Build Next-gen Splunk App

Custom UI & Visualization with React

Aprameya Mysore
Jet Propulsion Laboratory, California Institute of Technology

Wei Tao
Splunk

Jet Propulsion Laboratory
California Institute of Technology

Aprameya Mysore

Data Visualization Architect
Jet Propulsion Laboratory, California Institute of Technology

JPL CyberSAM UI Team

Arun Viswanathan

CyberSAM Task Lead

Sami Sahnoune

Data Visualization Engineer

Mike Milano

Designer

Adit Dhanushkodi

Designer

Wei Tao

Senior Product Manager | Splunk

Agenda

DEV1345

Build Next- gen Splunk App with NASA JPL

Jet Propulsion Laboratory
California Institute of Technology

1) Background

Our 1st gen Situational Awareness implementation + its limitations

2) Solution & Implementation

Shift to React-based framework

3) Demo

Of application UI we have created so far

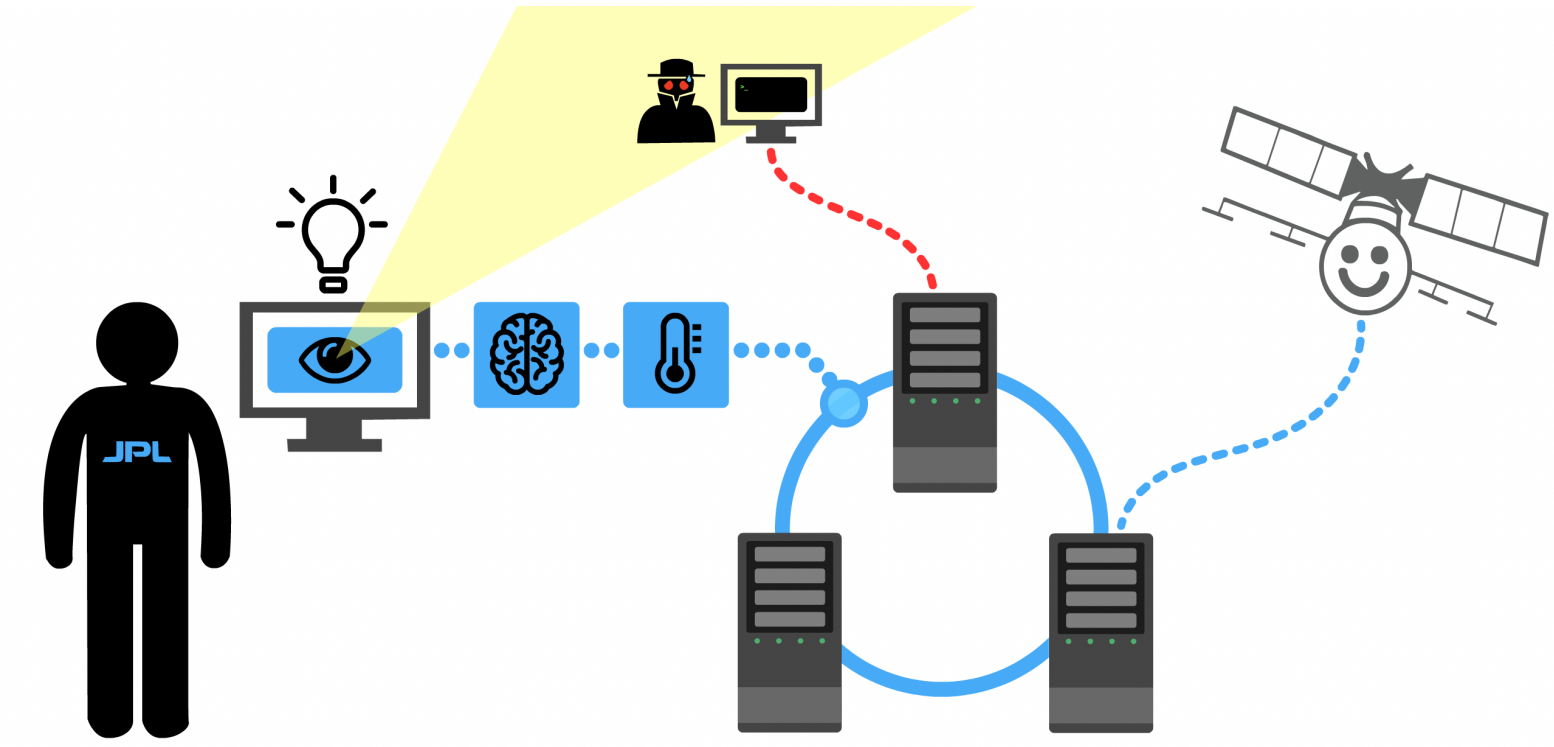
4) What's Next

Future direction of the custom app

5) Splunk Web Platform

What you can do to learn more

CyberSAM: Cyber Situational Awareness for Missions



splunk>enterprise App: Search & Reporting ▾ 2 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search

Save As ▾ New Table Close

```
1 index="_internal"
```

All time ▾

6,667,324 of 6,667,324 events matched No Event Sampling ▾ Job ▾ Verbose Mode ▾

Events (6,667,324) Patterns Statistics Visualization

Format Timeline ▾ – Zoom Out + Zoom to Selection × Deselect 1 day per column

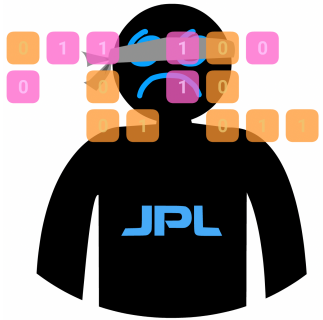
Aug 13, 2020

List ▾ Format 50 Per Page ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

< Hide Fields All Fields

SELECTED FIELDS
active_hist_searches 26
active_realtime_searches 12
bytes 100+
a clientip 58
a component 100+
cpu_seconds 100+
cumulative_hits 100+
current_queue_size 9
date_hour 24
date_mday 16
date_minute 60
a date_month 1
date_second 60
a date_wday 7
date_year 1
date_zone 3

i	Time	Event
>	8/26/20 10:02:27.534 PM	10.160.149.180 - admin [26/Aug/2020:22:02:27.534 -0700] "GET /en-US/splunkd/__raw/services/search/shelper?output_mode=json&snippet=true&snippetEmbedJS=false&namespace=search&search=search+index%3D%22%2Bin&useTypeahead=true&showCommandHelp=true&showCommandHistory=true&showFieldInfo=false&_=1598504502838 HTTP/1.1" 200 5248 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.125 Safari/537.36" - 142a60077e087bae8294e8426fd073f3 6ms bytes = 5248 | clientip = 10.160.149.180 | date_hour = 22 | date_mday = 26 | date_minute = 2 | date_month = august | date_second = 27 | date_wday = wednesday | date_year = 2020 | date_zone = -420 | file = shelper | host = udfplayground | ident = - | index = _internal | linecount = 1 | method = GET | other = - 142a60077e087bae8294e8426fd073f3 6ms | output_mode = json | punct = ..._-___[//:::._-]__"_/-/////?=&=&=&=&=+%%%&=&=&=&=& | referer = - | req_time = 26/Aug/2020:22:02:27.534 -0700 | root = en-US | source = /root/demo_dashboard_beta_app/splunk/var/log/splunk/splunkd_ui_access.log | sourcetype = splunkd_ui_access | spent = 6 | splunk_server = udfplayground | status = 200 | timeendpos = 54 | timestartpos = 24 | uri = /en-US/splunkd/__raw/services/search/shelper?output_mode=json&snippet=tru... | uri_path = /en-US/splunkd/__raw/services/search/shelper | uri_query = output_mode=json&snippet=true&snippetEmbedJS=false&namespace=search&... | user = admin | useragent = Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/537.36 (KHTML, li... | version = HTTP/1.1
>	8/26/20 10:02:27.442 PM	10.160.149.180 - admin [26/Aug/2020:22:02:27.442 -0700] "GET /en-US/splunkd/__raw/services/search/shelper?output_mode=json&snippet=true&snippetEmbedJS=false&namespace=search&search=search+index%3D%22%2Bi&useTypeahead=true&showCommandHelp=true&showCommandHistory=true&showFieldInfo=false&_=1598504502837 HTTP/1.1" 200 5249 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/537.36 (KHTML, lik



Solution #1: Manual Log Analysis

Challenges for users

Information Fatigue

Extremely large quantity of information directed to the user with no prioritization

Lack of Actionable Insight

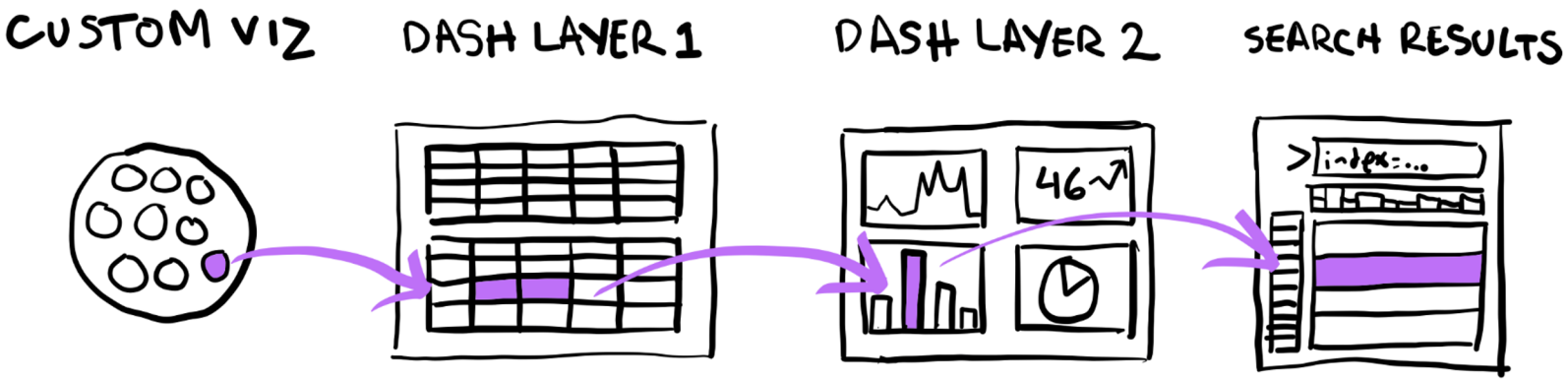
What does a user do with the information?

Lack of Interactivity

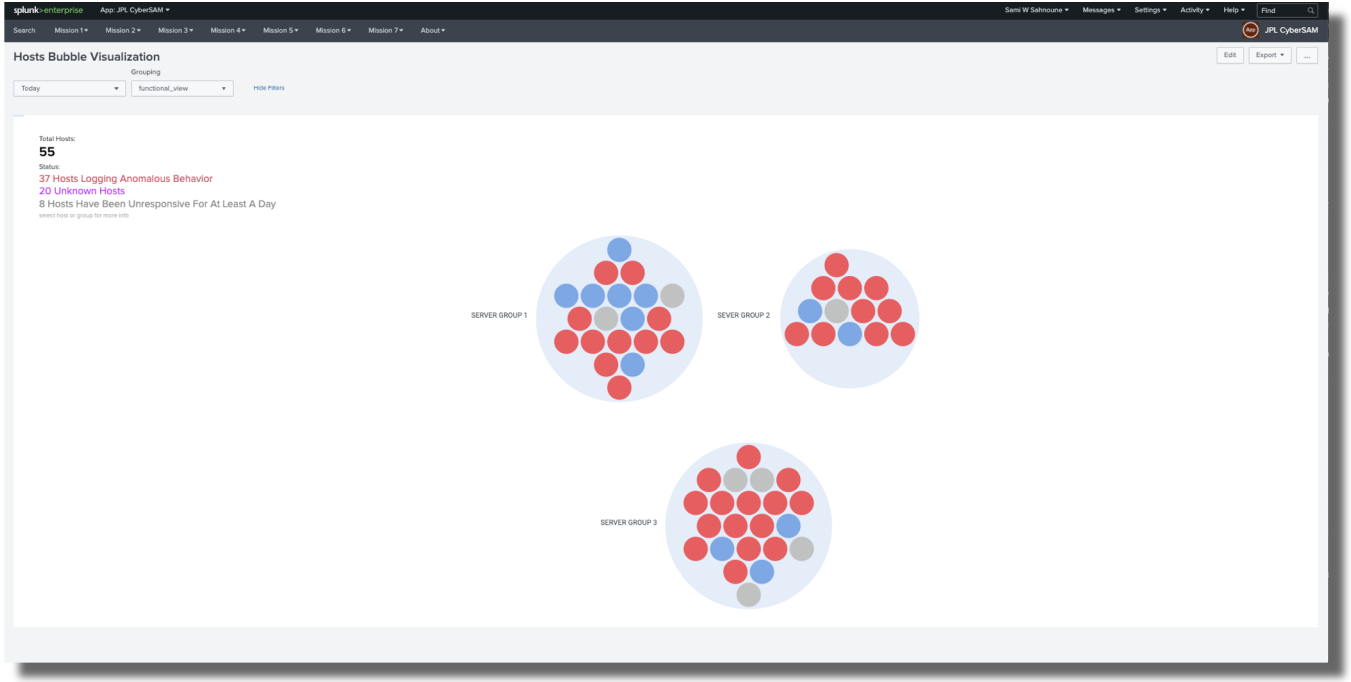
To explore/analyze patterns in the aggregate

Solution #2: Dashboard Based Interface

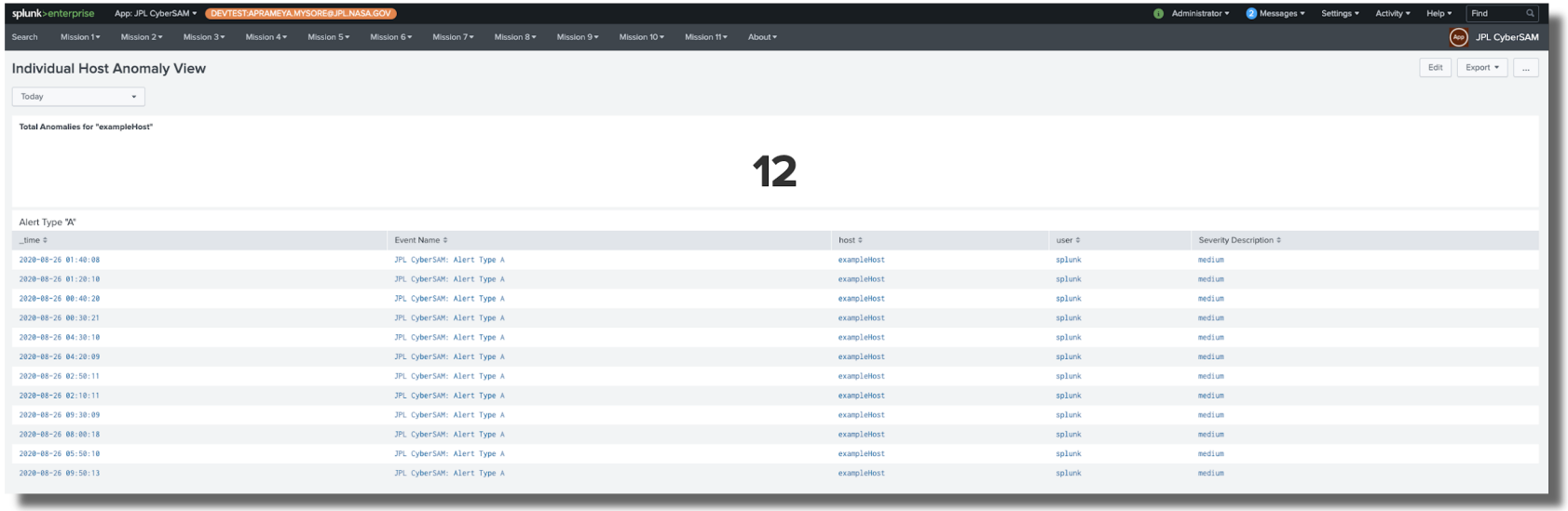
Progressive Disclosure Paradigm



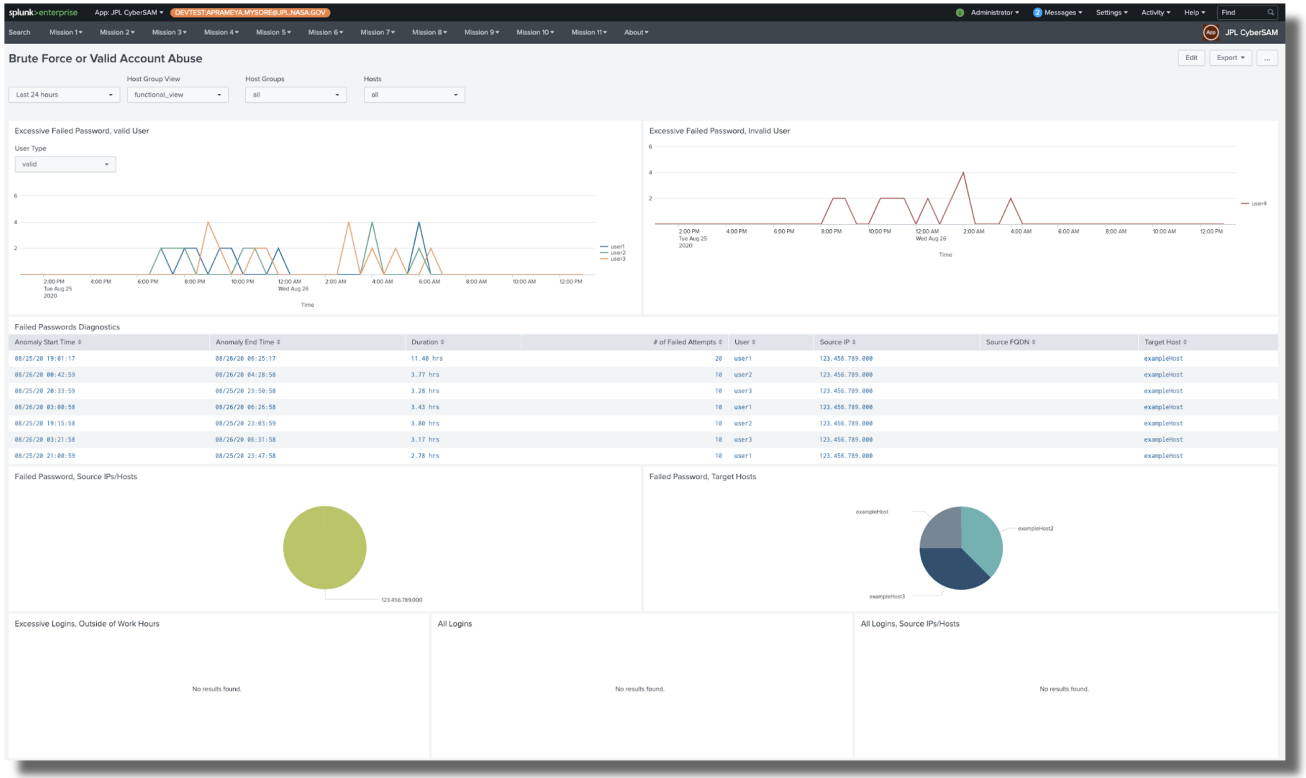
Step 1: D3.js Custom Viz



Step 2: Dashboard Layer 1



Step 3: Dashboard Layer 2



Step 4: Search Results

splunk>enterprise App: Search & Reporting ▾ 2 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search Save As ▾ New Table Close

1 index="_internal" All time ▾

6,667,324 of 6,667,324 events matched No Event Sampling ▾ Job ▾ Verbose Mode ▾

Events (6,667,324) Patterns Statistics Visualization

Format Timeline ▾ − Zoom Out + Zoom to Selection × Deselect 1 day per column

Aug 13, 2020

List ▾ Format 50 Per Page ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

< Hide Fields All Fields

SELECTED FIELDS

active_hist_searches 26
active_realtime_searches 12
bytes 100+
a clientip 58
a component 100+
cpu_seconds 100+
cumulative_hits 100+
current_queue_size 9
date_hour 24
date_mday 16
date_minute 60
a date_month 1
date_second 60
a date_wday 7
date_year 1
date_zone 3

i	Time	Event
>	8/26/20 10:02:27.534 PM	10.160.149.180 - admin [26/Aug/2020:22:02:27.534 -0700] "GET /en-US/splunkd/__raw/services/search/shelper?output_mode=json&snippet=true&snippetEmbedJS=false&namespace=search&search=search+index%3D%22%2Bin&useTypeahead=true&showCommandHelp=true&showCommandHistory=true&showFieldInfo=false&_=1598504502838 HTTP/1.1" 200 5248 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.125 Safari/537.36" - 142a60077e087bae8294e8426fd073f3 6ms bytes = 5248 clientip = 10.160.149.180 date_hour = 22 date_mday = 26 date_minute = 2 date_month = august date_second = 27 date_wday = wednesday date_year = 2020 date_zone = -420 file = shelper host = udfplayground ident = - index = _internal linecount = 1 method = GET other = - 142a60077e087bae8294e8426fd073f3 6ms output_mode = json punct = ..._-__[//:::._-]_"_/-/////?=&=&=&=&=+%%%&=&=&=&=& referer = - req_time = 26/Aug/2020:22:02:27.534 -0700 root = en-US source = /root/demo_dashboard_beta_app/splunk/var/log/splunk/splunkd_ui_access.log sourcetype = splunkd_ui_access spent = 6 splunk_server = udfplayground status = 200 timeendpos = 54 timestartpos = 24 uri = /en-US/splunkd/__raw/services/search/shelper?output_mode=json&snippet=tru... uri_path = /en-US/splunkd/__raw/services/search/shelper uri_query = output_mode=json&snippet=true&snippetEmbedJS=false&namespace=search&... user = admin useragent = Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/537.36 (KHTML, li... version = HTTP/1.1
>	8/26/20 10:02:27.442 PM	10.160.149.180 - admin [26/Aug/2020:22:02:27.442 -0700] "GET /en-US/splunkd/__raw/services/search/shelper?output_mode=json&snippet=true&snippetEmbedJS=false&namespace=search&search=search+index%3D%22%2Bi&useTypeahead=true&showCommandHelp=true&showCommandHistory=true&showFieldInfo=false&_=1598504502837 HTTP/1.1" 200 5249 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/537.36 (KHTML, lik

Obstacles for Solution #2 at Scale

Dashboard frameworks are built for data presentation, not application workflow

Information Fatigue --> Dashboard Fatigue

Too many dashboards. Which one(s) to look at?

Dashboard Density + Code Bloat

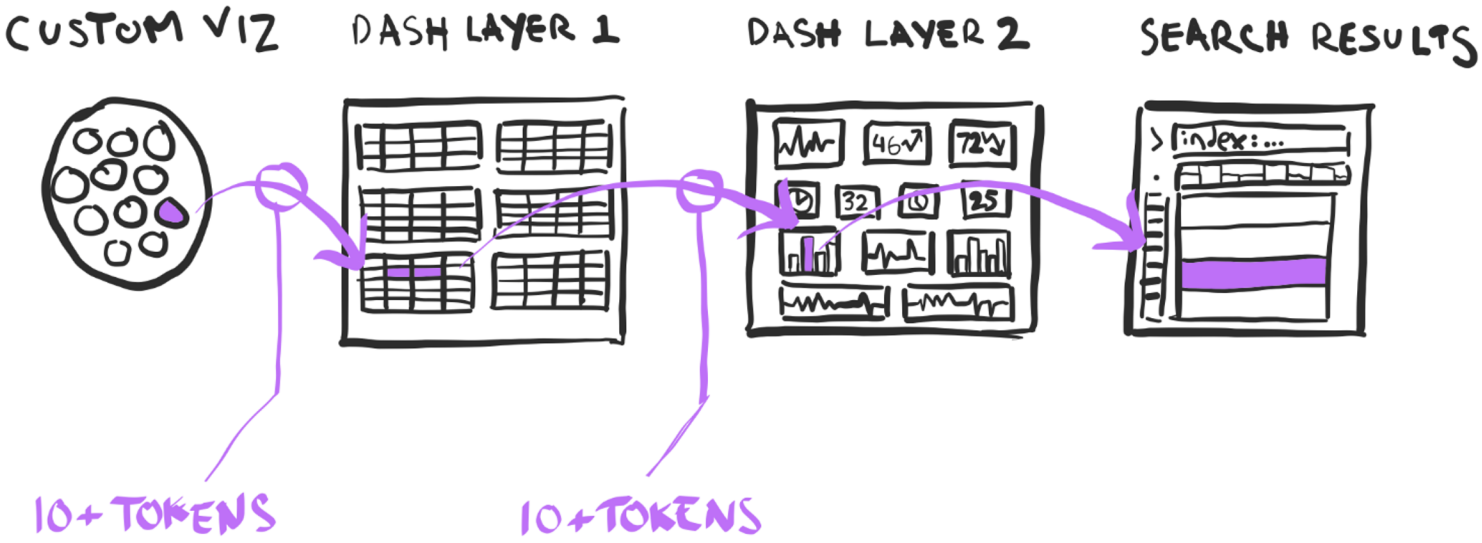
New analysis features end up worsening UX

Limitations of SplunkJS

Building advanced interactions is clunky in SplunkJS

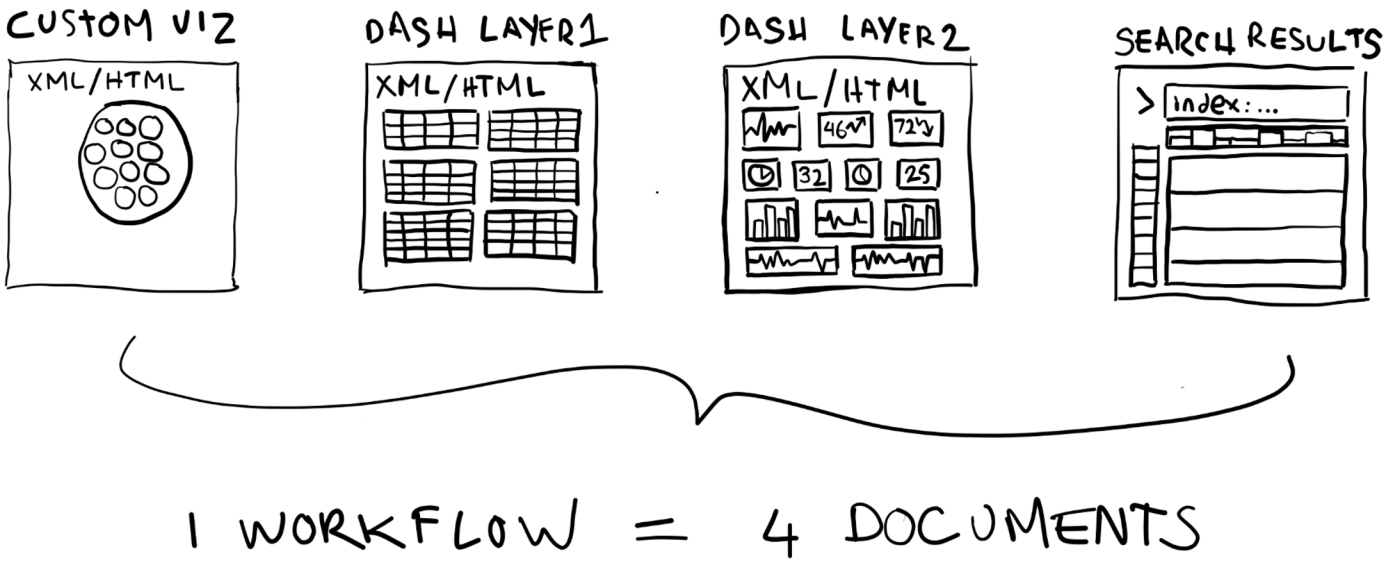
Issue 1: Dashboard Fatigue

Relying on dashboards dilutes salient info as more analysis features become available.



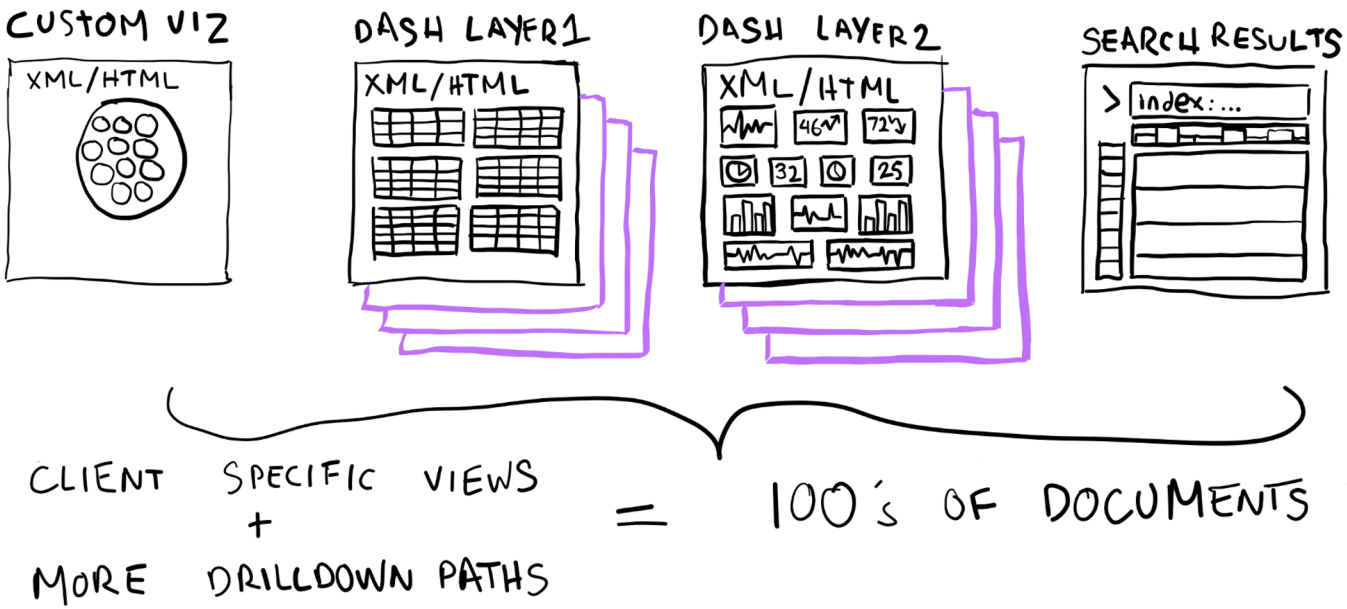
Issue 2: Bloated Codebase

Simple workflows require several html documents

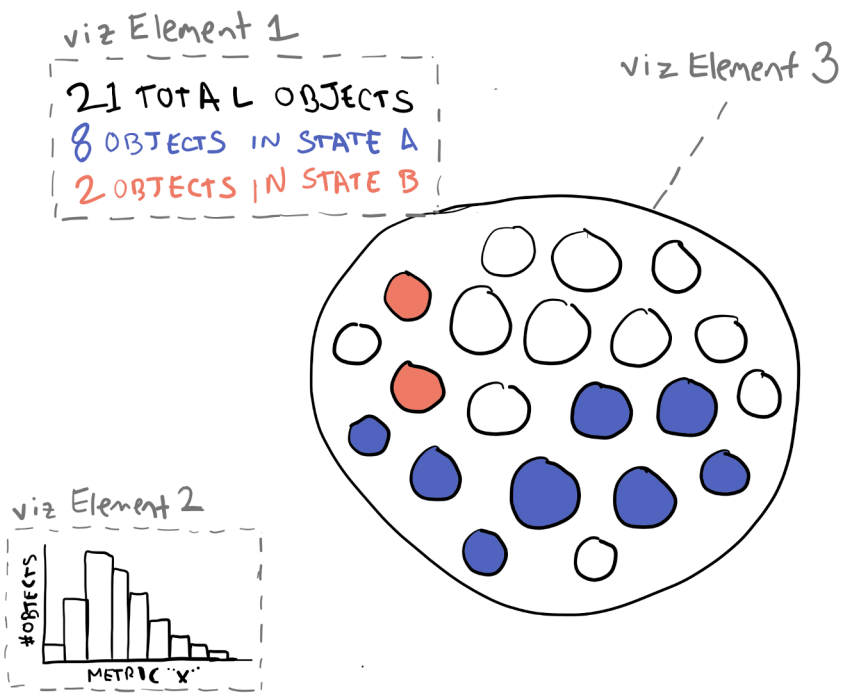


Issue 2: Bloated Codebase

Branching factor is overwhelming for users and developers



Issue 3: Clunky Component Management




```
return SplunkVisualizationBase.extend({
            initialize: () => {
            vizElement1.init()
            vizElement2.init()
            vizElement3.init()
     },
            formatData: (data) =>
{...},
            updateView: (data, config)
=> {

            vizElement1.draw()
         vizElement2.draw()
         vizElement3.draw()
     },
     _drilldown: (data, index) => {
            vizElement1.drilldown()
            vizElement2.drilldown()
            vizElement3.drilldown()
     }
})
```

Goals from Adopting the React Framework

The benefits we hope to achieve in the new implementation

Transition with Context

Single-page App that retains context without opening extra windows

Reusable Components

Compose complex components into views instead of 100s of Dashboards

Context Specific Views

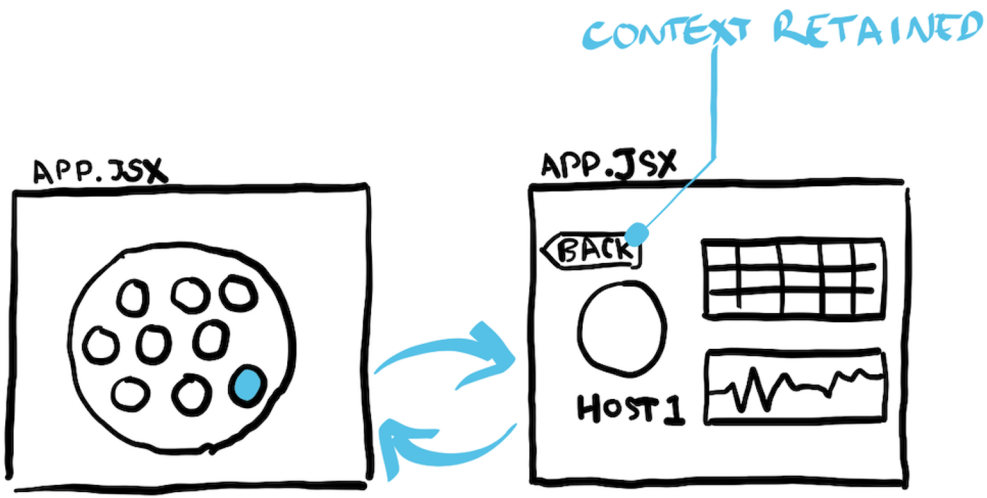
Dynamically present only relevant information

Reduce Code Bloating

Cleanliness and modularity in our codebase as we scale

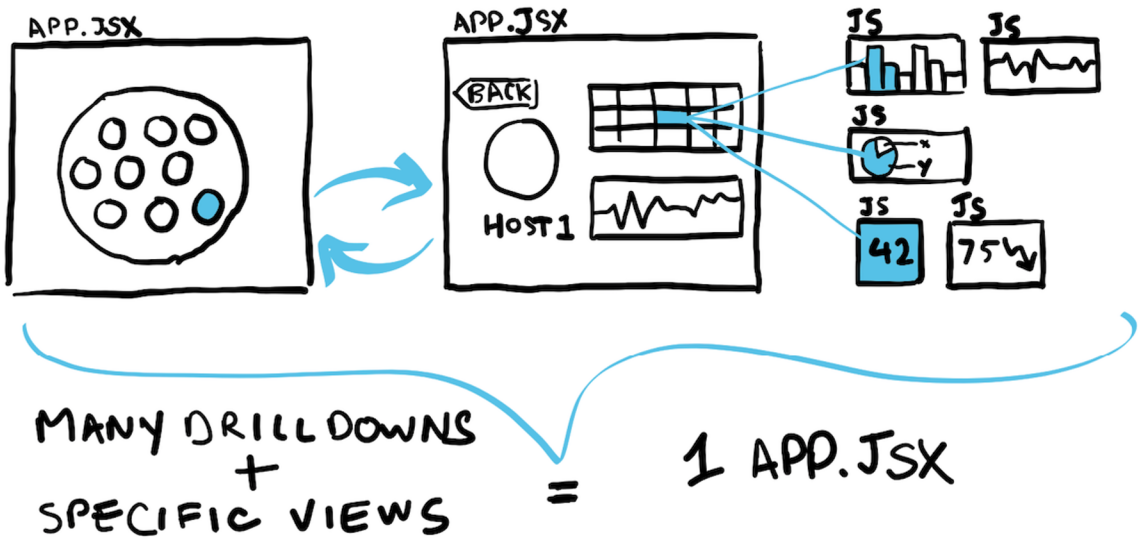
Solving Issue 1: Dashboard Fatigue

Using @splunk/search job and react-spring for dashboard-less transitions

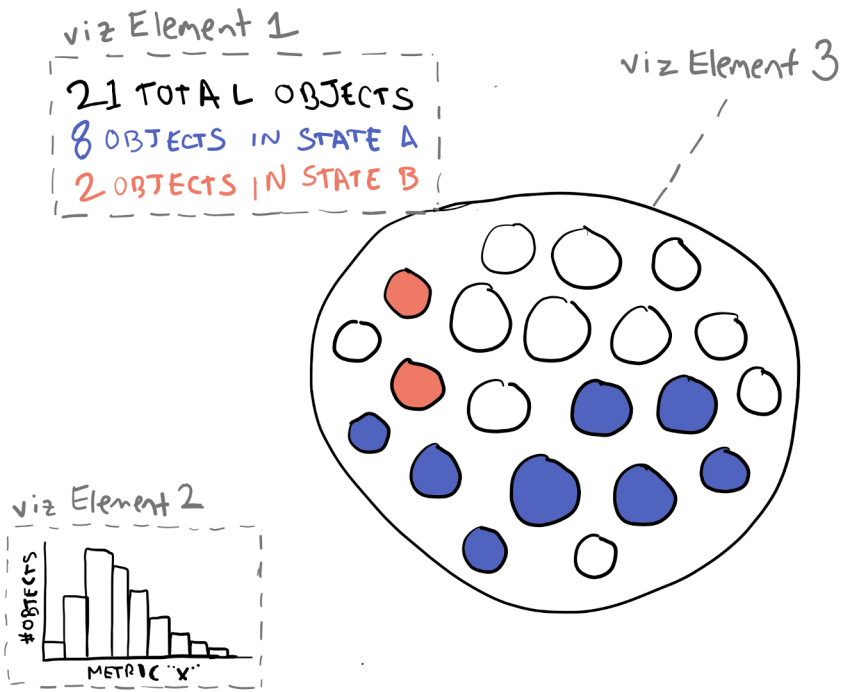


Solving Issue 2: Code Bloat

Leveraging modular components to present many views in a single page



Solving Issue 3: Managing Components




```
return (
        <ThemeProvider>
            <div>
                <vizElement1
                    prop1={prop1}
                    prop2={prop2}
                />
                <vizElement2 />
                <vizElement3 />
            </div>
        </ThemeProvider>
    );
```

Demo

What’s Next?

- Fully migrate all existing dashboard-based apps to React-based framework.
- Building React applications outside of Splunk and integrating with Splunk-based analytics.

A toolkit for developing UI at scale

UI Components Utilities Build Tools Code Quality Tools

Get Started

A few documents to help you get started with the Splunk UI packages.

Component Tutorial
Dashboard Extension
Working with Splunk UI and CoreJS

+ More

Community

Get help from other developers. Give back by contributing to the Splunk UI project.

Chat
Request a Feature
File a Bug

+ More

API Docs

Splunk UI is divided into many packages, which can be used separately. Click 'More' for the full list.

React UI
Splunk Utils
UI Utils

+ More

@splunk/react-ui
3.0.0

filter

Overview
Change Log
Licenses
Testing
Theming

Base
Accordion
Anchor
Button
Button Group
Card
Card Layout
Chip
Code
Collapsible Panel
Concertina
Definition List
Heading
JSON Tree
Link
List
Markdown
Menu
Message
Modal

Button

Use `Button` for clickable actions or as links to another page. `Button` automatically selects the appropriate tag.

Source Code

Examples API Test Hooks

Enabled

Show Code

Default Secondary Primary Flat Toggle

Disabled

Show Code

Default Secondary Primary Flat Toggle

With icons

Show Code

By default, icons appear to the left of button text. If you want an icon to appear the right of button text, add it as a child and correct margins or other positioning as necessary.

+ Add + Add + Add + Add

React-based Framework

Splunk Web Platform: our internal application building toolkit

Component Library

Basic and Complex Components with Themes

Visualization Library

22 Different Visualizations and Support for Custom Viz

Dashboard Framework

Supports Grid and Absolute Layouts and Multiple Data-sources

Splunk Utilities

Interact with Splunk Enterprise and Run Search Jobs

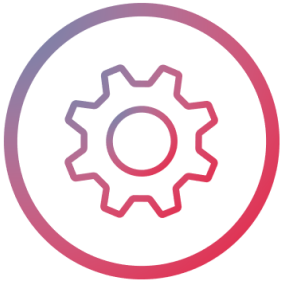
Development Tools

Babel Presets, Webpack and Linter Configs

Splunk Web Platform

Highlights and Development Principles

Modular



Use only what you need and update only when you want

Composable

Mix and match components for your exact use case

Accessible

WCAG 2.0 AA Compliant

Secure

Same security standards as Splunk products

Will more customers benefit from our framework?

My Question

Interested?

Let us know!

With your feedback, we hope to:

- Understand Needs of Splunk's Developer Community
- Gauge Interest in React-based Framework
- Evaluate Areas for Improvement
- Determine Need for Public Release and Timeline

To learn more about Splunk Web Platform

Join our Slack workspace (#webplatform):

splunkdevplatform.slack.com

Or Email:

webplatform@splunk.com

with your name, company, project idea and timeline.

Acknowledgements

- JPL CyberSAM team
- JPL CSIP Project
- JPL Splunk Admin Team

The research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration (80NM0018D0004).

Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement by the United States Government or the Jet Propulsion Laboratory, California Institute of Technology.

Jet Propulsion Laboratory
California Institute of Technology

jpl.nasa.gov