

Splunk4Industry: Manufacturing

Hands-On Workshop

X #Splunk4Industry



splunk>

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.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, 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. 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, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

Splunk, Splunk> 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.
© 2024 Splunk Inc. All rights reserved.



Please introduce yourself!

- Name
- Company/organisation
- Role
- Are you currently using Splunk?
- What does monitoring in Manufacturing mean to you?



splunk>

Workshop Agenda

- Introduction to Splunk: Building digital resilience
- Splunk in the Manufacturing Industry
- Navigating Splunk, exploring data, building dashboards
- Exploring an IIoT use case
- Security in Operational Technology
- Business Service Intelligence

There's a lot to learning Splunk!

- Clustering
- Data Models
- Alerting
- Pivot
- SDKs
- APIs
- DB Connect

- Advanced Searches
- SOAR
- Machine Learning (ML)

- Splunk Stream
- Deployment Server
- Federated Search
- Metrics

- Custom Visualisations
- HTTP Event Collector (HEC)
- Data Filtering
- Transformations
- Architecture

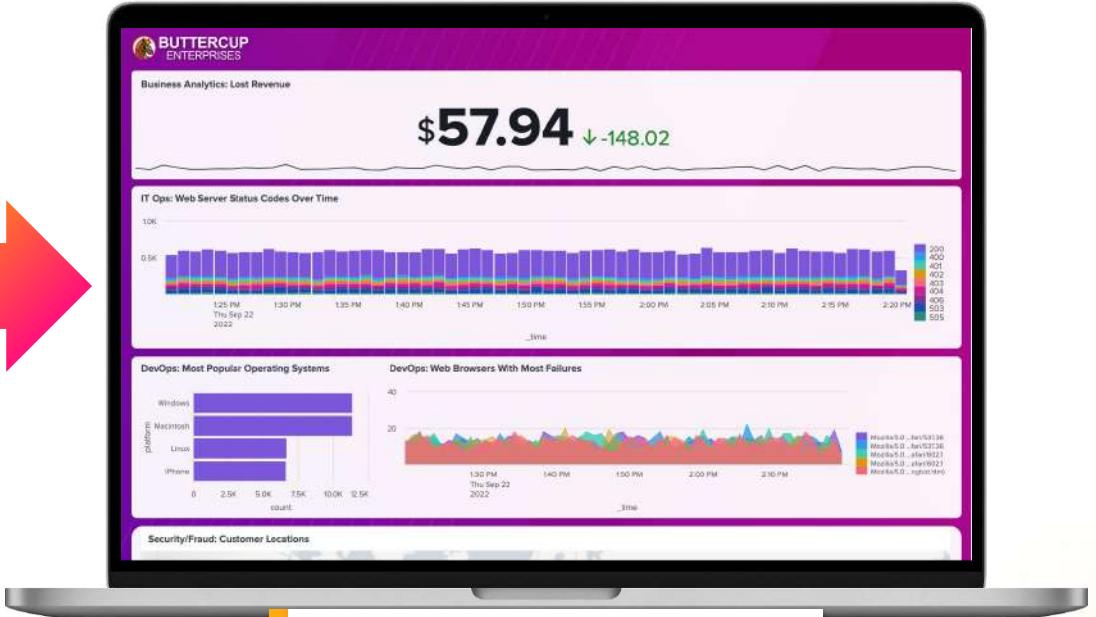
- Report Acceleration
- Common Information Model (CIM)
- Containers
- Best Practices
- And much more...

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

1st Objective for Today

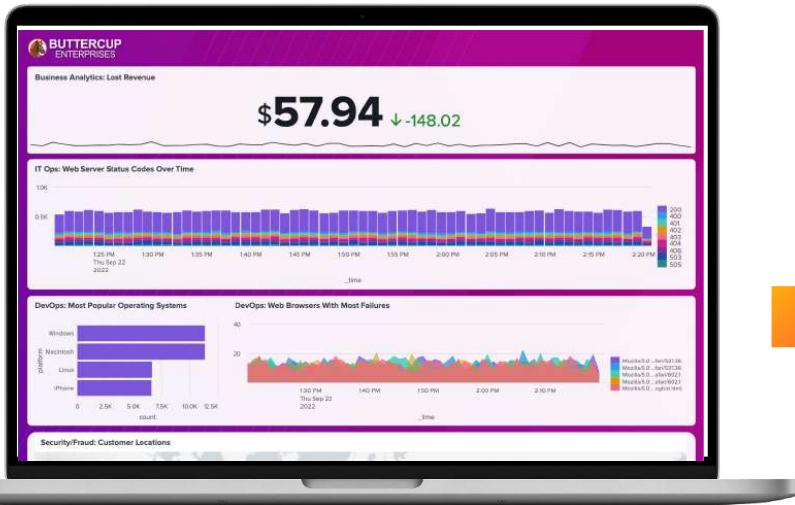


Go from messy machine data...



...to a dynamic, interactive dashboard!

2nd Objective for Today



Dynamic, interactive dashboard



...to Business Service Insights

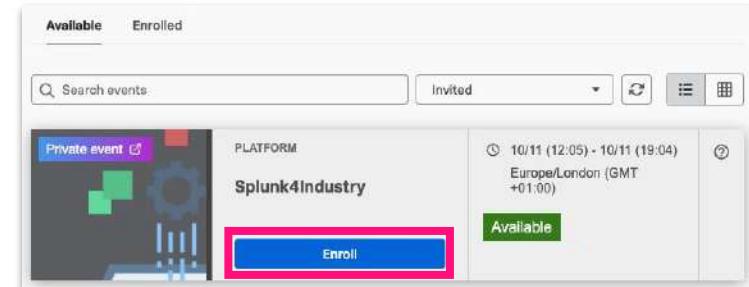


Enroll in Today's Workshop

Tasks

1. Get a splunk.com account if you don't have one yet:
<https://splk.it/SignUp>
2. Enroll in the Splunk Show workshop event:
<https://show.splunk.com/event/<eventID>>
3. Download the hands-on lab guide:
<https://splk.it/Manu-Lab-Guide>
Contains step-by-step instructions for all of today's exercises!
4. Download a copy of today's slide deck:
<https://splk.it/Manu-Attendee>

Goal



The screenshot shows a user interface for managing event enrollments. At the top, there are tabs for "Available" and "Enrolled". Below the tabs is a search bar labeled "Search events..." and a dropdown menu set to "Invited". The main area displays a card for an event titled "Private event". The card includes a small icon, the platform "Splunk4Industry", and the date and time "10/11 (12:05) - 10/11 (19:04) Europe/London (GMT +01:00)". To the right of the card, there is a green button labeled "Available" and a blue button labeled "Enroll", which is highlighted with a pink rectangle. A pink bar at the bottom right of the card contains the text "Enroll in today's event".

Enroll in today's event

What is Splunk?

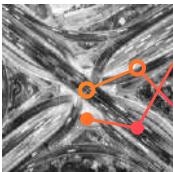


splunk>

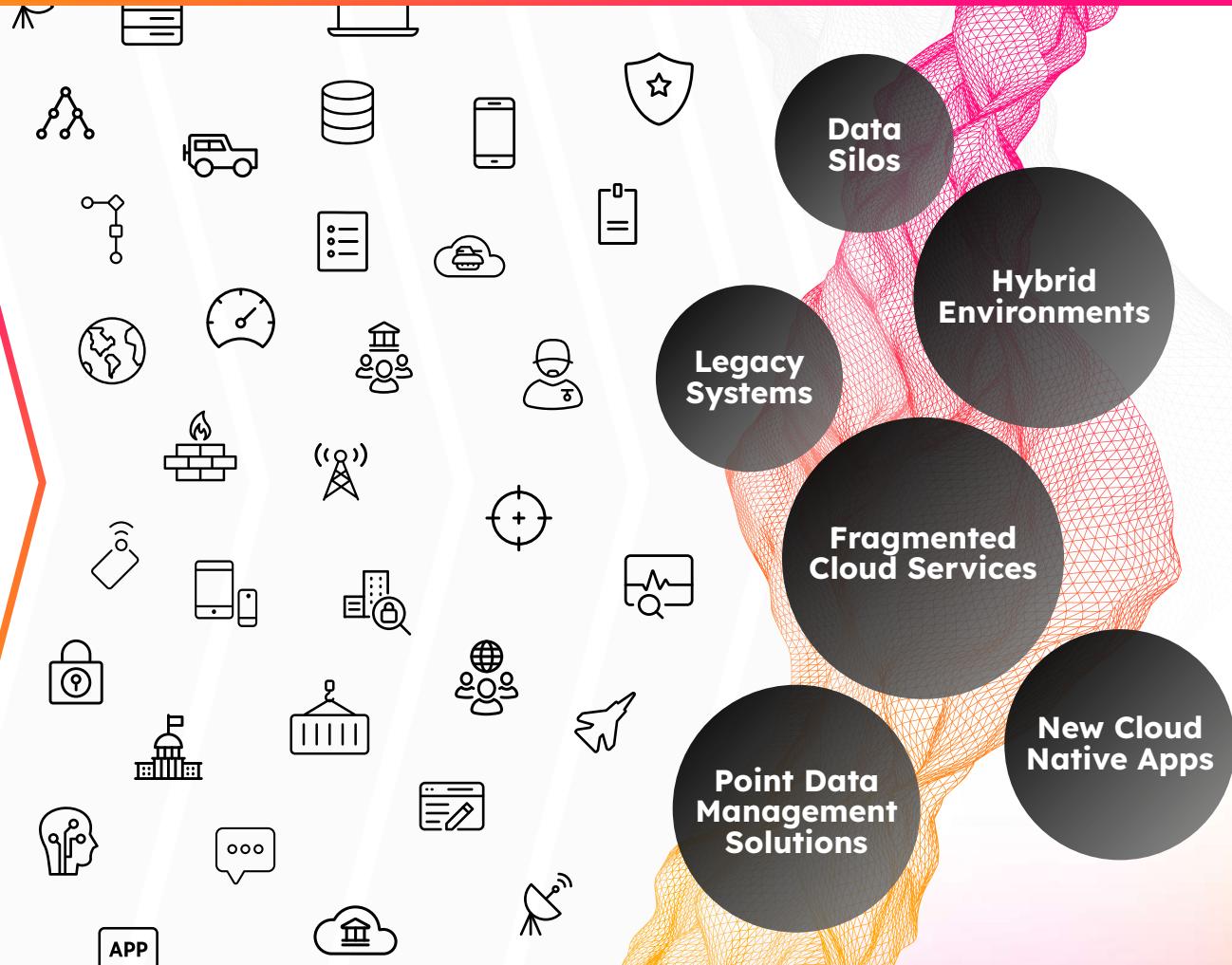


Data is your Competitive Advantage

Data isn't just a record.
Data makes things happen.
Splunk makes it possible.



Turning Real-time Data Into Action is Hard



The Power of Splunk

Delivering Unified Security and Observability

See

End-to-end visibility

No sampling or blind spots

Act

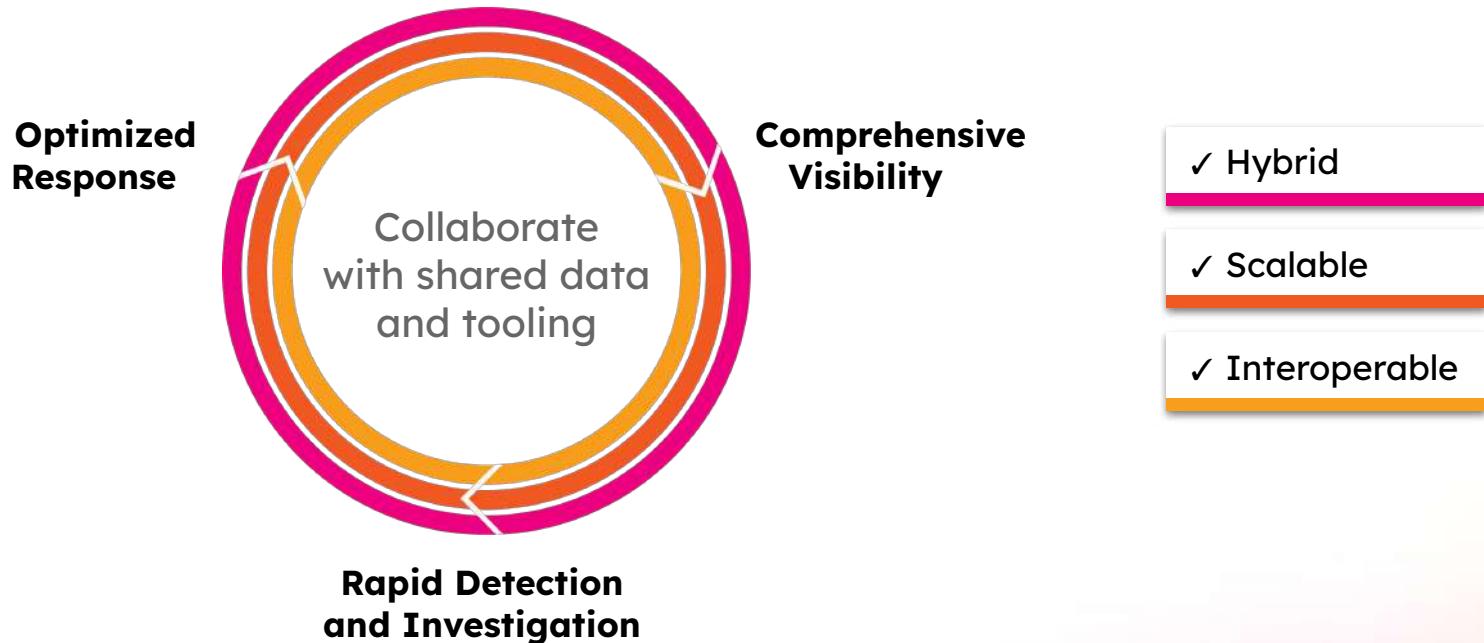
Investigate across massive data sets and take **action** fast

Extend

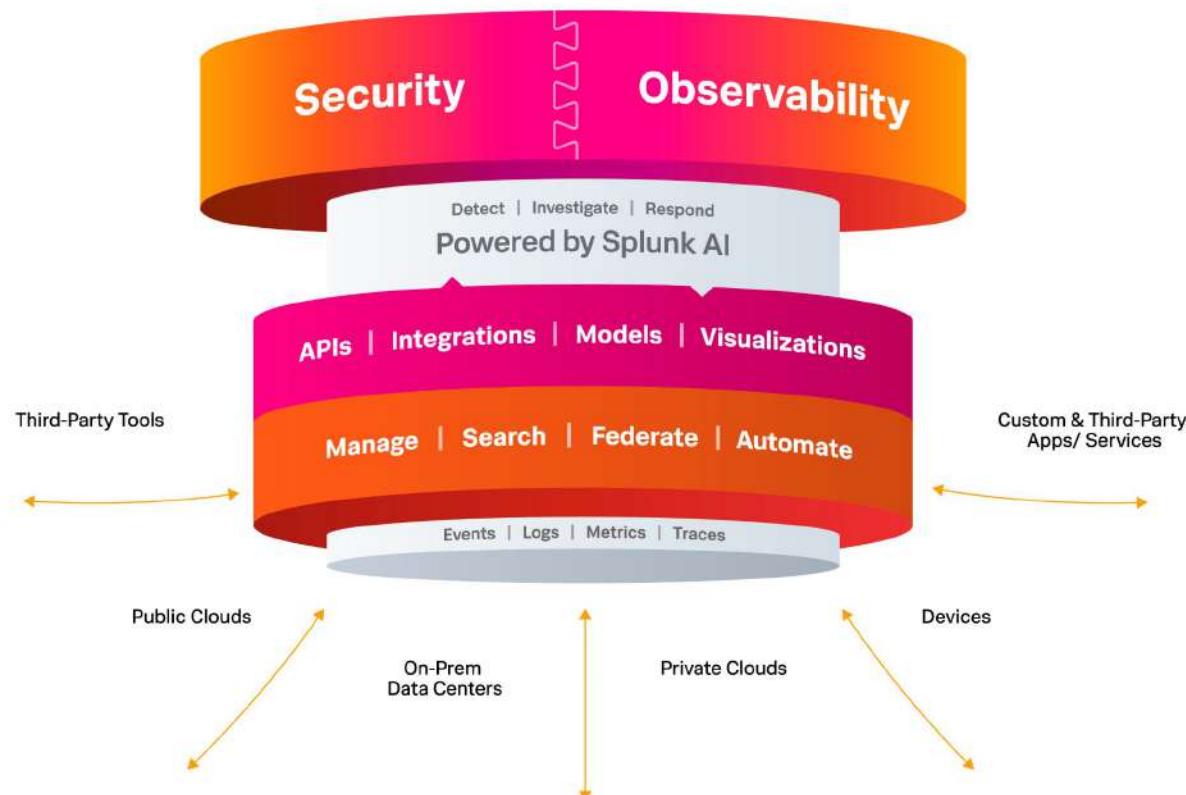
Extend the **platform** to use data to solve problems across the business



Splunk enables faster detection, investigation and response



The Unified Security and Observability Platform



Splunk as a Service

Fastest time to value | Minimum Infrastructure | Maximum Value

3 Simple Steps:

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



- **Fastest time to value**
- **Software as a service** - AWS or GCP
- **Secure** - ISO 27001, SOC 2 Type II, PCI DSS, HIPAA, FedRAMP Moderate, DoD IL5, IRAP
- **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



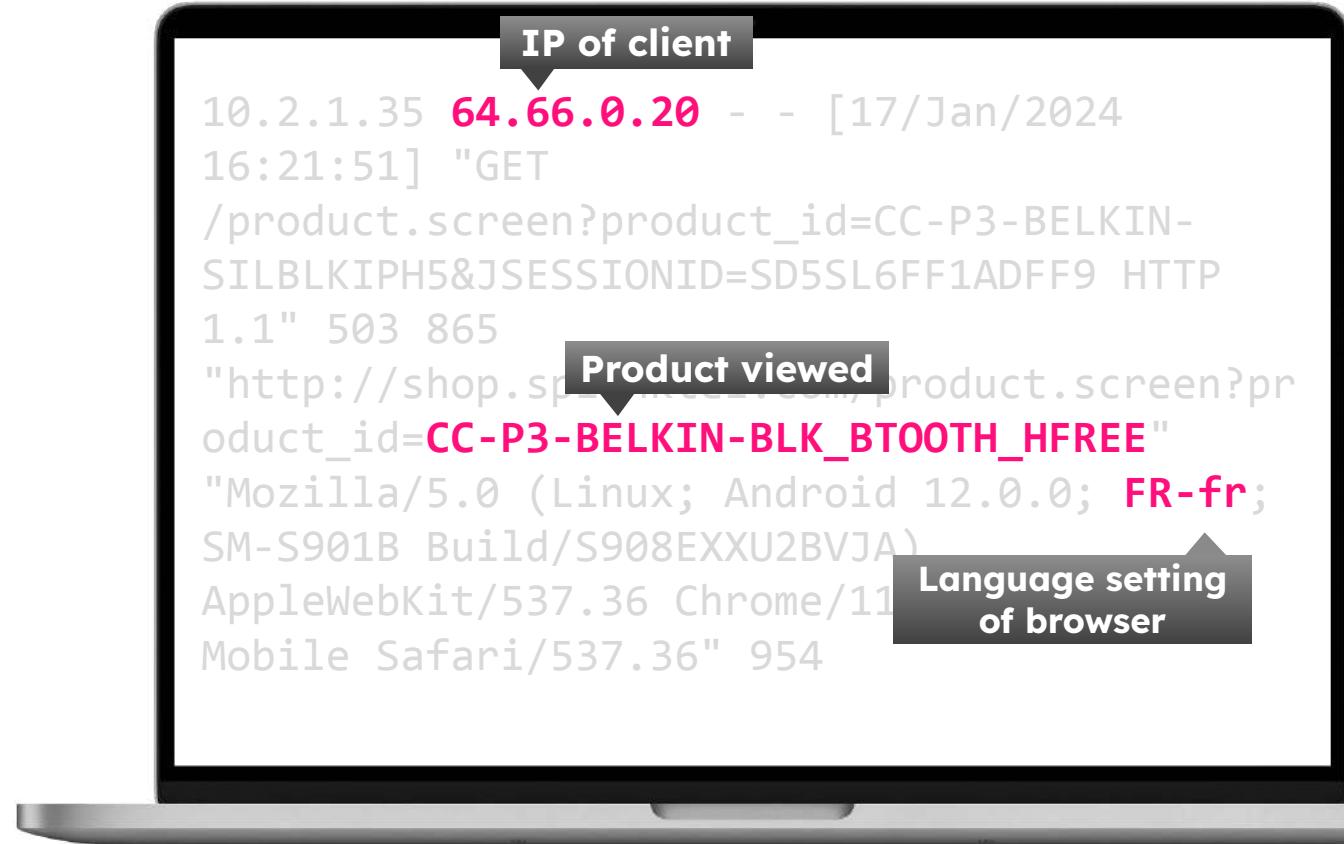
Splunk Cloud Service Description: <https://splk.it/SplunkCloudServDesc>

Machine data is valuable not complex!

```
10.2.1.35 64.66.0.20 - - [17/Jan/2024  
16:21:51] "GET  
/product.screen?product_id=CC-P3-BELKIN-  
SILBLKIPH5&JSESSIONID=SD5SL6FF1ADFF9 HTTP  
1.1" 503 865  
"http://shop.splunktel.com/product.screen?pr  
oduct_id=CC-P3-BELKIN-BLK_BT0OTH_HFREE"  
"Mozilla/5.0 (Linux; Android 12.0.0; FR-fr;  
SM-S901B Build/S908EXXU2BVJA)  
AppleWebKit/537.36 Chrome/114.0.5735.131  
Mobile Safari/537.36" 954
```

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?

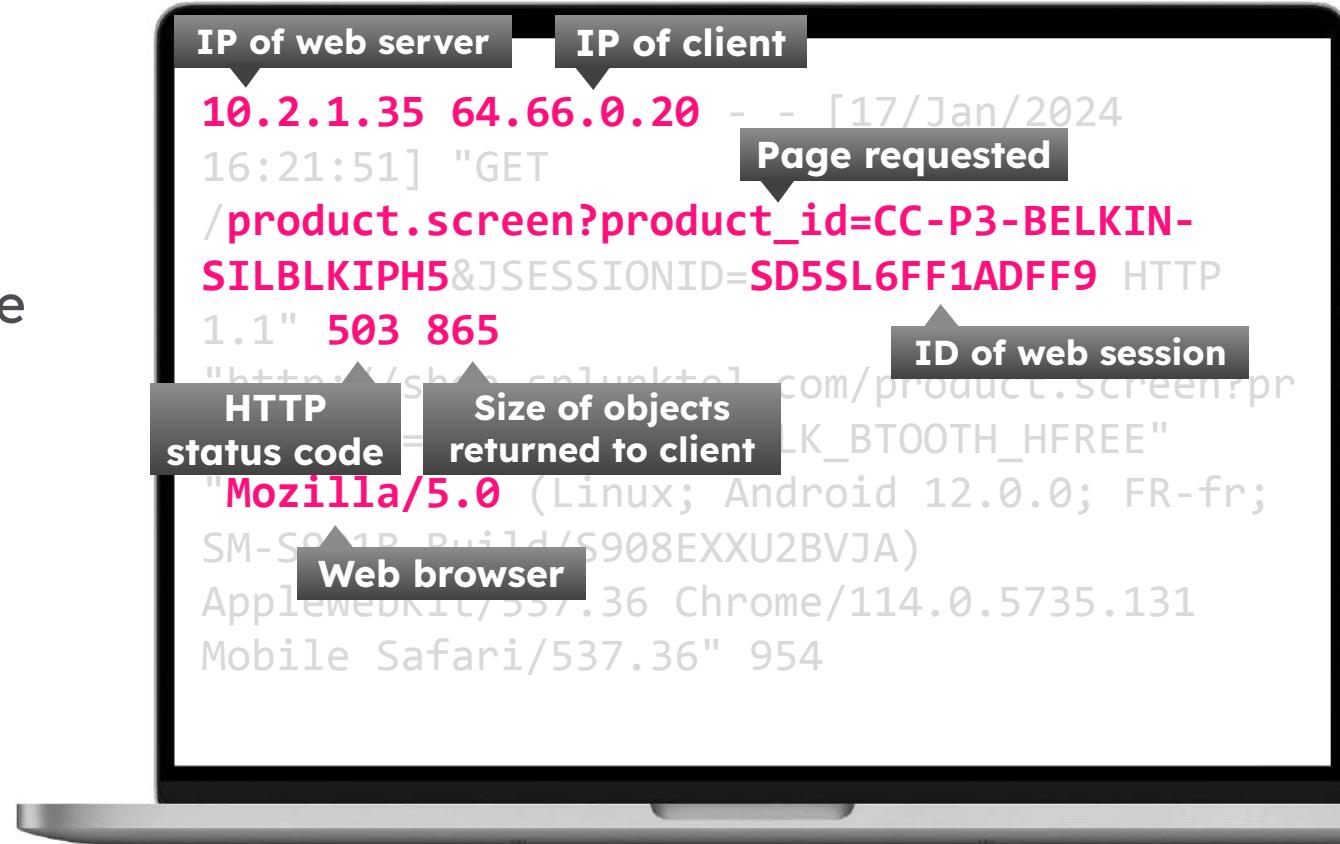
```
10.2.1.35 64.66.0.20 - - [17/Jan/2024  
16:21:51] "GET  
/product.screen?product_id=CC-P3-BELKIN-  
SILBLKIPH5&JSESSIONID=SD5SL6FF1ADFF9 HTTP  
1.1" 503 865  
"http://shop.splunktel.com/product.screen?pr  
oduct_id=CC-P3-BELKIN-BLK_<REDACTED>_HFREE"  
Mozilla/5.0 (Linux; Android 12.0.0; FR-fr;  
SM-S901B Build/S908EXXU2BVJA)  
AppleWebKit/537.36 Chrome/114.0.5735.131  
Mobile Safari/537.36 954
```

Platform

Handset model

IT Ops Use Case

Which web pages
are generating the
most errors?



Splunk in Manufacturing



splunk>

Industrial Data Contains Critical Insights

SOURCES



Alarms and Events

05/27/2014T10:24:17GMT applicationId="safetyObs" eventType="safety" assetID="CV1002384-1045" employeeId="114635" jobSite="PLEC-2014-GC" observationId="184568-451124-256" observation="Control Valve handle extracted to manual position. No lockout/tagout or other tag visible. Process is running." observationCriticality="5" imageId="PLEC-2014-GC-184568-451124-256" imageUri="https://mybucket.s3.amazonaws.com/PLEC-2014-GC-184568-451124-256.png"



Work Order

1543541, workorder, basic, 78544, pipefitting, CV1002384, "install manual bleed bypass", 04/13/2014, 05/21/2014, 25663, complete



Sensor Data

05/22/2014 03:17:31 Tag="CV1002384.ValvePos" Value="50" Quality="Good"
05/22/2014 03:17:46 Tag="CV1002384.ValveCmd" Value="100" Quality="Good"
05/22/2014 03:19:22 Tag="CV1002384.ValveCmd" Value="100" Quality="Good"
05/22/2014 03:19:27 Tag="CV1002384.ValvePos" Value="50" Quality="Bad"

Industrial Data Contains Critical Insights



SOURCES

Alarms and Events

Alarm Date

05/27/2014T10:24:17GMT applicationId="safetyObs" eventType="safety" assetID="CV1002384-1045" employeeId="114635" jobSite="PLEC-2014-GC" observationId="184568-451124-256" observation="Control Valve handle extracted to manual position. No lockout/tagout or other tag visible. Process is running." observationCriticality="5" imageId="PLEC-2014-GC-184568-451124-256" imageUri="https://mybucket.s3.amazonaws.com/PLEC-2014-GC-184568-451124-256.png"



Work Order

1543541, workorder, basic, 78544, pipefitting, CV1002384, "install manual bleed bypass", 04/13/2014, 05/21/2014, 25663, complete



Sensor Data

05/22/2014 03:17:31 Tag="CV1002384.ValvePos" Value="50" Quality="Good"

05/22/2014 03:17:46 Tag="CV1002384.ValveCmd" Value="100" Quality="Good"

05/22/2014 03:19:22 Tag="CV1002384.ValveCmd" Value="100" Quality="Good"

05/22/2014 03:19:27 Tag="CV1002384.ValvePos" Value="50" Quality="Bad"

Industrial Data Contains Critical Insights



SOURCES

Alarms and Events

Alarm Date

05/27/2014T10:24:17GMT applicationId="safetyObs" eventType="safety" assetID="CV1002384-1045" employeeId="114635" jobSite="PLEC-2014-GC" observationId="184568-451124-256" observation="Control Valve handle extracted to manual position. No lockout/tagout or other tag visible. Process is running." observationCriticality="5" imageId="PLEC-2014-GC-184568-451124-256" imageUri="https://mybucket.s3.amazonaws.com/PLEC-2014-GC-184568-451124-256.png"

Alarm Type

Asset ID



Work Order

Technician

Asset ID

Completed

1543541, workorder, basic, 78544, pipefitting, CV1002384, "install manual bleed bypass", 04/13/2014, 05/21/2014, 25663, complete



Sensor Data

05/22/2014 03:17:31 Tag="CV1002384.ValvePos" Value="50" Quality="Good"

05/22/2014 03:17:46 Tag="CV1002384.ValveCmd" Value="100" Quality="Good"

05/22/2014 03:19:22 Tag="CV1002384.ValveCmd" Value="100" Quality="Good"

05/22/2014 03:19:27 Tag="CV1002384.ValvePos" Value="50" Quality="Bad"

Industrial Data Contains Critical Insights



SOURCES

Alarms and Events

Alarm Date	Alarm Type	Asset ID
05/27/2014T10:24:17GMT applicationId="safetyObs" eventType="safety" assetID="CV1002384-1045" employeeId="114635" jobSite="PLEC-2014-GC" observationId="184568-451124-256" observation="Control Valve handle extracted to manual position. No lockout/tagout or other tag visible. Process is running." observationCriticality="5" imageId="PLEC-2014-GC-184568-451124-256" imageUri="https://mybucket.s3.amazonaws.com/PLEC-2014-GC-184568-451124-256.png"		



Work Order

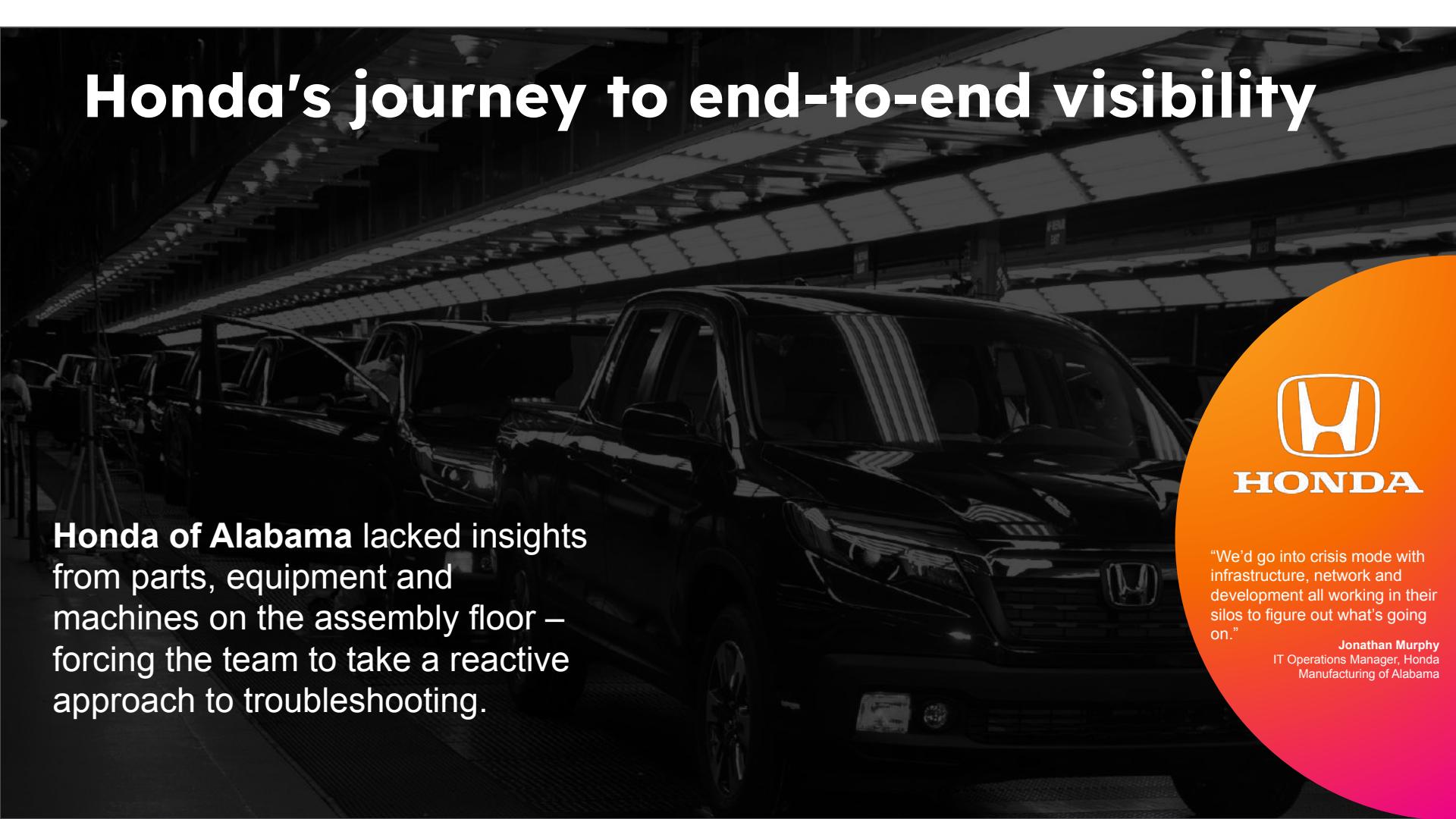
Technician	Asset ID	Completed
1543541, workorder, basic, 78544, pin fitting, CV1002384, "install manual bleed bypass", 04/13/2014, 05/21/2014, 25663, complete		



Sensor Data

MTBF	Asset ID	Quality
05/22/2014 03:17:31 Tag="CV1002384.ValvePos" Value="50" Quality="Good" 05/22/2014 03:17:46 Tag="CV1002384.ValveCmd" Value="100" Quality="Good" 05/22/2014 03:19:22 Tag="CV1002384.ValveCmd" Value="100" Quality="Good" 05/22/2014 03:19:27 Tag="CV1002384.ValvePos" Value="50" Quality="Bad"		

Honda's journey to end-to-end visibility



Honda of Alabama lacked insights from parts, equipment and machines on the assembly floor – forcing the team to take a reactive approach to troubleshooting.



HONDA

"We'd go into crisis mode with infrastructure, network and development all working in their silos to figure out what's going on."

Jonathan Murphy
IT Operations Manager, Honda
Manufacturing of Alabama

Honda drives production efficiencies with Splunk



“Splunk allows us to act on [our] data, providing insights, answering questions and solving problems we may not have even known we had.”

*– Charlie Studdard, Staff Engineer, IT Innovation Team,
Honda Manufacturing of Alabama*

Exceeded
environmental
standards

Increased
profitability and
efficiency

70%
faster mean time
to resolution

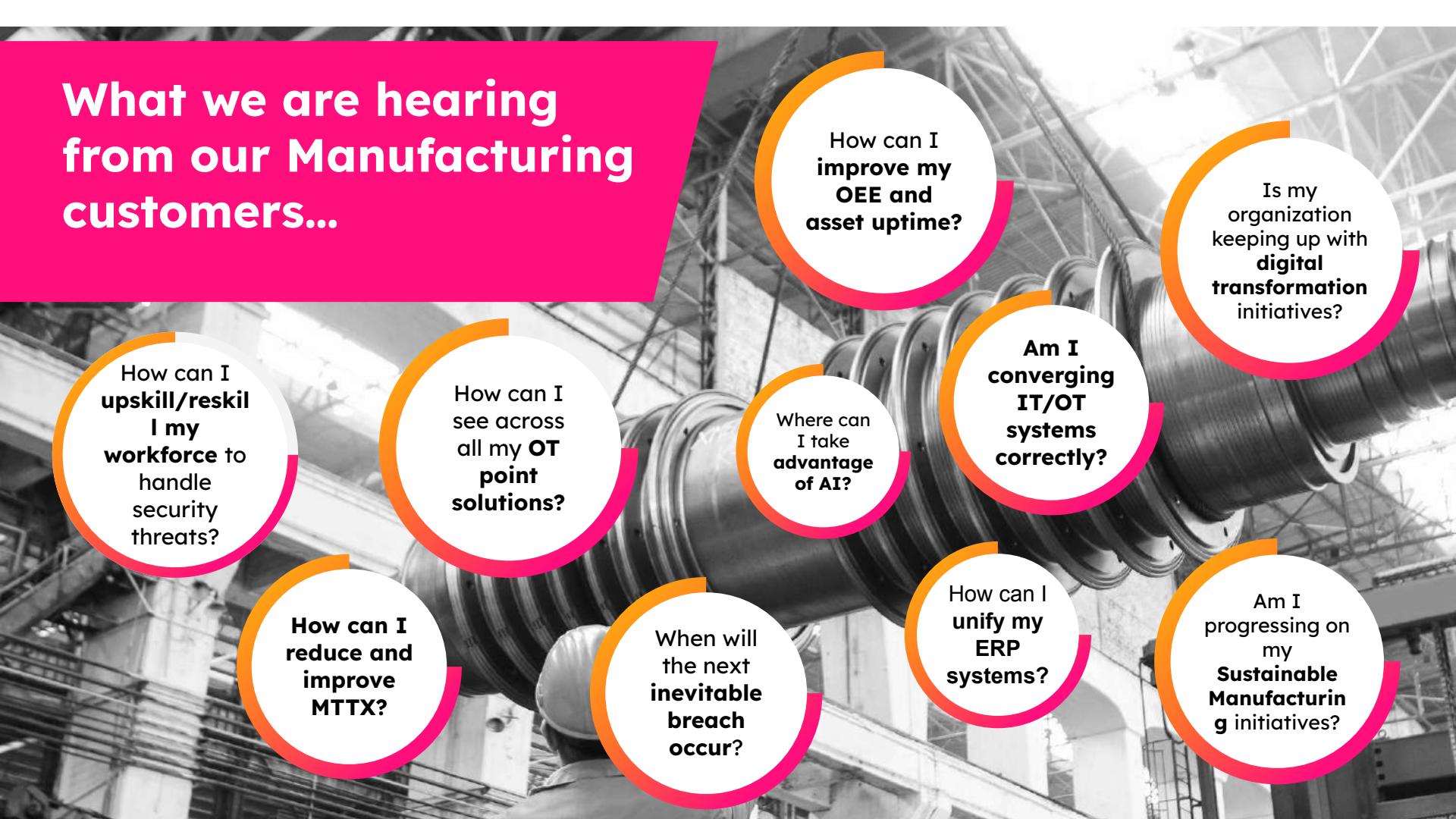


Your systems need to be secure and reliable



We help
the world's
leading
enterprises
become more
digitally resilient





What we are hearing from our Manufacturing customers...

How can I upskill/reskill my workforce to handle security threats?

How can I reduce and improve MTTX?

How can I see across all my OT point solutions?

When will the next inevitable breach occur?

How can I improve my OEE and asset uptime?

Where can I take advantage of AI?

Am I converging IT/OT systems correctly?

How can I unify my ERP systems?

Is my organization keeping up with digital transformation initiatives?

Am I progressing on my Sustainable Manufacturing initiatives?

It's especially hard for manufacturing organizations to be resilient today



Complex cybersecurity threats



Digital disruptions that impact IT systems



Siloed processes, tools, and expertise



Pressure to digitally transform



Build digital resilience with Splunk

Edge to Enterprise Visibility at Your Fingertips

Detect, investigate and respond faster to IT/OT Cybersecurity threats

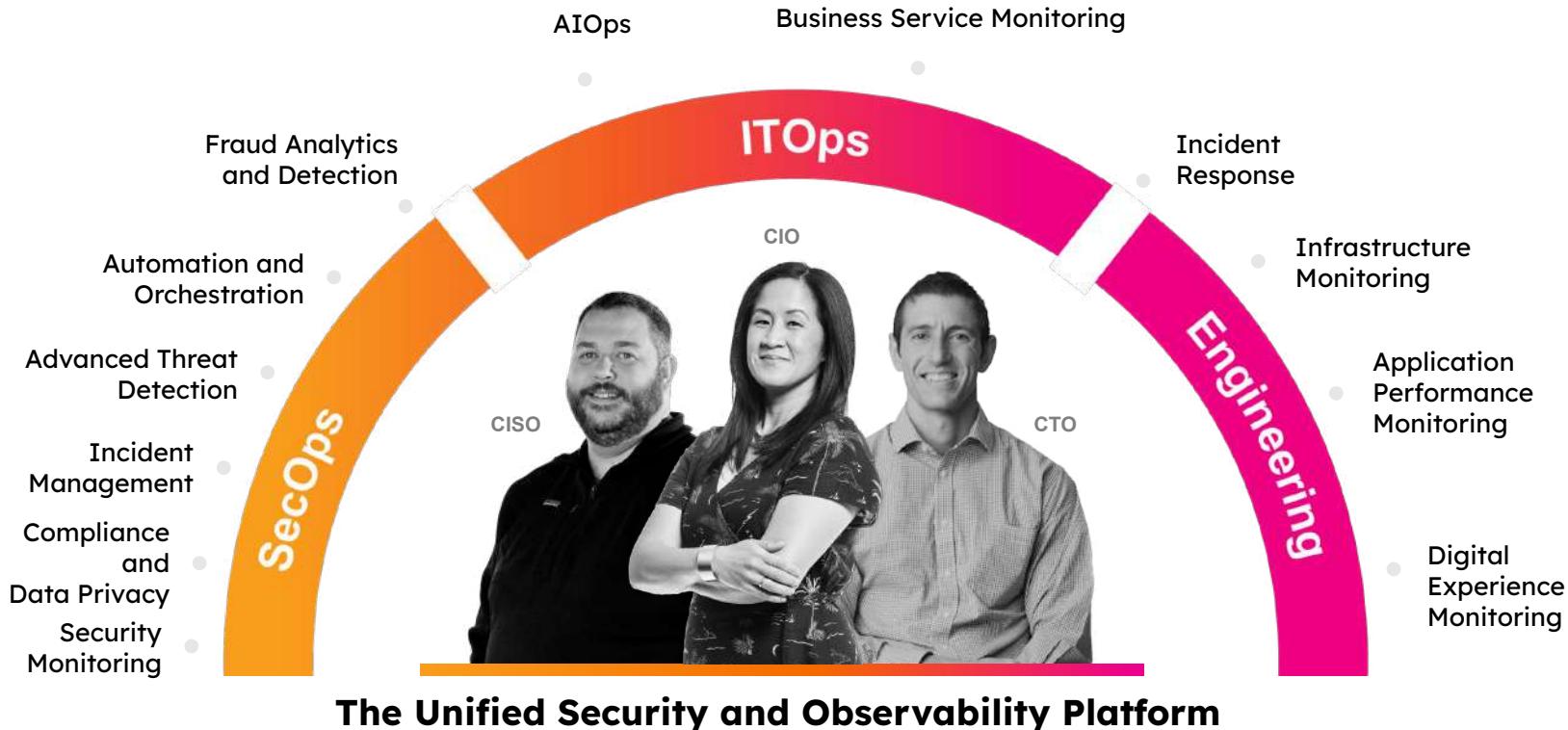
Keep operational systems up and running with **end-to-end business, process and service monitoring**



Improve data centric computing and integration of IT/OT systems

Transform operations from reactive to proactive and adapt to new opportunities

Bringing SecOps, ITOps and Engineering together for greater digital resilience



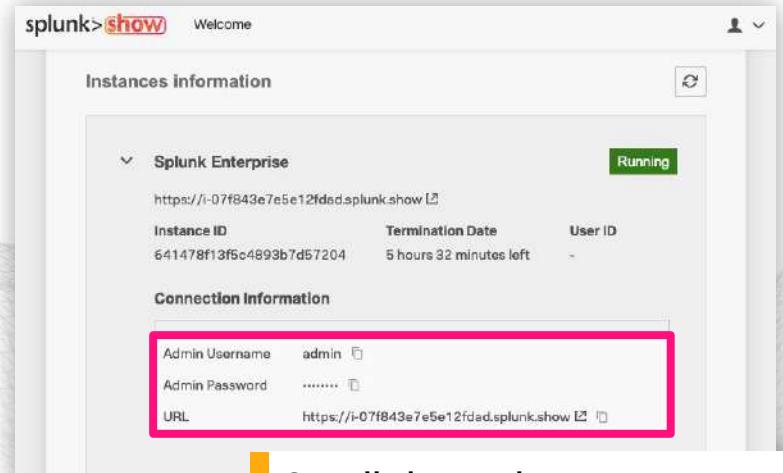
Let's get started

splunk>



Login to Splunk

Locate your instance URL and credentials
in the Splunk Show event
<https://show.splunk.com>



The screenshot shows the Splunk Show interface with the following details:

- Instances information:** Splunk Enterprise is listed as "Running".
- Connection Information:** Admin Username: admin, Admin Password: [redacted], URL: <https://i-07f843e7e5e12fded.splunk.show>.

Scroll down the event page
and expand the **Splunk Enterprise** section to view
your login details

Log in to your Splunk instance



The screenshot shows a web browser displaying a Splunk instance's login page with the following elements:

- Header: splunk>enterprise
- Form fields: Username, Password, Sign In button.

Login using the credentials
from Splunk Show

Apps and Add-ons

- 3100+ free apps and add-ons available from <https://splunkbase.splunk.com/>
- 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

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**





Create an App and Add Some Data

Tasks

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

Select source

- var
- backups
- cache
- crash
- lib
- local
- lock
- log
- apt
- audit
- dist-upgrade
- fsck
- landscape
- squid3
- unattended-upgrades
- upstart
- weblogs
- alternatives.list

Reminder
Download the [lab guide](#) for step-by-step instructions!

Open your app and have a play!

The screenshot shows the Splunk Enterprise search interface. At the top, it says "splunk>enterprise" and "App: Splunk 4 Rookies". Below that is a navigation bar with "Search", "Datasets", "Reports", "Alerts", and "Dashboards". A callout points to the "App: Splunk 4 Rookies" dropdown with the text "The currently selected app". To the right of the search bar is a "Time picker - choose your search time range" with a dropdown set to "Last 60 minutes". The main area shows a "New Search" for "action=purchase status=200" which found "261 events (15/05/2018 07:49:00.000 to 15/05/2018 08:49:00.000)". Below the search bar are tabs for "Events (261)", "Patterns", "Statistics", and "Visualization". The "Events" tab is selected. It includes "Format Timeline" and zoom controls. The main view is an "Event histogram" with green bars representing event counts over time. Below the histogram is a table with columns "Time" and "Event". The table shows several log entries. A callout points to the first entry with "Event timestamp". Another callout points to the raw log data with "Raw event data". On the left side of the table, there's a sidebar with "source 1", "sourcetype 1", and a section titled "INTERESTING FIELDS" listing fields like "action", "category_id", "clientip", etc. A callout points to this sidebar with "Metadata fields extracted at search time".

The currently selected app

Time picker - choose your search time range

Search bar - type anything here to search

Event histogram

Event timestamp

Raw event data

Metadata fields extracted at search time

Time	Event
15/05/2018 08:49:08.127	12.138.60.5 - [15/May/2018 08:49:08:127] "GET /cart.do?action=purchase&itemId=EST-20&product_id=RP-SN-81&JSESSIONID=SD1SL2FF10 flowershop.com/category.screen?category_id=GIFTS" "Googlebot/2.1 (http://www.googlebot.com/bot.html)" 873 host = ip-172-31-31-62 source = /var/log/weblogs/noise_apache_1.log sourcetype = access_combined
15/05/2018 08:48:54.193	12.138.60.4 - [15/May/2018 08:48:54:193] "POST /product.screen?product_id=FL-DLH-02&JSESSIONID=SD7SL2FF3ADFF8 HTTP/1.1" 200 629 "http://www.myflowershop.com/cart.do? action=purchase&itemId=EST-20&product_id=FL-DLH-02" "Googlebot/2.1 (http://www.googlebot.com/bot.html)" 256 host = ip-172-31-31-62 source = /var/log/weblogs/noise_apache_1.log sourcetype = access_combined
15/05/2018 08:48:46.196	203.92.58.136 - [15/May/2018 08:48:46:196] "GET /cart.do?action=purchase&itemId=EST-15&product_id=K9-BD-01&JSESSIONID=SD1SL10FF1ADFF7 HTTP/1.1" 200 3831 "http://www. myflowershop.com/category.screen?category_id=BOUQUETS" "Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.6.3; en-US) AppleWebKit/533.4 (KHTML, like Gecko) Chrome/5.0.375.3 Safari/533.4" 897 s/noise_apache_1.log sourcetype = access_combined

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 ensure accurate search 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

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

Pipe character: Output of left is input to right

e.g. index=main action=purchase

#	Time	Event
>	16/01/2024 11:03:08.000	27.182.8.8 - - [16/Jan/2024:11:03:08:11] "GET /cart.do?action=viewProduct..;id=MCD-5A75E557B0D-S263LBFF1640F3 HTTP/1.1" 200 3435 "http://www.buttercupenterprises.com/product.screen?product_id=95F2*7*90211a/5.0 (Linux; Android 12.0; 0; API level 31; Build/AS400XXIA973) AppleWebKit/537.36 Chrome/114.0.5735.81 Mobile Safari/1537.36 (compatible; Googlebot/2.1; http://www.google.com/bot.html)" 388 host: Domane-Demo source: /var/log/weblogs/noise_apache.log/7 sourcetype = access_combined
>	16/01/2024 11:03:08.000	131.178.231.243 -- [16/Jan/2024:11:03:08:11] "POST /product.screen?uid=5ac95574-aeb7-417e-ae38-df11f63d2788&product_id=99-5A75E553D0D1D01SL4FF9ADP76 HTTP/1.1" 200 2311 "http://www.buttercupenterprises.com/product.screen?product_id=PP-5" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_4) AppleWebKit/537.36 Chrome/107.0.5304.122 Safari/1537.30" 703 host: Domane-Demo source: /var/log/weblogs/noise_apache.log/7 sourcetype = access_combined
>	16/01/2024 11:03:08.000	12.118.68.4 - - [16/Jan/2024:11:03:08:11] "GET /product.screen?uid=a81e7945-ef09-4a55-94c1-888f06e804&product_id=0-0-3473E553D0D1D01SL4FF9ADP76 HTTP/1.1" 404 3158 "http://www.buttercupenterprises.com/product.screen?product_id=99-2" "Mozilla/5.0 (iPhone; CPU iPhone OS 19_0 like Mac OS X) AppleWebKit/60K17865.15 Version/19.0 Mobile/19A346 Safari/602.1" 682 host: Domane-Demo source: /var/log/weblogs/noise_apache.log/7 sourcetype = access_combined
>	16/01/2024 11:03:08.000	12.118.68.5 - - [16/Jan/2024:11:03:08:11] "GET /product.screen?uid=8499ff2-2e4f-44ab-af74-8988cb12b8&product_id=98-5A75E553D0D1D01SL4FF9ADP76 HTTP/1.1" 505 1316 "http://www.buttercupenterprises.com/product.screen?product_id=99-1" "Mozilla/5.0 (Windows; Win32) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.82 Safari/1537.36" 877 host: Domane-Demo source: /var/log/weblogs/noise_apache.log/7 sourcetype = access_combined

Functions

```
| 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 1st Scenario

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 and Fraud**



**BUTTERCUP
ENTERPRISES**

What Does the Business Want to See?

We Need to Create a Dashboard With Two 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



Buttercup Enterprises: Add all of this to a single dashboard with a custom background image



This is the dashboard we're aiming for!



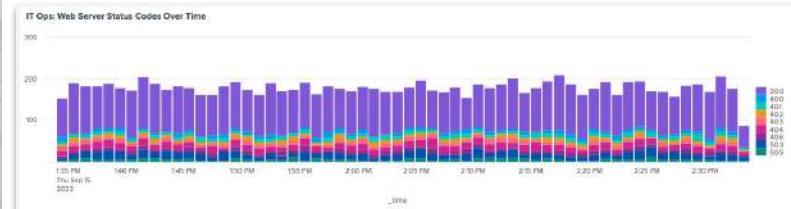
IT Operations Team

Investigate Successful Versus 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



Splunk Dashboards

Classic Dashboards (Simple XML)



- Easy to deploy a **wide variety of visualisations**, but **hard to craft a story**
- **Flexible and extensible**, but **time consuming** to build something truly beautiful (e.g. custom JS, CSS)
- **PDF export loses look/feel** of dashboard

Dashboard Studio



- Create **powerful, story-telling dashboards** with **advanced visualisation tools**
- **Streamlined editing experience** with **flexible layouts**
- Support for **images, text boxes, shapes, lines and icons**, with **intact PDF export**
- **No custom code required**

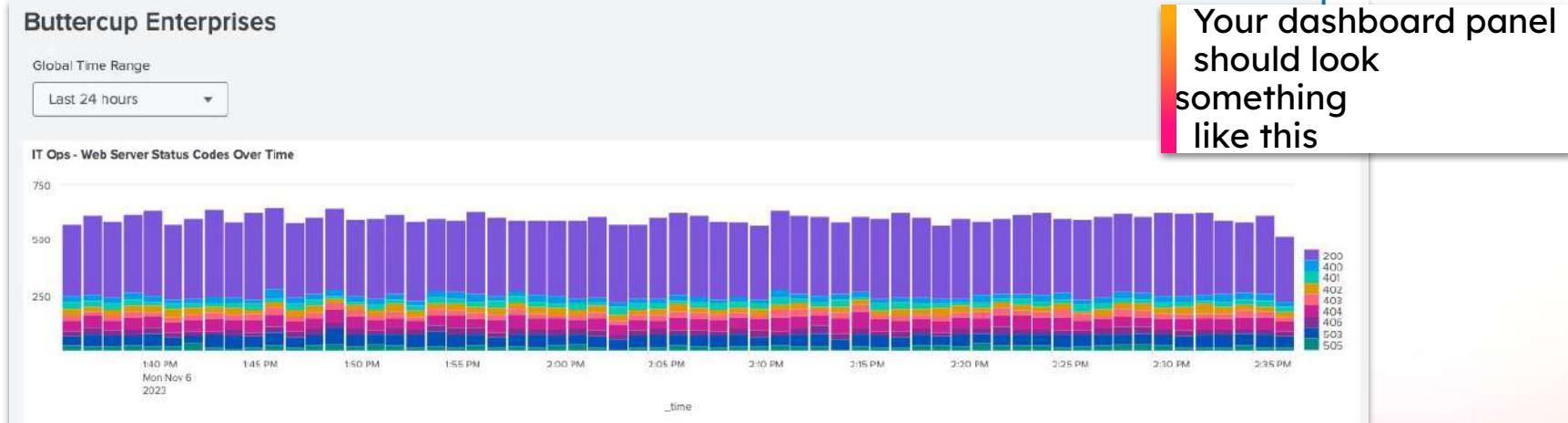


IT Operations Team

Investigate successful versus unsuccessful web server requests over time

Solution:

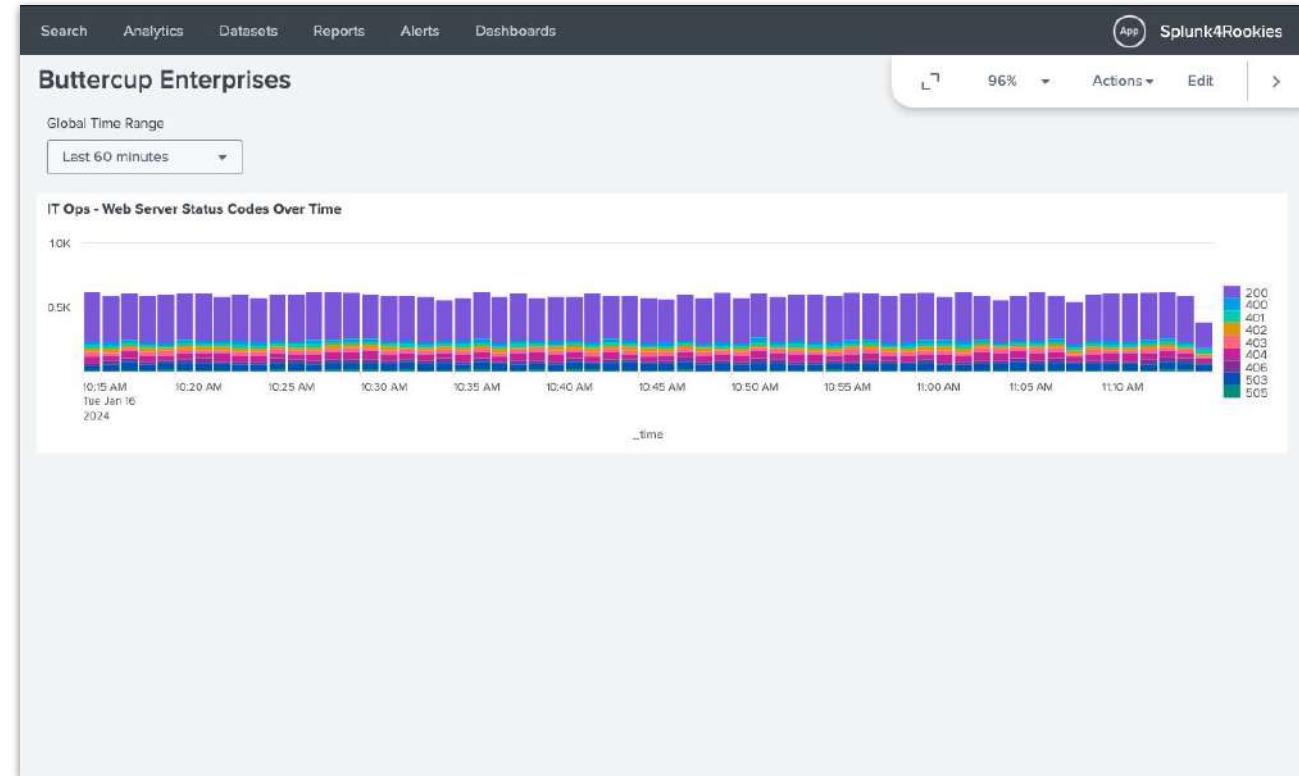
```
index=main sourcetype=access_combined | timechart count by status limit=10
```



Your dashboard so far...



IT Operations team ✓





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

New Search

`index=main sourcetype=access_combined`

Search for all web server events

i	Time	Event
>	03/04/2023 15:10:51.000	1.19.11.11 -- [03/Apr/2023 15:10:51] "GET /cart.do?action=purchase&product_id=ZSG-2&JSESSIONID=SD2SL10FF10ADFF9 HTTP/1.1" 200 1474 "http://www.buttercupenterprises.com/product.screen?product_id=MCF-3" "Mozilla/5.0 Macintosh Intel Mac OS X 10_12_2) AppleWebKit/537.36 Chrome/54.0.2840.98 Safari/537.36" 313

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

The screenshot shows a table with two columns: 'Time' and 'Event'. An arrow points to the 'Event' column for the row '03/04/2023 15:10:51.000'. A dropdown menu titled 'Event Actions' is open over this row, containing options: 'Build Event Type' and 'Extract Fields'. A pink box highlights the 'Extract Fields' option.

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 Next

Select Fields

Highlight one or more values in the sample event to create fields. You can indicate one value is required, meaning it must exist in an event for the regular expression to match. Click on highlighted values in the sample event to modify them. To highlight text that is already part of an existing extraction, first turn off the existing extractions. [Learn more](#)

The screenshot shows the 'Select Fields' step. A sample event is displayed with several values highlighted in yellow. An 'Extract' button is shown above a configuration panel. The panel includes fields for 'Field Name' (set to 'platform') and 'Sample Value' (set to 'Macintosh'). A pink box highlights the 'platform' field name. A green box highlights the 'Add Extraction' button.

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

7. Give the new field a name, lowercase is recommended



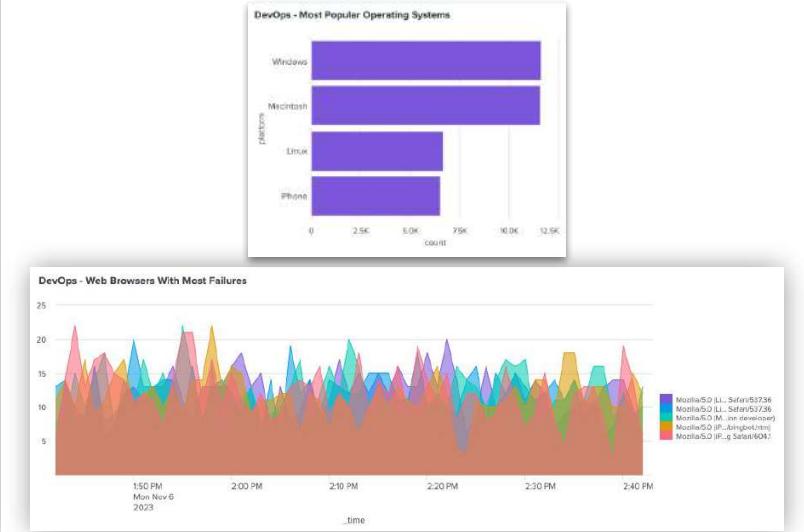
DevOps Team

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



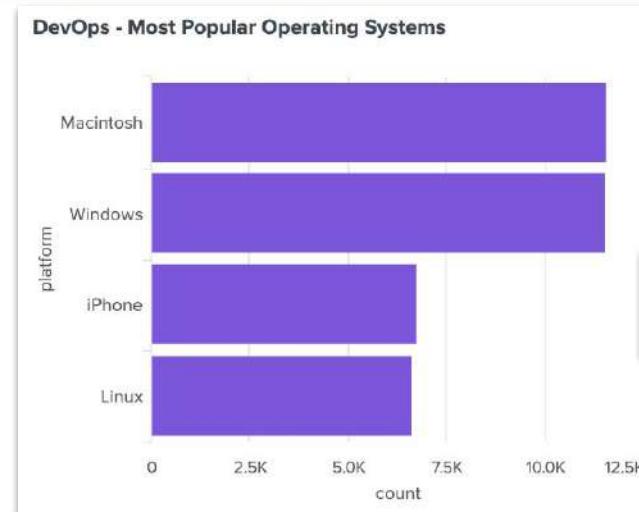


DevOps Team

Show the most common customer operating systems

Solution:

```
index=main sourcetype=access_combined | top limit=20 platform showperc=f
```



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

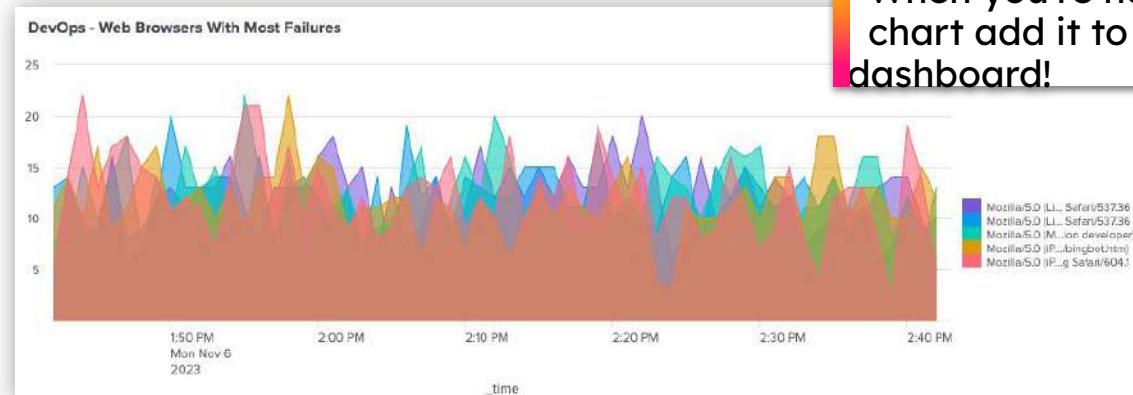


DevOps Team

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

Solution:

```
index=main 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!

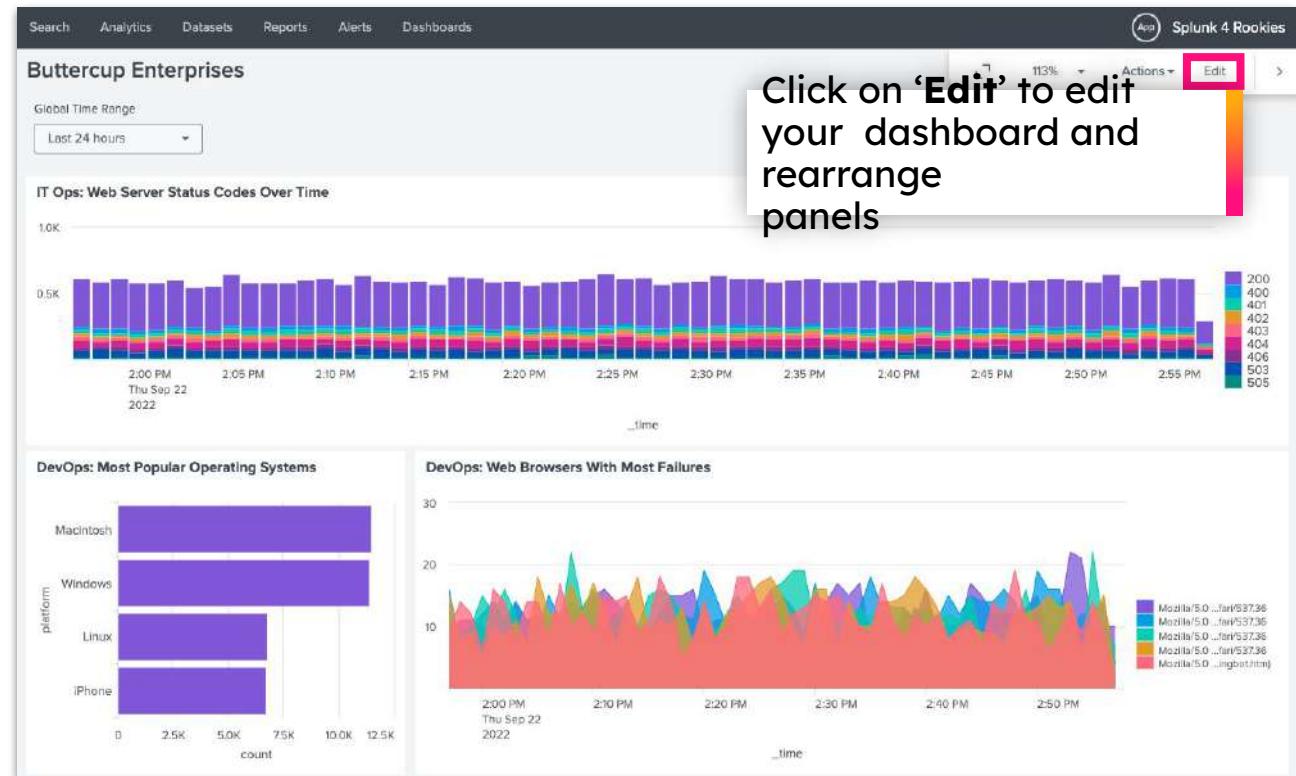
Your dashboard so far...



IT Operations team ✓



DevOps team ✓



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:

```
index=main sourcetype=access_combined  
| stats distinct_count(clientip) by status
```

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

Calculates statistics based on fields in your events

```
index=main 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>

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

Usage:

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

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

Enriches IP data on-the-fly with location data

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

The `iplocation` command produces additional fields containing geographic data

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

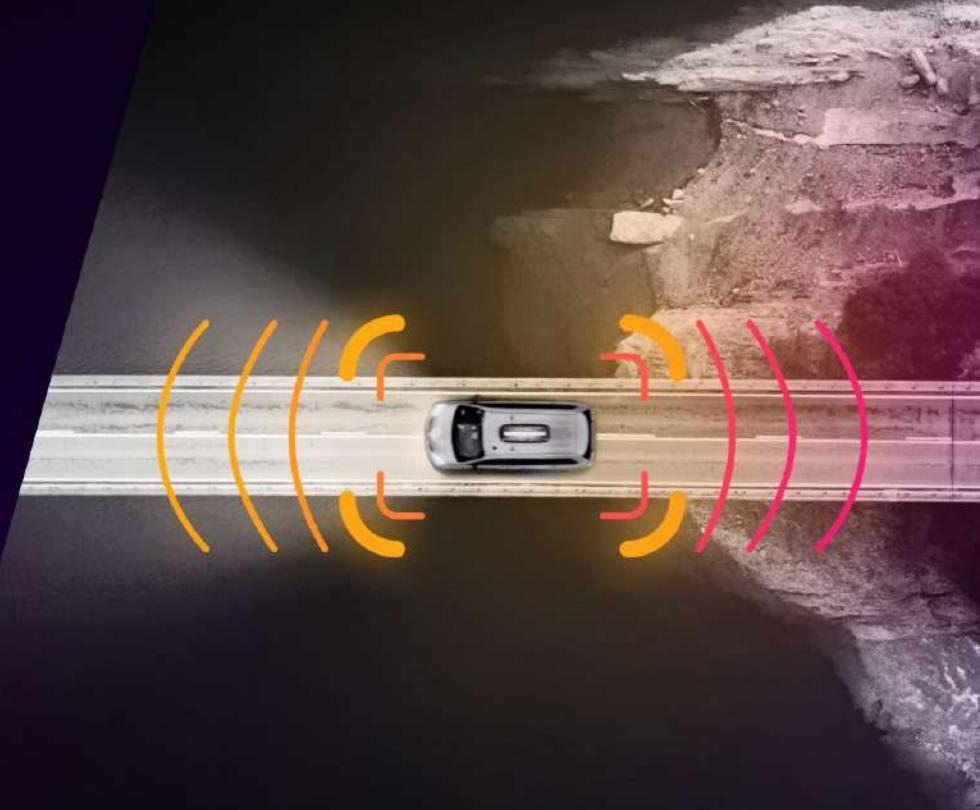
Split your results by a specific field for more detailed analysis



Additional Case Studies

Manufacturing

splunk>



Heineken becomes the world's most resilient brewer with Splunk

“For the first time we can see all the performance of our middleware systems and each of the integrations running on them, in one single view.”



100%

visibility into
3000+ systems

25M

monthly app
messages in
one view

★ Heineken®

Guus Groeneweg
Global Product Owner for Digital Integration
Heineken



Meggitt Enhances Security with Splunk

“Splunk reveals where our security has potential to improve and, when there are issues, helps us figure out what went wrong so we can prevent it from happening again. It's been an absolute game changer for us.”

40

global sites secured
with the help of AI

100%

increase in security coverage for staff workstations

1 Day

to create dashboards to enable secure remote working

MEGGITT

James Steel
Detection and Response Team Manager
Meggitt



Bosch Improves Their Digital Resilience at the Plant Level

“Splunk technology helps us to decide measures faster and with better results. Across the organization, it's creating a higher quality of work.”

20s

to run a query,
versus 15 minutes
prior to Splunk

All

employees can now query data

80+

critical alerts implemented by Bosch Manufacturing Solutions



BOSCH

Claus Giehl

*Industry 4.0 Innovation and Product Manager,
Bosch Manufacturing Solutions*

Today's 2nd Scenario

Your Company

- **Buttercup Manufacturing** is a large national producer of widgets that involves a complex product assembly line process
- The company is also responsible for supplying parts to a wind turbine manufacturer “Splunk Turbines”

Your Roles

- You will help **Splunk Turbines Co.** to generate some dashboards based on wind turbine metrics
- You will also use Splunk to build out a view of the production line assembly so that issues and performance can be closely monitored



Experimenting with IIoT data



splunk>

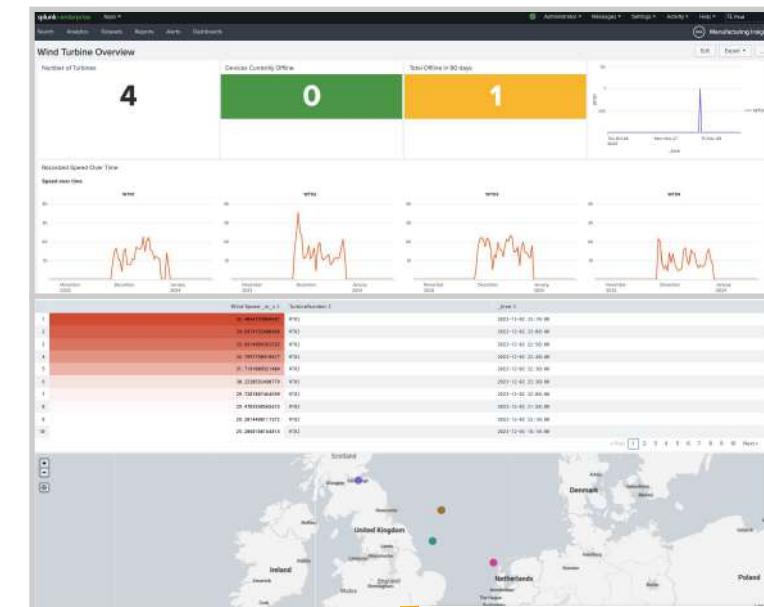


Example searches across IIoT data

Tasks

1. Create a custom app for IIoT data exploration
2. Practice using queries and commands learnt earlier
3. Build a “Wind Turbine Overview” dashboard
4. Answer the lab questions

Goal



Final Dashboard

Operational Technology Security

splunk>



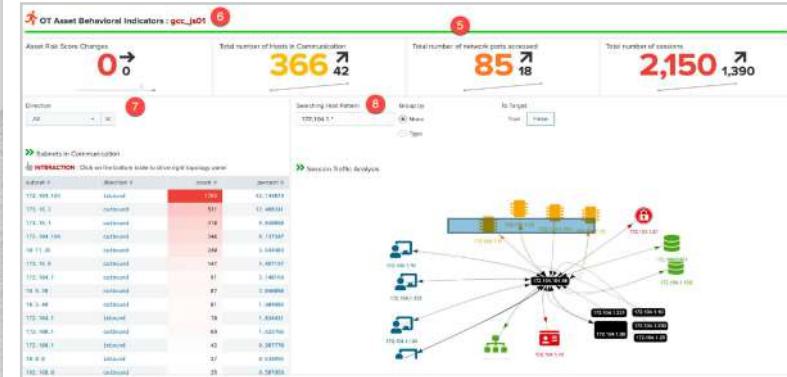


Operational Technology: Security

Tasks

1. Explore the “OT Security” add-on to Splunk Enterprise Security
2. Answer the lab questions

Goal



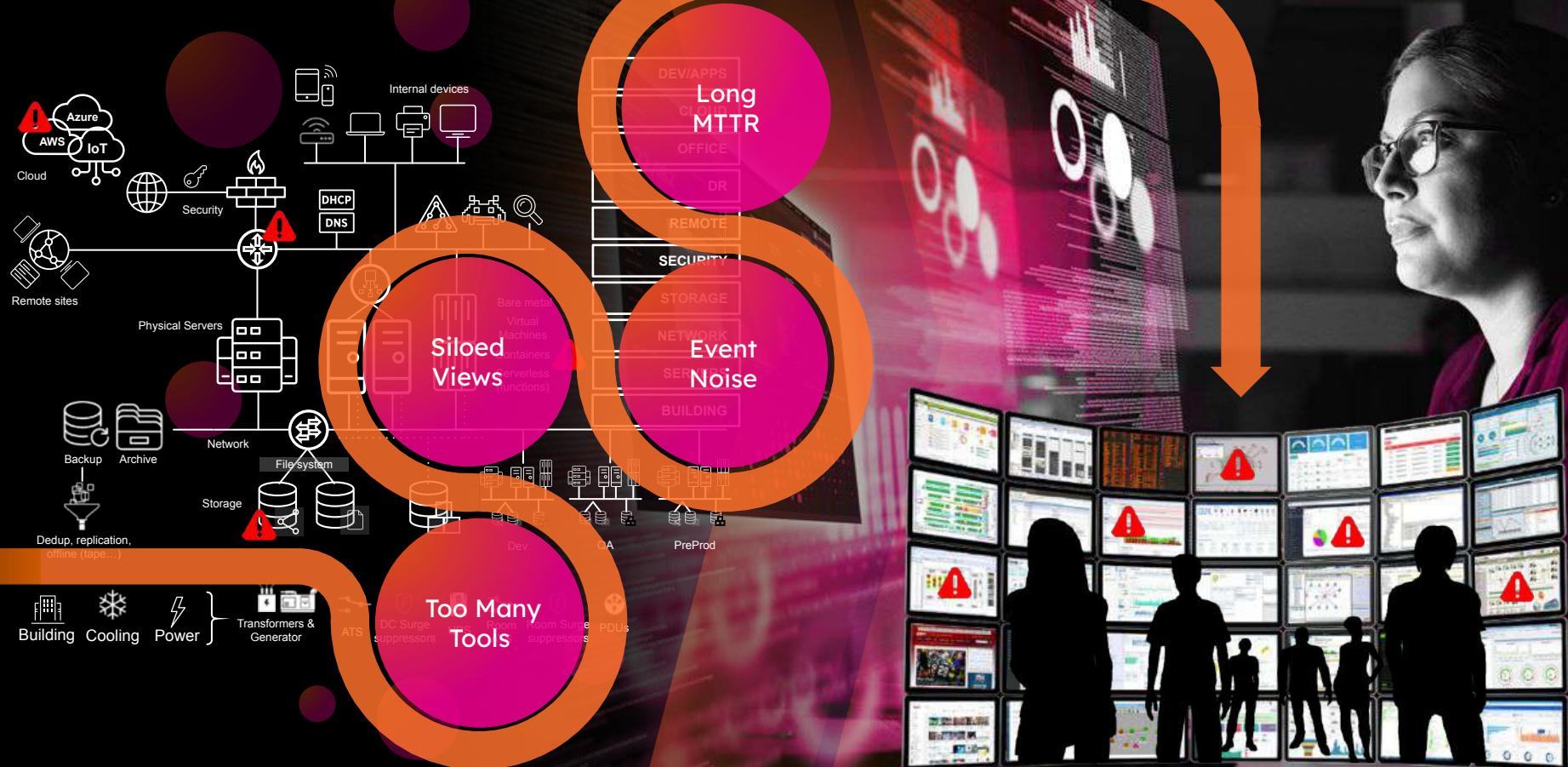
Service Intelligence

Gaining insight into health across the business



Complexity obscures the data you need

IT Ops teams continue to struggle to monitor, investigate, analyze & act



The impact can be significant

Putting revenue, customer experience, employee effectiveness & innovation at risk



Lost Revenue

Outages and incidents impact the services and apps driving revenues



Poor Customer Experiences

Customers click away and brand reputation is damaged



Decreased Employee Effectiveness

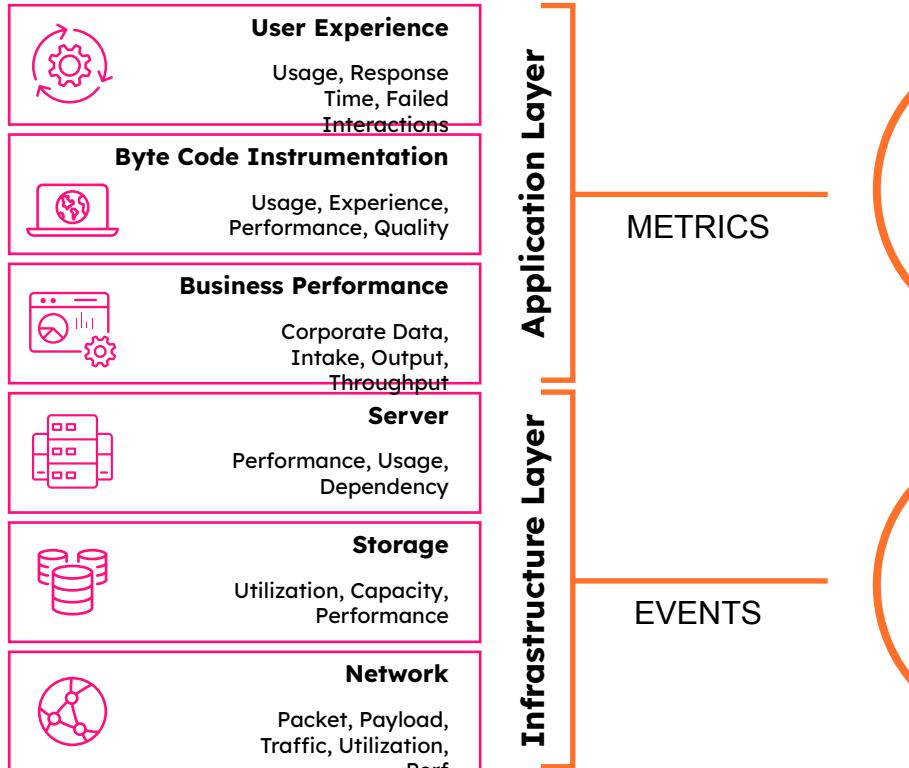
Teams thrash, finger-point, and key employees leave



Struggle to Innovate

IT spends too much time fixing problems instead of innovating and transforming

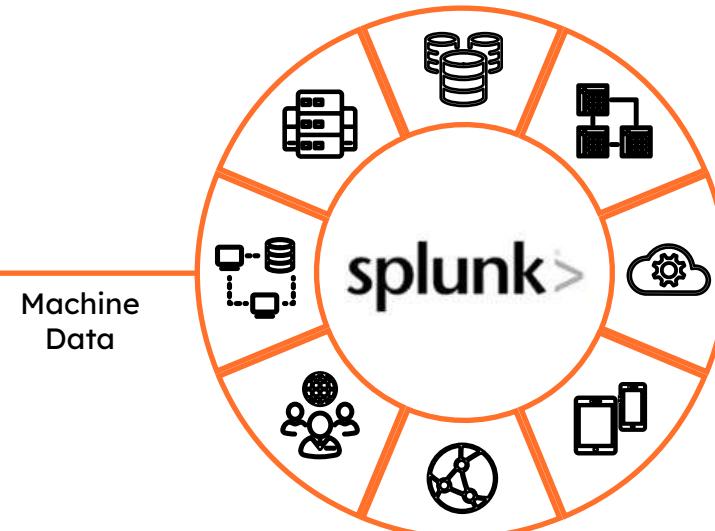
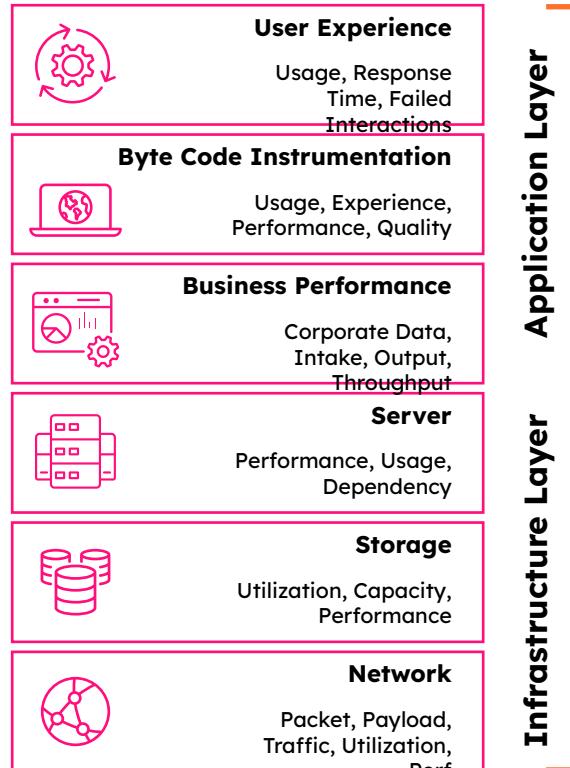
The Old Ways Disappoint



Challenges

- Many disparate components
- Brittle integrations
- Data is summarized and lost
- Longer root-cause identification
- End-to-end view challenging
- Labor-intensive to manage
- Not agile for digital business

Splunk IT Service Intelligence Platform Approach

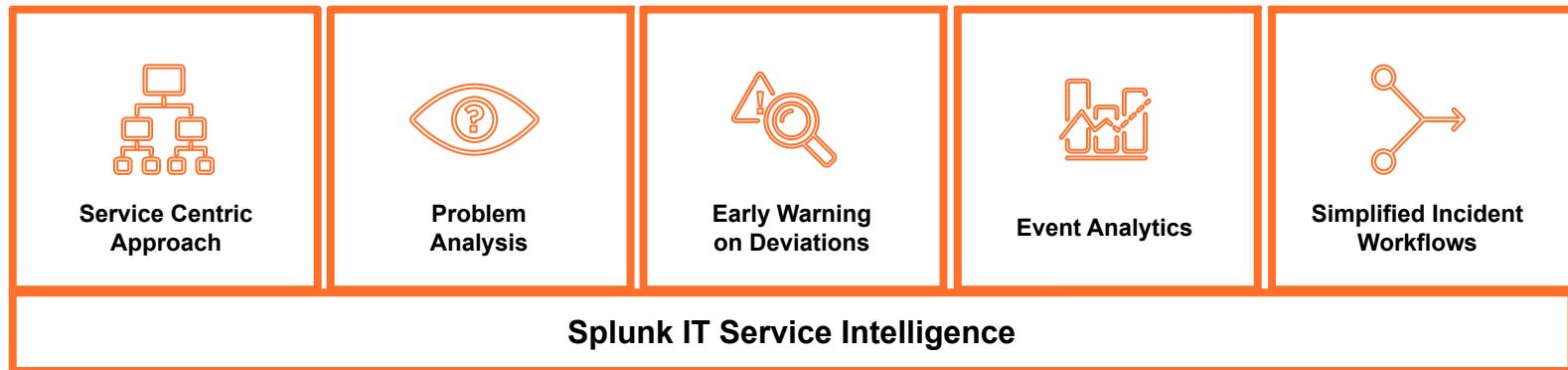


Splunk Approach:

- Repository for **ALL** data
- Data in original raw format
- Machine learning
- Simplified architecture
- Fewer resources to manage
- Collaborative approach

Splunk IT Service Intelligence

Data-driven service monitoring and analytics



splunk> Enterprise

splunk> Cloud

Time-Series Index

Schema-on-Read

Data Model

Common
Information Model

Splunk IT Service Intelligence Key Concepts



Number of visitors

Revenue

Transactions per day



CPU Utilisation

Query Response Time

Storage Free



KPIs



SERVICE HEALTH SCORES

Severity	Entity Name
Critical	mysql-02
Normal	mysql-01
Normal	mysql-03
Normal	mysql-04

Entities and Entity Types

Create entity types to manage similar entities in bulk. Create

Entities Entity types

An entity is an IT component such as a host that contains

8 Entities Bulk Action Edit Columns data

Filters have been applied on the overall list of entities

<input type="checkbox"/>	Title	Aliases
<input type="checkbox"/>	I-0867530967	I-0867530967, 10.2.2.41
<input type="checkbox"/>	I-0867530968	I-0867530968, 10.2.2.41
<input type="checkbox"/>	I-0867530969	I-0867530969, 10.2.2.41
<input type="checkbox"/>	I-0867530970	I-0867530970, 10.2.2.41
<input type="checkbox"/>	mysql-01	mysql-01, 10.2.2.1
<input type="checkbox"/>	mysql-02	mysql-02, 10.2.2.2
<input type="checkbox"/>	mysql-03	mysql-03, 10.2.2.3
<input type="checkbox"/>	mysql-04	mysql-04, 10.2.2.4

ENTITIES

Service Intelligence

Demo



splunk>

Revenue

\$3,343.82 



Performance



Task for today



Robot 1

Health Score
93



Temperature



Vibrations



Output



Robot 2

Health Score
92



Temperature



Vibrations



Output



Robot 3

Health Score
71



Temperature



Vibrations



Output



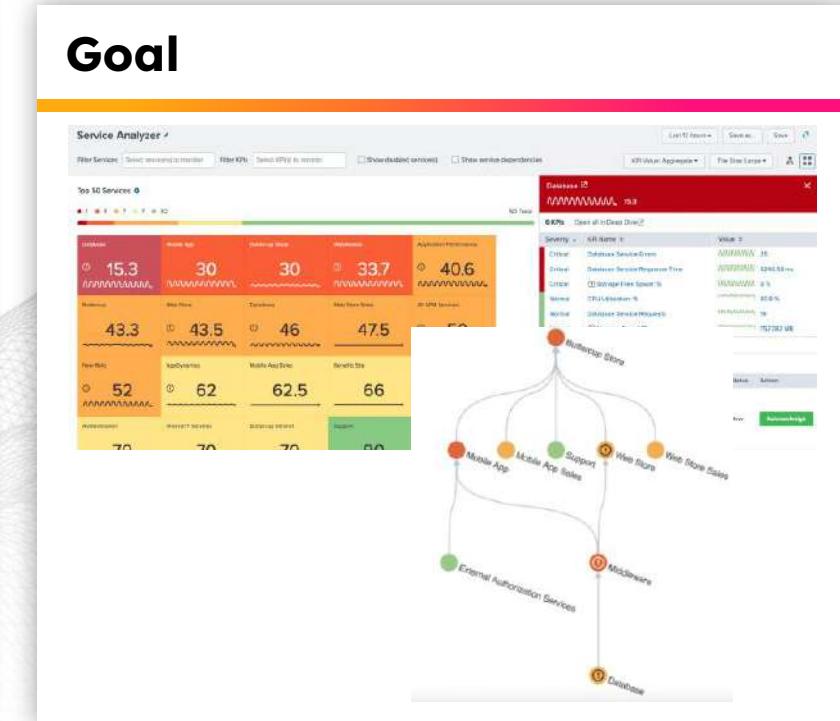


Explore the ITSI capability

Tasks

1. Switch to the ITSI demo instance
2. Investigate Glass Tables
3. Investigate the Service Analyzer
4. Explore Deep Dives
5. View Alerting capabilities

Goal



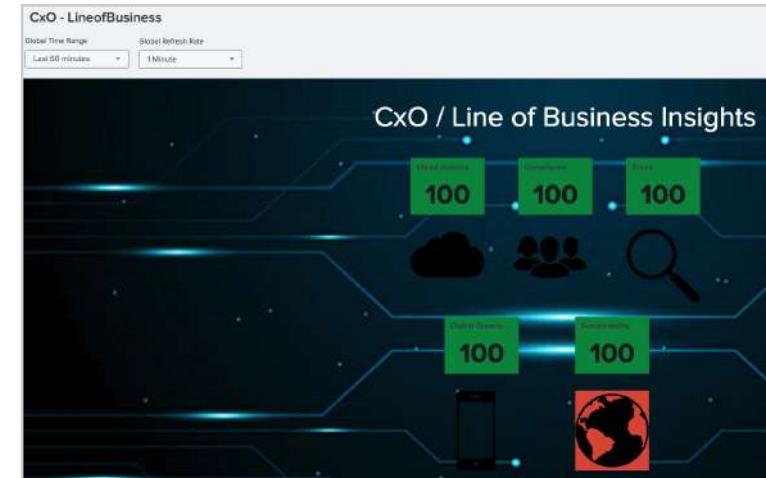


Building a new service view

Tasks

1. Build a service view based on “Product Line Assembly”
2. Add some KPIs to be monitored
3. Build a custom Glass Table for CxO & Line of Business

Goal





Build your own service!

Tasks

1. With the time left, see if you can build a service that represents something you'd like to see for your organisation

Goal

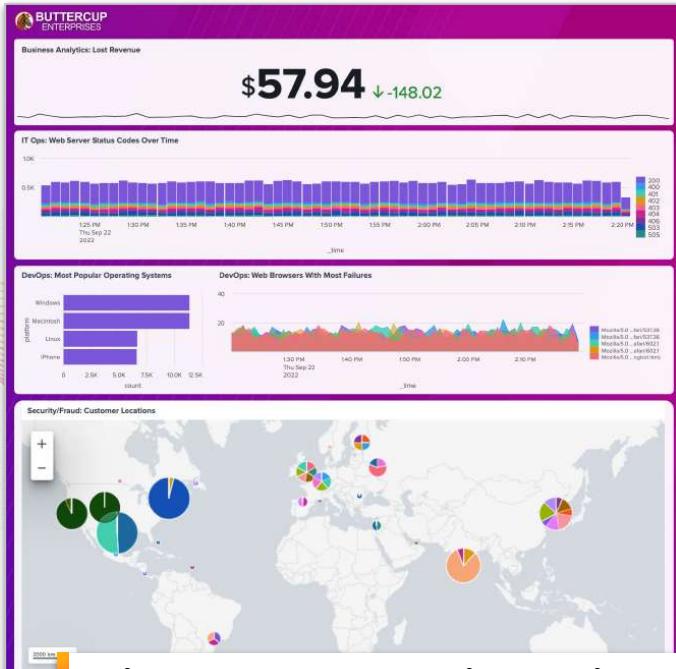


You Finished the Hands-on Exercises!

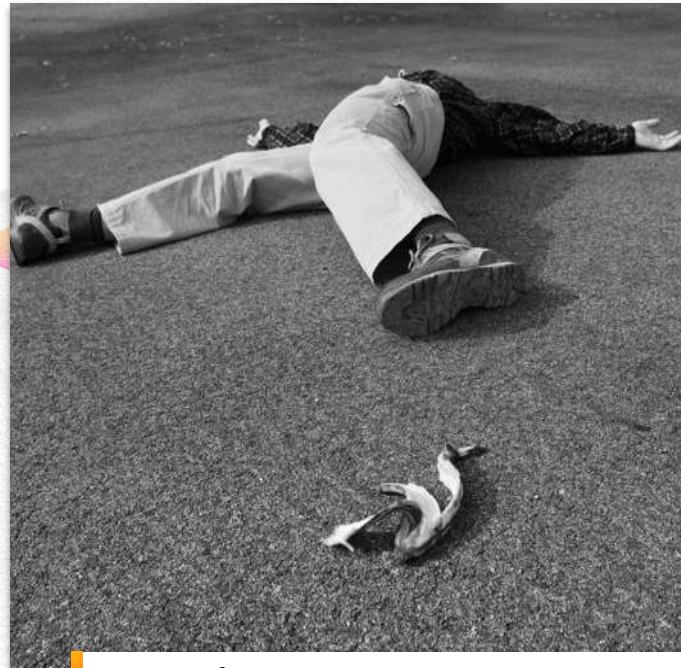
You made it!



How Did You Do?



Did you end up like this?...



Or this?

Splunk Resources

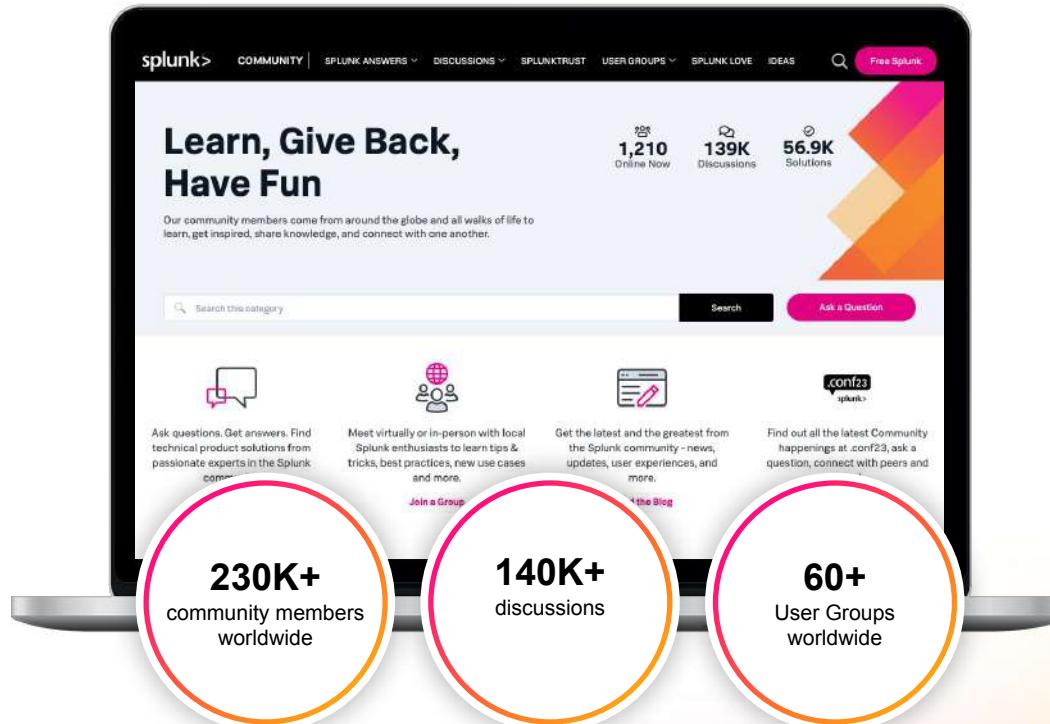
Where to go after today's workshop



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 Events

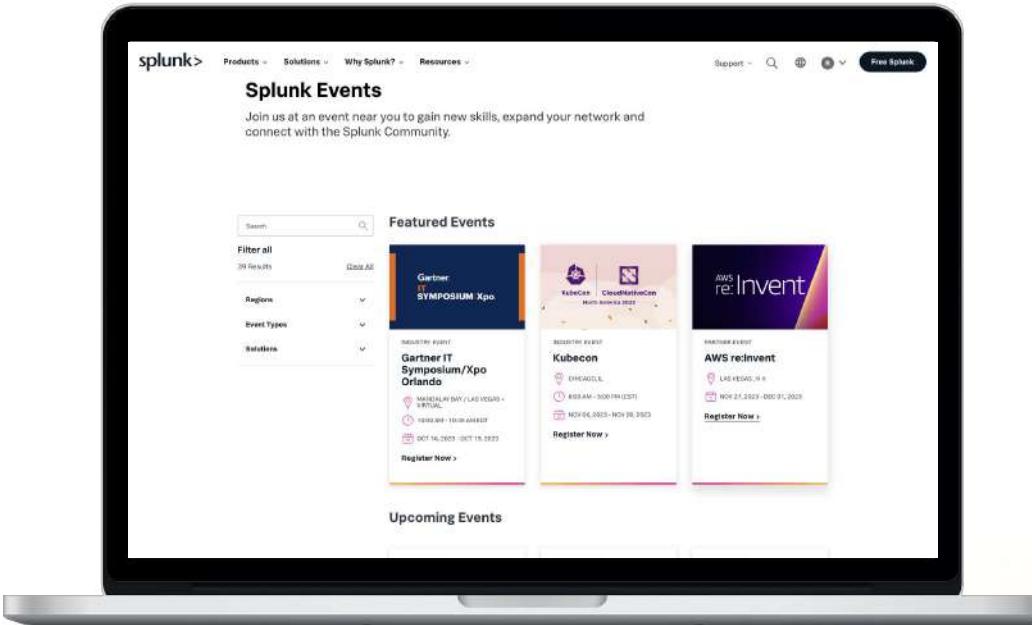
<https://splunk.com/events>

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



<https://conf.splunk.com>

- Join us at .conf24!
- Hundreds of on-demand sessions from product updates to learning new Splunk skills!



Documentation

<https://docs.splunk.com>

- Search reference for SPL
- Step-by-step tutorials

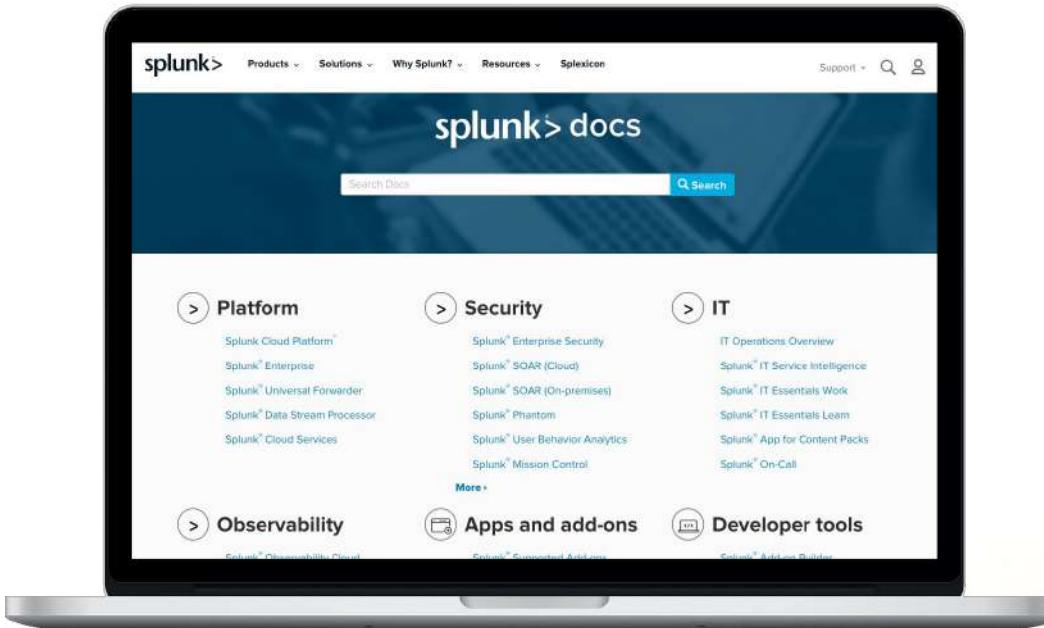
Search:

<https://splk.it/SplunkSearchTutorial>

Dashboard Studio:

<https://splk.it/SplunkDashStudioTutorial>

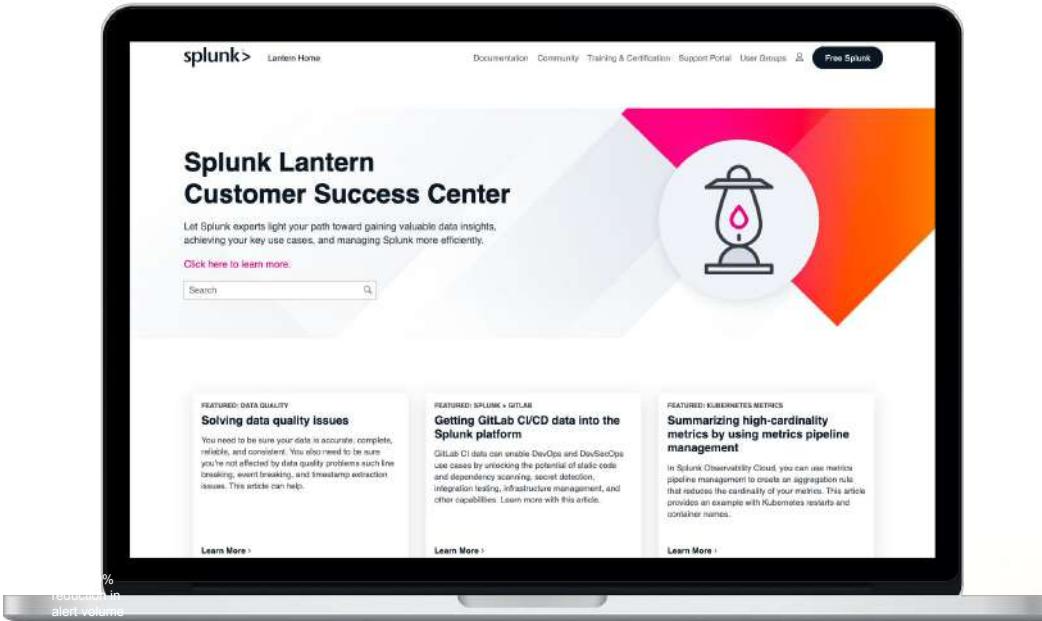
- Product references
- Procedures/guides
- And more!



Splunk Lantern

<https://lantern.splunk.com>

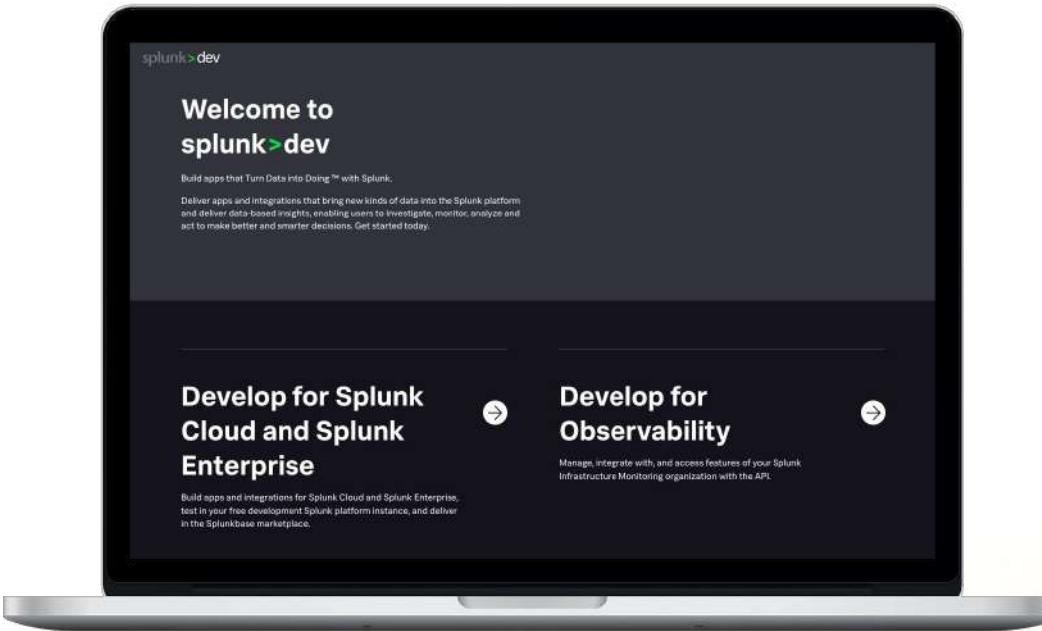
- Use case library
- Step-by-step procedures
- Map use cases to data sources
- Splunk Success Framework to realize value across your organisation



Developer Resources

<https://dev.splunk.com>

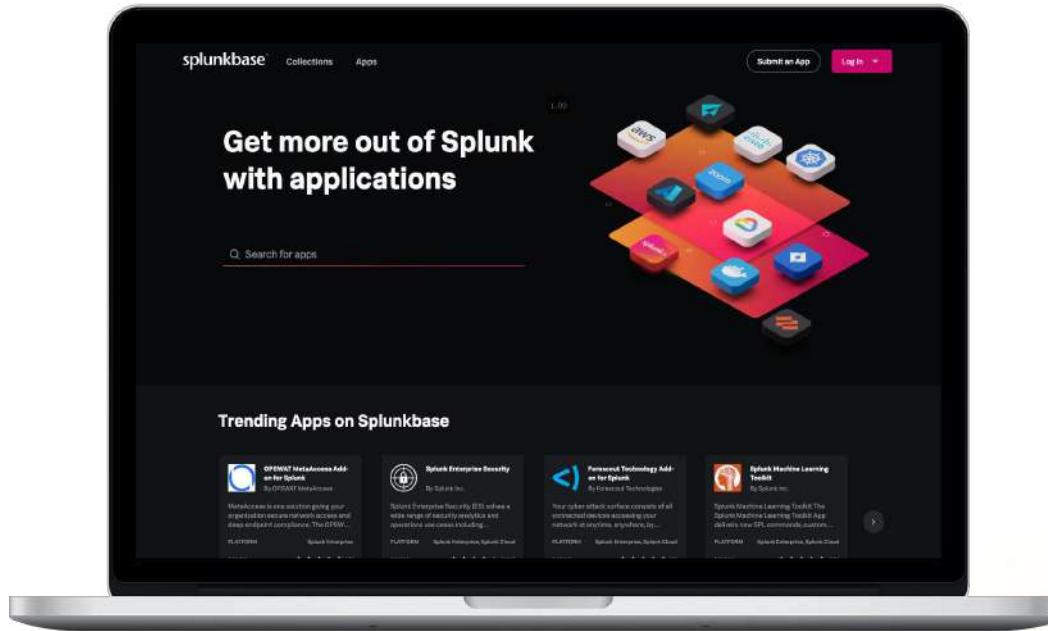
- Developer Guide
- API Reference
- Tutorials
- Downloads
APIs, libraries, tools
- Code examples
- Free Developer licence



Splunk Apps & Add-ons

<https://splunkbase.splunk.com>

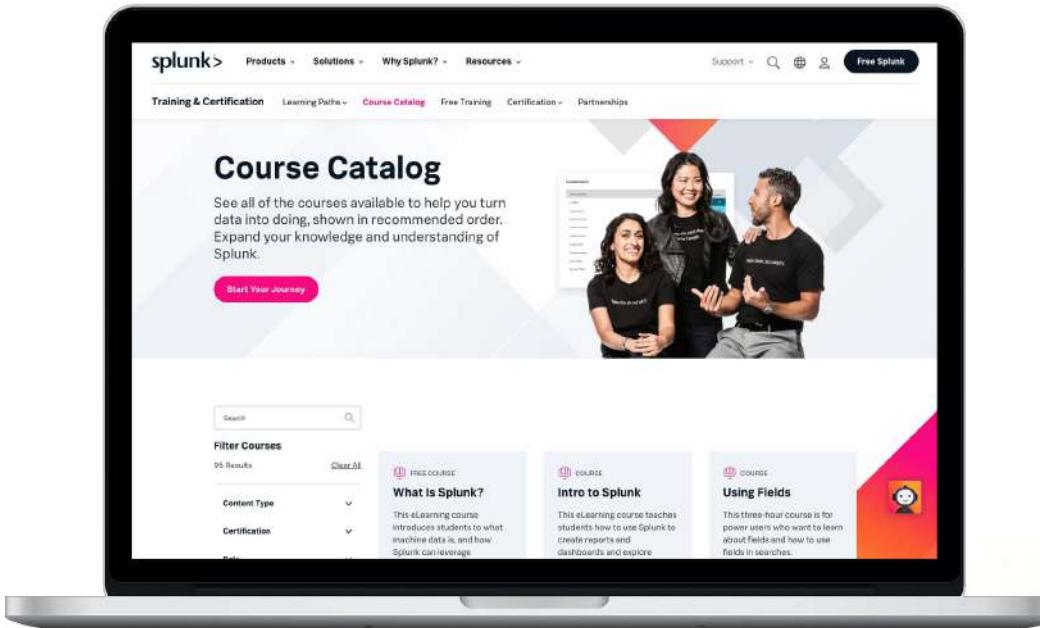
- 3100+ apps and add-ons
- Pre-built searches, reports, visualisations and integrations for specific use cases and technologies
- Download apps and customise them based on your requirements
- Fast time to value from your data
- Build and contribute your own apps!



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



Thank you

