Mason Competitive Cyber

Love our Logs: Using Splunk to Identify Threats and Patterns

Media Recording Notice

This meeting is more than likely recorded. Got a problem with that? Emit a sharp screech at the nearest exec now.

Upcoming Competitions & Events

- Cyber Fusion
  - Each college sends one team, ours is set this year
- BSidesNOVA
  - Team of 8, $20 registration fee, team full
- CryptoParty
  - March 3 10:30am to 6:00pm
  - Includes food, a little swag, a CTF w/ prizes, etc
  - Register and see schedule at cryptoparty.gmu.io

Know of other competitions? *Tell us**

Setting up our own Splunk

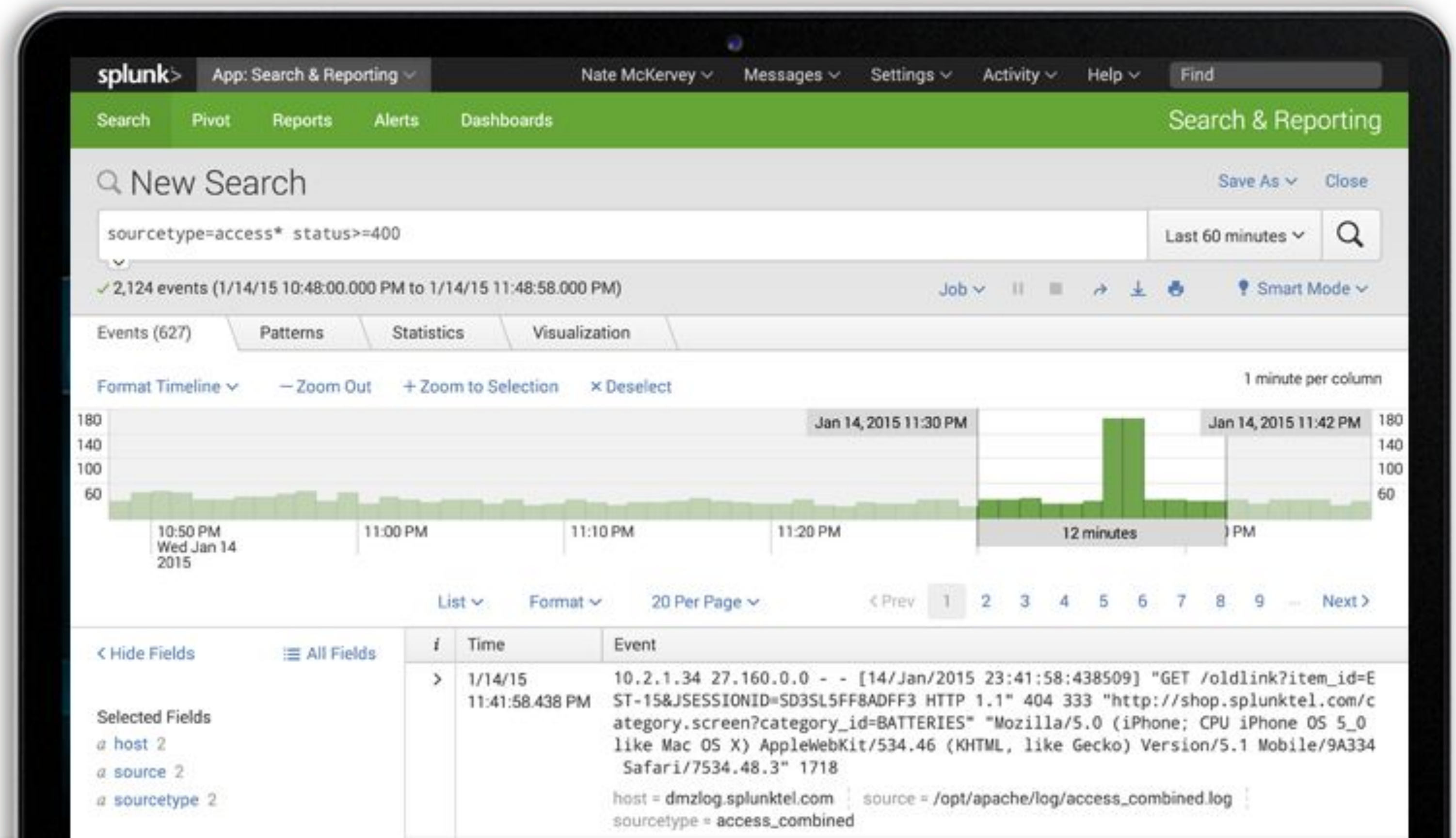
- **On Linux and installed/can install Docker?**
  - Install Docker
  - **Google "Docker Hub Splunk"**
  - Should be one or two commands, maybe docker pull and docker run, with a ton of flags
- **Otherwise**, google your OS along with splunk enterprise install
  - Windows has an installer
  - Linux also has an installer

Hopefully people with more success will be around to help

By the time it ends you should have something similar looking to the next slide

What are we covering?

- Splunk
  - Essentially “Google for your logs”
  - This isn’t a paid talk, we aren’t a sponsor



```
sourcetype=access* status>=400
```

✓ 2,124 events (1/14/15 10:48:00.000 PM to 1/14/15 11:48:58.000 PM)

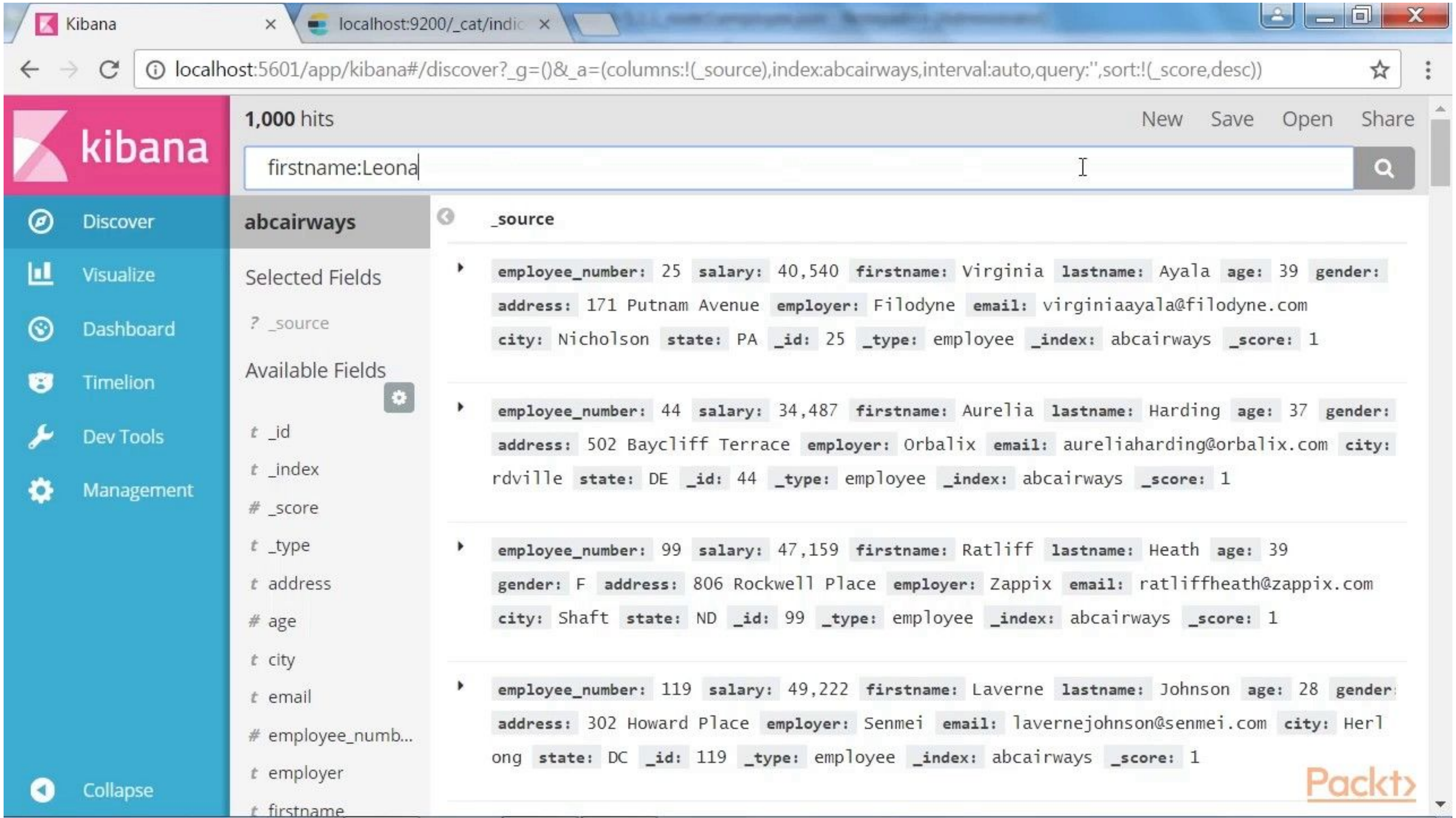
1/14/15
11:41:58.438 PM

```
10.2.1.34 27.160.0.0 - - [14/Jan/2015 23:41:58:438509] "GET /oldlink?item_id=E
ST-15&JSESSIONID=SD3SL5FF8ADFF3 HTTP 1.1" 404 333 "http://shop.splunktel.com/c
ategory.screen?category_id=BATTERIES" "Mozilla/5.0 (iPhone; CPU iPhone OS 5_0
like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9A334
 Safari/7534.48.3" 1718
```

host = dmzlog.splunktel.com | source = /opt/apache/log/access_combined.log
sourcetype = access_combined

Considering alternatives

- Most popular is an ELK stack
  - Elasticsearch, logstash, kibana



localhost:5601/app/kibana#/discover?_g=()&_a=(columns:!(_source),index:abcairways,interval:auto,query:'',sort:!(_score,desc))

1,000 hits

firstname:Leona

abcairways

Selected Fields

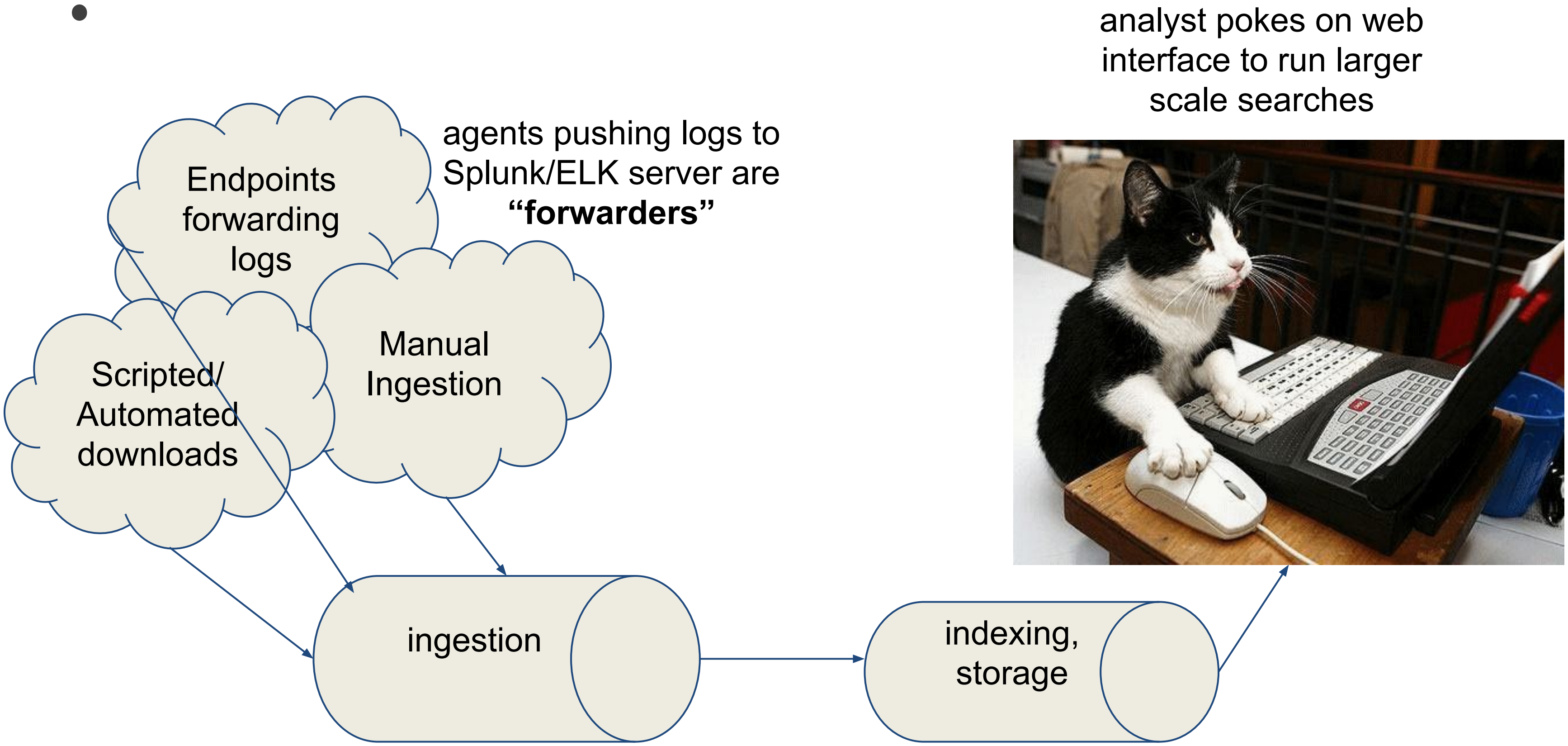
? _source

Available Fields

t _id
t _index
_score
t _type
t address
# age
t city
t email
# employee_numb...
t employer
t firstname

```
_source

employee_number: 25 salary: 40,540 firstname: Virginia lastname: Ayala age: 39 gender:
address: 171 Putnam Avenue employer: Filodyne email: virginiaayala@filodyne.com
city: Nicholson state: PA _id: 25 _type: employee _index: abcairways _score: 1

employee_number: 44 salary: 34,487 firstname: Aurelia lastname: Harding age: 37 gender:
address: 502 Baycliff Terrace employer: Orbalix email: aureliaharding@orbalix.com city:
rdville state: DE _id: 44 _type: employee _index: abcairways _score: 1

employee_number: 99 salary: 47,159 firstname: Ratliff lastname: Heath age: 39
gender: F address: 806 Rockwell Place employer: Zappix email: ratliffheath@zappix.com
city: Shaft state: ND _id: 99 _type: employee _index: abcairways _score: 1

employee_number: 119 salary: 49,222 firstname: Laverne lastname: Johnson age: 28 gender:
address: 302 Howard Place employer: Senmei email: lavernejohnson@senmei.com city: Herl
ong state: DC _id: 119 _type: employee _index: abcairways _score: 1
```

Similar Procedure



agents pushing logs to Splunk/ELK server are **“forwarders”**

analyst pokes on web interface to run larger scale searches

Forwarders

- Generally comes as a program, forwards a variety of configured logs to the Splunk server
  - Cross platform, “Splunk Universal Forwarder”
- Pushes it to an external port on the splunk server

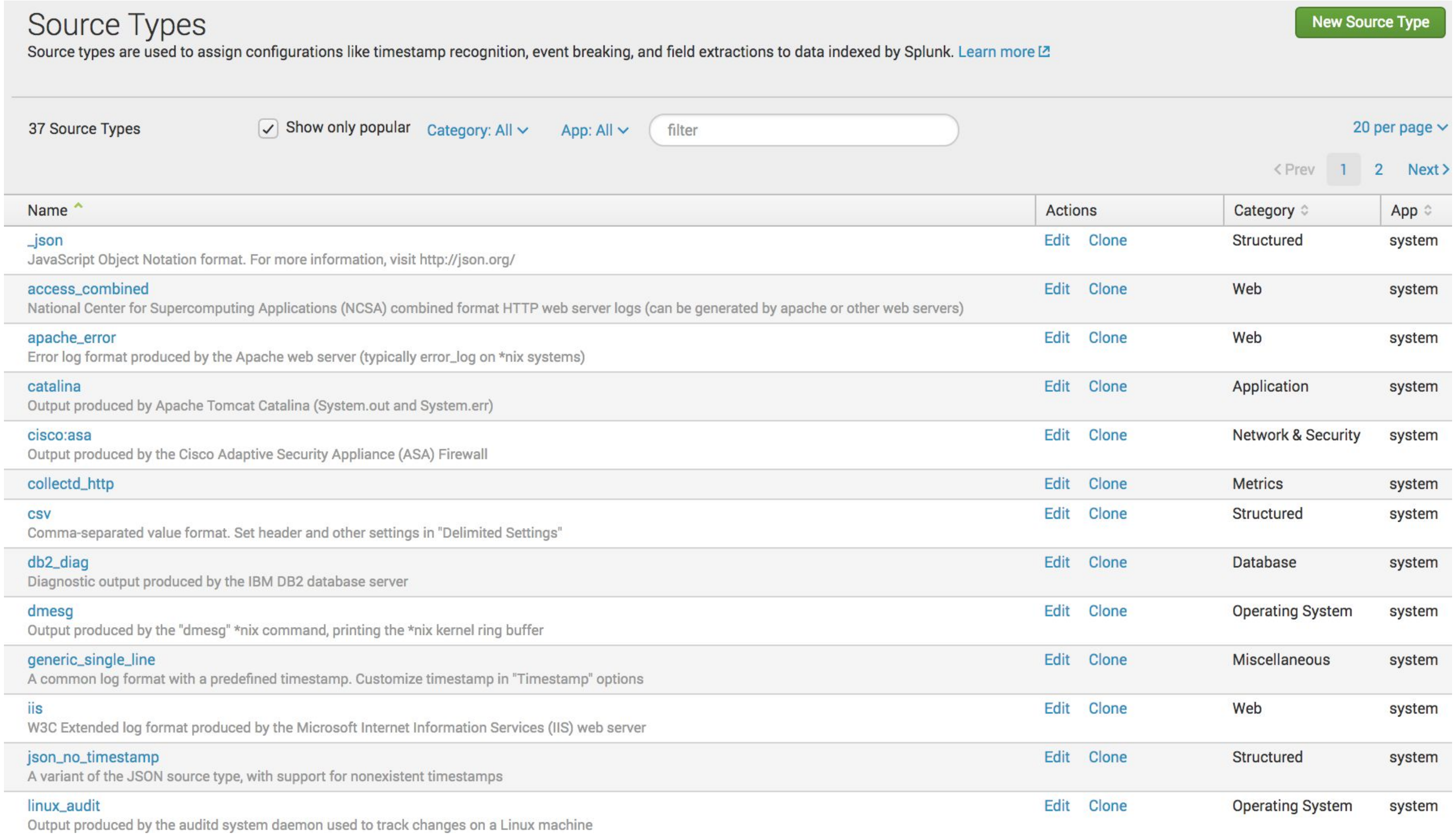
Sourcetypes

- **Super important**
  - Affects how things are formatted, for instance JSON
  - Affects what fields you can search
- Without them, and without manual field extraction, it's basically grep with visualizations

A default field that identifies the data structure of an event. A source type determines how Splunk Enterprise formats the data during the indexing process.

How to get them

- Configure them on the server in a config
- Install app
- “New” under Source Types, configuring regexes, breaks, etc



Source Types

Source types are used to assign configurations like timestamp recognition, event breaking, and field extractions to data indexed by Splunk. Learn more

37 Source Types

☑ Show only popular

Name	Actions	Category	App
_json JavaScript Object Notation format. For more information, visit http://json.org/	Edit Clone	Structured	system
access_combined National Center for Supercomputing Applications (NCSA) combined format HTTP web server logs (can be generated by apache or other web servers)	Edit Clone	Web	system
apache_error Error log format produced by the Apache web server (typically error_log on *nix systems)	Edit Clone	Web	system
catalina Output produced by Apache Tomcat Catalina (System.out and System.err)	Edit Clone	Application	system
cisco:asa Output produced by the Cisco Adaptive Security Appliance (ASA) Firewall	Edit Clone	Network & Security	system
collectd_http	Edit Clone	Metrics	system
csv Comma-separated value format. Set header and other settings in "Delimited Settings"	Edit Clone	Structured	system
db2_diag Diagnostic output produced by the IBM DB2 database server	Edit Clone	Database	system
dmesg Output produced by the "dmesg" *nix command, printing the *nix kernel ring buffer	Edit Clone	Operating System	system
generic_single_line A common log format with a predefined timestamp. Customize timestamp in "Timestamp" options	Edit Clone	Miscellaneous	system
iis W3C Extended log format produced by the Microsoft Internet Information Services (IIS) web server	Edit Clone	Web	system
json_no_timestamp A variant of the JSON source type, with support for nonexistent timestamps	Edit Clone	Structured	system
linux_audit Output produced by the auditd system daemon used to track changes on a Linux machine	Edit Clone	Operating System	system

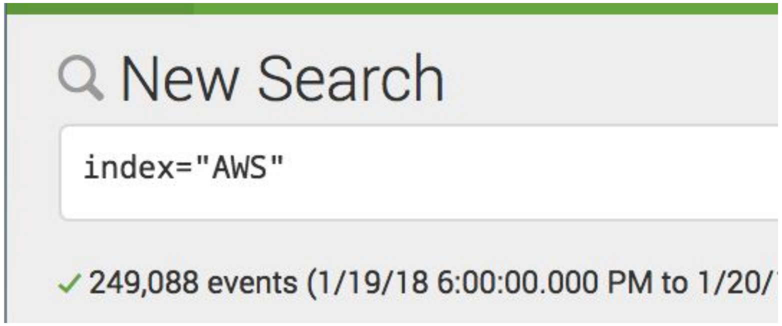
Consider more than just Splunk

- Collect as much as possible
- Normalize data as much as possible
  - Trying to add JSON, CSV, etc
- CSVs? Add headers
- Normalize times
  - At least be timezone aware

headers example:
→ ip address,date,time
172.31.4.4,11/04/2016,23:22

Indexes

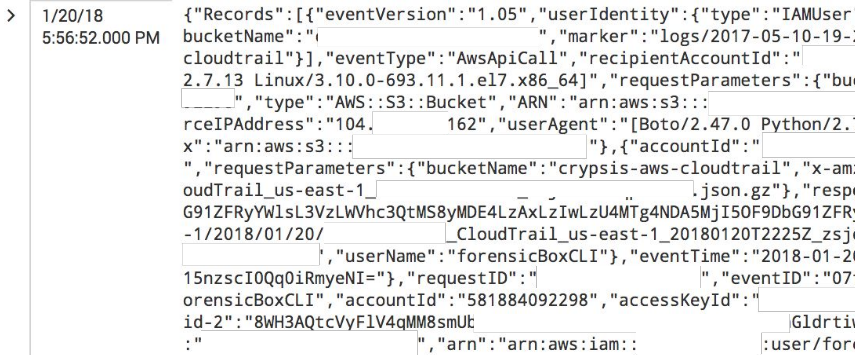
- Repository for data
- Good to have when you’re doing distinct sets, such as “endpoints” or “webservers”, etc
- You query at least one index when you search



New Search

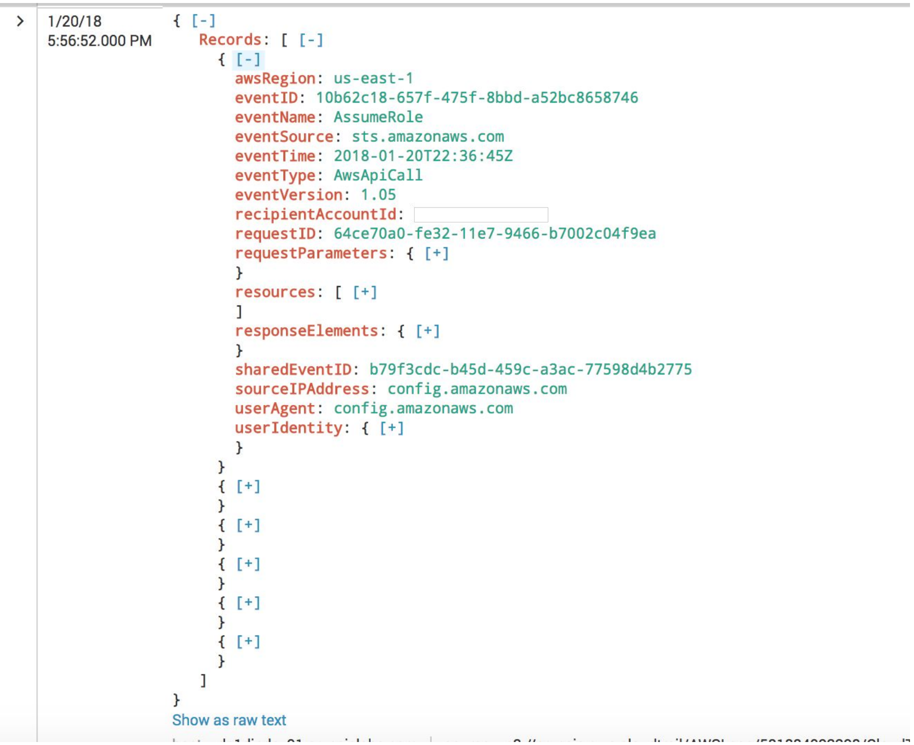
```
index="AWS"
```

✓ 249,088 events (1/19/18 6:00:00.000 PM to 1/20/



1/20/18
5:56:52.000 PM

```
{"Records":[{"eventVersion":"1.05","userIdentity":{"type":"IAMUser
bucketName":"[redacted]","marker":"logs/2017-05-10-19-
cloudtrail"}],"eventType":"AwsApiCall","recipientAccountId":"[redacted]
2.7.13 Linux/3.10.0-693.11.1.el7.x86_64]","requestParameters":{"bu
[redacted]","type":"AWS::S3::Bucket","ARN":"arn:aws:s3:::[redacted]
rceIPAddress":"104.[redacted]162","userAgent":"[Boto/2.47.0 Python/2.
x":"arn:aws:s3:::[redacted]"},{"accountId":"[redacted]
","requestParameters":{"bucketName":"crypsis-aws-cloudtrail","x-am
oudTrail_us-east-1_[redacted].json.gz"},"resp
G91ZFRyYWlsL3VzLWVhc3QtMS8yMDE4LzAxLzIwLzU4MTg4NDA5MjI5OF9DbG91ZFR
-1/2018/01/20/[redacted]_CloudTrail_us-east-1_20180120T2225Z_zsj
[redacted]","userName":"forensicBoxCLI"},"eventTime":"2018-01-2
15nzscIOQq0iRmyeNI="},"requestID":"[redacted]","eventID":"07
orensicBoxCLI","accountId":"581884092298","accessKeyId":"[redacted]
id-2":"8WH3AQtcVyFlV4qMM8smUb[redacted]Gldrti
:"[redacted]","arn":"arn:aws:iam::[redacted]:user/for
```



1/20/18
5:56:52.000 PM

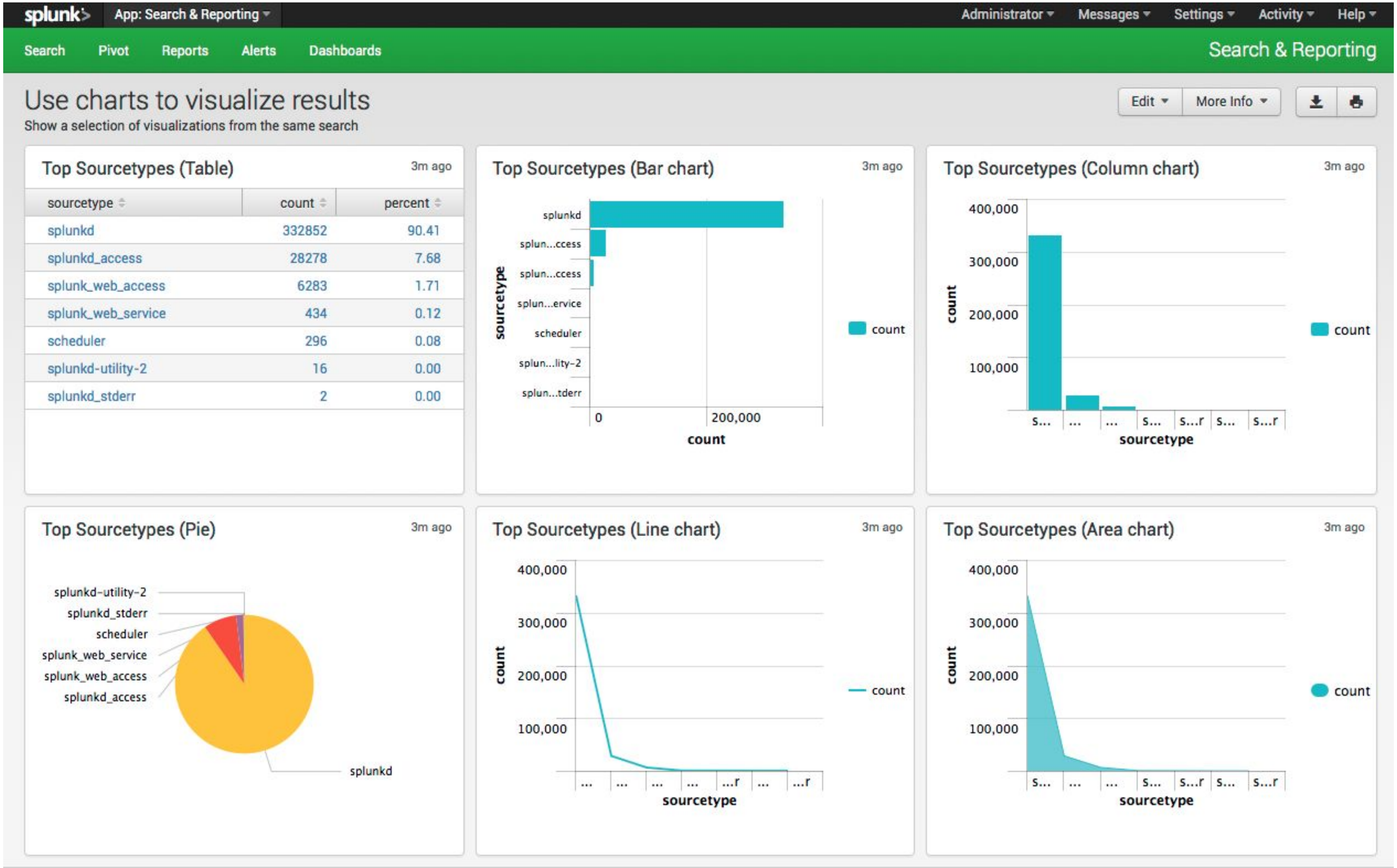
```
{ [-]
  Records: [ [-]
    { [-]
      awsRegion: us-east-1
      eventID: 10b62c18-657f-475f-8bbd-a52bc8658746
      eventName: AssumeRole
      eventSource: sts.amazonaws.com
      eventTime: 2018-01-20T22:36:45Z
      eventType: AwsApiCall
      eventVersion: 1.05
      recipientAccountId: [redacted]
      requestID: 64ce70a0-fe32-11e7-9466-b7002c04f9ea
      requestParameters: { [+]
      }
      resources: [ [+]
      ]
      responseElements: { [+]
      }
      sharedEventID: b79f3cdc-b45d-459c-a3ac-77598d4b2775
      sourceIPAddress: config.amazonaws.com
      userAgent: config.amazonaws.com
      userIdentity: { [+]
      }
    }
    { [+]
    }
    { [+]
    }
    { [+]
    }
    { [+]
    }
    { [+]
    }
  ]
}
```

Different functions

- Makes heavy use of “piping”
  - Directs the output of the first step to the second step
  - Example: **index=”snort” |table classification,name**
  - Makes a table of names and classifications from snort index
  - Basic searches don’t need piped
- **table, chart, top, head, tail, rex, stats, etc**

Dashboards

- Sexy data visualizations



Use charts to visualize results

Show a selection of visualizations from the same search

Top Sourcetypes (Table) 3m ago

sourcetype	count	percent
splunkd	332852	90.41
splunkd_access	28278	7.68
splunk_web_access	6283	1.71
splunk_web_service	434	0.12
scheduler	296	0.08
splunkd-utility-2	16	0.00
splunkd_stderr	2	0.00

Top Sourcetypes (Bar chart) 3m ago

Top Sourcetypes (Column chart) 3m ago

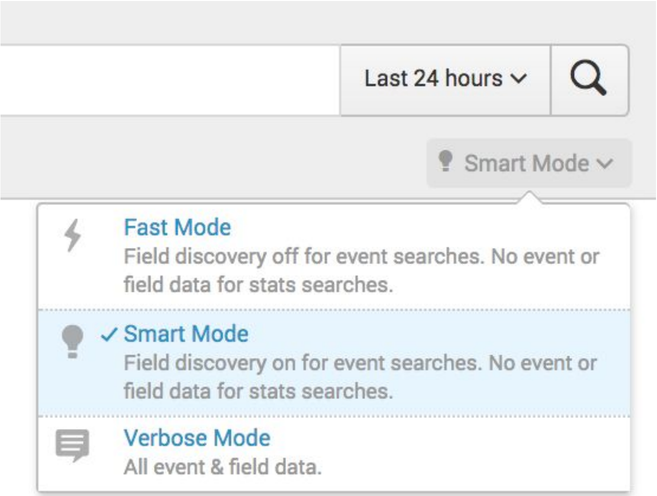
Top Sourcetypes (Pie) 3m ago

Top Sourcetypes (Line chart) 3m ago

Top Sourcetypes (Area chart) 3m ago

Quirks

- Search defaults to last 24 hour smart mode
- Default login: admin:changeme
  - You’re prompted to change, can skip though
- **By default, by design, you can ingest data from the server to search**
- API is off by default


Last 24 hours

Smart Mode

Fast Mode
Field discovery off for event searches. No event or field data for stats searches.

✓ Smart Mode
Field discovery on for event searches. No event or field data for stats searches.

Verbose Mode
All event & field data.

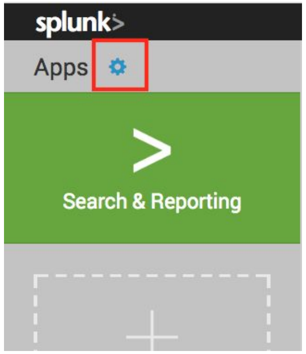
Demo

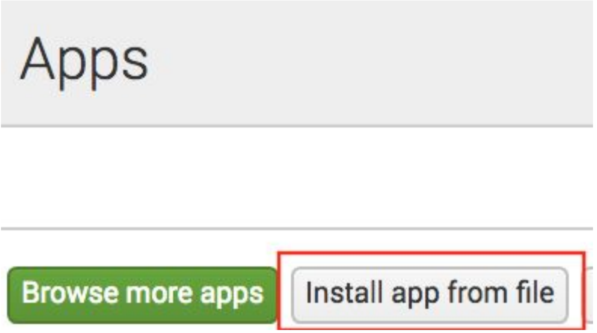
- Step 0: Register for **tctf.competitivecyber.club**
- Step 1: Log into **tctf.competitivecyber.club**
- Step 2: Go to **Love Your Logs** under challenges and download **solution.gz** and **splunk-for-snort_05.tgz**

http://35.171.89.40:8000

Step 1: Snort the Data

Click gear on the right, then click Install App from file to install the Snort App

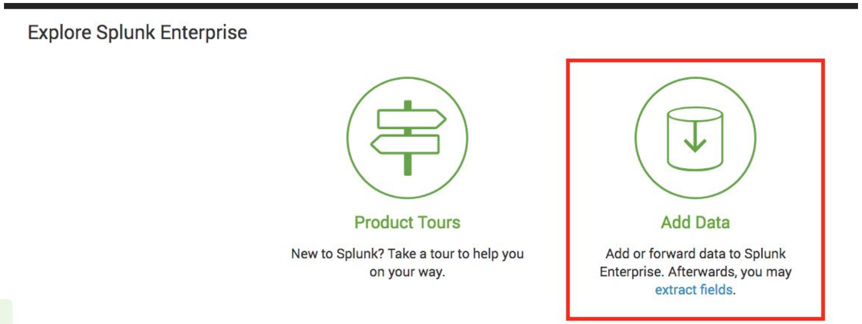




Select the app file (the snort file), upload, install, profit

Step 2: Add the data

Click Add Data on the homepage (click logo to go back), may require clicking dropdown



Explore Splunk Enterprise

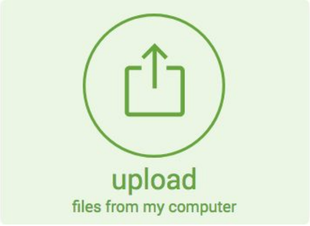
Product Tours

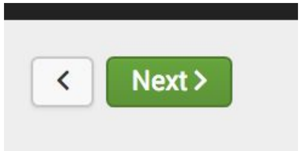
New to Splunk? Take a tour to help you on your way.

Add Data

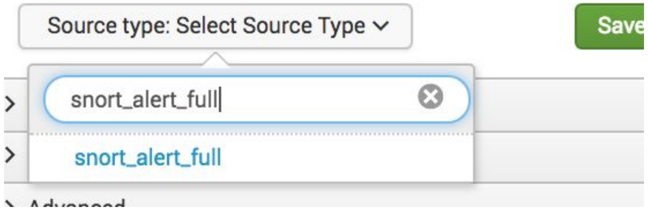
Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

Upload **solution.gz**

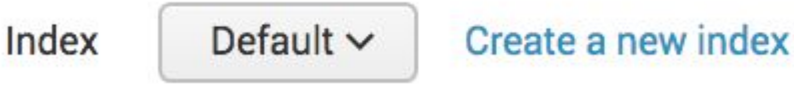




Select sourcetype as snort_alert_full



Create new index name “snort”, default options, press **Save** then **Next, Next, Submit**

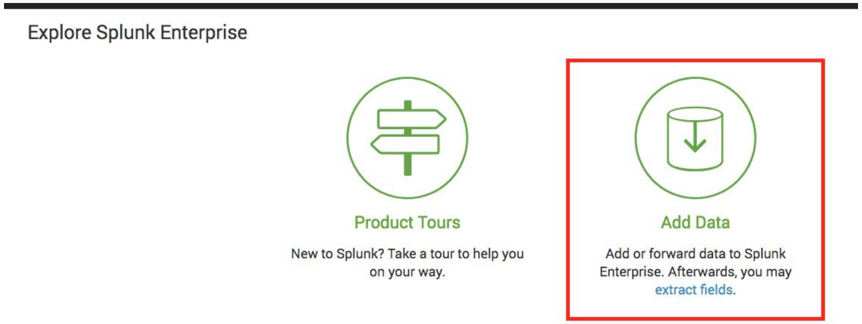


Step 3: Play around

Playing around live
I’ll be around to help

Pay careful attention to the actual text of the **Love Your Logs** challenge message, how it was written was very deliberate

Cleanup


Explore Splunk Enterprise

Product Tours
New to Splunk? Take a tour to help you on your way.
Add Data
Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

Docker:

docker kill $(docker ps -q)
docker rm $(docker ps -a -q)
docker rmi splunk/splunk

Other:

google the opposite of what you googled to get there
struggling? ask me or someone else

Proud Sponsors

Thank you to these organizations who give us their support:

BATTELLE

It can be done™