

AWS

S U M M I T

ELK in the wild – Real life log analysis on AWS

Asaf Yigal, VP Product Co-Founder, Logz.io

May 2017



Who Am I?

Asaf Yigal – VP Product ,
Logz.io

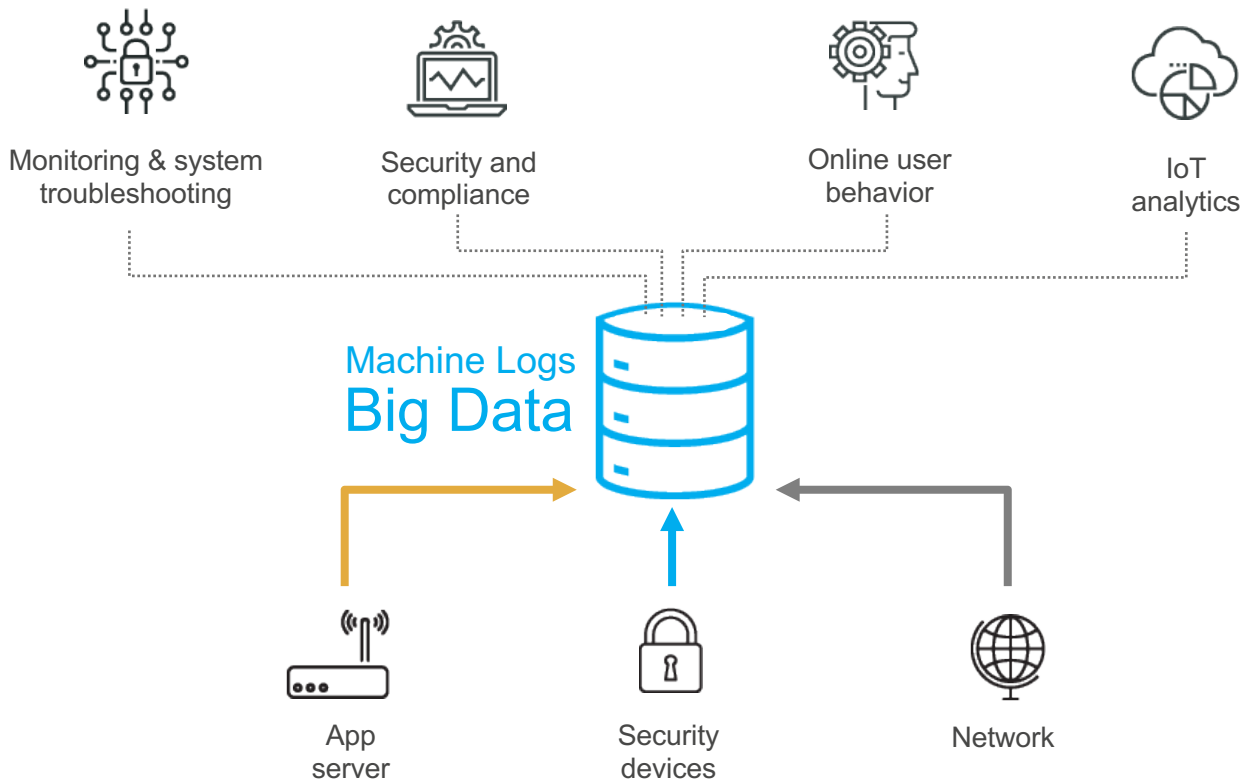
1,000 companies from
80 different countries use
Logz.io



Agenda

- Why log analysis is important ?
- Introducing ELK
- Security at British Airways
- DDoS attack detection at Dyn

Fundamental to Understanding Machines



Open Source ELK +/-



Simple and beautiful

It's simple to get started and play with ELK and the UI is just beautiful



Open Source

The largest user base with a vibrant open source community that supports and improves the product



Fast. Very fast.

Built on the Elasticsearch search engine, ELK provide blazing quick responses even when searching through millions of documents



Not Production Ready

Building production ready ELK deployment is a great challenge organization face. With hundreds of different configurations and support matrix, making sure it's always up is difficult



Hard to Scale

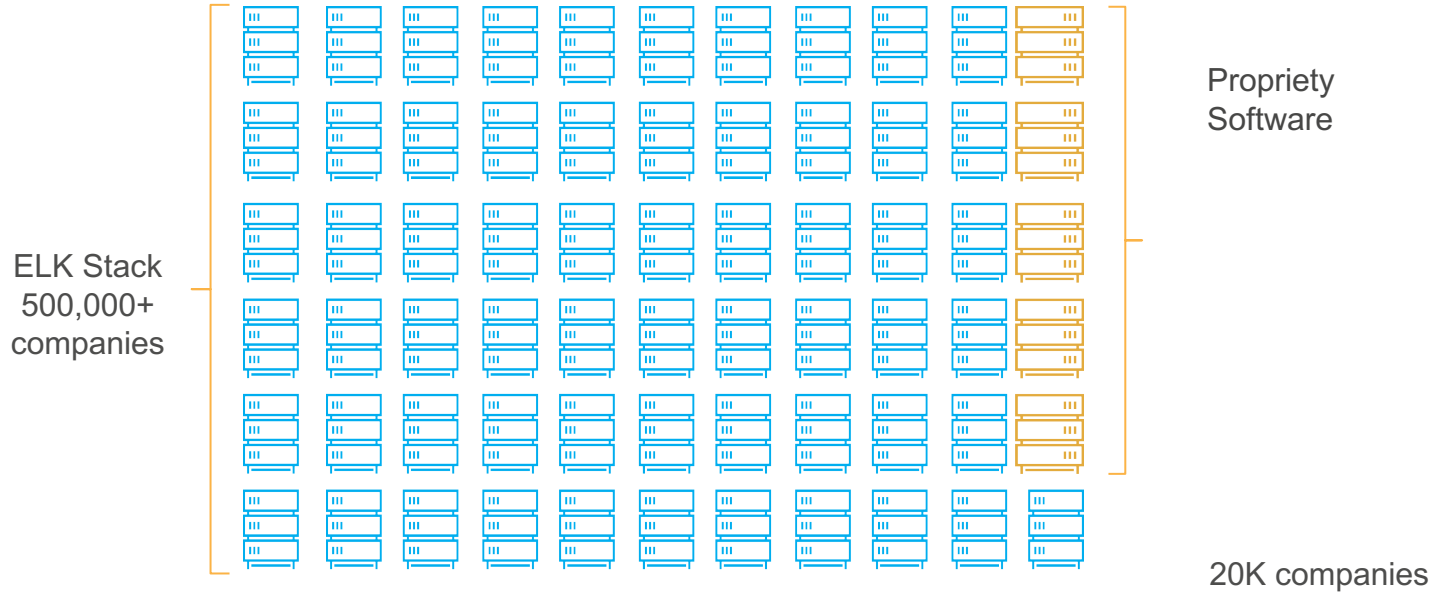
Data piles up and organization experience usage bursts. It's super-complex building elastic ELK deployments that can scale up and down



Poor Security

Logs include sensitive data and open source ELK offers no real security solution, from authentication to role based access

ELK Stack 2017



Simple and beautiful



Open Source/Flexible



Fast. Very fast.

Production Requirements

1. No logs should be dropped (trivial, ah)
2. Highly Available
3. Secure which means encryption and access control
4. Index management, shard allocation
5. Data should be parsed and mapping configured
6. Data should be retained for x days
7. Configuration management and monitoring
8. Data spikes should handled up to 10x normal capacity
9. Visualization and dashboards
10. Archive long retention
11. Alerts

Security at British Airways

Challenges

Why Logz.io

ELB Health

Discover Visualize **Dashboard** Settings

Last 24 hours

ELB - Traffic Health

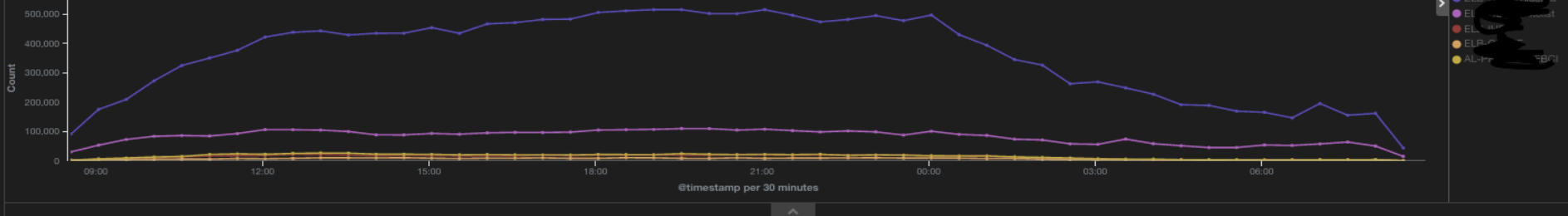
Filter...



Contribute



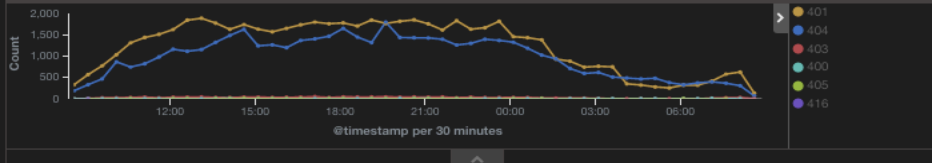
ELB - All ELB Traffic By ELB



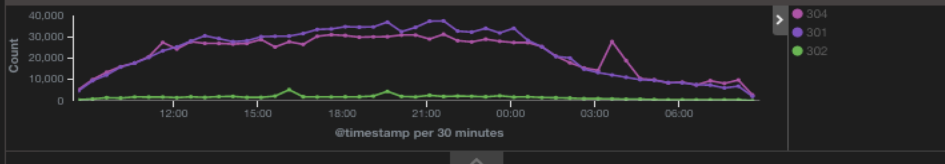
ELB - Backend Responses 2XX



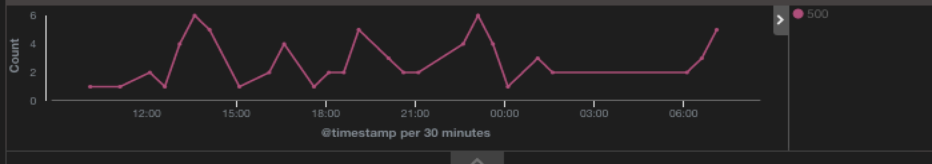
ELB - Backend Responses 4XX



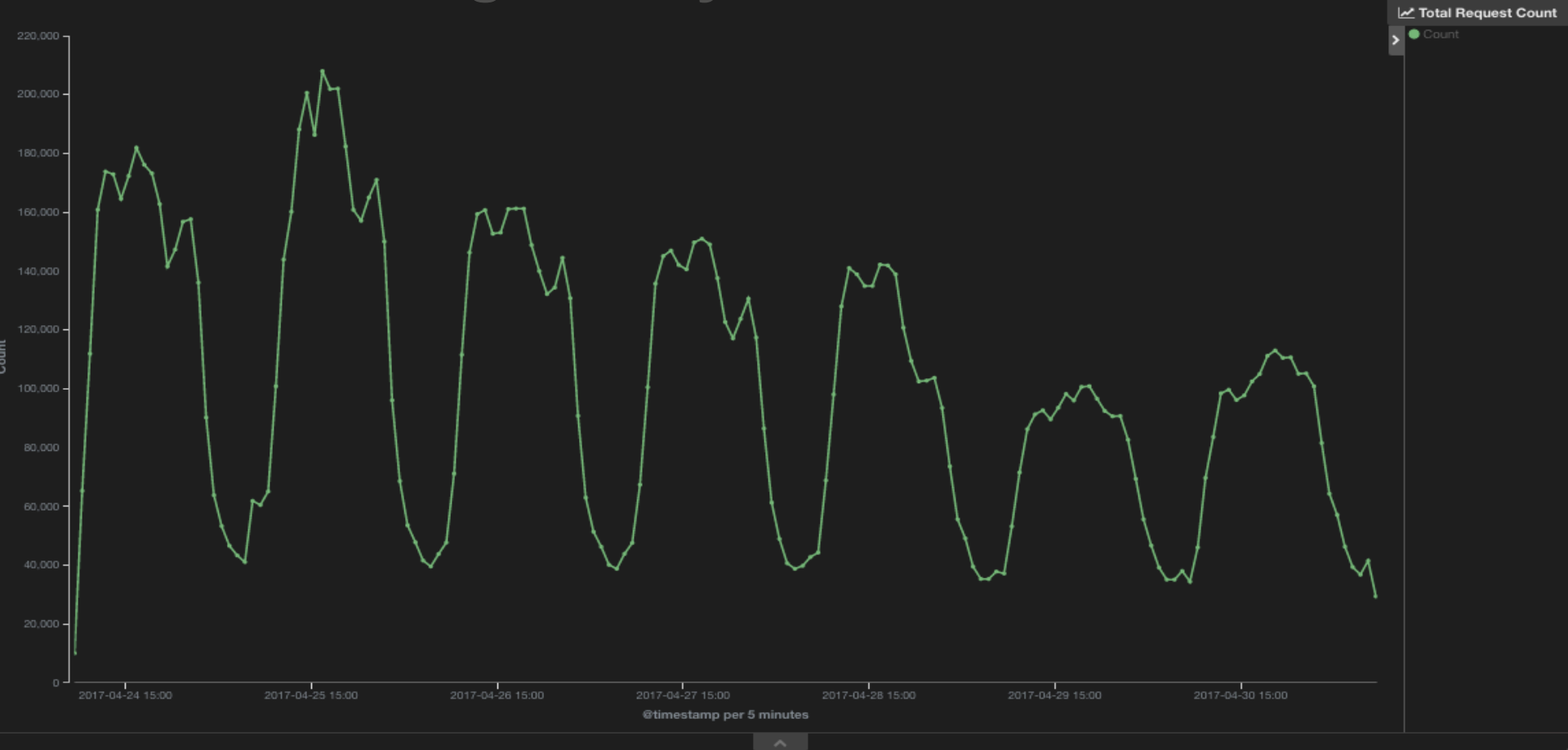
ELB - Backend Responses 3XX



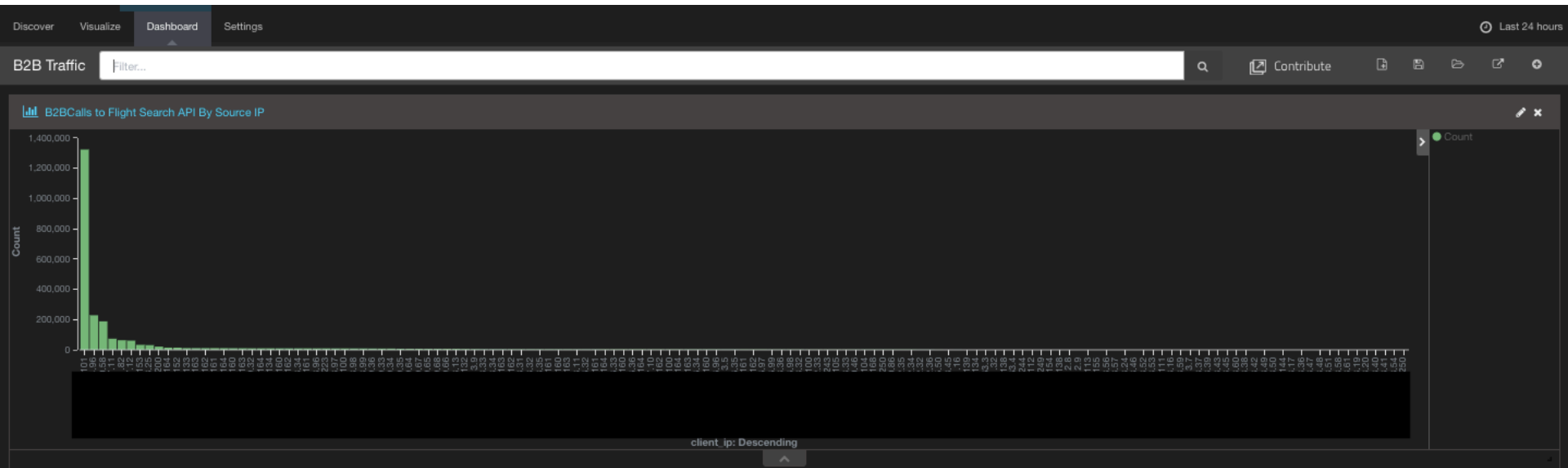
ELB - Backend Responses 5XX



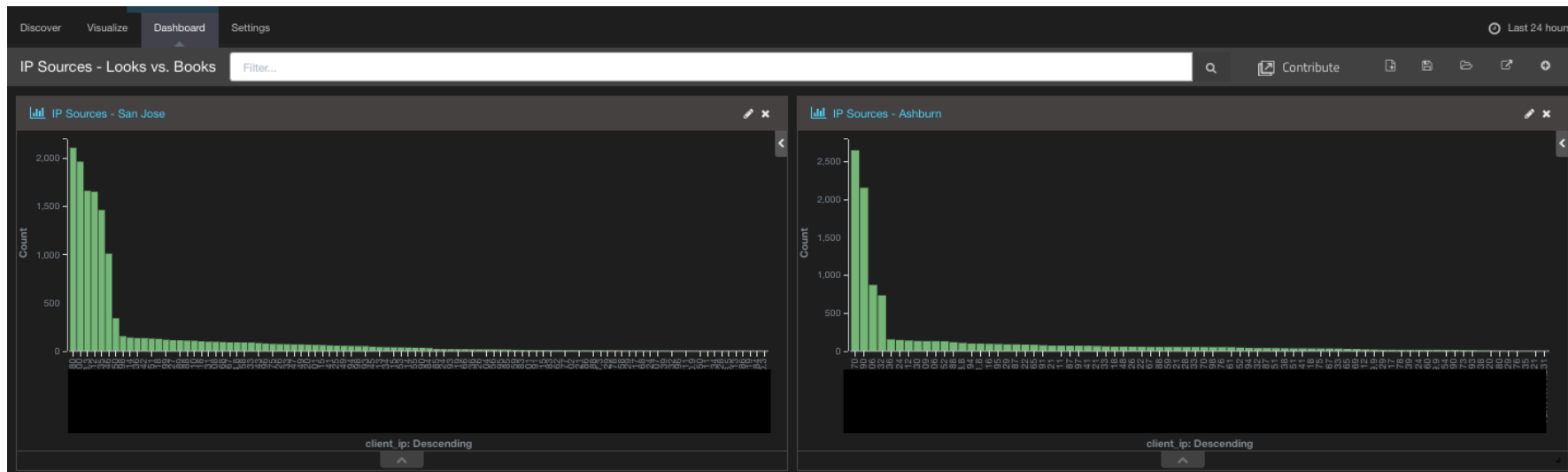
Understanding Weekly trends



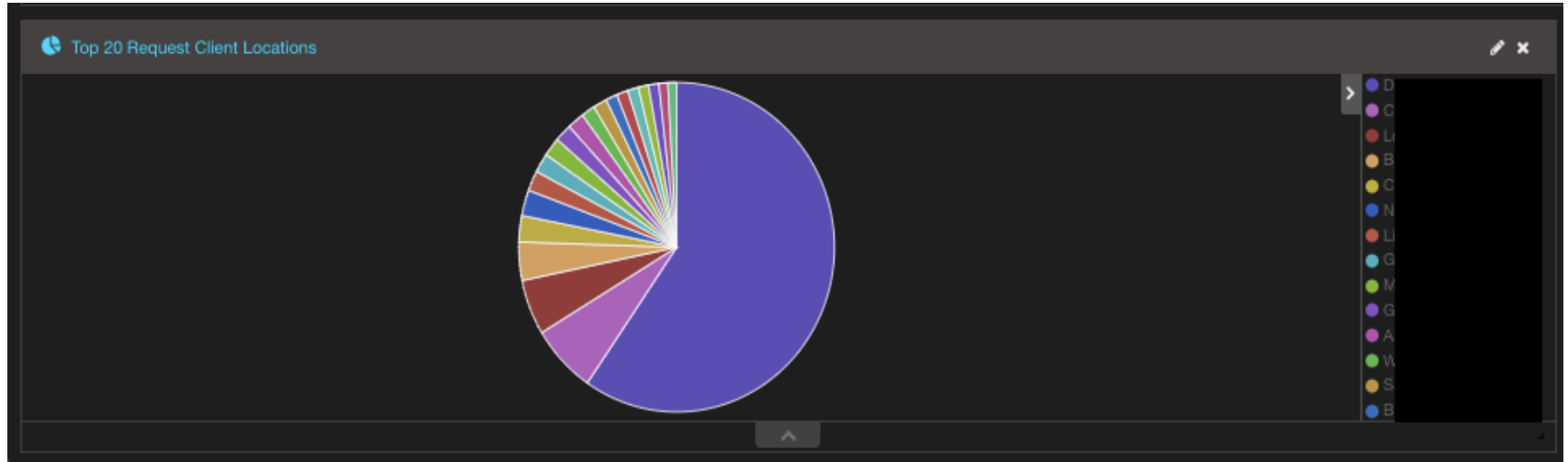
Understanding who is crawling the site



Understanding traffic



Understanding Client Location

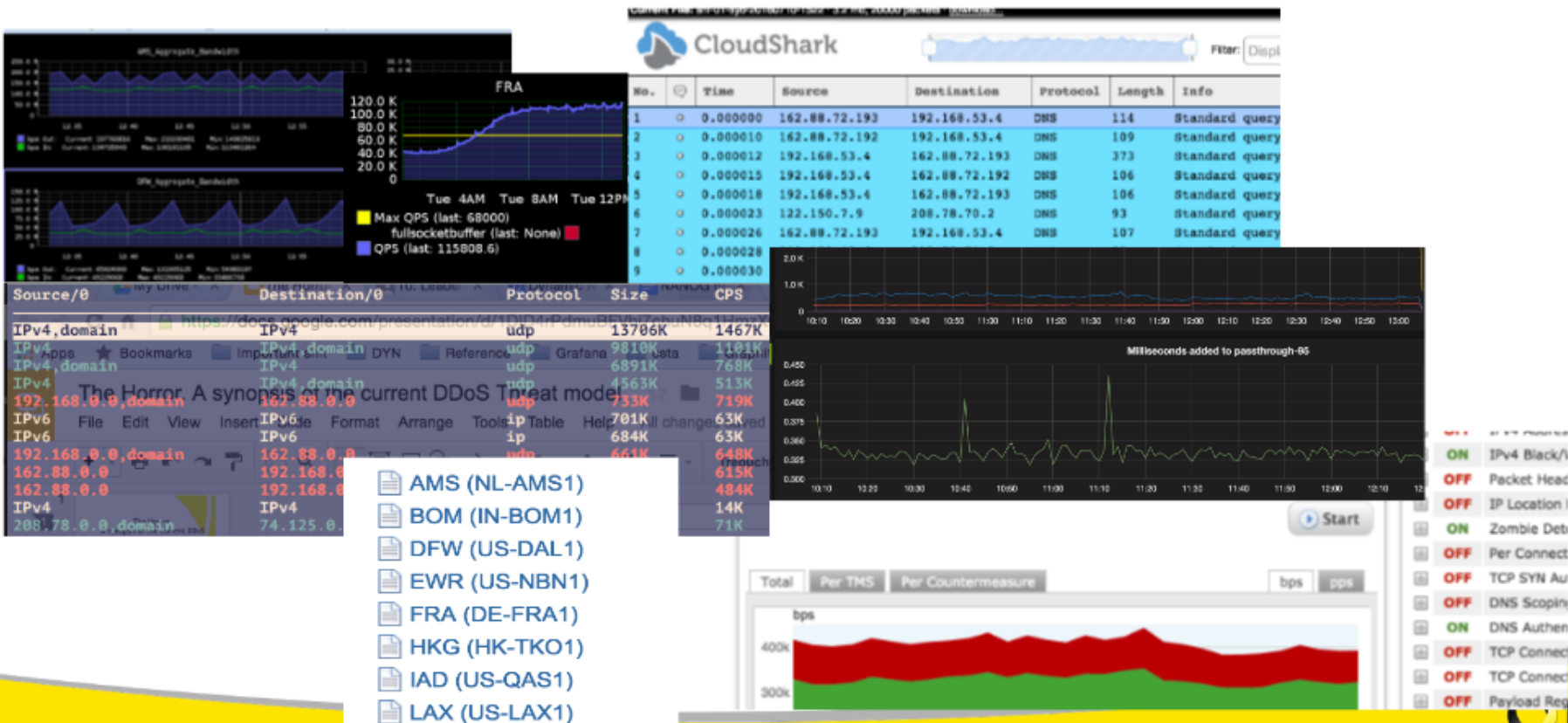


DDoS attacks detection at Dyn



https://img.memesuper.com/182956f180cfb7a8c95d6dda68a1d351_you-get-a-ddos-attack-ddos-meme_625-468.jpeg

Numerous methods of detection



Understand Normal

- We leverage monitoring to define normal.
- We alert in reasonable ways when critical metrics become abnormal
- Too many alerts and your “teams tasked with reactive reliability” will get burned out.
- Normal shouldn't be subjective. Socialize your key performance indicators!



Logz.io Alerts APP 02:03

IPFIX - Too many inbound packets

Description

<https://goo.gl/RaAW9G>

Severity

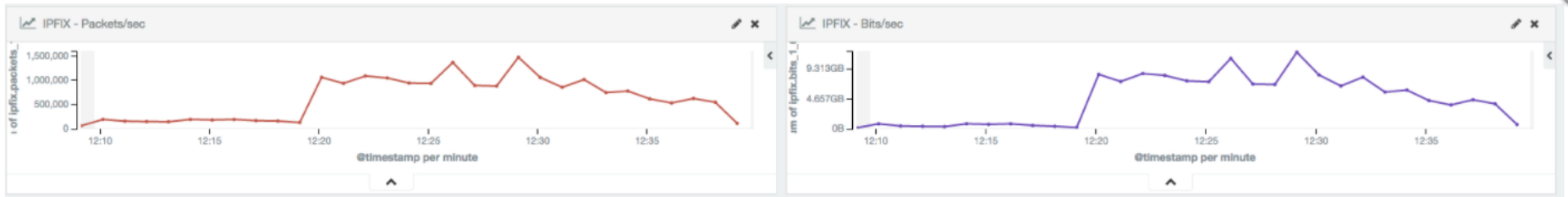
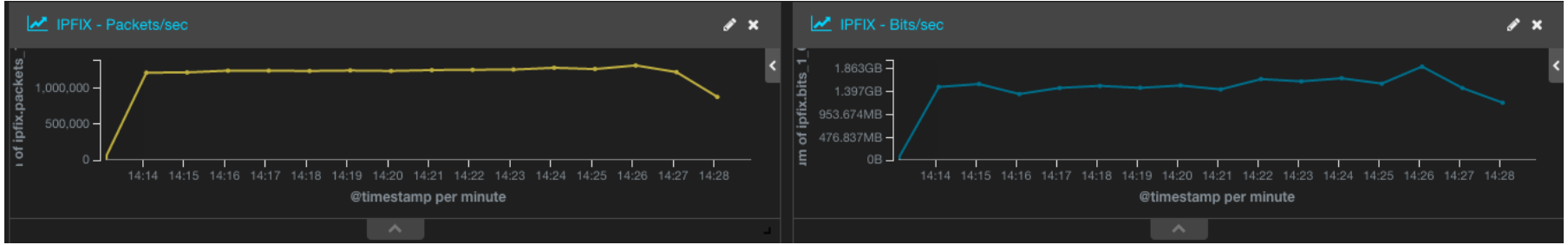
MEDIUM

Alert event samples

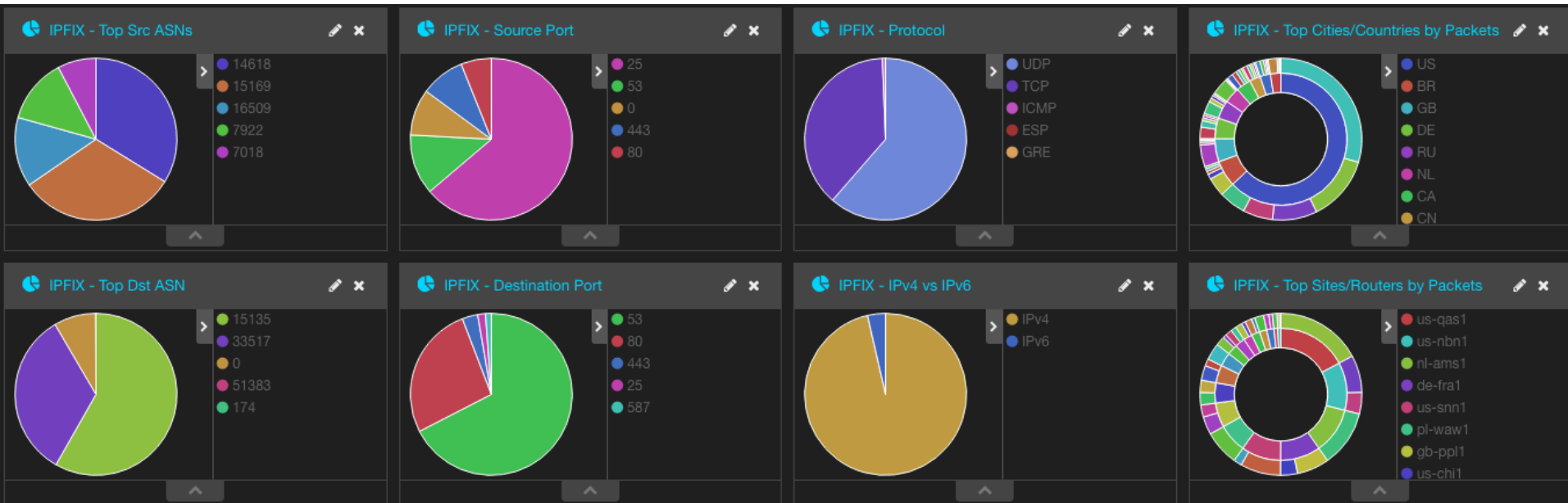
The following have met the alert condition:

```
[[  
  "ipfix.sourceIPv4Address" : "1[REDACTED]9",  
  "ipfix.packetDeltaCount" : 2835000.0  
]]
```

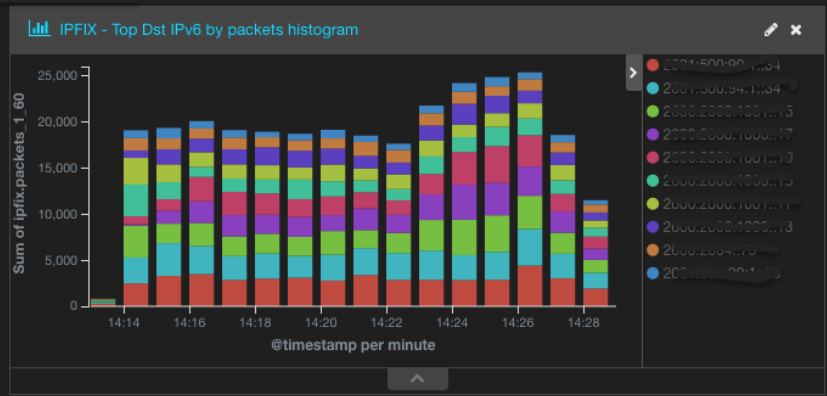
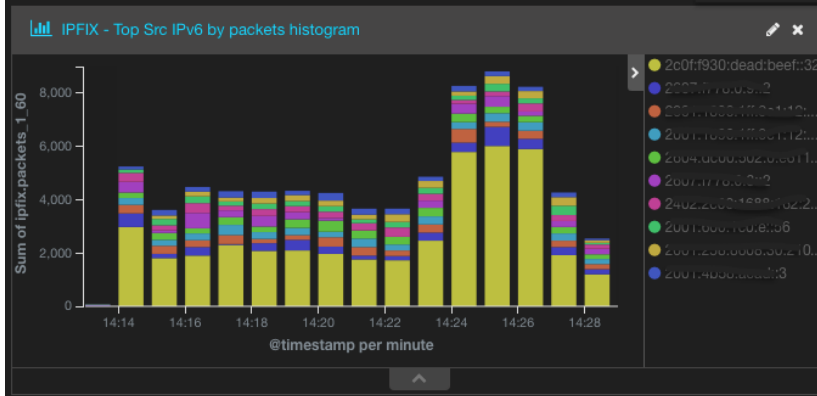
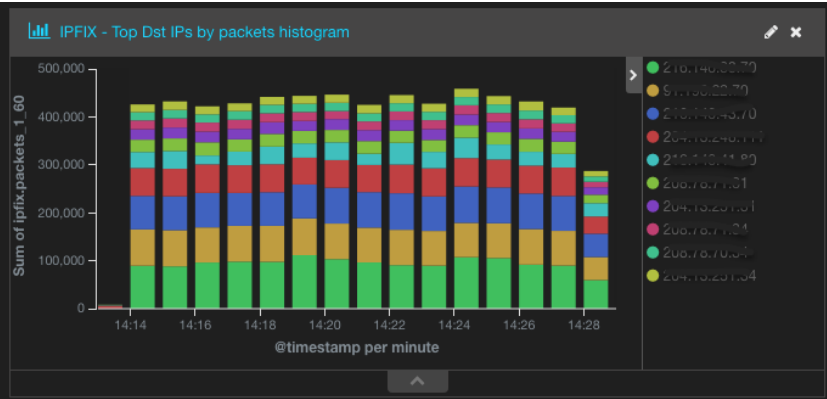
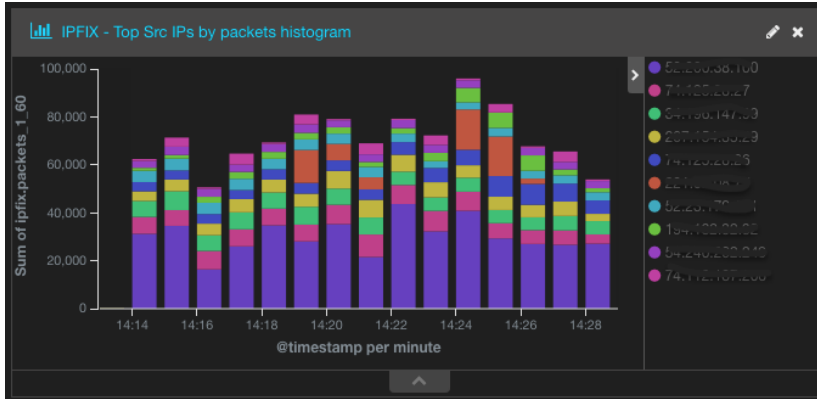
Netflow



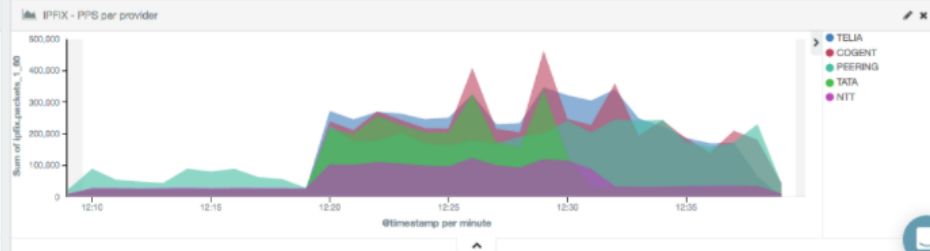
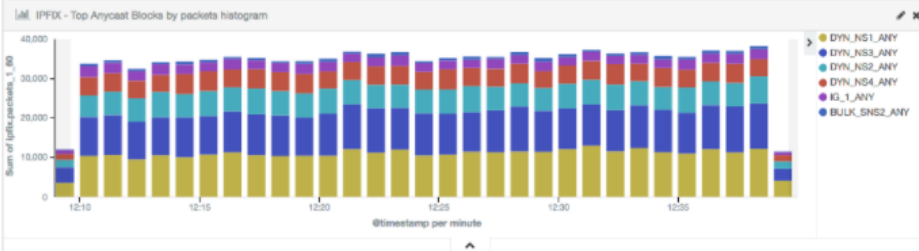
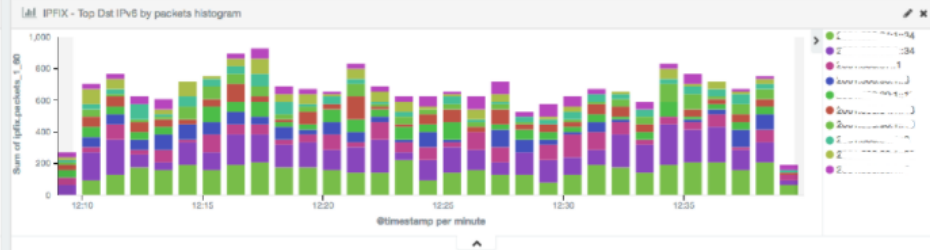
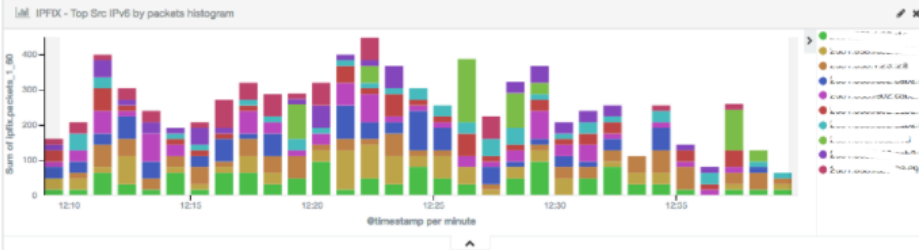
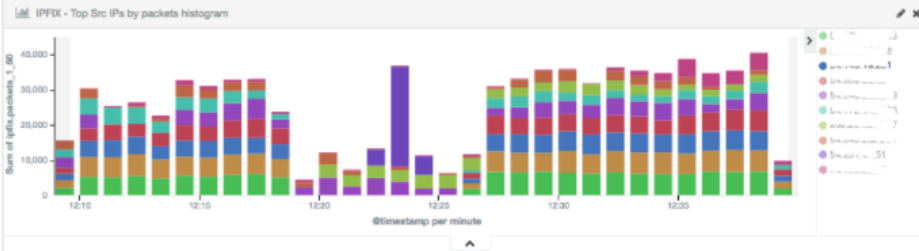
Fast breakdown of SRC & DST port, proto, ASN, Site, etc.



Quick sort and analysis of v4 and v6 IPs



Examples of attack



How to Learn More

- Lots of resources online
- Try the Logz.io blog for detailed guides, benchmarks and troubleshooting guides on building ELK stacks
- @logzio
- @asafyigal

AWS

S U M M I T

Asaf Yigal (@asafyigal)
Logz.io (@logzio)

