Splunking the 2018 Midterm Elections!

Corey Marshall | Splunk for Good Director
Satoshi Kawasaki | Splunk for Good Ninja

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. 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. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL 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. © 2019 Splunk Inc. All rights reserved.

Bio: Corey Marshall

Splunk for Good Director

BA in Political Science from Lewis & Clark College

Master's in Public Policy from the University of Chicago

- Advising government and non-profits on open data for more than 15 years, including working with
  - City and County of San Francisco
  - Accenture
  - Office of Chicago Mayor Richard M. Daley
- Joined Splunk in 2013
- Lead company’s efforts in
  - Employee service and engagement
  - Community giving
  - Social impact initiatives

Bio: Satoshi Kawasaki

BS in Aerospace Engineering from Georgia Tech

hobbes3

- Joined Splunk in 2013
  - 3 years in Splunk Professional Services (PS)
  - 3+ years in Splunk for Good
- Previous conf talks:
  - conf14: *I want that cool viz in Splunk!*
  - conf15: *Enhancing dashboards with javascript!*
  - conf17: *Speed up your searches!*
  - conf17: *Splunking to fight human trafficking!*
  - conf17: *Splunking the 2016 presidential election!*
- This year's conf talks:
  - conf19: *Speed up your searches!*

    YOU ARE HERE
  - conf19: *Splunking refugees with help from NetHope and Cisco!*
  - conf19: *Splunking the 2018 midterm election!*

© 2019 SPLUNK INC.

Splunk for Good

Big data can make a big difference

- $100 million Splunk Pledge has issued licenses and training worth over $40 million.
- Provide workforce training to veterans and opportunity youth to train the workforce of tomorrow.
- Engaging our partners in initiatives to promote STEM and develop shared solutions for humanitarian response and human trafficking.
- Supporting life-changing research at top universities.
- More than 100k hours of paid volunteer time.

WOUNDED WARRIOR PROJECT

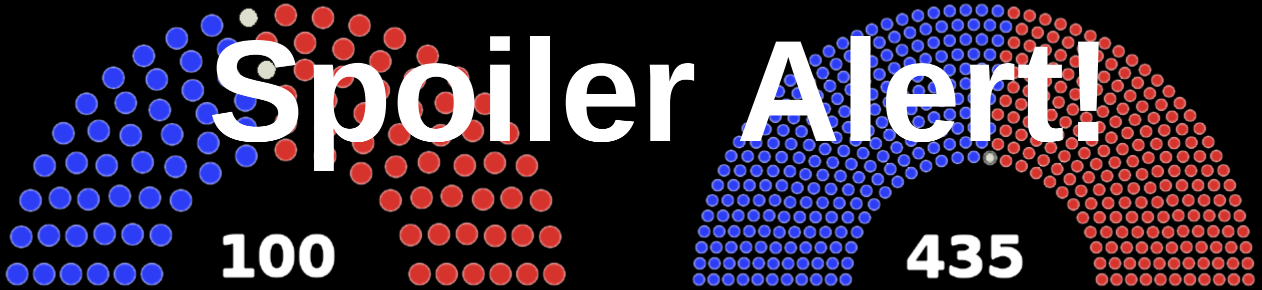
NETHOPE

TEAM RUBICON

npower

© 2019 SPLUNK INC.

2018 midterm election



Spoiler Alert!

elections.splunkforgood.com

The 2016 presidential election also available!

© 2019 SPLUNK INC.

Our goals and requirements

Goals

- Publically showcase Splunk's ability to ingest and analyze non-traditional[1] and open data
- Show how Splunk can correlate data from different sources
- Provide a meaningful story or discovery

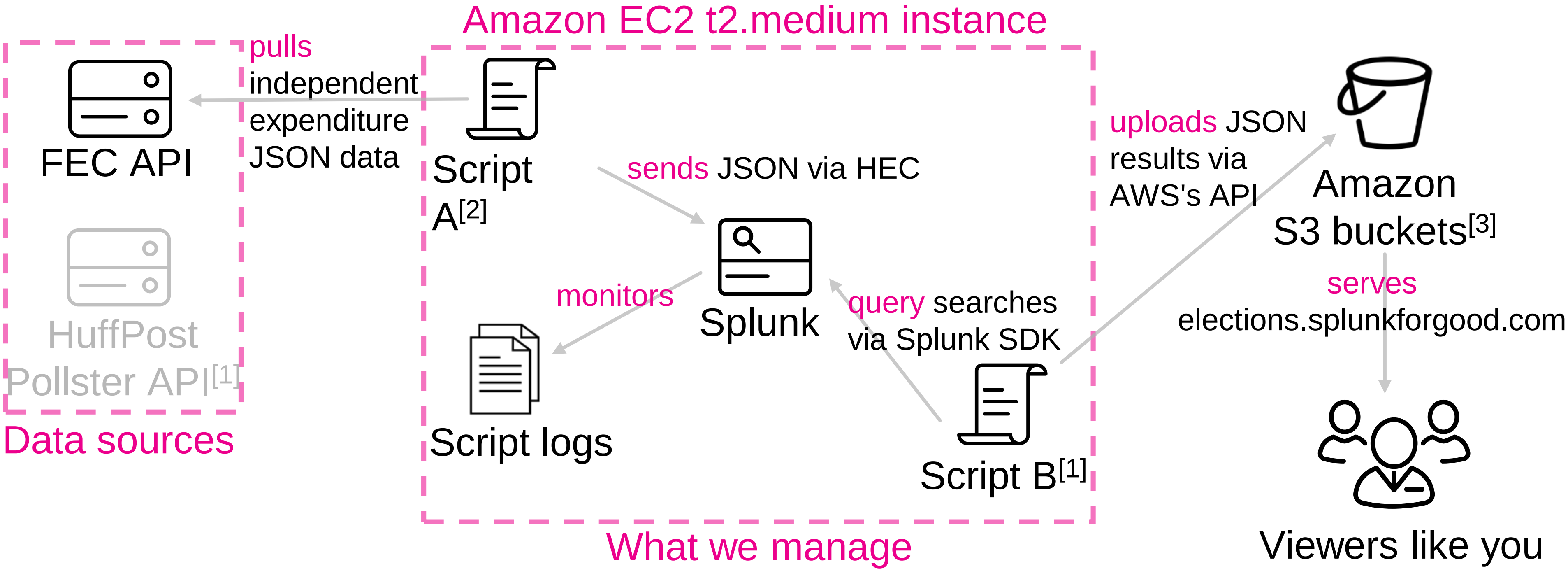
Requirements

- Create a *public-facing* website
- Scale to handle public traffic
- Try to be unbiased and neutral
- Show off some custom, kick-ass visualizations

[1]Not security or IT data

© 2019 SPLUNK INC.

The architecture


Amazon EC2 t2.medium instance
FEC API
HuffPost Pollster API[1]
Data sources
pulls independent expenditure JSON data
Script A[2]
sends JSON via HEC
Splunk
monitors
Script logs
query searches via Splunk SDK
Script B[1]
What we manage
uploads JSON results via AWS's API
Amazon S3 buckets[3]
serves elections.splunkforgood.com
Viewers like you

[1]Only for the 2016 presidential election website.
[2]Custom Python scripts that runs on a schedule.
[3]Hosting html, css, and javascript as a static website (Amazon managed service).

© 2019 SPLUNK INC.

The easy[1] steps

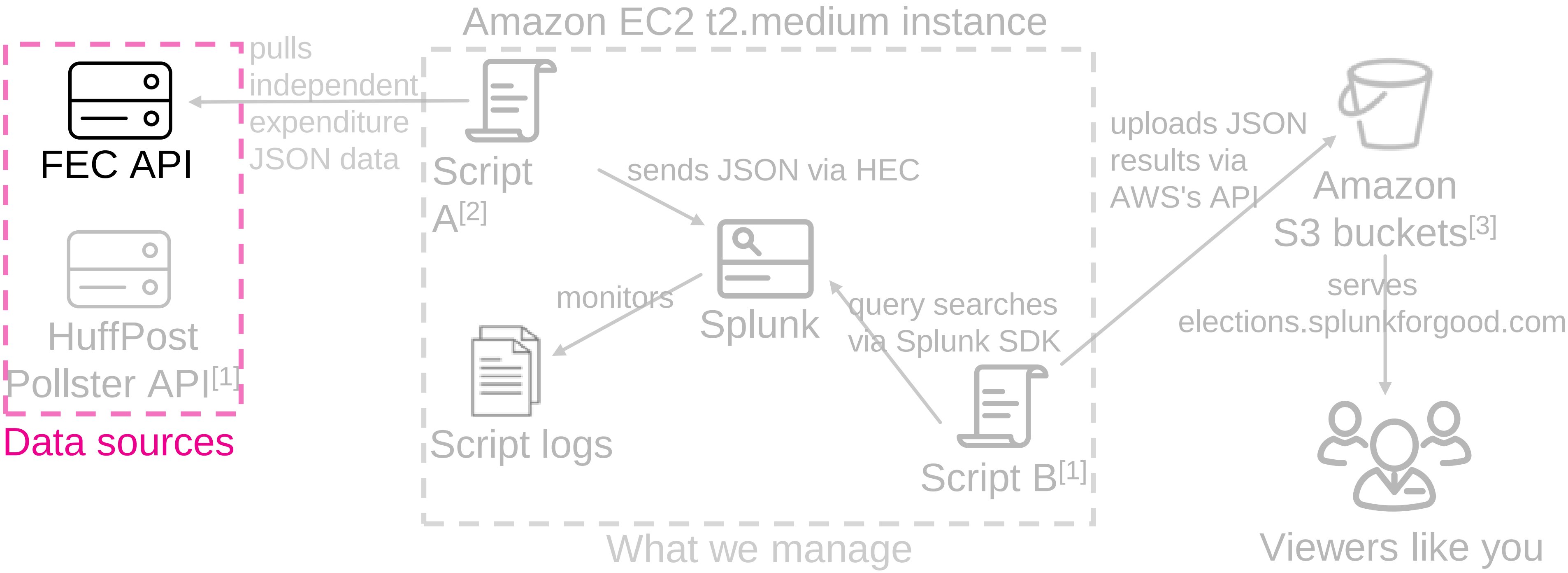
How to go from a private Splunk instance to a public website

1. Preview the data
2. Pull the data
3. Send the data
4. Upload the data
5. Serve the data

[1] It's actually not that easy

© 2019 SPLUNK INC.

Step 1: Preview the data


Amazon EC2 t2.medium instance
pulls independent expenditure JSON data
FEC API
HuffPost Pollster API[1]
Data sources
Script A[2]
sends JSON via HEC
Splunk
monitors
Script logs
query searches via Splunk SDK
Script B[1]
uploads JSON results via AWS's API
Amazon S3 buckets[3]
serves elections.splunkforgood.com
Viewers like you
What we manage

© 2019 SPLUNK INC.

Data source: Federal Election Commission (FEC)

- FEC is an independent regulatory agency whose purpose is to enforce campaign finance law in federal elections.
- We focused on two main types of donations:
    - Individual donations (`schedule_a`)
    - Independent expenditures (`schedule_e`) of the "Super PACs"[1]
- Provides campaign finance data at https://www.fec.gov/data/.
- Also provides a documented REST API on the same dataset at https://api.open.fec.gov/developers/.

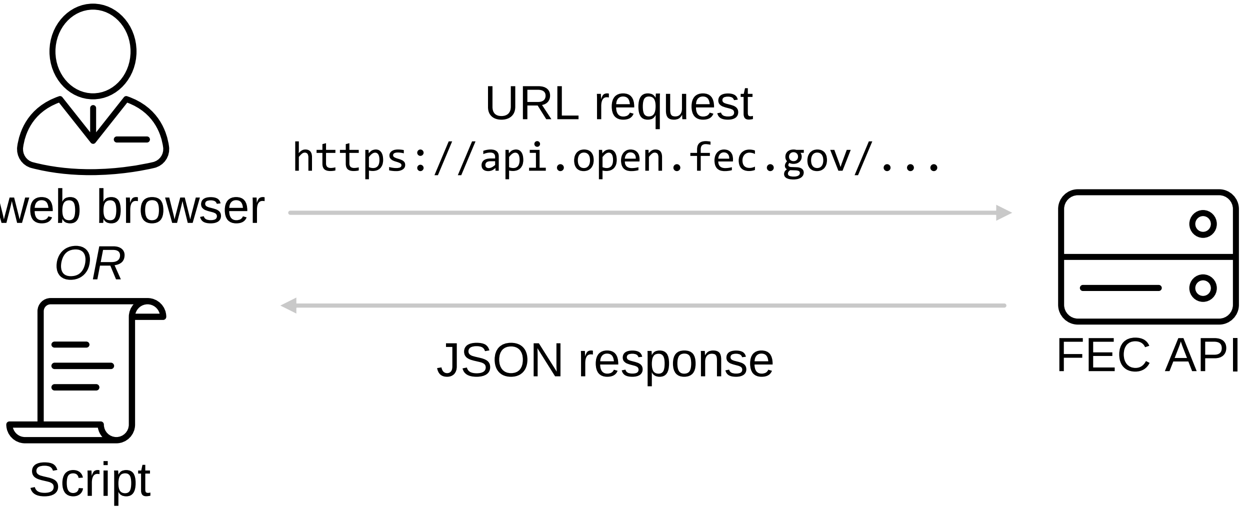
[1] The creation of the Super PACs came from the landmark ruling of *Citizens United v. FEC (2010)*.

© 2019 SPLUNK INC.

What is a REST API?

A website for scripts

A REST API is a set of URL endpoints to GET or POST text via http(s), ie a web browser.



Example URL:

`https://api.open.fec.gov/v1/candidate/P80001571/?api_key=DEMO_KEY`

© 2019 SPLUNK INC.

Example: REST API URL

Find the correct URL from the API documentation

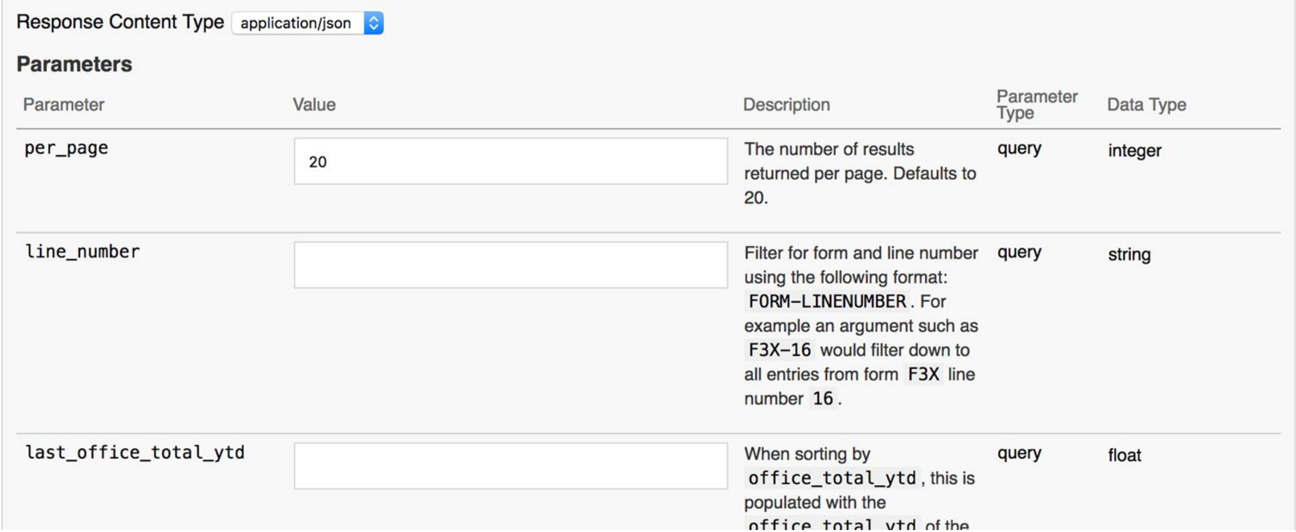
Base URL

Endpoint

```
https://api.open.fec.gov/v1/schedules/schedule_e/?candidate_id=P80001571
&per_page=100&is_notice=false&cycle=2016&api_key=DEMO_KEY
```

Parameters (starts after ? and separated by &)

Key/Authentication (optional, also sometimes in the header instead)



Response Content Type application/json

Parameters

Parameter	Value	Description	Parameter Type	Data Type
per_page	20	The number of results returned per page. Defaults to 20.	query	integer
line_number		Filter for form and line number using the following format: `FORM-LINENUMBER`. For example an argument such as `F3X-16` would filter down to all entries from form `F3X` line number `16`.	query	string
last_office_total_ytd		When sorting by `office_total_ytd`, this is populated with the `office_total_ytd` of the	query	float

© 2019 SPLUNK INC.

REST API response

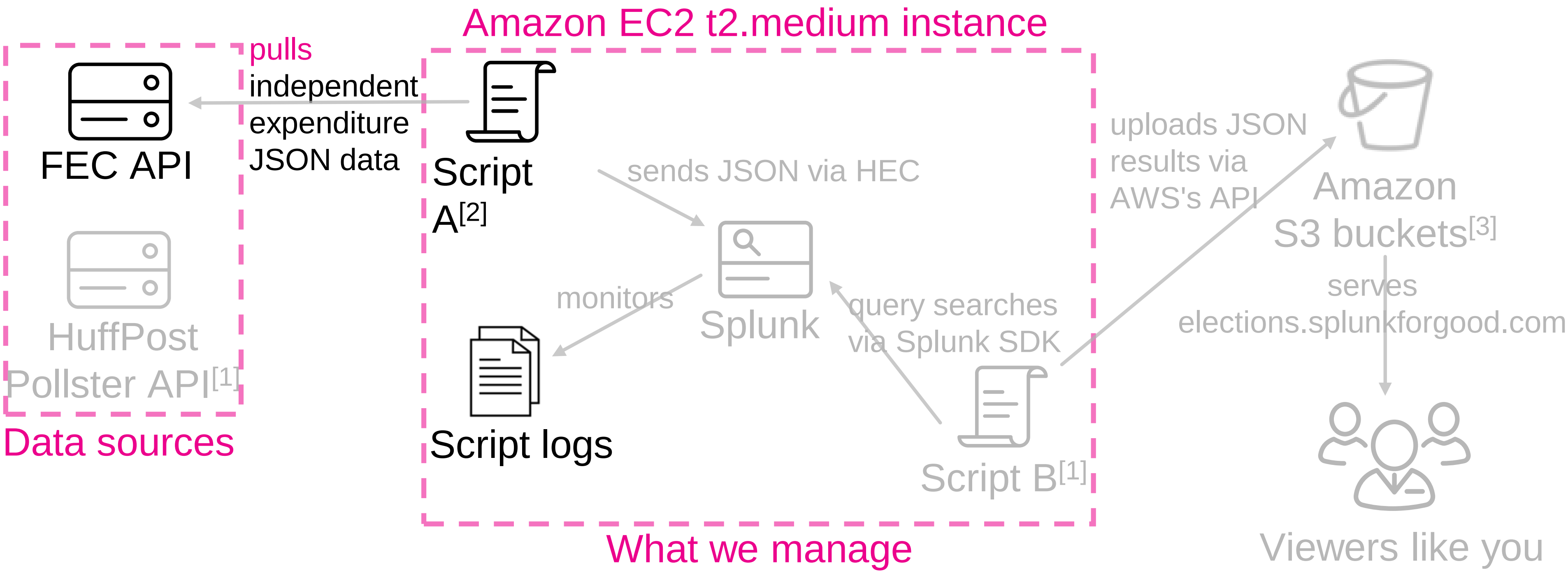
The JSON response

```
{"api_version":"1.0","pagination":{"count":18207,"pages":183,"last_indexes":{"last_index":"4010420171358323494","last_expenditure_date":"201
6-11-28T00:00:00"},"per_page":100},"results":[{"payee_name":"ACTBLUE TECHNICAL
SERVICES","office_total_ytd":603.07,"conduit_committee_id":"C00626234","payee_street_1":"366 SUMMER
STREET","report_type":"YE","expenditure_description":"CREDIT CARD PROCESSING
FEES","filer_suffix":null,"original_sub_id":null,"conduit_committee_street1":null,"conduit_committee_name":null,"image_number":"201701319042
196565","payee_suffix":null,"conduit_committee_city":null,"conduit_committee_zip":null,"payee_prefix":null,"independent_sign_name":"RANDOLPH
,
SUSANNAH","expenditure_amount":18.74,"back_reference_transaction_id":null,"file_number":1144979,"payee_middle_name":null,"cand_office_state"
:null,"expenditure_date":"2016-12-
31T00:00:00","memo_code_full":null,"cand_office_district":null,"report_year":2016,"candidate_id":"P80001571","candidate_prefix":null,"notary
_sign_name":null,"filer_first_name":"SUSANNAH","filing_form":"F3X","action_code_full":"ADD","category_code":"001","candidate_first_name":"DO
NALD","filer_last_name":"RANDOLPH","committee_id":"C00626234","candidate_suffix":null,"memoed_subtotal":false,"payee_city":"SOMERVILLE","ele
ction_type":"G2020","filer_prefix":null,"candidate_last_name":"TRUMP","payee_zip":"021443132","schedule_type":"SE","conduit_committee_state"
:null,"payee_state":"MA","conduit_committee_street2":null,"filer_middle_name":null,"candidate":{"two_year_period":2016.0,"idx":88448,"candid
ate_id":"P80001571"},"payee_first_name":null,"schedule_type_full":"ITEMIZED INDEPENDENT EXPENDITURES","dissemination_date":"2016-12-
21T00:00:00","notary_commission_expiration_date":null,"link_id":4013120171369074356,"candidate_middle_name":"J","election_type_full":null,"a
ction_code":"A","is_notice":false,"payee_last_name":null,"support_oppose_indicator":"S","memo_code":null,"pdf_url":"http:\/\/docquery.fec.go
v\/cgi-
bin\/fecimg\/?201701319042196565","payee_street_2":null,"line_number":"24","committee":{"city":"ORLANDO","party_full":null,"street_1":"701
DELANEY PARK DRIVE","cycles":[2018,2016],"party":null,"candidate_ids":[],"committee_type_full":"Super PAC (Independent Expenditure-
Only)","street_2":null,"organization_type":null,"zip":"32806","designation":"U","cycle":2016,"treasurer_name":"SUSANNAH
RANDOLPH","designation_full":"Unauthorized","state":"FL","organization_type_full":null,"committee_id":"C00626234","state_full":"Florida","co
mmittee_type":"O","name":"HELPING ELECT REFORMERS"},"sub_id":"4021020171370394552","independent_sign_date":"2017-01-
31T00:00:00","memo_text":null,"notary_sign_date":null,"back_reference_schedule_name":null,"candidate_office":"P","category_code_full":"Admin
istrative\/Salary\/Overhead Expenses ","candidate_name":"TRUMP, DONALD J"},{"payee_name":"WESTERN TRAILS GUN AND KNIFE
SHOWS","office_total_ytd":9315895.8800000008,"conduit_committee_id":"C00580100","payee_street_1":"ATTN: KARL
LANGE","report_type":"YE","expenditure_description":"VOID - BOOTH RENTAL - EVENT
CANCELLED","filer_suffix":null,"original_sub_id":null,"conduit_committee_street1":null,"conduit_committee_name":null,"image_number":"2017050
49053505223","payee_suffix":null,"conduit_committee_city":null,"conduit_committee_zip":null,"cand_office_state":null,"independent_sign_name"
:"ADKINS, MARY ROSE","expenditure_amount":-9.17,"back_reference_transaction_id":null,"file_number":1161245,"payee_middle_name":null
```

....

© 2019 SPLUNK INC.

Step 2: Pull the data


Amazon EC2 t2.medium instance
FEC API
pulls independent expenditure JSON data
Script A[2]
sends JSON via HEC
Splunk
monitors
Script logs
query searches via Splunk SDK
Script B[1]
uploads JSON results via AWS's API
Amazon S3 buckets[3]
serves elections.splunkforgood.com
Viewers like you
HuffPost Pollster API[1]
Data sources
What we manage

© 2019 SPLUNK INC.

Paginate for complete results

FEC API is limited up to 100 results per response

```
{"api_version":"1.0","pagination":{"count":18207,"pages":183,"last_indexes":{"last_index":"4010420171358323494","last_expenditure_date":"201
6-11-28T00:00:00"}},"per_page":100},"results":[{"payee_name":"ACTBLUE TECHNICAL
SERVICES","office_total_ytd":603.07,"conduit_committee_id":"C00626234","payee_street_1":"366 SUMMER
STREET","report_type":"YE","expenditure_description":"CREDIT CARD PROCESSING
FEES","filer_suffix":null,"original_sub_id":null,"conduit_committee_street1":null,"conduit_committee_name":null,"image_number":"201701319042
196565","payee_suffix":null,"conduit_committee_city":null,"conduit_committee_zip":null,"payee_prefix":null,"independent_sign_name":"RANDOLPH
,
SUSANNAH","expenditure_amount":18.74,"back_reference_transaction_id":null,"file_number":1144979,"payee_middle_name":null,"cand_office_state"
:null,"expenditure_date":"2016-12-
31T00:00:00","memo_code_full":null,"cand_office_district":null,"report_year":2016,"candidate_id":"P80001571","candidate_prefix":null,"notary
_sign_name":null,"filer_first_name":"SUSANNAH","filing_form":"F3X","action_code_full":"ADD","category_code":"001","candidate_first_name":"DO
NALD","filer_last_name":"RANDOLPH","committee_id":"C00626234","candidate_suffix":null,"memoed_subtotal":false,"payee_city":"SOMERVILLE","ele
ction_type":"G2020","filer_prefix":null,"candidate_last_name":"TRUMP","payee_zip":"021443132","schedule_type":"SE","conduit_committee_state"
:null,"payee_state":"MA","conduit_committee_street2":null,"filer_middle_name":null,"candidate":{"two_year_period":2016.0,"idx":88448,"candid
ate_id":"P80001571"},"payee_first_name":null,"schedule_type_full":"ITEMIZED INDEPENDENT EXPENDITURES","dissemination_date":"2016-12-
21T00:00:00","notary_commission_expiration_date":null,"link_id":4013120171369074356,"candidate_middle_name":"J","election_type_full":null,"a
ction_code":"A","is_notice":false,"payee_last_name":null,"support_oppose_indicator":"S","memo_code":null,"pdf_url":"http:\/\/docquery.fec.go
v\/cgi-
bin\/fecimg\/?201701319042196565","payee_street_2":null,"line_number":"24","committee":{"city":"ORLANDO","party_full":null,"street_1":"701
DELANEY PARK DRIVE","cycles":[2018,2016],"party":null,"candidate_ids":[],"committee_type_full":"Super PAC (Independent Expenditure-
Only)","street_2":null,"organization_type":null,"zip":"32806","designation":"U","cycle":2016,"treasurer_name":"SUSANNAH
RANDOLPH","designation_full":"Unauthorized","state":"FL","organization_type_full":null,"committee_id":"C00626234","state_full":"Florida","co
mmittee_type":"O","name":"HELPING ELECT REFORMERS"},"sub_id":"4021020171370394552","independent_sign_date":"2017-01-
31T00:00:00","memo_text":null,"notary_sign_date":null,"back_reference_schedule_name":null,"candidate_office":"P","category_code_full":"Admin
istrative\/Salary\/Overhead Expenses ","candidate_name":"TRUMP, DONALD J"},{"payee_name":"WESTERN TRAILS GUN AND KNIFE
SHOWS","office_total_ytd":9315895.8800000008,"conduit_committee_id":"C00580100","payee_street_1":"ATTN: KARL
LANGE","report_type":"YE","expenditure_description":"VOID - BOOTH RENTAL - EVENT
CANCELLED","filer_suffix":null,"original_sub_id":null,"conduit_committee_street1":null,"conduit_committee_name":null,"image_number":"2017050
49053505223","payee_suffix":null,"conduit_committee_city":null,"conduit_committee_zip":null,"cand_office_state":null,"independent_sign_name"
:"ADKINS, MARY ROSE","expenditure_amount":-9.17,"back_reference_transaction_id":null,"file_number":1161245,"payee_middle_name":null
.........
```

© 2019 SPLUNK INC.

FEC API calls

Script A paginates to get the full result

Python - `import requests` and `import json` and a simple `while` loop.

```
https://api.open.fec.gov/v1/schedules/schedule_e/?candidate_id=P80001571
&per_page=100&is_notice=false&cycle=2016&api_key=DEMO_KEY
```

↓ to fetch the next set of results

```
https://api.open.fec.gov/v1/schedules/schedule_e/?candidate_id=P80001571
&per_page=100&is_notice=false&cycle=2016&api_key=DEMO_KEY&last_index=401
0420171358323494&last_expenditure_date=2016-11-28T00:00:00
```

↓ to fetch the next set of results

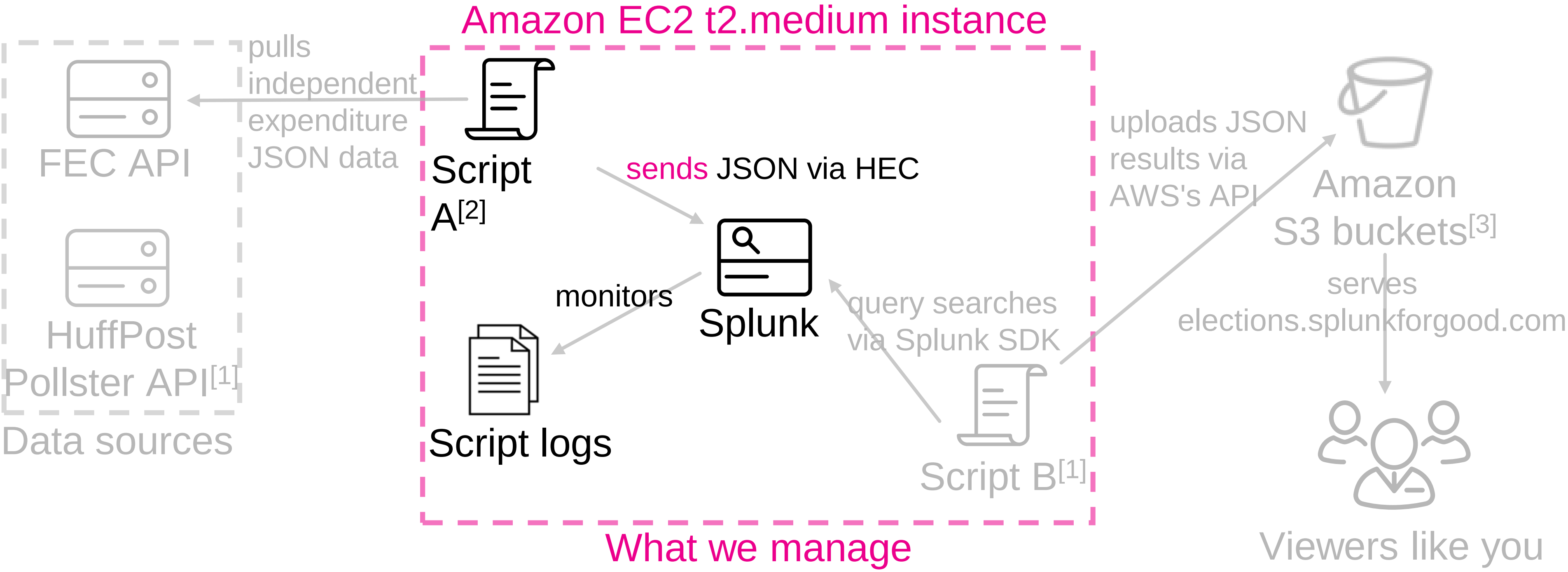
```
https://api.open.fec.gov/v1/schedules/schedule_e/?candidate_id=P80001571
&per_page=100&is_notice=false&cycle=2016&api_key=DEMO_KEY&last_index=402
1020171370392792&last_expenditure_date=2016-11-08T00:00:00
```

↓ to fetch the next set of results

Script A repeats until finished (takes about 200 times)

© 2019 SPLUNK INC.

Step 3: Send the data


Amazon EC2 t2.medium instance
FEC API
HuffPost Pollster API[1]
Data sources
pulls independent expenditure JSON data
Script A[2]
sends JSON via HEC
Splunk
monitors
Script logs
query searches via Splunk SDK
Script B[1]
uploads JSON results via AWS's API
Amazon S3 buckets[3]
serves elections.splunkforgood.com
Viewers like you
What we manage

© 2019 SPLUNK INC.

Send the data from JSON

Each JSON response has at most 100 Splunk event

```
{"api_version":"1.0","pagination":{"count":18207,"pages":183,"last_indexes":{"last_index":"4010420171358323494","last_expenditure_date":"201
6-11-28T00:00:00"},"per_page":100},"results":[{"payee_name":"ACTBLUE TECHNICAL
SERVICES","office_total_ytd":603.07,"conduit_committee_id":"C00626234","payee_street_1":"366 SUMMER
STREET","report_type":"YE","expenditure_description":"CREDIT CARD PROCESSING
FEES","filer_suffix":null,"original_sub_id":null,"conduit_committee_street1":null,"conduit_committee_name":null,"image_number":"201701319042
196565","payee_suffix":null,"conduit_committee_city":null,"conduit_committee_zip":null,"payee_prefix":null,"independent_sign_name":"RANDOLPH
,
SUSANNAH","expenditure_amount":18.74,"back_reference_transaction_id":null,"file_number":1144979,"payee_middle_name":null,"cand_office_state"
:null,"expenditure_date":"2016-12-
31T00:00:00","memo_code_full":null,"cand_office_district":null,"report_year":2016,"candidate_id":"P80001571","candidate_prefix":null,"notary
_sign_name":null,"filer_first_name":"SUSANNAH","filing_form":"F3X","action_code_full":"ADD","category_code":"001","candidate_first_name":"DO
NALD","filer_last_name":"RANDOLPH","committee_id":"C00626234","candidate_suffix":null,"memoed_subtotal":false,"payee_city":"SOMERVILLE","ele
ction_type":"G2020","filer_prefix":null,"candidate_last_name":"TRUMP","payee_zip":"021443132","schedule_type":"SE","conduit_committee_state"
:null,"payee_state":"MA","conduit_committee_street2":null,"filer_middle_name":null,"candidate":{"two_year_period":2016.0,"idx":88448,"candid
ate_id":"P80001571"},"payee_first_name":null,"schedule_type_full":"ITEMIZED INDEPENDENT EXPENDITURES","dissemination_date":"2016-12-
21T00:00:00","notary_commission_expiration_date":null,"link_id":4013120171369074356,"candidate_middle_name":"J","election_type_full":null,"a
ction_code":"A","is_notice":false,"payee_last_name":null,"support_oppose_indicator":"S","memo_code":null,"pdf_url":"http:\/\/docquery.fec.go
v\/cgi-
bin\/fecimg\/?201701319042196565","payee_street_2":null,"line_number":"24","committee":{"city":"ORLANDO","party_full":null,"street_1":"701
DELANEY PARK DRIVE","cycles":[2018,2016],"party":null,"candidate_ids":[],"committee_type_full":"Super PAC (Independent Expenditure-
Only)","street_2":null,"organization_type":null,"zip":"32806","designation":"U","cycle":2016,"treasurer_name":"SUSANNAH
RANDOLPH","designation_full":"Unauthorized","state":"FL","organization_type_full":null,"committee_id":"C00626234","state_full":"Florida","co
mmittee_type":"O","name":"HELPING ELECT REFORMERS"},"sub_id":"4021020171370394552","independent_sign_date":"2017-01-
31T00:00:00","memo_text":null,"notary_sign_date":null,"back_reference_schedule_name":null,"candidate_office":"P","category_code_full":"Admin
istrative\/Salary\/Overhead Expenses ","candidate_name":"TRUMP, DONALD J"},{"payee_name":"WESTERN TRAILS GUN AND KNIFE
SHOWS","office_total_ytd":9315895.8800000008,"conduit_committee_id":"C00580100","payee_street_1":"ATTN: KARL
LANGE","report_type":"YE","expenditure_description":"VOID - BOOTH RENTAL - EVENT
CANCELLED","filer_suffix":null,"original_sub_id":null,"conduit_committee_street1":null,"conduit_committee_name":null,"image_number":"2017050
49053505223","payee_suffix":null,"conduit_committee_city":null,"conduit_committee_zip":null,"cand_office_state":null,"independent_sign_name"
:"ADKINS, MARY ROSE","expenditure_amount":-9.17,"back_reference_transaction_id":null,"file_number":1161245,"payee_middle_name":null
.........
```

© 2019 SPLUNK INC.

What is Splunk HTTP Event Collector?

HEC is simply a REST API to POST events to Splunk directly.
You must enable and configure HEC in Splunk before sending data.

Python - Use a simple `for` loop to combine all expenditures and POST them all at once.

Header:

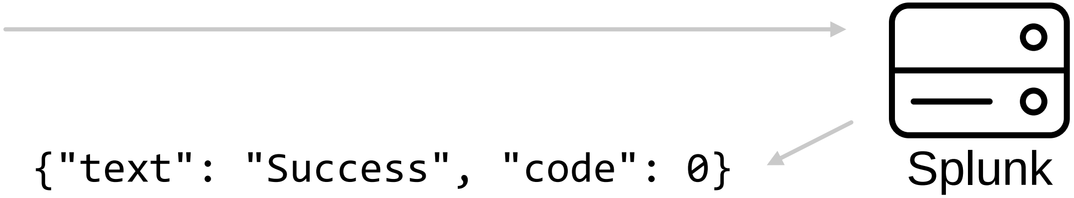
```
Authorization: Splunk B5A79AAD-...
```

Body[1]**:**

```
{
"index": "fec",
"sourcetype": "fec_schedule_e",
"time": 1568841992,
"event": {"payee_name":"ACTBLUE
TECHNICAL SERVICES",
"office_total_ytd":...}
}
{
"index": "fec",
...
```

URL request

`https://splunk.company.com:8088/services/collector`

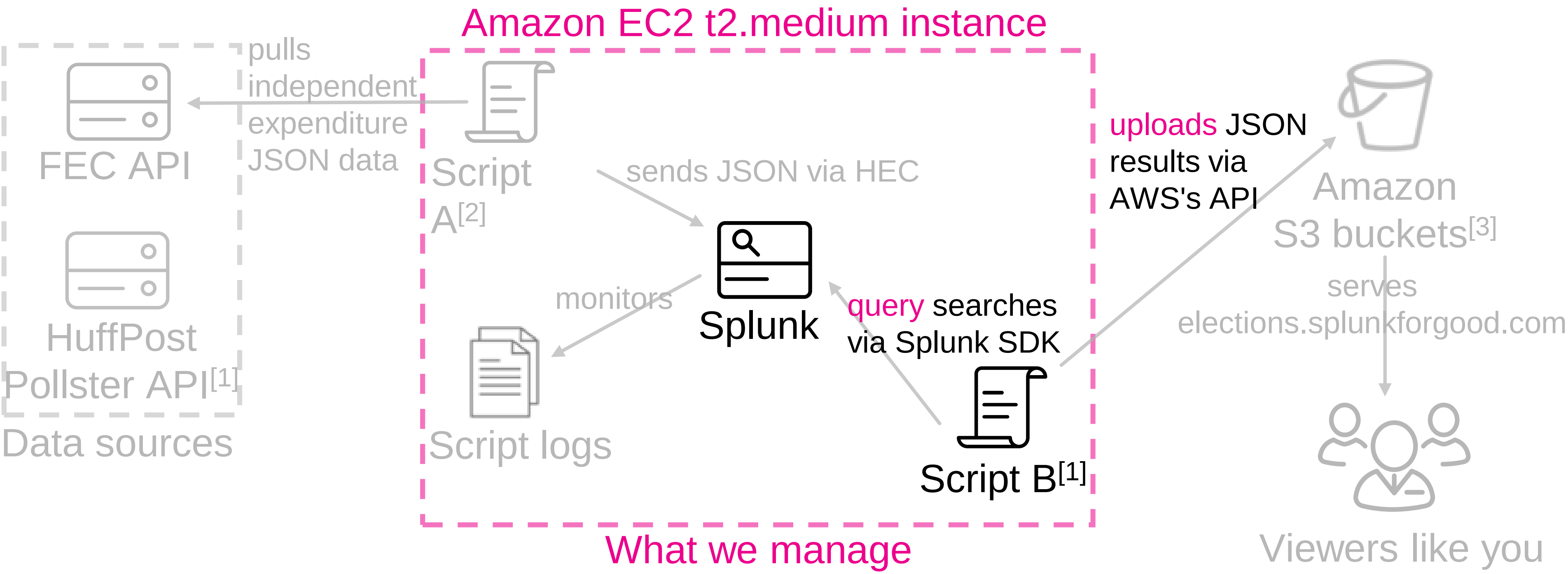


`{"text": "Success", "code": 0}`

[1] The entire body needs to be a string. The easiest way in Python is to do `json.dumps(hec_events)`.

© 2019 SPLUNK INC.

Step 4: Upload the data



Amazon EC2 t2.medium instance
pulls independent expenditure JSON data
FEC API
HuffPost Pollster API[1]
Data sources
Script A[2]
sends JSON via HEC
monitors
Script logs
Splunk
query searches via Splunk SDK
Script B[1]
uploads JSON results via AWS's API
Amazon S3 buckets[3]
serves elections.splunkforgood.com
Viewers like you
What we manage

© 2019 SPLUNK INC.

Running searches and uploading to S3

Script B does the following in Python:

1. Use the Splunk Python SDK to authenticate and create a "data cube" by running one, big `stats` search that returns an aggregated Splunk result in CSV[1].
   a. The search is basically the sum of expenditures by committee, toward (for/against), and candidate.
2. Use the AWS API to authenticate and upload that CSV to an AWS S3 bucket.

[1] We use a CSV since it takes up less size than the full JSON version that Splunk outputs.

© 2019 SPLUNK INC.

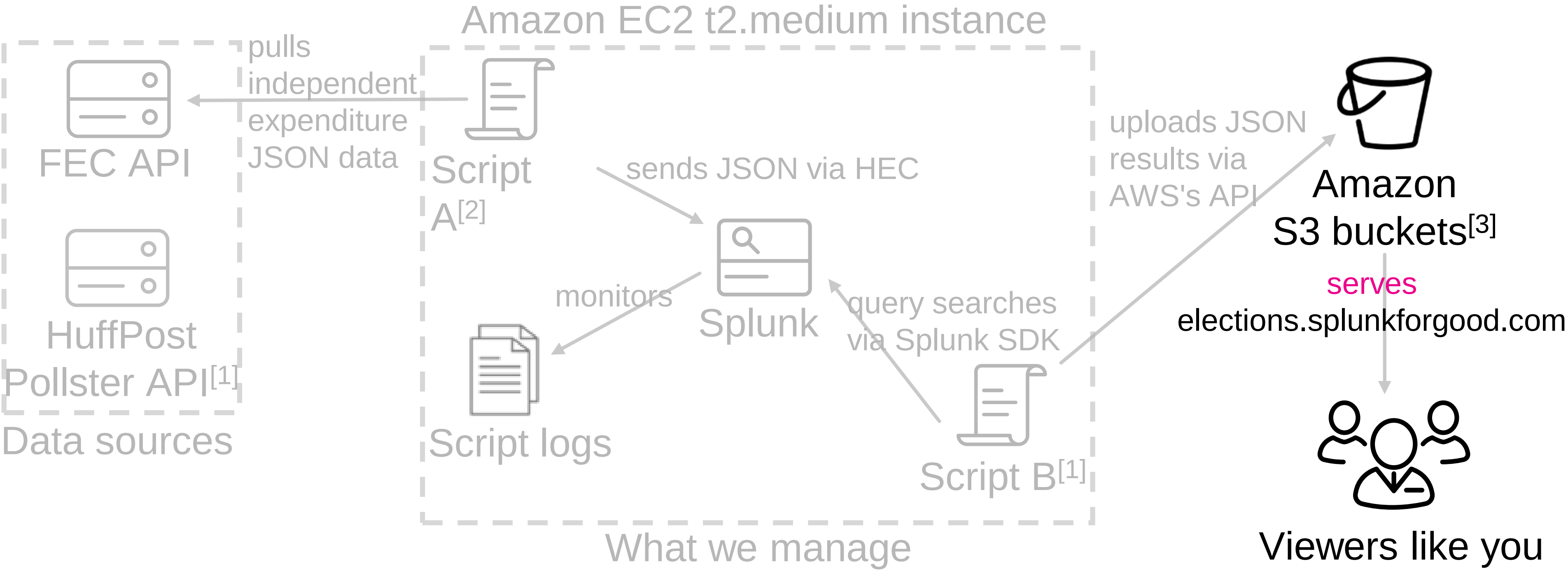
The Splunk search

Building a massive "data cube" to power all D3.js visualizations

```
| tstats sum(f.expenditure_amount) as spent first(f.total) first(f.committee_id) first(f.committee.name) first(f.toward)
first(f.candidate_id) first(f.name) first(f.office) first(f.state) first(f.party)
   from datamodel=fec_schedule_e by f.sub_id
| rename f.* as * first(f.*) as * | fillnull value=0 total
| append
   [| inputlookup candidates.csv
   | table candidate_id name office state party total
   | eval spent=0 | fillnull value="null" committee_id toward candidate_id ]
| lookup state state | lookup party party | lookup office office
| eval party_orig=party | eval party_full_orig=party_full | eval party=if(party="DEM" OR party="REP", party, "OTHERS")
| eval party_full=if(party="DEM" OR party="REP", party_full, "Others")
| stats sum(spent) as spent first(total) as total first(committee.name) first(name) first(office*) first(state*)
first(party*)
   by committee_id toward candidate_id
| rename first(*) as * | rename committee.name as outer name as inner toward as ribbon spent as count
| eval inner_img=candidate_id.".jpg"
| eval ribbon_color=case(ribbon="supporting", "#24a222", ribbon="opposing", "#d9d9d9", 0=0, "null")
| eval inner_color=case(party="REP", "#d8241e", party="DEM", "#1576b6", 0=0, "grey")
| eval outer_link="https://www.fec.gov/data/committee/".committee_id."/?cycle=2018"
| eval inner_link="https://www.fec.gov/data/candidate/".candidate_id."/?cycle=2018"
```

© 2019 SPLUNK INC.

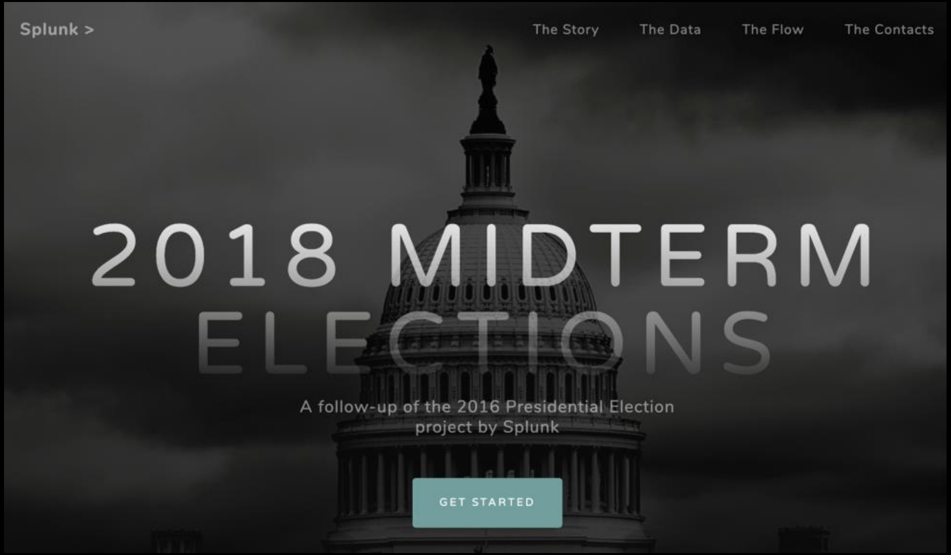
Step 5: Serve the data



© 2019 SPLUNK INC.

The website

HTML, JavaScript, and CSS



No need to reinvent the wheel when we can just search for existing free themes and styles!

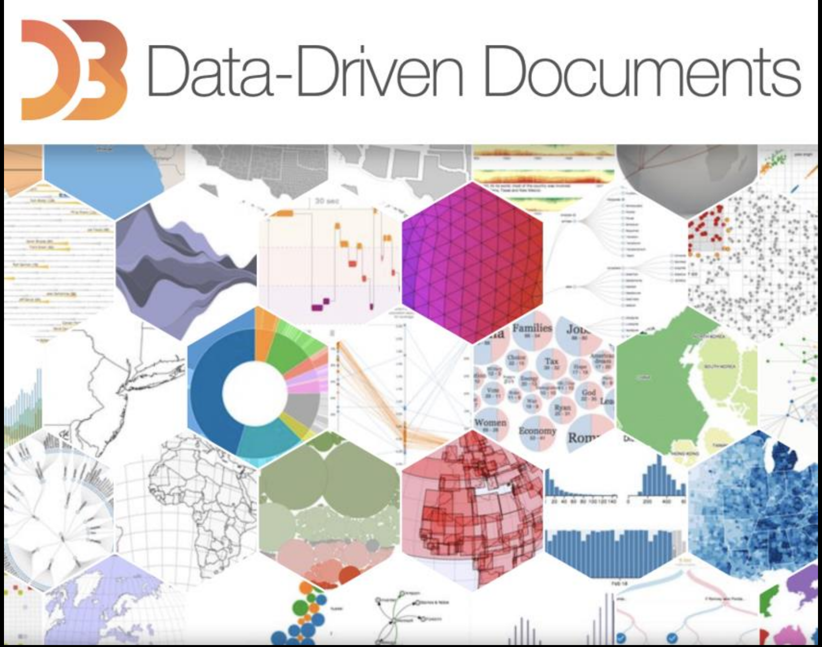
We modified a Bootstrap[1] theme called "Grayscale" by Blackrock Digital for the site.

[1]Bootstrap is a front-end framework by Twitter.

© 2019 SPLUNK INC.

D3.js

Ultimate control over visualization



D3.js is a JavaScript library to basically loop through the rows in data and create shapes (in <SVG>) based on the values.

However, D3.js doesn't use the GPU so plotting too much will slow down the web browser.

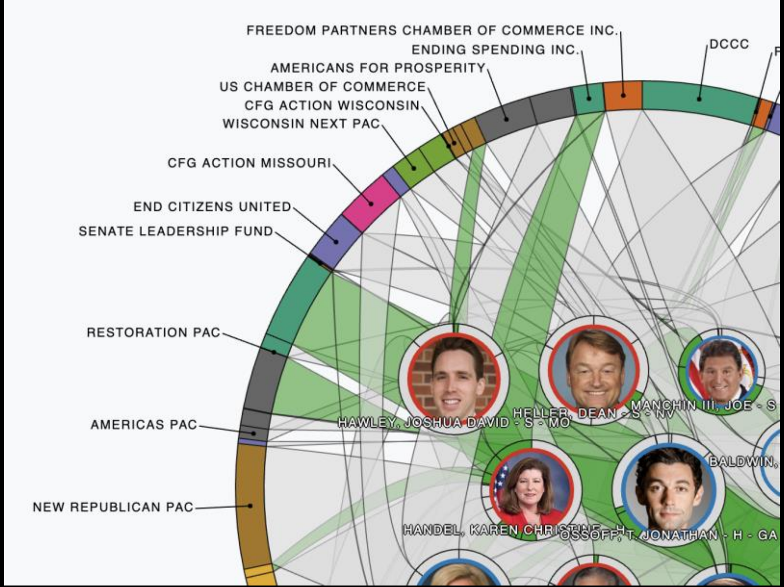
Almost all custom visualizations Splunk apps are written in D3.js.

D3.js is *not* easy... you must draw almost every line and shape from scratch. Your math- and coordinate-fu must be strong.

© 2019 SPLUNK INC.

The JavaScript (JS) libraries

Putting it all together



RequireJS loads all the necessary JS libraries:

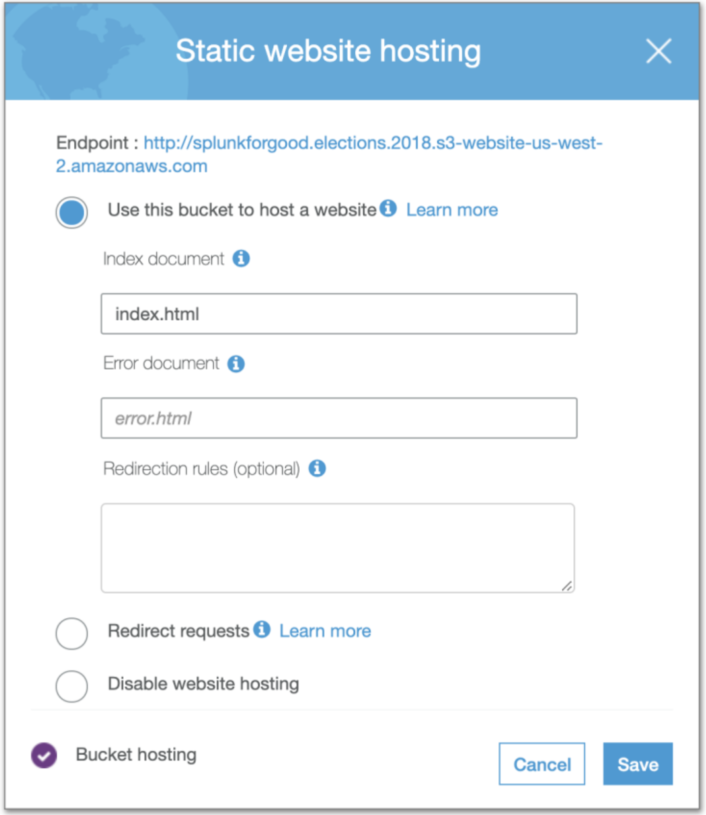
- D3.js
- jQuery (needed for Bootstrap)
- Underscore.js (a more powerful data query language for JavaScript)
- Moment.js (time string manipulation)

This visualization is available as an app called "Halo – Custom Visualization" on SplunkBase: https://splunkbase.splunk.com/app/3514/.

© 2019 SPLUNK INC.

Let Amazon handle the "web server"

Pay as you go



Static website hosting ✕

Endpoint : http://splunkforgood.elections.2018.s3-website-us-west-2.amazonaws.com

● Use this bucket to host a website ⓘ Learn more

Index document ⓘ

index.html

Error document ⓘ

error.html

Redirection rules (optional) ⓘ

○ Redirect requests ⓘ Learn more

○ Disable website hosting

✓ Bucket hosting

Cancel Save

S3 is a managed service, which means we don't need to administer, maintain, or scale our own web servers. But S3 can only host static files. But remember the "data cube" gets updated via Script B.

If we need even more performance, then we can use Amazon CloudFront (CDN) for multiple regional caching.

The website entire codebase, including the "data cube" is available at https://github.com/hobbes3/website_fec_2018 (replace 2018 with 2016 as well).

© 2019 SPLUNK INC.

Some data challenges

It gets even harder...

We have to pull the complete FEC results every time due to the pagination's new `last_index`. Normally it would make sense to use the JSON's `expenditure_date` as Splunk's `_time`, but repeatedly indexing overlapping historical data creates "bucket spread" and can slow down searches. So Splunk's `_time` is simply set to the current time.

The FEC has reporting deadlines, so the latest data isn't the most updated. Generally, summing up individual amounts usually doesn't equal the total aggregated sum reported by the FEC's other endpoints. You gain granularity of individual expenditures but lose accuracy...

Closing remarks

Corey Marshall | Splunk for Good Director

.conf19

splunk>

© 2019 SPLUNK INC.

As flexible as you think Splunk is…

Big data can make a big difference

Splunk is a powerful tool to explore interesting and impactful new use cases. There are lots of opportunities to make an impact with data and Splunk:

- Fascinating way to explore the impacts of money on our electoral system.
- Lots of open data available right under our noses, but very few are aware of it.
- Find ways to leverage open and public data sources to enrich your work.
- Showcase Splunk to an entirely new audience through compelling visualizations.

And there's always more we can do:

- Interesting use case that improves visibility and transparency.
- What other causes could benefit from Splunk expertise?

© 2019 SPLUNK INC.

.conf19®

splunk>®

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION

Q&A

Corey Marshall | Splunk for Good Director
Satoshi Kawasaki | Splunk for Good Ninja

.conf19
splunk>