making sense of content security policy reports @ scale

ivan leichtling
ivanlei@yelp.com
@c0wl

How I Learned to Stop Worrying And Love Logs

Logs are the Heart of Security

If you don't know what's in your logs,

you don't know what's happening

- Detection
- Monitoring
- Alerting
- Incident Response
- Forensic Analysis
- Application Security

Remember, This Talk Applies to All Logs

We're talking about Content Security Policy reports.

This talk really applies to *all* your logs.

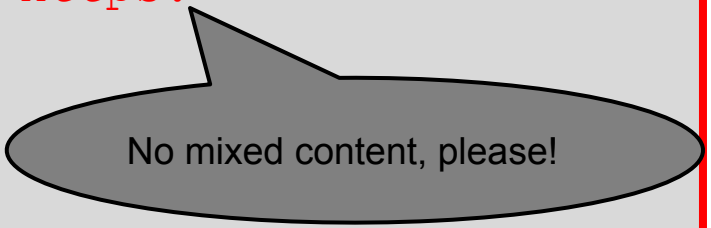
At least, it applies to all of ours.

So What's Content Security Policy

Some *newish* hotness for browser security.

Add a header to your HTTP response and get extra security in the browser.

```
HTTP/1.1 200 OK
Date: Thu, 13 Nov 2014 18:17:06 GMT
Content-Security-Policy: default-src https:
Content-Length: 1337
...
```



CSP Reports

Even better, let the browser tell us when something goes wrong.


```
HTTP/1.1 200 OK
Date: Thu, 13 Nov 2014 18:17:06 GMT
Content-Security-Policy: default-src https:; report-uri
https://biz.yelp.com/gimme_reports
Content-Length: 1337
...
```

No mixed content and
lemme know if it happens!

What's a Report Look Like?

I went to https://biz.yelp.com/foo but it loaded cooladvert.bro over HTTP and I showed a mix content warning.


```
{
 "csp-report": {
  "document_uri": "https://biz.yelp.com/foo",
  "blocked_uri": "http://www.cooladvert.bro/hmm?x=asdfnone",
  "referrer": "https://biz.yelp.com",
  "source_file": "https://biz.yelp.com/foo",
  "violated_directive": "script-src https:",
  "original_policy": "report-uri https://biz.yelp.com/gimme_reports; default-src
https:"
 }
}
```

Okay, We Made Sense of the Report

Is the Talk Over?

Reading one log line was easy.

But we've got lots of log lines.

Discard Unhelpful Reports

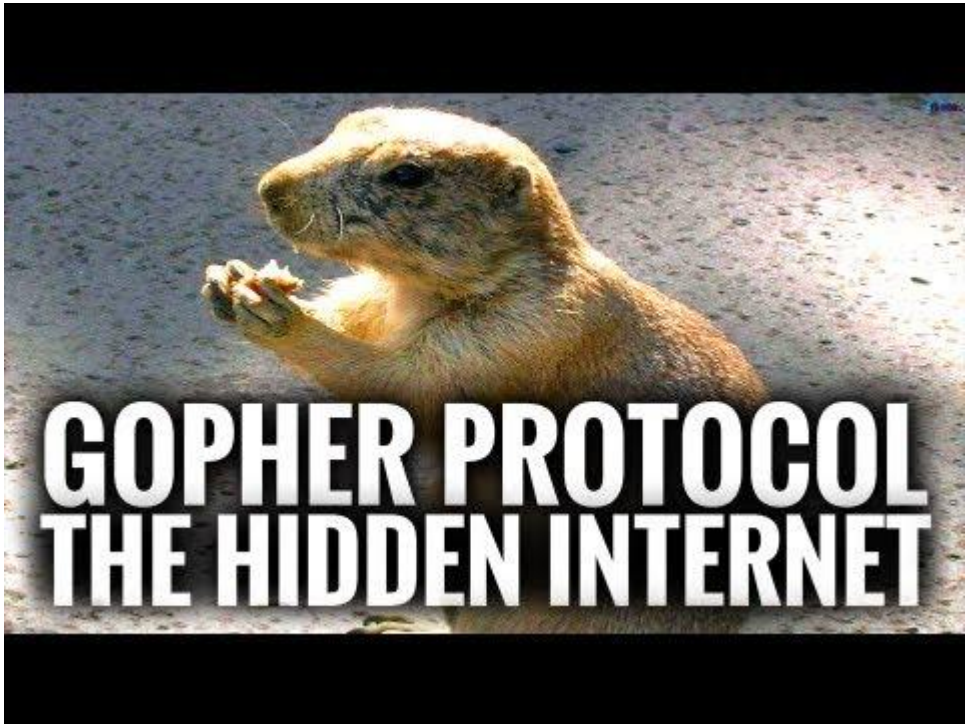
Get rid of malformed and malicious log lines

Web browser won't always work right... but POST endpoints will always receive malicious data.

Discard Unhelpful Reports

`blocked_uri` and `source_file` must start with `http`

- chromeinvoke://
- safari-extension://
- gopher://
- ...



Discard Unhelpful Reports

`document_uri` must be for the right domain

Imitation is the highest form of flattery…

but why do other sites copy my CSP headers?

- Client side ad injectors
- Weird proxy services
- People who read my blog post about CSP

Now Put the Logs in an Elk

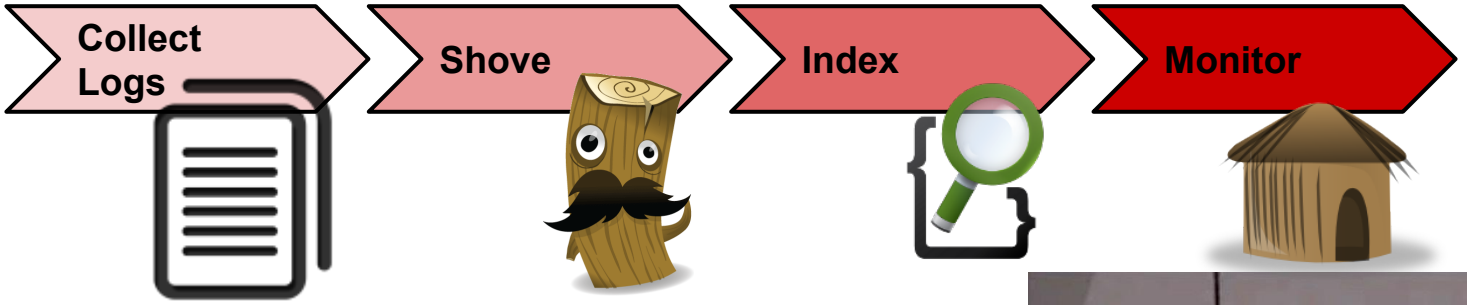
Not Logs In That Elk, Logs In This ELK!

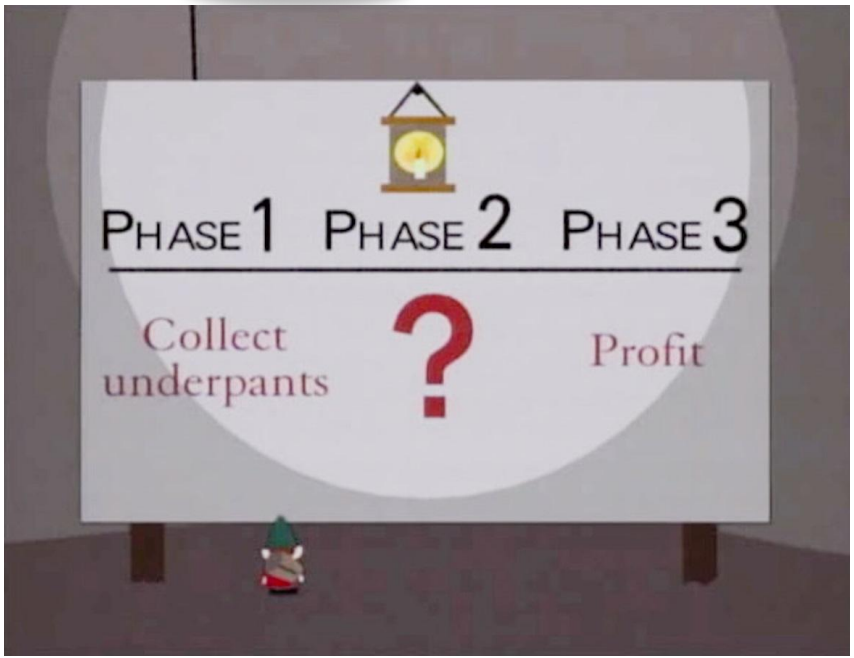
elasticsearch.

logstash

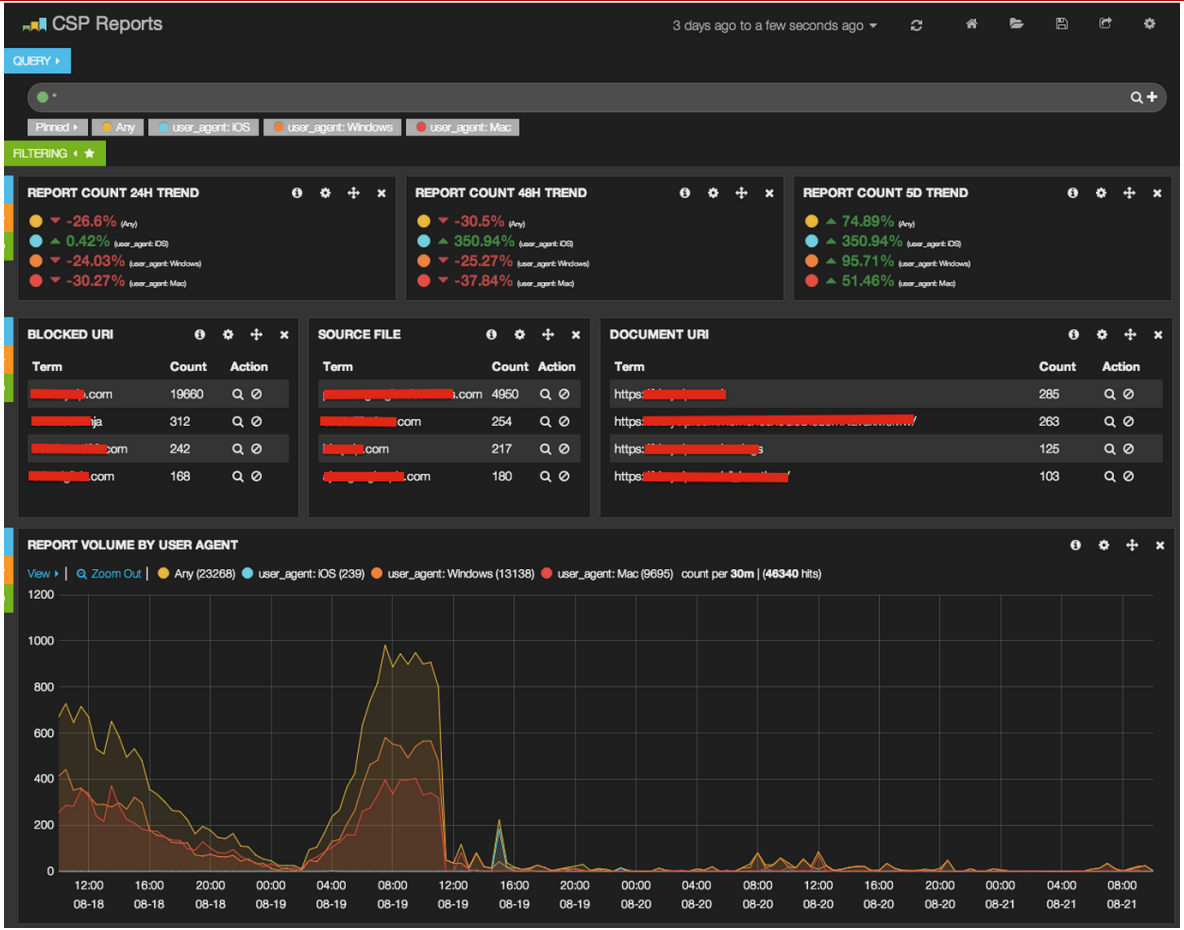
kibana

This Is How We Go From Log to Profit





Monitoring CSP Reports With Kibana

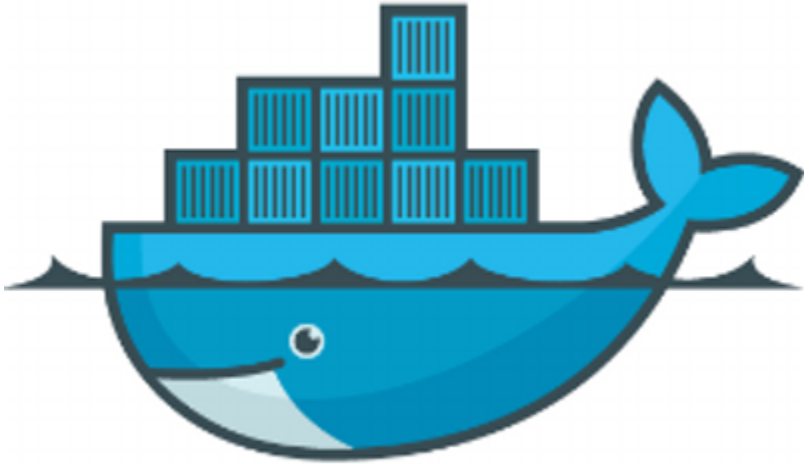


Yay!

Looks Complicated, Really It's Easy

yelp

You could go from 0 to ELK stack in ~5 minutes using a docker container



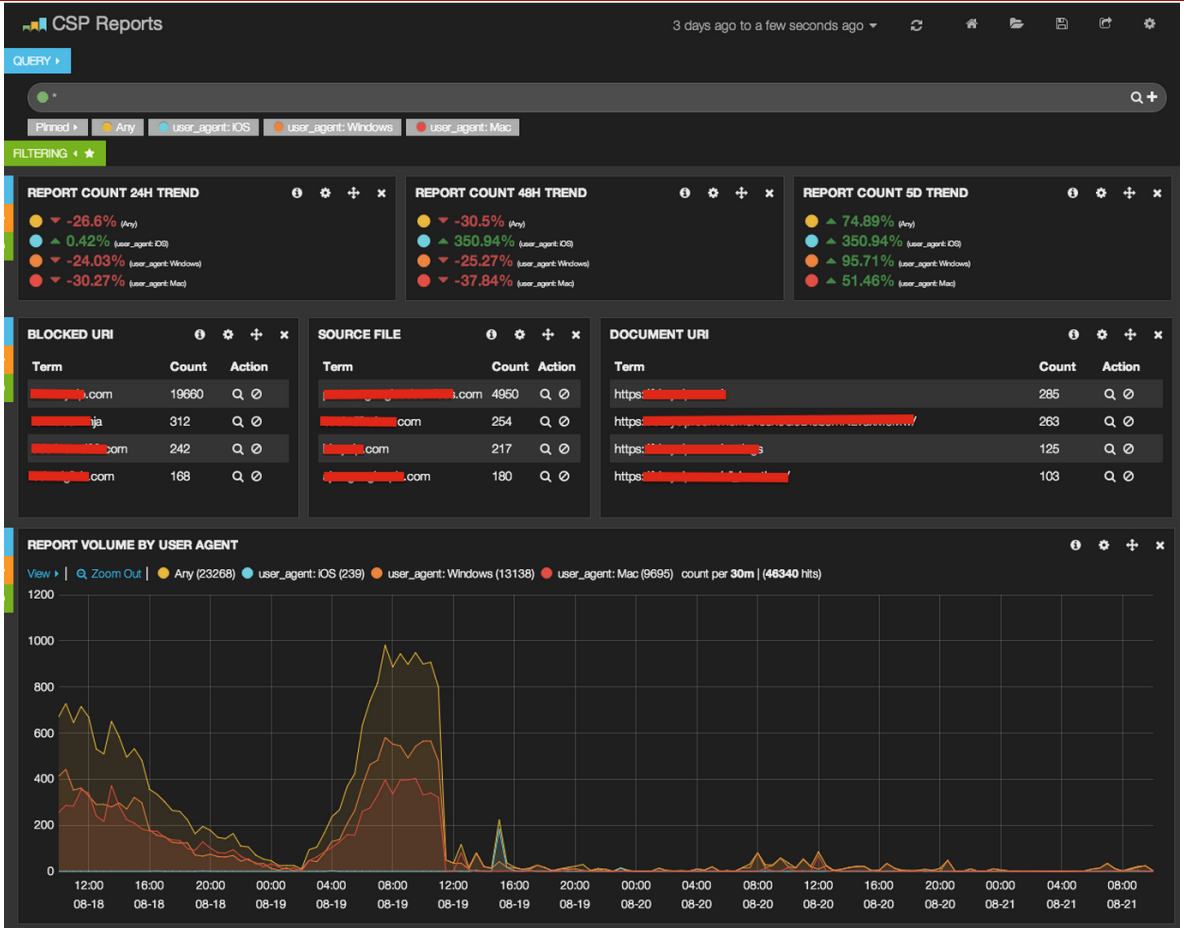
Here's the Logstash Config

```
$ /opt/bin/logstash -f ./csp_logstash.conf
```

```
input {
    pipe {
        command => "scribereader --tail csp_reports"
        codec   => "json"
    }
}

output {
    elasticsearch {
        host     => "elasticsearch-csp-elb"
        port     => 31337
        index    => "logstash-csp-reports-%{+yyyy.MM.dd}"
        protocol => "http"
    }
}
```

This Dashboard Took ~10 Min to Create

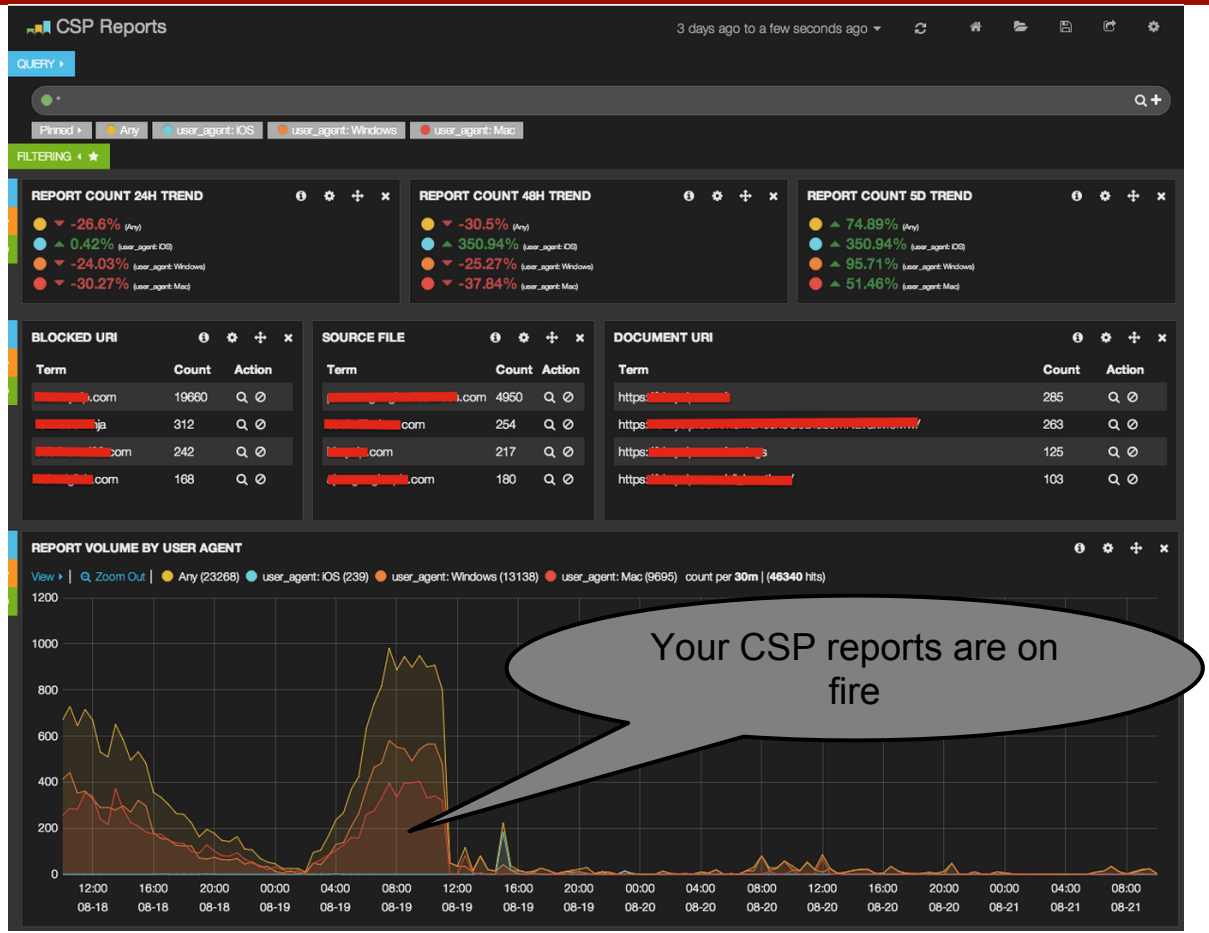


FAST!

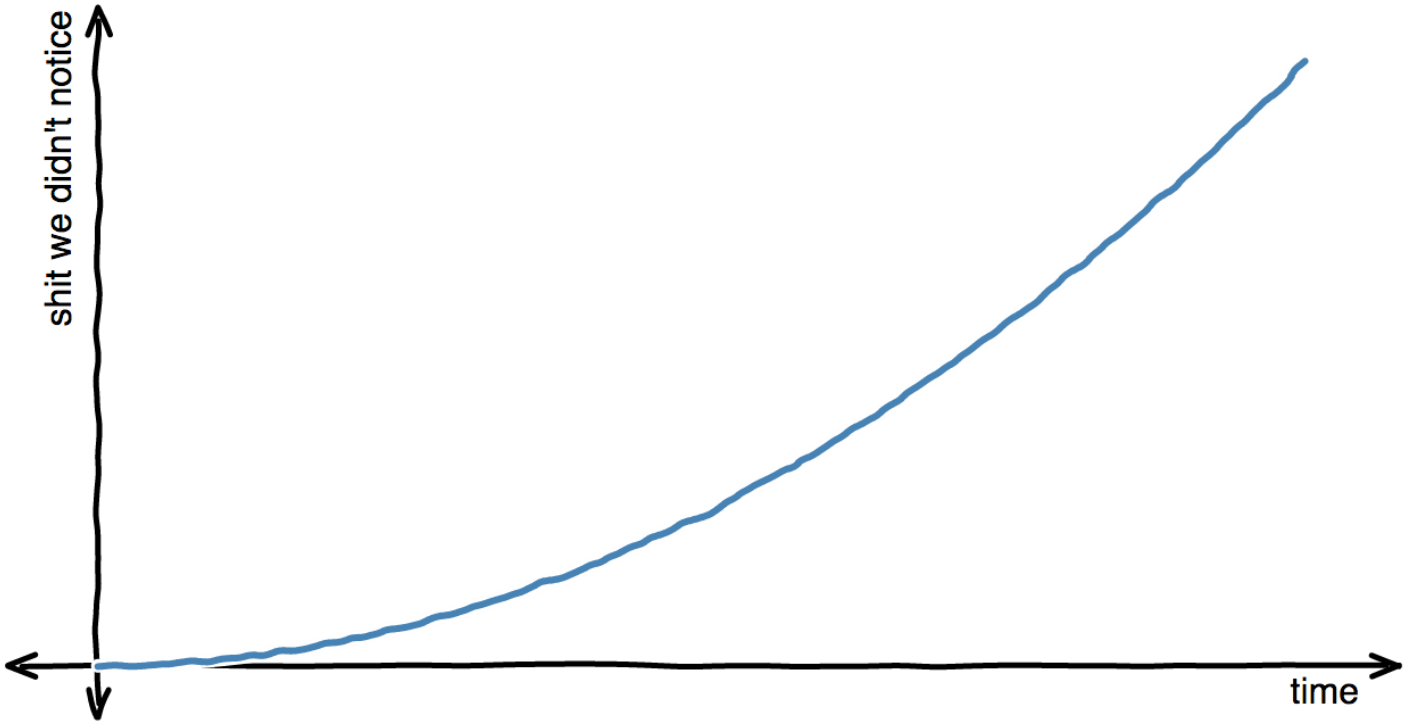
Monitor Anything? Call Me Interested!

Did You Notice This Spike?

Your security team is watching an animated gif

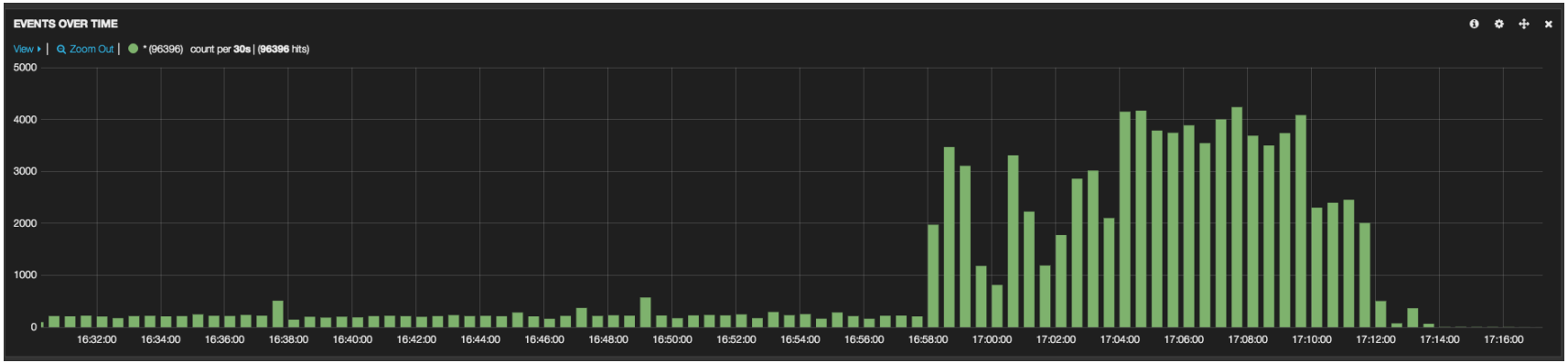


How Graphs Work For Security



Don't Stop At Monitoring, You Need Alerts!

How Does Yelp Alert When This Happens?



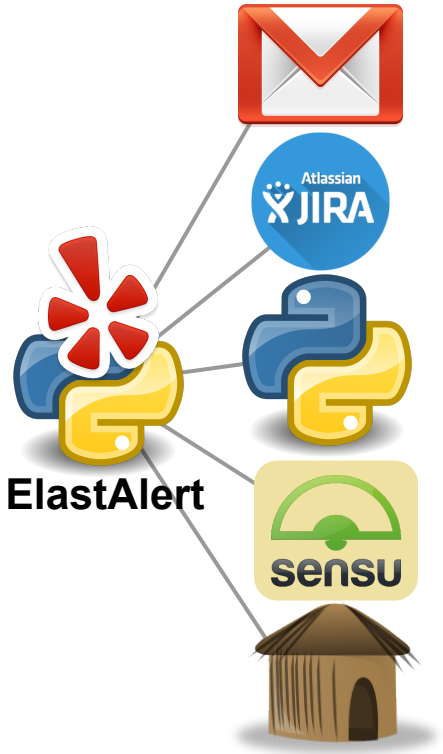
ElastAlert - Generic Alerting From ElasticSearch

```
# Usually our yaml files have more comments in them
es_host: "elasticsearch-csp-elb"
es_port: 31337
index: "logstash-csp-reports"

name: "CSP report spike"
type: "spike"
hours: 2
spike_height: 3

query: "csp.yelp_site=='biz'"

alert: "email"
email: "hey-csp-just-spiked@yelp.com"
```



ElastAlert - Highly Flexible Alerting & Workflows

yelp

Rules Types

- Spike
- Flatline
- Blacklist
- Whitelist
- Frequency

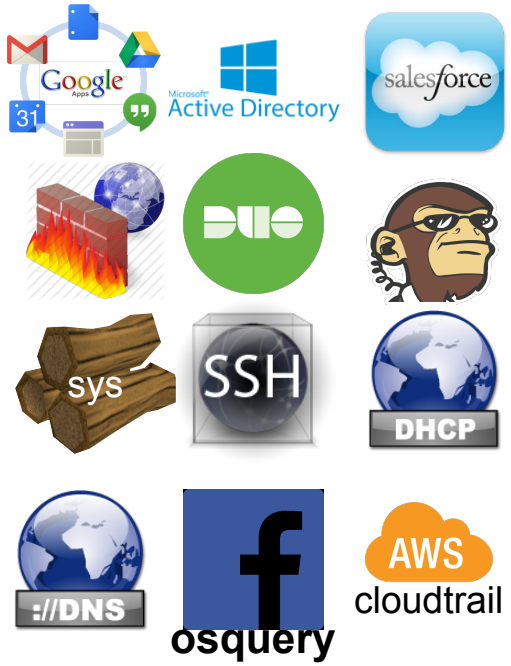
Alert Types

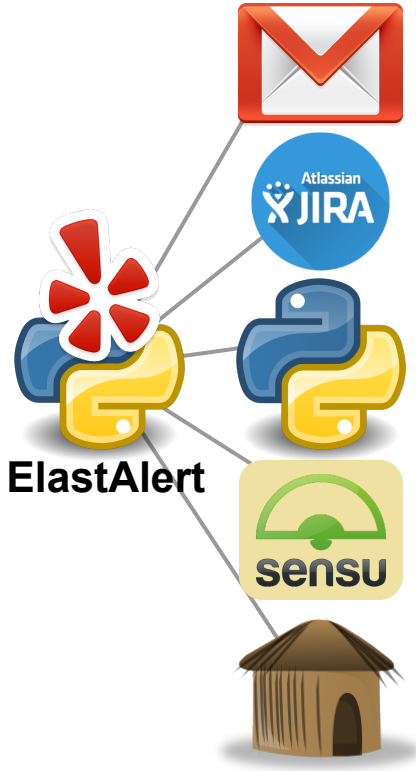
- Email
- JIRA
- Sensu
- Custom Action
- Stdout

Make Sense of Any Log @ Scale

yelp

Collect All Logs → Shove Through Logstash → Index in ElasticSearch → **Visualize with Kibana Alert with ElastAlert**






Questions?
ivan leichtling
ivanlei@yelp.com
@c0w1
WORLD TARGETS IN MEGADEATHS
WAR ALERT ACTIONS BOOK