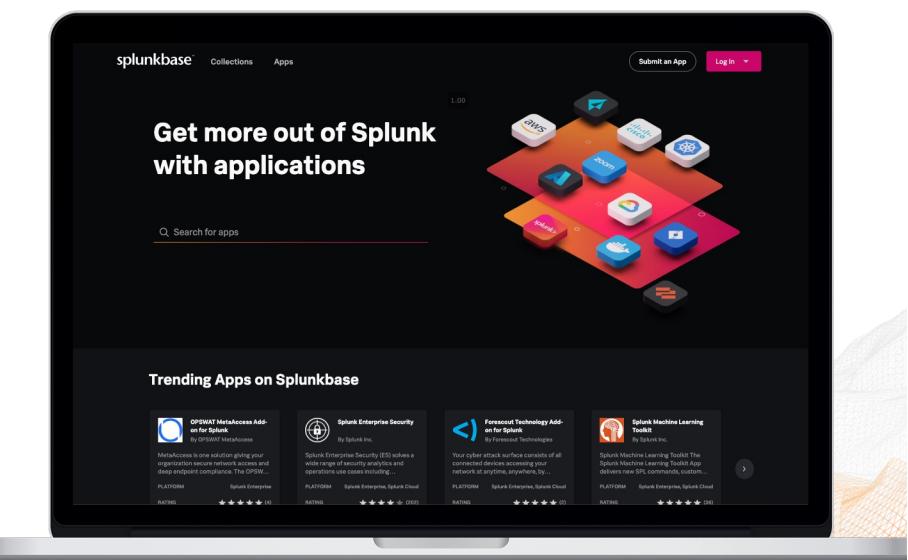


splunk> turn data into doing®

Splunk Apps & Add-ons

<https://splunkbase.splunk.com/>

- > 2800+ apps and add-ons
- > Pre-built searches, reports, visualisations 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!

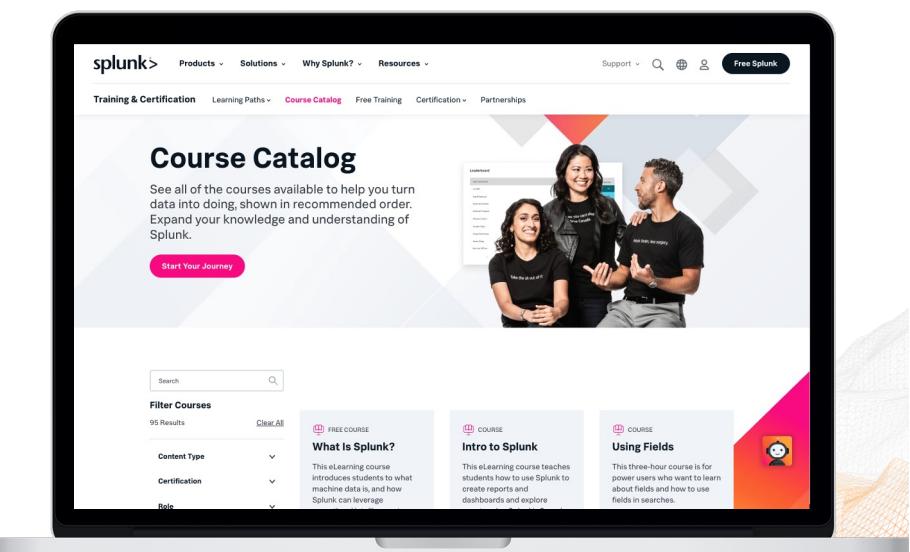


splunk > turn data into doing®

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!
Free single-subject eLearning courses to kick start your Splunk learning



Thank You



splunk > turn data into doing™