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> turn data into doing®

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

#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

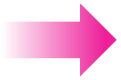
Enjoys Michigan Football

$whoami

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

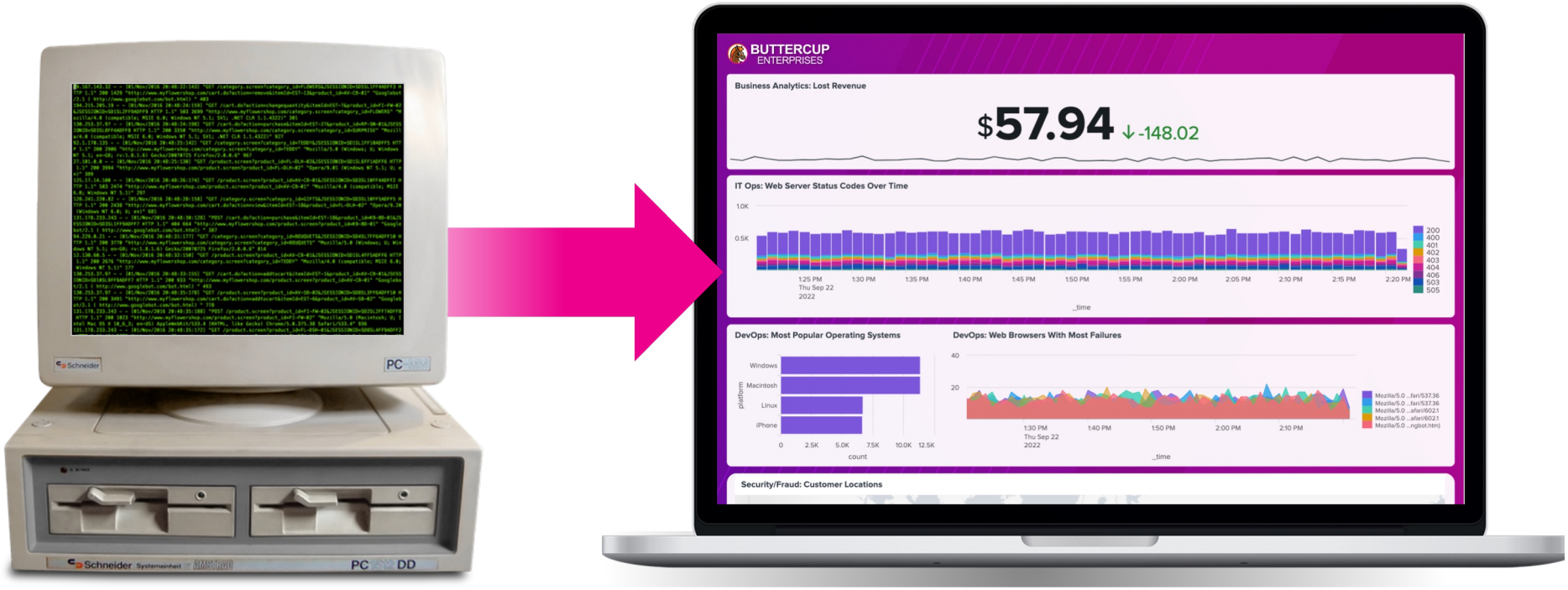
There's a Lot More to Splunk…

- 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



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

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

Enterprise Security
Detect, Investigate & Response

- Single pane of glass
- Security Metrics & Incident Response
- Adaptive Response
- Collaboration

Splunk Enterprise
Investigate

Realm of Known

- Log Aggregation
- Rules, statistics, correlation
- Ad hoc searches and data pivot

Human-driven

Splunk UBA
Detect

Realm of Unknown

Risky Behavior Detection
Entity Profiling, Scoring
Kill chain, Graph analysis

ML-driven

Phantom®

- Security Orchestration and Automation

splunk> turn data into doing®

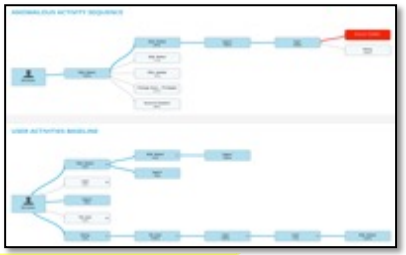
Different *lenses* into the same data

IT Ops Center

Security Ops Center

Compliance Ops Center

Mission Ops Center, etc…



Different People, Asking Different Questions, Of the Same Data

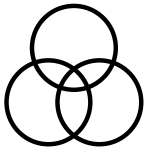
Data Reuse = Greater Data Leverage

Users only *see* what they should

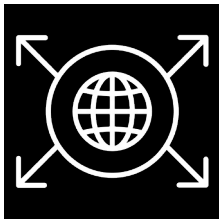
Why Re-invent the Wheel?

splunk> **Machine Data Fabric**

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

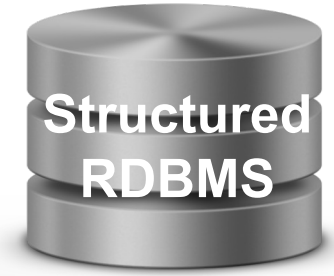
Challenge: Adapt to Variety and Variability of Data

Other Guys

Schema at Write

SQL

ETL



Splunk

Schema at Read

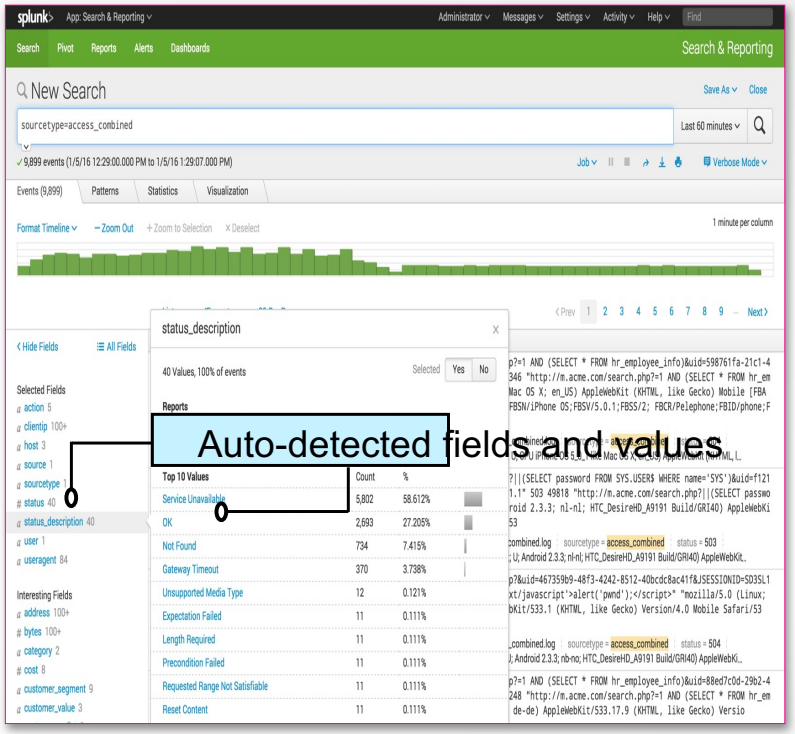
Search

Universal Indexing

Unstructured

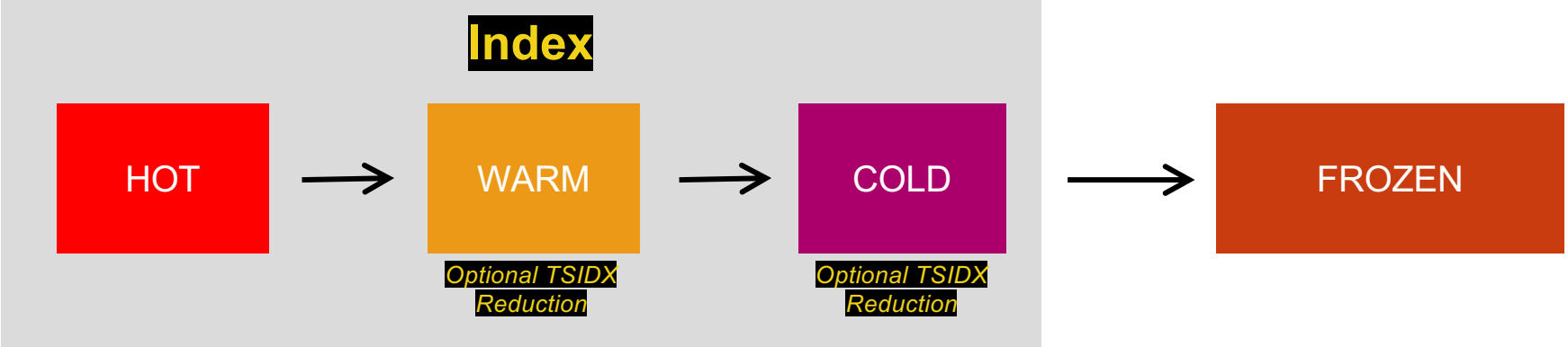
Volume | Velocity | Variety

Schema at Read



splunk>

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

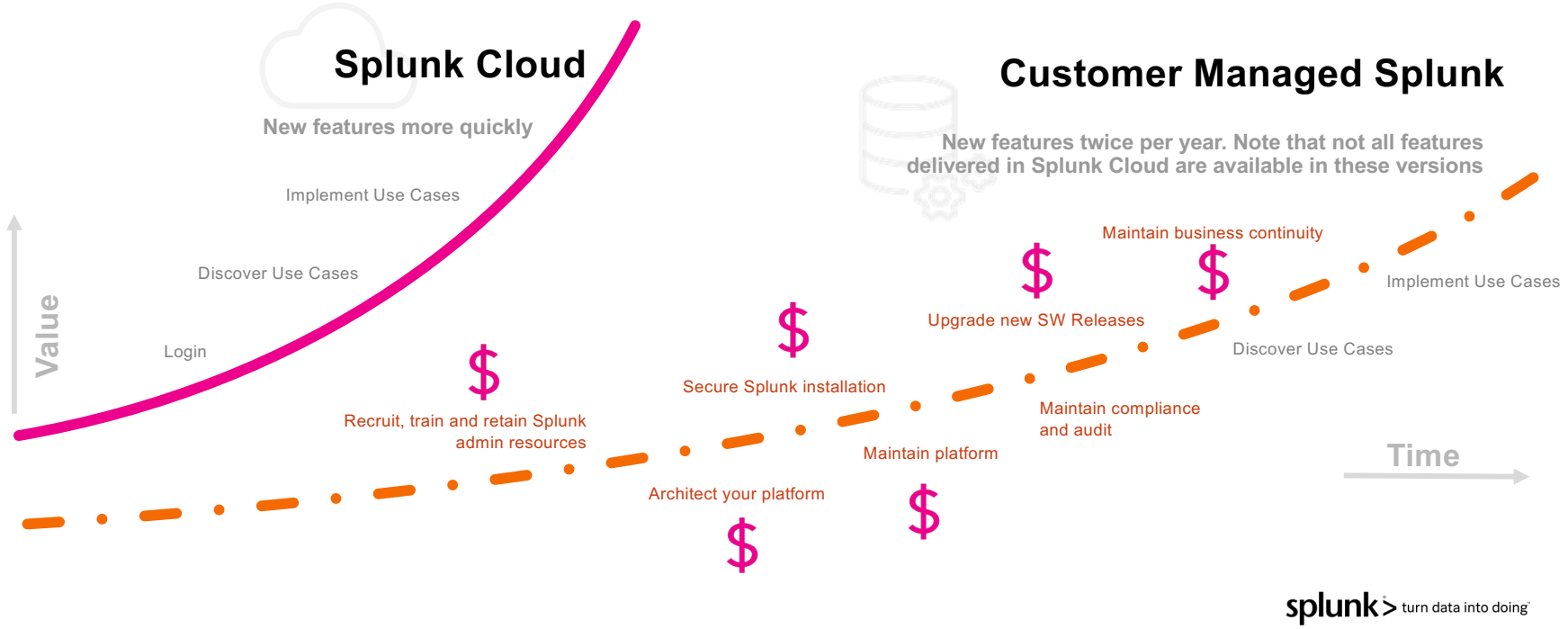
- Customer runs their own Splunk license on-prem or on IaaS (AWS, Azure, Google, other public/private cloud)
- Customer manages their infrastructure
- Customer is responsible for installation, setup, updates and upgrades
- Your IT team is responsible for a successful deployment
- Risk is predominantly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

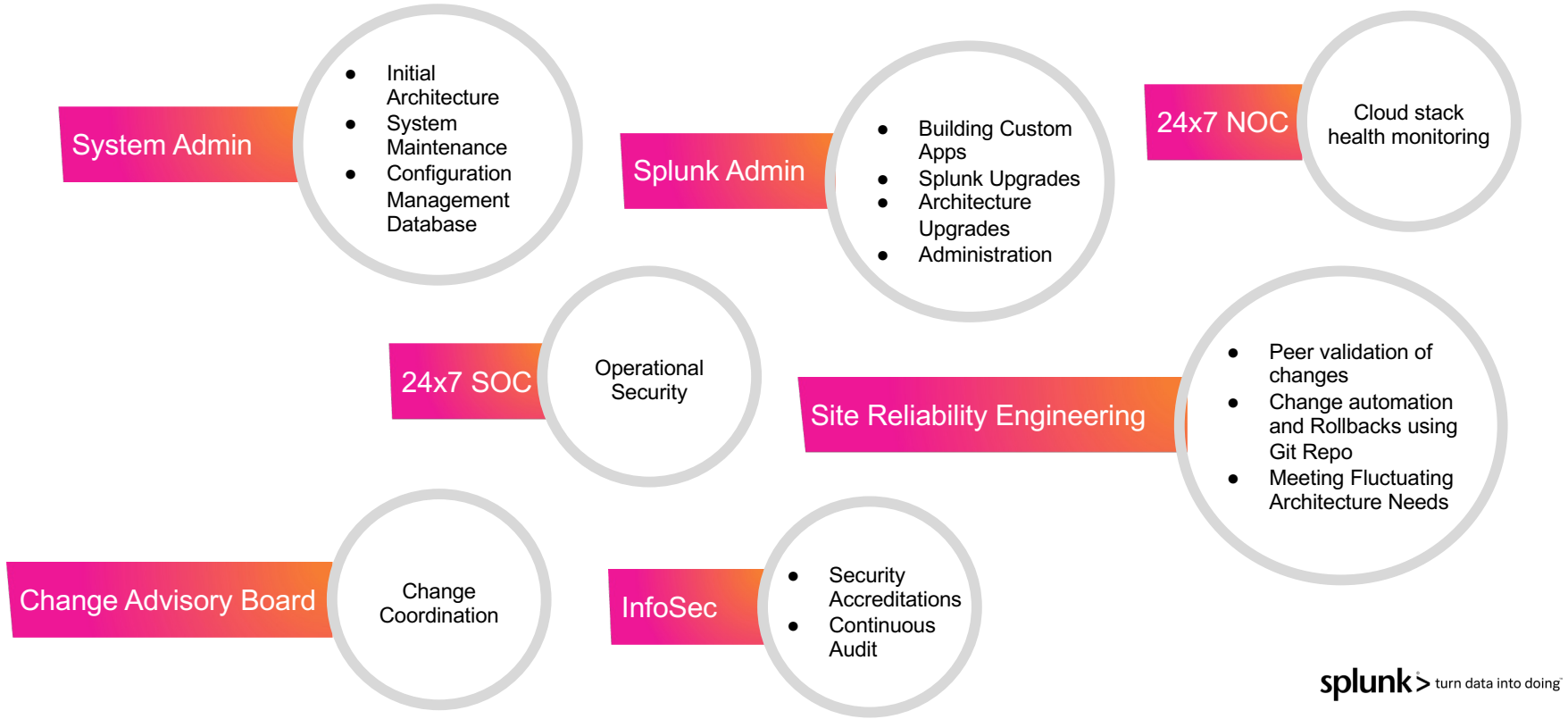
Get more value and get it faster

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



splunk> turn data into doing

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
Admin Tasks: Ongoing	Scale up HW	Customer	Splunk
	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
User Tasks	Search, alerts, reports, dashboards	Customer	Customer

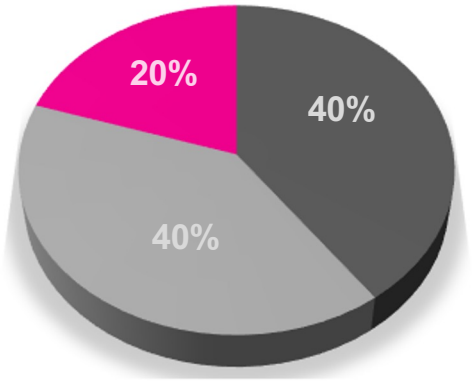
Managing a Splunk deployment involves 12 on-going admin tasks, 8 of which are conducted by Splunk for a Cloud based deployment

splunk> turn data into doing®

Reallocate your Time

To focus on higher value tasks directly tied to business outcomes

Customer Managed Splunk

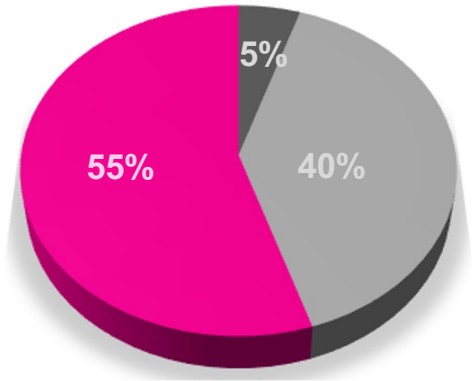


35%

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

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

Splunk Cloud SaaS



High Value use case delivery, adoption enablement, value realization

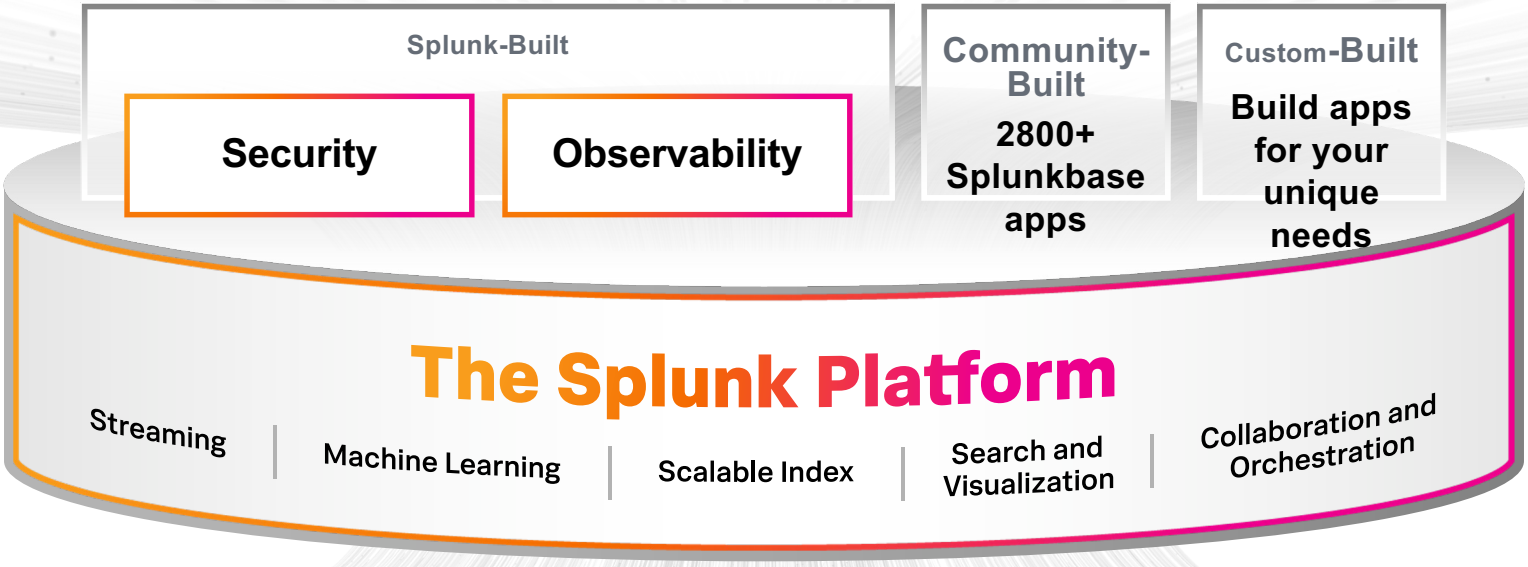
Data and user onboarding

Platform management

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

splunk> turn data into doing®

Introducing Splunk



0010 01010 0101 **Events** | **Logs** | **Metrics** | **Traces**

Public Clouds

Third-Party Tools

On-Prem Data Centers

Apps / Services

Edge

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> turn data into doing

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**

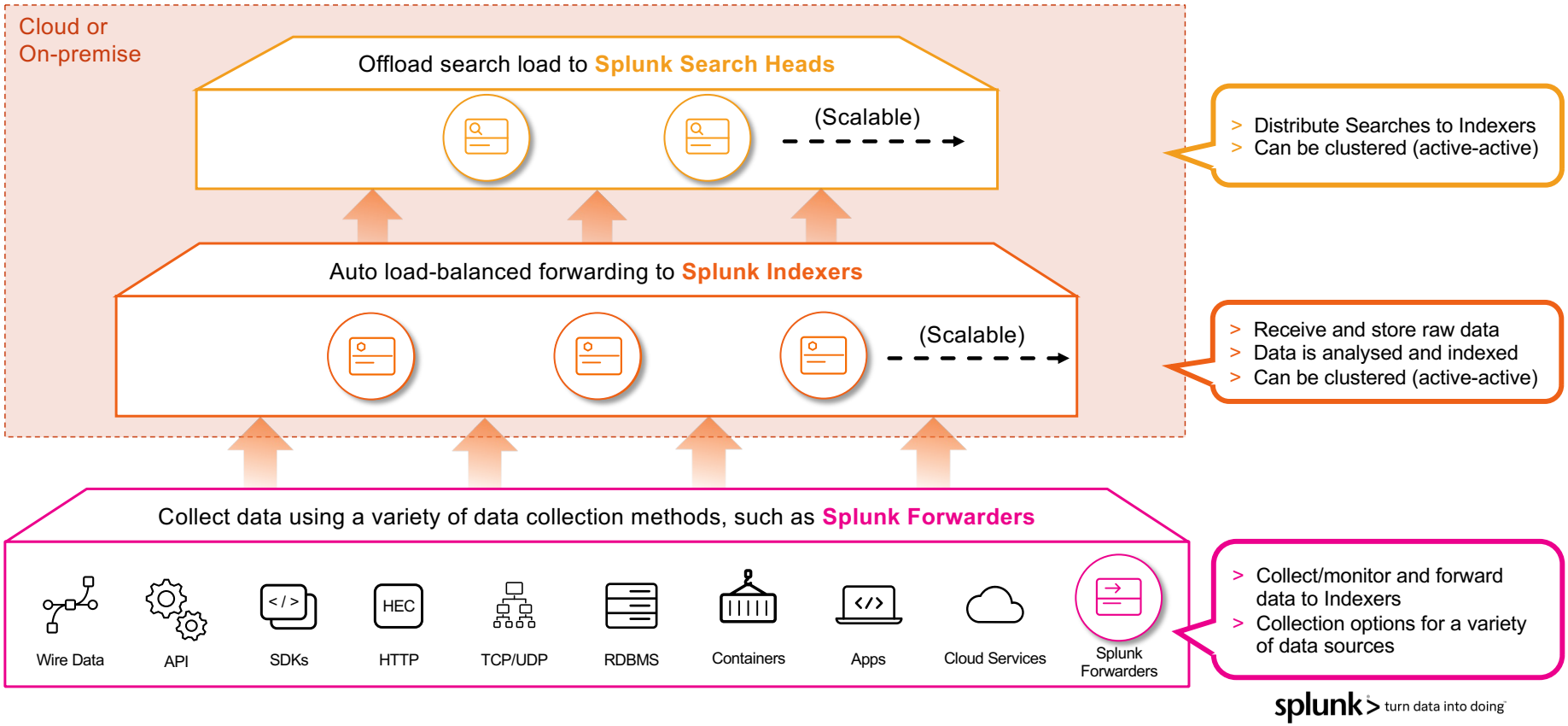
Flexible options for data collection and forwarding

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

splunk> turn data into doing®

Scales to Petabytes Per Day

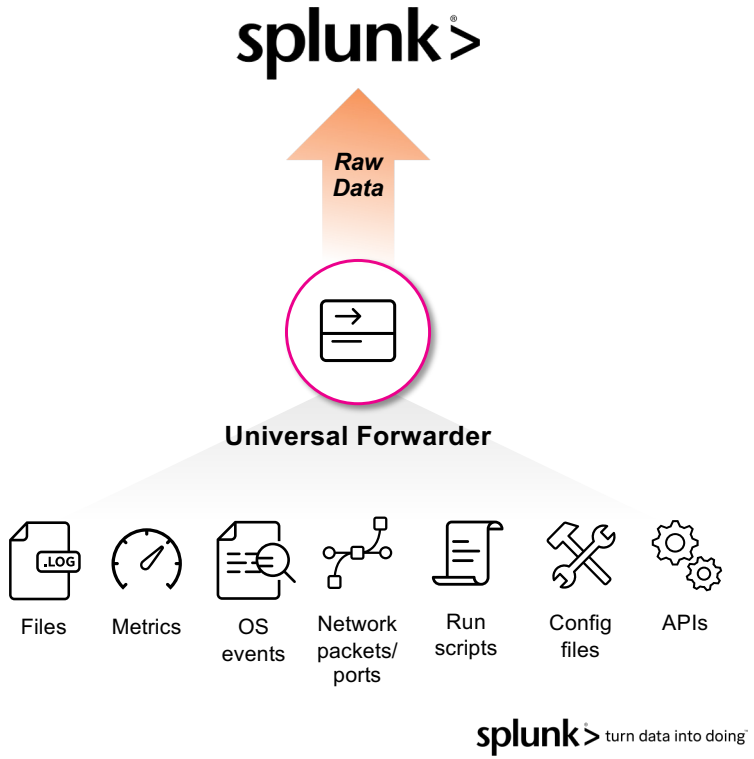
Enterprise-Class Scale, Resilience and Interoperability



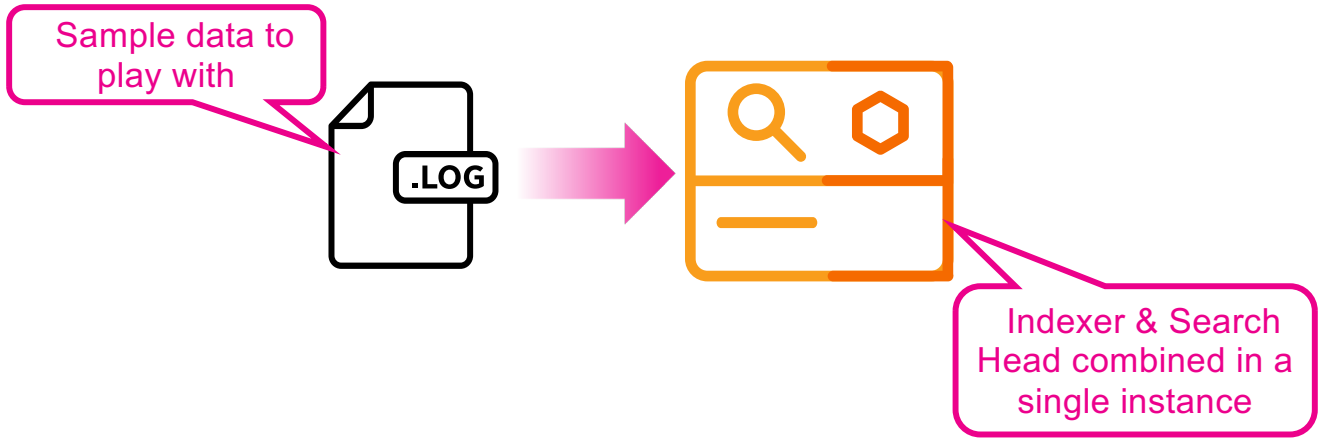
splunk> turn data into doing

What is a Splunk Universal Forwarder?

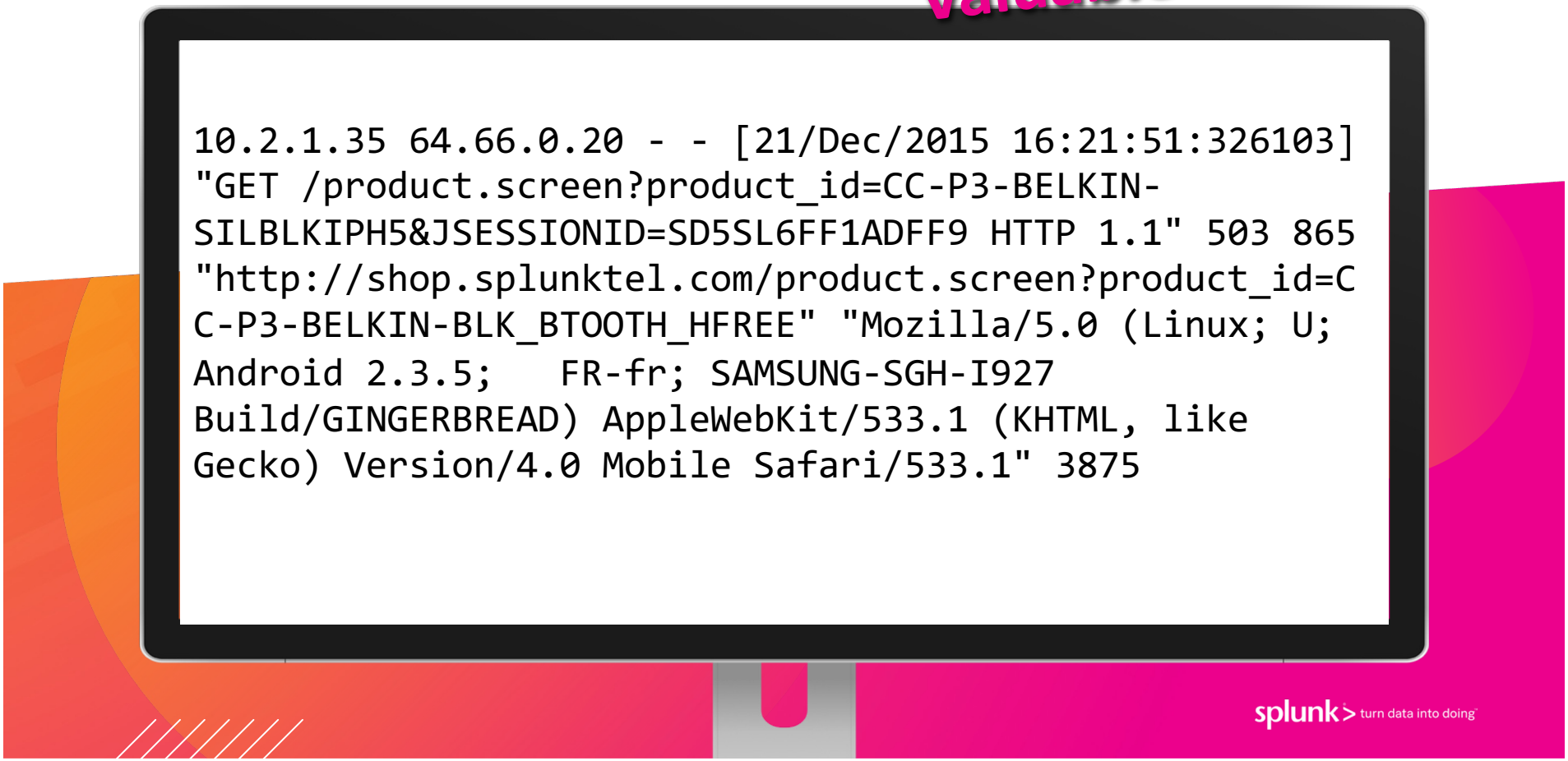
- Reliable collection of data from remote locations
- Includes methods for collecting from a variety of data sources
- Lightweight but powerful:
  - ✓ Buffering / guaranteed delivery
  - ✓ Encryption
  - ✓ Compression
  - ✓ Load balancing
  - ✓ And more!
- Very small footprint
- Just forwards data –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



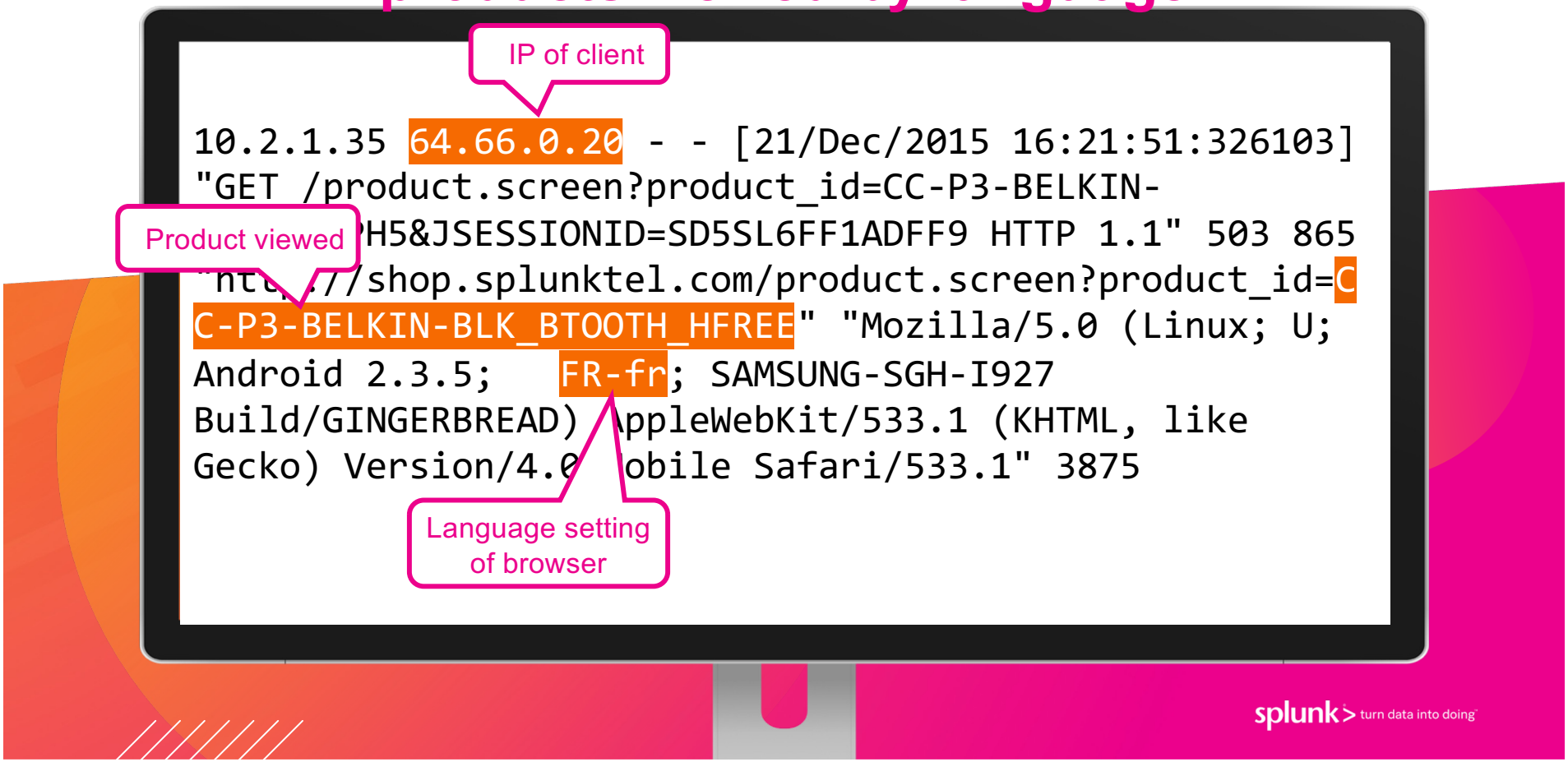
Today's Environment



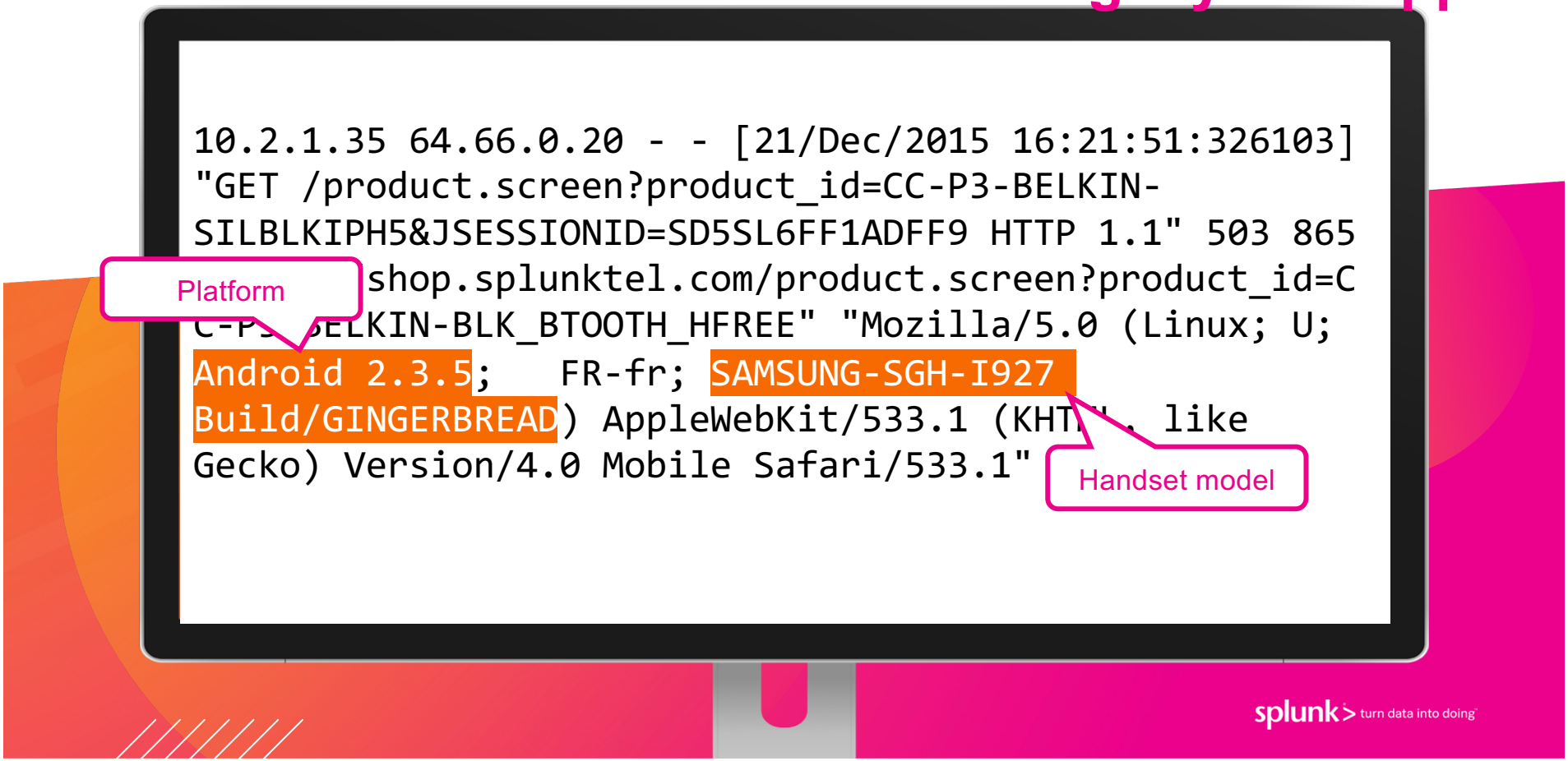
Machine Data is ~~Complex~~ Valuable!



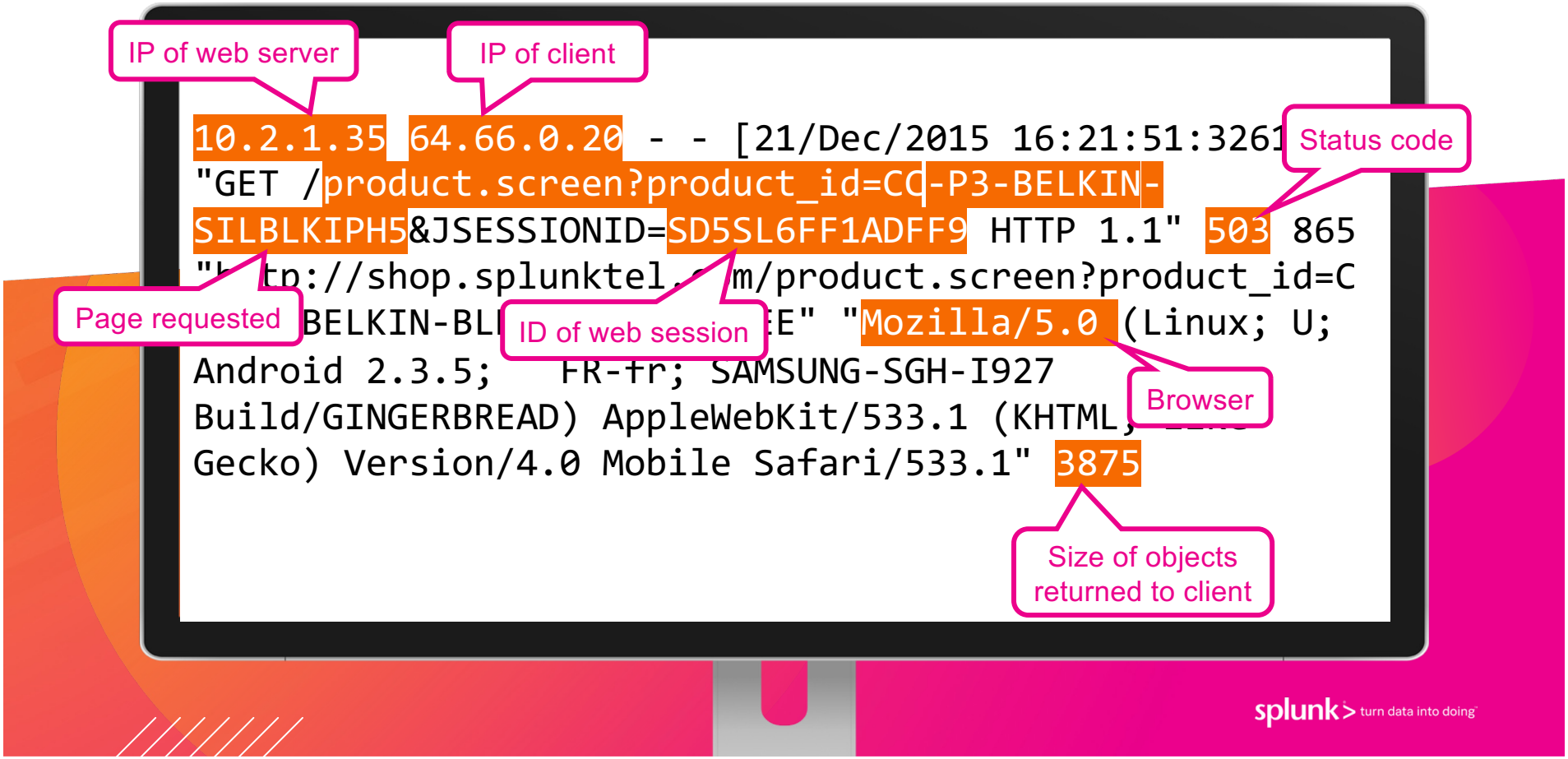
Marketing Use Case: Show the top products viewed by language



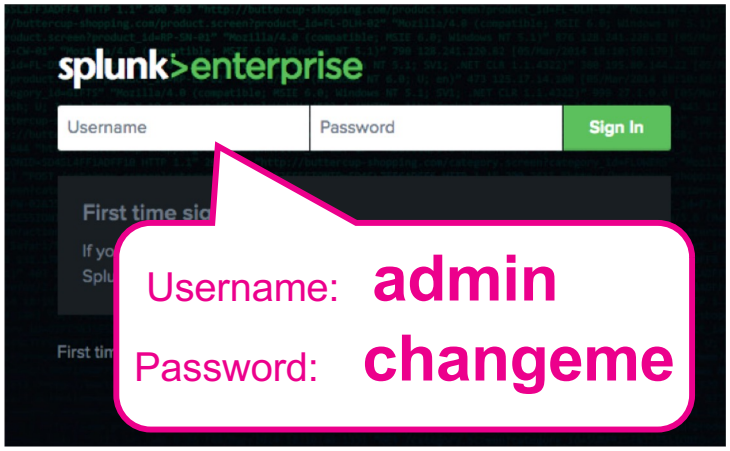
DevOps Use Case: Which mobile handsets should I test the most before releasing my new app?

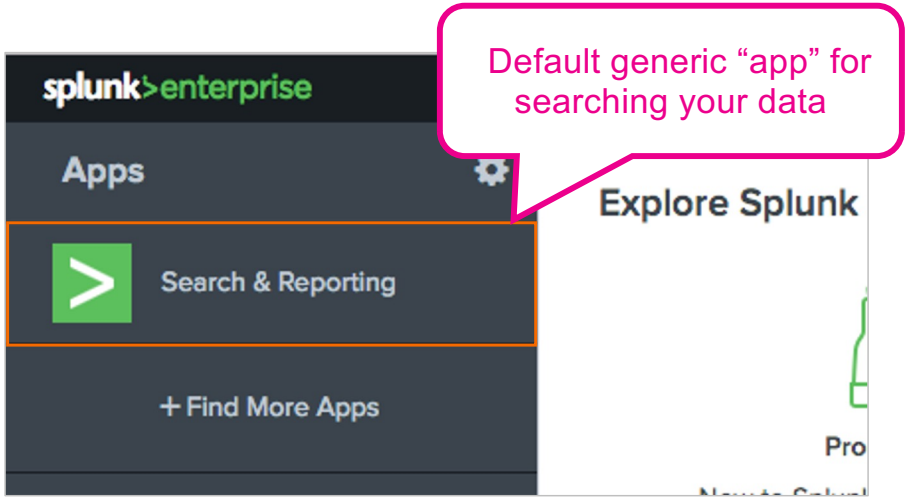


IT Operations Use Case: Web pages with errors



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

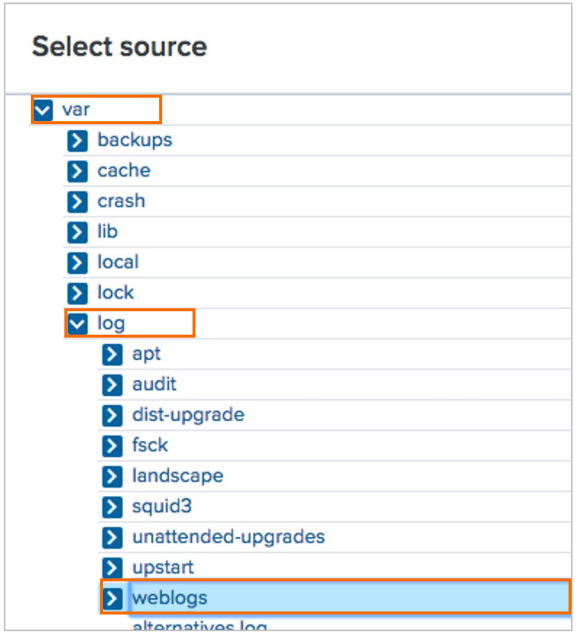
Add-ons

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:

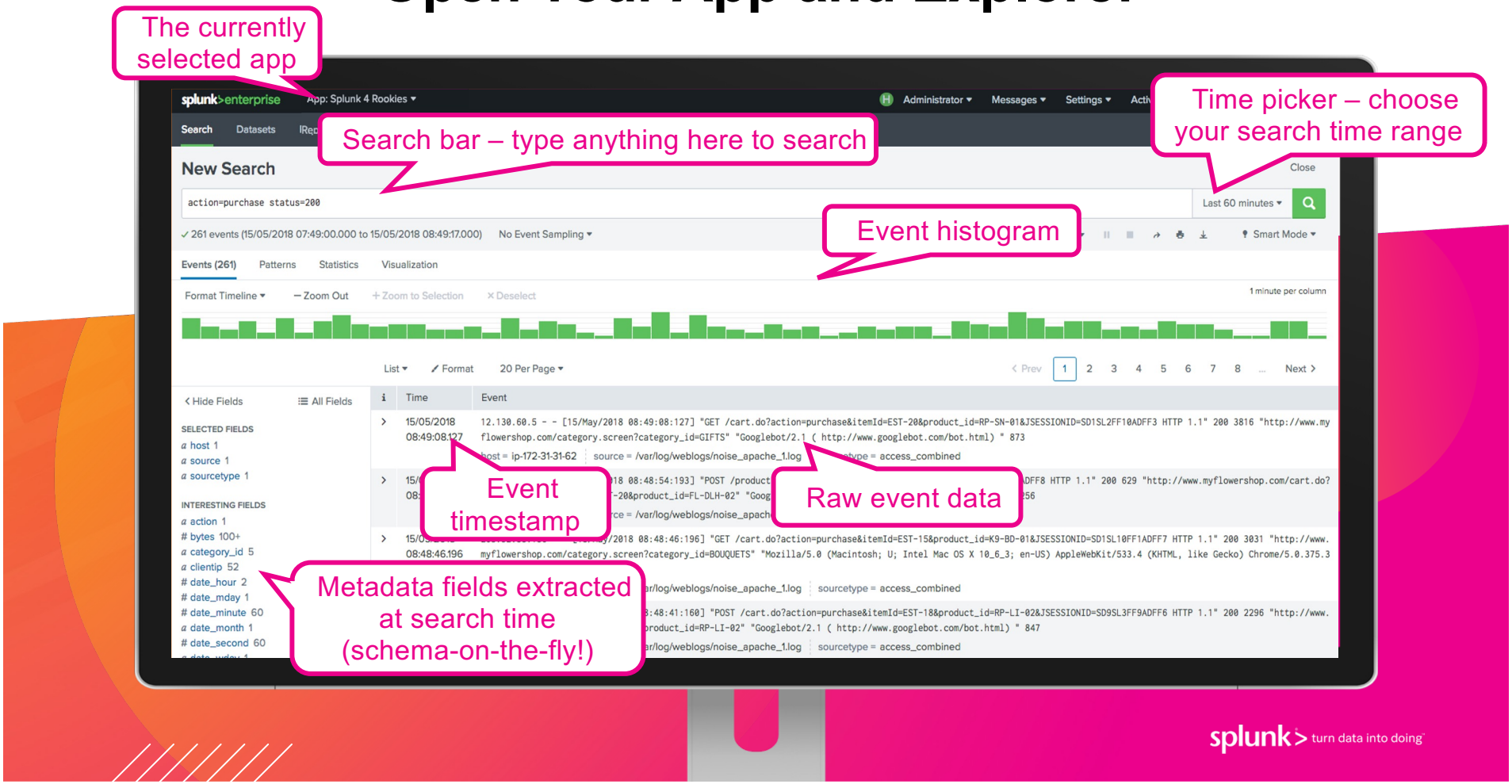
1. Create a new app
2. Monitor a directory: /var/log/weblogs
1. Select a source type: access_combined
1. View your data in Splunk



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

splunk> turn data into doing

Open Your App and Explore!



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)

Search terms

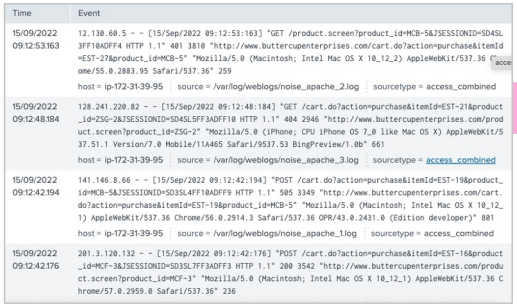
Commands

```
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` `| rename count as "number of events"`



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

status	number of events
200	850
400	81
401	76
402	50
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**

What Does the Business Want to See?

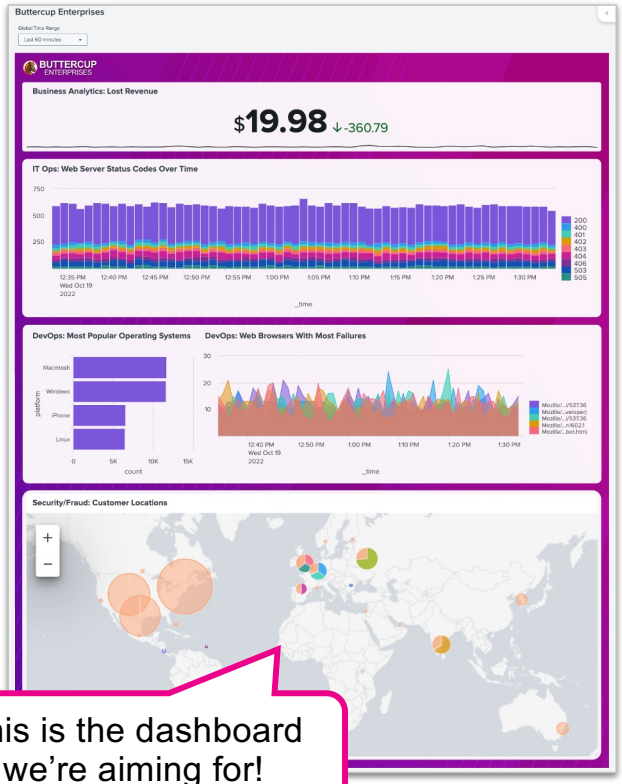
We need to create a dashboard with four views:

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



This is the dashboard we're aiming for!

splunk> turn data into doing

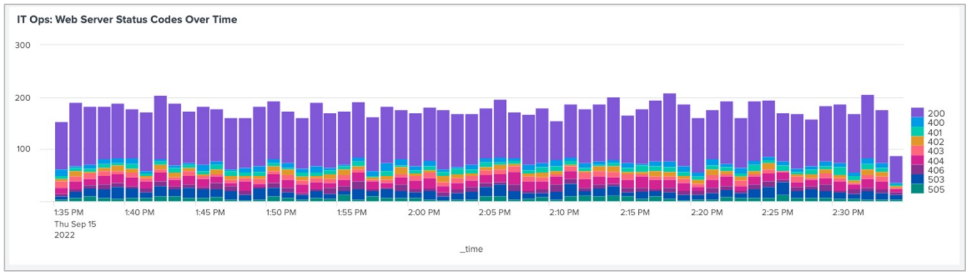
Lab Exercise 3: IT Operations Team

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!

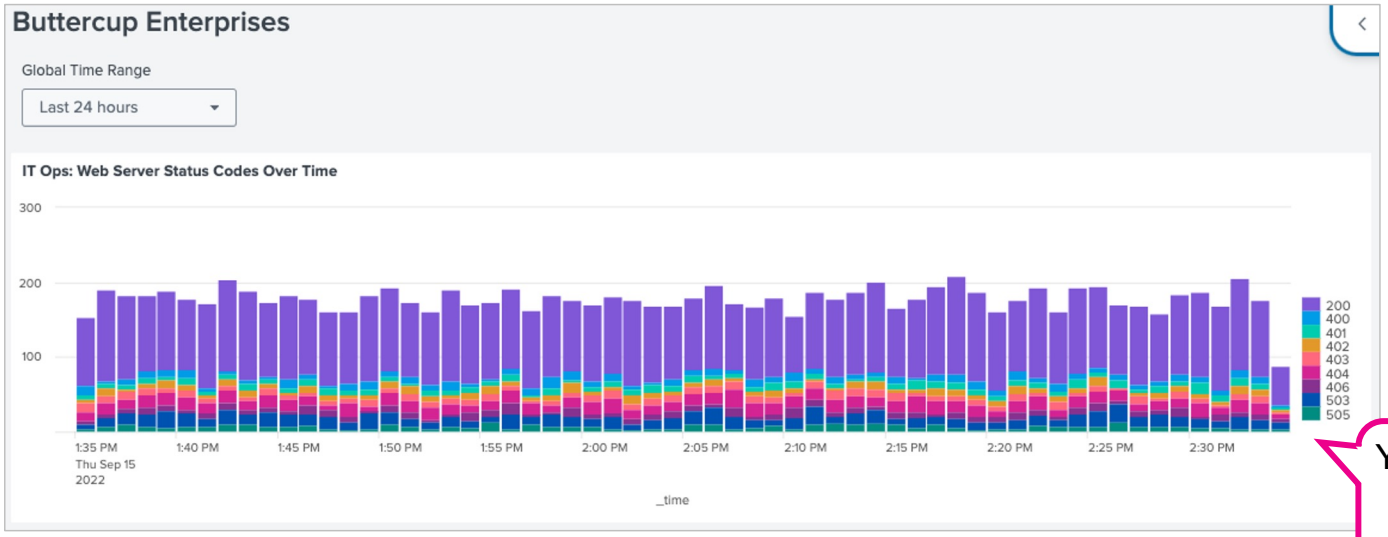
Goal:



Your Dashboard so far…

Solution:

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

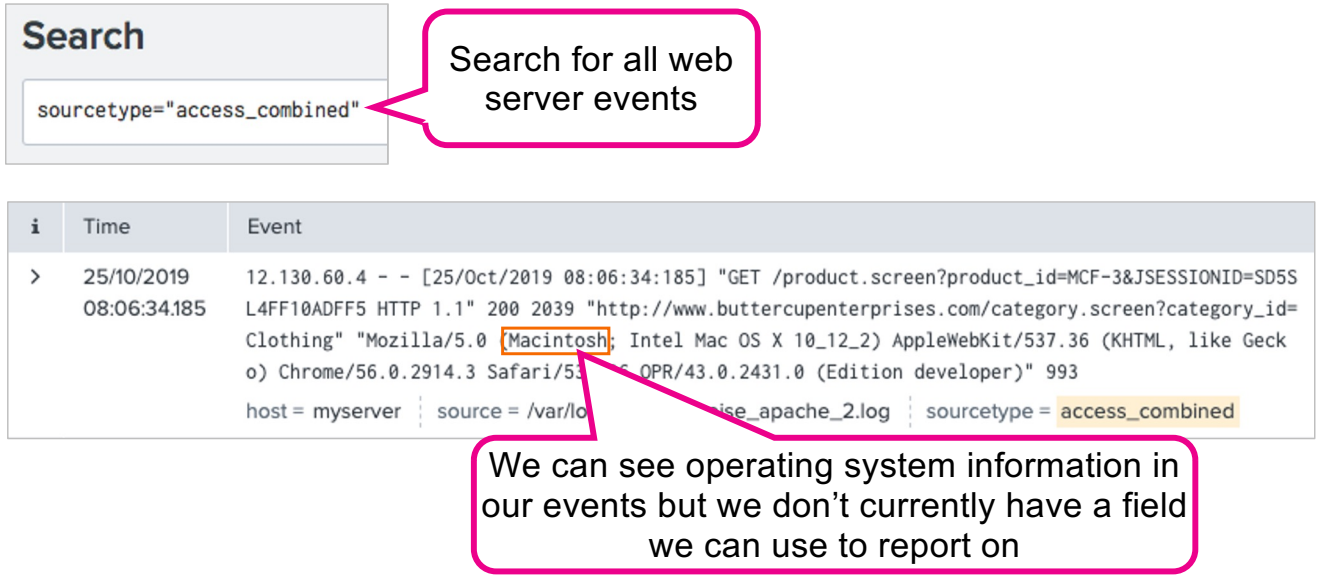


Your dashboard should hopefully look something like this

DevOps Team

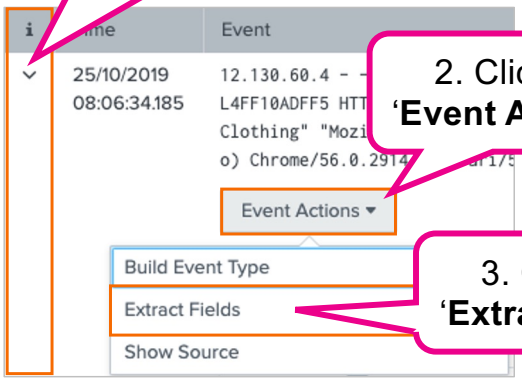
Show the most common customer operating systems and which web browsers are experiencing the most failures

Step 1: Show the most common customer operating systems



Extracting a New Field

1. Click on the arrow to expand an event

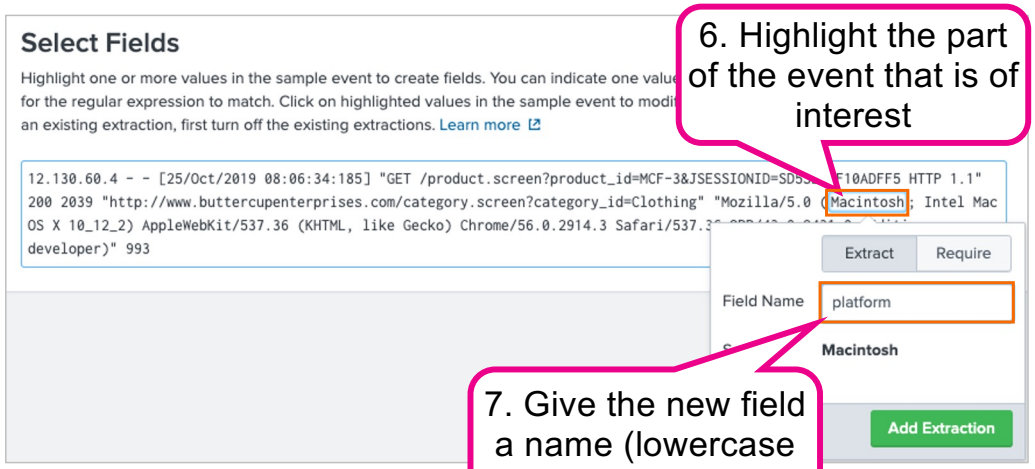


2. Click on '**Event Actions**'

3. Click on '**Extract Fields**'

4. Click on '**Regular Expression**'

5. Click on '**Next**'



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

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

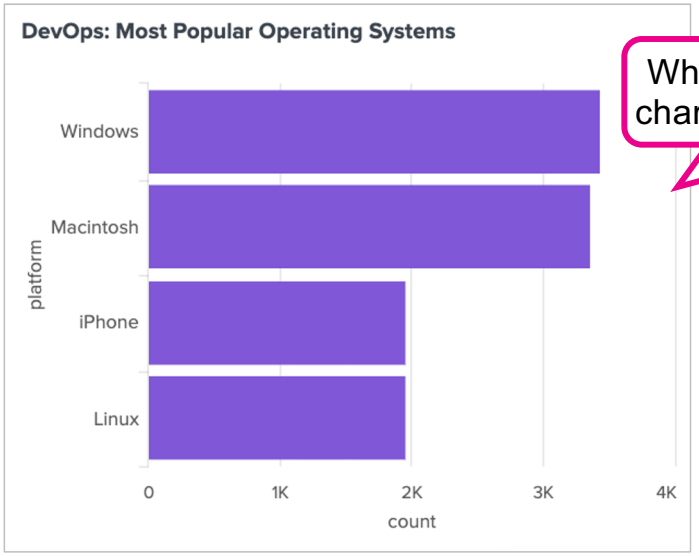
Goal:

Lab Exercise 4: DevOps Team

Show the most common customer operating systems

Solution:

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



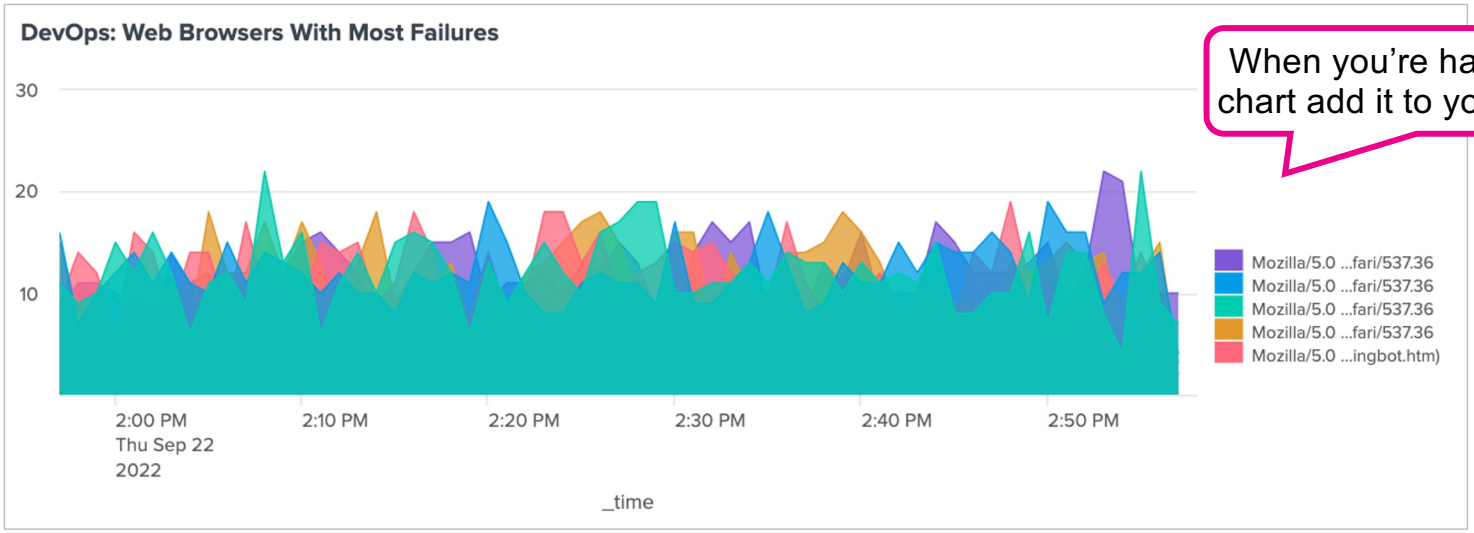
When you're happy with your chart add it to your dashboard!

Lab Exercise 4: DevOps Team

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

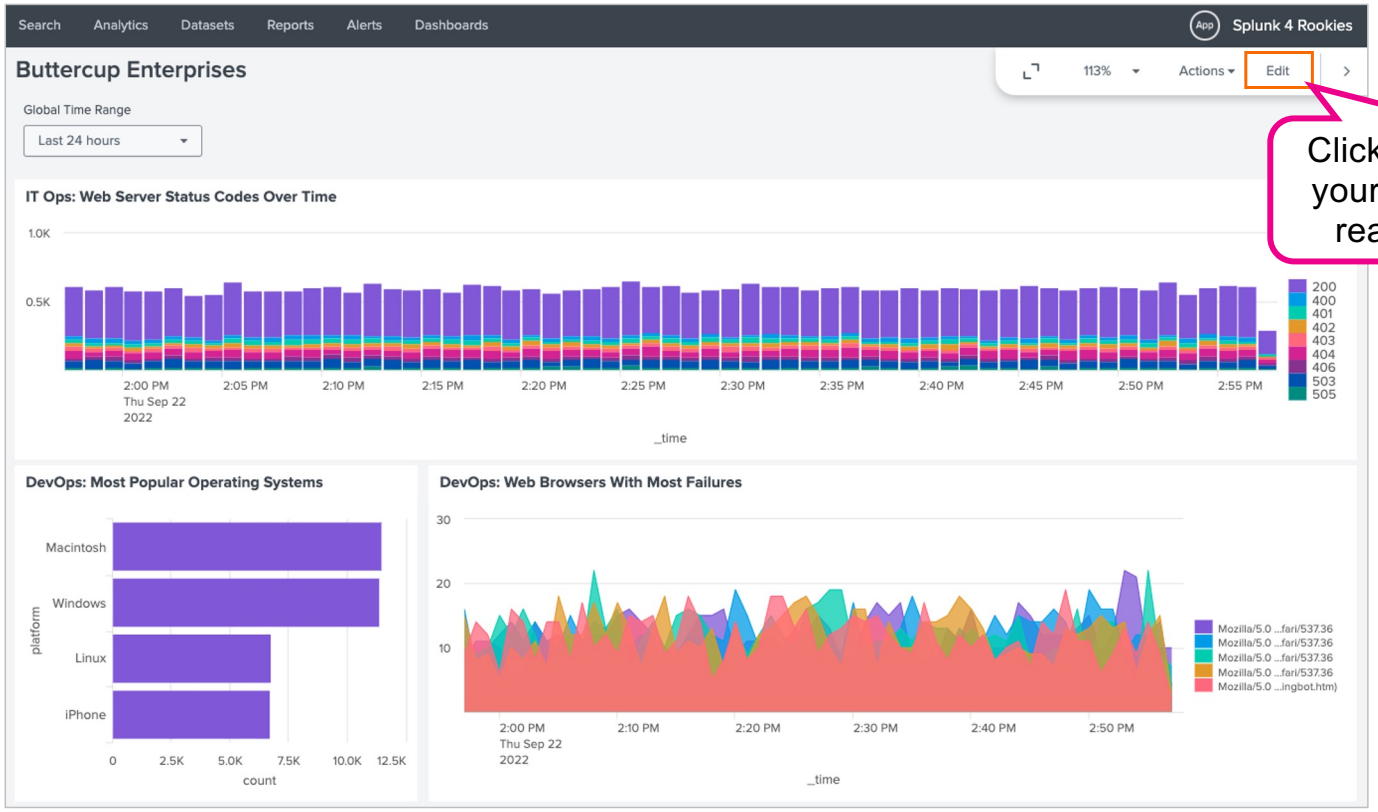
Solution:

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



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

Your Dashboard so far…



Click on '**Edit**' to edit your dashboard and rearrange panels

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

_time	200	400	401	402	403	404
2022-10-05 11:20:00	368	29	26	20	18	50
2022-10-05 11:21:00	374	23	19	25	33	57

Want to know more? Check out:

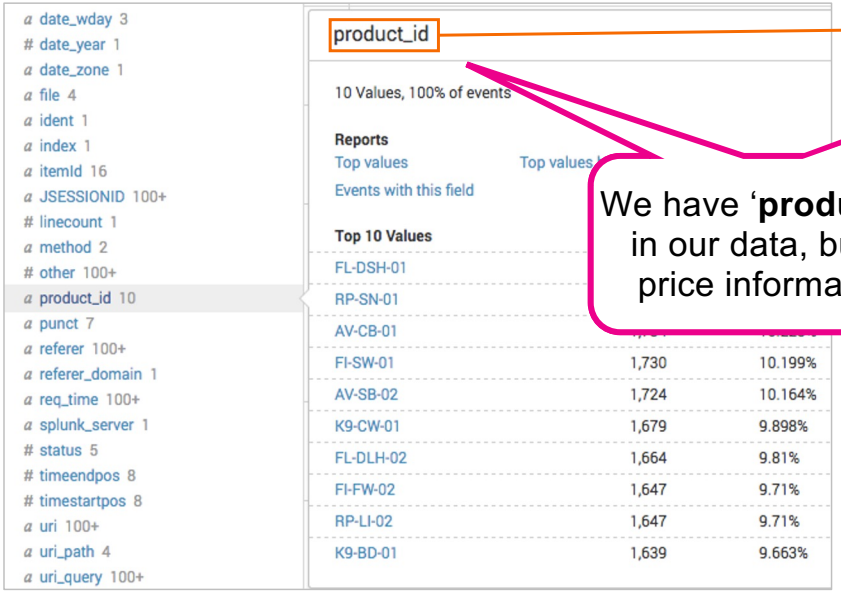
> Splunk Quick Reference Guide: https://splk.it/SplunkQuickRef

splunk> turn data into doing

Business Analytics Team:

Show lost revenue from the website

Fields extracted from events by Splunk:



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

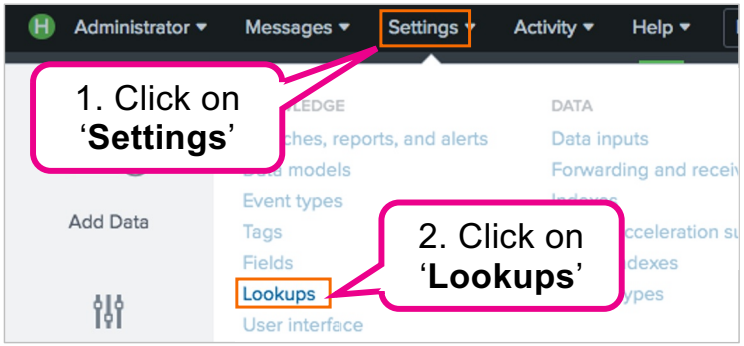
External CSV file:

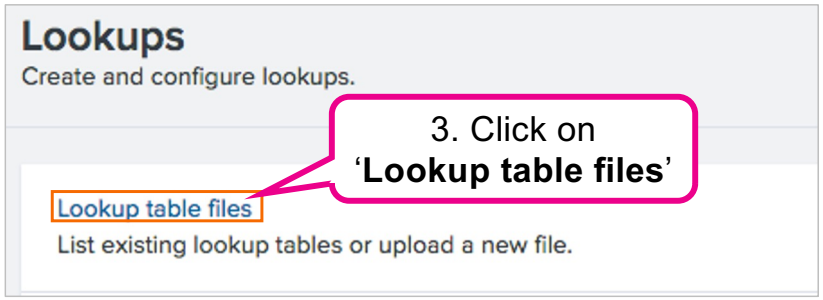
```
category,product_id,product_name,product_price
Clothing,BS-2,Batguy Slippers,25.7
Books,MCB-5,Mad Comics- Batguy,12
Books,MCB-6,Mad Comics- Bronze M
Books,MCF-3,Mad Comics- Flyman,1
Books,ZSG-2,Zombie Survival Guid
Clothing,CM-1,Costume- ManHawk,97.5
Gifts,DFS-2,Double Fudge Sundae,22.75
Gifts,PP-5,Pony Potpourri,9.99
Clothing,BW-3,Batguy Watch,9.99
Gifts,WPSS-2,Waterproof Scratch and Sniff,4.99
```

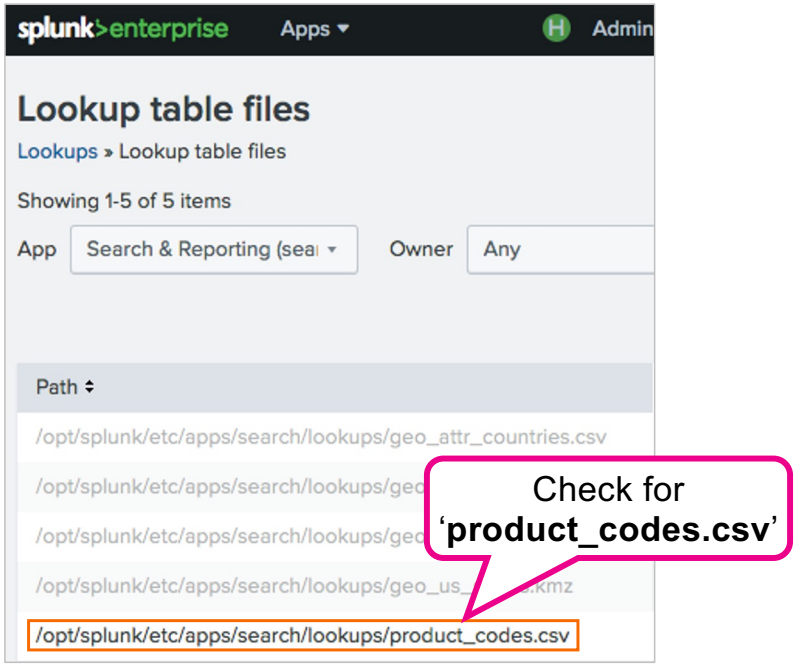
This is the information we need!

Verify That the Lookup File Exists

- A lookup file has already been uploaded for you!







Enriching Data with the `lookup` Command

Usage:

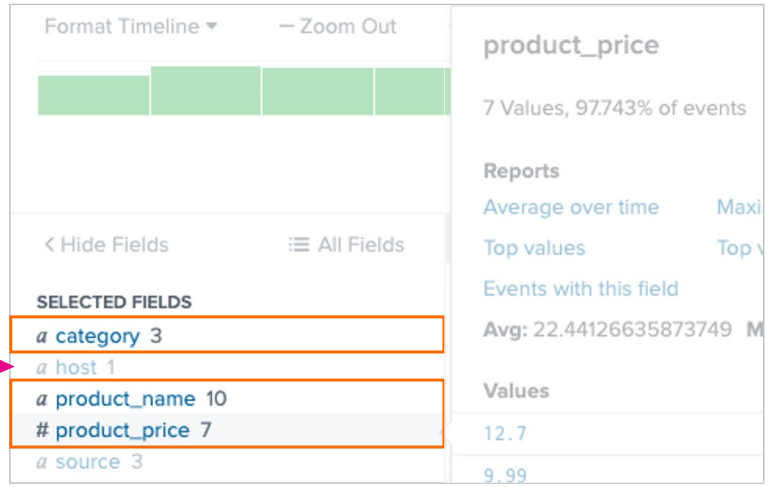
```
<your search> | lookup product_codes.csv product_id
```

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



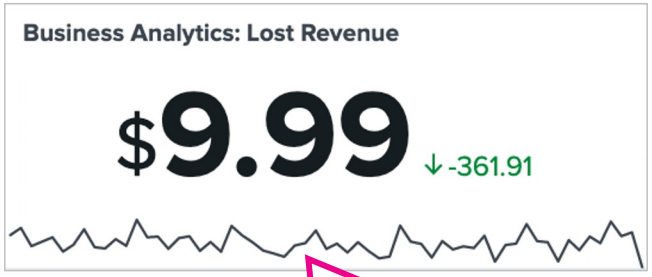
Lab Exercise 5: Business Analytics Team

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:



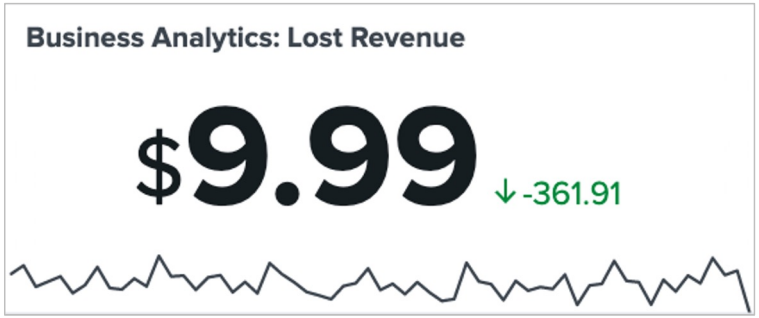
When you're happy with your visualisation, add it to your dashboard!

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:

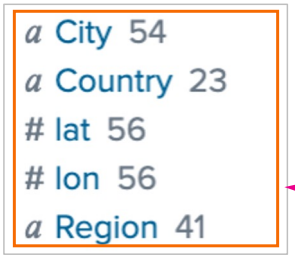
```
<your search> | iplocation clientip | geostats count by <field>
```

Split your results by a specific field for more detailed analysis

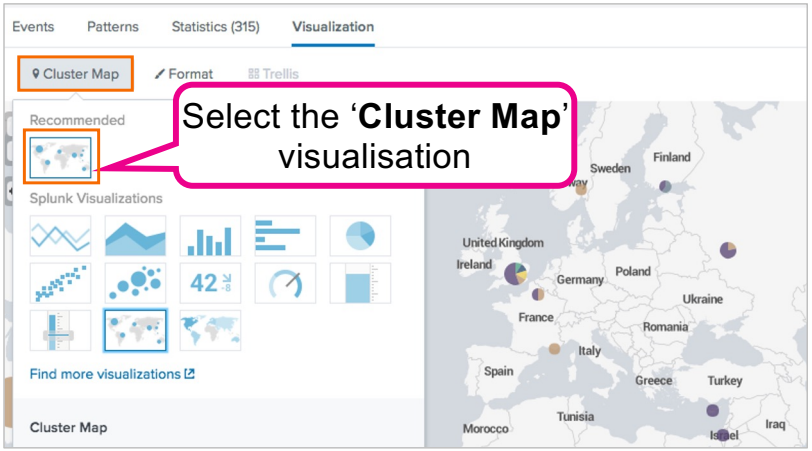
Enriches IP data on-the-fly with location data

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

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



The `iplocation` command produces additional fields containing geographic data



splunk> turn data into doing

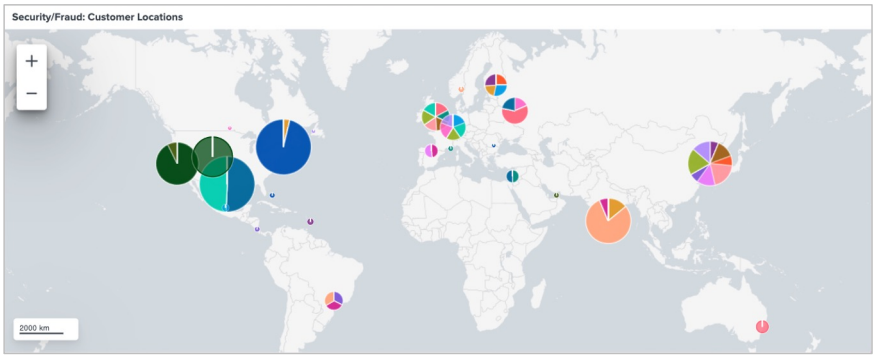
Lab Exercise 6: Security/Fraud Teams

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:

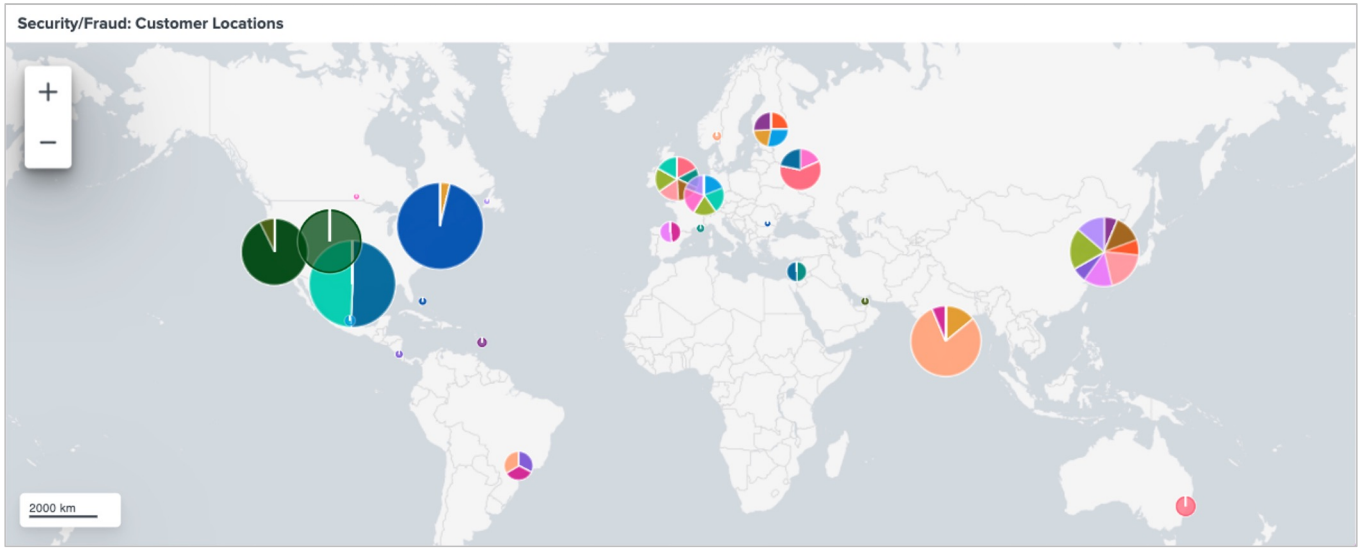


Lab Exercise 6: Security/Fraud Teams

Show website activity by geographic location

Solution:

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

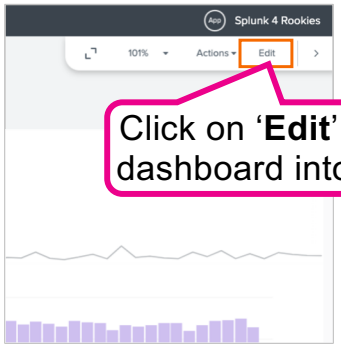


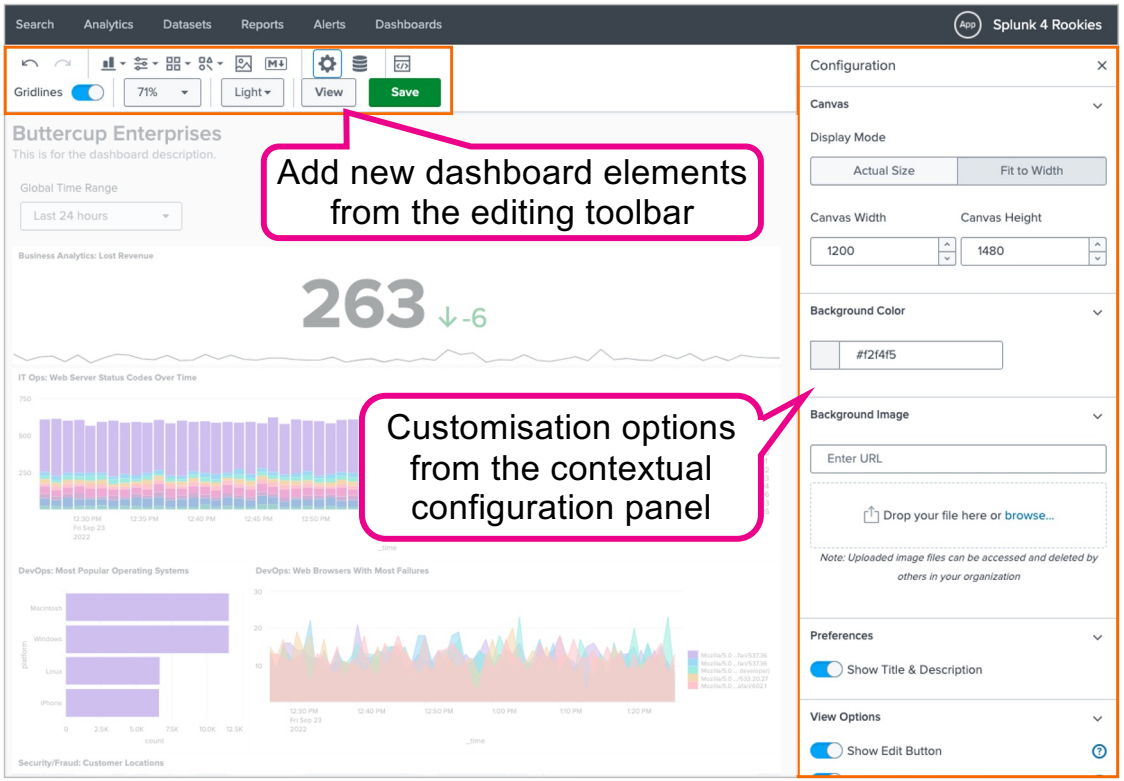
Create powerful, story-telling dashboards with Dashboard Studio

- ✓ 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





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

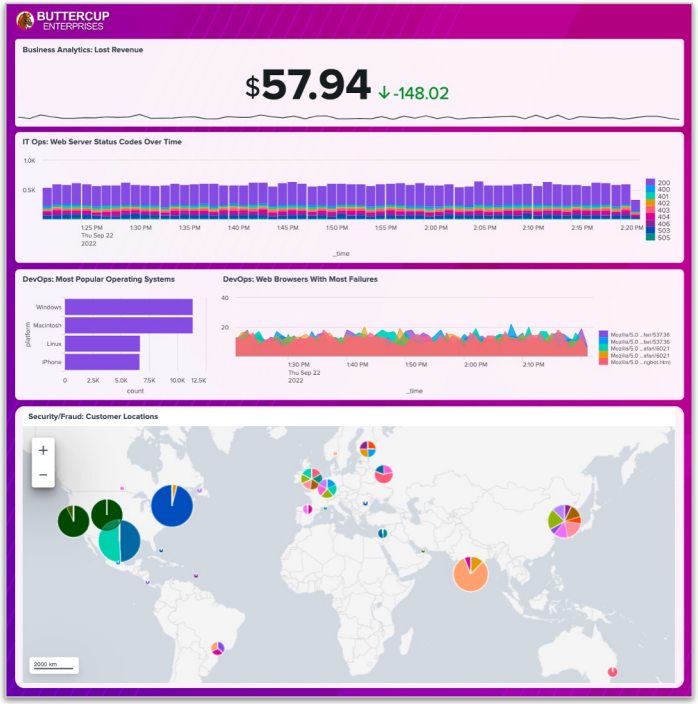
3. Link your dashboard panels to the global time picker

Goal:

You Finished the Hands-on Exercises!

How Did You Do?

Did you end up like this?...



Or this?

Splunk Resources

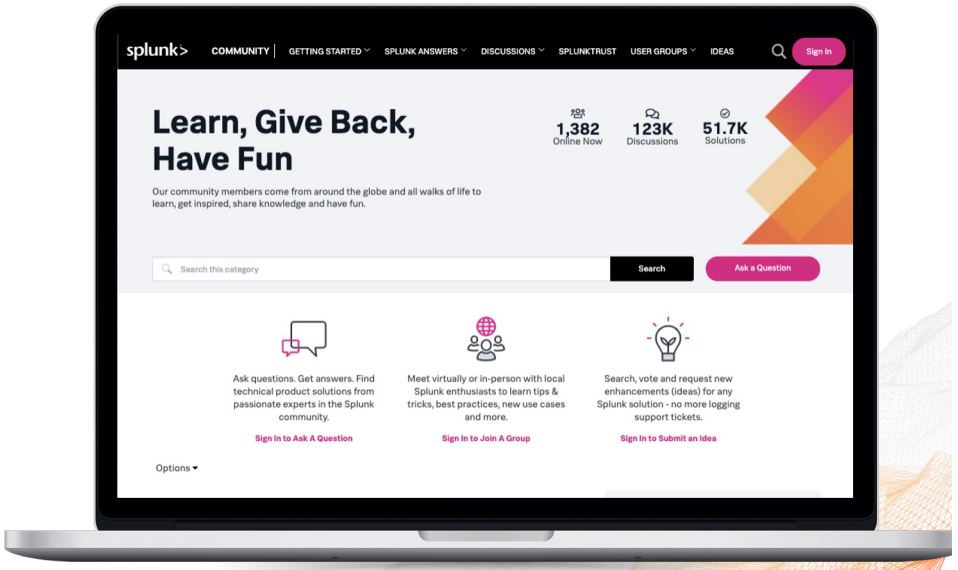
Where to go after today's workshop

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



230K+ community members worldwide

125K+ product questions and answers

150+ User Groups worldwide

splunk> turn data into doing

Splunk Events

https://events.splunk.com

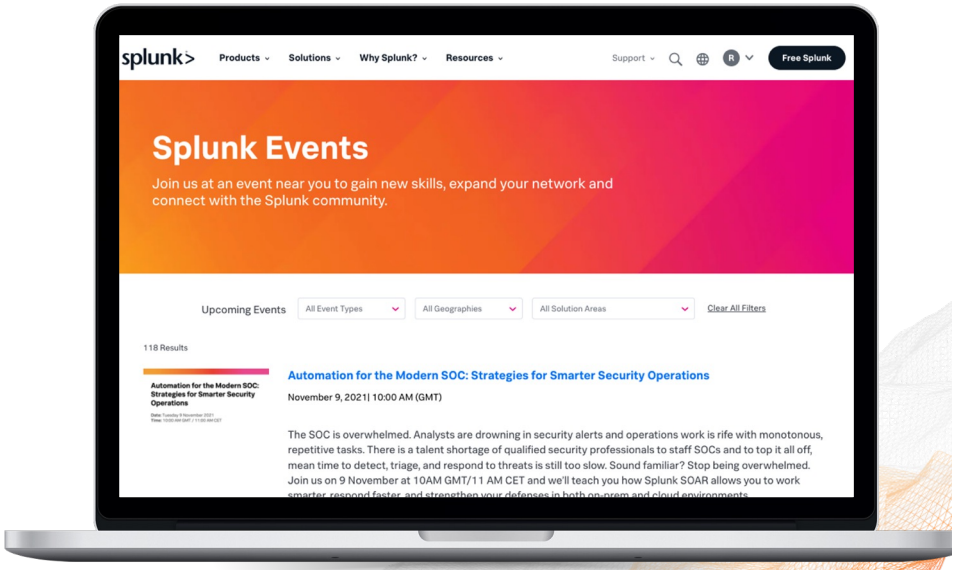
> Expand your network and connect with the global and local Splunk community

.conf

https://conf.splunk.com

> Join us at .conf23!

> Hundreds of on-demand sessions from product updates to learning new Splunk skills!

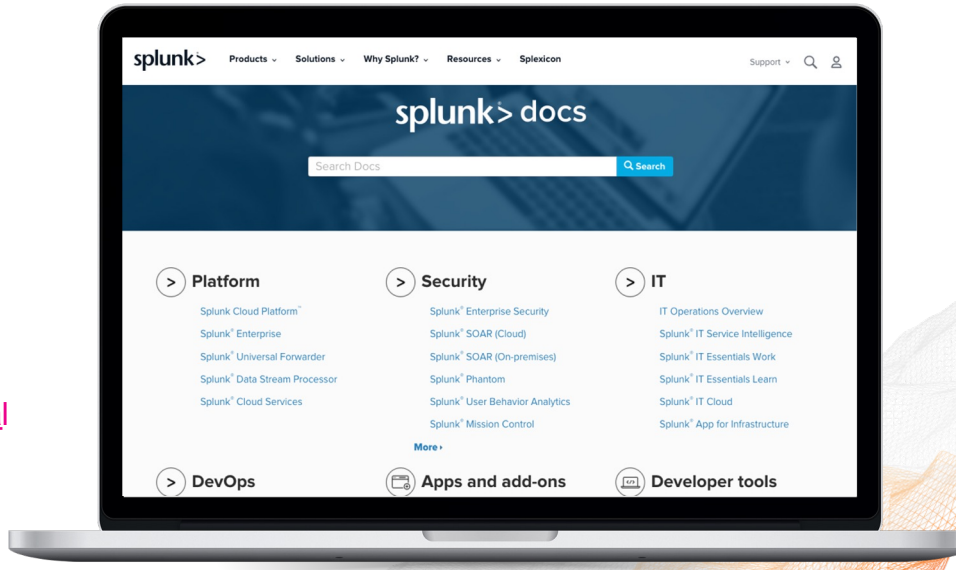


splunk> turn data into doing

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!

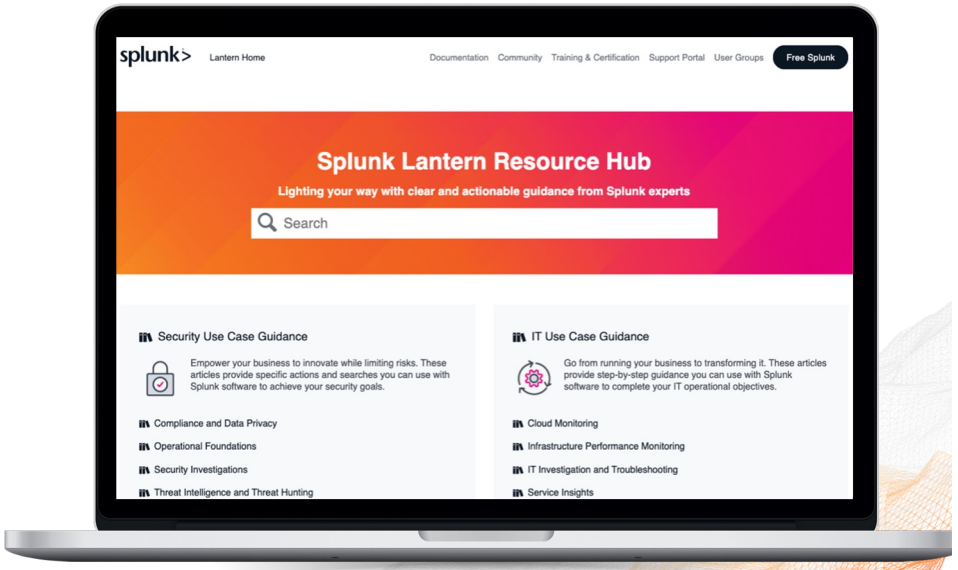


splunk> turn data into doing

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

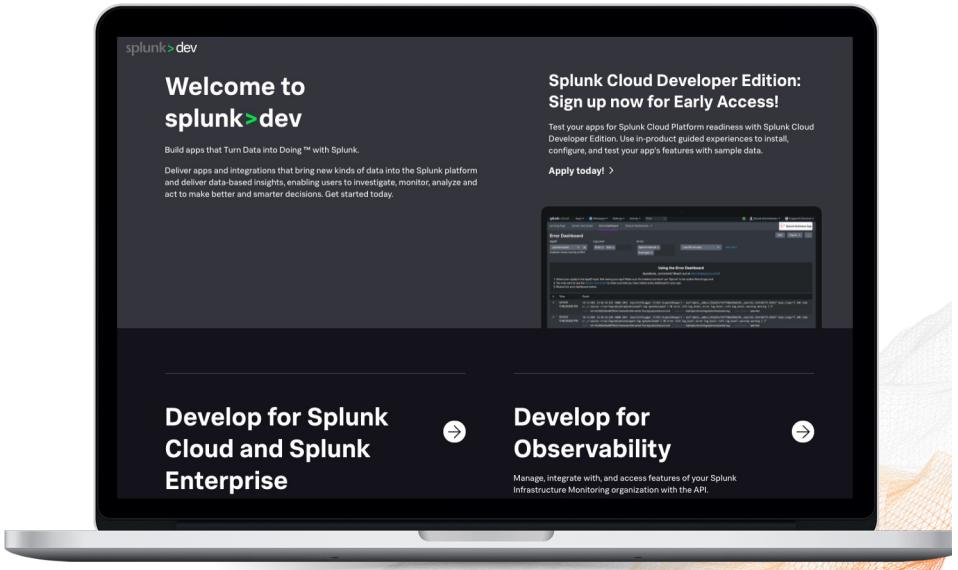


splunk> turn data into doing

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

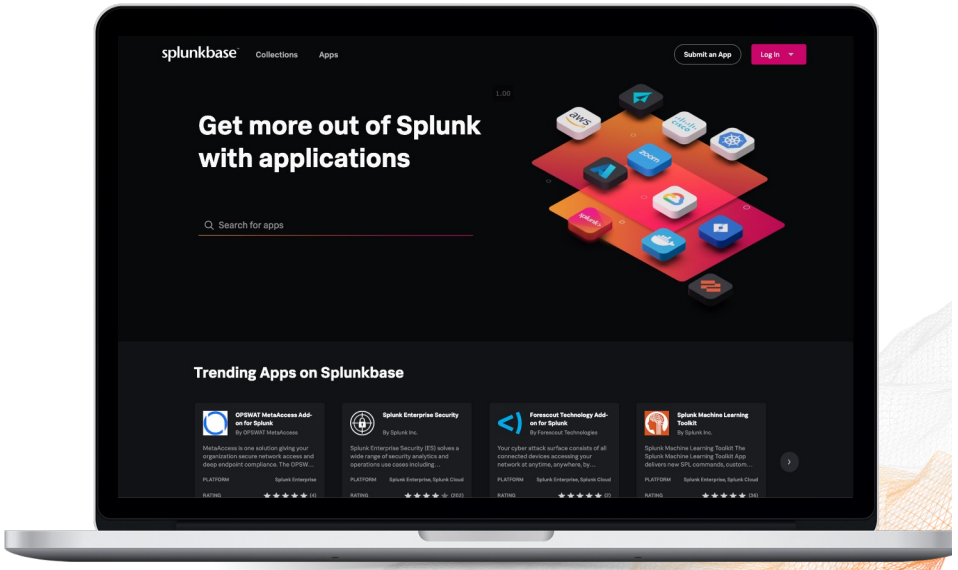


splunk> turn data into doing

Splunk Apps & Add-ons

https://splunkbase.splunk.com/

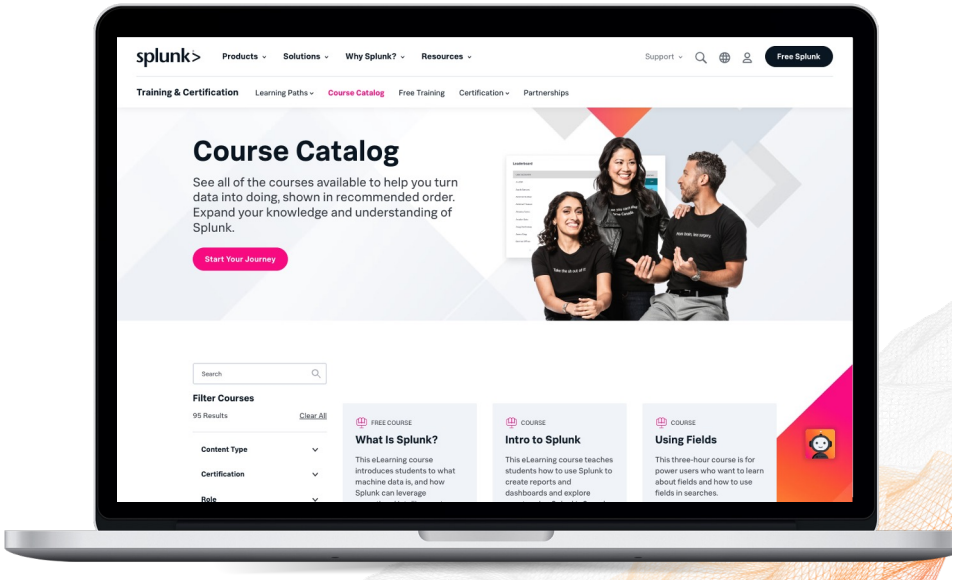
- 2800+ apps and add-ons
- Pre-built searches, reports, visualisations and integrations for specific use cases and technologies
- Download apps and customise them based on your requirements
- Fast time to value from your data
- Build and contribute your own apps!



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



splunk> turn data into doing

Thank You